

SISTEMAS INFORMÁTICOS

DESARROLLO DE APLICACIONES WEB

Ilerna

ILERNA

© Ilerna Online S.L., 2021

Maquetado e impreso por Ilerna Online S.L.

© Imágenes: Shutterstock

Impreso en España - Printed in Spain

Reservado todos los derechos. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin autorización previa y por escrito de los titulares del copyright. La infracción de dichos derechos puede constituir un delito contra la propiedad intelectual.

Ilerna Online S.L. ha puesto todos los recursos necesarios para reconocer los derechos de terceros en esta obra y se excusa con antelación por posibles errores u omisiones y queda a disposición de corregirlos en posteriores ediciones.

1.^a edición: enero 2021

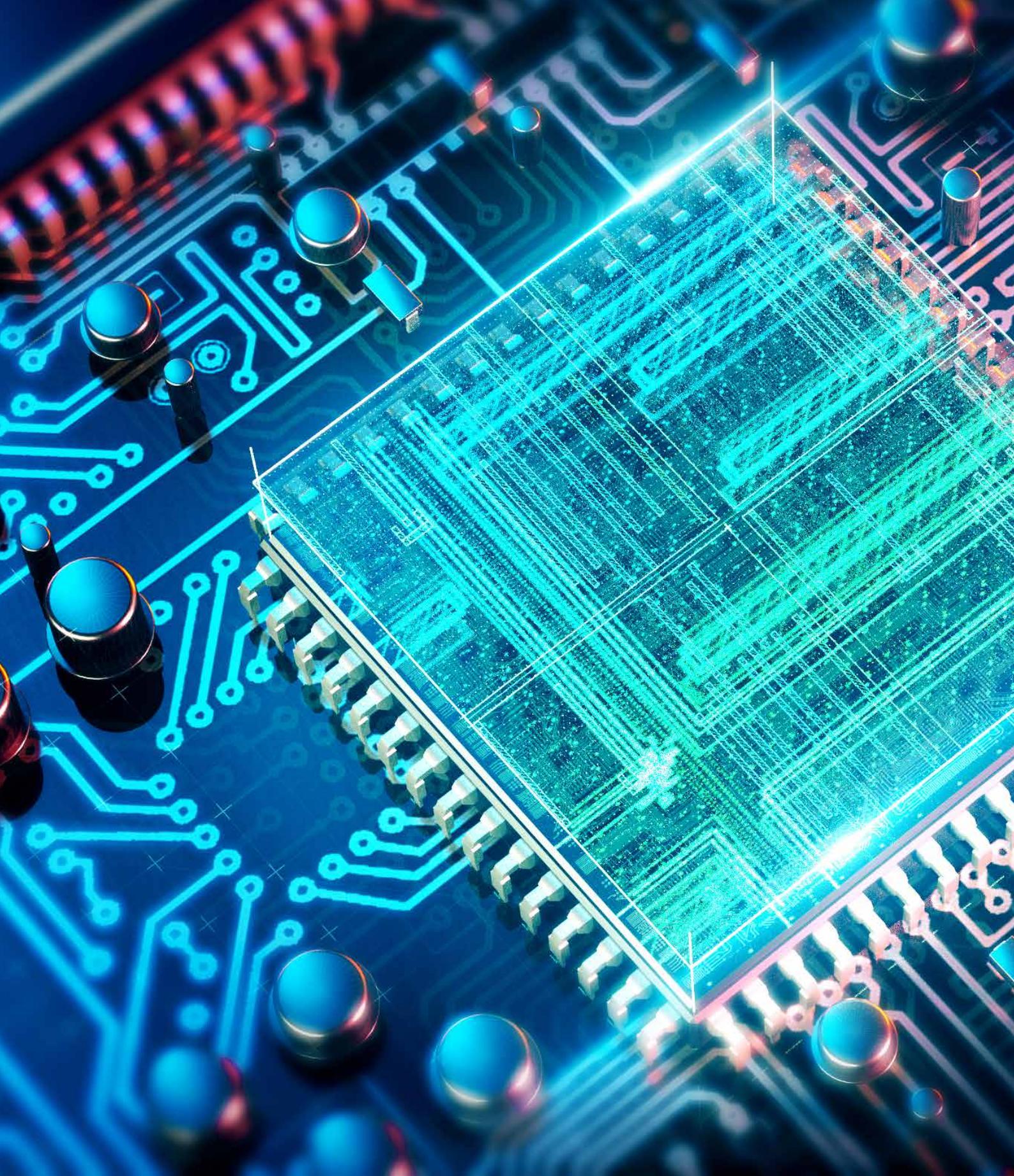
ÍNDICE

Sistemas informáticos

1. Instalación software libre y propietario.....	6
1.1. Estructura y componentes de un sistema informático.	
Periféricos y adaptadores para la conexión de dispositivos.....	7
1.2. Tipos y topologías de red.....	14
1.3. Mapa físico y lógico de una red.....	19
1.4. Arquitectura de un sistema operativo	23
1.5. Funciones del sistema operativo.....	25
1.6. Tipos de sistemas operativos	27
1.7. Tipos de aplicaciones.....	29
1.8. Licencias y tipos de licencias.....	30
1.9. Gestores de arranque.....	31
1.10. Máquinas virtuales	32
1.11. Consideraciones previas a la instalación de sistemas operativos libres y propietarios	35
1.12. Instalación de sistemas operativos. Requisitos, versiones y licencias	36
1.13. Instalación y desinstalación de aplicaciones. Requisitos, versiones y licencias.....	41
1.14. Actualización de sistemas operativos y aplicaciones	44
1.15. Archivos de inicio de sistemas operativos.....	46
1.16. Registro del sistema.....	47
1.17. Actualización y mantenimiento de controladores de dispositivos	49
2. Administración de software de base.....	52
2.1. Administración de usuarios y grupos locales	53
2.2. Seguridad de cuentas de usuario.....	57
2.3. Seguridad de contraseñas	59
2.4. Configuración del protocolo TCP/IP. Direcciones IP y máscaras de subred.....	62
2.5. Servicio de Nombres de Dominios (DNS).....	66
2.6. Archivos de configuración de red.....	68
2.7. Optimización de sistemas para ordenadores portátiles. Archivos de red sin conexión	70
2.8. Principales comandos de sistemas operativos libres y propietarios.....	72

3. Administración de la información.....	74
3.1. Sistema de archivos	75
3.2. Tipos de sistemas de archivos.....	76
3.3. Gestión de sistemas de archivos mediante comandos y entornos gráficos	77
3.4. Gestión de enlaces	80
3.5. Estructura de directorios de sistemas operativos libres y propietarios.....	84
3.6. Búsqueda de información del sistema mediante comandos y herramientas gráficas	86
3.7. Identificación del software instalado mediante comandos y herramientas gráficas	90
3.8. Gestión de la información del sistema. Rendimiento. Estadísticas.....	92
3.9. Montaje y desmontaje de dispositivos en sistemas operativos .	94
3.10. Automatización.....	97
3.11. Herramientas de administración de discos. Particiones y volúmenes. Desfragmentación y revisión	102
4. Administración de dominios	106
4.1. Estructura cliente-servidor.....	107
4.2. Protocolo LDAP	108
4.3. Concepto de dominio. Subdominios. Requisitos necesarios para montar un dominio	111
4.4. Conceptos clave de Active Directory	119
4.5. Administración de cuentas. Cuentas predeterminadas	121
4.6. Contraseñas. Bloqueos de cuenta. Cuentas de usuarios y equipos	124
4.7. Perfiles móviles y obligatorios	127
4.8. Carpetas personales.....	129
4.9. Plantillas de usuario. Variables de entorno.....	131
4.10. Administración de grupos. Tipo. Estrategias de anidamiento. Grupos predeterminados.....	135
4.11. Instalación de Windows Server y Ubuntu Server	138
5. Administración del acceso al dominio	140
5.1. Equipos de dominio	141
5.2. Permisos y derechos	142
5.3. Administración del acceso a recursos. Samba. NFS	144

5.4.	Permisos de red. Permisos locales. Herencia. Permisos efectivos	147
5.5.	Delegación de permisos	151
5.6.	Listas de control de acceso (ACL Access Control List)	152
5.7.	Directivas de grupo. Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbito de las directivas. Plantillas	154
6.	Resolución de incidencias y asistencia técnica	156
6.1.	Interpretación, análisis y elaboración de documentación técnica. Interpretación, análisis y elaboración de manuales de instalación	157
6.2.	Instalación y configuración de sistemas operativos y aplicaciones. Licencias de cliente y licencias de servidor	163
6.3.	Instalaciones desatendidas e implementación de archivos de respuesta	167
6.4.	Servidores de actualizaciones automáticas	170
6.5.	Partes de incidencias y protocolos de actuación	172
6.6.	Administración remota	176
	Bibliografía / webgrafía	179
	Solucionario	180



1

INSTALACIÓN SOFTWARE LIBRE Y PROPIETARIO

Entendemos por **sistema informático** aquel sistema que almacena y procesa información interrelacionando el hardware y el software de un ordenador.

El hecho de utilizar un **software libre** implica que los usuarios podrán **modificar, copiar, ejecutar e incluso mejorar dicho programa**.

Para cubrir las necesidades que se nos plantean en el ámbito de la informática es preciso tener en cuenta algunos factores que podemos resumir en dos:

Conocer en profundidad el hardware

Antes de escoger el software que vamos a emplear, debemos tener muy presente en qué equipos vamos a instalar el sistema operativo y las aplicaciones. Sus características técnicas, su conectividad y sus prestaciones serán elementos clave para la elección. Si los equipos están en red, además, debemos tener muy clara la estructura que utilizaremos para alcanzar el máximo rendimiento.

Conocer en profundidad el software

Debemos conocer el tipo de programa que se necesita, sus funcionalidades y la licencia bajo la que se distribuye, así como otros aspectos que detallaremos a continuación.

1.1. ESTRUCTURA Y COMPONENTES DE UN SISTEMA INFORMÁTICO. PERIFÉRICOS Y ADAPTADORES PARA LA CONEXIÓN DE DISPOSITIVOS

Componentes lógicos de un PC

youtu.be/uK5VsRsEVKc



El sistema informático se compone de una parte central que procesa la información, que conocemos como ordenador, y unos dispositivos que actúan como periféricos que facilitan la entrada y la salida de información.

Para que un ordenador funcione de forma correcta debe estar formado por dos tipos de elementos: **los componentes lógicos o programas (software)** y, por otro lado, los **componentes físicos y electrónicos (hardware)**.

En el caso de los **componentes físicos (hardware)** podemos encontrar **diferentes tipos, dependiendo del rendimiento que necesitemos para nuestro equipo**. Aunque en este caso, comentaremos los fundamentales.

Caja, torre o chasis: recinto donde se alojan los principales componentes que forman un ordenador y se encarga de su protección. Este recinto suele ser metálico o de plástico.



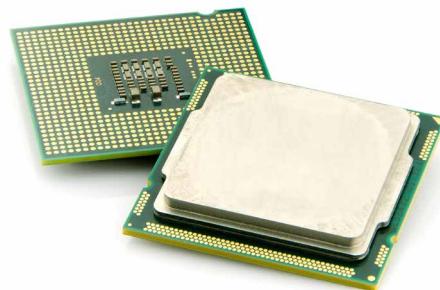
Fuente de alimentación: es un transformador de corriente eléctrica alterna que procede del sistema eléctrico en corriente continua con un voltaje apropiado que permite el funcionamiento de los distintos componentes que forman el ordenador.



Placa madre (motherboard) o placa base (mainboard): es el elemento principal del ordenador, en el cual se van a conectar todos los componentes. También es conocido como un **componente integrador**.



CPU (Unidad Central de Procesamiento): es la encargada de interpretar y procesar las instrucciones de un programa informático a través de operaciones aritméticas, lógicas y entrada/salida del sistema. Se puede considerar el cerebro de cualquier dispositivo.



<p>Disco duro: es el dispositivo que funciona como memoria del ordenador. Se utiliza para almacenar archivos y programas, ya que es capaz de almacenar datos, incluso estando el ordenador apagado.</p>	
<p>Memoria RAM (Random Access Memory): es un componente que permite intercambiar información entre el sistema operativo, el software, el procesador y otros dispositivos. Dispone de una gran velocidad de lectura y escritura y está en plena comunicación con gran parte de los componentes del ordenador. Es un tipo de memoria volátil, es decir, los datos no se quedan almacenados cuando el equipo no tiene energía.</p>	
<p>Tarjeta gráfica o tarjeta de vídeo: es una tarjeta que se encarga de procesar los datos que son enviados desde el ordenador y transformarlos en datos visibles y comprensibles para el usuario.</p>	
<p>Tarjeta de sonido o placa de sonido: es una tarjeta de expansión que permite al ordenador enviar información de audio a un dispositivo de audio, como, por ejemplo, unos auriculares o altavoces.</p>	
<p>Tarjeta de red: es una tarjeta que da la posibilidad a la máquina de acceder a una red y compartir sus recursos.</p>	

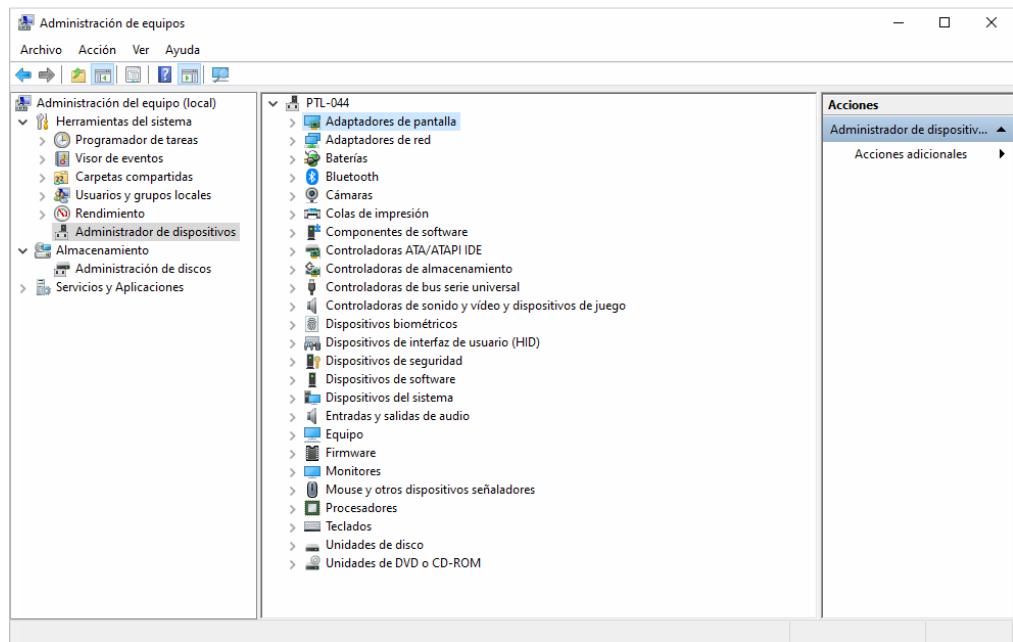
Unidades de almacenamiento adicionales (CD-ROM, discos secundarios, etcétera).	
Periféricos de entrada y salida (monitor, teclado, etcétera).	

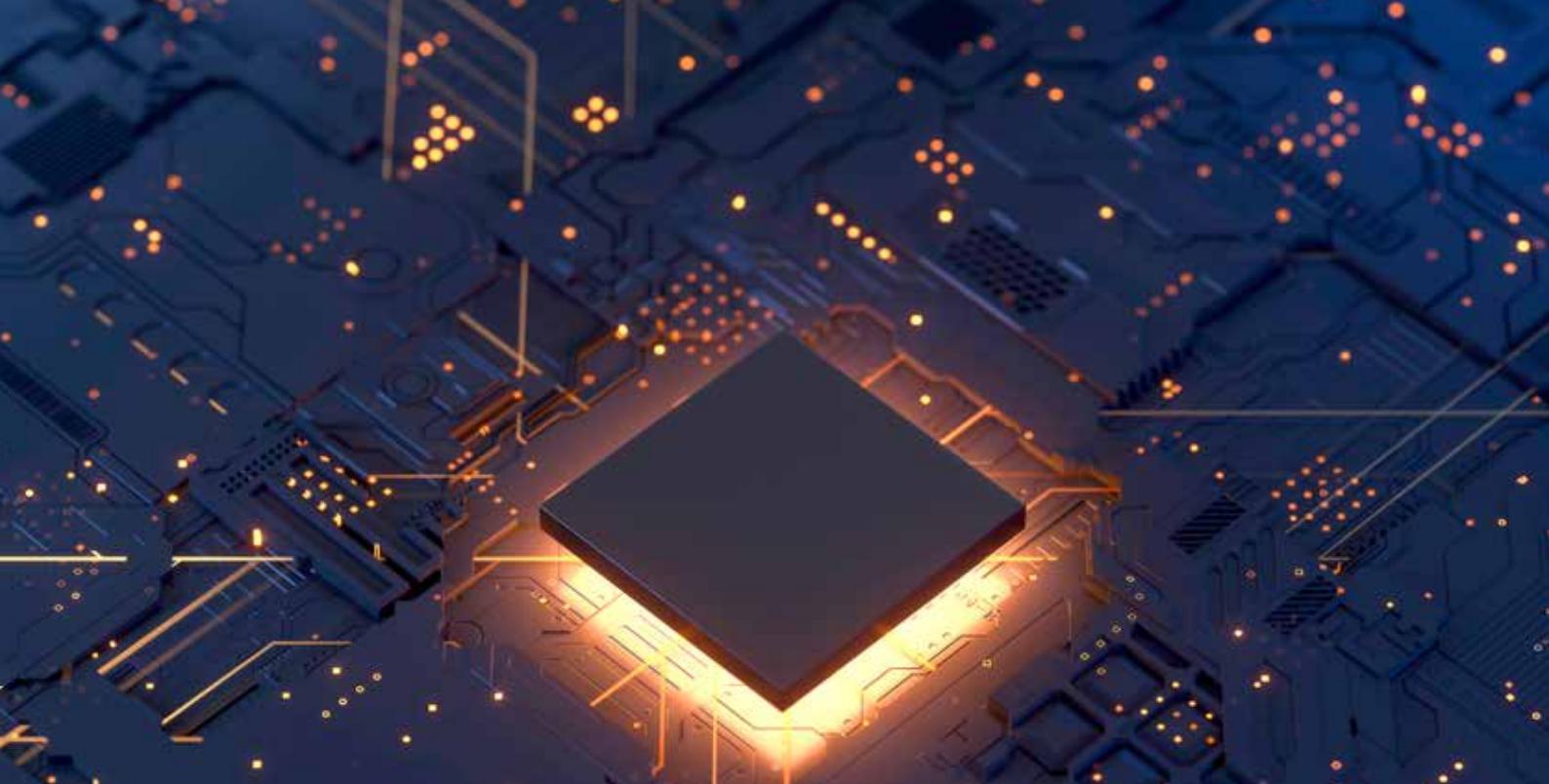


Diferencia entre CPU, ALU, Núcleo del sistema, UC y Memoria principal
youtu.be/G03Zx_AtUhk



En sistemas operativos como Windows podemos acceder a diferentes herramientas como el *Administrador de dispositivos*, el cual nos muestra una lista de todos los componentes hardware que nos podemos encontrar conectados a nuestro ordenador. Desde aquí se nos ofrece la opción de actualizar o instalar *drivers*, útil para el estado de determinados de periféricos externos como tarjetas de red o tarjetas gráficas de alto rendimiento que no estén totalmente configuradas en un estado inicial del sistema.





Para dar sentido a todos los componentes anteriores, necesitamos añadir los componentes lógicos o programas (software):

- Sistema operativo
- Aplicaciones

Si nos fijamos en la arquitectura interna del sistema informático, debemos atender a los siguientes conceptos:

- **Unidad central de proceso (CPU)**

Es un elemento esencial de cualquier ordenador ya que tiene como misión ejecutar las instrucciones de un programa. La CPU también se conoce con el nombre de procesador central.

Físicamente está formada por circuitos de naturaleza electrónica, que en un ordenador se encuentran integrados en una pastilla o chip denominado microprocesador. Está compuesto por la Unidad de control, la ALU y los buses de entrada y salida de datos.

- **Unidad de control (UC)**

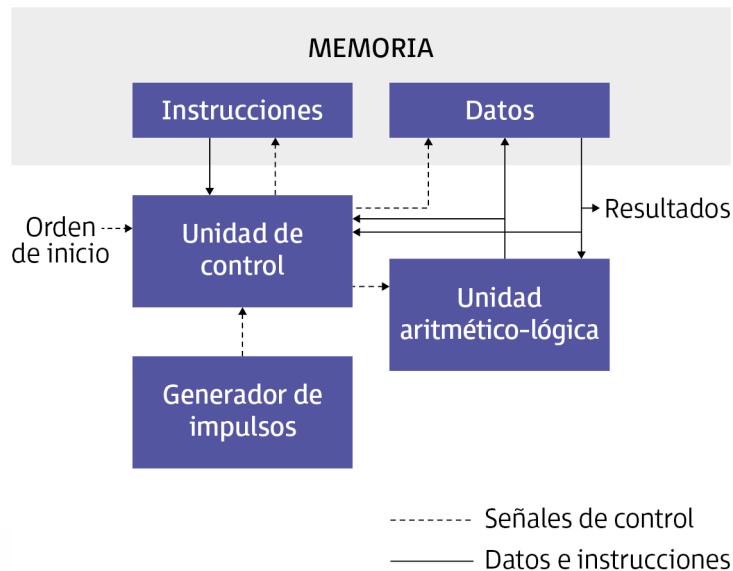
Es la parte pensante del sistema informático. Su tarea fundamental es recibir información para interpretarla y procesarla mediante las órdenes que envía al resto de componentes del sistema.

- **Unidad aritmético-lógica (ALU)**

Es un circuito digital que calcula operaciones aritméticas, como la suma, la resta o la multiplicación, y operaciones lógicas, como las comparaciones, and u or. Conforma uno de los tres bloques en los que se divide la CPU.

• Memoria principal

También se conoce como memoria central o memoria RAM. Es un componente necesario para que se pueda procesar la información. Para que un programa pueda ser procesado por la CPU, primero tiene que almacenarse en la memoria principal.



• Buses

Es una vía de comunicación que conecta dos o más componentes del ordenador. Se trata de un medio de transmisión compartido. Al bus se conectan múltiples dispositivos y una señal transmitida por cualquiera de ellos puede ser recibida por el resto de las unidades conectadas.

Funciones de un bus:

1. Soportar la información a transmitir.
2. Garantizar la correcta comunicación entre los elementos que comparten el bus.

• Ciclo de instrucción

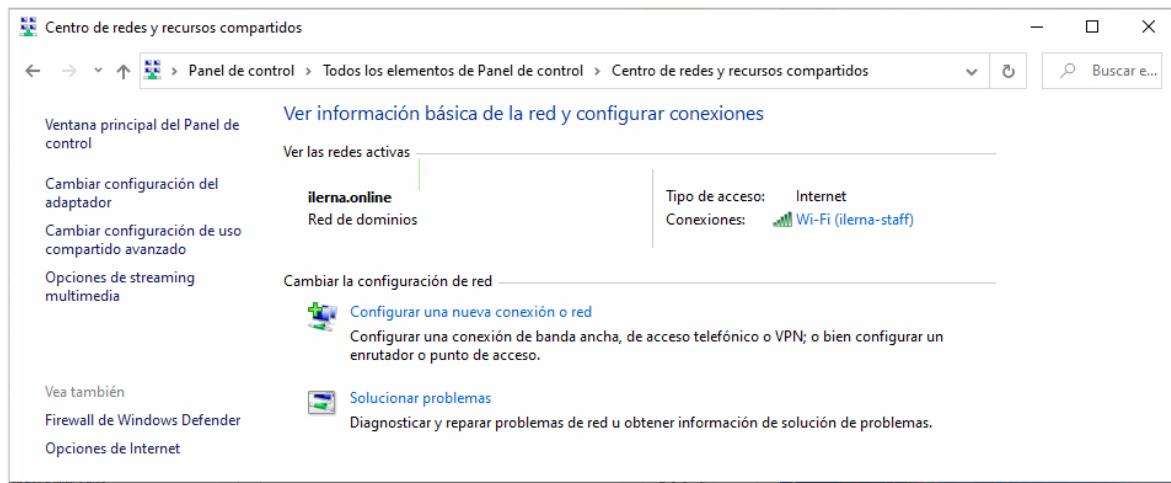
Es el conjunto de pasos que se realizan al procesar una instrucción de un programa. Está formado por la fase de búsqueda y la fase de ejecución.

El ordenador admitirá muchos otros periféricos físicos y si necesitamos ampliarlo a nivel de hardware será indispensable que conozcamos su arquitectura y su conectividad. Asimismo, las características del hardware condicionarán qué software se ejecutará correctamente en él y, por tanto, la elección del sistema operativo y las aplicaciones.

También se deberá tener en cuenta las características técnicas de la red que estemos empleando y su tipo de cableado.

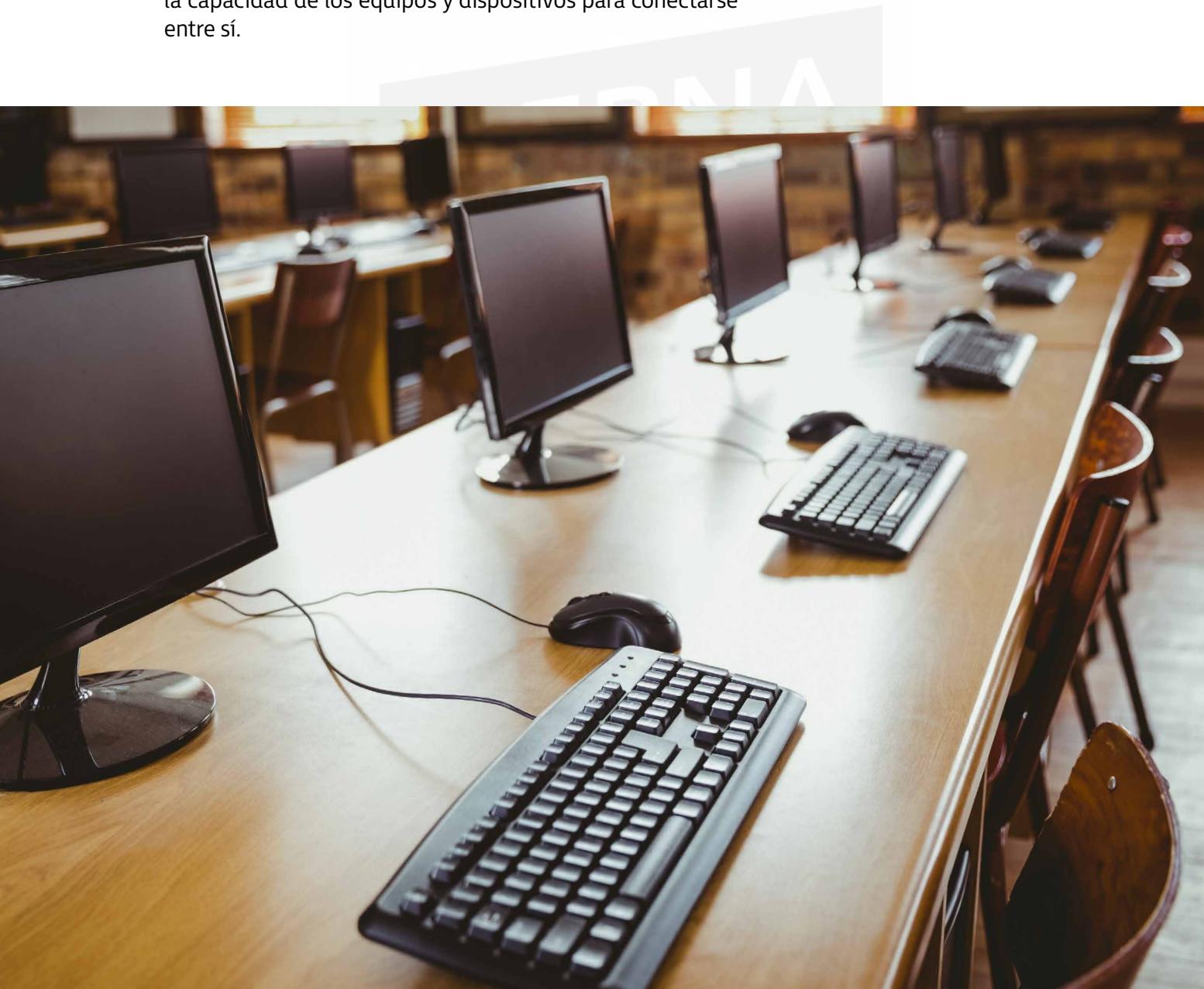
El ciclo de instrucción
youtu.be/hfdB-hkTOS4





El apartado “Red de Windows” nos ofrece una perspectiva general de qué equipos están conectados a la misma.

Tanto si concebimos el sistema informático como un único equipo, como si pensamos en él como un conjunto de equipos en red, la conectividad es un término clave en la disciplina que nos ocupa. Dicho término hace referencia a la capacidad de los equipos y dispositivos para conectarse entre sí.





ponte a prueba

¿Cuáles de las siguientes fases forman el ciclo de instrucción?

- a) Fase de desarrollo y fase de búsqueda
- b) Fase de búsqueda y fase de ejecución
- c) Fase de creación y fase de desarrollo
- d) Fase de creación y fase de ejecución

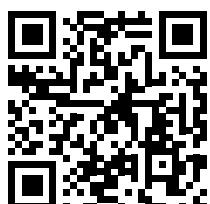
La memoria principal es conocida como memoria central o memoria RAM.

- a) Verdadero
- b) Falso



Tipos de redes

youtu.be/TsPfUuVCw8Q



En ocasiones, pese a que a priori la conectividad no sea posible, contamos con la opción de usar adaptadores. Así, por ejemplo, si deseamos habilitar una red inalámbrica y los ordenadores no cuentan con tarjetas de red wifi en su placa madre, podemos adquirir adaptadores de red extraíbles e insertarlos en sus respectivos puertos USB.

En definitiva, todo sistema informático estará compuesto de hardware (recursos físicos) y de software (recursos lógicos). Si queremos entender la definición de sistema informático en un sentido más amplio, a todo ello deberemos añadir a los usuarios (recursos humanos) y, por supuesto, la información.

1.2. TIPOS Y TOPOLOGÍAS DE RED

Una **red de ordenadores** es un conjunto de equipos interconectados entre sí que permiten compartir recursos e información. Para ello es necesario que los ordenadores dispongan de una tarjeta de red, cables de conexión, dispositivos periféricos y un software adecuado.

Es posible diferenciar **varios tipos de redes según su extensión:**

- **PAN (red de área personal):** cuando los equipos están situados a pocos metros de distancia unos de otros y se utilizan solo para uso personal. Estas redes aparecieron debido al avance tecnológico, para que el usuario no tuviera solo un equipo informático, sino también tabletas, móviles y televisores. A estos equipos no se les saca todo el provecho que ofrecen sus prestaciones de manera independiente, por lo que es conveniente realizar una red entre todos los dispositivos de un mismo usuario.

Una de las cosas que hacen tan atractivas a este tipo de redes es lo sencilla y automática que resulta su configuración. Además, suelen comunicarse de forma inalámbrica y no tienen ningún tipo de coste.

Ejemplos de este tipo de redes pueden ser la **conexión del ratón inalámbrico** al ordenador o la **conexión del móvil** a la televisión de forma automática.

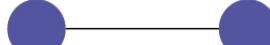
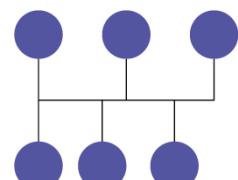
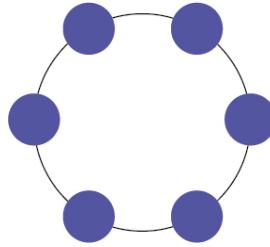
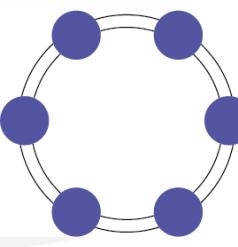
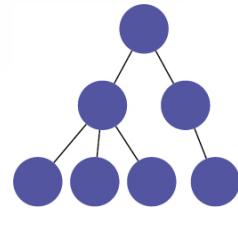
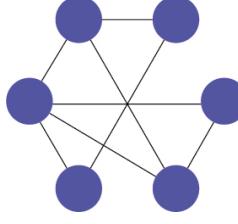
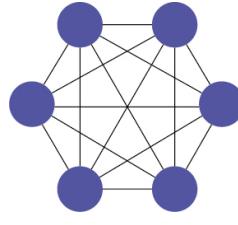
- **WLAN.** Red LAN inalámbrica (*Wireless Local Area Network*) que transmite información de forma inalámbrica.
- **LAN (red de área local):** dispone de un concentrador. A él se conectan todos los nodos de un edificio mediante un *router*.

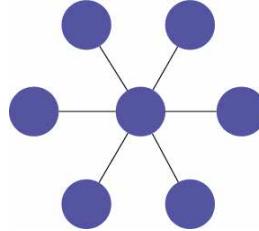
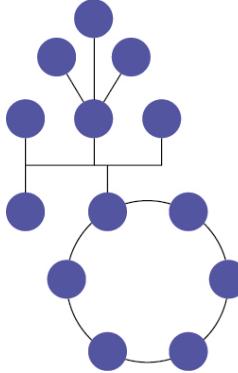
WAN
Wide Area Network
Redes geográficas



- **MAN (red de área metropolitana):** puede abarcar desde varios edificios hasta una ciudad entera. Se basa en la interconexión de varias LAN. Un ejemplo claro de este tipo de redes es la televisión por cable. Las operadoras compiten por los servicios de cables en la ciudad, por lo que aprovechan para ofrecer televisión, teléfono e internet.
- **WAN (red de área extensa):** este tipo de redes permite interconectar distintas ciudades o incluso un país. A diferencia de las redes de área de local, presentan una menor velocidad de transmisión y, por tanto, su tasa de error es mayor. Esto se debe a la gran extensión que abarcan. Independientemente del tipo de red que se decida utilizar, debemos saber que toda red presenta una topología diferente. Es decir, un diseño específico en los planos físico y lógicos. Dado que toda red es, en esencia, un conjunto de equipos (nodos) interconectados, la manera en la que se establezcan las conexiones entre estos definirá su topología.

Las **topologías básicas** son las siguientes:

Punto a punto Un canal para comunicar solamente dos nodos.	
Bus Único canal de comunicaciones al que se conectan los distintos dispositivos.	
Anillo Los dispositivos conforman un círculo de manera que cada equipo está conectado al siguiente, exceptuando el último círculo, que está conectado al primero.	
Doble anillo Funciona igual que la topología en anillo. Además, posee un segundo anillo que conecta también todos los nodos.	
Árbol Se estructura como un árbol, en el que los dispositivos o estaciones ejercen de ramas.	
Malla Todos los nodos están conectados entre ellos. Así pues, para ir de un lugar a otro, la información puede seguir distintos caminos.	
Totalmente conexa Tiene las mismas características que la topología en malla, aunque contiene más conexiones, ya que todos los nodos están conectados entre sí.	

<p>Estrella</p> <p>Los dispositivos están conectados siempre a un punto central y todas las comunicaciones se realizan a través de este nodo.</p>	
<p>Híbrida</p> <p>Combina varias de las anteriores.</p>	

Para describir con claridad cómo funciona una red y su estructura puede emplearse lo que se denomina el modelo **OSI** (*Open System Interconnection*). Dada la gran variedad de tecnologías y fabricantes en el ámbito de las comunicaciones, este modelo se creó en los años ochenta para sentar unos estándares de referencia. Se trata de un modelo que se estructura en capas, que definen las diferentes etapas por las que deben circular los datos para pasar de un dispositivo a otro dispositivo de la misma red.

Las capas son siete y se agrupan de la siguiente forma:

Aplicación	La más cercana al usuario.
Presentación	Se encarga de que la información enviada a la capa de aplicación pueda ser leída con éxito.
Sesión	Garantiza la comunicación entre dos puertos (<i>hosts</i>).
Transporte	Transporta los datos del emisor hasta el receptor.
Red	Responsable de que exista conectividad entre dos hosts diferentes.
Vínculo de datos	Acceso al medio.
Física	Transmite las señales.



Topologías de red

youtu.be/W1M_-lETphg

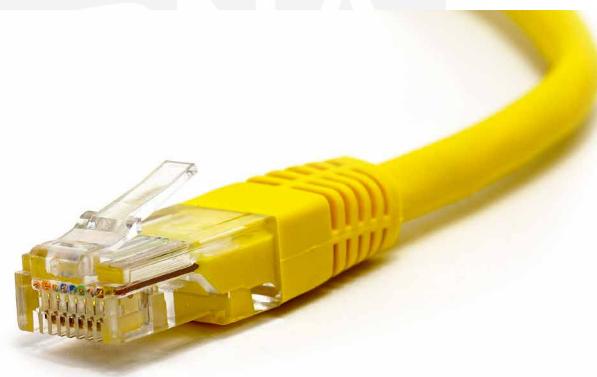


A continuación, repasaremos algunos de los conectores de red más frecuentes:

- **Red con conectores BNC.** Emplea cable coaxial y es la más compleja de configurar. Los avances en este campo han propiciado que actualmente se encuentre en desuso.



- **Red con conectores RJ-45.** Para este tipo de redes se emplean cables Ethernet de 8 pines. Su uso es aún frecuente en redes cableadas.



- **Red inalámbrica.** El wifi ha supuesto una revolución en este ámbito, pues nos permite habilitar redes sin necesidad de cablearlas físicamente.





ponte a prueba

¿De qué tipo es una red de conexión bluetooth?

- a) PAN
- b) WAN
- c) LAN
- d) MAN

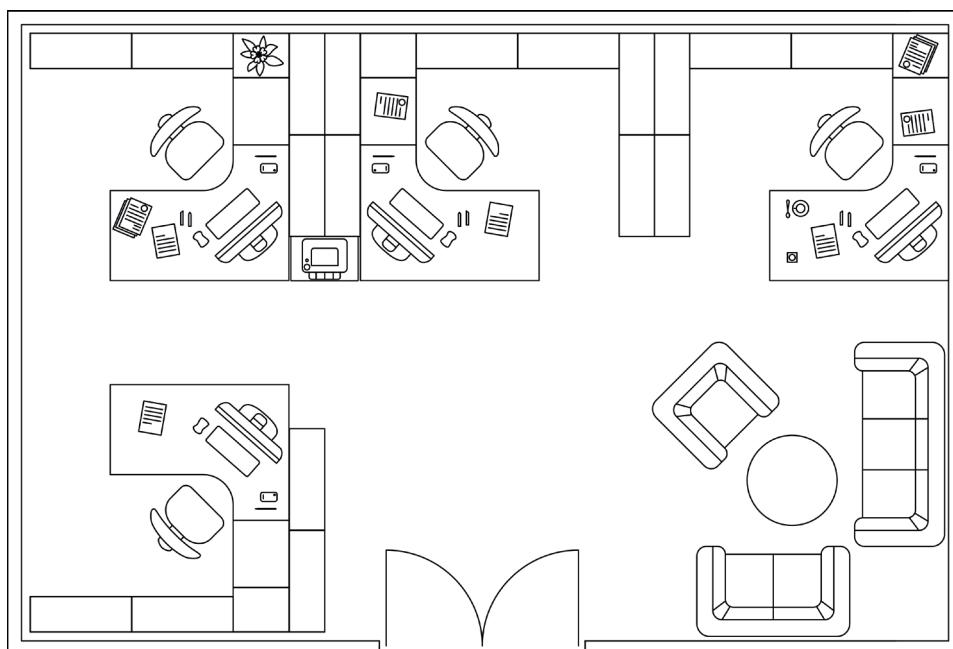
1.3. MAPA FÍSICO Y LÓGICO DE UNA RED

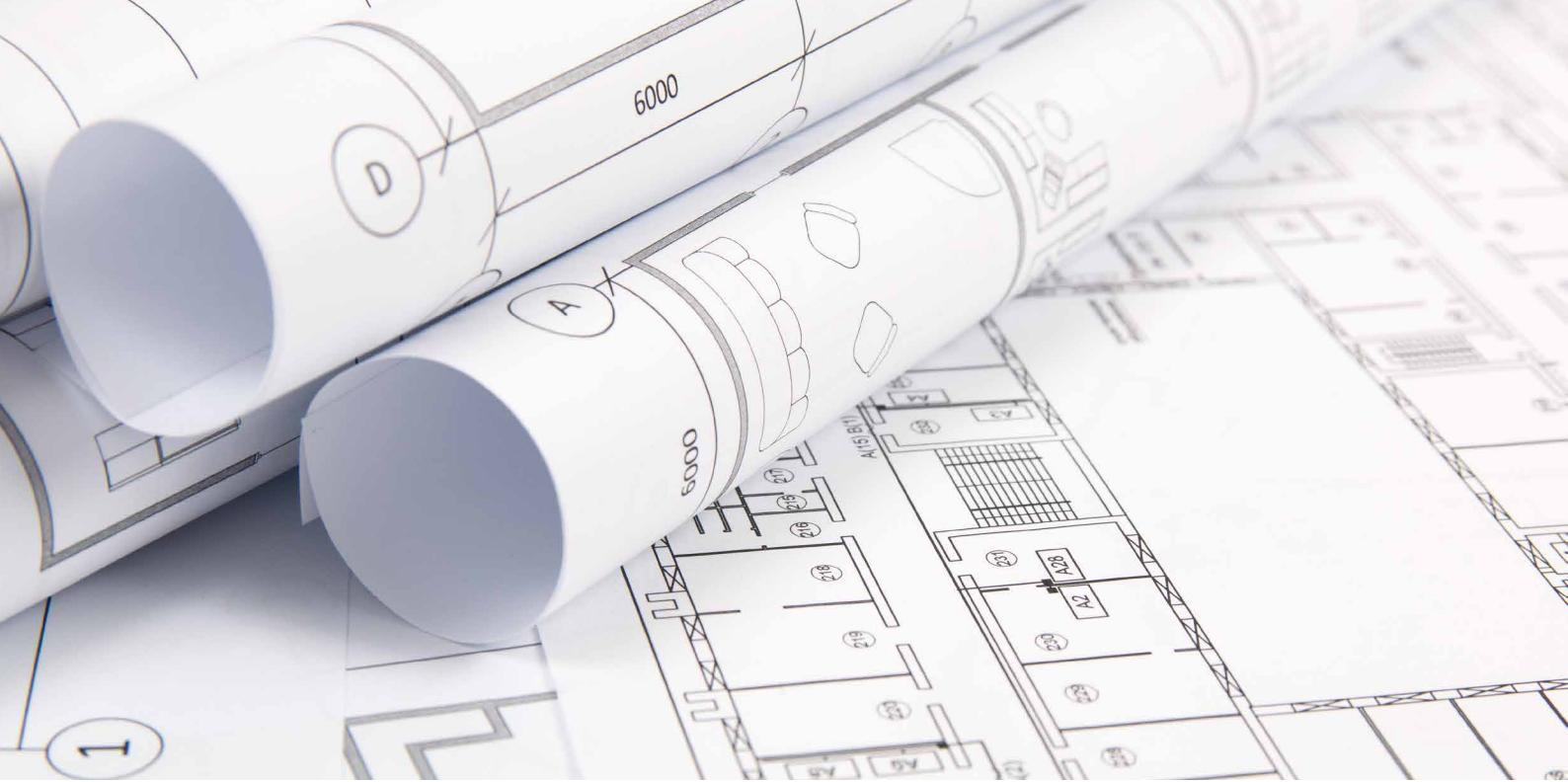
A la hora de crear una red o de modificar la que tenemos habilitada es muy importante que hayamos documentado su estructura.

Dicha documentación deberá llevarse a cabo en dos frentes.

Mapa físico

Es una representación gráfica de una red en el mundo real. ¿En qué planta se encuentra cada ordenador? ¿En qué lugar de la oficina está ubicado? Todo ello deberá tenerse en cuenta para garantizar que la señal de red llegue a cada equipo de la mejor forma posible.

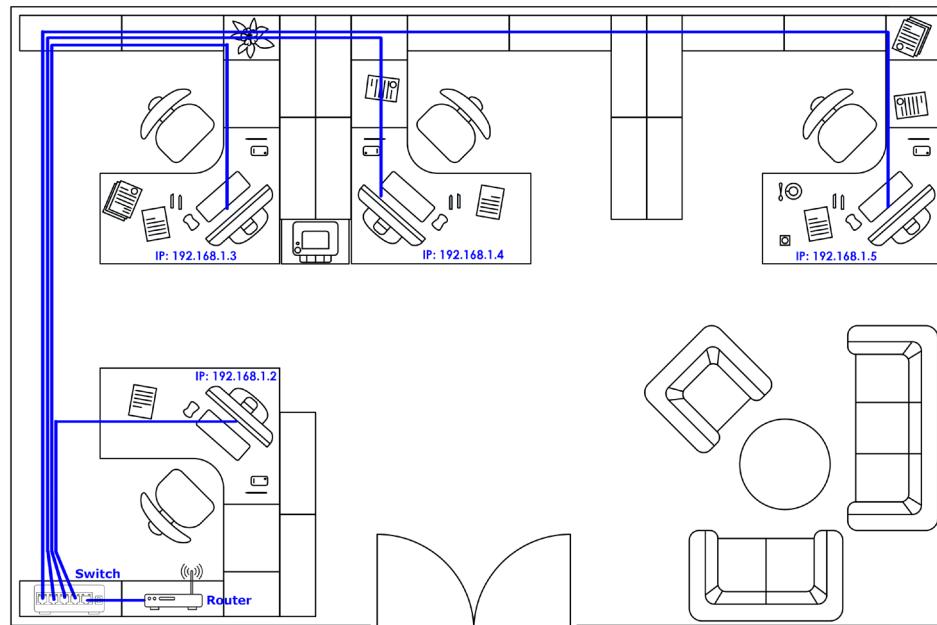




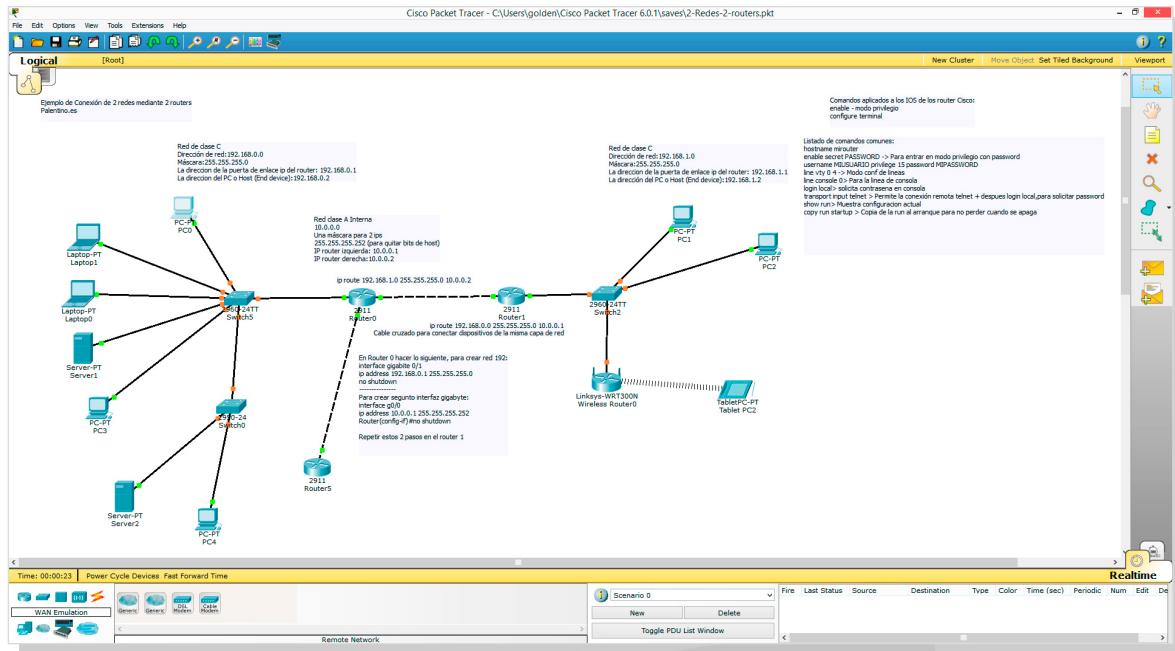
Habitualmente, los mapas físicos se realizan de forma manual por los técnicos, aunque en la actualidad existen diferentes aplicaciones propias de las marcas de los equipos que utilicemos en la red (). Estas nos ofrecen la posibilidad de subir los mapas como archivos en determinados formatos para mostrar la representación de este mapa en un ordenador y poder interactuar con los diferentes componentes o consultar información sobre los equipos de esta.

Mapa lógico

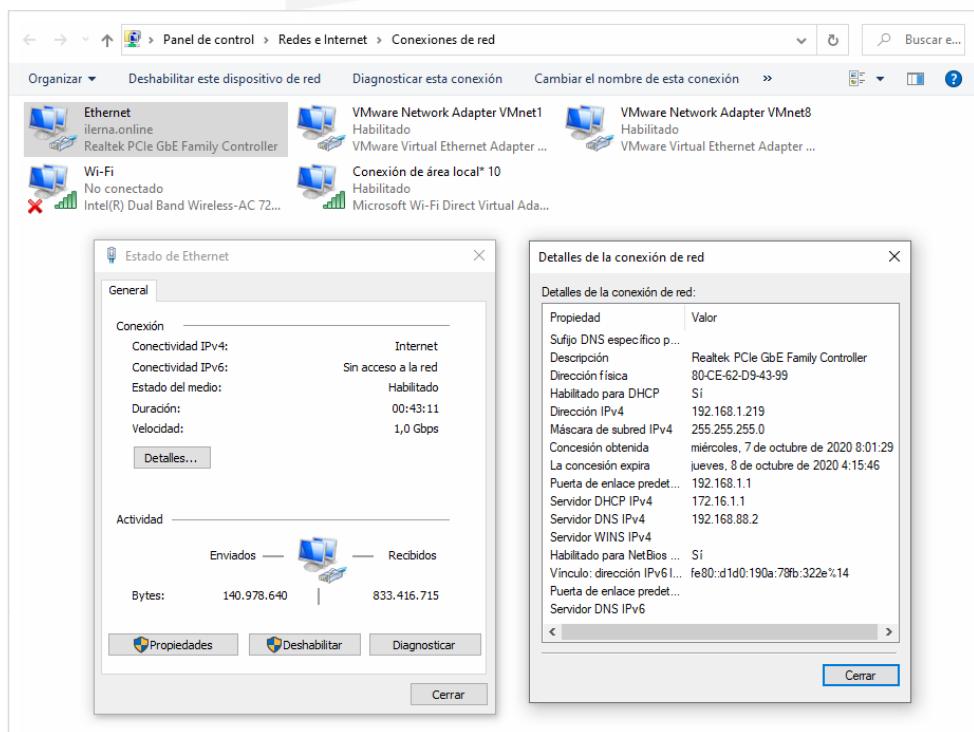
Documentación que hace referencia a los aspectos internos de la red. Es necesario saber qué dirección IP tiene asignada cada ordenador, a qué subred pertenece, etc.



Este mapa es una representación mucho más técnica que la anterior, que nos facilita el mantenimiento de la red y la incorporación de nuevos nodos en esta. Al igual que en el caso anterior, los proveedores de este tipo de hardware nos ofrecen entornos preparados para mostrar esta información.

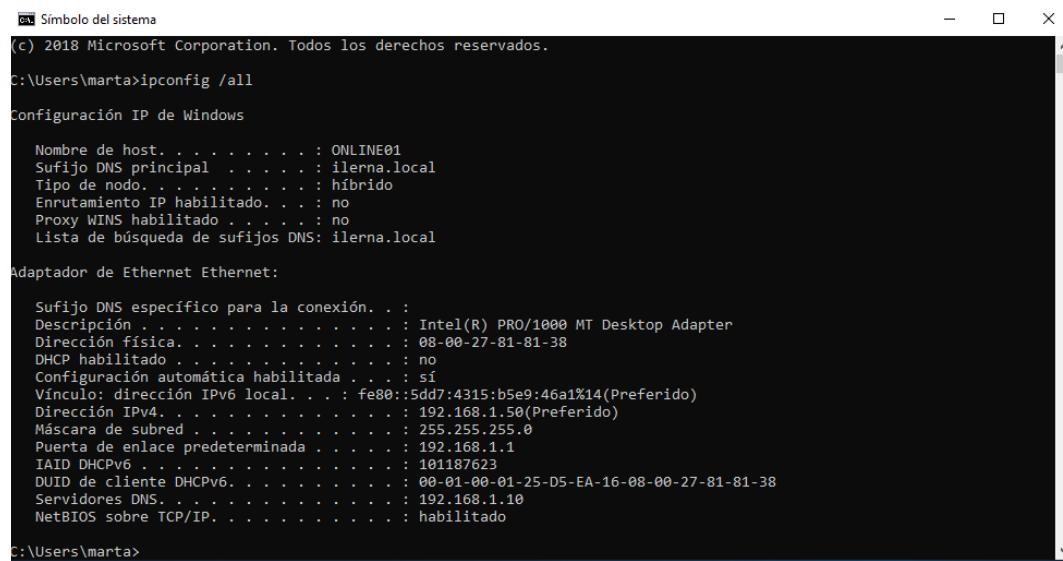


Los diferentes entornos de los sistemas operativos más utilizados hoy en día proporcionan diferentes aplicaciones preinstaladas que nos ayudan a obtener la información necesaria de los equipos. Nos referimos, por ejemplo, a la dirección IP, DECHP, DNS, etc.



La dirección IP es uno de los datos que deberemos documentar a la hora de realizar un mapa físico de la red.

De todos modos, cuando se comprueba estos temas de forma masiva en redes muy grandes, se suele utilizar la consola de comandos, ya que es más liviana y nos ofrece toda la información necesaria con los comandos adecuados.



```
Símbolo del sistema
(c) 2018 Microsoft Corporation. Todos los derechos reservados.
C:\Users\marta>ipconfig /all
Configuración IP de Windows

Nombre de host . . . . . : ONLINE01
Sufijo DNS principal . . . . . : ilerna.local
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado. . . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: ilerna.local

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión . . . :
Descripción . . . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . . . . . . . . . . . : 08-00-27-81-81-38
DHCP habilitado . . . . . . . . . . . . . . : no
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::5dd7:4315:b5e9:46a1%14(Preferido)
Dirección IPv4. . . . . . . . . . . . . . . . : 192.168.1.50(Preferido)
Máscara de subred . . . . . . . . . . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . . . . . . . . . . . . : 101187623
DUID de cliente DHCPv6. . . . . . . . . . . . . : 00-01-00-01-25-D5-EA-16-08-00-27-81-81-38
Servidores DNS. . . . . . . . . . . . . . . . : 192.168.1.10
NetBIOS sobre TCP/IP. . . . . . . . . . . . . . : habilitado

C:\Users\marta>
```

ponte a prueba

El mapa lógico de la red nos mostrará una representación gráfica real de la situación de los componentes de la red dentro de un determinado espacio.

- a) Verdadero
- b) Falso

1.4. ARQUITECTURA DE UN SISTEMA OPERATIVO

A lo largo de las últimas décadas, los sistemas operativos han ido evolucionando de forma notable. Además, las consolas de tipo texto como DOS han dejado paso a interfaces más modernas de tipo gráfico como Windows o Mac OS X.

En la práctica podemos distinguir en la arquitectura de todos ellos los siguientes elementos clave:

Núcleo del sistema

Se trata del componente del sistema que está ejecutándose permanentemente en la memoria. Es la parte que se encarga de gestionar los recursos del ordenador.

Entre las tareas que realiza, cabe destacar la de asignar CPU y memoria a los procesos.

Nombre	PID	Descripción	Estado	Grupo
AarSvc		Agent Activation Runtime	Detenido	AarSvcGroup
AarSvc_12b951		Agent Activation Runtime_12b951	Detenido	AarSvcGroup
AdobeARMservice	4308	Adobe Acrobat Update Service	En ejecución	
AGMService	4372	Adobe Genuine Monitor Service	En ejecución	
AGSService	4328	Adobe Genuine Software Integrity Service	En ejecución	
AIRouter		Servicio de enruteador de AllJoyn	Detenido	LocalServiceN...
ALG		Servicio de puerta de enlace de nivel de aplicación	Detenido	LocalServiceN...
AppIDSvc		Identidad de aplicación	Detenido	netsvcs
Appinfo		Información de la aplicación	En ejecución	netsvcs
AppMgmt		Administración de aplicaciones	Detenido	AppReadiness
AppReadiness		Preparación de aplicaciones	Detenido	
AppVClient		Microsoft App-V Client	Detenido	
AppXSvc		Servicio de implementación de AppX (AppXSVC)	Detenido	wsappx
AssignedAccessManagerSvc		Servicio AssignedAccessManager	Detenido	AssignedAcce...
AudioEndpointBuilder	2792	Compilador de extremo de audio de Windows	En ejecución	LocalSystemN...
Audiosrv	3428	Audio de Windows	En ejecución	LocalServiceN...
autotimesvc		Hora de la red de telefonía móvil	Detenido	autoTimeSvc
AxInstSV		Instalador de ActiveX (AxInstSV)	Detenido	AxInstSVGroup
BcastDVRUserService		Servicio de usuario de difusión y GameDVR	Detenido	BcastDVRUser...
BcastDVRUserService_12b951		Servicio de usuario de difusión y GameDVR_12b951	Detenido	BcastDVRUser...
BDESVC		Servicio Cifrado de unidad BitLocker	Detenido	netsvcs
BFE	476	Motor de filtrado de base	En ejecución	LocalServiceN...
RITS		Servicio de transferencia inteligente en segundo plano (RITS)	Detenido	netsvcs

El sistema operativo gestiona los servicios y procesos que se ejecutan en él.

La API del núcleo

Las siglas API corresponden a Interfaz de Programación de Aplicaciones. La API comprende el conjunto de servicios que ofrece el sistema operativo a las aplicaciones. Estos pueden llamar al sistema operativo para valerse de él.

Así, por ejemplo, mediante dichas llamadas el sistema puede efectuar operaciones básicas como abrir archivos, modificarlos, cerrarlos, etc. También puede ejecutar instrucciones de entrada y salida para operaciones relacionadas con gráficos y sonido, comunicaciones, etc.

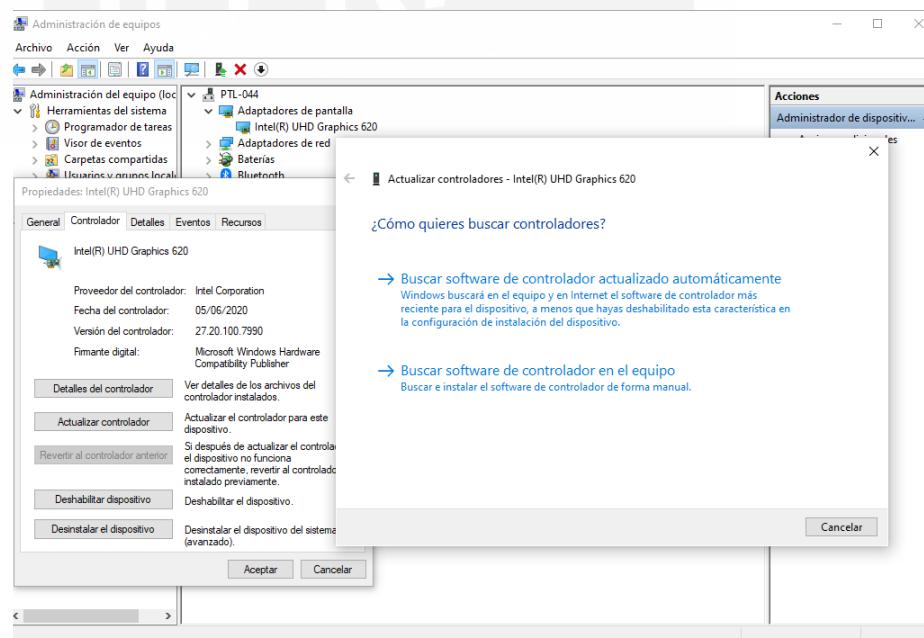


El sistema de archivos

Gracias a él obtenemos una estructura lógica de la información grabada en las unidades de disco y podemos trabajar con directorios y archivos. Dada la importancia de este sistema, es frecuente que forme parte del *kernel* o núcleo.

Controladores o drivers

Permiten que el sistema interactúe con los diversos dispositivos de hardware del equipo. Por ejemplo, si conectamos al sistema un disco duro Serial ATA será imprescindible contar con el *driver* correspondiente para poder trabajar con él.



Los controladores de Windows permiten que el sistema interactúe con los diversos dispositivos de hardware del equipo.

Toda esta gestión se llevará a cabo, naturalmente, a partir de las órdenes que el sistema operativo recibe. Para introducirlas podemos usar una interfaz gráfica o bien un intérprete de comandos tipo DOS.

```

C:\Windows\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\USERS\lidia>dir
El volumen de la unidad C es Windows 7 Main
El n mero de serie del volumen es: BEBB-4C00

Directorio de C:\USERS\lidia

12/09/2014 11:39 <DIR> .
12/09/2014 11:39 <DIR> ..
12/09/2014 11:41 <DIR> .dvdcss
16/04/2013 19:50 34 .adocs.dat
05/06/2014 17:11 <DIR> .VirtualBox
16/05/2013 10:14 <DIR> .VirtualBox.old
19/06/2013 17:07 <DIR> .VirtualBox.sav
20/06/2014 18:23 <DIR> .zenmap
05/06/2014 16:39 228 2014-06-05-14-38-57.059-VBoxSVC.exe-5104.log

04/06/2014 18:14 <DIR> Contacts
07/10/2014 19:33 <DIR> Desktop
10/06/2014 22:27 <DIR> Documents
13/09/2014 13:32 <DIR> Downloads
03/04/2013 10:14 <DIR> dwhelper
06/06/2014 10:18 <DIR> Favorites
04/06/2014 18:14 <DIR> Links
06/10/2014 19:13 <DIR> Music
12/03/2013 20:41 30.946 ovpntray.log
01/02/2014 20:03 <DIR> Pictures
04/06/2014 18:14 <DIR> Saved Games
04/06/2014 18:14 <DIR> Searches
01/10/2013 18:24 <DIR> Videos
10/07/2013 19:17 26 wifi.txt
19/06/2013 17:07 <DIR> y25wave
4 archivos 31.924 bytes
20 dirs 36.888.424.448 bytes libres

C:\USERS\lidia>_

```

El ejecutable “Command” de Windows nos brinda la opción de introducir comandos desde la consola del sistema.

1.5. FUNCIONES DEL SISTEMA OPERATIVO

Si nos remitimos al apartado anterior y lo examinamos con detenimiento, deduciremos cuáles son las principales funciones del sistema. A modo de resumen convendremos que son las siguientes:

Administraci n de procesos

Cuando existen varios programas a la espera para ser procesados, el sistema operativo debe decidir el orden de procesamiento de estos, así como asignar los recursos necesarios para su proceso.

Administraci n de recursos

El sistema operativo tiene la capacidad de distribuir de forma adecuada y en el momento oportuno los diferentes recursos (memoria, dispositivos, etc.) entre los diversos programas que se encuentran en proceso. Para hacerse cargo de este proceso lleva un registro que le permite conocer qué recursos están disponibles y cuáles están siendo utilizados, por cuánto tiempo y por quién, etc.

Control de operaciones de entrada y de salida

Mediante esta actividad el sistema operativo decide qué proceso hará uso del recurso, durante cuánto tiempo y en qué momento.

Administración de la memoria

Supervisa qué áreas de memoria están en uso y cuáles están libres. Además, determina cuánta memoria asignará a un proceso y en qué momento. También libera la memoria cuando ya no es requerida para el proceso.

Recuperación de errores

El sistema operativo contiene rutinas que intentan evitar perder el control de una tarea cuando se suscitan errores en la transferencia de información hacia y desde los dispositivos de entrada y salida. Estas tareas son las siguientes:

- Gestión y asignación de la memoria y la CPU (en la siguiente imagen).
- Gestión de las unidades de almacenamiento de la información.
- Gestión de las operaciones de entrada/salida.
- Mediación entre el hardware y el software a través de los drivers.

Gestión de usuarios y permisos

Aplica una serie de permisos a los usuarios que les permiten acceder al sistema y así poder evitar acciones que afecten al trabajo que está realizando otro usuario.

Control de seguridad

Es necesario tener en cuenta la seguridad, tanto para el software como para los usuarios, así como también para la información que se encuentra almacenada en el sistema.

Administrador de tareas								
		Procesos						
Nombre	Estado	11% CPU	50% Memoria	1% Disco	0% Red	3% GPU	Motor de GPU	Consumo de ...
> 64-bit Synaptics Pointing Enhanc...		0%	2,5 MB	0 MB/s	0 Mbps	0%		Muy baja
> Adobe Acrobat Update Service (...		0%	0,9 MB	0 MB/s	0 Mbps	0%		Muy baja
> Adobe Genuine Software Integri...		0%	2,7 MB	0 MB/s	0 Mbps	0%		Muy baja
> Adobe Genuine Software Servic...		0%	2,0 MB	0 MB/s	0 Mbps	0%		Muy baja
Adobe RdrCEF (32 bits)		0%	33,7 MB	0 MB/s	0 Mbps	0%		Muy baja
Cargador de CTF		0,1%	4,0 MB	0 MB/s	0 Mbps	0%		Muy baja
Casting protocol connection list...		0%	2,6 MB	0 MB/s	0 Mbps	0%		Muy baja
COM Surrogate		0%	3,3 MB	0 MB/s	0 Mbps	0%		Muy baja
COM Surrogate		0%	1,6 MB	0 MB/s	0 Mbps	0%		Muy baja

La asignación de recursos que lleva a cabo el sistema operativo es clave a la hora de que el sistema informático funcione a la perfección.

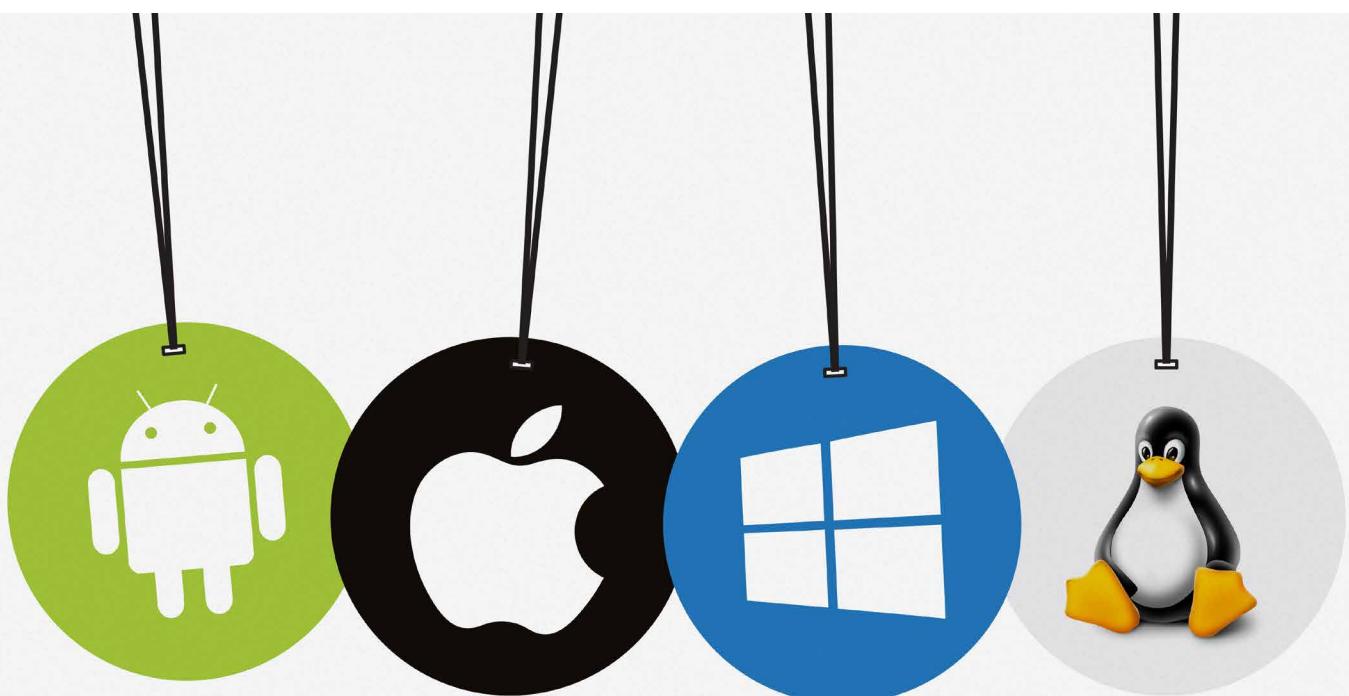
ponte a prueba

¿Cuáles de las siguientes opciones son funciones que desempeña un sistema operativo?

- a) Administración de procesos, administración de recursos, administración de la memoria y recuperación de errores.
- b) Administración de procesos, administración de recursos, administración de la memoria y gestión de la alimentación de los componentes.
- c) Administración del cableado de los discos, administración de recursos, administración de la memoria y gestión de la alimentación de los componentes.
- d) Ninguna de las opciones es correcta.

1.6. TIPOS DE SISTEMAS OPERATIVOS

Entendemos por **sistema operativo** el software encargado de poner en marcha un ordenador, garantizando su correcto funcionamiento. Además, se sitúa de intermediario entre el usuario y el hardware.



Existen diferentes formas por las que se pueden clasificar los sistemas operativos:

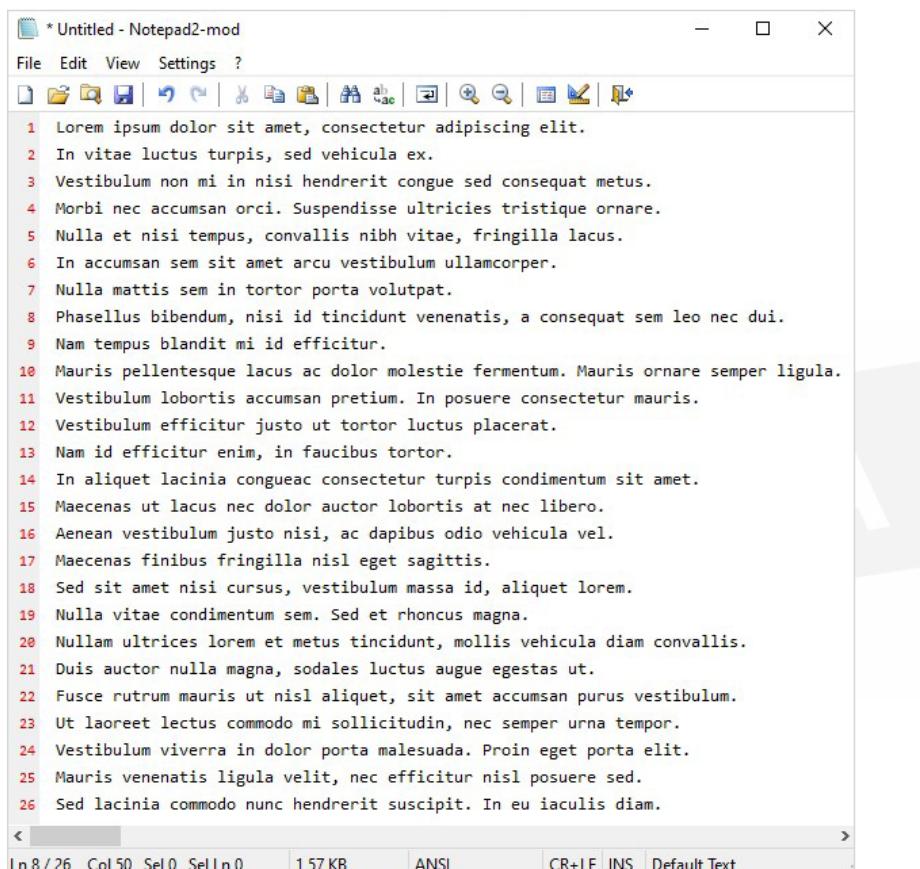
Según la cantidad de procesos que pueden gestionar, de forma simultánea	
Monotarea	Solamente mantiene un proceso en ejecución. Realiza tareas secuencialmente.
Multitarea	Permite ejecutar varios procesos a la vez. En algunos casos, dos procesos pueden utilizar dos CPU diferentes.
Según el número de usuarios	
Monousuario	Un único usuario trabaja con un solo ordenador. Algunos ejemplos pueden ser el sistema operativo DOS, el IBM-DOS o el DR-DOS, etc.
Multiusuario	Varios usuarios pueden trabajar simultáneamente. Se trata de sistemas operativos como UNIX, Windows 2000 Server o Windows XP.
Según el número de procesadores	
Monoproceso	Solamente permite realizar un proceso a la vez. Al realizar tareas rotatorias con intercambio muy rápidas es posible simular la multitarea.
Multiproceso	Permite ejecutar diferentes tareas al mismo tiempo, ya que ofrece realizar varios procesos de forma simultánea.
Según los servicios que ofrece	
Centralizados	Todos los recursos se encuentran en una misma máquina.
Distribuidos	Los recursos utilizados pueden estar en diferentes máquinas que deben estar conectadas en red.
Según el tipo de licencia	
Propietarios	Aquellos que tienen limitaciones de uso. Son propiedad de alguna empresa.
Libres	Aquellos que permiten la modificación del producto. Usar el programa libremente.

1.7. TIPOS DE APLICACIONES

Podríamos hacer una primera clasificación de aplicaciones con base en la licencia bajo la que se distribuyen. Sin embargo, también podemos tener en cuenta otros criterios para su clasificación y dividirlas en estos tres tipos:

Aplicaciones locales

Se almacenan en la unidad de disco local de un equipo y solamente este tiene acceso a ellas.



El famoso "Bloc de notas" de Windows es un buen ejemplo de aplicación local.

Aplicaciones en red

En este caso se ejecutan en un entorno de red local. En consecuencia, las aplicaciones suelen tener dos componentes: el primero se ejecuta de manera local y el segundo de manera remota.

Aplicaciones web o en la nube

La mayor parte del software se ejecuta en un servidor remoto y queda accesible a través de internet. Con frecuencia, los datos también se almacenan online.



Google Docs permite trabajar en la nube con una suite ofimática.

Por supuesto, también podemos clasificar las aplicaciones en función del fin para el que fueron programadas. De esta forma, establecemos categorías como ofimática (Word, Excel, etc.), optimización del sistema (CCleaner, Defraggle, etc.) y así, sucesivamente.

1.8. LICENCIAS Y TIPOS DE LICENCIAS



Licencias freeware, shareware y comercial
youtu.be/wOqv8xjTfZg



Dependiendo del tipo de software, es posible dividir las aplicaciones en:

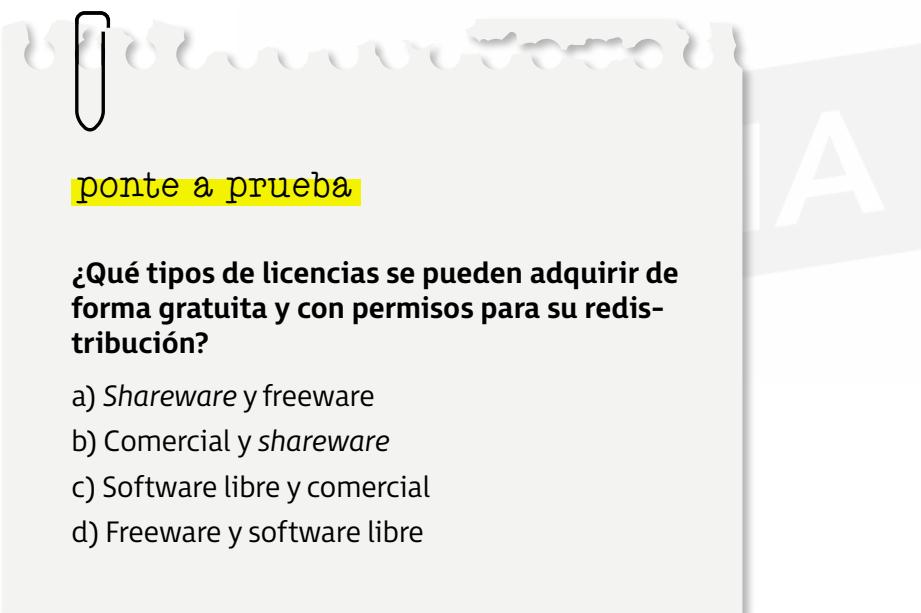
- **Gratuitas (freeware):** este tipo de licencia permite la redistribución de la aplicación. Incluyen su código fuente, pero no permiten modificarlo. No son un software libre.
- **Libres:** está disponible para que cualquier tipo de usuario pueda utilizarlo, copiarlo o distribuirlo, ya sea en su formato original o habiendo realizado modificaciones.
- **Propietarios:** este software es aquel cuyas copias, redistribuciones o modificaciones, en cierta medida, están prohibidas por el propietario. Para realizar este tipo de acciones es necesario solicitar permiso a su propietario o pagar por ello.
- **Comerciales:** son aplicaciones desarrolladas por una empresa, cuyo objetivo es obtener beneficio con su utilización.

Según las licencias de distribución, el software comercial puede ser de varios tipos:

- **OEM:** este tipo de licencia forma parte de un equipo nuevo, ya sea portátil o de sobremesa. Una vez activamos este tipo de licencia, el hardware queda unido a

esta licencia. Una vez adquirida, queda en propiedad del comprador. Los fabricantes ponen las limitaciones del máximo de veces que este software puede reinstalarse. Está totalmente prohibida su venta y cesión a terceros, salvo si en las condiciones de compra está especificado.

- **Retail:** este tipo de licencia suele tener un coste más elevado que las licencias OEM. Sin embargo, es posible reinstalar este software tantas veces como necesitemos, ya que pasa a ser de entera propiedad del usuario. Este puede cederlo a terceros o incluso venderlo.
- **Licencia por volumen:** este tipo de software con licencia por volumen está destinado a grandes usuarios, normalmente empresas. Las condiciones son similares a las OEM, pero sin afectar a nuevos equipos. Se trata de determinar el número de equipos en los que se utilizará, quedando el fabricante autorizado para comprobar las licencias en uso. Este tipo de licencia no se puede ceder a terceros.



ponte a prueba

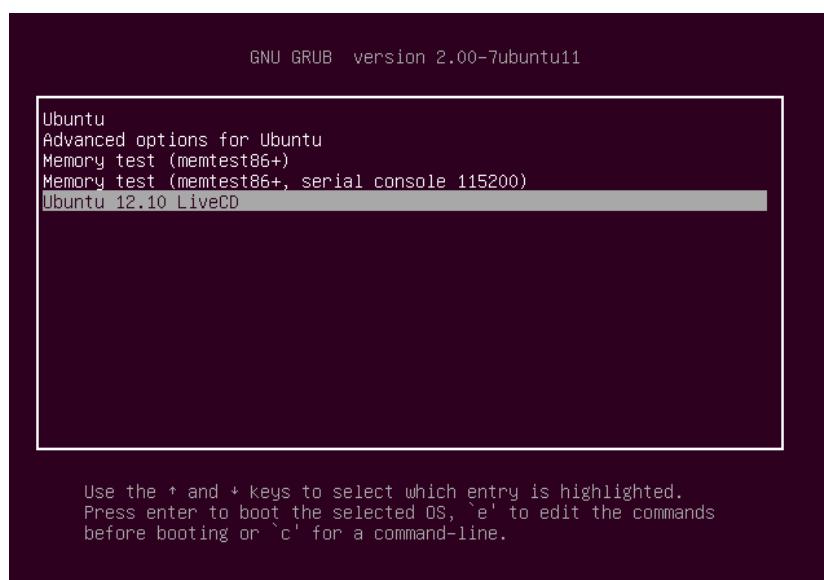
¿Qué tipos de licencias se pueden adquirir de forma gratuita y con permisos para su redistribución?

- a) Shareware y freeware
- b) Comercial y shareware
- c) Software libre y comercial
- d) Freeware y software libre

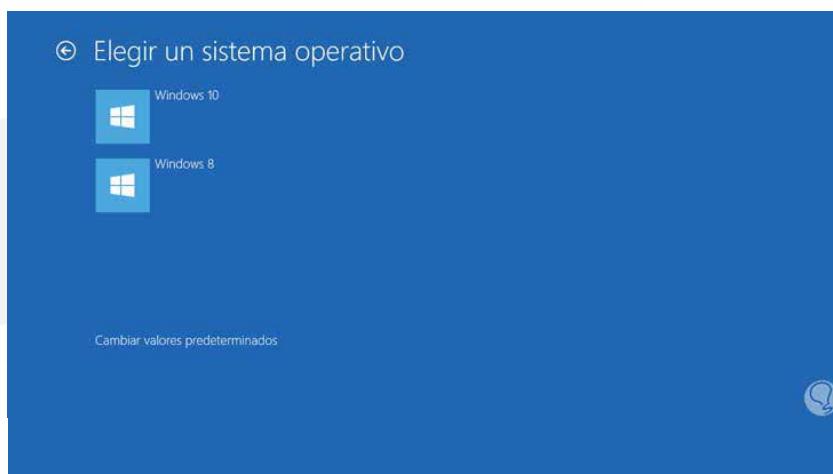
1.9. GESTORES DE ARRANQUE

Los **gestores de arranque** son un pequeño programa que se ejecuta una vez iniciada la BIOS. Su función es preparar los elementos más básicos que precisa el sistema operativo para funcionar y, a veces, nos brinda opciones antes de iniciar el sistema operativo en sí.

Por ejemplo, si tenemos instalados dos sistemas operativos en un mismo equipo, un gestor de arranque como GRUB (<http://www.gnu.org/software/grub/>) nos permite elegir el que deseemos.



Aunque hay otras elecciones dependiendo del sistema operativo. Y es que las versiones de Windows actuales también ofrecen un gestor de arranque que combina diferentes sistemas operativos.



1.10. MÁQUINAS VIRTUALES

Las máquinas virtuales son un software que nos permite instalar sistemas operativos, de tal forma que el sistema crea que está instalado en otro equipo distinto.

Encontramos dos tipos diferentes de máquinas virtuales: las de sistema y las de proceso. Aunque las más habituales y conocidas son las de sistema.

Las máquinas virtuales de sistema emulan un ordenador completo y nos permiten ejecutar un sistema operativo en su interior.

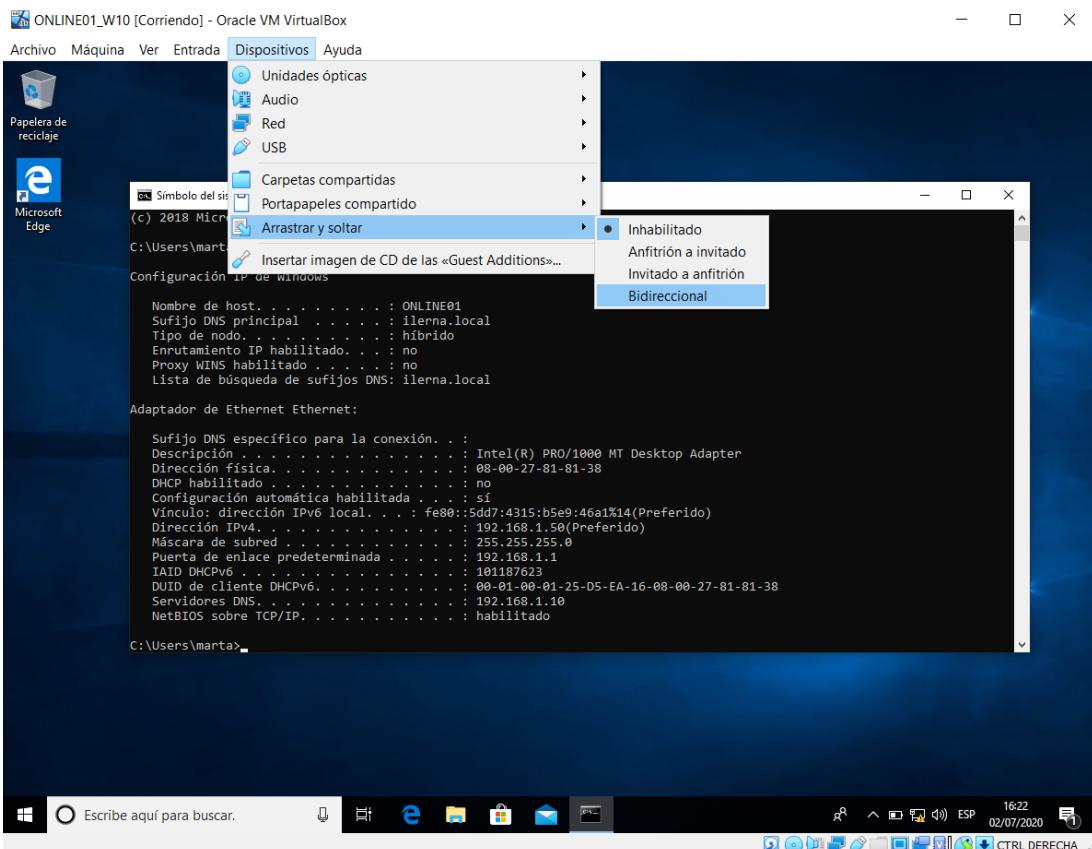
Estas máquinas utilizan el hardware real instalado en la máquina, aunque simulan tener componentes aparte.

Hay que tener en cuenta que no podremos instalar más potencia de hardware de la cual dispongamos en la máquina virtual. No obstante, esto no quiere decir que los componentes deban tener las mismas capacidades.

Por ejemplo, si tenemos 16 GB de RAM instalados en la máquina virtual, podremos dedicar 2 GB. De este modo, simulará ser un equipo con 2 GB de RAM, con las limitaciones que esto conlleve.

En el caso de otros componentes, como las disqueteras de CD-ROM o tarjetas de Red, pueden crearse y sus características dependerán del tipo de software que empleemos.

Para el sistema operativo que instalaremos todo funcionará como si de un PC normal se tratase, totalmente aparte del equipo anfitrión. Los programas de software más utilizados proporcionan herramientas para facilitar la comunicación entre estos dos equipos.



Las máquinas virtuales de proceso son algo diferentes a las comentadas anteriormente. En este caso, no emulan todo un equipo completo, sino que ejecutan un proceso concreto como una aplicación.

Este tipo de máquinas son muy útiles a la hora de crear aplicaciones para varias plataformas. En vez de programar específicamente para un sistema, estas crean un entorno de ejecución que nos permite lidiar con el sistema operativo.



ponte a prueba,

Las máquinas virtuales nos permiten incrementar el hardware instalado en una máquina de forma que podremos mejorar las prestaciones de un sistema informático e instalar más sistemas operativos en este.

- a) Verdadero
- b) Falso

El caso más común de este tipo de máquinas son las de Java, donde podemos crear un aplicativo en este tipo de lenguaje y ejecutarlo en los diferentes sistemas operativos. Y es que el encargado de su funcionamiento será la máquina virtual de Java, que tendremos instalada en estos sistemas.

The screenshot shows the official Oracle Java website. At the top, there's a red header with the Java logo and navigation links for 'Descargar' and 'Ayuda'. Below the header, a large button says 'Descarga gratuita de Java'. To the right of this button is a search bar with a magnifying glass icon. A yellow callout box highlights an important update about the Oracle Java license change, dated April 16, 2019. It mentions that the new license is substantially different from previous ones and provides a link to the 'licencia pública general de código abierto'. At the bottom of the page, there's a red button labeled 'Descarga gratuita de Java' and a footer with links to '¿Qué es Java?', 'Tengo Java?', and 'Necesita ayuda?'.



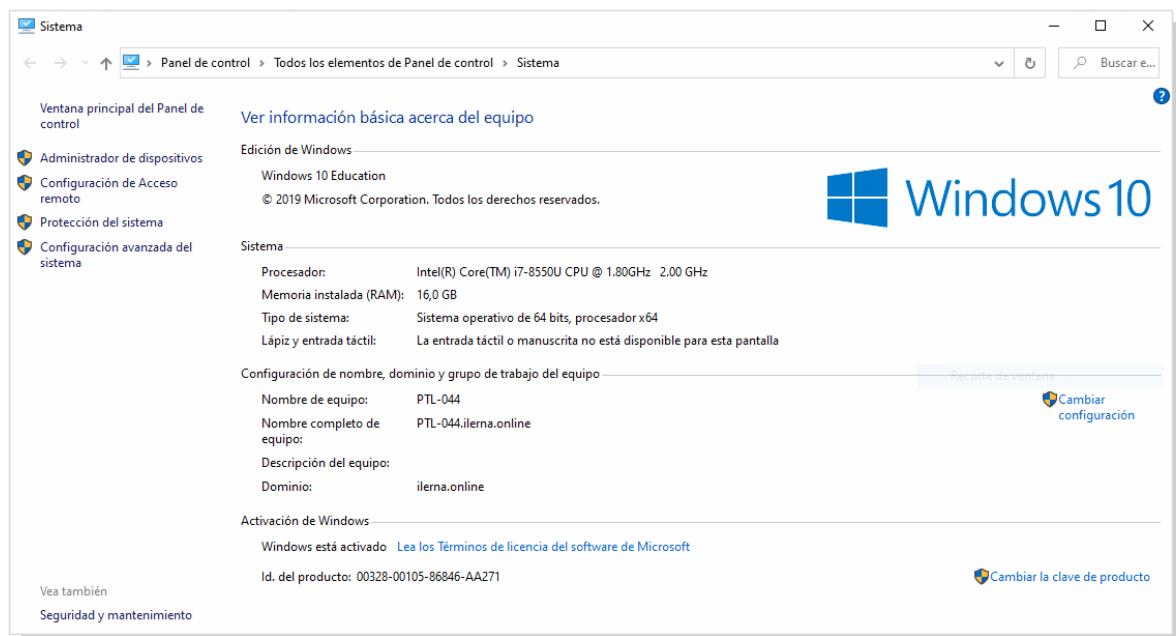
1.11. CONSIDERACIONES PREVIAS A LA INSTALACIÓN DE SISTEMAS OPERATIVOS LIBRES Y PROPIETARIOS

Además del tipo de licencia del sistema operativo que elijamos, hay otra serie de factores que debemos tener muy presentes antes de comenzar con la instalación.

Repasemos los más importantes:

Requisitos de hardware

Generalmente, la documentación de los sistemas operativos ofrece información exhaustiva acerca de las características mínimas requeridas. Analizaremos en profundidad este aspecto en el siguiente apartado.



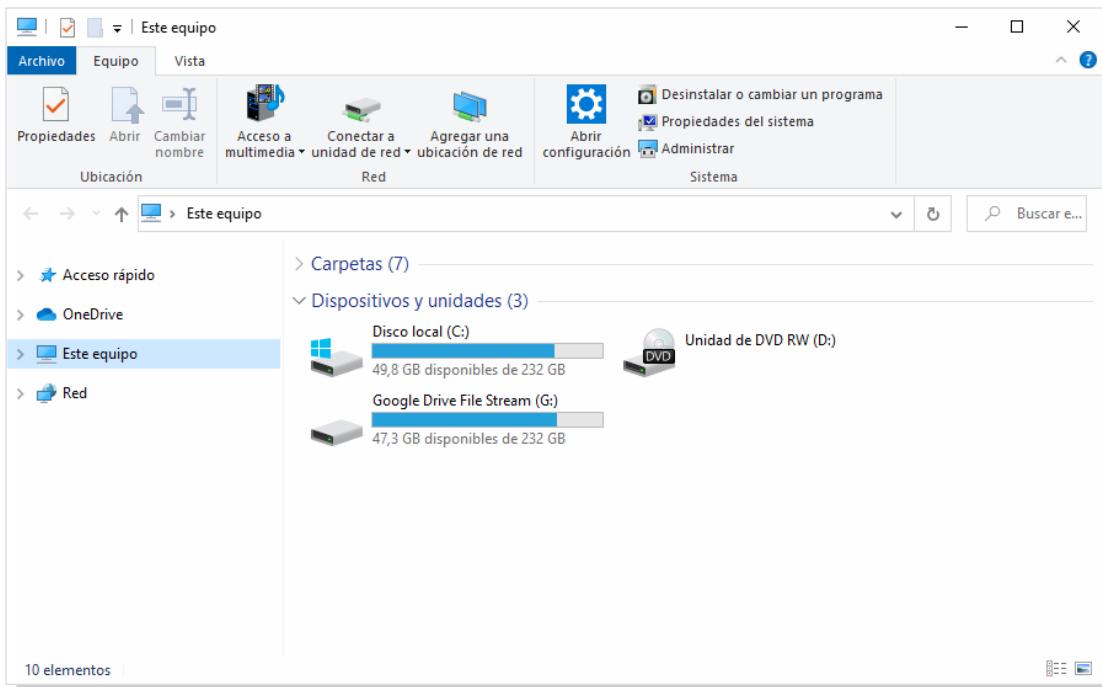
Medios desde los que llevaremos a cabo la instalación del sistema operativo

El equipo debe contar con los periféricos precisos para leer los ficheros de instalación del sistema (lector de DVD, puertos USB, tarjeta de red, etc.).

Unidad de destino del sistema operativo

¿Qué disco o partición es la óptima para instalar el sistema? En líneas generales, siempre será el que brinde mayor rapidez en la lectura y escritura de datos.

Además, también será importante planificar dónde almacenaremos nuestros archivos de usuario. Lo ideal es que el sistema operativo y los archivos se encuentren en diferentes particiones.



Por otra parte, y con toda probabilidad, la instalación del sistema operativo conllevará la destrucción de los datos de la partición elegida, de modo que antes de llevarla a cabo es vital realizar una copia de seguridad de estos.

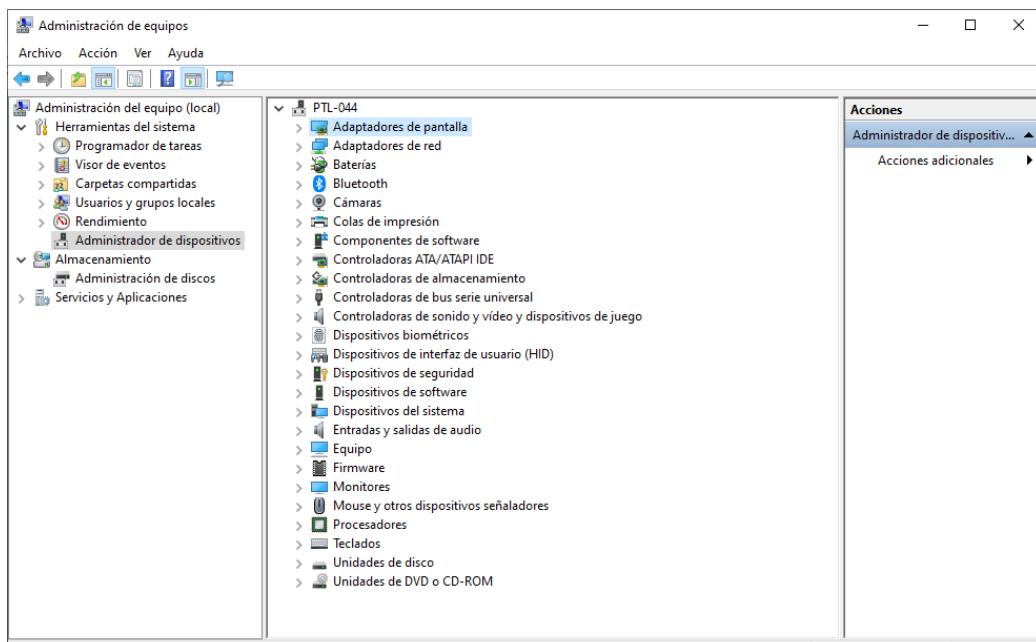
1.12. INSTALACIÓN DE SISTEMAS OPERATIVOS. REQUISITOS, VERSIONES Y LICENCIAS

Un sistema operativo es un programa que grabamos en el disco duro de nuestro ordenador y que, al iniciarse, una parte de él se carga en la memoria. Por lo tanto, este sistema va a ocupar una parte del disco duro y de la memoria de nuestro ordenador. Además, también debemos contar con una tarjeta gráfica y un microprocesador adecuados para soportar su ejecución.

La inmensa mayoría de los sistemas operativos especifican unos requisitos mínimos que debemos cumplir para obtener un buen funcionamiento.

Los requisitos principales para tener en cuenta son:

- Tipo y velocidad de la CPU
- Cantidad de memoria RAM instalada
- Espacio requerido en el disco duro
- Tipo de tarjeta gráfica
- Dispositivos necesarios (lector de DVD, puerto USB, etc.)

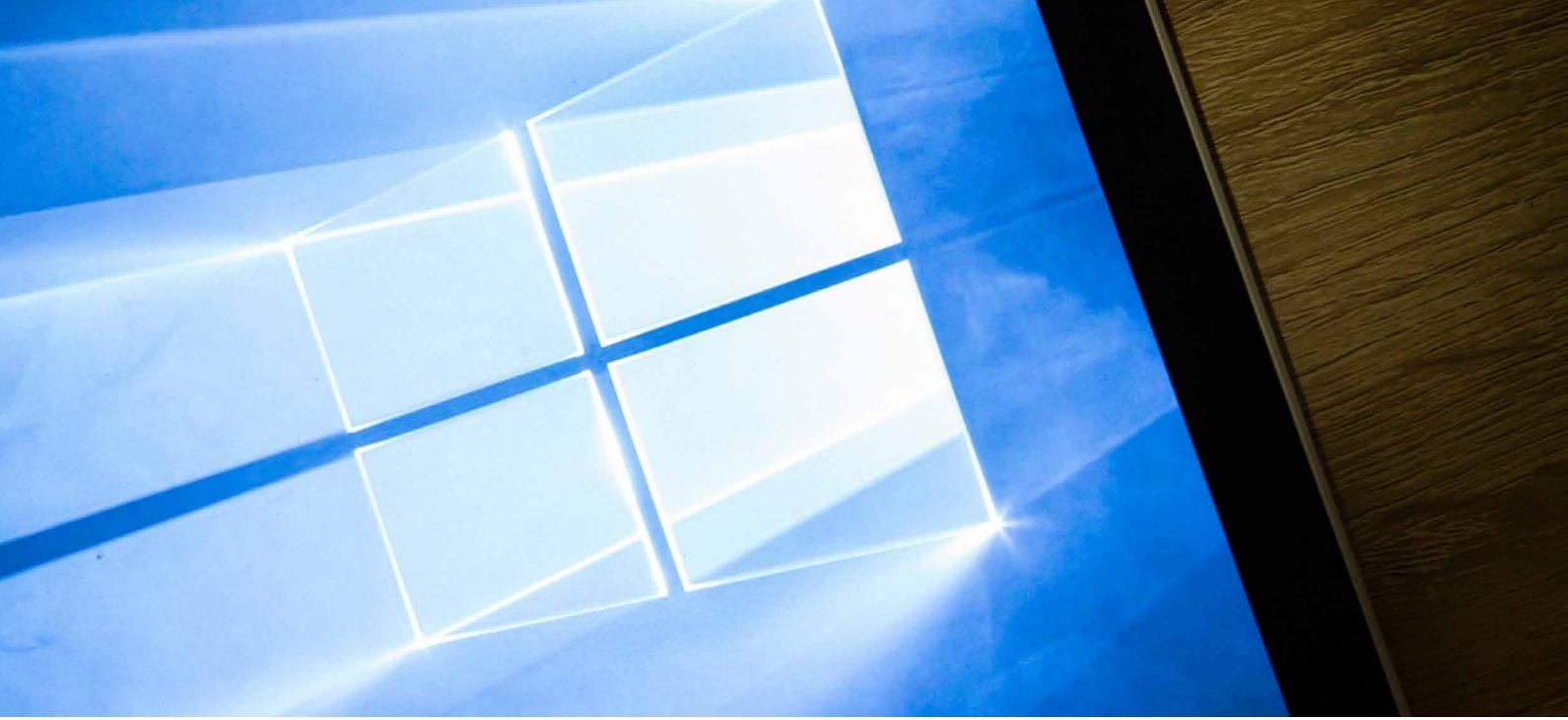


No obstante, en la documentación también suelen especificarse unos requerimientos recomendados. La idea es que los cumplamos para obtener un rendimiento óptimo. En caso de que no sea así, siempre tenemos la posibilidad de decantarnos por una versión más antigua del sistema operativo. Windows XP tiene unos requisitos más bajos que Windows 8, por ejemplo.

Dado que sistemas como Windows ofrecen distintas modalidades, otro factor a considerar es qué modalidad precisamos. Así, por ejemplo, Windows 10 se distribuye en versiones que van desde la Starter (con menos funcionalidades de conectividad y personalización) a la Ultimate (la más completa).

Habitualmente, durante la instalación, se suele preguntar qué componentes queremos agregar para, de este modo, poder personalizar las funcionalidades del sistema operativo. Si por el contrario, no se nos ofrece ninguna opción, significa que la instalación se va a llevar a cabo de manera casi automática.

Una misma versión del sistema puede distribuirse en distintas versiones con diferentes funcionalidades.



Si vamos a instalar un sistema en régimen de propietario, es imprescindible que adquiramos una licencia. Por norma general, cada versión precisa una licencia distinta.

Por último, si no deseamos dedicar una partición al sistema que queremos instalar, contamos con la posibilidad de instalarlo en una máquina virtual, utilizando software como **VirtualBox** (<https://www.virtualbox.org/>) o como **VMware Workstation** (<https://www.vmware.com/es/products/workstation-pro.html>).

Veamos ahora los pasos esenciales para la instalación de **Windows 10**:

1. **Cambiar el orden de arranque** de dispositivos en la BIOS para que se ejecute la instalación desde el DVD. Este punto puede sustituirse por la opción de modificar el dispositivo de arranque sin acceder a la BIOS que hemos visto en puntos anteriores.
2. **Introducir el DVD** original en la bandeja o el **USB de arranque** con la ISO oficial.
3. **Arrancar** el PC.
4. Pulsar el botón **Siguiente**.
5. Hacer clic en **Instalar ahora**.
6. Aceptar los términos de licencia y pulsar **Siguiente**.
7. Decidir si queremos actualizar a Windows 10 usando una **versión anterior del sistema** o si queremos realizar una **instalación nueva**. Optaremos por la segunda opción.
8. **Particionaremos el disco duro**. Si tenemos ya creada una partición seguiremos adelante. De lo contrario, no dirigiremos hacia *Opciones de unidad*. Pulsaremos

luego sobre *Nuevo* para crear una partición nueva y seleccionaremos el tamaño deseado.

CONCEPTO

Las **particiones** son divisiones lógicas en el disco físico. El sistema operativo trata cada partición como si fuera un disco independiente, de modo que podemos tener diferentes sistemas operativos en particiones distintas.

Llegado este punto, distinguimos entre los siguientes tipos de particiones:

- Particiones primarias

Cuentan con la característica de poder ser reconocidas como particiones de arranque. En realidad, un disco formateado consta de una única partición primaria que abarca todo el espacio disponible. Su número está limitado a cuatro.

- Particiones extendidas o secundarias

Actúan como complemento o ampliación de las particiones primarias y permiten definir más unidades lógicas. Se crearon para saltarse la limitación de cuatro particiones primarias por disco.

9. Una vez creadas las particiones, las formatearemos pulsando en **Formatear**. Se iniciará el proceso de instalación de Windows 10 propiamente dicho. El sistema se reiniciará.
10. Definiremos un **nombre de usuario y de equipo** y pulsaremos en *Siguiente*.
11. Introduciremos la **clave de producto**.
12. Activaremos las **actualizaciones de seguridad**.
13. Definiremos la **fecha y hora** del sistema y la zona horaria.
14. Elegiremos la **configuración de red**.

Una vez finalizados los pasos, la instalación habrá terminado y podremos ver el escritorio de Windows 10.

Vemos ahora los pasos clave de una instalación de Linux. Como ejemplo, usaremos **Ubuntu 12**:

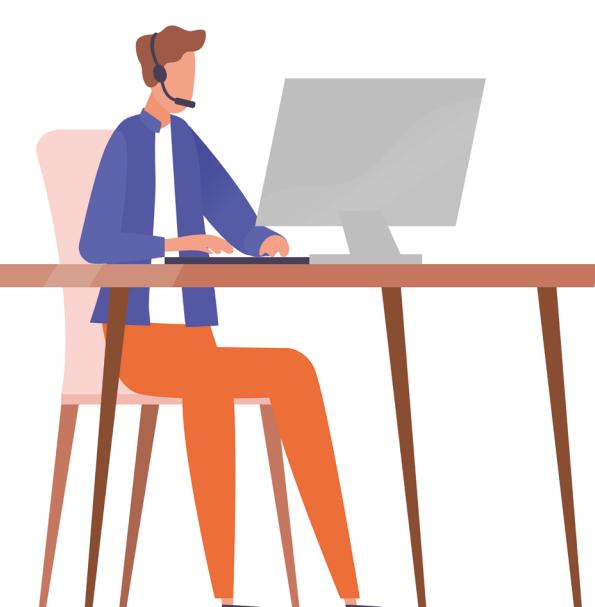
1. Configuramos la BIOS para que **arranque desde el DVD o el pendrive**.
2. **Reiniciamos el PC** con el DVD o el pendrive insertado.
3. Entramos en **GRUB**, el gestor de arranque. Podemos

probar Ubuntu sin instalar para ver si detecta nuestro hardware. No obstante, elegiremos *Instalar*. Para ello, haremos clic en el ícono *Install Ubuntu*.

4. Se inicia el **asistente**. Elegimos el idioma.
5. Confirmamos que reunimos los requisitos mínimos de instalación pulsando en **Continuar**.
6. Elegimos si vamos a **descargar las actualizaciones del sistema** y otras características.
7. Definimos las **particiones de disco**. Aquí se nos presentan tres opciones:
 - Eliminar el sistema operativo anterior e instalar.
 - Instalar Ubuntu juntamente con Windows.
 - Particionar el disco manualmente. Esta opción nos permite crear particiones. Lo ideal es definir tres: en la partición *root*, instalamos el sistema con un formato de archivos EXT4. En la partición *home* almacenamos los documentos. La partición *swap* se usa para grabar archivos temporales cuando se acaba la memoria RAM.
8. Hacemos clic en **Instalar ahora**.
9. Definimos la **zona horaria**.
10. Configuramos el **teclado**.
11. Damos de alta un **nombre de usuario y una contraseña**.

Con esto, accederemos al escritorio de Ubuntu. Como hemos apuntado ya, también tenemos la posibilidad de **instalar sistemas operativos en una máquina virtual**.

Veamos ahora cómo hacerlo en **VirtualBox**:

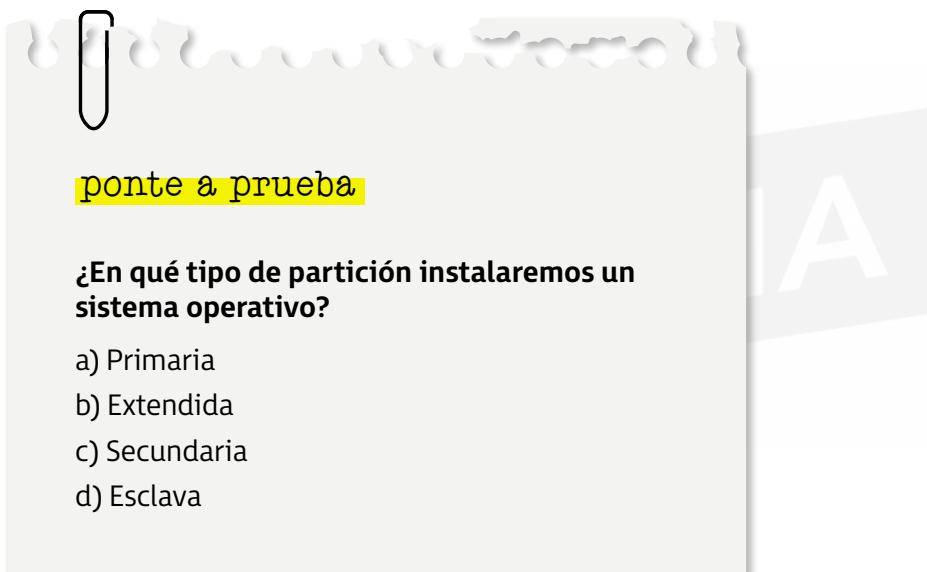
- 
1. Descargamos e instalamos VirtualBox (<https://www.virtualbox.org/>).
 2. **Ejecutamos el software**: la interfaz de VirtualBox se divide en tres áreas: a la izquierda, aparecen nuestras máquinas virtuales ya creadas. A la derecha, vemos el estado de nuestra máquina. El área superior nos permite controlar la máquina virtual.
 3. **Creamos la máquina virtual** pulsando en *Nueva*.
 4. En el asistente, elegimos el **sistema operativo** que vamos a instalar.
 5. **Definimos la memoria RAM** que le asignaremos al sistema operativo.
 6. **Configuramos el disco duro virtual**: establecemos su nombre, su tamaño y el resto de las opciones. En este caso escogemos *Dinámico* y así su tamaño irá aumentando conforme aumente el espacio que precisa la

máquina virtual.

7. Hacemos clic en ***Crear*** y la máquina virtual quedará creada y lista.
8. **Introducimos el disco de instalación del sistema operativo.** En el menú de configuración entramos en *Almacenamiento* y seleccionamos la unidad escogida anteriormente.
9. **Iniciamos la máquina** que hemos creado haciendo clic en el botón *Iniciar*. El proceso de instalación del sistema operativo comenzará.

Los pasos serán los mismos que hemos definido en Windows o en Ubuntu. Una vez finalizado el proceso tendremos a nuestra disposición un sistema operativo completo accesible desde VirtualBox.

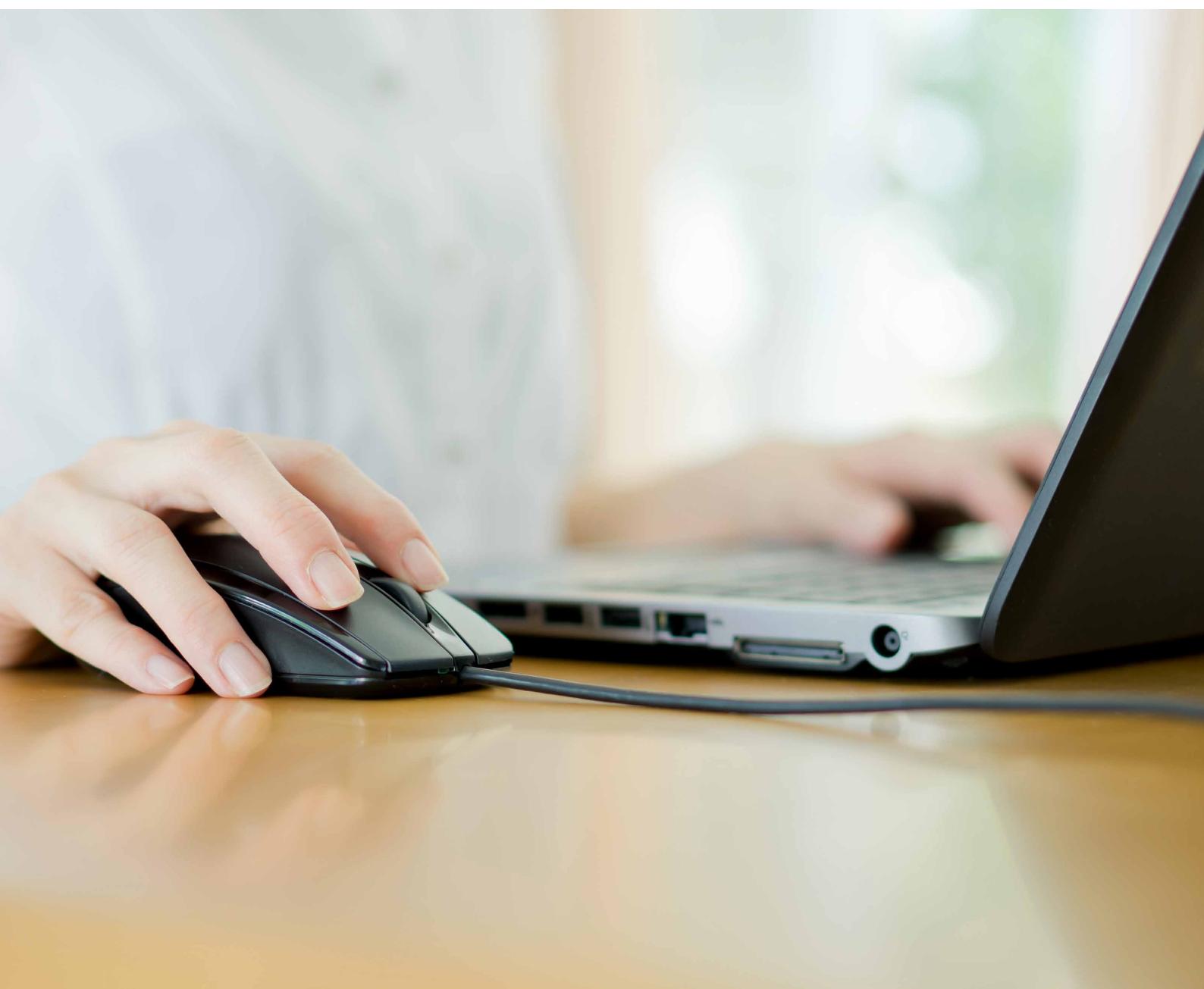
En caso de utilizar la plataforma de virtualización VMware Workstation el proceso es muy similar al descrito para VirtualBox.



1.13. INSTALACIÓN Y DESINSTALACIÓN DE APLICACIONES. REQUISITOS, VERSIONES Y LICENCIAS

Buena parte de lo que hemos aprendido en referencia a los sistemas operativos es aplicable a las aplicaciones. Antes de instalarlas debemos estar seguros de que cumplimos lo especificado en la documentación:

- **Requisitos:** nuestro hardware y sistema operativo son aptos para la ejecución de las aplicaciones.
- **Versiones:** la versión más reciente, más completa y cara no será necesariamente la mejor. Deberemos estudiar cuál responde mejor a los fines que perseguimos.

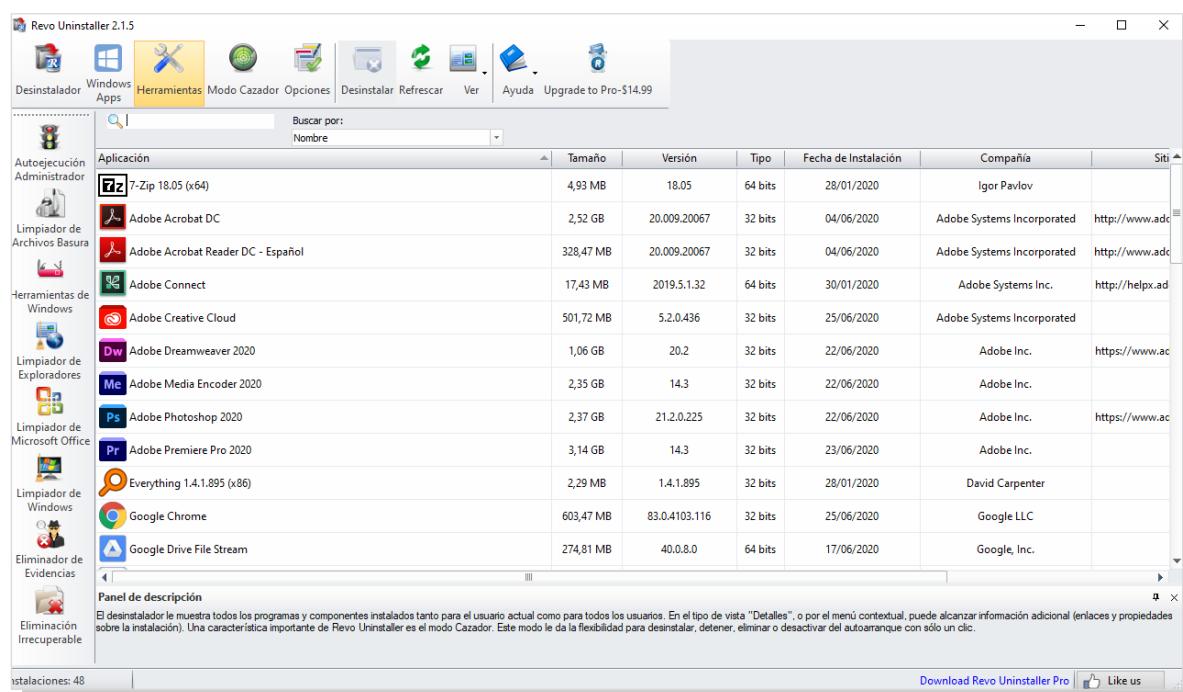
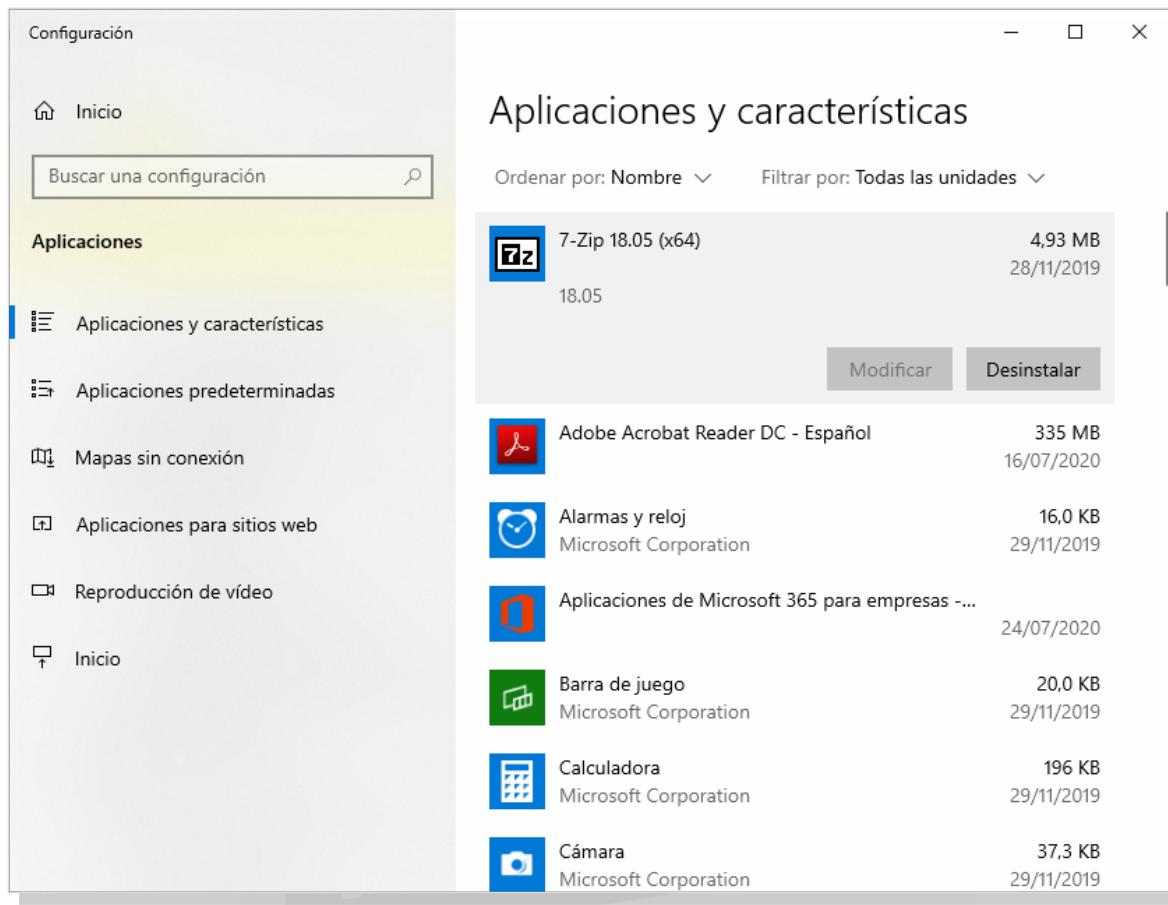


- **Licencia:** en el caso de aplicaciones con licencia *shareware* o comercial deberemos actuar de acuerdo con la legalidad vigente.

La instalación de una aplicación implica llevar a cabo las operaciones precisas para que los usuarios del equipo puedan ejecutarla. Normalmente disponen de un asistente, aunque en casos muy específicos, las aplicaciones se distribuyen en un paquete comprimido que bastará con descomprimir.

La desinstalación es el proceso inverso y el sistema operativo suele brindar herramientas para este fin, tales como la sección **Agregar y quitar programas de Windows**, accesible a través del **Panel de control**. De nuevo, será un

asistente el que se encargará de eliminar, no solo los archivos de la aplicación en sí, sino también las trazas que hayan podido quedar en los ficheros de configuración del sistema operativo.



Por último, debemos señalar que las sucesivas instalaciones y desinstalaciones van dejando restos en los ficheros de configuración. A la larga, estos restos pueden incidir negativamente en el rendimiento de nuestro sistema operativo. Por este motivo, es conveniente agregar únicamente aquellos programas que nos resulten imprescindibles.



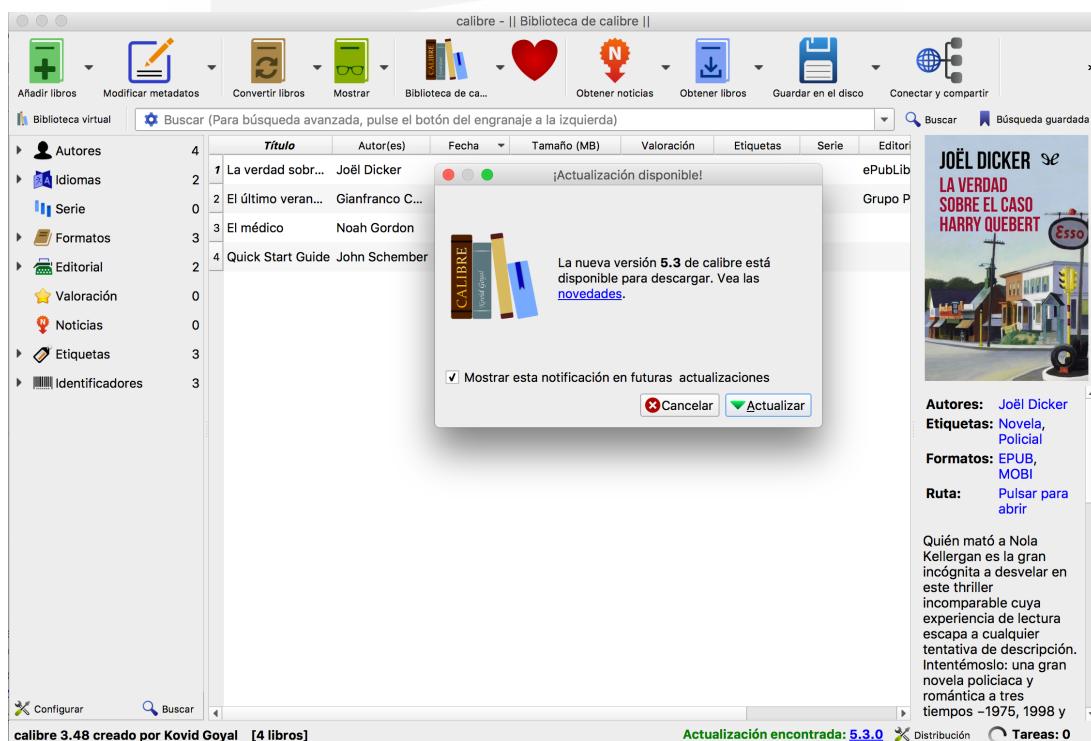
Para llevar a cabo una desinstalación más rigurosa, que se encargará de borrar trazas que el sistema operativo no borraría, podemos usar aplicaciones específicas para este fin, como **RevoUninstaller**.

1.14. ACTUALIZACIÓN DE SISTEMAS OPERATIVOS Y APLICACIONES

Al instalar una nueva versión de una aplicación que ya estaba presente en nuestro sistema pueden darse dos posibilidades:

- **Actualización:** basta con instalar la nueva versión sin desinstalar la previa para que el software se actualice.
- **Instalación en limpio:** algunas veces debemos desinstalar la versión previa antes de instalar la nueva.

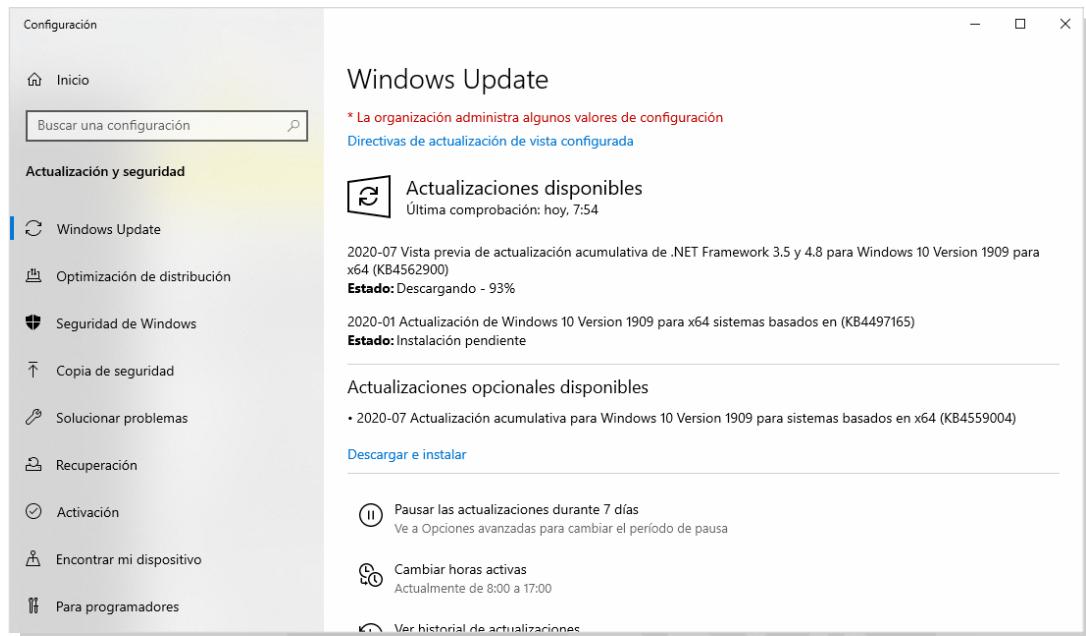
Para saber cómo actuar consultaremos la documentación del software. En ocasiones nos advertirá desde su propia interfaz de que hay actualizaciones disponibles.



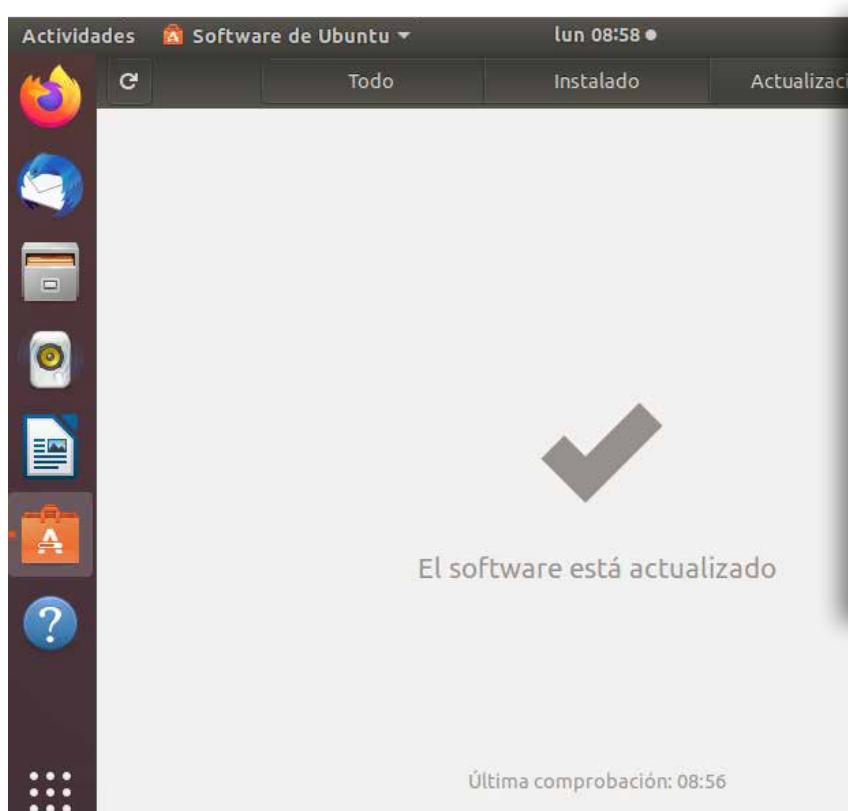
El software, en ocasiones, nos advertirá desde su propia interfaz de que hay actualizaciones disponibles.

Los sistemas operativos también acostumbran a advertirnos de que hay actualizaciones disponibles. Estas no solo mejorarán y perfilarán las funcionalidades, sino que también redundarán en una mayor seguridad. Por este motivo, es importante descargarlas e instalarlas.

En el caso de Windows, contamos con el módulo denominado Windows Update.



En cambio, para sistemas operativos Linux lo más común es utilizar los comandos *Update* y *Upgrade* para comprobar si requiere actualizaciones. Aunque cada vez es más habitual encontrar aplicaciones como en los sistemas operativos Ubuntu, donde cuentan con una aplicación (Centro de Software de Ubuntu) para comprobar el estado de actualizaciones del sistema y no tener que utilizar el entorno de texto.



ponte a prueba

Tener el sistema operativo actualizado a sus últimas versiones mejorará y perfilará sus funcionalidades y nos ofrecerá una mayor seguridad.

- a) Verdadero
- b) Falso

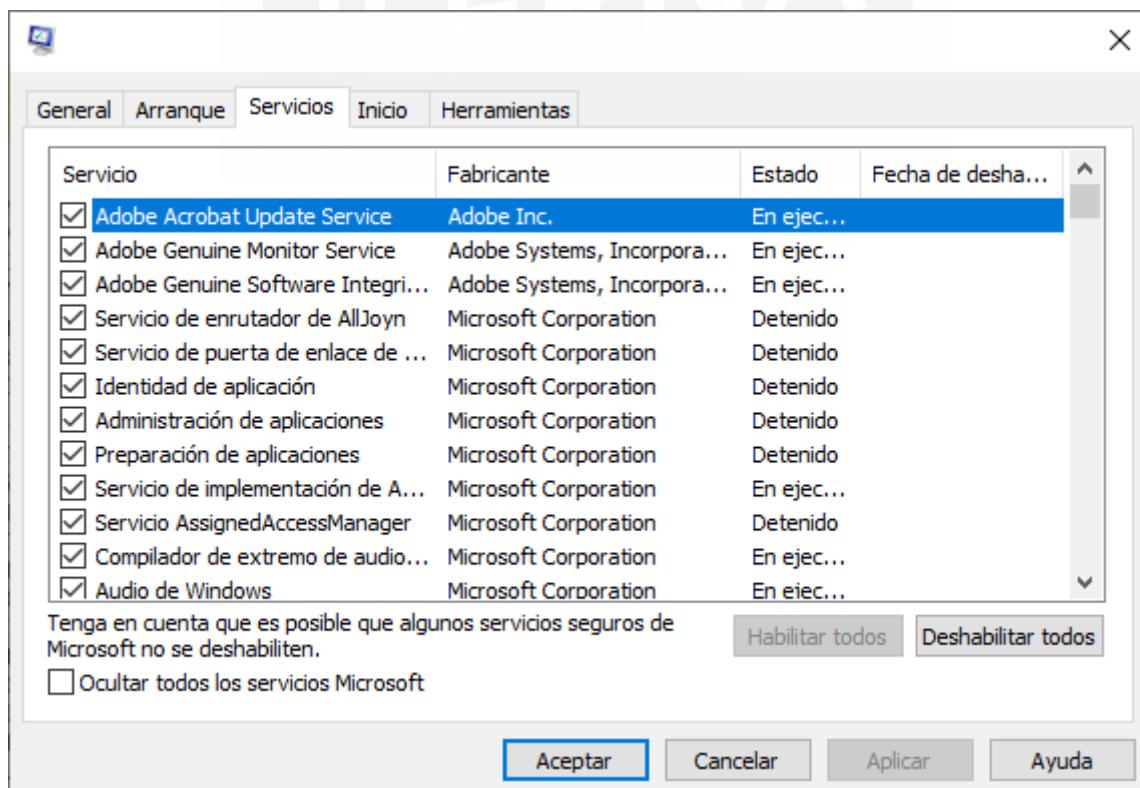
1.15. ARCHIVOS DE INICIO DE SISTEMAS OPERATIVOS

Los pasos al iniciar un ordenador pueden variar dependiendo de diversos factores, tales como el dispositivo de arranque, la existencia de particiones en este, etc. No obstante, en líneas generales consta de los siguientes pasos:

1. En un primer momento, la BIOS inicia la pantalla y el teclado y verifica la memoria RAM, la fecha y otros datos. El orden de arranque de los periféricos es clave para determinar que el sistema se inicie correctamente.
2. A continuación, se carga el gestor de arranque y, seguidamente, el sistema operativo en sí. En esta fase, se ejecutan lo que denominamos archivos de inicio. Estos se ocupan de cargar en memoria los servicios o los programas residentes como los antivirus, etc.

Con frecuencia, los archivos de inicio pueden editarse con un editor de texto simple como el **Bloc de notas**. En algunos casos contamos con la posibilidad de operar cambios en ellos a través de un software específico.

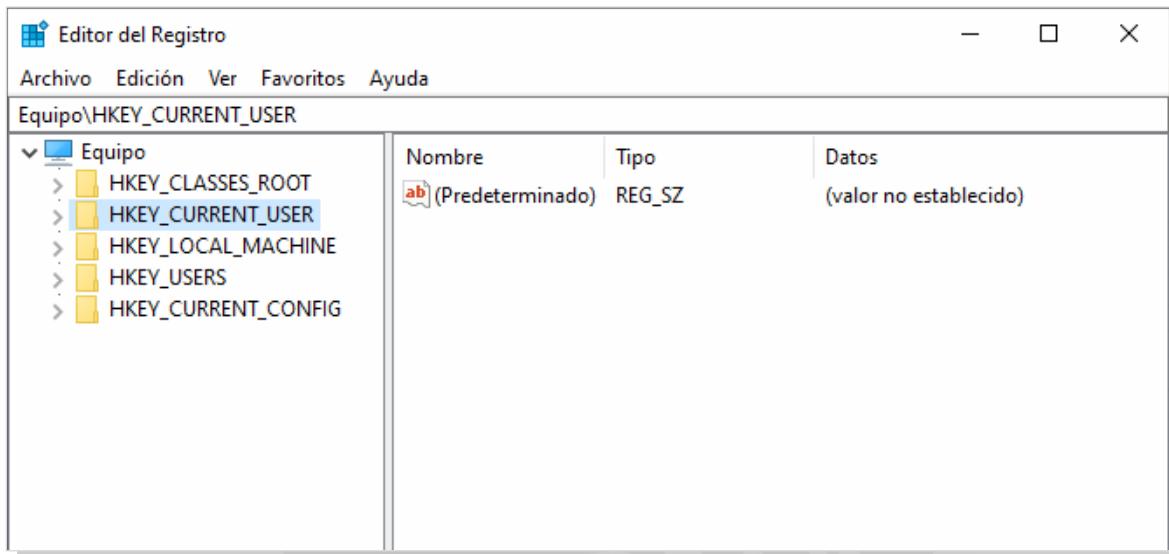
En Windows, por ejemplo, podemos emplear con este fin **MSConfig**. Para ello, pulsaremos **Win+R** y, en el cuadro de diálogo que se mostrará, teclearemos **MSConfig**.



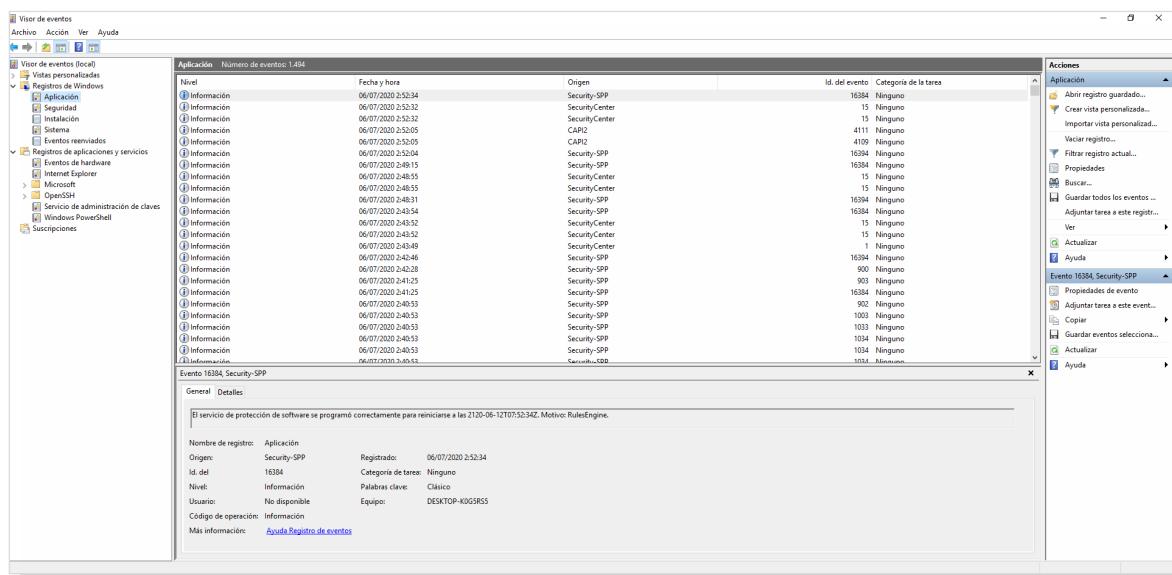
1.16. REGISTRO DEL SISTEMA

En determinados sistemas operativos, como Windows, se nos brinda un registro a través del cual se centraliza la configuración del sistema operativo, sus servicios y las aplicaciones que tenemos instaladas.

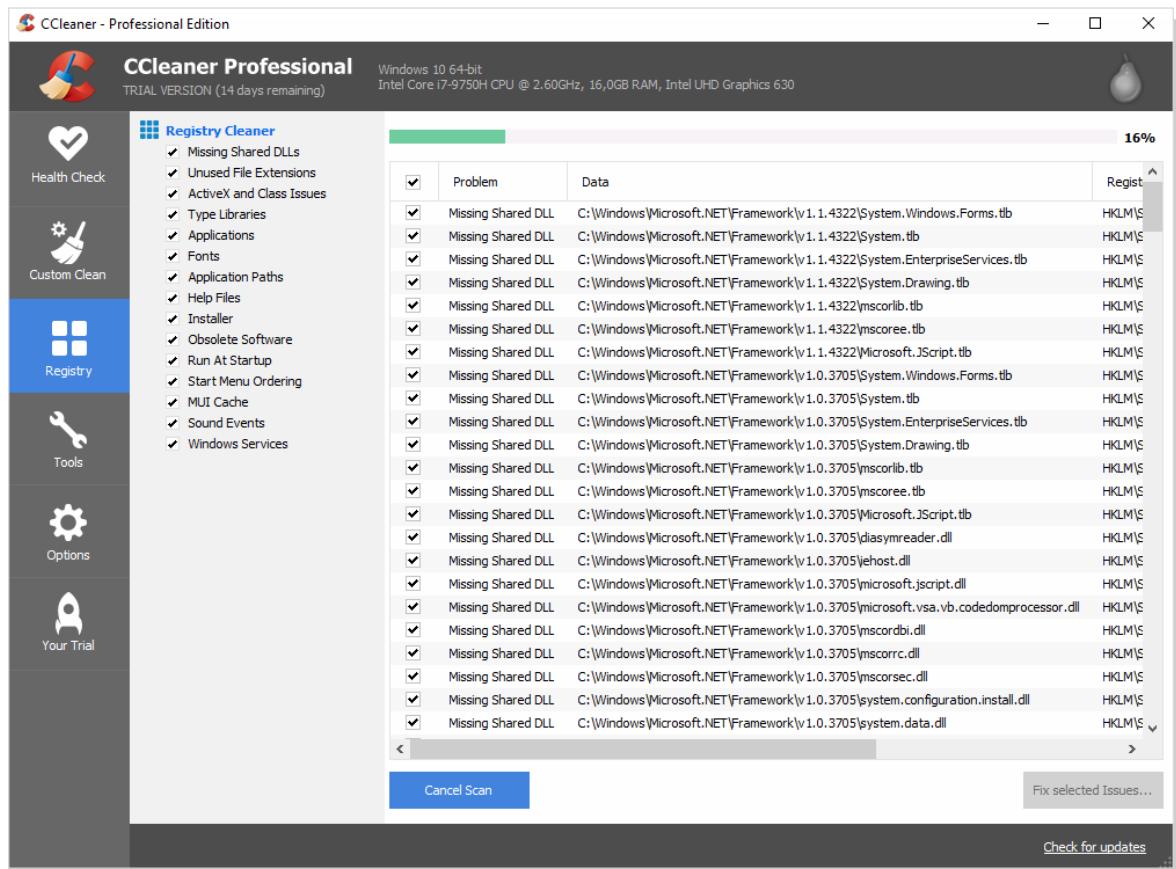
Para acceder al registro pulsaremos **Win+R** y, en el cuadro de diálogo que se mostrará, teclearemos **Regedit**.



En los mismos sistemas de Windows encontramos otras herramientas como el *Visor de eventos* para complementar la información de los registros del sistema, ya que de este modo podemos agruparlos en diferentes clasificaciones.



Para un funcionamiento idóneo del registro y, en definitiva, del sistema operativo, es preciso realizar regularmente un mantenimiento y una limpieza. Para ello, pueden emplearse aplicaciones como **CCleaner**.



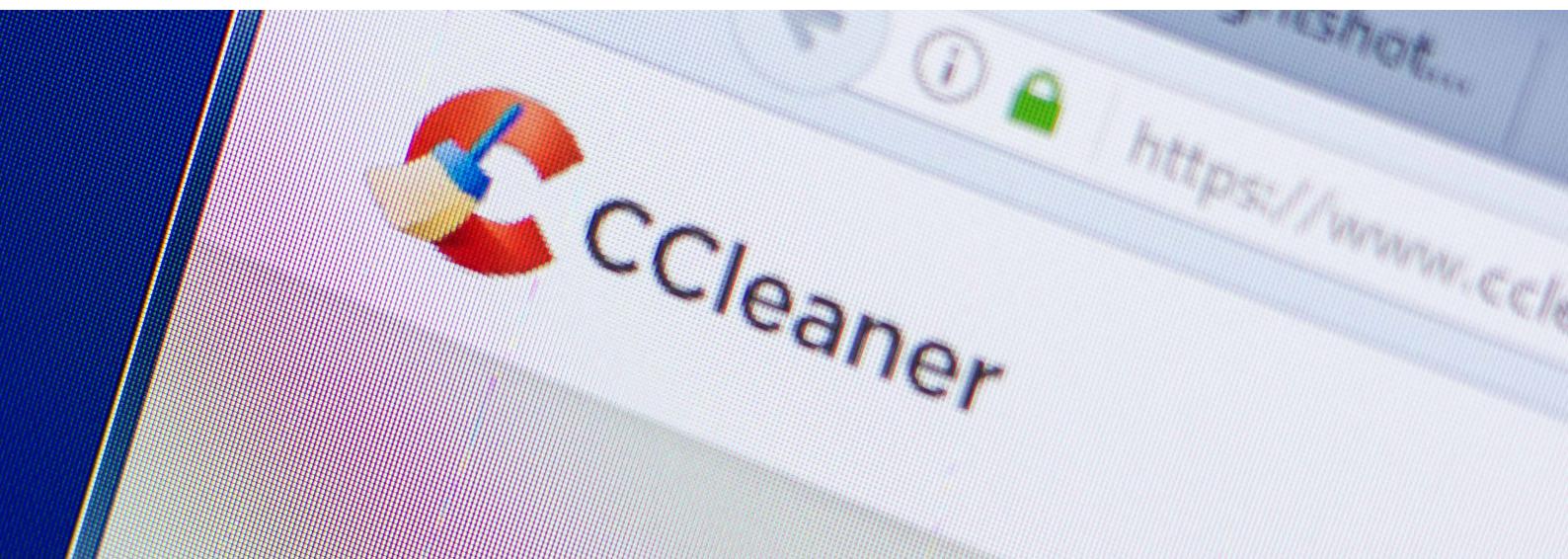
BUSCA EN LA WEB

www.piriform.com/
ccleaner/download

ponte a prueba

Para un funcionamiento óptimo de los
registros, debemos realizar regularmente un
mantenimiento y limpieza de estos.

a) Verdadero
b) Falso



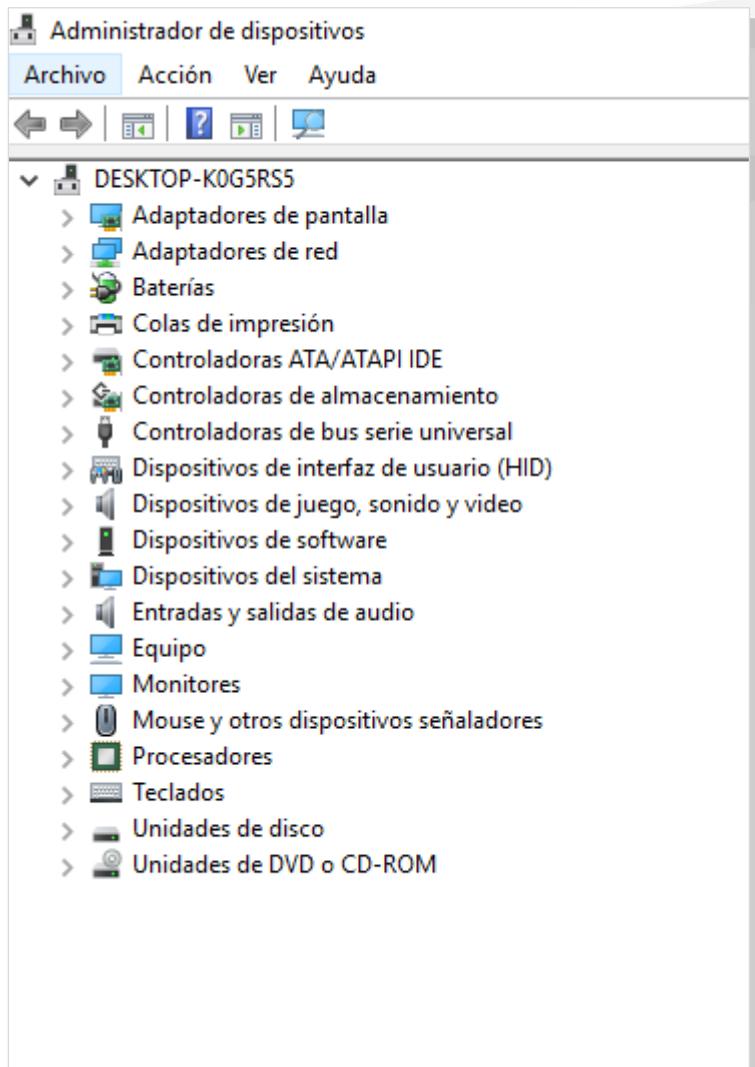
1.17. ACTUALIZACIÓN Y MANTENIMIENTO DE CONTROLADORES DE DISPOSITIVOS

Cuando adquirimos equipos o dispositivos, los fabricantes de hardware acostumbran a incluir drivers o controladores que permiten que el sistema operativo pueda trabajar con ellos. Es muy habitual que vayan apareciendo nuevas versiones de dichos drivers para optimizar el rendimiento del hardware, corregir posibles errores, etc.

Por tanto, es conveniente actualizar los controladores para maximizar el rendimiento y minimizar la posibilidad de que surjan problemas en el futuro.

Para ello contamos con diversas opciones:

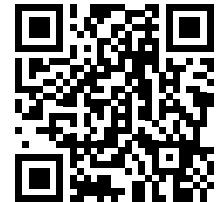
- **Actualización desde el propio sistema:** cuando el sistema operativo nos permite comprobar si hay nuevas versiones podemos actualizarlas directamente. En Windows, esta tarea se puede llevar a cabo desde el Administrador de dispositivos.





¿Qué son los controladores o drivers?

youtu.be/VziSxt-m8aQ



- **Descarga online:** casi todos los fabricantes disponen de una web desde la que nos podemos descargar las nuevas versiones.

The screenshot shows the HP Controladores y descargas website. At the top, there is a cookie consent banner with options to accept or decline cookies for personalization, advertising, and analytics. Below the banner, the HP logo and navigation tabs for 'Particulares', 'Profesionales', and 'Soporte' are visible. A search bar is on the right. The main header reads 'Controladores y descargas'. Below the header, there are three main sections: 'Controladores y descargas' (with a download icon), 'Resolución de problemas' (with a monitor icon), and 'Foros de soporte' (with a user icon). Under 'Controladores y descargas', there is a 'Buscar por producto' field and a 'Detectar mi producto' section with a 'Buscar ahora' button.

Captura de pantalla de la página web de descarga de los controladores de HP.

Dada la importancia de los drivers, lo ideal es respaldar todos los que tengamos instalados en un momento en el que todo funcione correctamente. De este modo, si más adelante necesitamos reinstalar el sistema operativo, podremos restaurarlo sin tener que buscar y descargar individualmente cada uno de ellos. Con este fin podemos emplear aplicaciones como **Double Driver**.

The screenshot shows the Double Driver [Backup] application window. The title bar reads 'Double Driver [Backup]' and 'Version 4.1.0'. The menu bar includes Home, Backup, Restore, Select, Save, Print, Clear, Help, About, and Exit. The main area is a table listing drivers with columns for Name, Version, Date, Provider, and Class. Several drivers are checked, including 'Intel(R) UHD Graphics 630', 'NVIDIA GeForce GTX 1650', and 'NVIDIA High Definition Audio'. At the bottom, there are buttons for 'Scan Current System', 'Scan Other System', and 'Backup Now'.







2

ADMINISTRACIÓN DE SOFTWARE DE BASE

Cuando hablamos de **software** nos referimos al conjunto de instrucciones que se desarrollan de forma ordenada para realizar una tarea concreta. Y si especificamos un poco más, podemos decir que el software de base es el programa encargado de controlar el ordenador.

Cuando tenemos que administrar un sistema multiusuario es fundamental saber cuáles son los usuarios y los grupos. Una vez identificados, podremos crear las cuentas de usuario y grupos de manera organizada y estructurada.

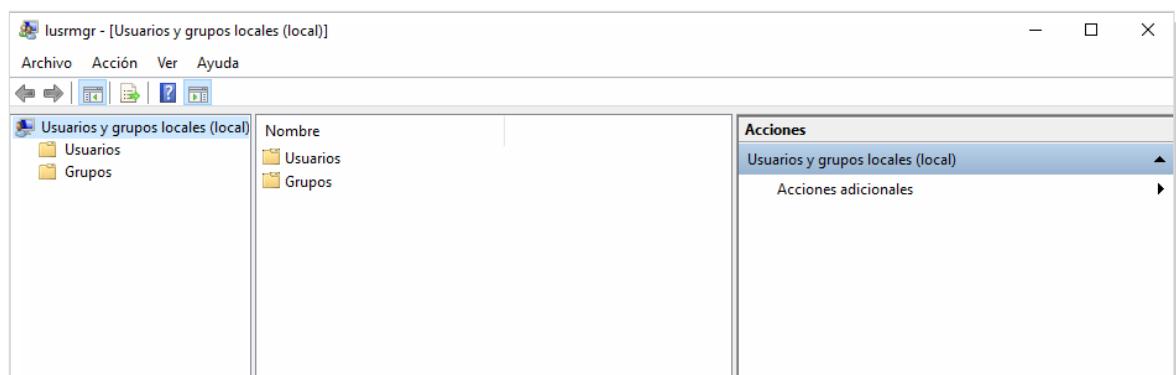
Además, debemos tener en cuenta también una serie de aspectos específicos, relacionados con el nombre de los usuarios, las contraseñas y las restricciones (en función del horario, del uso del espacio del disco, etc.).

A continuación, iremos desarrollando los siguientes apartados:

2.1. ADMINISTRACIÓN DE USUARIOS Y GRUPOS LOCALES

Mediante las cuentas de usuarios se identifica y autentifica un individuo con el sistema. Cuando sobre un mismo equipo pueden trabajar varias personas, donde cada una puede tener su propio espacio de trabajo (fondos de escritorios, carpetas e incluso sus propias aplicaciones), debemos tener en cuenta los usuarios y sus grupos.

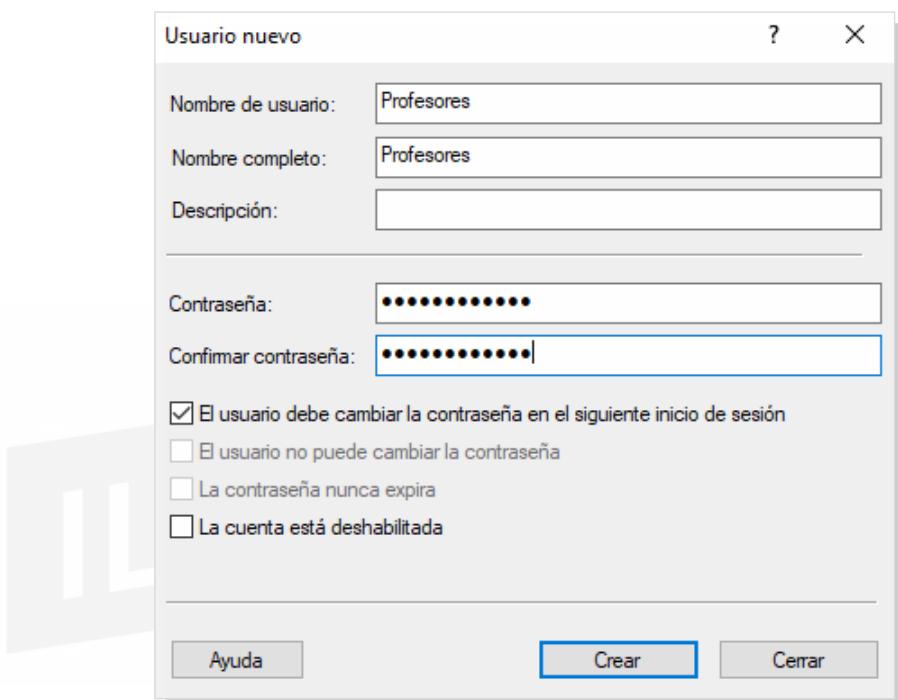
Si nos centramos en nuestro centro educativo, como ejemplo, podemos tener varios tipos de personas que utilicen un ordenador en las aulas, como son: los profesores, los alumnos o un trabajador del departamento de informática. Por seguridad, cada grupo tiene una serie de restricciones y limitaciones a la hora de trabajar sobre el mismo equipo.



El usuario administrador es el encargado de dar acceso a los usuarios y controlar todas las operaciones que vayan a desarrollar a través de las cuentas de usuario. Este usuario no tiene límites a la hora de trabajar sobre el sistema.

Nombre	Nombre completo	Descripción
Administrador		Cuenta integrada para la administración del equipo o dominio
DefaultAccount		Cuenta de usuario administrada por el sistema.
lerna		
Invitado		Cuenta integrada para el acceso como invitado al equipo o dominio
Online		
WDAGUtilityAc...		Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

Los sistemas operativos multiusuario (como Windows 10 o Linux) nos ofrecen la posibilidad de que cada usuario se registre de forma obligatoria al iniciar sesión.



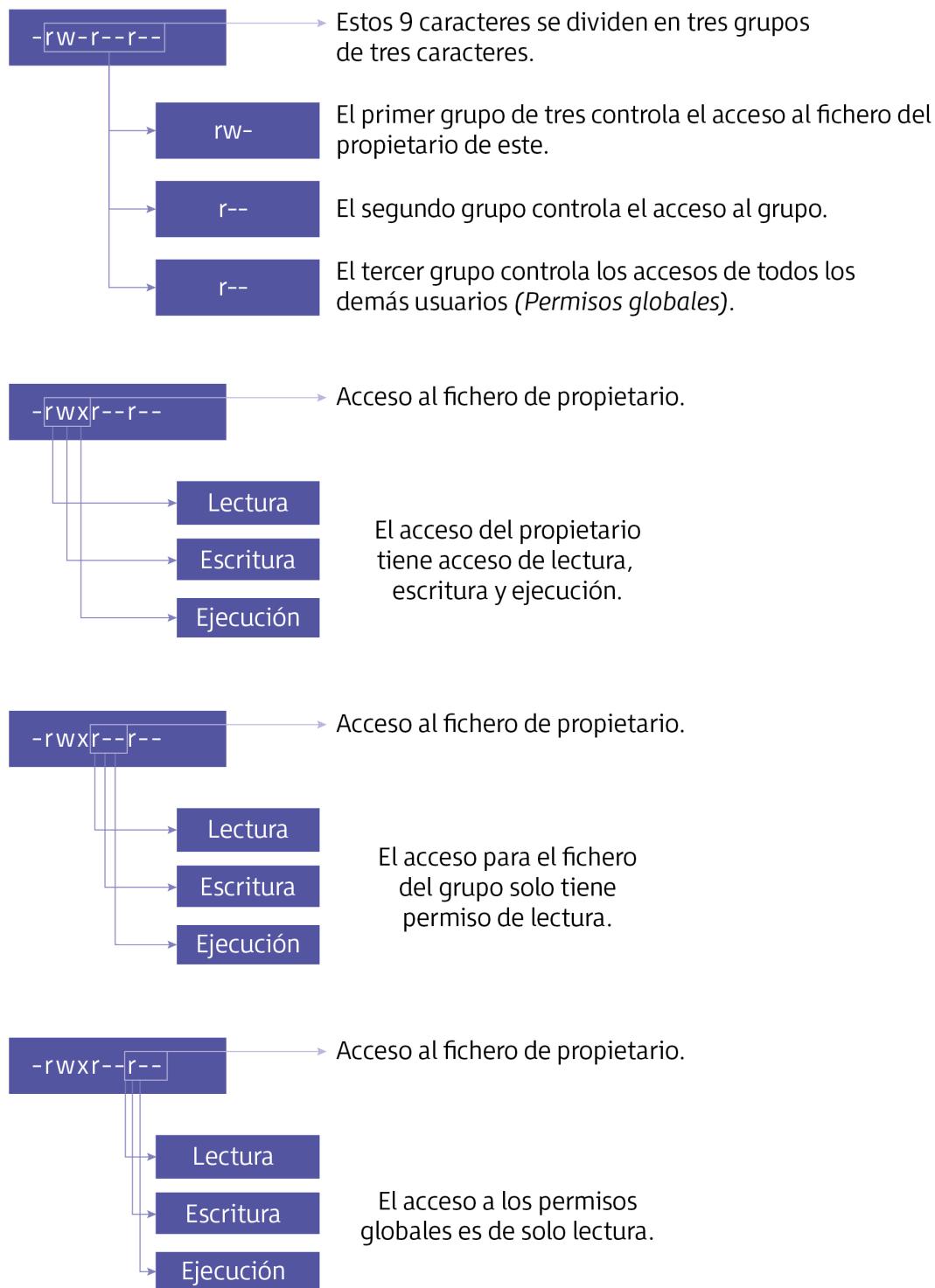
Así, cada uno de ellos dispone de su propio *login* (nombre de usuario) y *password* (contraseña). Gracias a estos datos se puede controlar el acceso de los usuarios. La estructuración mediante usuarios también nos permite asignar permisos y restricciones para cada uno de ellos.

Por ejemplo, a la hora de trabajar con ficheros, podemos establecer diferentes permisos en función del usuario:

- **Lectura (read)**: el usuario tiene la posibilidad de abrir y leer los contenidos del fichero.
- **Escritura (write)**: con este permiso, el usuario puede, además, hacer cualquier modificación sobre el fichero.
- **Ejecución (execute)**: ofrece al usuario la posibilidad de ejecutar el fichero.

La gestión de usuarios la llevará a cabo el usuario administrador o *root*, que es el que dispone de todos los permisos sin ninguna limitación.

La siguiente figura ejemplifica la gestión de permisos en Linux:



Para simplificar la administración de recursos tenemos la opción de **establecer grupos de usuarios**. Si volvemos a nuestro ejemplo del centro de enseñanza, un grupo de usuarios lo conformarían los alumnos o los profesores en general. De esta forma, utilizando los grupos, es más fácil para el administrador conceder o denegar permisos a varios usuarios a la vez, en lugar de hacerlo de forma individual.

Usuarios y grupos locales (local)	Nombre	Descripción
Usuarios	Administradores	Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Grupos	Administradores de Hyper-V	Los miembros de este grupo tienen acceso completo y sin restricciones a todas las características de Hyper-V.
	Duplicadores	Pueden replicar archivos en un dominio
	IS_JURS	Grupo integrado usado por Internet Information Services.
	Invitados	De forma predeterminada, los invitados tienen el mismo acceso que los miembros del grupo Usuarios, excepto la cuenta de invitado que tiene más restricciones
	Lectores del registro de eventos	Los miembros de este grupo pueden leer registros de eventos del equipo local
	Operadores criptográficos	Los miembros tienen autorización para realizar operaciones criptográficas
	Operadores de asistencia de control de acceso	Los miembros de este grupo pueden consultar de forma remota los atributos de autorización y los permisos para los recursos de este equipo.
	Operadores de configuración de red	Los miembros en este equipo pueden tener algunos privilegios administrativos para administrar la configuración de las características de la red
	Operadores de copia de seguridad	Los operadores de copia de seguridad pueden invalidar restricciones de seguridad con el único propósito de hacer copias de seguridad o restaurar archivos.
	Propietarios del dispositivo	Los miembros de este grupo pueden cambiar la configuración de todo el sistema.
	System Managed Accounts Group	Los miembros de este grupo los administra el sistema.
	Usuarios	Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar la mayoría de aplicaciones
	Usuarios avanzados	Los usuarios avanzados se incluyen para la compatibilidad con versiones anteriores y poseen derechos administrativos limitados
	Usuarios COM distribuidos	Los miembros pueden iniciar, activar y usar objetos de COM distribuido en este equipo.
	Usuarios de administración remota	Los miembros de este grupo pueden acceder a los recursos de WMI mediante protocolos de administración (como WS-Management a través del servicio Administración remota de Windows). Esto se aplica a los sistemas operativos que admiten WS-Management.
	Usuarios de escritorio remoto	A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente
	Usuarios del monitor de sistema	Los miembros de este grupo tienen acceso a los datos del contador de rendimiento de forma local y remota
	Usuarios del registro de rendimiento	Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar procedimientos de seguimiento y recopilar seguimientos de eventos localmente y a través del acceso remoto a través de la consola de administración remota
	IernaUsers	Usuarios de Ierna Online

Hay dos situaciones clave en las que usar grupos resulta extremadamente útil:

- **Creación de grupos para la asignación de recursos:** ideal si hemos instalado un nuevo recurso y queremos asignarlo a varios usuarios. Así, por ejemplo, si acabamos de agregar un escáner en red, podemos crear un grupo llamado *Usuarios_escaner* al que le ofreceremos acceso para escanear.

Seguidamente, elegiremos a los usuarios que precisan acceso a dicho periférico y los incluiremos.

- **Gestión simplificada de usuarios:** para no tener que definir los permisos de cada usuario de manera individualizada, podemos crear grupos que reúnan una serie de características en lo referente a privilegios de acceso.

Por ejemplo, si creamos el grupo *Administrativos_red* y asignamos a todos los administrativos de la empresa a dicho grupo, la tarea se simplificará sustancialmente frente a la alternativa de tener que definir los mismos permisos para cada trabajador.



ponte a prueba

En un sistema Linux, podemos representar los diferentes permisos con 9 caracteres que se dividen en grupos de tres caracteres. ¿A qué hace referencia el primer grupo de tres caracteres (empezando por la izquierda)?

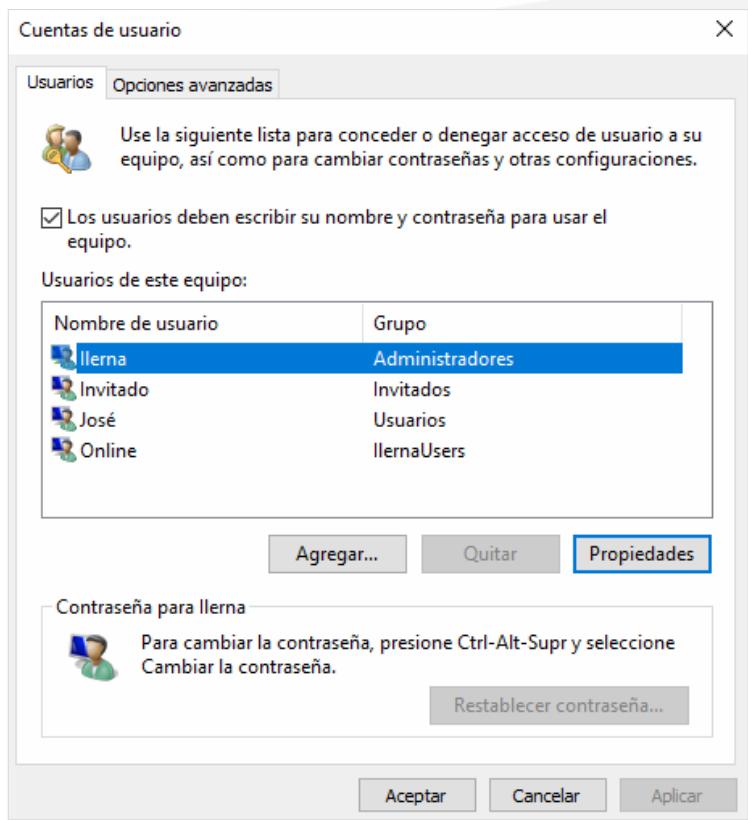
- a) El propietario de fichero
- b) El grupo de usuarios
- c) Todos los usuarios
- d) Ninguna de las respuestas es correcta

2.2. SEGURIDAD DE CUENTAS DE USUARIO

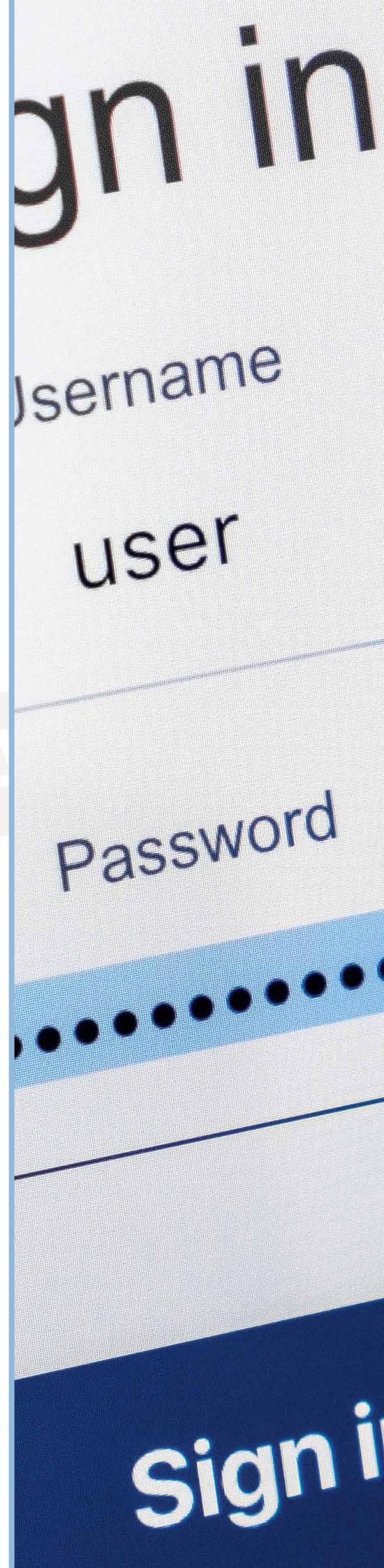
Si estamos habituados a trabajar en un equipo al que únicamente nosotros tenemos acceso, es usual que lo hagamos como administradores. Es decir, teniendo todos los privilegios. Sin embargo, es muy importante que iniciemos sesión solamente con dicha cuenta o con otras que nos brinden permisos avanzados si las operaciones que vamos a desarrollar lo requieren.

Además, para maximizar la seguridad, siempre que nos sea posible, debemos tener en cuenta las siguientes pautas:

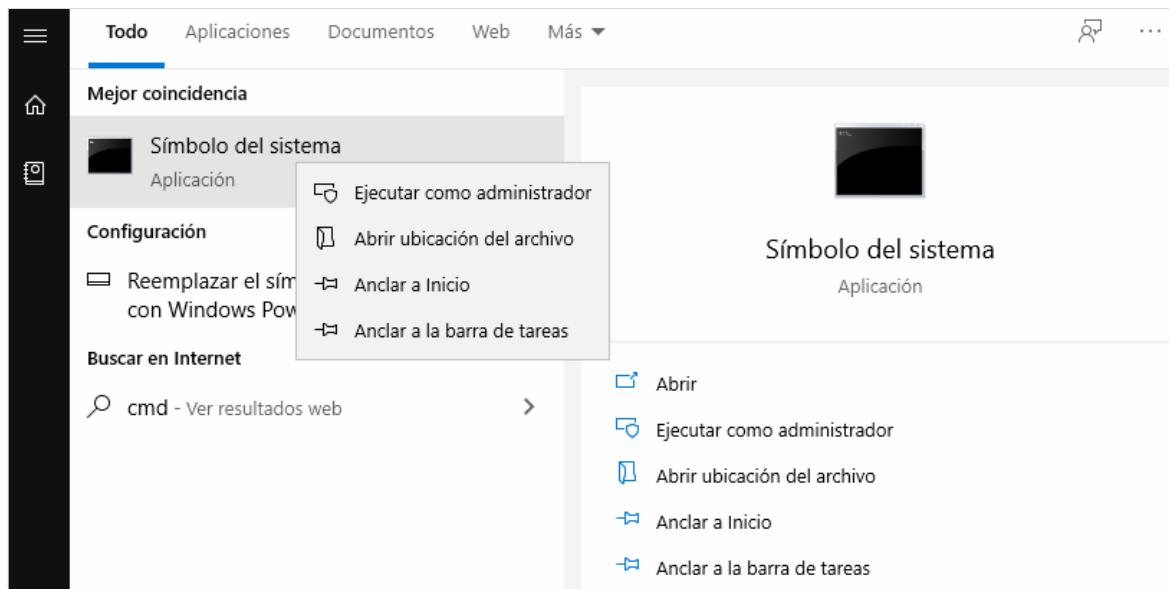
- **Cuenta de administrador:** cambiar el nombre de la cuenta de administrador y asignarle una contraseña segura.
- **Cuentas de invitado:** es preferible mantenerlas deshabilitadas, ya que es bastante frecuente que no necesiten la introducción de ninguna contraseña y pueden comprometer la seguridad.
- **Cuentas de usuario:** se le deben asignar únicamente los permisos que sean estrictamente necesarios.



En el caso de Windows, por ejemplo, podemos utilizar una cuenta de usuario sin privilegios para iniciar sesión sin comprometer la seguridad.



Después, si fuera necesario, podemos emplear el comando **Ejecutar** como administrador accesible desde el menú contextual, y se nos solicitará la contraseña.



El uso de la cuenta de administrador se debe limitar a aquellas situaciones en las que necesitamos disponer de privilegios: realizar cambios en la configuración, instalar una nueva aplicación, dar de alta un nuevo usuario, etc. Al finalizar estas tareas, debemos seguir trabajando con una cuenta estándar.

PARA + INFO

- Cualquier acción que hagamos con la cuenta de administrador afecta a todo el ordenador y, por tanto, al resto de cuentas de usuario.
- Si cometemos un error o un descuido como administradores, afectará a todos los usuarios.



Por otra parte, si un virus infecta el ordenador cuando estamos utilizando una cuenta de administrador, podrá tener control total sobre el equipo, resultando así más difícil de eliminar. Sin embargo, si la infección se produce utilizando una cuenta de usuario estándar, la limitación en los permisos reducirá mucho sus efectos nocivos.

Por último, cabe señalar que es de vital importancia tener en cuenta la seguridad en la administración de usuarios, ya que es muy fácil que una persona no autorizada pueda terminar usando nuestra máquina.

2.3. SEGURIDAD DE CONTRASEÑAS

Características de las contraseñas seguras
youtu.be/mTNcFVeL4bU



En el caso de las cuentas de usuario de administrador, la seguridad en las contraseñas es muy importante, ya que los administradores tienen poderes sobre otras cuentas y sobre la configuración del equipo. Para el resto de las cuentas también es necesario establecer una contraseña de acceso para proteger su espacio privado.

Las contraseñas son un elemento clave para proteger las cuentas de usuario y la información que se almacena en los equipos y en la red. Por lo que, es muy importante velar por la confidencialidad de las mismas. Cuanto más segura sea una contraseña, mayor protección nos ofrecerá.

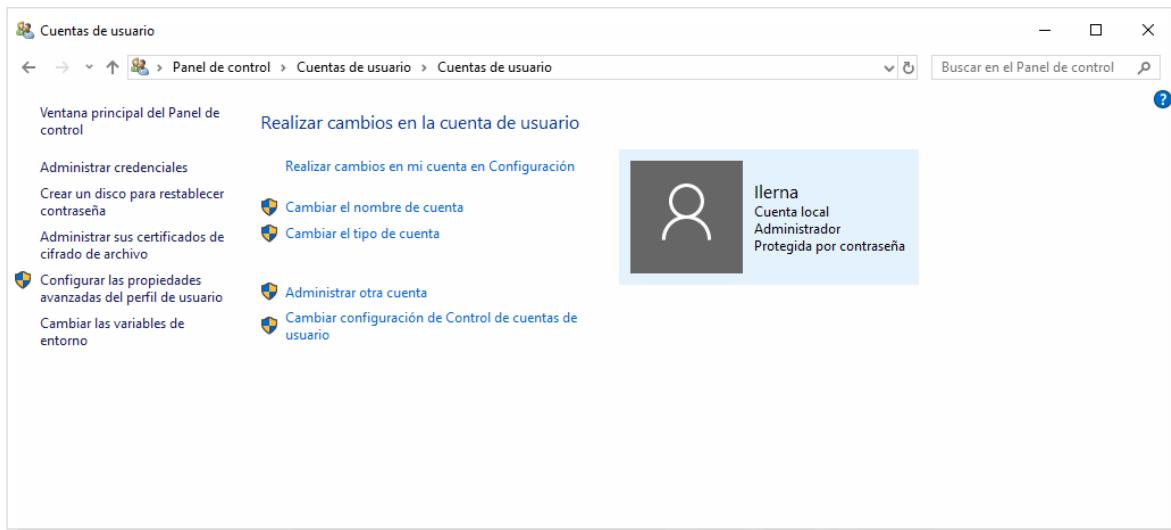
Los sistemas operativos suelen ofrecer al administrador la posibilidad de establecer cuáles serán las características de las contraseñas para que estas sean más fiables, por ejemplo:

- **Número de caracteres:** toda contraseña debe tener un mínimo de ocho caracteres. Cuantos más caracteres, mayor seguridad.
- **Tipo de caracteres:** las contraseñas deben contener diferentes tipos de símbolos: mayúsculas, minúsculas, números y caracteres no alfanuméricos, como, por ejemplo, el símbolo del dólar, la parrilla, etc.
- **Elección de términos:** la palabra que ejerce de contraseña debe evitar corresponderse con datos demasiado obvios, como nombres de familiares, de la empresa, etc.

Lo ideal es que tampoco se corresponda con términos que se encuentran en los diccionarios para evitar, en la medida de lo posible, que la cuenta sea *hackeada* mediante técnicas de fuerza bruta (introducción automatizada y masiva de términos del diccionario hasta dar con el correcto).

- **Renovación periódica de la contraseña:** para maximizar la seguridad, las contraseñas deberán cambiarse con regularidad. Las nuevas deben ser significativamente distintas a las anteriores.

En Windows 10 podemos habilitar y modificar contraseñas entrando en el panel de control. Una vez allí, hacemos clic en *Cuentas de usuario y protección infantil* y luego en *Cuentas de usuario*. De esta forma, nos va a permitir crear una contraseña para la cuenta.



CONCEPTO

Debemos saber que la cuenta de usuario invitado tiene los mismos privilegios que un usuario estándar, pero es anónima y sin contraseña. Por defecto, viene deshabilitada y, desde el punto de vista de la seguridad, es conveniente que se mantenga así.

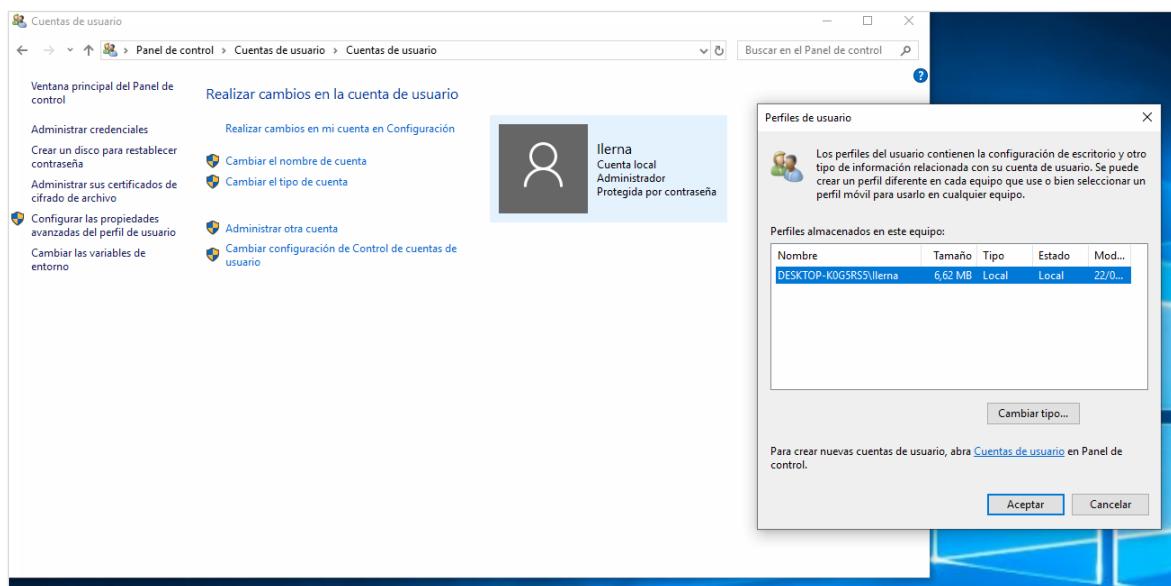
Administración de perfiles locales de usuario

En los sistemas operativos multiusuario podemos definir diferentes perfiles. Cada perfil estará integrado por una serie de archivos que contienen información relativa a la configuración de ese usuario específico.

Entre la información más destacada que suele almacenarse en los perfiles encontramos los siguientes datos:

- Configuración del escritorio del usuario.
- Configuración de las aplicaciones a las que tendrá acceso el usuario.
- Accesos a carpetas, impresoras en red, etc.

Lo más habitual es que el perfil de los usuarios se cree automáticamente al darlos de alta o cuando inician sesión en el equipo por primera vez. No obstante, las características del perfil pueden y deben variar en función de las necesidades de la persona que lo utilizará. El administrador será el encargado de crear los perfiles idóneos y de asignarlos a las cuentas.



La creación de perfiles de usuario en Windows 10 se realiza a través del "Panel de control".

ponte a prueba

En las cuentas de usuario de administrador, la seguridad en las contraseñas es muy importante. ¿Qué características deberíamos aplicar en las contraseñas para ofrecer una mayor seguridad?

- a) Utilizar términos conocidos para evitar olvidar la contraseña, 4 caracteres como máximo y mantener siempre la misma contraseña.
- b) Usar 8 caracteres como mínimo, no usar términos obvios, renovar la contraseña periódicamente y usar diferentes símbolos.
- c) Permitir modificar la contraseña solo al usuario Administrador y que esta no sufra cambios.
- d) Solo utilizar caracteres numéricos y 8 caracteres como máximo.

2.4. CONFIGURACIÓN DEL PROTOCOLO TCP/IP. DIRECCIONES IP Y MÁSCARAS DE SUBRED

Para configurar debidamente el servidor de redes es fundamental tener unas nociones elementales de cómo funciona el protocolo TCP/IP.

La **dirección IP** constituye el concepto más fundamental en el campo que nos ocupa. Gracias a ella podemos identificar cada equipo. Toda dirección IP consta siempre de cuatro números enteros de 4 bytes separados por puntos que pueden oscilar entre 0 y 255.

Así pues, su formato será W.X.Y.Z (por ejemplo: 192.168.1.6), donde W, X, Y y Z nunca podrán ser mayores de 255. Dentro de una misma red no pueden, en ningún caso, existir dos direcciones IP iguales. De este modo, cada dirección deberá constituir un número irrepetible y único. En total, cada dirección IP consta de 32 bits (o lo que es lo mismo, 4 bytes).

A partir de estos datos, es importante tener en cuenta lo siguiente:

- **Dirección de red.** los primeros bits de la dirección IP constituyen la dirección de red. Así pues, todos los equipos que pertenecen a una misma red contienen en su dirección IP la misma dirección de red.

Esto comporta que, al pertenecer a una misma red, dichos equipos pueden comunicarse entre sí de forma directa, sin intermediación alguna. Los datos se transmitirán por el cable Ethernet o por el medio elegido.

- **Dirección del equipo:** los últimos bits de la dirección IP constituyen la dirección del equipo en la red, y deben ser distintos para cada equipo.

EJEMPLO

Por ejemplo, en una determinada red, los tres primeros bytes de una dirección pueden constituir la red y el último byte, la dirección del equipo. Así, todos los equipos poseerán direcciones IP del tipo 192.168.0.X, donde X será un número comprendido entre 0 y 255. Será el que identificará al equipo en la red.

¿Cómo determinamos qué parte corresponde a la red y cuál al equipo? Esto se realiza mediante la **máscara de red o máscara de subred**. Estos parámetros establecen la longitud de ambas mitades.

La máscara de red o de subred es, en definitiva, una dirección IP que tiene asignado un valor de 255 para todos los bytes de la parte correspondiente a la dirección de red, y un 0 a todos los bytes correspondientes a la dirección del equipo.

Así pues, en nuestro ejemplo, donde las direcciones de los equipos son del tipo 192.168.0.X, la máscara de subred será la siguiente: 255.255.255.0.

```

C:\Windows\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\USERS\LIDIA>ipconfig
Configuración IP de Windows

Adaptador de LAN inalámbrica Wireless Network Connection 3:
  Sufijo DNS específico para la conexión.: home
  Vínculo: dirección IPv6 local . . . : fe80::55ca:4da0:cef5:24c6%16
  Dirección IPv4. . . . . : 192.168.1.13
  Máscara de subred . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 192.168.1.1

Adaptador de Ethernet Local Area Connection:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión.: .
  Adaptador de Ethernet VirtualBox Host-Only Network:
    Sufijo DNS específico para la conexión.: .
    Vínculo: dirección IPv6 local . . . : fe80::9d8a:b07c:c4ad:2726%19
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : .

Adaptador de túnel isatap.(D00F6807-D483-4934-BFE8-408EB25D8E6A):
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión.: .
  Adaptador de túnel isatap.home:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión.: home
  Adaptador de túnel Teredo Tunneling Pseudo-Interface:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión.: .
  Adaptador de túnel isatap.(0EC06B49-FCA5-436F-8A4D-FEA628FA57A):

```

El comando Ipconfig nos brinda información acerca de nuestra IP y nuestra máscara de subred.

Una parte de la dirección IP puede utilizarse para identificar la red en sí, y la otra como identificador del ordenador dentro de ella. Una posible división de los distintos tipos de direcciones IP daría lugar a tres clases de redes:

- **Direcciones IP de clase A:** en ellas únicamente el primer entero de 4 bytes identifica la red. Los tres restantes se refieren a los equipos dentro de ella. Así, si en una dirección W.X.Y.Z de clase A, solamente W identifica la red, X.Y.Z hacen referencia a los ordenadores.
- **Direcciones IP de clase B:** en este caso, las dos primeras cifras identifican la red. Las restantes se refieren a los equipos que hay dentro de ella. En consecuencia, en una dirección W.X.Y.Z de clase B, el segmento W.X identifica la red; Y.Z, los ordenadores.
- **Direcciones IP de clase C:** los tres primeros enteros identifican la red, mientras que el último se refiere a los equipos dentro de ella. Así, en una dirección W.X.Y.Z de clase C, W.X.Y identifican la red. Únicamente Z se refiere a los ordenadores.

IP Address

CONCEPTO

Dividir la red en subredes facilita la identificación de los equipos que se encuentran conectados a la misma, especialmente cuando los equipos son muy numerosos. A este proceso de división se lo denomina *subnetting*. Para efectuarlo, se usa una máscara de subred.

La división en subredes plantea que, si una red de una clase determinada desperdicia muchas direcciones IP, esta puede ser dividida en subredes más pequeñas que aprovechen mejor el espacio de direccionamiento.

Partiendo, por ejemplo, de una red dada, para obtener dos subredes será necesario coger un único bit de los reservados para direccionar hosts, ya que con él pueden representarse dos números.

Si fueran tres subredes ya se necesitaría un bit más, que daría como resultado la posibilidad de obtener cuatro subredes. Al utilizar bits de hosts para crear subredes, cuantas más subredes se necesiten, menos hosts podrá albergar cada una.

	0	1	8	16	24	31
clase A	0	red		número de host		
clase B	1	0	número de red		número de host	
clase C	1	1	0	número de red		número de host
clase D	1	1	1	0	dirección multicast	
clase E	1	1	1	1	reservado	

- Cantidad de redes por cada clase:

Clase A → 7 bits para direccionar redes → 2^7 redes

Clase B → 14 bits para direccionar redes → 2^{14} redes

Clase C → 21 bits para direccionar redes → 2^{21} redes

CONCEPTO

$2^n - 2$ donde "n" es el número de bits reservados para hosts.

Se restan 2 porque el primero se reserva para identificar la red y el último para la IP de broadcast.

- Cantidad de hosts por cada red de cada clase:

Clase A → 24 bits para direccionar hosts → $2^{24} - 2$ hosts

Clase B → 16 bits para direccionar hosts → $2^{16} - 2$ hosts

Clase C → 8 bits para direccionar hosts → $2^8 - 2$ hosts

Llegado esto punto, retengamos los siguientes conceptos asociados a la IP:

- **Dirección IP privada:** es la dirección que posee cada equipo o dispositivo que se conecta a nuestra red a través del protocolo TCP/IP. Podemos asignarla nosotros o hacer que se asigne de manera automática a través del DHCP.
- **Dirección IP pública:** es la dirección que usamos para identificarnos en la red cuando nos conectamos a otras redes externas, como internet. Nos la asigna nuestro proveedor de internet, por lo que en principio no podemos configurarla.

Las IP públicas que nos asignan los ISP pueden ser:

- **Estáticas:** la IP es fija, es decir, siempre es la misma. Los ISP suelen cobrarnos por este servicio, que por otra parte nos permite un mayor control y nos brinda la posibilidad de asignar la IP a un nombre de dominio del tipo www.dominio.com. De este modo es posible publicar sitios web que siempre estén accesibles.
- **Dinámicas:** es la más habitual. El ISP nos asigna una dirección que queda libre cada vez que nos conectamos a la red. La dirección se modifica cada vez que nos desconectamos y reconectamos.

Por último, debemos señalar que la versión 4 del protocolo IP, que da lugar a direcciones con el formato que hemos visto, permite algo más de 4.000 millones de direcciones distintas.

No obstante, los sistemas operativos recientes incorporan ya IPv6, una nueva versión que admite muchas más direcciones.



ponte a prueba

¿Qué clase de red tiene como máscara el valor 255.255.0.0?

- Clase A
- Clase B
- Clase C
- Clase D

En las direcciones de clase A, ¿cuántos bloques de enteros de 4 bytes dedicaremos a identificar los equipos?

- 4
- 2
- 1
- 3



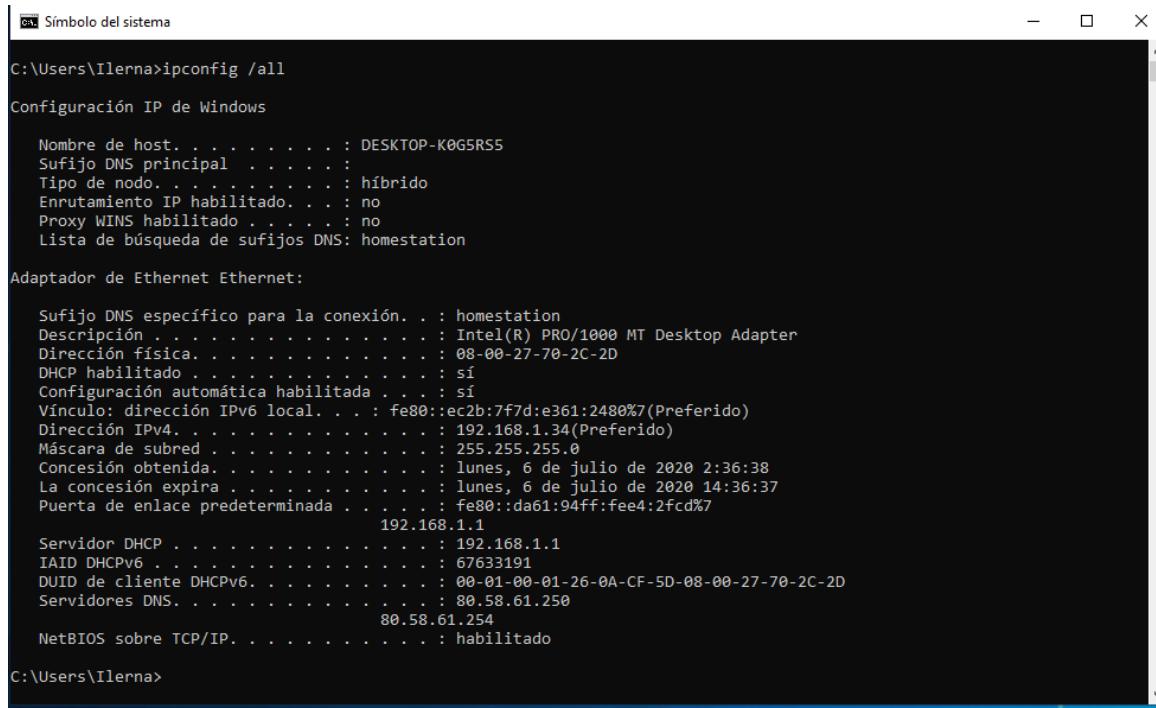
2.5. SERVICIO DE NOMBRES DE DOMINIOS (DNS)

Los servidores DNS (Sistema de Nombres de Dominios) juegan un papel muy importante en el rendimiento de la navegación en internet. Escogerlos y configurar nuestra conexión de red de forma adecuada incrementará significativamente la calidad de nuestra navegación. Estos tienen la misión de evitar recordar la IP del equipo al que nos queremos conectar.

Cuando navegamos por la red, accedemos a cualquier página web desde un navegador y escribimos su dirección `www.pagina.dominio`. Es el servidor DNS el que relaciona el nombre escrito con la IP que tiene alojada la página que queremos visualizar.

Para comprobar el estado de los servidores DNS en un equipo se puede realizar de varias formas (interfaz gráfica o de texto), aunque habitualmente se hace la comprobación por consola de comandos del sistema operativo. Ya que de este modo podemos comprobar la conectividad del equipo junto a su información de una forma muy sencilla y rápida.

Para realizar estas comprobaciones mediante consola de comandos utilizaremos la instrucción “`ipconfig`” en el caso de sistemas operativos Windows y “`ifconfig`” en sistemas operativos Linux y en ambos casos combinada con la sentencia “`/all`” para mostrar toda la información.



```
C:\Users\Ilerna>ipconfig /all

Configuración IP de Windows

Nombre de host . . . . . : DESKTOP-K0G5RS5
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado. . . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: homestation

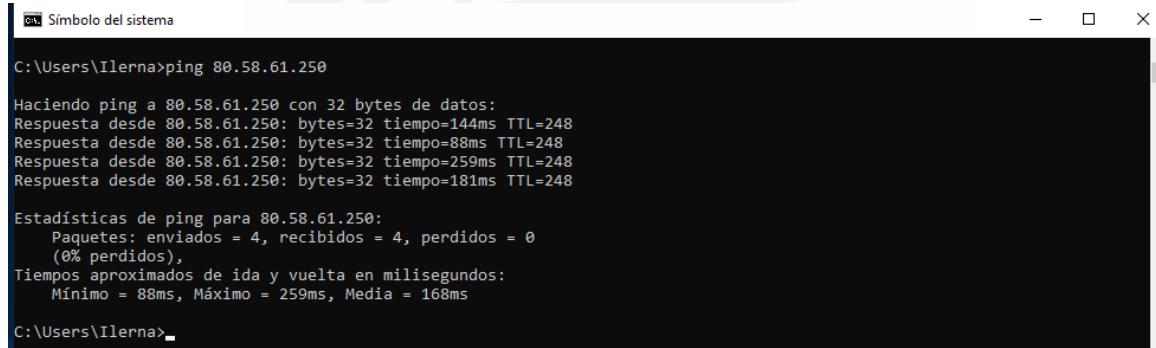
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : homestation
Descripción . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . . . . . . : 08-00-27-70-2C-2D
DHCP habilitado . . . . . . . . . : sí
Configuración automática habilitada . . . . : sí
Vínculo: dirección IPv6 local. . . . : fe80::ec2b:7f7d:361:2480%7(Preferido)
Dirección IPv4. . . . . . . . . . : 192.168.1.34(Preferido)
Máscara de subred . . . . . . . . . : 255.255.255.0
Concesión obtenida. . . . . . . . . : lunes, 6 de julio de 2020 2:36:38
La concesión expira . . . . . . . . : lunes, 6 de julio de 2020 14:36:37
Puerta de enlace predeterminada . . . . . : fe80::da61:9aff:fee4:2fc%7
192.168.1.1
Servidor DHCP . . . . . . . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . . . . . . . : 67633191
DUID de cliente DHCPv6. . . . . . . : 00-01-00-01-26-0A-CF-5D-08-00-27-70-2C-2D
Servidores DNS. . . . . . . . . . . . . . . . . . . . : 80.58.61.250
80.58.61.254
NetBIOS sobre TCP/IP. . . . . . . . . . . . . . . . . . . . . . . . . . . . . : habilitado

C:\Users\Ilerna>
```

Una vez vemos las direcciones que identificarán nuestro equipo dentro de la red, simplemente podemos comprobar el funcionamiento del servicio DNS con la instrucción "ping", tanto para saber si el servidor está funcionando de forma correcta, como para mostrar su funcionamiento.

Para comprobar que el servidor DNS funciona correctamente, podemos hacer ping a la IP de nuestro servidor.



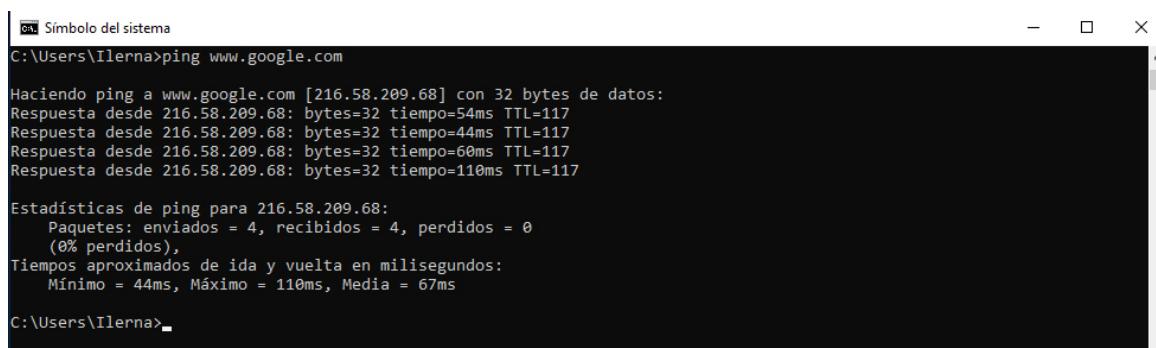
```
C:\Users\Ilerna>ping 80.58.61.250

Haciendo ping a 80.58.61.250 con 32 bytes de datos:
Respuesta desde 80.58.61.250: bytes=32 tiempo=144ms TTL=248
Respuesta desde 80.58.61.250: bytes=32 tiempo=88ms TTL=248
Respuesta desde 80.58.61.250: bytes=32 tiempo=259ms TTL=248
Respuesta desde 80.58.61.250: bytes=32 tiempo=181ms TTL=248

Estadísticas de ping para 80.58.61.250:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 88ms, Máximo = 259ms, Media = 168ms

C:\Users\Ilerna>
```

Para comprobar el funcionamiento del servidor DNS web, podemos hacer ping a una URL y ver cómo este la resuelve de forma correcta mostrándonos su IP.



```
C:\Users\Ilerna>ping www.google.com

Haciendo ping a www.google.com [216.58.209.68] con 32 bytes de datos:
Respuesta desde 216.58.209.68: bytes=32 tiempo=54ms TTL=117
Respuesta desde 216.58.209.68: bytes=32 tiempo=44ms TTL=117
Respuesta desde 216.58.209.68: bytes=32 tiempo=60ms TTL=117
Respuesta desde 216.58.209.68: bytes=32 tiempo=110ms TTL=117

Estadísticas de ping para 216.58.209.68:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 44ms, Máximo = 110ms, Media = 67ms

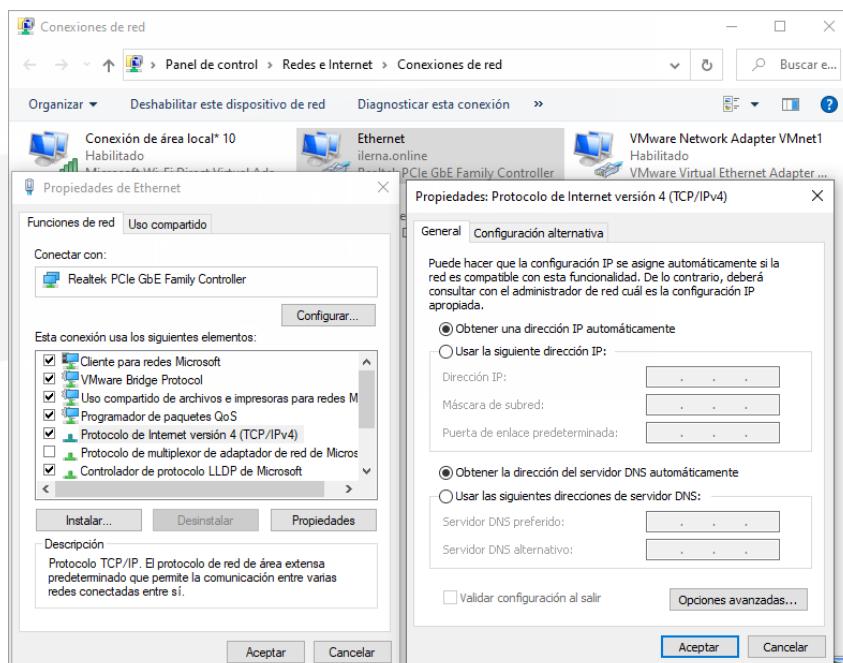
C:\Users\Ilerna>
```

No solo basta con escoger los servidores más rápidos, sino que además es necesario configurar nuestro sistema operativo correctamente. Aprenderemos más adelante cómo hacerlo.

2.6. ARCHIVOS DE CONFIGURACIÓN DE RED

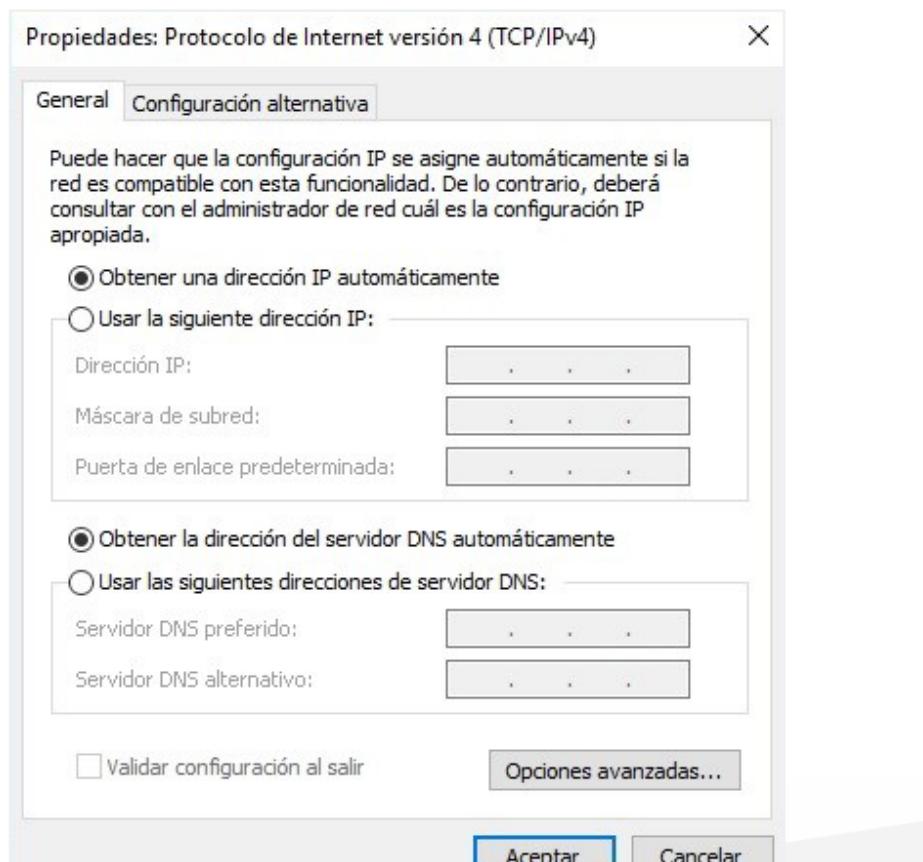
Toda comunicación en red sigue el modelo TCP/IP. Como protocolo, rige las normas al realizar este proceso de comunicación. La configuración de nuestro equipo forma parte de la red y sigue una serie de pasos que a continuación vamos a detallar.

A través del Panel de control vamos a configurar la dirección IP, la máscara de subred, el DNS y los demás elementos de la configuración de red en un equipo que ejecute Windows 10.



- 1. Panel de control / redes e internet.**
- 2. Centro de redes y recursos compartidos.** En el apartado *Ver redes activas*, observaremos la conexión por la que nos podemos enlazar a la red y hacemos clic en ella.
- 3. Propiedades del adaptador.** Una vez realizado este paso tendremos que elegir la sección *Protocolo de internet (TCP/IP v4)*.

Aunque actualmente podemos operar con las dos versiones de direcciones IP (v4/ v6), para la realización de este manual escogeremos la forma más sencilla. Una vez elegida la opción, seleccionamos propiedades.



Área de configuración de la dirección IP, la máscara de subred y el DNS en Windows.

Una vez configurada la dirección IP, la máscara de subred correspondiente y servidores DNS, le podemos dar a **Aceptar**. La información se almacena en los archivos de configuración del sistema. En este aspecto Windows es bastante opaco, puesto que el registro y otras áreas centralizan la configuración.

No obstante, en el caso de Linux la configuración de red se almacena en `/etc/network/interfaces`.



ponte a prueba

¿En qué directorio de Linux encontraremos la configuración de la red?

- etc/network/interfaces
- dev/network/config
- bin/network/interfaces
- etc/config/network



2.7. OPTIMIZACIÓN DE SISTEMAS PARA ORDENADORES PORTÁTILES. ARCHIVOS DE RED SIN CONEXIÓN

Los ordenadores portátiles poseen unas características propias que debemos tener en cuenta, tanto a la hora de instalar sus sistemas operativos, como en el momento de protegerlos contra posibles intrusiones.

Se pueden resumir bajo los siguientes puntos:

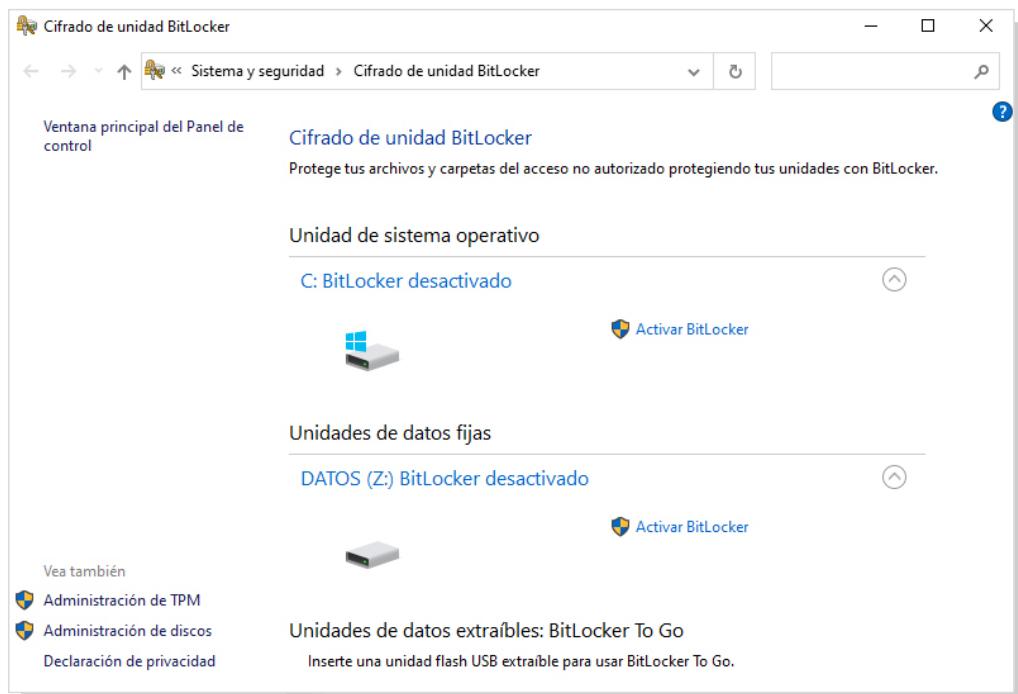
- **Mayor vulnerabilidad.** Puesto que salen con regularidad de los hogares y oficinas, la información que contienen resulta más vulnerable a intrusiones. Si tienen acceso inalámbrico a la red, la vulnerabilidad se duplica. Si llegaran caer en las manos inadecuadas, el intruso no solo tendrá acceso a los ficheros contenidos en el disco duro local, sino también a los que estén en red.
- **Menor rendimiento y otras características.** Pese a que los portátiles de última generación están equiparándose cada vez más a los ordenadores de sobremesa, en equipos portátiles antiguos o de gama baja el rendimiento será menor.

Lo mismo sucederá en aspectos como la capacidad del disco duro, la cantidad de memoria RAM que equipan, etc.

Así pues, a la hora de configurar la seguridad de un ordenador portátil es conveniente aplicar las siguientes premisas:

- **Habilitar contraseñas adicionales.** Además de la contraseña de inicio de sesión, podemos habilitar la de la BIOS e instalar software adicional para proteger archivos y carpetas.

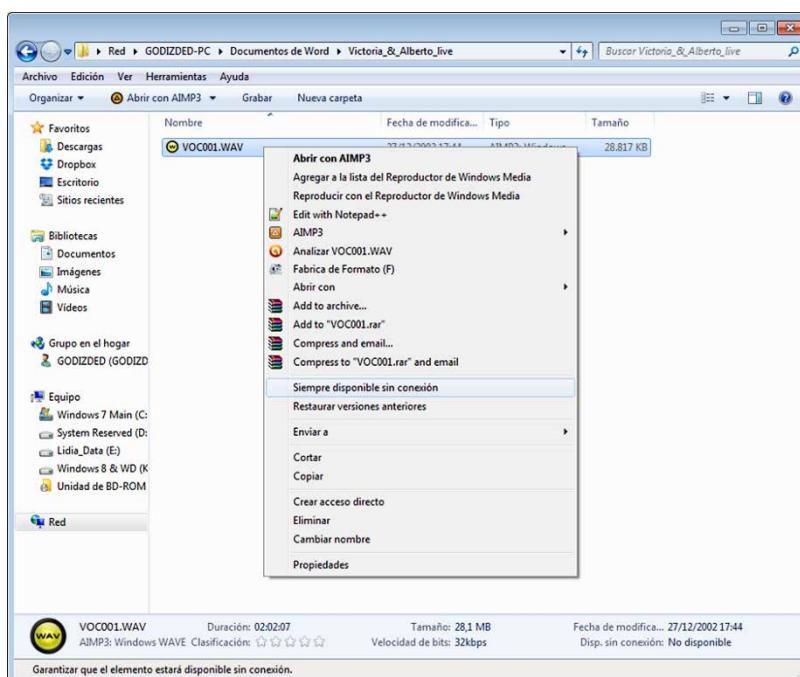
- **Sistemas de autenticación fuertes.** Los lectores de huellas dactilares o de tarjetas inteligentes se utilizan cada vez más para proteger equipos portátiles. Gracias a estos dispositivos, nadie tendrá acceso si no posee la tarjeta (similar a las de crédito) o si no puede autentificarse mediante huella dactilar.
- **Encriptación de unidades de disco.** Sistemas como el Cifrado de unidad BitLocker de Windows 10 permiten encriptar discos para que no sean accesibles sin contraseña.



El "Cifrado de unidad BitLocker" de Windows 10 permite encriptar discos para que no sean accesibles sin contraseña.

En lo referente al rendimiento, para portátiles lentos podemos optimizar el sistema llevando a cabo cambios en la configuración. Algunos de los gestos más efectivos serán los siguientes:

- Desactivar los sonidos del sistema. Por ejemplo, en Windows 10 podemos hacerlo a través de *Hardware y sonido*, en el Panel de control.
- Eliminar aplicaciones que no se usen. En Windows 10 esta acción puede realizarse a través del Panel de control, en *Agregar o quitar programas*.
- Desactivar efectos visuales. En Windows 10 esta acción puede realizarse a través de las *Propiedades de Equipo*.
- Desactivar los programas que se cargan en el inicio. Para ello, pulsaremos **Win+R** y teclearemos **MSConfig**.



Desactivar efectos visuales maximizará el rendimiento de Windows.

Por último, es importante que tengamos en cuenta que, si el equipo portátil abandona la oficina y deja de tener conexión a la red, los archivos que se encuentren accesibles a través de ella dejarán de estar disponibles.

Los sistemas operativos acostumbran a brindar herramientas para prevenir este problema. En Windows 10, por ejemplo, basta con pulsar sobre el archivo o sobre la carpeta con el botón secundario del ratón y, en el menú contextual, elegir el comando **Siempre disponible sin conexión**.

2.8. PRINCIPALES COMANDOS DE SISTEMAS OPERATIVOS LIBRES Y PROPIETARIOS

Los sistemas operativos más utilizados hoy en día cuentan con interfaz gráfica para su funcionamiento básico y, cada vez más, todos estos sistemas integran diferentes aplicaciones por defecto que nos ayudan a gestionar todos los recursos del sistema (como hemos visto en el caso de Windows).

Todas estas interfaces gráficas ayudan a los usuarios del sistema a realizar operaciones u obtener información de un modo más visual y atractivo para la vista. Aunque esto no ha hecho que el entorno más clásico de los sistemas desaparezca, ya que, en la actualidad, todos los sistemas operativos contemplan diferentes formas de acceder a su formato de texto, donde nos podremos manejar a base de

instrucciones en el sistema y podremos realizar todas las operaciones que nos permita el sistema operativo.

El moverse a través de instrucciones dentro del sistema operativo como método de utilización de este nos es lo más habitual, ya que, como hemos comentado, las interfaces gráficas son más intuitivas y cómodas para los usuarios (sobre todo los más inexpertos). De todos modos, en muchas de las operaciones de mantenimiento o detección de errores se siguen utilizando mucho, sobre todo para configuraciones de equipos en red, ya que los entornos de texto agilizan mucho las peticiones debido a que no consumen tantos recursos como los entornos gráficos.

Existen una serie de comandos que nos ofrecen la posibilidad de movernos y gestionar los sistemas operativos. Aunque aprenderse todos los comandos de un sistema es algo prácticamente imposible, sí que deberemos conocer los más utilizados:

Comando		Acción
cd		Moverse de directorio
dir	ls	Mostrar el contenido del directorio
rm	remove	Eliminar
mv	move	Mover
cp	copy	Copiar
mkdir		Crear directorio
fsutil	touch	Crear fichero
ipconfig	ifconfig	Información de las direcciones del equipo
/?	help	Ayuda

Para una mayor información sobre los comandos de cada sistema operativo, consultaremos las páginas oficiales de estos, donde nos proporcionan información sobre estos de una forma más detallada. Y es que, con comandos más complejos, la utilización de las opciones de que dispone o el formato que tiene que cumplir puede variar.



ponte a prueba

¿Qué información muestra el comando “dir” en Windows?

- a) Mostrar el contenido del directorio.
- b) Analiza el disco principal del sistema.
- c) Muestra una lista con las tareas programadas del sistema.
- d) Muestra una lista de los procesos activos en el sistema.

¿Qué acción realiza la palabra reservada “ls” en una sentencia de comandos en Linux?

- a) Mostrar el contenido del directorio.
- b) Nos ofrece un editor de texto para crear ficheros.
- c) Devuelve información detallada de la red.
- d) Eleva los privilegios a root para poder lanzar el comando.



3

ADMINISTRACIÓN DE LA INFORMACIÓN

Podemos administrar y organizar la información gracias a los sistemas de archivos. En este tema veremos cuáles son los más comunes y sus características principales.

Además, aprenderemos a administrar las particiones de los dispositivos de almacenamiento, a automatizar tareas y a utilizar comodines y herramientas de búsqueda.

Finalmente, nos vamos a centrar en las herramientas orientadas al mantenimiento de las particiones, ya que nos van a permitir desfragmentarlas para maximizar su velocidad y corregir los posibles errores.

3.1. SISTEMA DE ARCHIVOS

El **sistema de archivos** es el área del sistema operativo que se ocupa de gestionar la utilización de los medios que empleamos para almacenar la información en las diferentes particiones del disco. Los datos que guardamos en ellas se representan en modo textual o gráfico. Utilizando un gestor de archivos podemos administrar estos medios con gran facilidad.

Un sistema de archivos se puede dividir en dos tipos de objetos fundamentales:

- **Archivos**

Los archivos o ficheros son un conjunto de datos ordenados en los que se almacena la información. Tenemos tanto los que emplea el propio sistema operativo para trabajar internamente como los que generamos nosotros mediante todo tipo aplicaciones.

- **Directorios**

Los directorios o carpetas nos ofrecen la posibilidad de clasificar los datos, es decir, los archivos, y poner orden en el sistema. Un directorio se puede definir como un contenedor que puede contener archivos y a su vez otros directorios dentro de él.

Así pues, la estructura resultante es jerárquica y ramificada. Lo que obtenemos a partir de ella se denomina estructura en árbol.

3.1.1. Los ARCHIVOS

Son un mecanismo de almacenar información en el disco y posteriormente volver a leerla sin que el usuario deba preocuparse por cómo y dónde se ha almacenado la información.



Es posible dividir los archivos en dos grandes grupos, por un lado, tenemos los archivos ejecutables y los no ejecutables o archivos de datos. La diferencia entre ambos es que los ejecutables pueden funcionar por ellos mismos y los archivos de datos necesitan un programa para ser utilizados.

Existe una gran variedad de extensiones de archivos y así pertenecer a diferentes categorías, como pueden ser: archivos de sistema, de vídeo, de audio, imágenes, archivos comprimidos, etc.

3.1.2. Los DIRECTORIOS

Son considerados una división lógica en el almacenamiento de archivos u otros subdirectorios. Estos directorios forman una estructura jerárquica, en la que un usuario que se encuentre en un directorio en concreto pueda buscar o crear archivos en esa ruta especificada.

Como en todo árbol, existe un directorio raíz (root) que engloba el resto de los directorios y archivos.

3.2. TIPOS DE SISTEMAS DE ARCHIVOS

Existe un sinfín de sistemas de archivos distintos, como por ejemplo exFAT, HFS Plus, UFS, XFS. No obstante, los que usaremos más habitualmente son los siguientes:

- **fat32** (Tabla de Asignación de Archivos)

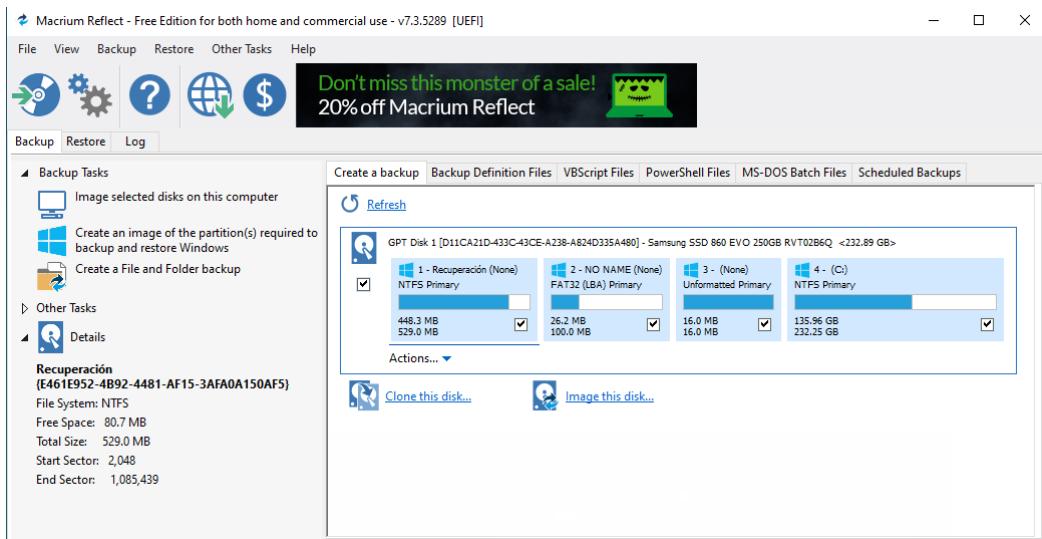
Sistema de archivos heredado de MS-DOS que podemos encontrar en las primeras versiones de Windows. Debido a esto, se considera un sistema universal y, pese a su antigüedad, aún se utiliza con cierta frecuencia.

- **NTFS (New Technology File System)**

Sistema de archivos diseñado para versiones más recientes de Windows. Gracias a él se consigue una mayor eficiencia y seguridad.

- **ext2, ext3 y ext4**

Diferentes versiones del sistema de archivos que encontramos principalmente en Linux.



Particiones NTFS vistas a través de la aplicación MacriumReflect.

La elección del tipo de sistema de archivos suele realizarse tras particionar el disco, en el momento de formatearlo. Pero, como veremos más adelante, podemos crear, eliminar y modificar las particiones usando herramientas del propio sistema operativo. Recordemos que un mismo disco físico puede tener varias particiones, y que el sistema operativo tratará cada una de ellas como un disco independiente.

3.3. GESTIÓN DE SISTEMAS DE ARCHIVOS MEDIANTE COMANDOS Y ENTORNOS GRÁFICOS

En cualquier sistema operativo, el gestor de archivos viene predefinido entre las aplicaciones básicas, ya que son los programas encargados de localizar archivos, ya sean propios o del sistema operativo.

En Windows, es posible acceder a la administración de archivos desde consola o símbolo del sistema, o bien desde un entorno gráfico conocido como *Explorer*. Por otro lado, en Linux, también está la posibilidad de acceder a través de comandos introducidos por consola o a través de programas gráficos como: Nemo, Nautilus, Dolphin, etc.



ponte a prueba

¿Qué sistema de archivos utiliza Windows 10?

- Fat32
- NTFS
- Ext3
- Ext2

Los directorios o también conocidos como ficheros son conjuntos de datos ordenados en los que almacenamos información.

- Verdadero
- Falso

```

Símbolo del sistema

Directorio de C:\Users\smalo\Documents

17/07/2020 08:23 <DIR> .
17/07/2020 08:23 <DIR> ..
15/03/2020 19:35 <DIR> Adobe
12/03/2020 14:54 29 Clave.txt
09/01/2020 17:13 352.256 Database1.accdb
08/05/2020 22:52 348.160 Database2.accdb
21/12/2019 10:32 <DIR> Downloads
12/03/2020 14:32 <DIR> es_windows_server_2016
14/11/2018 18:21 5.775.215.084 es_windows_server_2016.zip
28/04/2020 13:10 86.241 FCT_DAW_.docx
04/02/2020 12:45 <DIR> fscPortable
01/06/2020 12:53 <DIR> Grabaciones de sonido
25/06/2020 15:22 <DIR> NetBeansProjects
12/12/2019 00:59 <DIR> Plantillas personalizadas de Office
18/05/2020 11:26 5.239.577 Presentacion.pptx
01/06/2020 12:57 <DIR> Virtual Machines
11/06/2020 16:19 <DIR> Visual Studio 2017
17/01/2020 18:02 <DIR> VPPProjects

```

Uso del comando DIR en consola Windows.

A continuación, vamos a repasar algunas de las instrucciones más esenciales:

Instrucción	Definición	Ejemplo
DIR	Lista ficheros y directorios de la carpeta en la que se encuentre.	DIR unidad:\directorio\
CD	Para desplazarnos por las carpetas.	CD unidad:\directorio
MD	Crea el directorio especificado.	MD Juegos
RD	Elimina el directorio especificado.	RD Juegos
COPY	Copia ficheros.	COPY ..\ruta_archivo ..\ruta_destino
DEL	Borra ficheros.	DEL nombre_archivo
REN	Renombra ficheros.	REN nombre_original.txt nuevo_nombre.txt
MOVE	Mueve ficheros.	MOVE ..\ ruta_archivo ..\ ruta_destino

Existen muchas otras instrucciones. Para obtener ayuda sobre los parámetros que admiten ellas podemos escribir **?/?** tras ellas. Por ejemplo, **COPY/?** nos muestra ayuda sobre el comando que empleamos para copiar.

```
C:\Users\smalo\Documents>copy /?
Copia uno o más archivos en otra ubicación.

COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B] origen [/A | /B]
      [+ origen [/A | /B] [+ ...]] [destino [/A | /B]]

origen      Especifica el archivo o archivos que deben copiarse.
/A          Indica un archivo de texto ASCII.
/B          Indica un archivo binario.
/D          Permite que el archivo de destino se cree sin cifrar.
destino    Especifica el directorio y/o el nombre de archivo de los
           nuevos archivos.
/V          Comprueba si los nuevos archivos están escritos
           correctamente.
/N          Si está disponible, usa un nombre de archivo corto al copiar
           un archivo cuyo nombre no tiene el formato 8.3.
/Y          Suprime la solicitud de confirmación antes de
           sobrescribir un archivo de destino existente.
/-Y         Solicita confirmación antes de sobrescribir un archivo de
           destino existente.

Presione una tecla para continuar . . .
```

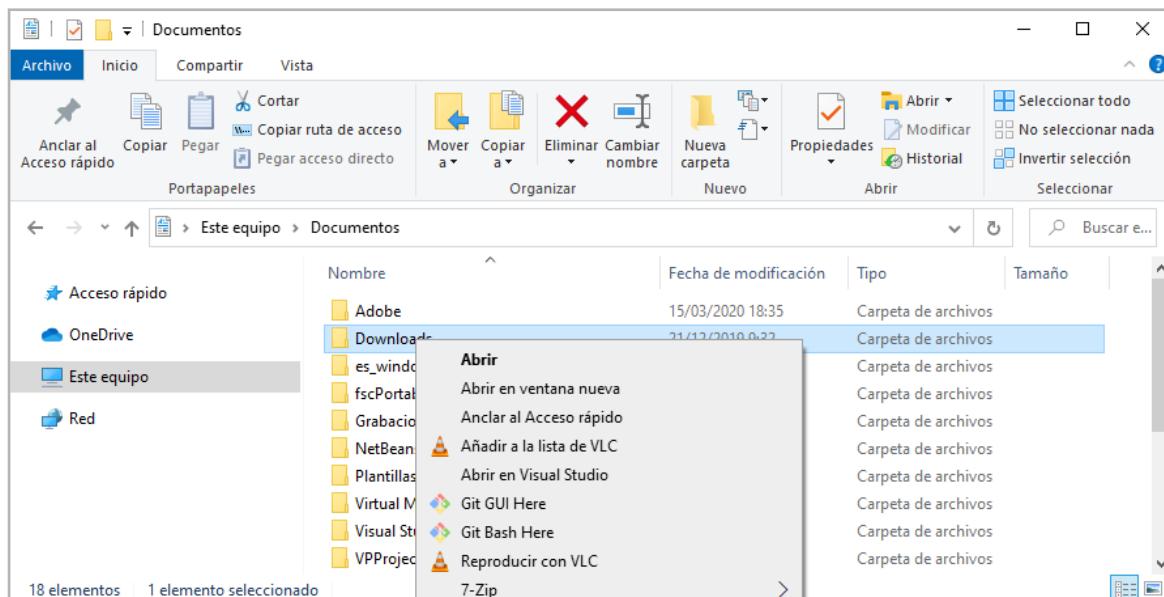
Ayuda comando copy desde consola Windows.

No obstante, los sistemas operativos actuales incorporan herramientas específicas que muestran los datos en un entorno gráfico para que el tratamiento de la información sea más intuitivo.

En Windows también se nos brindan múltiples opciones en este ámbito, como **FreeCommander** (<http://www.freecommander.com/>) o **UnrealCommander** (<http://x-diesel.com/>).

No obstante, los gestores gráficos que ofrecen los sistemas operativos actuales son funcionales y perfectamente aptos para gestionar el sistema.

En el caso de Windows encontramos el “Explorador”, donde tendremos diferentes directorios creados por defecto por el sistema, como las carpetas ya clásicas en este tipo de sistemas de Documentos, Imágenes o Descargas.



Explorador de archivos de Windows.



ponte a prueba

¿Cuál de las siguientes opciones es utilizada como comando para desplazarnos por los directorios del sistema?

- a) dir
- b) cd
- c) ls -s
- d) md

En cambio, en sistemas Linux podemos encontrar diferente variedad de opciones dependiendo de la versión de sistema operativo que utilicemos, aunque la más conocida es Nautilus.

Por último, apuntar que, aunque la versión gráfica es más intuitiva y más amable con el usuario no experimentado, para realizar determinadas tareas resulta más eficiente y rápido teclear comandos en el **Símbolo del sistema**.

3.4. GESTIÓN DE ENLACES

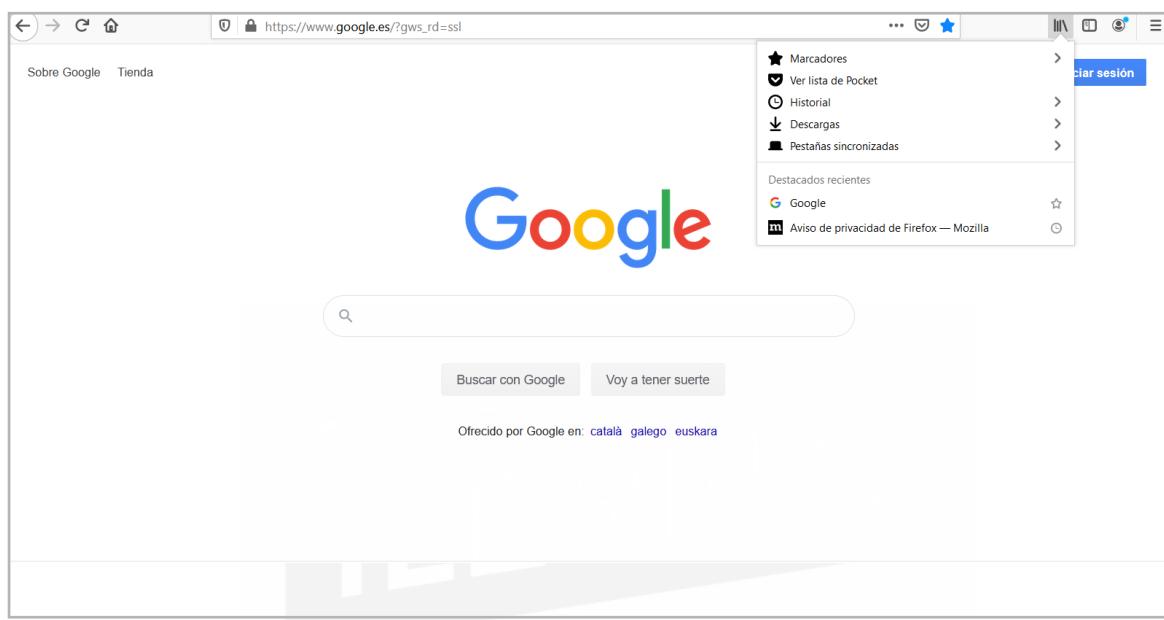
Los navegadores web nos brindan una opción extremadamente interesante: la posibilidad de guardar el enlace a una página que nos interesa de tal modo que, en adelante, podamos acceder a ella con un solo clic.

Todos los navegadores ofrecen unas características muy similares ante la gestión de los enlaces, aunque hay diferentes matices según el navegador que estemos utilizando.

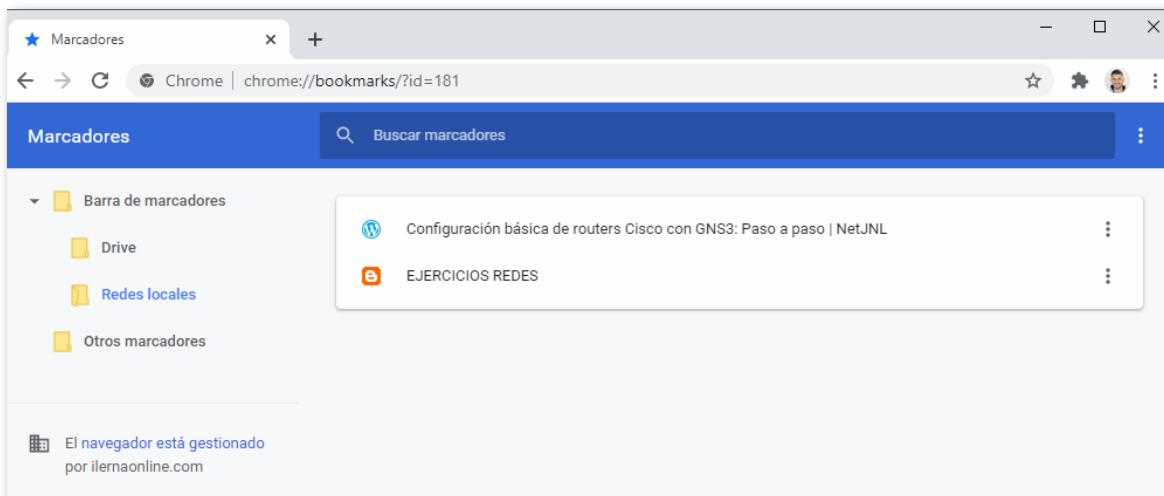
En **Google Chrome**, por ejemplo, podemos guardar enlaces pulsando sobre la estrella que se halla en el extremo derecho de la barra de direcciones. Los enlaces quedarán accesibles a través de la barra inmediatamente inferior.

Esta opción de almacenar los marcadores es muy común entre los diferentes navegadores. Aunque podemos almacenar los marcadores desde el menú de los navegadores web, la opción de marcar con la estrella se ha estandarizado en la gran mayoría de navegadores.

En las opciones del navegador, encontraremos las herramientas que nos permiten gestionar los diferentes enlaces que almacenemos. En el caso de Google Chrome, los encontramos en el menú de la parte superior, aunque en otros casos como Firefox, estos se gestionan desde el apartado de biblioteca.



Siguiendo con el ejemplo anterior, podemos ver que haciendo clic con el botón derecho sobre la barra inmediatamente inferior y eligiendo el comando **Administrador de marcadores**, podemos gestionar los enlaces.



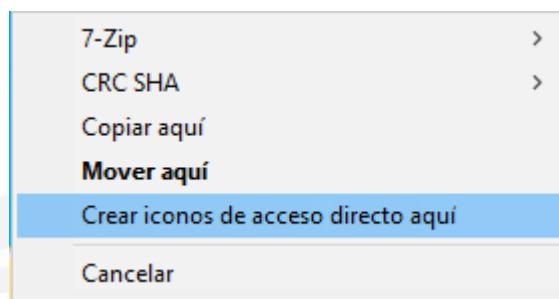
El “Administrador de marcadores” de Chrome nos permite gestionar los enlaces.

Observa que, en realidad, no guardamos las páginas web que nos han interesado. Únicamente creamos vínculos hacia las mismas. Si la página web deja de estar accesible, el vínculo deja de funcionar.

De igual manera, a menudo, los sistemas operativos nos permiten crear vínculos a ejecutables, carpetas y archivos que funcionan de manera similar: el vínculo que se crea es únicamente una vía rápida para acceder a la información. Pero si la información desaparece, dejamos de tener acceso a ella.

En Windows, dichos vínculos se denominan accesos directos. Podemos crearlos pulsando con el botón secundario del ratón sobre el elemento que deseamos vincular y arrastrándolo al punto donde queremos crear el vínculo.

En el menú contextual que se despliega, elegimos *Crear acceso directo aquí*.



Para crear el equivalente a los enlaces en Linux se utiliza la instrucción *ln*, cuyo formato es el siguiente:

- *ln -s nombre_archivo nombre_enlace*

Aunque al igual que en el caso de Windows, podremos crear accesos directos de una forma gráfica con los gestores gráficos que utilicemos.

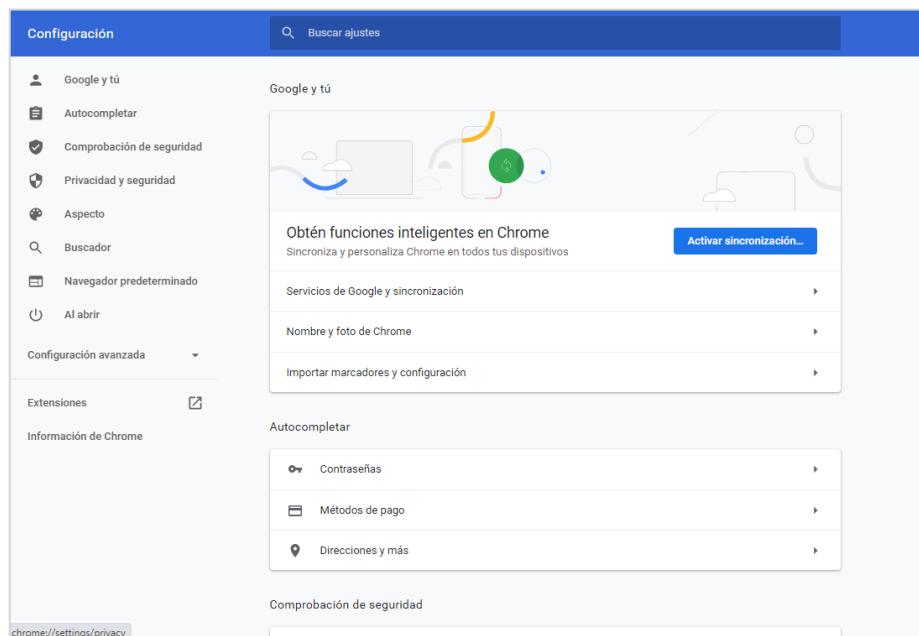


La gestión de enlaces es una opción que nos agilizará muchos procesos cotidianos en los sistemas informáticos, ya sea con enlaces a direcciones web o enlaces a aplicaciones instaladas en el sistema operativo.

Cabe destacar que en la mayoría de las instalaciones de aplicaciones en los sistemas operativos ya se crearán por defecto los diferentes accesos directos. En este caso nos ofrecerán la función de crear o anclar accesos directos en diferentes zonas que habilite el sistema operativo. En el caso de Windows, en la barra de tareas y el inicio y en el caso de sistemas Linux, en la barra lateral y el acceso rápido a las aplicaciones del sistema. Aunque cada sistema proporciona sus posibilidades, las opciones que ofrecen, al igual que los navegadores, son muy similares.

En cambio, en los navegadores web hay que configurarlos. En este caso, la mayoría de los navegadores ofrecen la opción de enlazar o importar los marcadores que hayamos elegido con un usuario determinado o en otros navegadores. Estas opciones pueden agilizar el proceso de generar marcadores utilizados habitualmente de una forma rápida, ya que tendremos la opción de sincronizar el usuario o el otro navegador para importar su configuración. De este modo, podemos traspasar información del navegador de una máquina a otra de una forma relativamente sencilla y cómoda.

En la actualidad, el aumento en el uso de dispositivos móviles para acceder a internet ha hecho que los navegadores web sean las aplicaciones más utilizadas. Por eso que han surgido nuevas formas más sencillas de tener sincronizados los diferentes dispositivos para un uso personal, facilitando de este modo la gestión de los datos en todos los dispositivos.



3.5. ESTRUCTURA DE DIRECTORIOS DE SISTEMAS OPERATIVOS LIBRES Y PROPIETARIOS

Hemos visto que la estructura de archivos y directorios en los sistemas operativos conforma un árbol. Esta estructura se encuentra jerarquizada para facilitar la labor a los usuarios. Como tales, siempre y cuando dispongamos de privilegios, podemos modificarla generando nuevas carpetas, eliminando otras, etc.

Sin embargo, tras instalar el sistema, la información suele estructurarse de acuerdo con unos estándares.

En las distribuciones de Linux, el sistema operativo libre por antonomasia, los elementos clave del árbol de directorios son, en esencia, los siguientes:

Directarios Linux	Almacenan.
/bin	Comandos esenciales que usará el usuario. En este directorio se almacenan archivos binarios/ejecutables, imprescindibles para el funcionamiento del sistema.
/boot	Archivos de arranque de Linux exceptuando los archivos de configuración.
/dev	Archivos que corresponden al hardware (ratón, teclado, disco duro, etc.).
/etc	Contiene los archivos de configuración del sistema.
/home	Estructura de árbol en la que cada usuario tiene su propio subdirectorio. Equivalente a la carpeta <i>Documents and Settings</i> de Windows.
/lib	Librerías y módulos del núcleo.
/media	Información para medios extraíbles.
/mnt	Monta los sistemas de archivos temporalmente.
/opt	En este directorio se almacenan los programas que instala el usuario y no forman parte del sistema operativo, por ejemplo: Spotify.
/proc	Informes de logs del núcleo.
/sbin	Comandos que solo puede ejecutar el administrador.
/srv	Datos de servicios.
/tmp	Archivos temporales.

/usr	Contiene aplicaciones y recursos disponibles para los usuarios del sistema operativo.
/var	Archivos que cambian dinámicamente.
/root	Carpeta <i>home</i> del administrador.
/proc	Documentación del sistema.



Carpetas de la raíz de un sistema Ubuntu.

En las versiones más recientes de Windows, el sistema operativo comercial más utilizado, se crea también su propia estructura árbol de directorios predeterminada. En ella destacan las siguientes carpetas:

- **Windows:** contiene los archivos del sistema operativo.
- **Archivos de programa:** aquí se guardan todos los programas que tenemos instalados en el PC.
- **Documents and settings:** aquí se guardan los datos de los usuarios que acceden al equipo: su escritorio, sus favoritos, etc.

Veamos algunas de sus subcarpetas:

- **Archivos comunes:** contiene datos de programas que van a utilizar varios usuarios o aplicaciones.

- **Usuarios:** contiene las carpetas de los diferentes usuarios. En cada una de ellas encontramos:
 - **Cookies:** cookies de páginas web.
 - **Escritorio:** contenidos de los accesos directos, archivos y carpetas del escritorio.
 - **Favoritos:** páginas web agregadas como favoritas.
 - **Menú inicio:** accesos directos del menú inicio del usuario en cuestión.
 - **Mis documentos:** archivos personales del usuario.

Nombre	Fecha de modificación	Tipo	Tam
Archivos de programa	01/04/2020 4:42	Carpeta de archivos	
Archivos de programa (x86)	22/06/2020 5:07	Carpeta de archivos	
PerfLogs	15/09/2018 2:33	Carpeta de archivos	
Usuarios	23/03/2020 8:06	Carpeta de archivos	
Windows	27/03/2020 7:49	Carpeta de archivos	

Carpetas de la raíz de un sistema Windows 10.

Por último, debemos señalar que lo ideal es que, pese a que de manera predeterminada todo se almacene en una misma partición, lo ideal es que los documentos de los usuarios se guarden en una partición independiente. De este modo, salvaguardarlos mediante backups resultará más sencillo.

Esta mecánica de trabajo también nos permite respaldar regularmente la partición en la que se halla el sistema operativo, independientemente de los datos de los usuarios. Así, en caso de fallos graves, podremos restaurarla respetando los documentos.

ponte a prueba,

¿En qué carpeta del sistema almacena un sistema operativo Windows la instalación de los programas que tenga instalados?

- a) etc
- b) Archivos de programa
- c) Documents and settings
- d) bin

3.6. BÚSQUEDA DE INFORMACIÓN DEL SISTEMA MEDIANTE COMANDOS Y HERRAMIENTAS GRÁFICAS

Es muy importante que la información de todas las particiones que tengamos esté ordenada. Para ello, debemos explotar al máximo las funcionalidades que nos ofrecen

las carpetas y clasificar los datos en función de los usuarios que vayan a acceder a los mismos, tipo de archivos, etc.

De todas formas, algunas veces, nos vemos obligados a buscar un determinado archivo o directorio y, para ello, podemos utilizar diferentes comandos o una interfaz gráfica.

Es de vital importancia que nos familiaricemos con lo que denominaremos comodines. Estos símbolos sirven para reemplazar cadenas de caracteres, tanto en comandos, como en diferentes herramientas gráficas.

En el caso de DOS y Windows disponemos de los siguientes comodines:

- **Asterisco (*)**: sustituye cadenas completas de caracteres y podemos utilizarlo para remplazar el nombre completo o alguna parte del nombre de cualquier archivo. También puede remplazar su extensión.

Ejemplo: si escribimos la expresión ***.txt** nos estamos refiriendo a documentos de texto que tengan cualquier nombre cuya extensión sea la de un documento de texto.

Si tecleamos **DEL *.txt**, estamos indicando que vamos a borrar todos los documentos de texto, independientemente de cuál sea su nombre.

- **Interrogación (?)**: remplaza un solo carácter, aunque se pueden poner varios símbolos de interrogación, según las necesidades.

Ejemplo: si escribimos la expresión **d???.txt** nos estamos refiriendo a cualquier documento de texto con extensión **.txt** que empiece por la letra d y esté seguida de dos caracteres más.

Si tecleamos **DEL d???.txt** solamente borraremos aquellos archivos con esta extensión, que cumplan este requisito (d03.txt, dat.txt, etc.).

PARA + INFO

Una vez que tenemos claro este concepto, podemos encontrar ficheros desde el *símbolo del sistema de Windows*, tecleando lo siguiente:

DIR [fichero a buscar] /s

Podemos observar que:

- El parámetro **/s** buscará en los subdirectorios.
- En el nombre del fichero a buscar podemos teclear comodines.
- Ejemplo: DIR s*.doc* buscará los archivos y directorios que empiecen con la letra s y cuya extensión sea DOC, DOCX, etc.

```

Símbolo del sistema - dir s*.doc /s
Directorio de E:\Mis documentos\Sergi\Dropbox\Interficie\Entrega_3
19/06/2014 14:09      514.717 Simulacro 2 MOD 5 .docx
19/06/2014 14:09      581.434 Simulacro 1 MOD 5 .docx
01/07/2014 11:56      703.374 Simulacro 2 MOD 5_solucionado.docx
30/06/2014 18:33      1.937.081 Simulacro 1 MOD 5_solucionado.docx
                           4 archivos   3.736.606 bytes

Directorio de E:\Mis documentos\Sergi\Dropbox\Punto_y_coma
23/04/2014 18:13      40.448 Sergi_Puertas_-_Punto_y_coma_Entrega_2_f.doc
30/05/2014 14:30      35.328 Sergi_Puertas_-_Punto_y_coma_Entrega_3.doc
14/09/2014 21:08      43.520 Sergi_Puertas_-_Punto_y_coma_Entrega_4.doc
14/09/2014 20:35      30.208 Sergi_Puertas_-_Punto_y_coma_Entrega_4_ANEXO
                           .doc
                           4 archivos   149.504 bytes

Directorio de E:\Mis documentos\Sergi\Dropbox\Samexistens
09/04/2014 12:50      54.784 Samexistens_-_Primera_parte_v0.01.doc
12/04/2014 19:20      96.256 Samexistens_-_Primera_parte_v0.02.doc
12/04/2014 19:51      98.816 Samexistens_-_Primera_parte_v0.03.doc
12/04/2014 20:30      88.064 Samexistens_-_Primera_parte_v0.03_Pier.doc
23/04/2014 18:54      97.792 Samexistens_-_Primera_parte_v0.04.doc
05/05/2014 21:47      193.536 Samexistens_-_Primera_parte_v0.05.doc
07/05/2014 18:55      232.960 Samexistens_-_Primera_parte_v0.06.doc
07/05/2014 18:55      232.960 Samexistens_-_Primera_parte_v0.07.doc
07/05/2014 21:38      218.624 Samexistens_-_Primera_parte_v0.07_Pier.doc
07/05/2014 21:39      218.624 Samexistens_-_Primera_parte_v0.08.doc
26/04/2014 11:44      136.704 Samexistens_-_Segunda_parte_v0.01.doc
09/04/2014 12:56      45.568 Samexistens_-_Sinopsis_-_Sergi_Puertas.doc
26/04/2014 11:29      136.704 Samexistens_-_Tercera_parte_v0.01.doc
10/04/2014 10:29      34.304 Samexistens_v0.02.doc
                           14 archivos   1.885.696 bytes

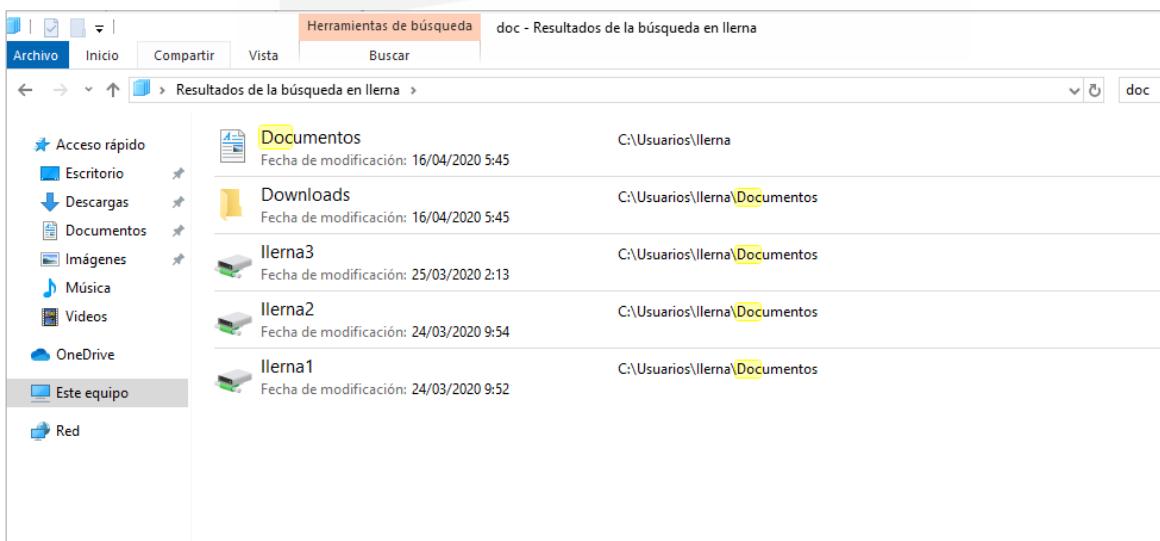
Directorio de E:\Mis documentos\Sergi\Dropbox\SGAE
19/09/2014 18:58      64.492 SINOPSIS Estripar la terra - Josep Maria Mir
0 - Autor Exprés.docx
30/09/2014 18:13      15.146 SINOPSIS Estripar la terra - Josep Maria Mir
0 - Autor Exprés [editado_SP].docx
                           2 archivos   79.638 bytes

```

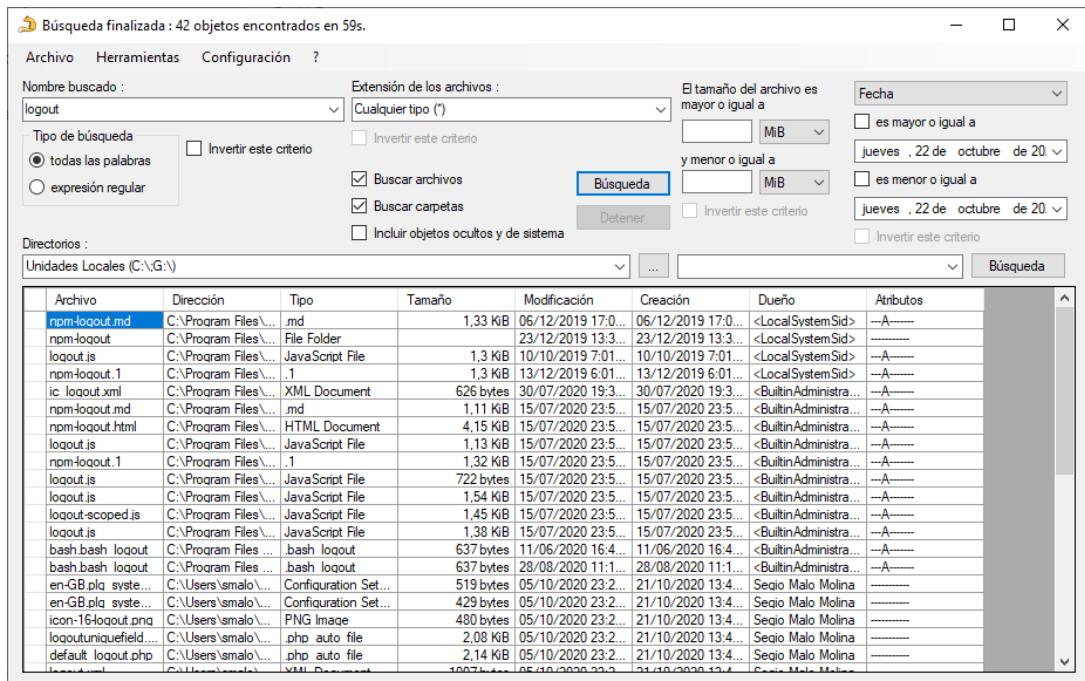
Búsqueda de archivos desde la línea de comando.

Si preferimos usar una herramienta gráfica, en Windows 10 podemos emplear la casilla situada en el área superior derecha del Explorador de Windows.

Dicha casilla también admite comodines y permite especificar otros detalles para filtrar la información, como el tamaño del fichero, su fecha, etc.



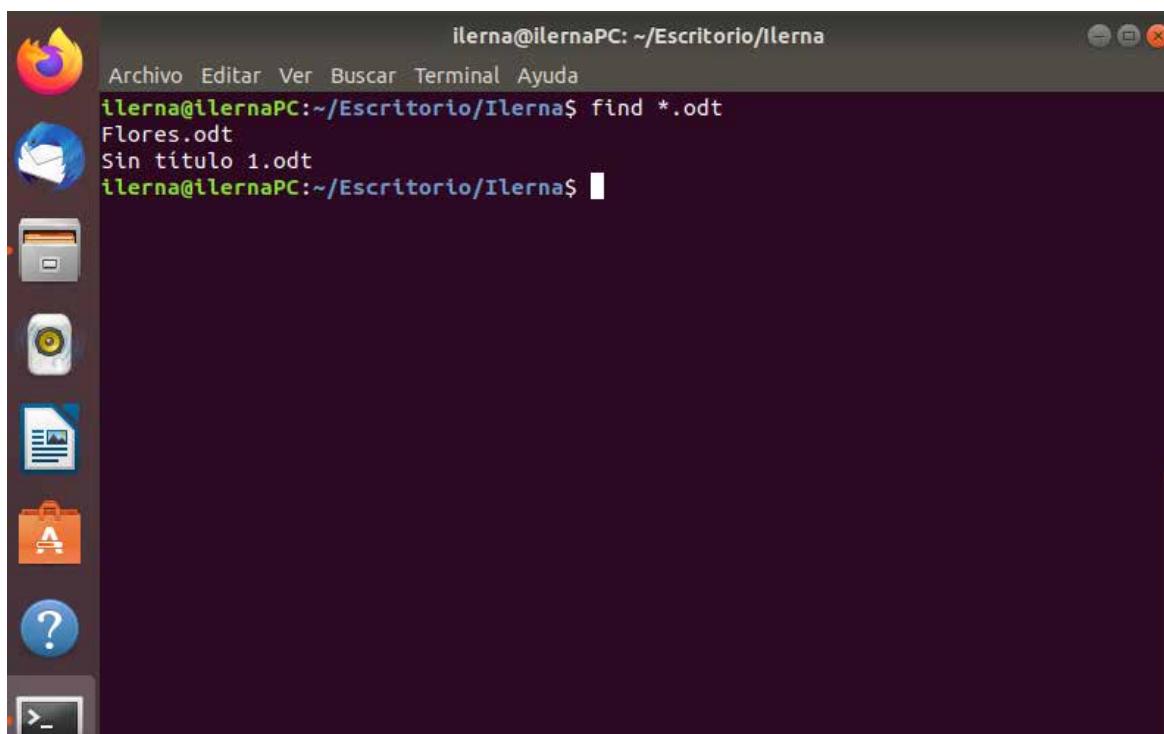
Por supuesto, como alternativa, también podemos utilizar software específicamente orientado a búsquedas como **FileSearch** (<http://sourceforge.net/projects/file-search/>), que nos brindará más opciones.



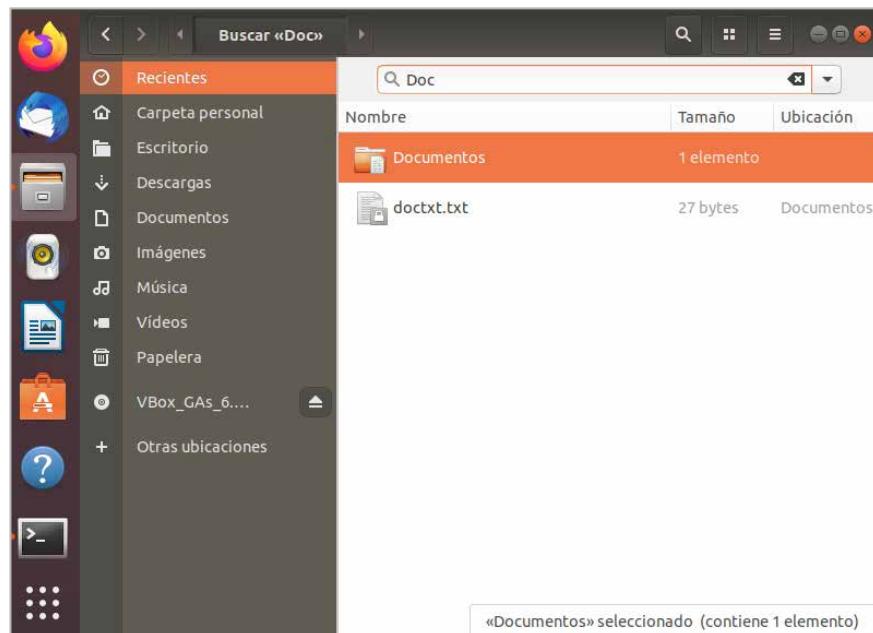
Búsqueda de archivos desde FileSearch.

En el caso de sistemas operativos libres, las búsquedas por interfaz gráfica o de texto son similares, aunque en esta última, con los comandos adecuados para el sistema operativo que utilicemos.

Para buscar en Linux, contamos con la posibilidad de emplear el comando *find* desde la consola. Como alternativa, podemos usar las opciones de búsqueda que nos brindan Nautilus, Krusader, Konqueror y los demás administradores de archivos.



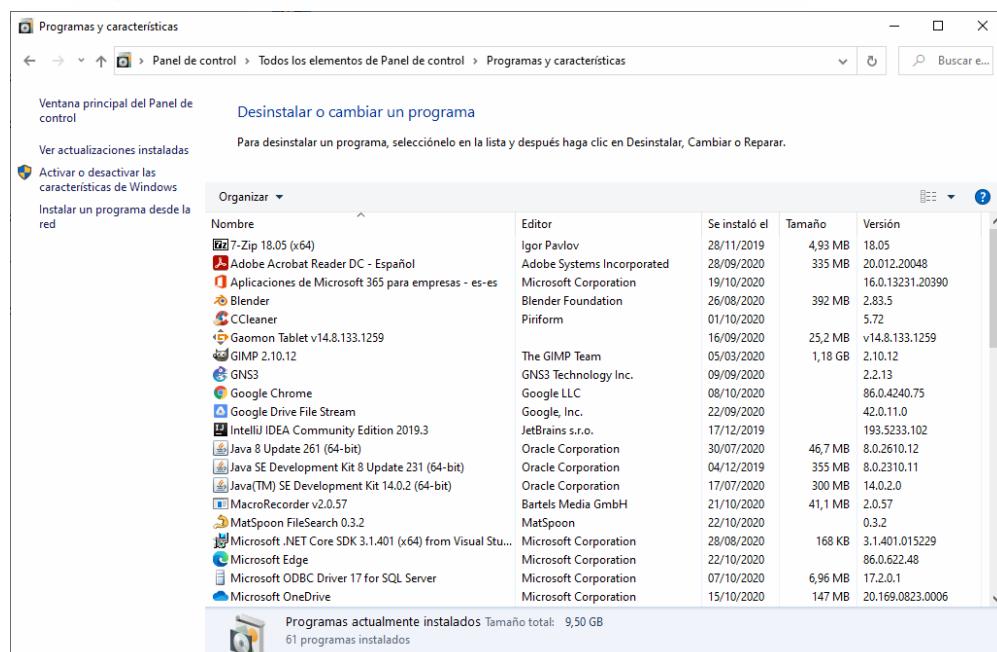
Búsqueda de archivos desde la terminal de Ubuntu.



Búsqueda de archivos desde el gestor de archivos de Ubuntu.

3.7. IDENTIFICACIÓN DEL SOFTWARE INSTALADO MEDIANTE COMANDOS Y HERRAMIENTAS GRÁFICAS

A la hora de determinar qué software tenemos instalado en un equipo, lo más sencillo es remitirse al área del sistema orientada a este fin. En Windows 10, por ejemplo, para esta acción podemos acceder al **Panel de control**, entrar en **Programas** y hacer clic en **Programas y características**.



Tras acceder al “Panel de control” entraremos en “Programas” y haremos clic en “Programas y características”.



No obstante, ahora que tenemos una idea general de cuál es la estructura de directorios de los principales sistemas operativos, también podemos examinar los programas instalados usando comandos.

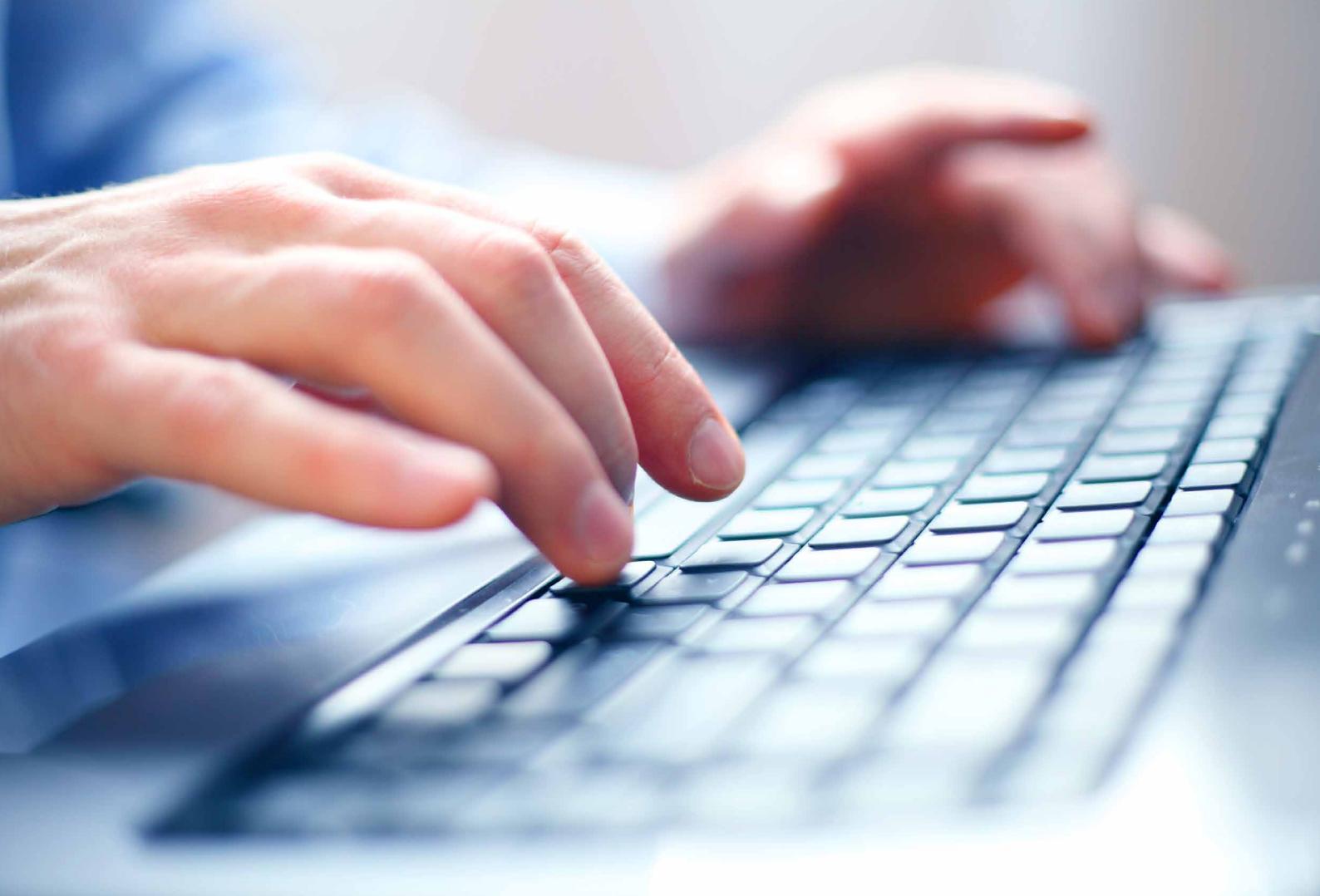
En Windows, debemos usar el **Símbolo del sistema** para desplazarnos a la carpeta **Archivos de programa**. Una vez allí, tecleamos **DIR** para listar el directorio y ver qué programas hay en el equipo.

```
20/10/2014 13:00 <DIR> .
14/05/2014 12:48 <DIR> ..
10/02/2014 21:31 <DIR> Adobe
25/04/2014 20:12 <DIR> AIMP3
13/02/2014 22:25 <DIR> ArcSoft
20/07/2013 16:29 <DIR> ASIO4ALL v2
22/04/2014 18:07 <DIR> AVAST Software
06/06/2014 21:09 <DIR> AVEO UVC Like Driver
25/08/2014 17:04 <DIR> Bitdefender
06/02/2013 15:52 <DIR> Calibre2
25/04/2014 20:12 <DIR> CDBurnerXP
26/05/2014 14:06 <DIR> Common Files
06/02/2013 15:03 <DIR> Configurador AEAT
06/06/2014 21:21 <DIR> D-Link
06/02/2013 15:26 <DIR> DAEMON Tools Lite
06/02/2013 16:01 <DIR> Ditto
02/04/2014 12:55 <DIR> DVD Maker
28/02/2013 18:35 <DIR> eMule
22/04/2014 18:01 <DIR> FileZilla FTP Client
15/05/2014 09:29 <DIR> Free Picture Solutions
20/07/2013 16:42 <DIR> FreeStopwatch
07/10/2013 20:32 <DIR> FreeTime
20/05/2013 18:55 <DIR> GixinDesktopManager
20/05/2013 19:05 <DIR> Google
27/08/2014 17:11 <DIR> GTK2-Runtime
05/10/2013 16:32 <DIR> Intel
18/04/2013 09:41 <DIR> Internet Explorer
06/06/2014 17:59 <DIR> Java
21/03/2013 13:59 <DIR> KMSpico
08/04/2014 17:56 <DIR> LinuxLive USB Creator
06/02/2013 15:44 <DIR> Logitech Gaming Software
20/10/2014 13:00 <DIR> Macrium
06/02/2013 15:17 <DIR> MatSpoon
21/11/2010 02:47 <DIR> Microsoft Analysis Services
30/03/2014 15:19 <DIR> Microsoft Games
06/02/2013 15:18 <DIR> Microsoft Office
06/02/2013 15:18 <DIR> Microsoft SQL Server Compact Edition
04/03/2013 14:00 <DIR> Microsoft Synchronization Services
25/11/2013 12:04 <DIR> Microsoft .NET
01/09/2014 15:06 <DIR> MiPony
13/09/2014 12:44 <DIR> Mozilla Firefox
14/07/2009 06:52 <DIR> Mozilla Maintenance Service
30/03/2014 15:18 <DIR> MSBuild
24/04/2014 11:36 <DIR> MSECache
20/07/2013 16:54 <DIR> My Company Name
NCH Swift Sound
```

También podemos identificar el software instalado mediante el comando **DIR**.

En Linux podemos consultar los paquetes instalados usando las herramientas gráficas que nos brinda el sistema o mediante el comando **dpkg**.

Por ejemplo, en sistemas operativos Ubuntu encontramos el Centro de Software de Ubuntu, donde podemos gestionar las aplicaciones que queremos instalar en el sistema.



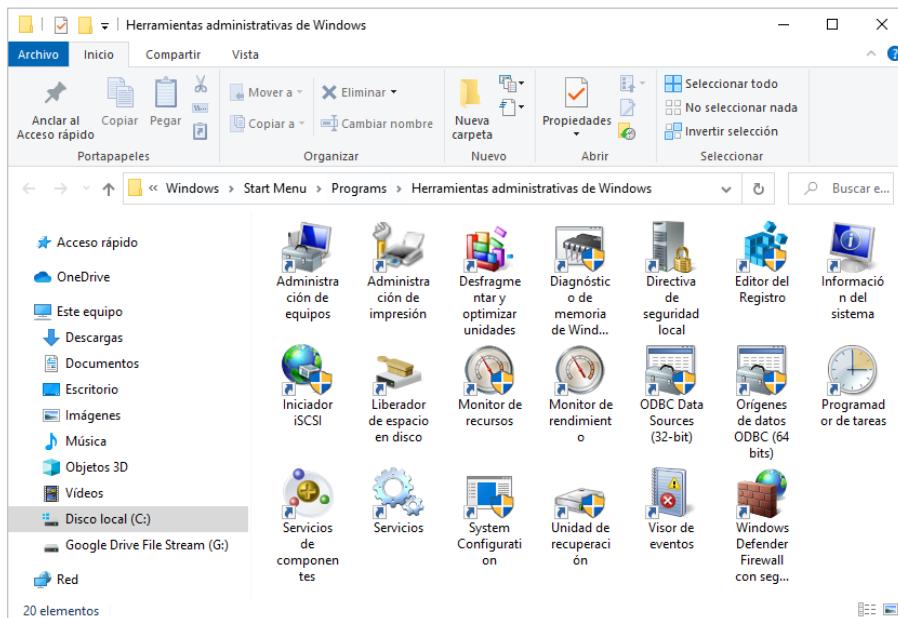
3.8. GESTIÓN DE LA INFORMACIÓN DEL SISTEMA. RENDIMIENTO. ESTADÍSTICAS

A menudo deseamos obtener datos cuantificables del rendimiento de nuestro equipo más allá de nuestras percepciones subjetivas acerca del mismo. En Windows 10 podemos acceder a un área dedicada a este fin, accediendo a las *Propiedades de Equipo*.

En la ventana que se abrirá debemos hacer clic en *Evaluación de la experiencia en Windows*. Las puntuaciones que se asignan a los diversos aspectos (gráficos, disco duro, etc.) están comprendidas entre 1,0 (el mínimo) y 7,9 (el máximo).

Esta evaluación de experiencia fue eliminada por Microsoft en la versión Windows 8.1, aunque a partir de esta versión, es posible visualizar esta evaluación, aunque no de manera gráfica.

El sistema operativo nos brinda otras herramientas complementarias para este fin, como el *Monitor de rendimiento*. Puedes acceder a ellas a través del Panel de control, entrando en *Sistema y seguridad* y haciendo clic en *Herramientas administrativas*.



"Herramientas administrativas" de Windows 10.

El Monitor de rendimiento permite generar informes a partir de los cuales se pueden elaborar estadísticas.

Como de costumbre, siempre contamos con la posibilidad de descargar e instalar software dedicado a este fin.

SiSoft Sandra (<http://wwwsisoftware.co.uk/>) es uno de los paquetes más reputados en este ámbito.

The screenshot shows the SiSoftware Sandra official classifier website. At the top, there are three small images of computer cases: Intel NUC BXNUC107FNK2 PC, Intel NUC Gemini Lake, and Intel NUC Barebone Mini PC Kit. Below them is a section titled "Posición más alta : Equipos" (Top position: Equipment) showing the top three positions:

Posición Mundial	Nombre	Puntos	Usuarios Creado
#1	ASUS	1.858.197 (+10.451)	3.281 27 octubre 2010
#2	AMD / ATI	1.633.500 (+8.802)	3.479 27 octubre 2010
#3	acer	1.419.647 (+6.300)	3.483 27 octubre 2010

Below this is a section titled "Posición más alta : Usuarios" (Top position: Users) showing the top three users:

Posición Mundial	Nombre	Puntos	Computadoras Creado	País	Equipo
#1	User	157.083 (-512)	552 21 septiembre 2020	India (India)	Mundial
#2	Home	43.448 (-161)	172 7 marzo 2020	Ireland (Ireland)	Ireland
#3	ASUS vivco	43.064 (-2.203)	7 18 julio 2020	USA (USA)	ASUS ASUS

At the bottom, there is a detailed table for the top two users, showing hardware specifications and performance metrics:

Posición Local	Usuario	Equipo	Computador	Identidad (ID) del resultado	Resultado	Capacidad	Velocidad	Estado Condición	Plataforma	Sistema operativo	Creado
#1 (>100,00%)	Intel Timppax2	intel Only	ASUS X79-DELUXE	NVIDIA GeForce GTX 980 16CU 3.00 GHz/7.11GHz/256-bit PCIe 3.0 x16 (Microsoft H264 Video Decoder MFT > NVIDIA HEVC Encoder MFT; Microsoft AAC Audio Decoder MFT > Microsoft AAC Audio Encoder MFT)	10,93MB/s	2048CU	1,61GHz	Normal	Desktop	Windows x64 10.0.5.23_1	4 abril 2016
#2 (>99,81%)	Intel Timppax2	intel Only	ASUS X79-DELUXE	NVIDIA GeForce GTX 980 16CU 3.00 GHz/7.11GHz/256-bit PCIe 3.0 x16 (Microsoft H264 Video Decoder MFT > NVIDIA HEVC Encoder MFT; Microsoft AAC Audio Decoder MFT > Microsoft AAC Audio Encoder MFT)	10,87MB/s	2048CU	1,53GHz	Normal	Desktop	Windows x64 10.0.5.23_1	23 febrero 2016

SiSoft Sandra permite comparar el rendimiento de nuestro equipo con el de otros usuarios del software.

En Linux podemos monitorizar el rendimiento empleando Sysstat, una colección de herramientas específicas para esto.

3.9. MONTAJE Y DESMONTAJE DE DISPOSITIVOS EN SISTEMAS OPERATIVOS

El montaje y el desmontaje de dispositivos es una técnica de administración de discos que generalmente se utiliza en Linux, pero que también está disponible en las versiones más recientes de Windows. Una unidad montada es, en definitiva, una partición asignada a una carpeta vacía de otra partición. Generalmente, a las unidades montadas se les asigna una etiqueta.

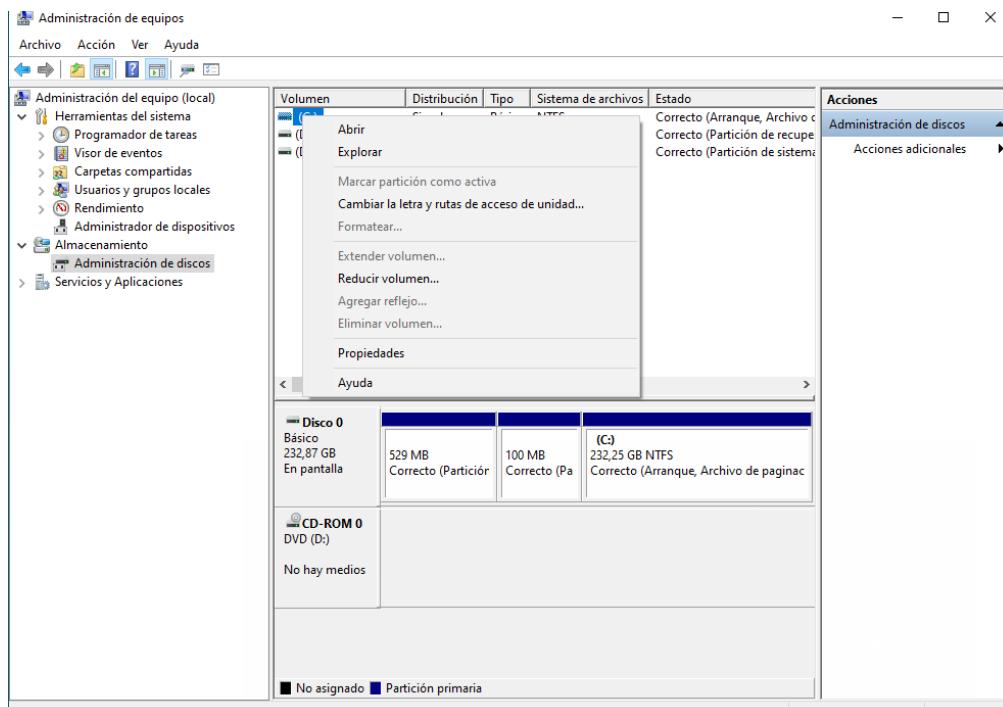
El montaje de dispositivos resulta particularmente útil cuando tenemos que compartir particiones o discos con grandes cantidades de usuarios, puesto que las unidades montadas nos ofrecen la posibilidad de ampliar la capacidad de almacenamiento de una unidad o una partición.

Así, si por ejemplo disponemos de una carpeta de red llamada **DATOS** en la que los usuarios acostumbran a guardar la información y se está llenando, mientras nuestra unidad F: está vacía, podemos crear un directorio vacío llamado **NOVIEMBRE** en la carpeta **DATOS** y montar la unidad F: en dicho directorio. Hecho esto, los usuarios podrán guardar los nuevos ficheros en **DATOS\NOVIEMBRE** y aprovechar todo el espacio de la unidad F:.



Para el montaje de una unidad debemos entrar en Panel de control, acceder a *Sistema y seguridad* y hacer clic en *Herramientas administrativas*. Una vez allí, hacemos clic en *Administración de equipos*.

En la ventana que se muestra, accedemos al panel izquierdo y, en *Almacenamiento*, abrimos el apartado *Administración de disco*.



La sección “Administrador de discos”, accesible a través de la “Administración de equipos” de Windows.

Una vez listadas las particiones, hacemos clic con el botón derecho del ratón en la unidad que queremos montar. En el menú contextual pulsamos sobre la opción *Cambiar la letra y rutas de acceso de unidad*.

Seguidamente, pulsamos sobre *Agregar en Montar en la siguiente carpeta NTFS vacía* y, a continuación, escribimos la ubicación de una carpeta vacía. Tras aceptar los cambios, la unidad quedará montada.

Si más adelante deseamos desmontar la unidad, la misma sección de *Administración de discos* nos brinda la opción de hacerlo. Tras pulsar con el botón derecho del ratón sobre la unidad montada, hacemos clic en *Cambiar la letra y rutas de acceso de unidad*. Esto nos permitirá seleccionar el comando *Quitar*.

No obstante, como apuntábamos al principio, el montaje y desmontaje está muy extendido en Linux. Para ello, se utiliza el comando *mount*.

PARA + INFO

El formato de dicha instrucción desde la línea de comandos es el siguiente:

"mount -t" <sistema de ficheros> <Dispositivo> <Carpeta>

Así, por ejemplo, el comando *mount -t ntfs /dev/sda1 /data/win* monta una unidad de disco NTFS en la carpeta Win.

Para el desmontaje, utilizaremos el comando *umount*.

PARA + INFO

Su formato es el siguiente:

umount <Dispositivo>

Así pues, para desmontar el disco que hemos montado en el ejemplo anterior, teclearemos lo siguiente: *umount /data/win*

ponte a prueba

¿Cuál de las siguientes opciones reúne herramientas que nos brinda el sistema operativo Windows?

- a) Administración de equipos, administrador de discos y programador de tareas.
- b) Generador de eventos, programador de tareas y referenciador de registros.
- c) Publicador de contenido, administrador de equipos y administrador de discos.
- d) Referenciador de registros, administrador de discos y generador de eventos.

El monitor de rendimiento de Windows permite generar informes a partir de los cuales es posible elaborar estadísticas.

- a) Verdadero.
- b) Falso.

3.10. AUTOMATIZACIÓN

Existen una serie de tareas rutinarias que es preciso realizar con regularidad. Frente a la opción de ejecutarlas de manera manual, existe la posibilidad de automatizarlas para que se ejecuten sin que tengamos que estar pendientes de ellas.

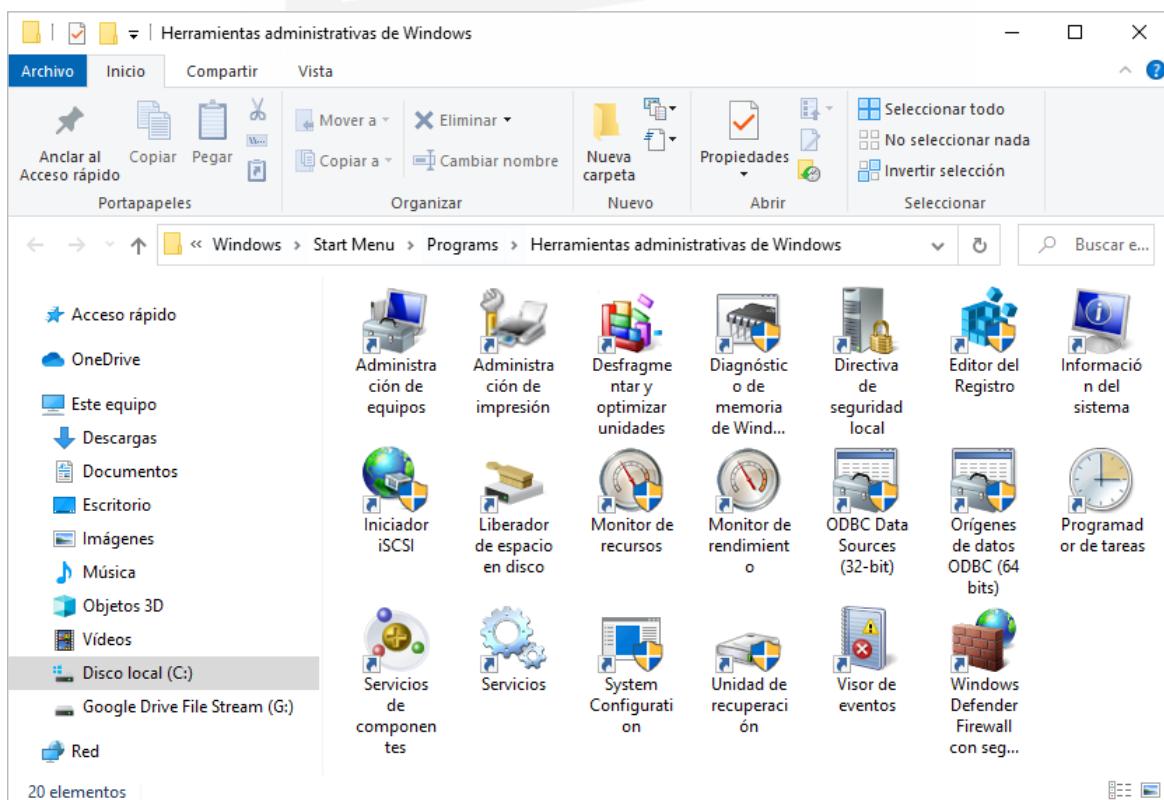
Son muchas las aplicaciones que brindan esta característica, pero hay dos casos en los que automatizar resulta particularmente interesante:

Copias de seguridad

Una de las tareas más importantes y a la que quizás no demos importancia, es la realización de copias de seguridad. Cualquier *malware*, error de hardware o fallo del sistema puede causar la pérdida de toda la información que tenemos almacenada en el sistema. Es por este motivo que las copias de seguridad de forma periódica son un proceso muy importante.

Para poder automatizar este tipo de tareas, Windows 10 incluye una función que nos permite crear copias de seguridad de forma automática.

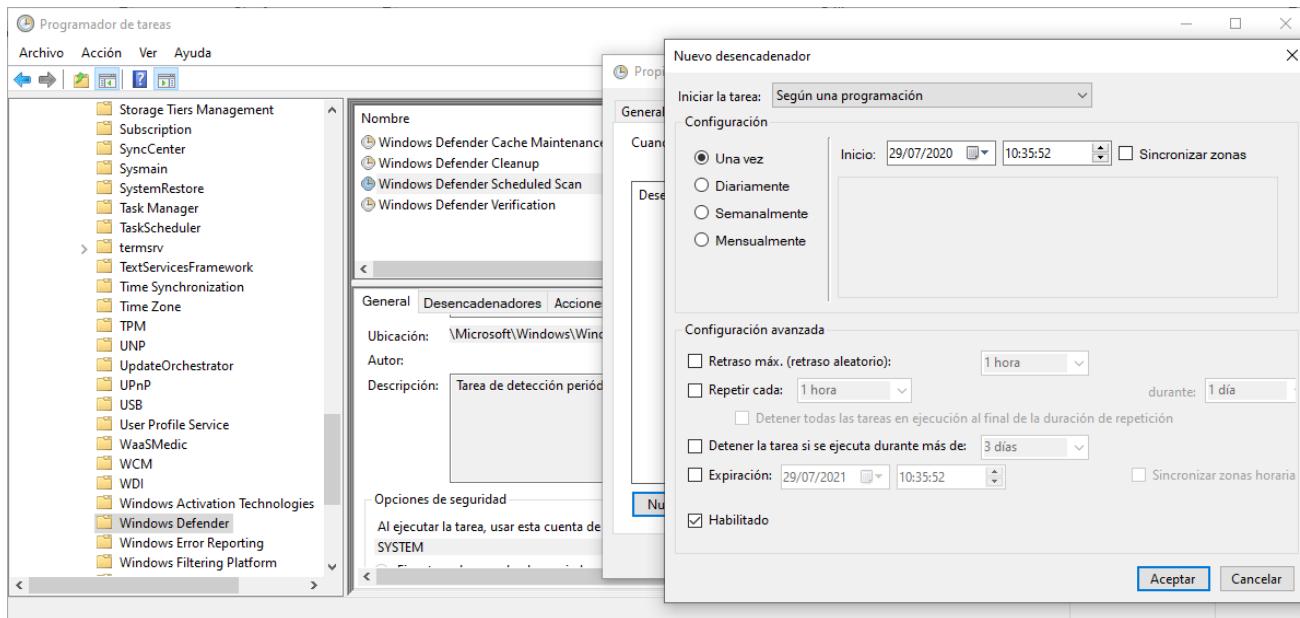
Estas copias de seguridad, también conocidas como backups, incluyen toda la información que está almacenada en el sistema y, ante cualquier fallo, es posible restaurar el sistema completamente en cuestión de minutos.



Administrar copias de seguridad en Windows 10.

Antivirus

Prácticamente todos los antivirus, ofrecen la opción de automatizar los análisis. En el caso de la seguridad de Windows, es posible programar un análisis de *Windows Defender*.



Administrar análisis programado.

Gracias a la automatización de estos procesos, podemos programar estas acciones de modo que se ejecuten durante la hora de comer, durante la noche o en aquellas horas que no consumirán recursos de sistema y no cuando los necesitaremos para trabajar.

En el caso de que una aplicación no nos brinde opciones de automatización, podemos programarla igualmente, utilizando las herramientas que nos ofrece el sistema operativo para este fin. En Windows contamos con el *Programador de tareas*.

Así, para automatizar una tarea mediante esta herramienta entraremos en el **Panel de control**, accederemos a **Sistema y seguridad** y haremos clic en **Herramientas administrativas**. Una vez allí, pulsaremos en **Administración de equipos**.

En la ventana que se mostrará, accederemos al panel izquierdo, donde pulsaremos sobre **Programador de tareas**.

El panel derecho nos brindará la opción de **Crear tarea**. Tras pulsar encima, podemos definir, entre otras cosas, qué tarea se va a ejecutar y en qué condiciones.



INTERNACIONAL

Administración de equipos

Archivo Acción Ver Ayuda

Resumen de Programador de tareas (actualización más reciente: 22/10/2020 16:20:33)

Administración del equipo (local)

- Herramientas del sistema
 - Programador de tareas
 - Visor de eventos
 - Carpetas compartidas
 - Usuarios y grupos locales
 - Rendimiento
 - Administrador de dispositivos
- Almacenamiento
 - Administración de discos
- Servicios y Aplicaciones

Acciones

- Programador de tareas
- Crear tarea básica...
- Crear tarea...
- Importar tarea...
- Mostrar todas las tareas...
- Deshabilitar el historial...
- Configuración de cuentas...
- Ver
- Actualizar
- Ayuda

Crear tarea

General Desencadenadores Acciones Condiciones Configuración

Especifique las condiciones que, junto a los desencadenadores, determinarán si se debe ejecutar la tarea. Si alguna de las condiciones especificadas no se cumple, no se ejecutará la tarea.

Inactivo

Iniciar la tarea solo si el equipo está inactivo durante: 10 minutos

Esperar a que esté inactivo durante: 1 hora

Detener si el equipo deja de estar inactivo

Reiniciar si el estado de inactividad se reanuda

Energía

Iniciar la tarea solo si el equipo está conectado a la corriente alterna

Detener si el equipo empieza a usar la batería

Activar el equipo para ejecutar esta tarea

Red

Iniciar solo si la siguiente conexión de red está disponible:

Cualquier conexión

Aceptar Cancelar

Resumen: 120 en total

Última actualización a las 22/10/2020 16:20:33

Actualizar

La sección "Programador de tareas", accesible a través de "Administración de equipos", nos permite automatizar tareas.



En ocasiones, las tareas rutinarias que debemos realizar con regularidad pueden completarse mediante comandos. Por supuesto, contamos con la posibilidad de escribirlos una a una mediante la ventana de *Símbolo del sistema* de Windows 10. Pero existe la opción de simplificar significativamente este proceso gracias a los ficheros de proceso de lotes.

Este tipo de archivos nos brindan la opción de procesar una secuencia de comandos a partir de un archivo de texto sin formato. Si hacemos doble clic sobre él, todas las tareas que contiene se ejecutarán, una tras otra, de manera automatizada.

Para crear un archivo de proceso por lotes, podemos usar cualquier editor de texto simple, incluido el Bloc de notas.

Para la automatización, debemos proceder del siguiente modo:

- **Elección de las tareas que se van a automatizar:** en un documento en blanco, tecleamos los comandos correspondientes a las tareas que deseamos automatizar, pulsando *Intro* tras escribir cada una de ellas.

```

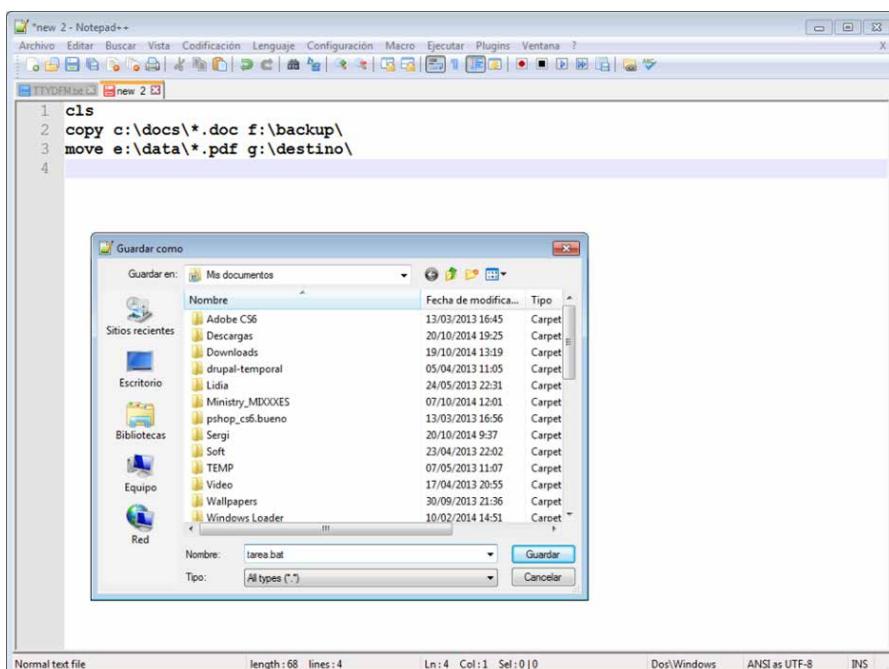
1 cls
2 copy c:\docs\*.doc f:\backup\
3 move e:\data\*.pdf g:\destino\
4

```

Normal text file length: 68 lines: 4 Ln: 4 Col: 1 Sel: 0 | 0 Dos\Windows ANSI as UTF-8 INS

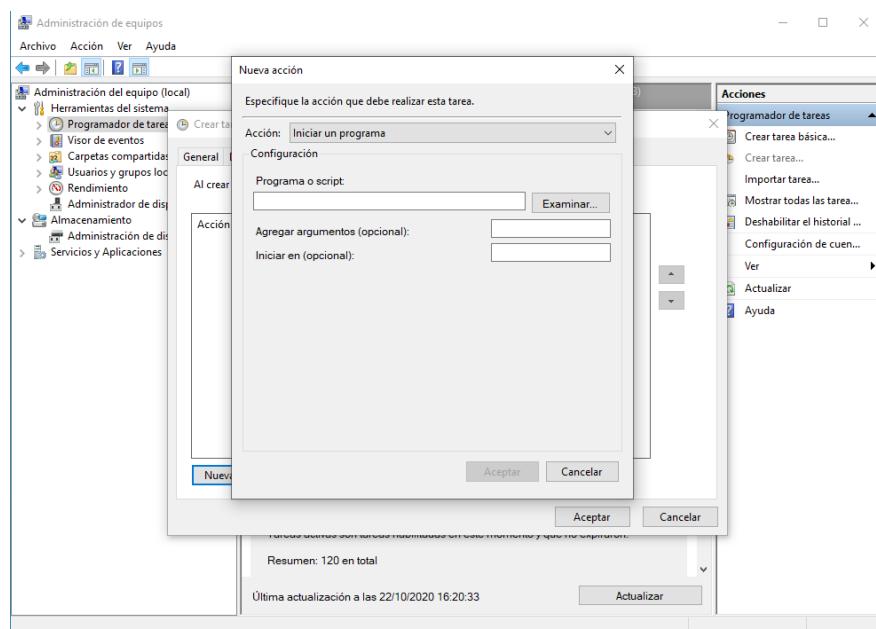
Escribimos los comandos.

- **Nombre del archivo:** al guardar el archivo, es muy importante que le asignemos la extensión .bat. Solo así, más adelante, cuando hagamos doble clic sobre él, todos los comandos que hayamos incluido se ejecutarán de forma secuencial.



Guardamos el archivo con extensión BAT.

- **Programación de las tareas automatizadas:** hecho esto, podemos programar la ejecución del archivo mediante la pestaña *Acciones del Programador de tareas*.



Programamos las condiciones en las que se ejecutará el archivo BAT.

Por último, señalar que gracias a aplicaciones como *Advanced BAT 2 EXE Converter* (<http://www.battoexe-converter.com/>) podemos convertir los archivos .bat en ejecutables .exe.

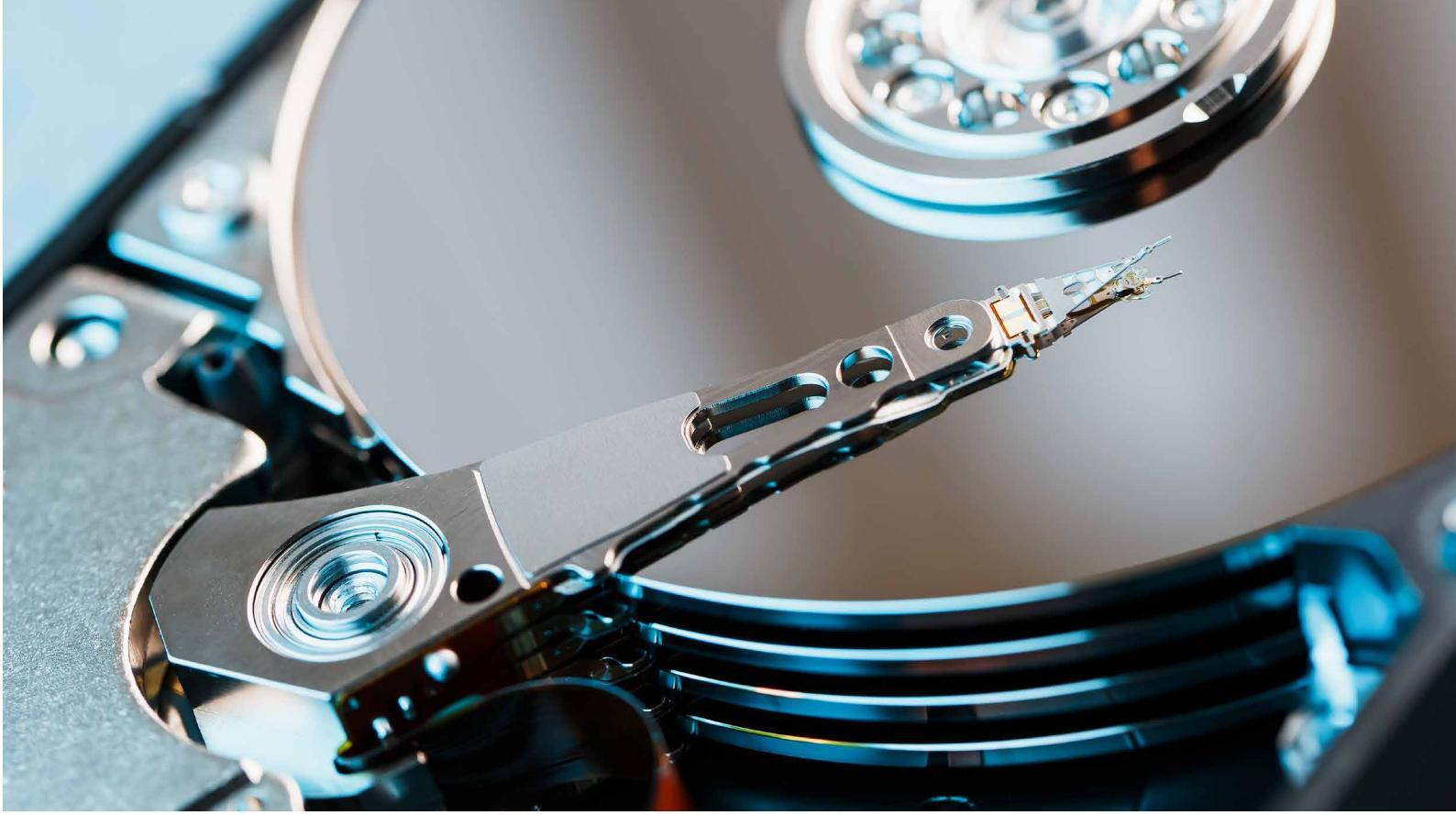
Si lo que precisamos es automatizar y programar tareas en Linux, podemos utilizar el servicio denominado **Cron**, pensado también para lanzar tareas regularmente en el momento que especifiquemos.

3.11. HERRAMIENTAS DE ADMINISTRACIÓN DE DISCOS. PARTICIONES Y VOLÚMENES. DESFRAGMENTACIÓN Y REVISIÓN

Como apuntábamos al principio del tema, una unidad física de disco puede dividirse en varias particiones. Cada partición puede tener su propio sistema de ficheros.

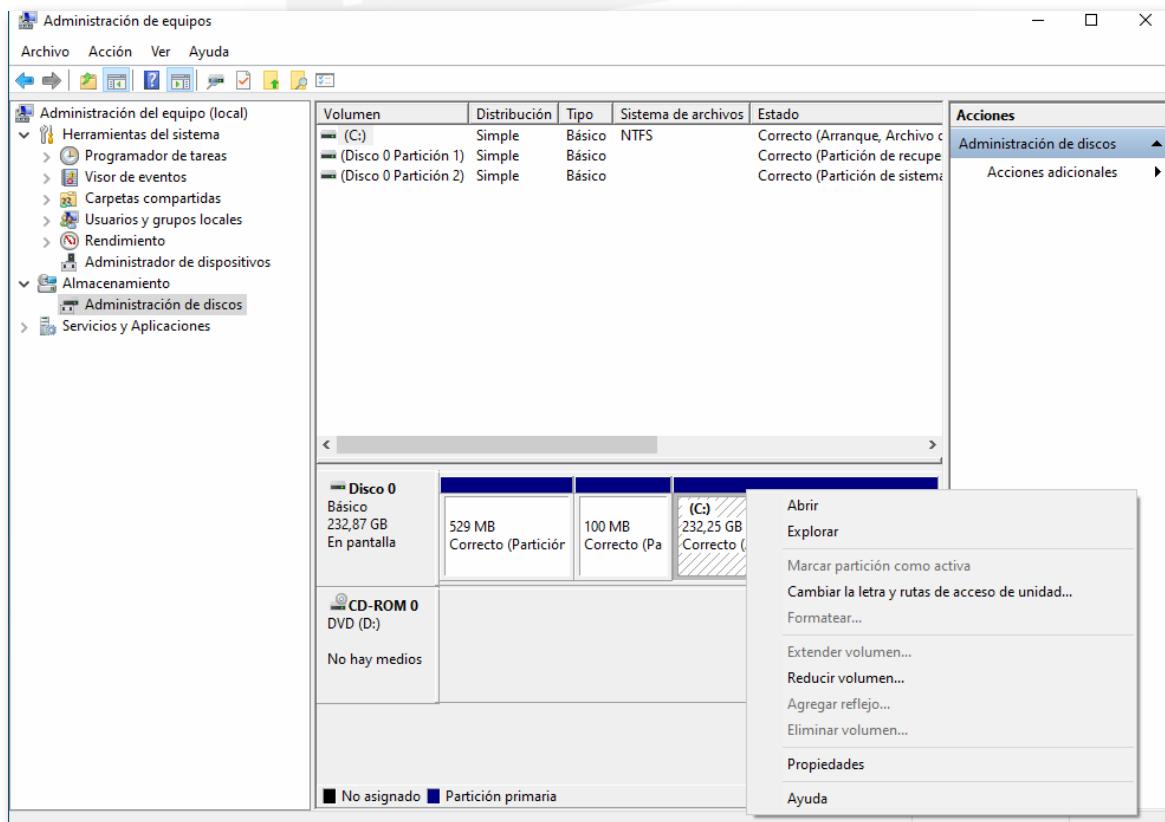
Estas particiones pueden definirse en el momento de instalar el sistema operativo. No obstante, también pueden generarse y modificarse desde el propio sistema.

En Windows, para modificar particiones, debemos entrar en **Panel de control**, acceder a **Sistema y seguridad** y hacer clic en **Herramientas administrativas**. Una vez allí,



haremos clic en **Administración de equipos**.

En la ventana que se muestra, accedemos al panel izquierdo y, en **Almacenamiento**, abrimos el apartado **Administración de discos**. Desde el área inferior de la ventana podemos crear nuevas particiones si hay espacio disponible, eliminar particiones y redimensionar las que tenemos creadas.



La "Administración de discos" en Windows 10 permite crear y eliminar particiones de disco.

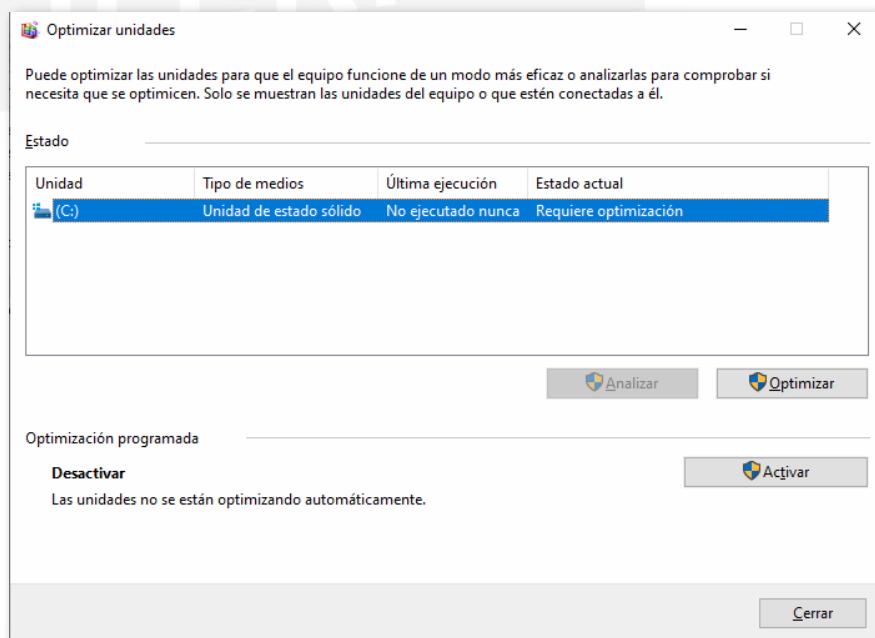
Por supuesto, para hacer uso de las herramientas que permiten administrar particiones es necesario disponer de privilegios de administrador, dado que eliminar una partición borra todos los datos que contiene la misma.

Estas son algunas de las herramientas más utilizadas para gestionar particiones en Linux:

- Gparted
- Pysdm
- Partitionmanager

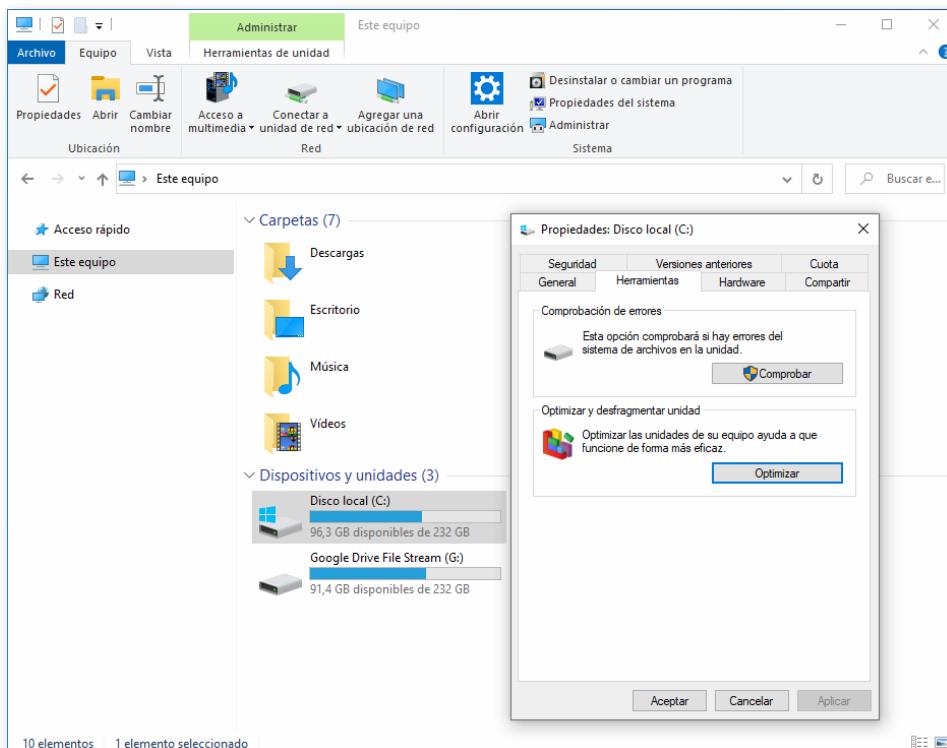
Por otra parte, cabe tener en cuenta que los sistemas de ficheros están sometidos a constantes procesos de creación, borrado y modificación de archivos que, a la larga, provocan que los ficheros se fragmenten y surjan huecos sin información en nuestras particiones. Esto origina una ralentización del acceso a los datos, puesto que los cabezales de los discos se ven obligados a desplazarse constantemente para acceder a la información.

Así pues, es conveniente que los desfragmentemos con regularidad. Para desfragmentar una partición en Windows 10 debemos acceder a las *Propiedades* de la misma a través de *Equipo*. En la pestaña *Herramientas*, hacemos clic en *Desfragmentar ahora*.



Desfragmentación de particiones en Windows 10.

Si lo que deseamos es analizar un disco en busca de errores, la propia pestaña *Herramientas* nos brinda la opción *Comprobar ahora*.



Análisis de disco en Windows 10.

En las versiones más recientes del sistema de ficheros que utiliza Linux, no es preciso desfragmentar las particiones. Si lo que deseamos es buscar errores en las mismas, usaremos el comando `fsck`.

BUSCA EN LA WEB

Puedes encontrar información detallada en español acerca de cómo utilizar **Gparted** de Linux en la página oficial de la aplicación:

gparted.org/display-doc.php?name=help-manual&lang=es

BUSCA EN LA WEB

Puedes encontrar información detallada en español acerca de cómo administrar discos en Windows en la página oficial de Microsoft:

windows.microsoft.com/es-es/windows7/managing-hard-disks-recommended-links



ponte a prueba

Una unidad física de disco no se puede dividir en varias particiones, sino que siempre se verá como una sola partición completa y para obtener más particiones necesitaremos más discos.

- a) Verdadero
- b) Falso

Los sistemas de ficheros están sometidos a constantes procesos de creación, borrado y modificación de archivos que, a la larga, provocará que los ficheros se fragmenten y surjan huecos sin información en nuestras particiones.

- a) Verdadero
- b) Falso



4

ADMINISTRACIÓN DE DOMINIOS

Mediante la Administración de dominios podemos **centralizar, simplificar y agilizar muy significativamente las tareas de gestión**. Crear un dominio en un equipo servidor al que se conecten equipos cliente resulta muy práctico a la hora de administrar redes.

Antes de profundizar en ello, debemos aclarar a qué nos referimos cuando hablamos de una estructura cliente-servidor.

4.1. ESTRUCTURA CLIENTE-SERVIDOR

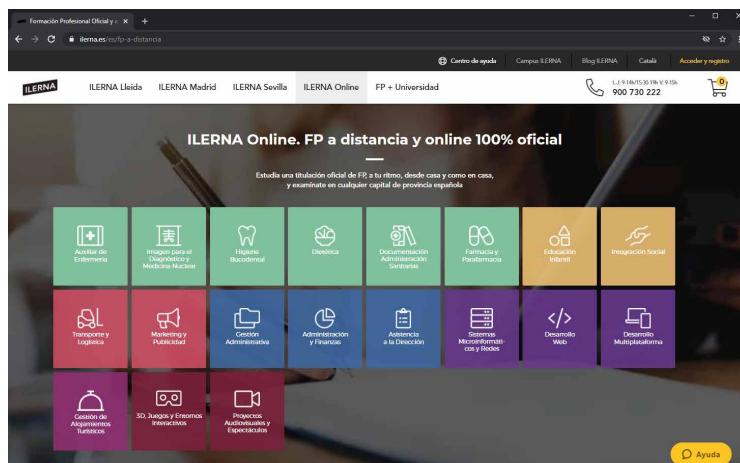
Al hablar de comunicación entre equipos informáticos es muy frecuente que encontremos lo que se denomina una estructura cliente-servidor. Este modelo de comunicaciones se empezó a aplicar y a desarrollar durante los años 80 y hoy en día sigue teniendo una enorme difusión, quizás por ser el que rige las redes TCP/IP. Su funcionamiento es bastante sencillo, ya que a partir de un equipo cliente, se necesita otro equipo servidor para que este realice aquellas funciones que tiene asignadas.

CONCEPTO

Pueden ser equipos diferentes o iguales. Una computadora puede ser cliente y servidor a la misma vez dependiendo del software.

En términos generales, la estructura cliente-servidor consta de los siguientes elementos.

- **Cliente:** es el sistema que precisa de servicios.
- **Servidor:** es el sistema que proporciona servicios.



Cuando nos conectamos a una página web, nuestro navegador ejerce de cliente y efectúa una petición al servidor.



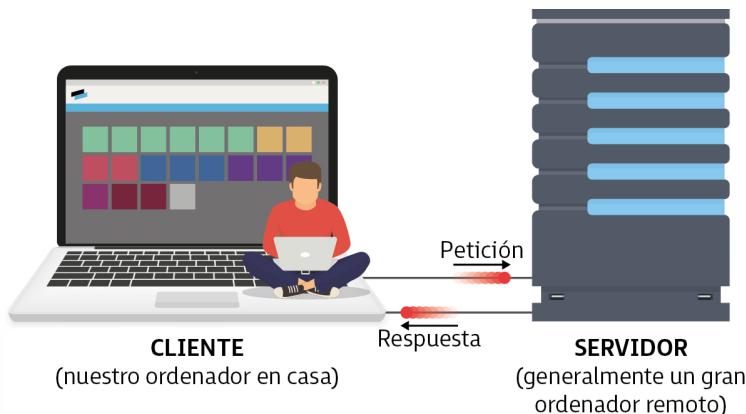
ponte a prueba

¿En una estructura cliente-servidor quién proporciona los servicios?

- a) El cliente.
- b) El servidor.
- c) El segundo equipo cliente del que dispone la estructura.
- d) En este tipo de estructuras no se proporcionan servicios.

Desde el punto de vista lógico, cliente y servidor son elementos separados que establecen su comunicación mediante la red de comunicaciones y colaboran para completar las tareas de forma conjunta. Cuando el cliente precisa de un servicio, realiza una petición y el servidor le da una respuesta. Será este segundo sistema el que reciba y procese la petición y le brinde el servicio requerido.

Un buen ejemplo de la estructura cliente-servidor lo encontramos en el servicio web que empleamos para navegar por internet. Cuando nos conectamos a una página web, nuestro navegador ejerce de cliente y efectúa una petición al servidor.



4.2. PROTOCOLO LDAP

Consideraremos el **LDAP** (*Lightweight Directory Access Protocol*) como un protocolo ligero de acceso a directorios. Se utiliza especialmente en las empresas. Este posee una estructura cliente-servidor y se emplea para acceder a servicios de directorio.

En la práctica, en muchos sentidos podemos considerarlo como una base de datos pensada para almacenar directorios. En dicha base, la información se organiza de manera jerárquica. Cada directorio puede, además, almacenar un amplio abanico de datos.

Las **características y funcionalidades** que nos brinda el protocolo LDAP son muchas. Las más destacables son las siguientes:

- **Acreditación de usuarios:** los usuarios pueden acceder a sus respectivas cuentas desde cualquier equipo en red acreditado mediante LDAP.
- **Búsqueda de datos:** los usuarios también pueden emplear LDAP como si se tratara de una guía virtual que brinda los datos de contacto de otros usuarios de manera sencilla y accesible. De ahí que LDAP se utilice con frecuencia en organizaciones como universidades, administraciones públicas, empresas, etc.

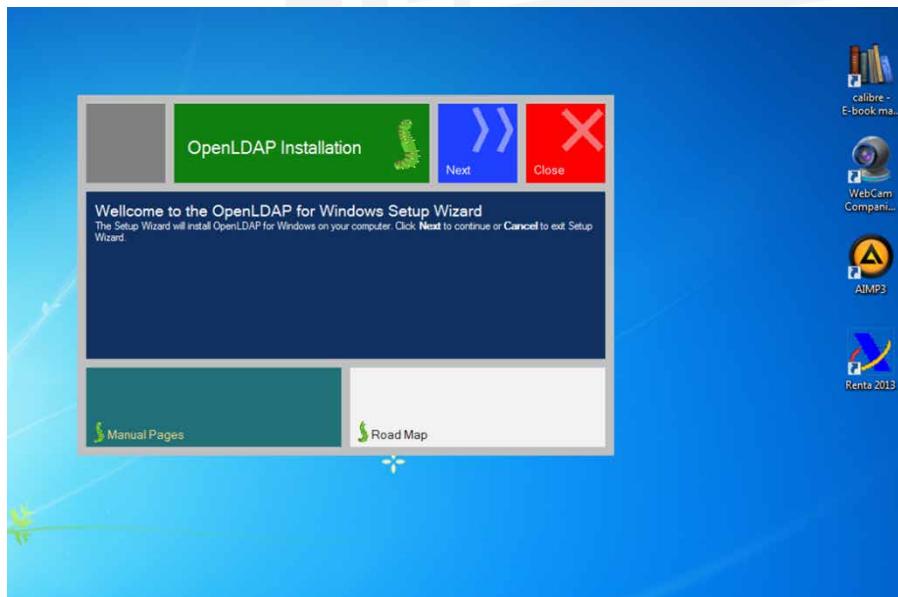
- **Centralización de la administración:** LDAP permite centralizar la gestión de cuentas de usuarios y sus permisos asociados.
- **Posibilidad de replicar la base de datos:** de hecho, una vez hayamos configurado la base de datos LDAP, podemos replicarla. Gracias a eso, se nos brinda la opción de configurar diversos servidores LDAP sincronizados. Cuando la red y cantidad de usuarios crecen rápidamente, la red puede balancear la carga entre varios servidores.

El protocolo LDAP brinda **gran rapidez en lectura y escritura de datos**, incluso cuando se da un gran volumen de accesos simultáneos. En definitiva, cuando uno de los clientes LDAP se conecta al servidor LDAP, el cliente puede consultar o modificar directorios. En el segundo caso, el servidor verifica que el usuario cuenta con los permisos necesarios antes de actualizar la información.

En la distribución Ubuntu de Linux, podemos iniciar la instalación del paquete ***OpenLDAP*** y sus utilidades en el servidor desde la ventana de terminal tecleando lo siguiente:

"sudo apt-get install slapdldap-utils"

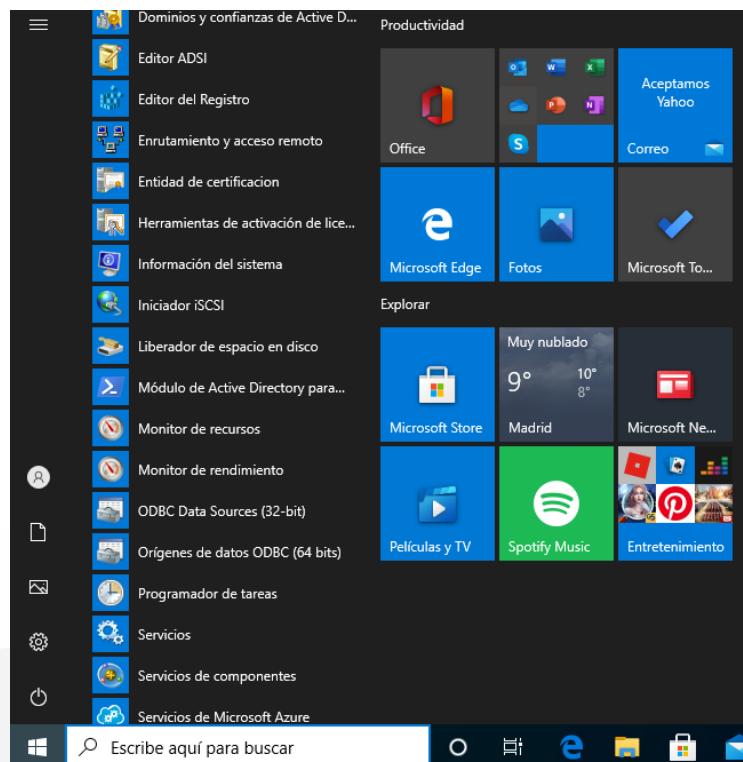
En Windows, para tal fin podemos utilizar *OpenLDAP for Windows* (<http://www.userbooster.de/en/download/openldap-for-windows.aspx>).



El protocolo LDAP se utiliza tanto en servidores Windows como en las diversas distribuciones de Linux.

No obstante, el sistema de Microsoft se refiere a su implementación del servicio de directorio en red como *Active Directory*. Dicho servicio emplea varios protocolos, entre los que se cuentan LDAP.

Así pues, en las versiones más recientes de Windows Server, LDAP se instala por defecto conjuntamente con Active Directory. Si bien en Windows 10 no podemos instalar Active Directory, sí podemos gestionarlo remotamente a través de la red mediante la aplicación *Sitios y servicios de Active Directory*, accesible a través del menú *Inicio*.



ponte a prueba

¿Cuál de las siguientes opciones agrupa las características que nos ofrece el protocolo LDAP?

- a) Acreditación de usuarios, búsqueda de datos, centralización de la información y posibilidad de replicar la base de datos.
- b) Asignación de velocidad de transmisión, búsqueda de datos y mayor protección en transmisión de datos por USB.
- c) Mayor protección en transmisiones de datos por USB, acreditación de usuarios y posibilidad de replicar la base de datos.
- d) Necesita de una memoria RAM superior a 4GB.



4.3. CONCEPTO DE DOMINIO. SUBDOMINIOS. REQUISITOS NECESARIOS PARA MONTAR UN DOMINIO

Cuando hablamos de dominio podemos encontrar dos definiciones muy diferentes, dependiendo de si estamos hablando de redes en sentido general o bien de la red de redes, es decir, de internet.

Veamos la diferencia entre ambas:

- **Dominios en redes:** si hablamos de redes en general, el dominio comprende un determinado grupo de ordenadores que están conectados y que han otorgado a uno de los equipos de dicha red la gestión de los usuarios, sus privilegios de acceso y otros datos.
- **Dominios en internet:** sin embargo, en el ámbito de los sitios de internet, el dominio hace referencia a la parte principal de una determinada dirección web. Por lo general, dicha parte hace referencia a la empresa u organización que gestiona el sitio. Es el nombre que le damos a una página web.

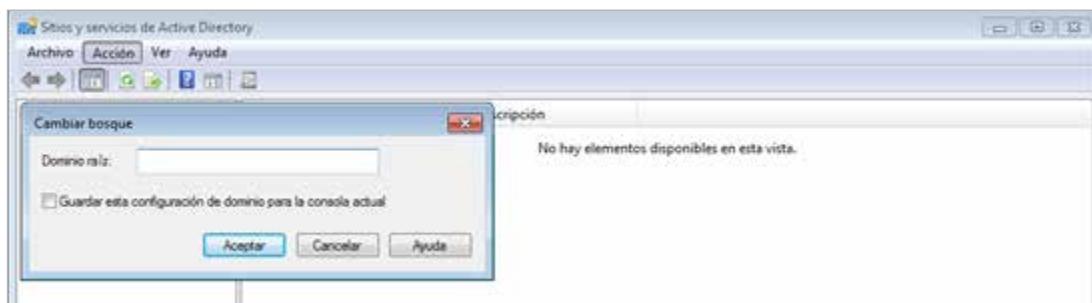
Así, por ejemplo, ilerna.es sería un dominio válido.

The screenshot shows the ILERNA website's homepage. At the top, there's a navigation bar with links for 'Centro de ayuda', 'Campus ILERNA', 'Blog ILERNA', 'Català', and 'Acceder y registrar'. Below the navigation, there's a search bar and a user icon. The main content area features a large image of a person working at a desk with a cup of coffee. Overlaid on this image are four sections for 'FP ONLINE', 'FP LLEIDA', 'FP SEVILLA', and 'FP MADRID', each with a yellow 'Estudia en ILERNA' button. At the bottom left, there's a box containing information about being officially registered with the Ministry of Education and the Community of Madrid.

En internet, los nombres de dominio suelen hacer referencia a la empresa u organización que gestiona el sitio.

Otro concepto con el que debemos estar familiarizados es el de subdominio. Al igual que el dominio, este también puede variar dependiendo de a qué nos refiramos:

- **Subdominios en redes:** en redes, los subdominios son subgrupos o subclasificaciones dentro del dominio. Su creación implica la creación de un dominio de segundo nivel, anidado dentro del dominio primario, que en Active Directory, por ejemplo, se denomina *Bosque*. La nueva estructura está relacionada con la primera, pero cuenta con características propias.



Conexión a un dominio de Active Directory desde Windows 10.

Los subdominios se utilizan sobre todo con fines administrativos o para separar los diversos bloques de una organización.

- **Subdominios en internet:** en internet, el subdominio suele hacer referencia a la parte de la dirección web que antecede al dominio y queda separado de este por un punto. Por lo general, se emplea para compartimentar grandes sitios web en diferentes áreas.

No obstante, podemos usar subdominios para muchos otros fines. Por ejemplo, para hacer pruebas y desarrollar nuevas páginas o aplicaciones. Si trabajamos en un subdominio, mantendremos intacta la estructura básica y nuestro posicionamiento en los motores de búsqueda no se verá afectado.

Así, por ejemplo, campus.ilerna.es sería un subdominio válido.

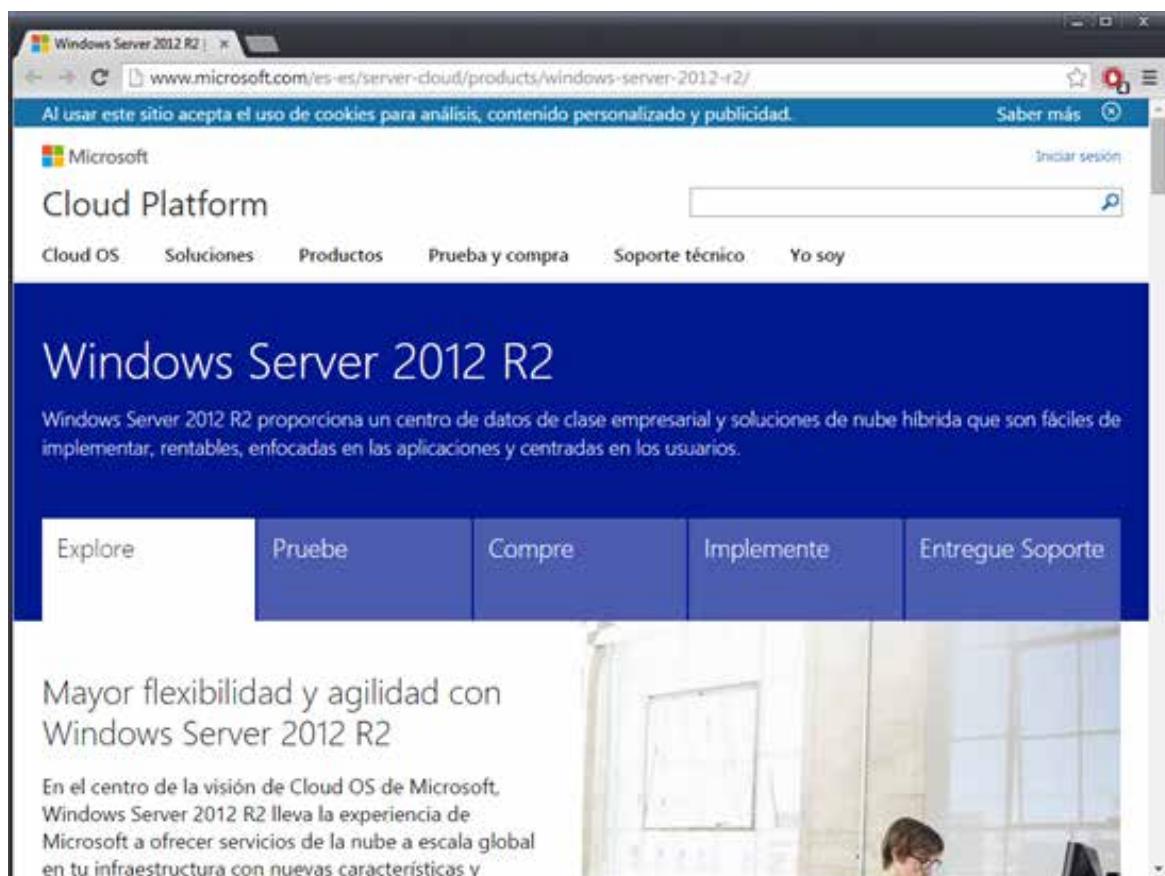


¿Qué necesitamos para crear un dominio? Para dar respuesta a esta cuestión, nuevamente tenemos que remitirnos a la distinción que hemos venido realizando en los anteriores apartados:

Requisitos para la creación de un dominio de red

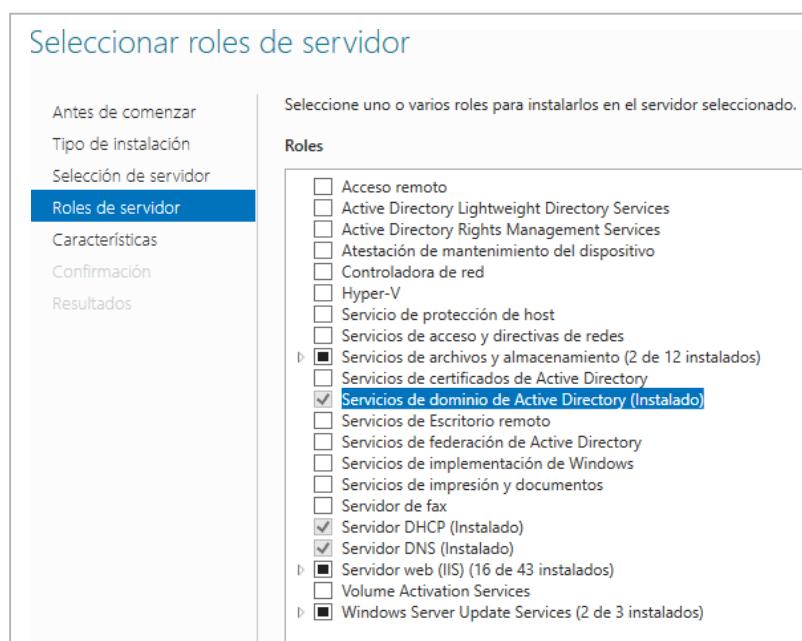
En este caso, el principal requisito es disponer de un sistema operativo orientado a servidor. En régimen propietario, por ejemplo, podemos emplear Windows Server.

Entre las tareas que realiza, cabe destacar la de asignar CPU y memoria a los procesos.



Para configurar el dominio en un servidor Windows actual debemos instalar los roles necesarios para gestionar el dominio de red.

El rol DNS del servidor nos facilita esta tarea, aunque para una correcta instalación de todas sus funcionalidades de forma correcta como Active Directory, debemos instalar los roles de AD/DS (Active DirectoryDomainServices) y DHCP para complementar el funcionamiento del primer rol de dominio. Proporcionaran todas las funcionalidades de control que nos ofrecen los sistemas Windows.

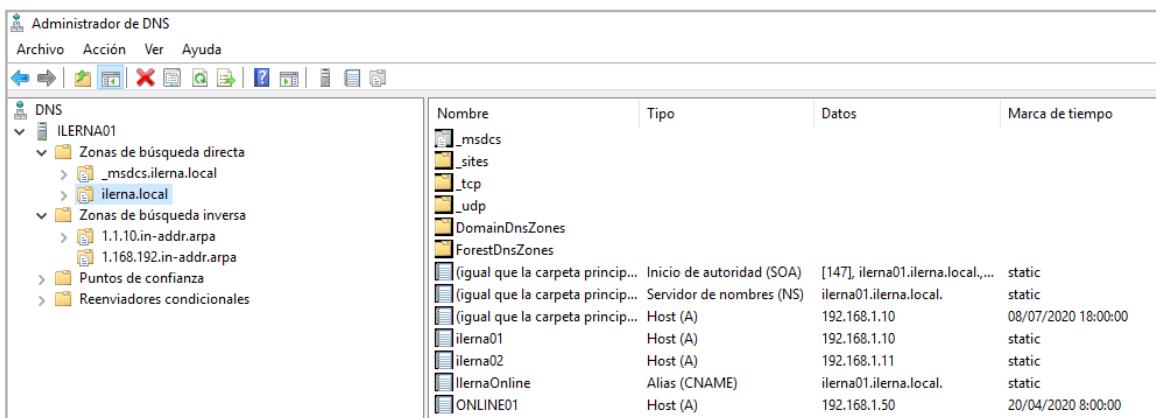


Una vez instalados los roles, debemos configurar toda la infraestructura del dominio.

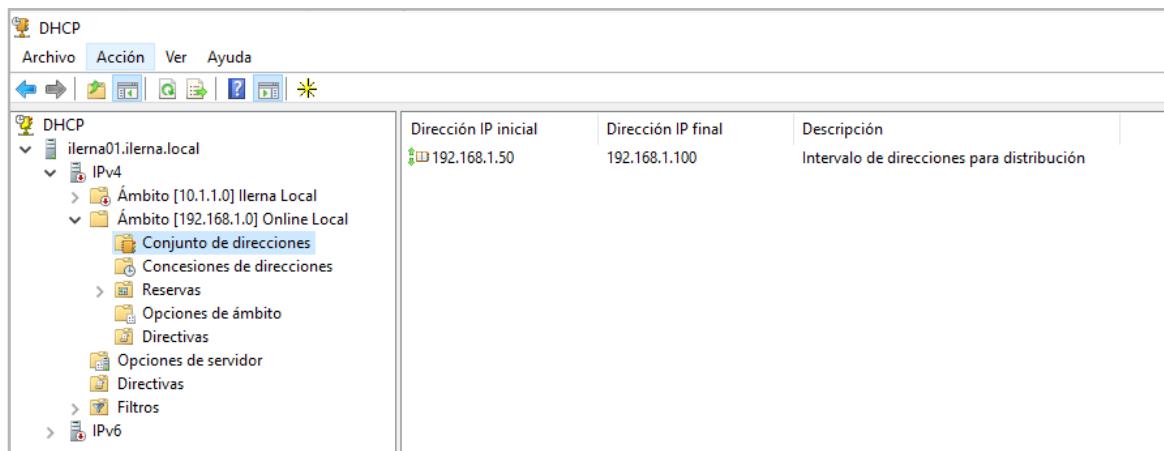
En primer lugar, configuraremos el servicio DNS, estableciendo un servidor principal de domino y un usuario administrador. En este punto hay que tener en cuenta que el servidor y el usuario que utilicemos deben tener los privilegios necesarios, ya que serán los denominados principales del *bosque* (siempre que sea el primero y no una instalación dentro de un dominio ya establecido), los cuales serán relevantes para configuraciones de escalabilidad del servicio, en el caso de que fuese necesario.

Para finalizar la instalación del rol, debemos promover el servidor a controlador de dominio, donde estableceremos características como el nombre del dominio, donde se recomienda poner un nombre que sea concreto y orientativo (Midominio.local).

Para un buen funcionamiento de este, debemos generar las zonas de búsqueda directa e inversa en el servicio DNS.



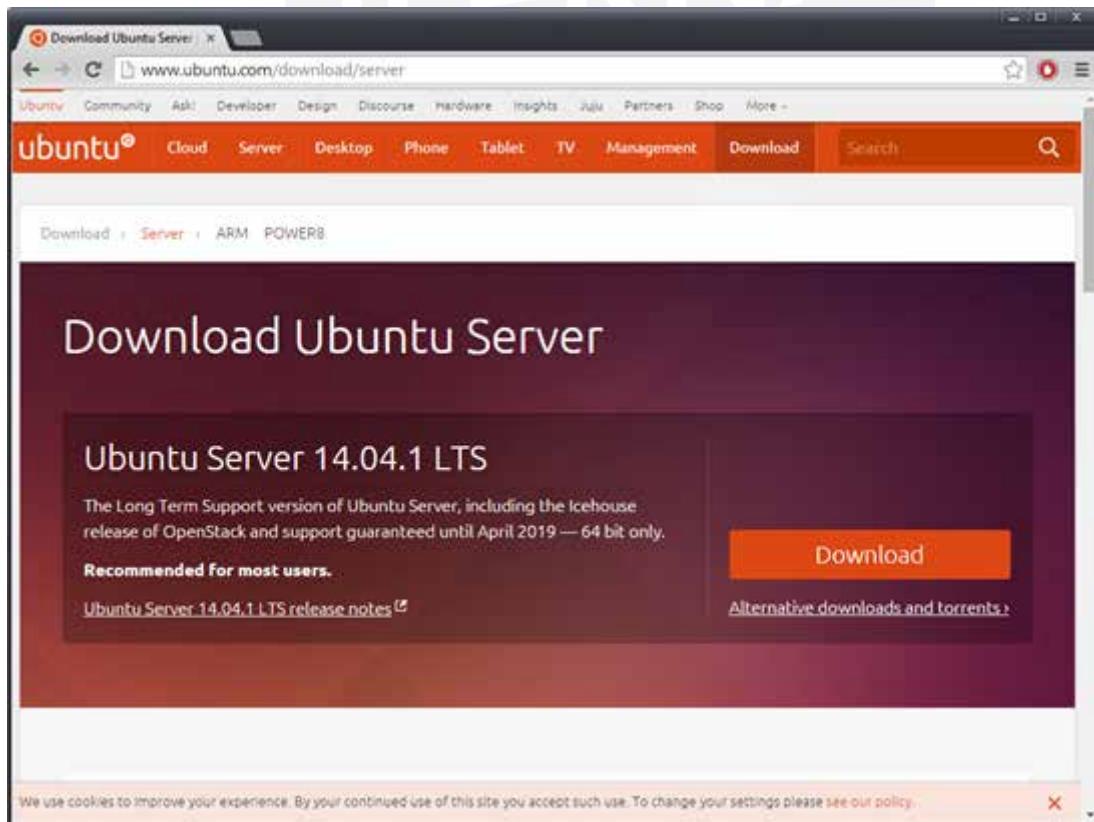
Establecer en el servicio DHCP el rango de IP a proporcionar a los equipos clientes conectados con el servicio DHCP.



En estas configuraciones podemos realizar todas las configuraciones del dominio, como las reservas de direcciones, configuraciones de correo electrónico, etc.

Las configuraciones de usuarios del dominio las veremos más adelante.

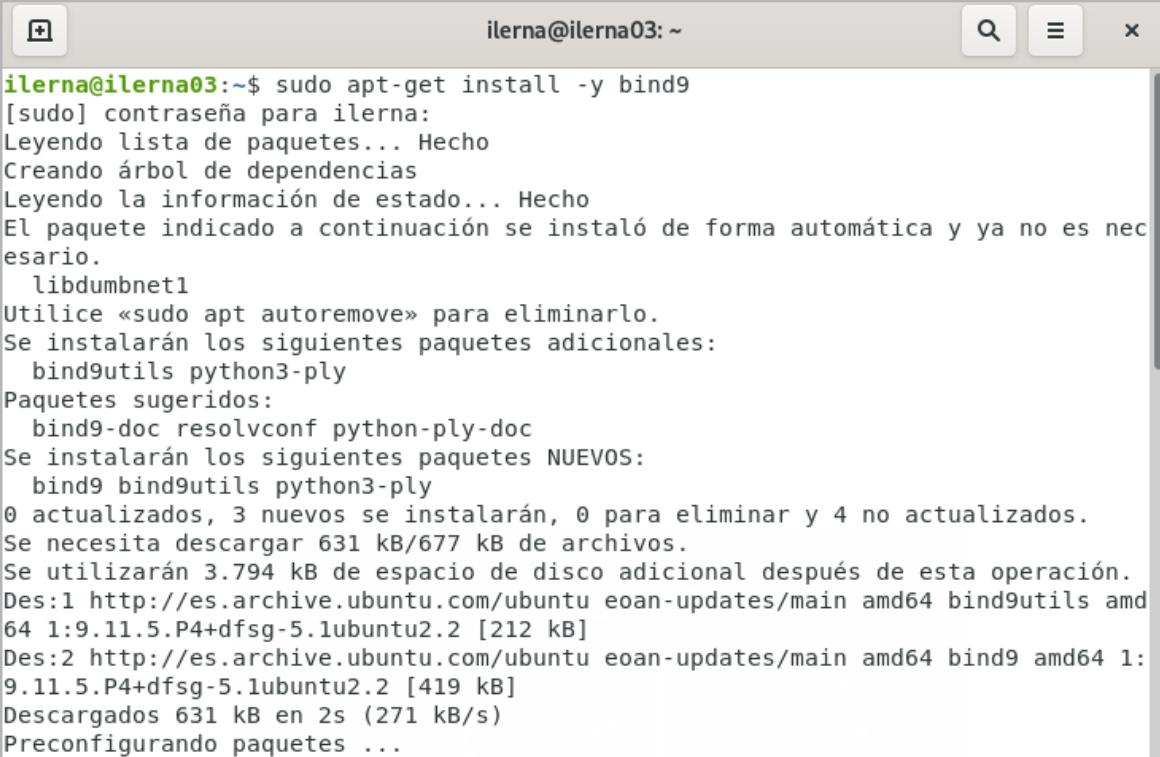
En régimen de software libre, por otra parte, podemos utilizar Ubuntu Server, una distribución de Linux ideada para este fin.



En régimen de software libre podemos utilizar Ubuntu Server para crear un dominio.

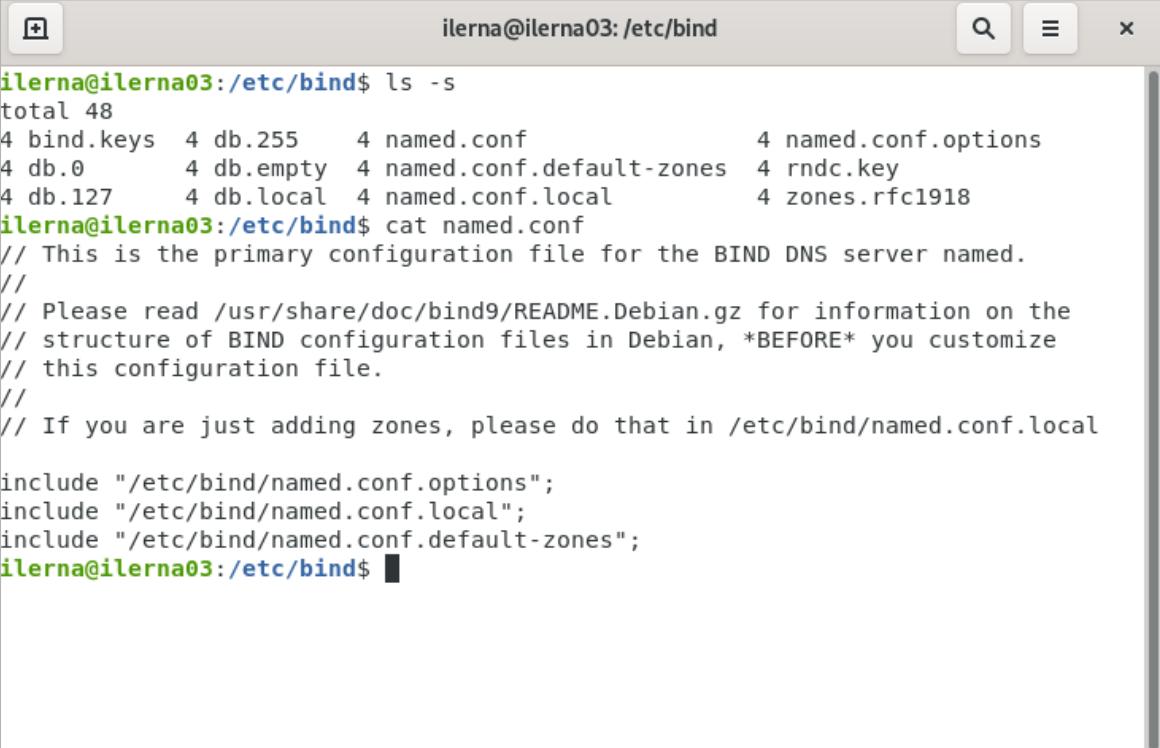
Para crear el dominio en servidor en Ubuntu tenemos que configurar el servidor DNS. Para ello, en primer lugar, debemos instalarlo desde los repositorios tecleando lo siguiente en la consola:

"sudo apt-get install -y bind9"



```
ilerna@ilerna03:~$ sudo apt-get install -y bind9
[sudo] contraseña para ilerna:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  libdumbnet1
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
  bind9utils python3-ply
Paquetes sugeridos:
  bind9-doc resolvconf python-ply-doc
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9utils python3-ply
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 631 kB/677 kB de archivos.
Se utilizarán 3.794 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu eoan-updates/main amd64 bind9utils amd64 1:9.11.5.P4+dfsg-5.lubuntu2.2 [212 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu eoan-updates/main amd64 bind9 amd64 1:9.11.5.P4+dfsg-5.lubuntu2.2 [419 kB]
Descargados 631 kB en 2s (271 kB/s)
Preconfigurando paquetes ...
```

A continuación, entramos en el directorio **/etc/bind/** para editar los archivos de configuración.



```
ilerna@ilerna03:/etc/bind$ ls -s
total 48
4 bind.keys  4 db.255    4 named.conf          4 named.conf.options
4 db.0       4 db.empty   4 named.conf.default-zones 4 rndc.key
4 db.127     4 db.local   4 named.conf.local      4 zones.rfc1918
ilerna@ilerna03:/etc/bind$ cat named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
ilerna@ilerna03:/etc/bind$
```



Al igual que en el caso anterior, debemos configurar todos los parámetros de configuración del servicio. En este caso, dependerá de la distribución de Linux que utilicemos, aunque en este caso no dispondremos del servicio de Active Directory, ya que este es propio de los sistemas Windows.

En este caso las configuraciones se realizaran mediante la modificación de los ficheros "named.conf.options" donde configuraremos las opciones de *bind* y la comunicación entre la red privada.

```
ilerna@ilerna03:/etc/bind$ ls -s
total 48
4 bind.keys 4 db.255 4 named.conf 4 named.conf.options
4 db.0 4 db.empty 4 named.conf.default-zones 4 rndc.key
4 db.127 4 db.local 4 named.conf.local 4 zones.rfc1918
ilerna@ilerna03:/etc/bind$ cat named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

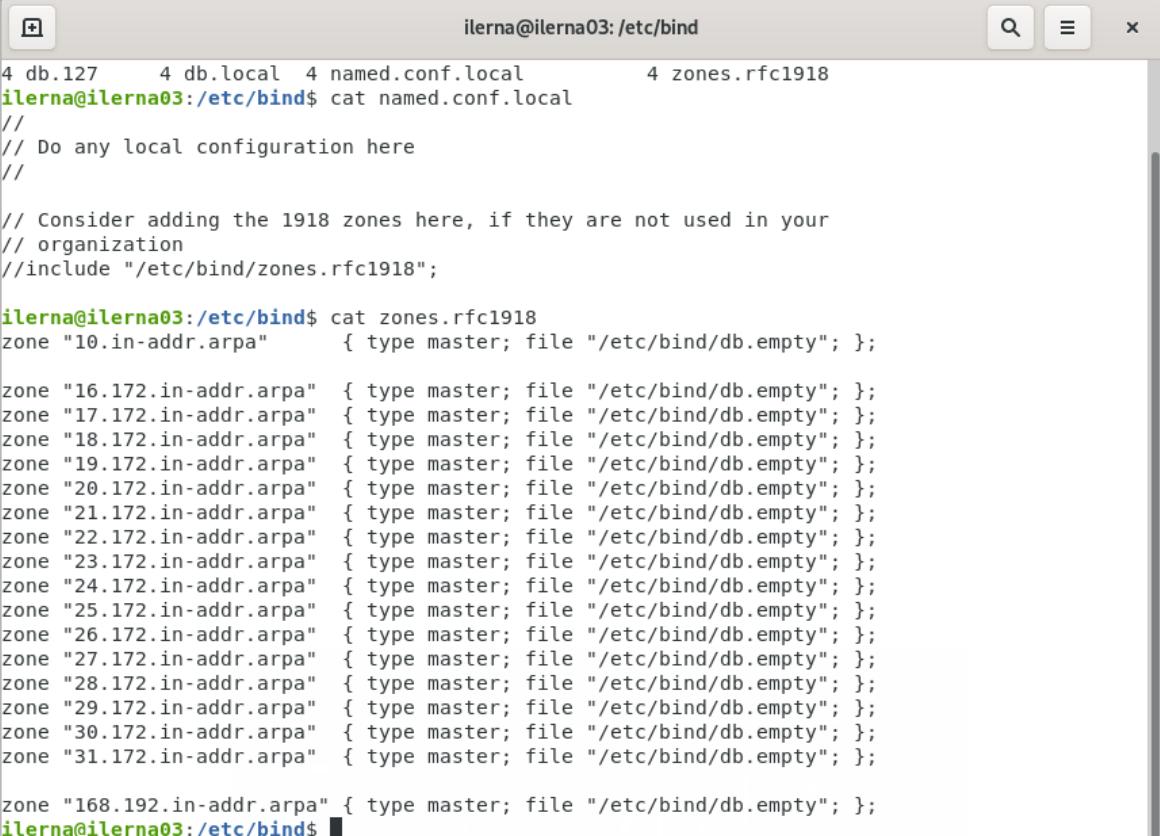
    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };

};

ilerna@ilerna03:/etc/bind$
```

En el fichero “named.conf.local” junto con el fichero “zones.rfc1918” configuraremos las zonas de búsqueda.



```

4 db.127      4 db.local  4 named.conf.local      4 zones.rfc1918
ilerna@ilerna03:/etc/bind$ cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

ilerna@ilerna03:/etc/bind$ cat zones.rfc1918
zone "10.in-addr.arpa"      { type master; file "/etc/bind/db.empty"; };

zone "16.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "17.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "18.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "19.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "20.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "21.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "22.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "23.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "24.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "25.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "26.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "27.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "28.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "29.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "30.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };
zone "31.172.in-addr.arpa"   { type master; file "/etc/bind/db.empty"; };

zone "168.192.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
ilerna@ilerna03:/etc/bind$ █

```

Una vez configurado el servicio encontramos en el directorio “var/cache/bind” los ficheros para configurar las direcciones de los equipos conectados al dominio.

- **Requisitos para la creación de un dominio en internet:** para la creación de un dominio en internet debemos contratar el servicio con una de las muchas empresas que se dedican a este fin. No es infrecuente que alguna de ellas nos ofrezca a la vez un espacio web en el que alojar nuestras páginas online para darles difusión a través de internet.

Entre las empresas que ofrecen este servicio, tenemos, sin ir más lejos, **1 and 1** (www.1and1.es/dominios), **Hostalia** (www.hostalia.com/dominios/) y **ESdominios** (www.esdominios.com/).

La administración del dominio se lleva a cabo de manera remota, a través del navegador web, y para ello no es preciso utilizar un sistema operativo orientado a servidor. La empresa a través de la cual contratemos el servicio nos proporcionará la información necesaria acerca de cómo gestionarlo.



4.4. CONCEPTOS CLAVE DE ACTIVE DIRECTORY

Active Directory es una herramienta de Microsoft para **gestionar servidores y administrar en ellos usuarios, grupos, etc.**. Gracias a esta herramienta podemos gestionar los inicios de sesión de los equipos que están conectados a la red, definir políticas, etc.

Para poder utilizarlo de una forma correcta, debemos familiarizarnos con la terminología que emplea el software.

Estos son los **conceptos clave** que podemos encontrarnos en dicho proceso:

- **Objeto**: genérico que empleamos para referirnos a cualquiera de los componentes que conforman el directorio (usuarios, grupos, impresoras, carpetas compartidas, etc.). Cada objeto puede tener sus características y un nombre que permita identificarlo.
- **Directorio**: Active Directory se basa en el concepto de directorio, que es un repositorio en el que se guarda toda la información referente a usuarios, grupos, recursos, etc.
- **Dominio**: conjunto de objetos dentro del directorio que conforman un subconjunto administrativo. Dentro de un *bosque* puede haber varios dominios. Cada uno de ellos puede tener su propio conjunto de objetos y unidades organizativas.

- **Controlador de dominio:** comprende el conjunto de objetos del directorio para un determinado dominio. Es decir, en un determinado dominio puede haber varios controladores de dominio.
- **Árboles:** los árboles son simplemente conjuntos de dominios que poseen una raíz común. Están organizados jerárquicamente y su jerarquía se refleja en los nombres. Así, por ejemplo, los dominios *todo.es* y *parte.todo.es* forman parte del mismo árbol. Por el contrario, *otraparte.es* no forma parte de dicho árbol.
- **Bosque:** el bosque abarca todos los dominios dentro de su ámbito, que por otra parte están interconectados por lo que se denomina *Relaciones de confianza*. En definitiva, todos los dominios de un bosque confían automáticamente entre sí, y los distintos árboles pueden compartir recursos entre sí. Un bosque contiene siempre al menos un dominio, que ejerce de raíz del bosque.
- **Unidades organizativas:** contenedores de objetos que permiten organizarlos jerárquicamente en subgrupos dentro del dominio. Gracias a ellas podemos definir estructuras lógicas que faciliten la organización y hagan que la administración sea más sencilla.
- **Relaciones de confianza:** son un método de comunicación entre dominios, árboles y bosques que rige la seguridad de la red. Gracias a ello, los usuarios de Active Directory pueden autenticarse en otro dominio del directorio.

Las relaciones de confianza pueden ser de diversos tipos. Veamos las más comunes:

- **Unidireccionales:** funcionan en una única dirección.
- **Bidireccionales:** funcionan en ambas direcciones.
- **Transitivas:** en ellas la confianza se propaga, por ejemplo, si *Uno* confía en *Dos* y *Dos* confía en *Tres*, de ello se desprende que *Uno* confía en *Tres*.
- **Delegación de control entre dominios:** permite a los usuarios de un dominio administrar recursos de otro dominio. Es necesario que entre los dos dominios se haya establecido una relación de confianza. La delegación de control la realizaremos solamente a usuarios en los que confiemos plenamente.

En Active Directory podemos establecer distintos tipos de grupos. Estos se emplean para reunir a usuarios, equipos y otros tipos de cuenta en entidades administrables.

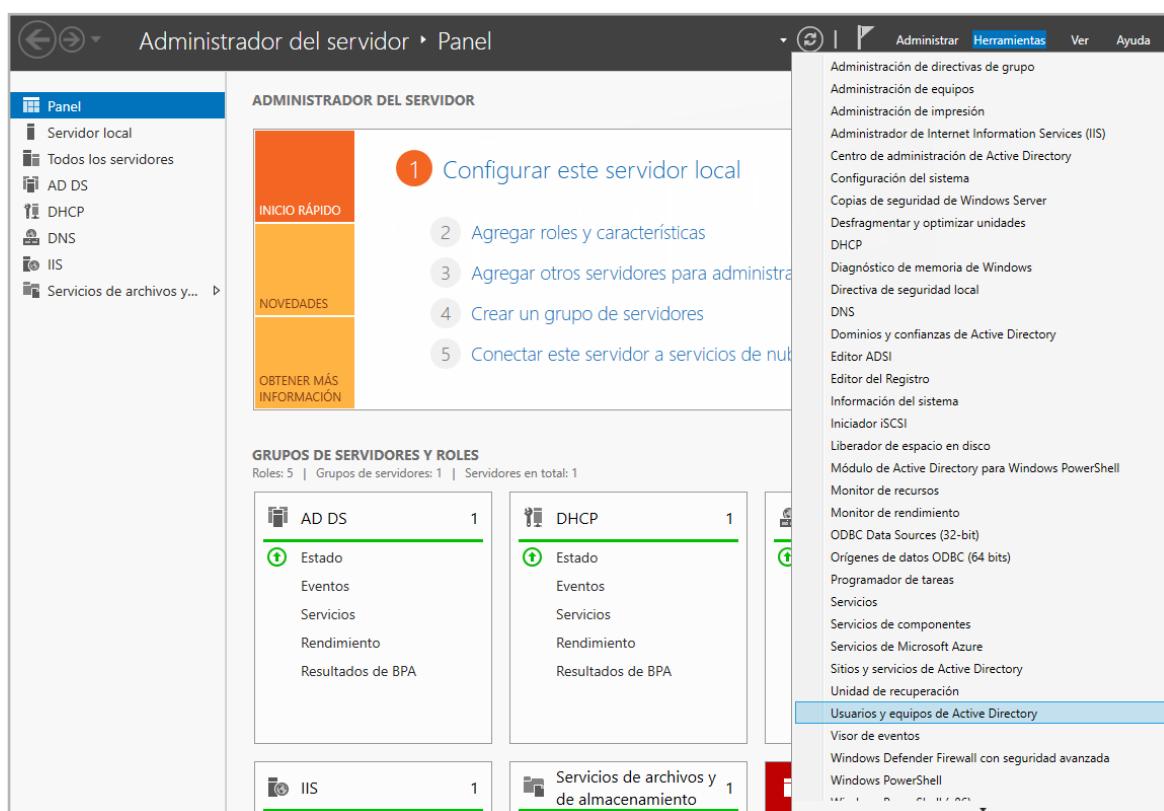
En los siguientes puntos veremos más en detalle las opciones que nos ofrecen las cuentas de usuarios y los grupos.

4.5. ADMINISTRACIÓN DE CUENTAS. CUENTAS PREDETERMINADAS

Generalmente, tras crear el directorio en aplicaciones como Active Directory, nos interesará generar cuentas de usuario para asignarlas a las distintas personas que van a acceder a la red.

A nivel interno, las cuentas de usuario son elementos de una base de datos de directorio a los que se les asigna de manera automatizada unos identificadores para garantizar la seguridad. Tras dar de alta a los usuarios, estos pueden acceder y utilizar los recursos del dominio que tengan asignados.

En Windows podemos gestionar las cuentas entrando en *Server Manager* y posteriormente en *Local Server*. Las acciones de agregar y eliminar usuarios se llevan a cabo desde el apartado *Active DirectoryUsers and Computers*.



Esta herramienta del sistema nos permitirá gestionar los usuarios y grupos del dominio de una forma muy similar a la que encontramos en las versiones cliente de Windows.

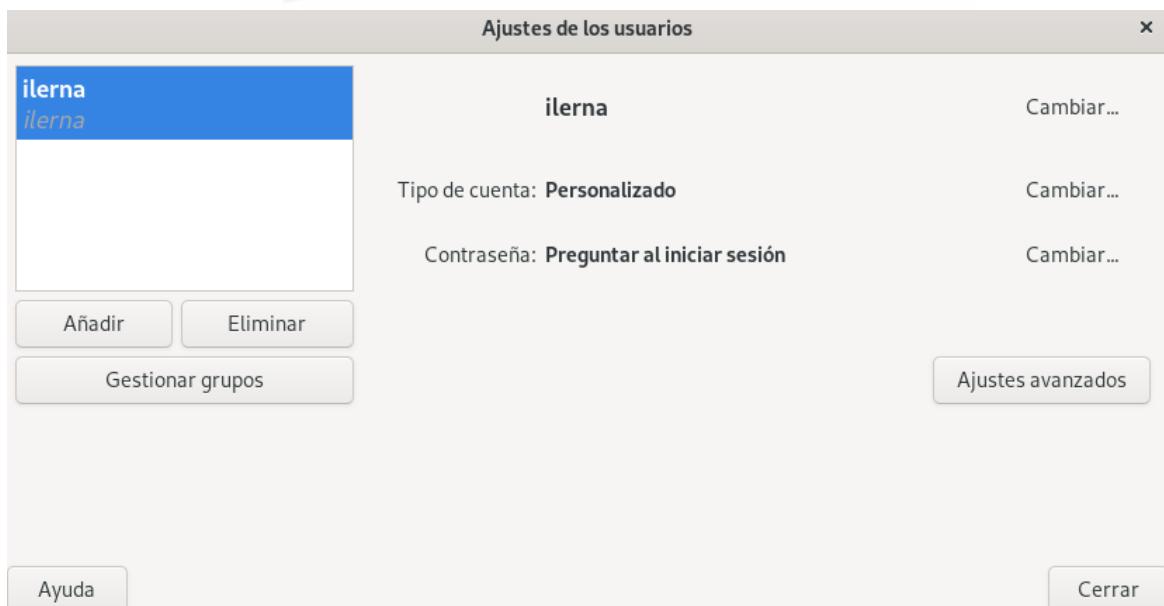
Desde esta misma herramienta de Active Directory también podremos gestionar los equipos enlazados al dominio u otros servidores que gestionen la red, con el objetivo de tener un mayor control sobre las conexiones en dominio.

Usuarios y equipos de Active Directory			
Nombre	Tipo	Descripción	
Administrador	Usuario	Cuenta integrada para la administración del equipo o dominio	
Administradores clave	Grupo de seguridad - Global	Los miembros de este grupo pueden realizar operaciones administrativas en el sistema o dominio.	
Administradores clave de la organización	Grupo de seguridad - Universal	Los miembros de este grupo pueden realizar operaciones administrativas en todos los sistemas y dominios de la organización.	
Administradores de DHCP	Grupo de seguridad - Local	Miembros que tienen acceso administrativo al servicio DHCP.	
Administradores de empresas	Grupo de seguridad - Universal	Administradores designados de la empresa.	
Administradores de esquema	Grupo de seguridad - Universal	Administradores designados del esquema.	
Admins. del dominio	Grupo de seguridad - Global	Administradores designados del dominio.	
Controladores de dominio	Grupo de seguridad - Global	Todos los controladores de dominio del dominio.	
Controladores de dominio clonables	Grupo de seguridad - Global	Se pueden clonar los miembros del grupo que sean controladores de dominio.	
Controladores de dominio de sólo lectura	Grupo de seguridad - Global	Los miembros de este grupo son controladores de dominio de sólo lectura.	
DnsAdmins	Grupo de seguridad - Dominio local	Grupos de administradores de DNS.	
DnsUpdateProxy	Grupo de seguridad - Global	Cuentas DNS que tienen permiso para efectuar actualizaciones directas en el sistema.	
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de este grupo son controladores de dominio de sólo lectura.	
Equipos del dominio	Grupo de seguridad - Global	Todas las servidores y estaciones de trabajo unidos al dominio.	
Grupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local	Los miembros de este grupo no pueden replicar las contraseñas a otros dominios.	
Grupo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden replicar las contraseñas a otros dominios.	
Invitado	Usuario	Cuenta integrada para el acceso como invitado al equipo o dominio.	
Invitados del dominio	Grupo de seguridad - Global	Todos los invitados del dominio.	
Propietarios del creador de directivas de grupo	Grupo de seguridad - Global	Los miembros de este grupo pueden modificar la directiva de grupo.	
Protected Users	Grupo de seguridad - Global	Los miembros de este grupo tienen protecciones adicionales frente a cambios en la configuración.	
Publicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden publicar certificados en el dominio.	
Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden obtener propiedades de acceso.	
Usuarios de DHCP	Grupo de seguridad - Dominio local	Miembros que tienen acceso de solo vista al servicio DHCP.	
Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios del dominio.	

Los servidores Linux habitualmente son utilizados en modo texto, ya que de este modo aliviamos al sistema de la carga de la interfaz gráfica.

Veamos los comandos más básicos que se emplean en servidores Linux para agregar o eliminar usuarios:

- **sudo adduser usuario**: crea una cuenta de usuario.
- **sudo deluser usuario**: elimina una cuenta de usuario.



Cabe destacar que podemos instalar diferentes interfaces gráficas en servidores Linux y cada una de ellas puede tener unas opciones diferentes de gestión.

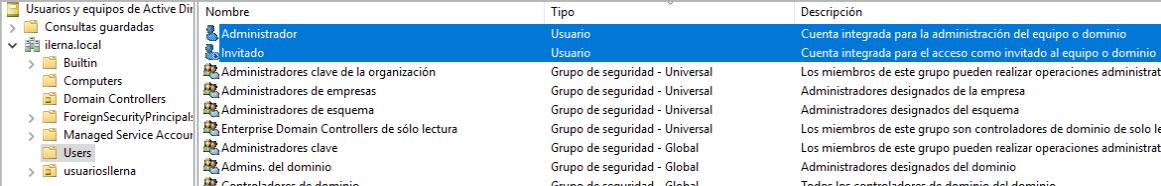
```
ilerna@ilerna03:~$ sudo adduser usuario
[sudo] contraseña para ilerna:
Añadiendo el usuario `usuario' ...
Añadiendo el nuevo grupo `usuario' (1001) ...
Añadiendo el nuevo usuario `usuario' (1001) con grupo `usuario' ...
Creando el directorio personal `/home/usuario' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para usuario
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []: usuario
    Número de habitación []: 1
    Teléfono del trabajo []: 1111111111
    Teléfono de casa []: 1111111111
    Otro []: 111111
¿Es correcta la información? [S/n] s
ilerna@ilerna03:~$
```

En cualquiera de los casos, al instalar el sistema operativo se generan unas cuentas predeterminadas al crear el dominio.

En el listado de usuarios del *Centro de administración* de Active Directory de Windows Server, por ejemplo, encontramos tres cuentas predeterminadas:

- **Administrador**
- **Invitado**
- **Asistente de ayuda**

Como es lógico, cada una de las cuentas tiene asignada una combinación distinta de privilegios y permisos. Recorremos que el Administrador es quien cuenta con plenos derechos en el dominio. La cuenta de *Invitado*, por otra parte, tiene derechos y permisos muy limitados.



Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la administración del equipo o dominio
Invitado	Usuario	Cuenta integrada para el acceso como invitado al equipo o dominio
Administradores clave de la organización	Grupo de seguridad - Universal	Los miembros de este grupo pueden realizar operaciones administrativas en el dominio
Administradores de empresas	Grupo de seguridad - Universal	Administradores designados de la empresa
Administradores de esquema	Grupo de seguridad - Universal	Administradores designados del esquema
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de este grupo son controladores de dominio de solo lectura
Administradores clave	Grupo de seguridad - Global	Los miembros de este grupo pueden realizar operaciones administrativas en el dominio
Admins. del dominio	Grupo de seguridad - Global	Administradores designados del dominio
Controladores de dominio	Grupo de seguridad - Global	Todos los controladores de dominio del dominio

Al igual que sucede en Windows 10, la cuenta de Administrador de dominio en Windows Server tendrá plenos privilegios.

Hay que tener en cuenta que la instalación de los servicios de red como los de dominio crea grupos de usuarios por defecto y se les asigna un usuario administrador del dominio, el cual tendrá los privilegios de este tipo de usuario en todo el dominio.

Nombre	Tipo	Tipo de DC	Sitio	Descripción
ILERNA01	Equipo	GC	Default-First-Site	

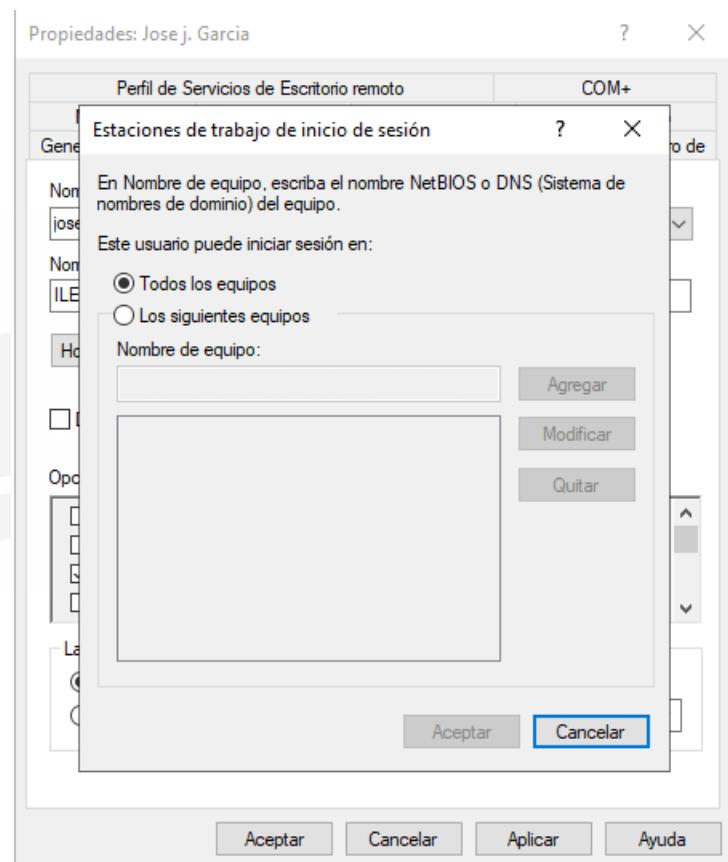
Las cuentas de usuarios del dominio suelen estar vinculadas a ciertos equipos para mejorar el rendimiento de la red, aunque con ellas podemos acceder a cualquier equipo que esté conectado al dominio, teniendo siempre los permisos necesarios.



ponte a prueba

En servicios de administración de usuarios como Active Directory de Windows, podemos generar diferentes usuarios para un dominio y asignarles diferentes permisos y roles de usuarios para obtener un mayor control dentro de la red.

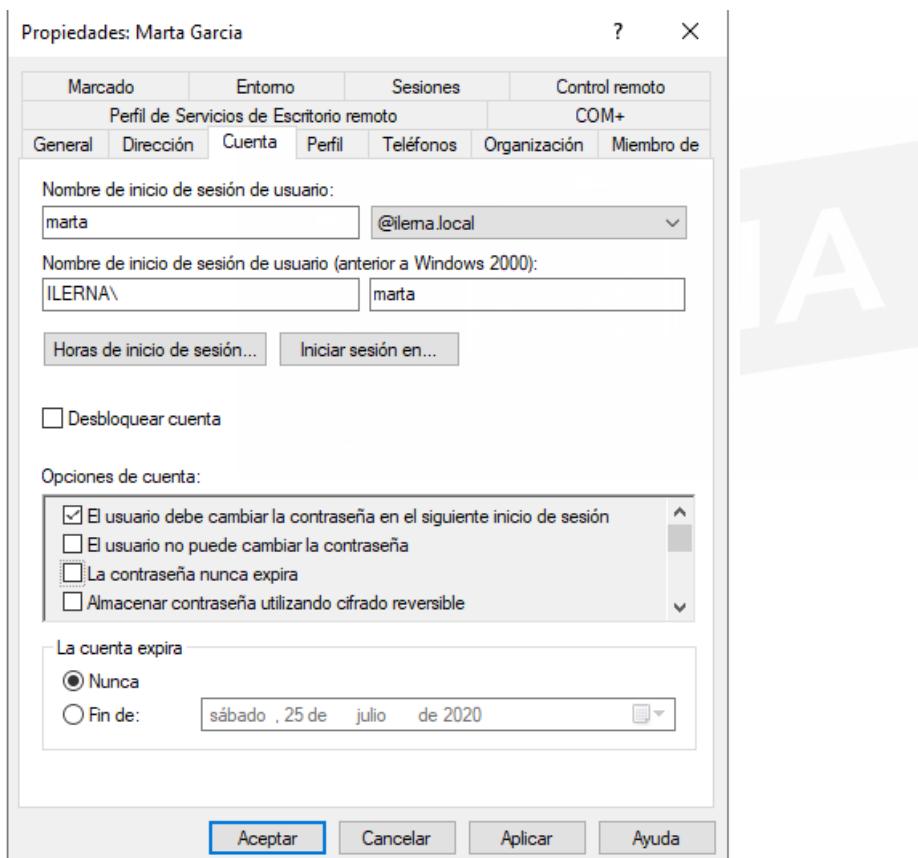
- a) Verdadero
- b) Falso



4.6. CONTRASEÑAS. BLOQUEOS DE CUENTA. CUENTAS DE USUARIOS Y EQUIPOS

Como hemos visto anteriormente, a los distintos usuarios dados de alta en el dominio se les asignarán distintos privilegios. Por lo que es de vital importancia que les asignemos contraseñas seguras.

A la hora de ponerlo en práctica, servicios como Active Directory son los que se encargan de autenticar la identidad de los usuarios. Así, cada vez que una de las personas que usa la red inicia sesión en el dominio, se comprueban sus credenciales en el directorio. Todas ellas deben tener su propio nombre de usuario y su propia contraseña. Si varios usuarios comparten una misma cuenta comprometeremos la seguridad.



El Administrador y el resto de los usuarios inscritos en el dominio deberán introducir su contraseña para poder hacer uso de los privilegios que tienen asignados.

Tras solicitar el acceso a los recursos del dominio mediante la introducción de los datos, los usuarios pueden acceder a ellos si estos son correctos. En caso contrario, se les deniega el acceso.



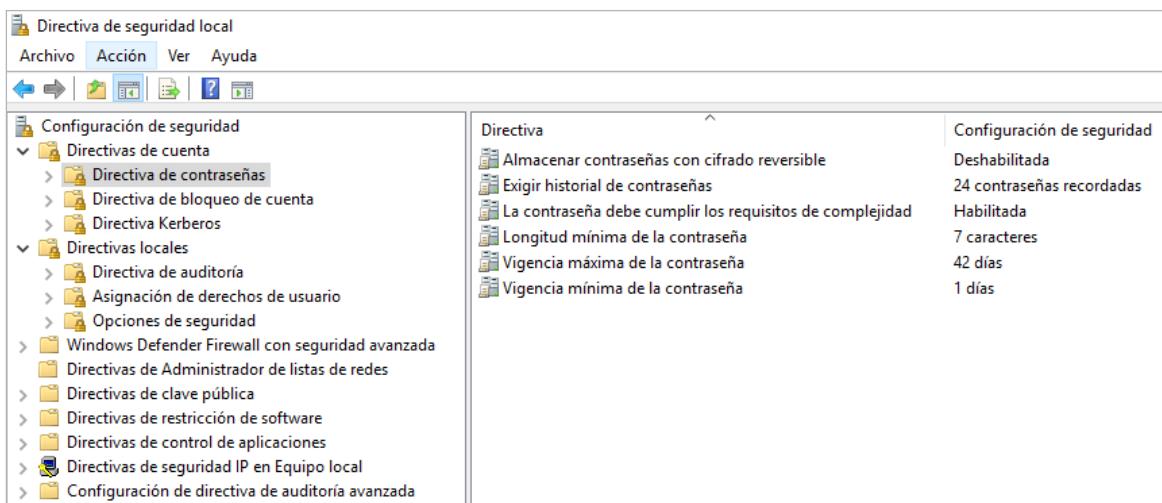
Para impedir que usuarios no autorizados realicen infinitos intentos de entrar introduciendo infinitos nombres de usuario y contraseñas, podemos definir una serie de parámetros que la bloquearán después de que se cumpla una determinada condición.

En **Active Directory**, por ejemplo, podemos definir un parámetro etiquetado como *Umbral de bloqueos de cuenta*. Si por ejemplo lo definimos como tres intentos de inicio de sesión incorrectos, la cuenta quedará inaccesible.

Mediante otros parámetros, como *Duración de bloqueos de cuenta* o *Restablecer la cuenta de bloqueos después de*, podemos restaurar la cuenta pasado un intervalo de tiempo.

Asimismo, los bloqueos de cuenta pueden ir en función, no solo del inicio de sesión con datos incorrectos, sino también de otros parámetros. Así, podemos definir bloqueos de cuentas si un usuario mantiene su sesión iniciada durante demasiado tiempo, etc.

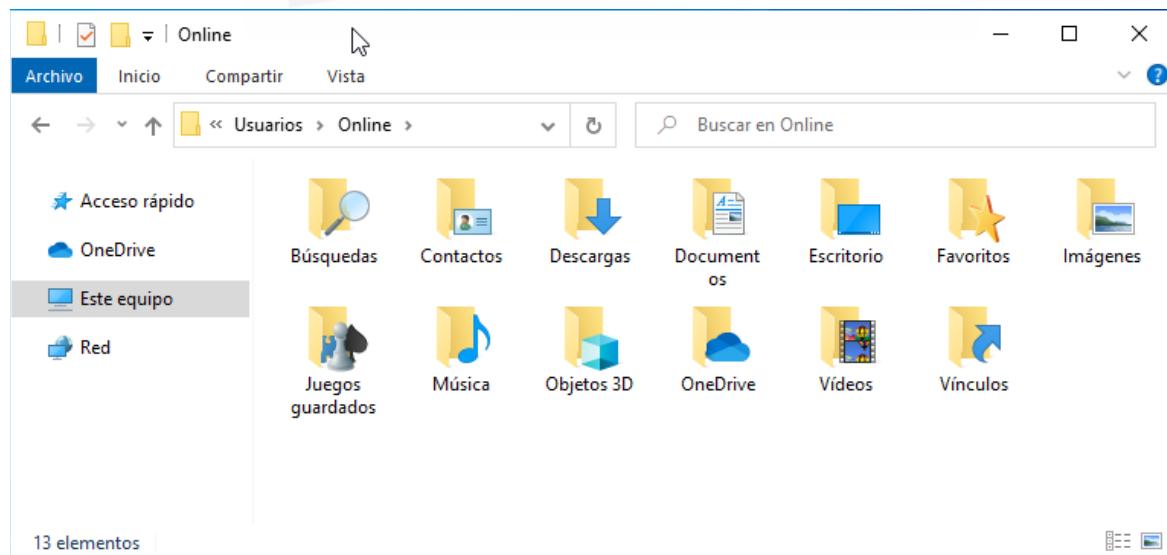
Para definir los bloqueos en Active Directory, entramos en *Configuración de seguridad local* y, posteriormente, hacemos clic en *Directiva de bloqueo de cuentas*.



4.7. PERFILES MÓVILES Y OBLIGATORIOS

Como hemos visto con anterioridad, los perfiles de usuario nos permiten asignar a los usuarios del sistema características como los archivos y carpetas que utilizarán y la configuración de su escritorio. Toda esta información se lee y se carga cada vez que un usuario inicia sesión.

Por defecto, los perfiles suelen ser locales. Esto comporta que el perfil se generará en el equipo en el cual el usuario inicia sesión. En Windows 10, por ejemplo, la ubicación de los ficheros será **C:\Usuarios\Nombre_de_usuario**.



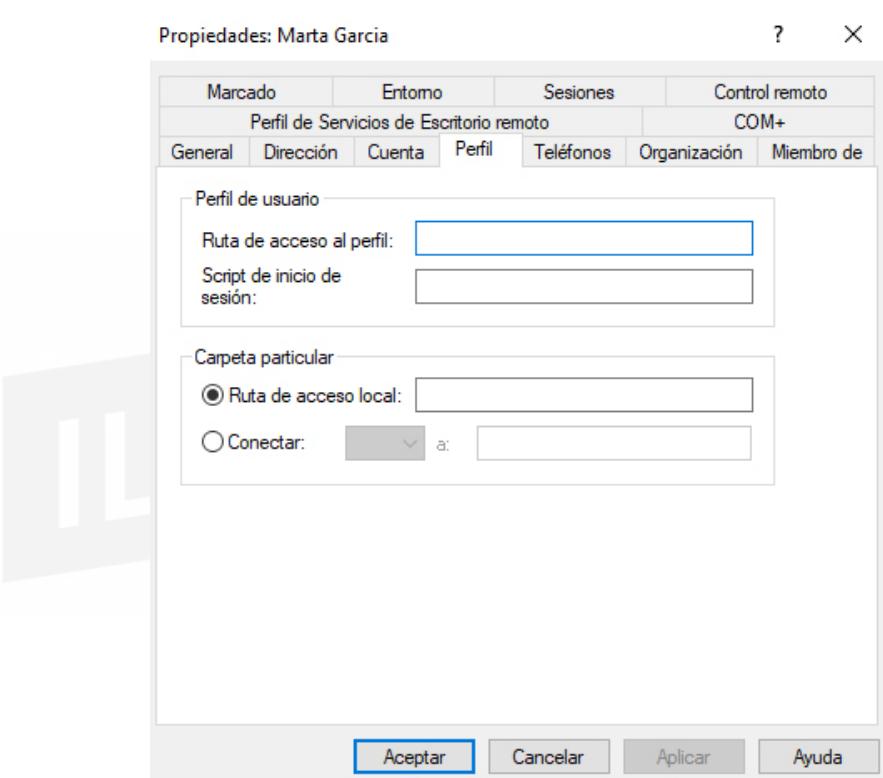
Perfil de un usuario en Windows 10.

Sin embargo, tenemos la posibilidad de crear lo que se denominan perfiles móviles. En definitiva, se trata de que el usuario tenga siempre acceso a su perfil, independientemente del equipo desde el que inicie sesión. Así, aunque

no se encuentre en su ordenador habitual, no tiene que configurar aplicaciones, dispondrá de sus documentos, etc.

La creación de un perfil móvil puede realizarla el administrador o un usuario con privilegios. Estos lo definirán en un directorio del servidor, de modo que quede compartido en red. Lo harán a través del apartado **Usuarios y equipos** de **Active Directory**.

Así, tras entrar como **administrador** en este apartado, hacemos clic con el botón derecho del ratón en la cuenta de usuario y, a continuación, pulsamos en **Propiedades**. En **Perfil** buscamos el parámetro **Ruta de acceso al perfil** y escribimos la información relativa a la ubicación de la información.



Los perfiles obligatorios se definen por el hecho de ser de solo lectura y únicamente pueden ser modificados por un administrador. En definitiva, cuando el usuario inicie sesión se cargará su perfil, pero en ningún caso se guardará ninguna configuración o dato cuando este cierre sesión.

En caso de que queramos que el perfil móvil sea obligatorio, al introducir la información correspondiente a la ruta de acceso en el perfil, le agregamos la extensión **.man**. Para convertir un perfil móvil en un perfil obligatorio accedemos al archivo **ntuser.dat**, donde se almacena la información referente al perfil, y le cambiamos la extensión por **ntuser.man**.

4.8. CARPETAS PERSONALES

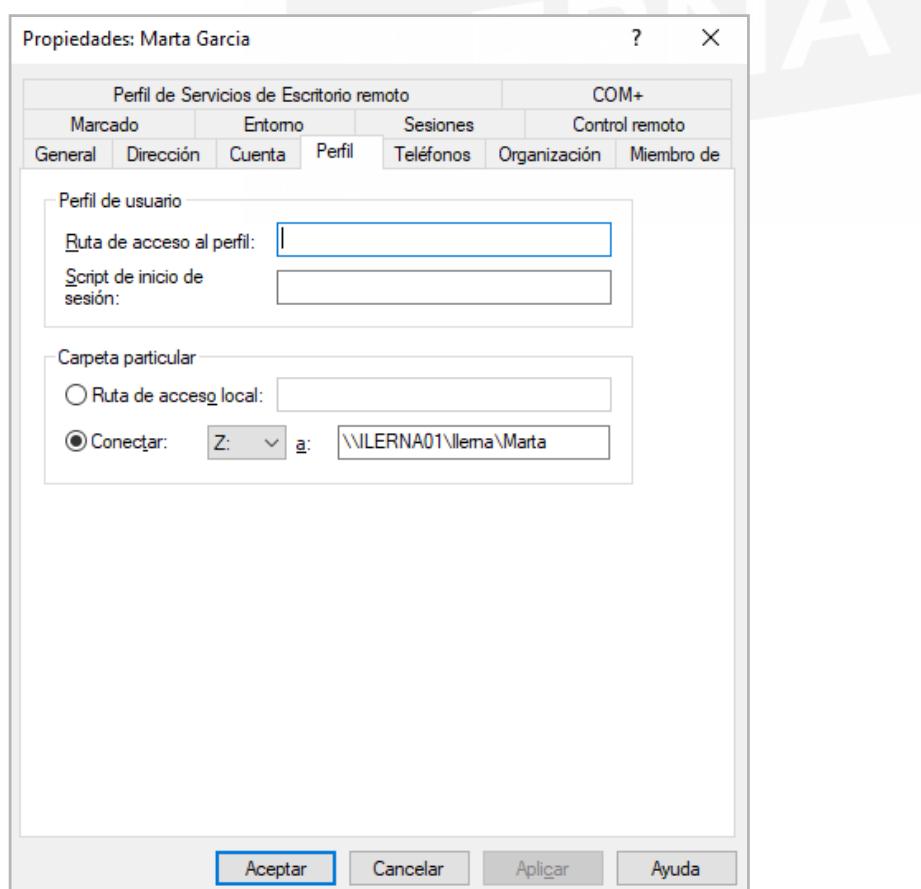
Una vez que ya hemos puesto en marcha nuestro dominio en red, se nos ofrece la posibilidad de crear en el servidor un directorio general en el que cada usuario puede almacenar su información personal en una subcarpeta propia.

Así, cada usuario va a disponer de una subcarpeta de trabajo que, a menudo, tendrá el nombre del propio usuario. También es frecuente que el espacio compartido en el servidor, que no es más que una carpeta, aparezca en los equipos cliente como una unidad de red.

Para asignar dichas carpetas personales en Windows Server necesitamos la herramienta **Usuarios y equipos** de Active Directory.

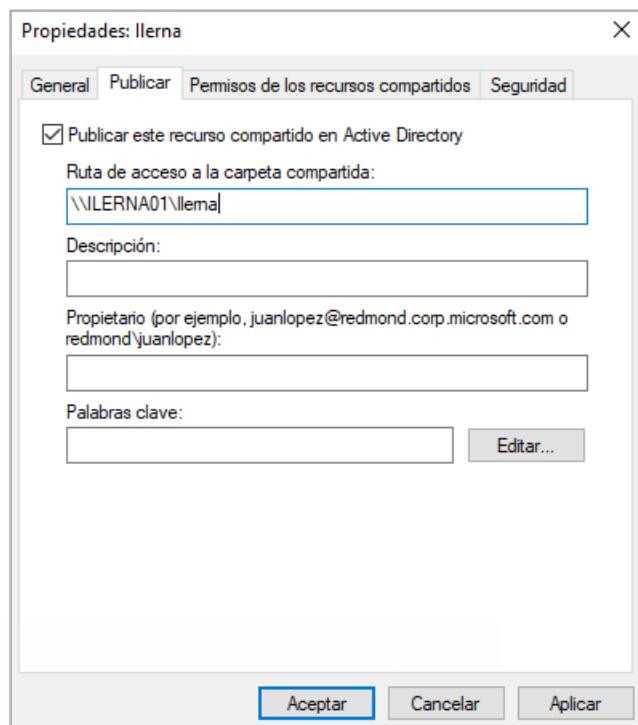
En el *Perfil* de los usuarios, activamos la opción **Carpeta particular**. Una vez hecho esto, elegimos la carpeta.

Si queremos que el usuario vea el área de almacenamiento compartido que se le ha asignado en el servidor como una unidad de almacenamiento en su árbol de directorios local, hacemos clic en **Conectar** y seleccionamos una letra de unidad, por ejemplo “Z:”.

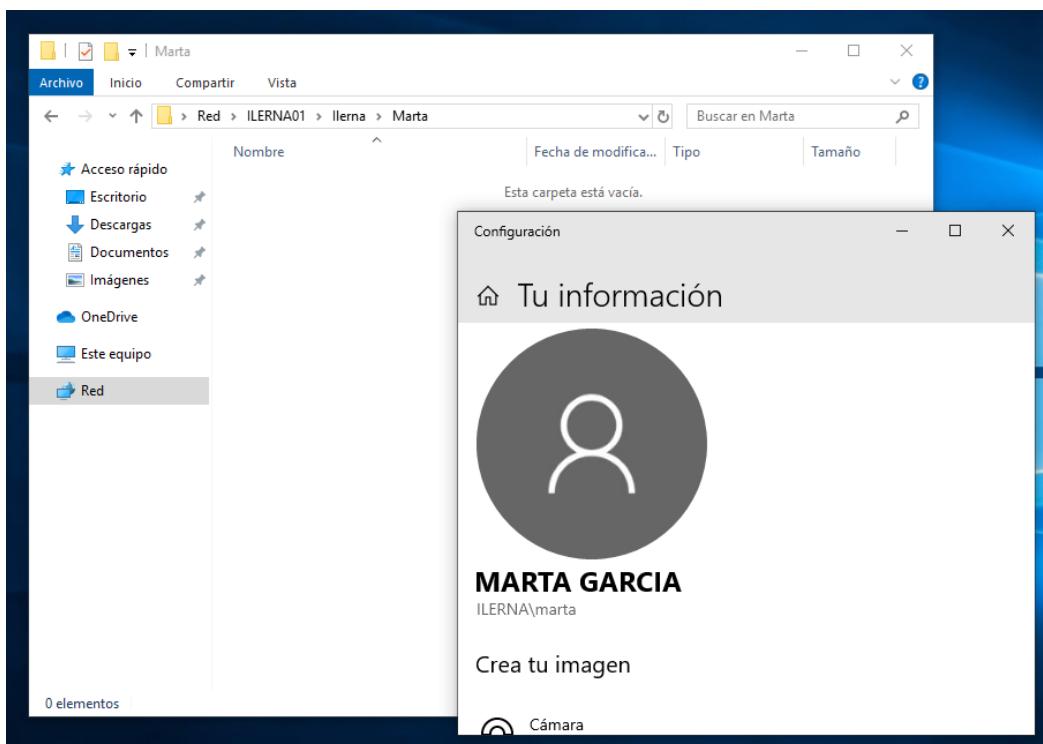


Subcarpetas de usuario en la carpeta “Users” de Windows 10.

Hay que tener en cuenta que los directorios que indiquemos para los usuarios del dominio tienen que ser recursos compartidos del servidor.



Estos directorios serán visibles para los usuarios que indiquemos, aunque estos se podrían asignar directamente a grupos de usuarios para agilizar el proceso. No obstante, hay que definir muy bien los permisos que damos a cada usuario para acceder a los recursos compartidos, ya que, por defecto vienen con control total.





4.9. PLANTILLAS DE USUARIO. VARIABLES DE ENTORNO

Las plantillas de usuario se utilizan para ahorrarnos una gran cantidad de trabajo. Nos permiten, en resumen, **definir una serie de características comunes que posteriormente podemos aplicar a un gran número de usuarios**. Imaginemos, por ejemplo, que queremos definirlas para todos los usuarios del departamento de marketing.

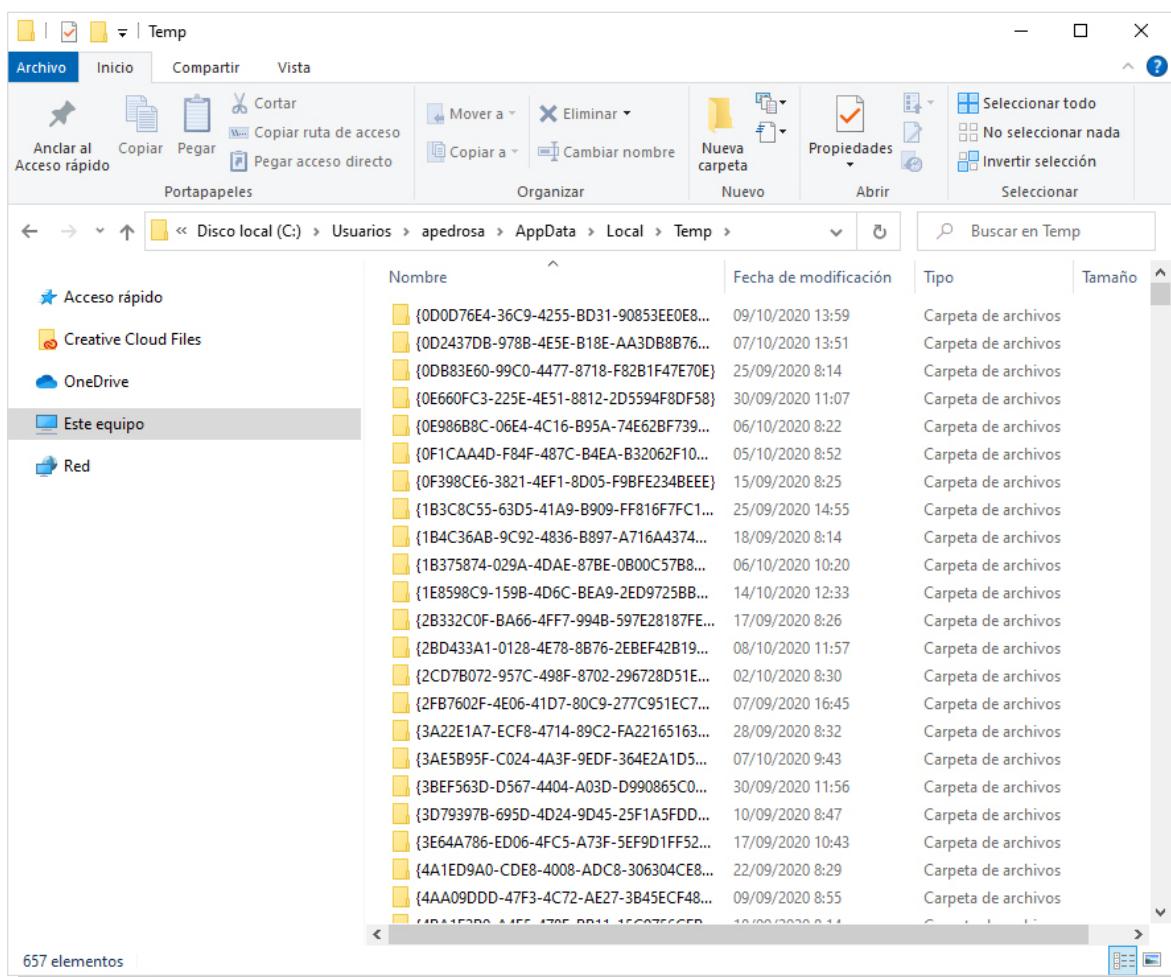
En este caso, creamos una plantilla de usuario etiquetada como *Marketing*, rellenamos sus datos y luego la aplicamos a todos los usuarios de dicho departamento.

Como de costumbre, para completar esta tarea en Windows Server usamos la herramienta *Usuarios y equipos de Active Directory*. Tras crear un nuevo usuario, nos cercioramos de marcar la casilla que desactiva la cuenta, pues no vamos a emplearla como tal, sino solo como plantilla.

Posteriormente, creados los usuarios, accedemos a sus **propiedades** y le asignamos el perfil que hemos definido.

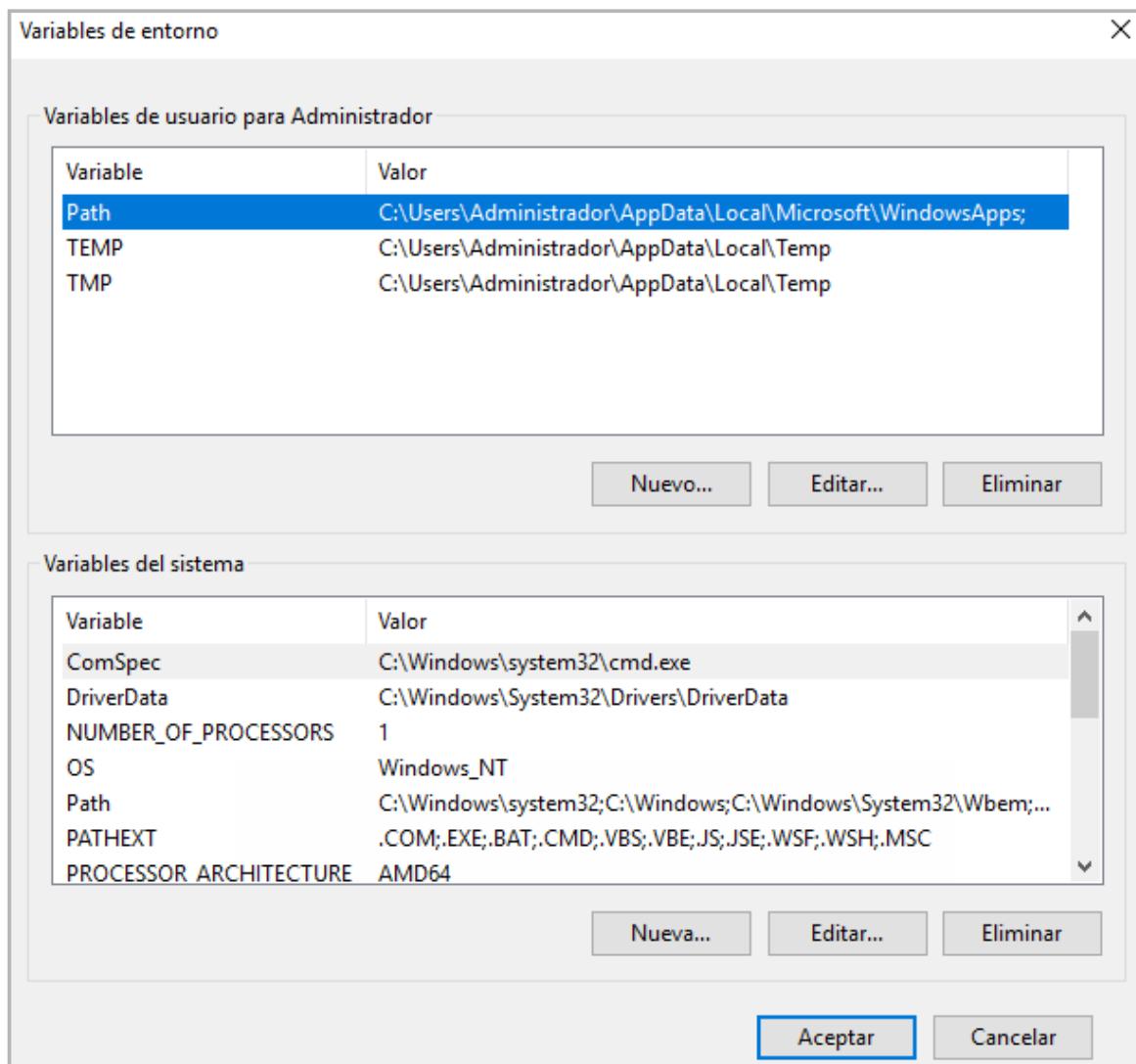
Las variables de entorno, por su parte, conforman un conjunto de valores que se ejecutan al inicio de la sesión del usuario y afectan al comportamiento de comandos y procesos.

Si por ejemplo tecleamos **%TMP%** en la barra de direcciones del Explorador de Windows, accedemos a la carpeta temporal del usuario con el que hemos iniciado sesión (generalmente **\Users\Nombre_usuario\AppData\Local\Temp**). Dicha equivalencia queda definida por una variable de entorno.



Si tecleamos "%TMP%" en la barra de direcciones del "Explorador de Windows", accedemos a la carpeta temporal del usuario con el que hemos iniciado sesión.

Para editar las variables de entorno en Windows Server, agregar nuevas variables o borrar las que se han creado por defecto, abrimos **Administración de equipos**, entramos en **Administración del equipo** y, a continuación, hacemos clic en **Propiedades**. En el apartado **Opciones avanzadas**, podemos acceder a **Variables de entorno** y modificar su **configuración**.



Las variables de Windows más comunes son:

- **%APPDATA%:** directorio de las carpetas ocultas para datos de las aplicaciones.
- **%USERPROFILE%:** directorio del usuario de la sesión.
- **%WINDIR%:** ruta por defecto de la instalación de Windows.
- **%PROGRAMFILES%:** directorio que almacena la instalación de los programas.

Estas variables de entorno no siempre conducen a directorios. Otra variable como %TIME% nos devuelve la hora actual del sistema.

Como usuarios del sistema podemos editar y crear variables de este tipo. Hay que tener en cuenta que determinados programas de software como Oracle Database crean variables de este tipo en el sistema para gestionar mejor sus recursos.



En el caso del sistema operativo Linux, la función de las variables de entorno es la misma que en Windows, aunque los nombres de estas son diferentes.

En Linux encontramos variables como:

- '**SHELL**': intérprete de comandos.
- '**LANG**': idioma actual del sistema.
- '**HOME**': directorio actual del usuario de la sesión.

Para modificar los valores de estas variables debemos acceder a tres archivos de texto almacenados en el sistema.

/etc/environment → variables independientes del intérprete de comandos.

/etc/profile → para definir variables que serán válidas para todas las *shells* interactivas que exijan login. Si queremos definir únicamente variables de usuario el directorio es `~/.bash_profile`.

/etc/bash.bashrc → igual que el anterior, aunque para consolas no logueadas. El equivalente para variables de usuario es `~/.bashrc`.



ponte a prueba

Las variables de entorno nos permiten definir características comunes que podremos aplicar a diferentes usuarios.

- a) Verdadero
- b) Falso

¿Cuál de las siguientes opciones son variables de entorno (por defecto) en un sistema operativo Windows?

- a) %TMP%
- b) %Windows%
- c) %Documentos%
- d) %C:%

4.10. ADMINISTRACIÓN DE GRUPOS.

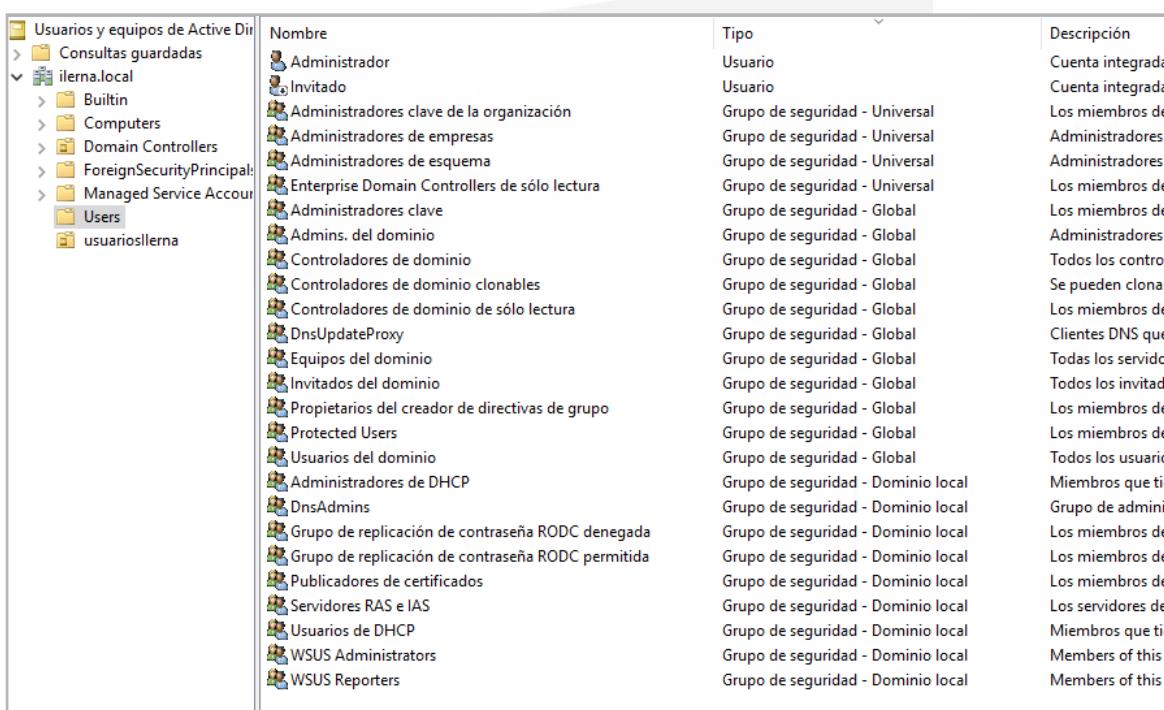
TIPO. ESTRATEGIAS DE ANIDAMIENTO.

GRUPOS PREDETERMINADOS

Si la empresa u organización cuya red administramos tiene un elevado número de departamentos y usuarios es fundamental que planeemos una estrategia para estructurarla en grupos.

De este modo, definir los permisos y el acceso a los recursos resultará mucho más rápido. Pensemos, por ejemplo, en organizaciones de quinientos o más usuarios. Definir sus características de manera individualizada no resulta operativo. Los grupos nos permiten aunar las cuentas de usuario en unidades fácilmente administrables. Cuando añadimos un usuario a un grupo, este recibe todos los privilegios de usuario asignados al grupo y los permisos referentes a sus recursos compartidos.

En Windows Server los procesos de administración de grupos se llevan a cabo mediante la herramienta **Usuarios y equipos** de Active Directory.



Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada
Invitado	Usuario	Cuenta integrada
Administradores clave de la organización	Grupo de seguridad - Universal	Los miembros de
Administradores de empresas	Grupo de seguridad - Universal	Administradores de
Administradores de esquema	Grupo de seguridad - Universal	Administradores de
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal	Los miembros de
Administradores clave	Grupo de seguridad - Global	Los miembros de
Admins. del dominio	Grupo de seguridad - Global	Administradores del
Controladores de dominio	Grupo de seguridad - Global	Todos los controlad
Controladores de dominio clonables	Grupo de seguridad - Global	Se pueden clonar
Controladores de dominio de sólo lectura	Grupo de seguridad - Global	Los miembros de
DnsUpdateProxy	Grupo de seguridad - Global	Clientes DNS que
Equipos del dominio	Grupo de seguridad - Global	Todas los servidores
Invitados del dominio	Grupo de seguridad - Global	Todos los invitados
Propietarios del creador de directivas de grupo	Grupo de seguridad - Global	Los miembros de
Protected Users	Grupo de seguridad - Global	Los miembros de
Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios
Administradores de DHCP	Grupo de seguridad - Dominio local	Miembros que tie
DnsAdmins	Grupo de seguridad - Dominio local	Grupo de adminis
Grupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local	Los miembros de
Grupo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local	Los miembros de
Publicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de
Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de
Usuarios de DHCP	Grupo de seguridad - Dominio local	Miembros que tie
WSUS Administrators	Grupo de seguridad - Dominio local	Members of this g
WSUS Reporters	Grupo de seguridad - Dominio local	Members of this g

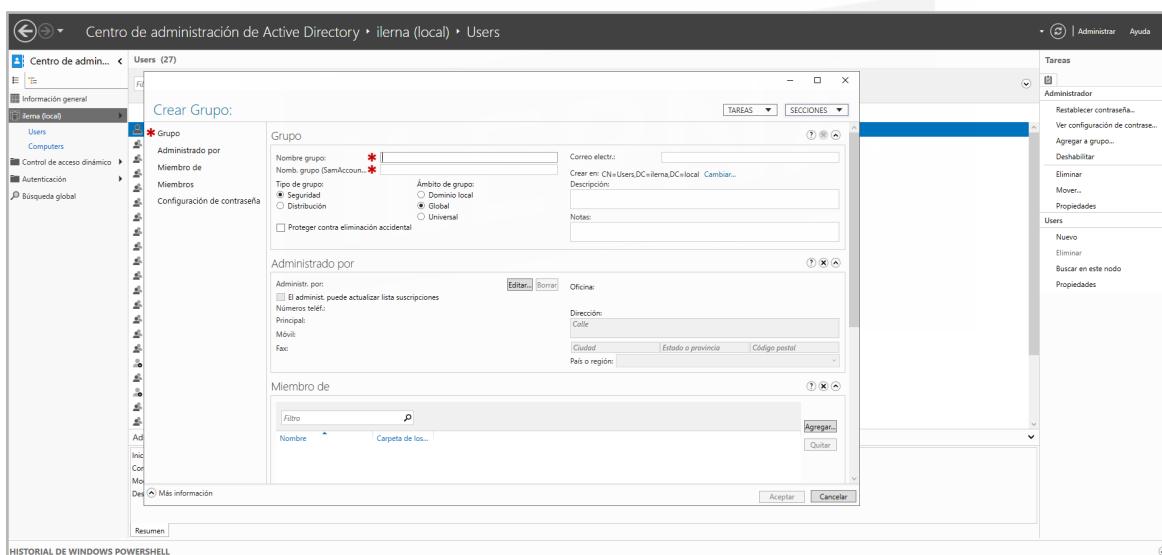
Distinguimos entre los siguientes **tipos de grupos**:

- **Grupos de distribución:** pensados solamente para usarse con aplicaciones de correo electrónico.
- **Grupos de seguridad:** se utilizan para administrar permisos de acceso a los diversos recursos de la red.

También podemos establecer esta **otra clasificación** de grupos en función de su **ámbito**:

- **Grupos de ámbito universal:** pueden emplearse en cualquier parte de un mismo bosque. Tras definir un grupo universal podemos asignarle usuarios, anidarlos y usar listas de control de acceso para definir permisos.
- **Grupos de ámbito global:** los permisos que conferimos a este grupo son válidos en cualquier dominio, pero sus miembros solo pueden realizar acciones en el dominio en el que está dado de alta el grupo global.
- **Grupos de ámbito local:** los miembros dados de alta en este pueden realizar acciones en cualquier dominio, pero sus permisos son efectivos únicamente para recursos del dominio en el que fue creado el grupo.

Para una mejor gestión de estos parámetros dentro de Active Directory encontramos la herramienta *Centro de administración de Active Directory*, la cual nos proporciona una interfaz gráfica muy amigable para gestionar los diferentes parámetros que queramos aplicar en los grupos.



Por otra parte, hay una serie de grupos que se crean de forma predeterminada. En Windows, por ejemplo, son los siguientes:

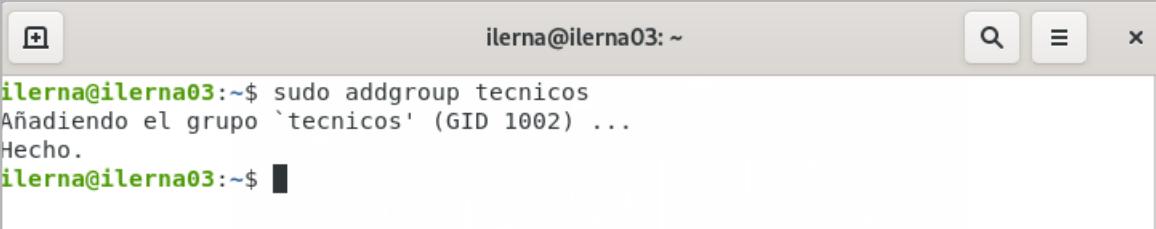
- Administradores
- Operadores de copia de seguridad
- Operadores criptográficos
- Usuarios de COM distribuido
- Invitados
- IIS_IUSRS
- Operadores de configuración de red

- Usuarios del registro de rendimiento
- Usuarios del monitor de sistema
- Usuarios avanzados
- Usuarios de escritorio remoto
- Replicador
- Usuarios
- Ofrecer aplicaciones auxiliares de asistencia remota

En los sistemas operativos Linux, al igual que sucedía con las cuentas de usuario, tendremos las dos formas de gestión por comandos o por la interfaz gráfica, aunque en esta última cabe destacar que según la interfaz que instalamos, algunos detalles pueden variar.

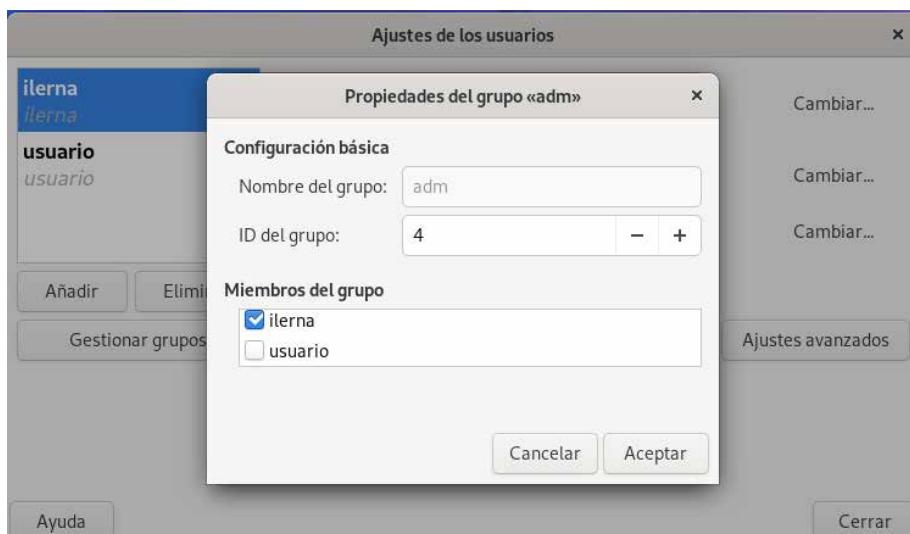
Por consola de comandos, donde utilizaremos:

```
sudo addgroup nombreGrupo
sudo delgroup nombreGrupo
```



```
ilerna@ilerna03:~$ sudo addgroup tecnicos
Añadiendo el grupo `tecnicos' (GID 1002) ...
Hecho.
ilerna@ilerna03:~$
```

Y por interfaz gráfica, donde accederemos a la aplicación de usuarios y grupos, que nos permitirá gestionar las propiedades de los grupos de una forma más amigable.



Finalmente, es importante que tengamos presente que los grupos pueden anidarse entre sí. El anidamiento de grupos consiste en hacer un grupo miembro de otro, de tal modo que utilice sus características.

4.11. INSTALACIÓN DE WINDOWS SERVER Y UBUNTU SERVER

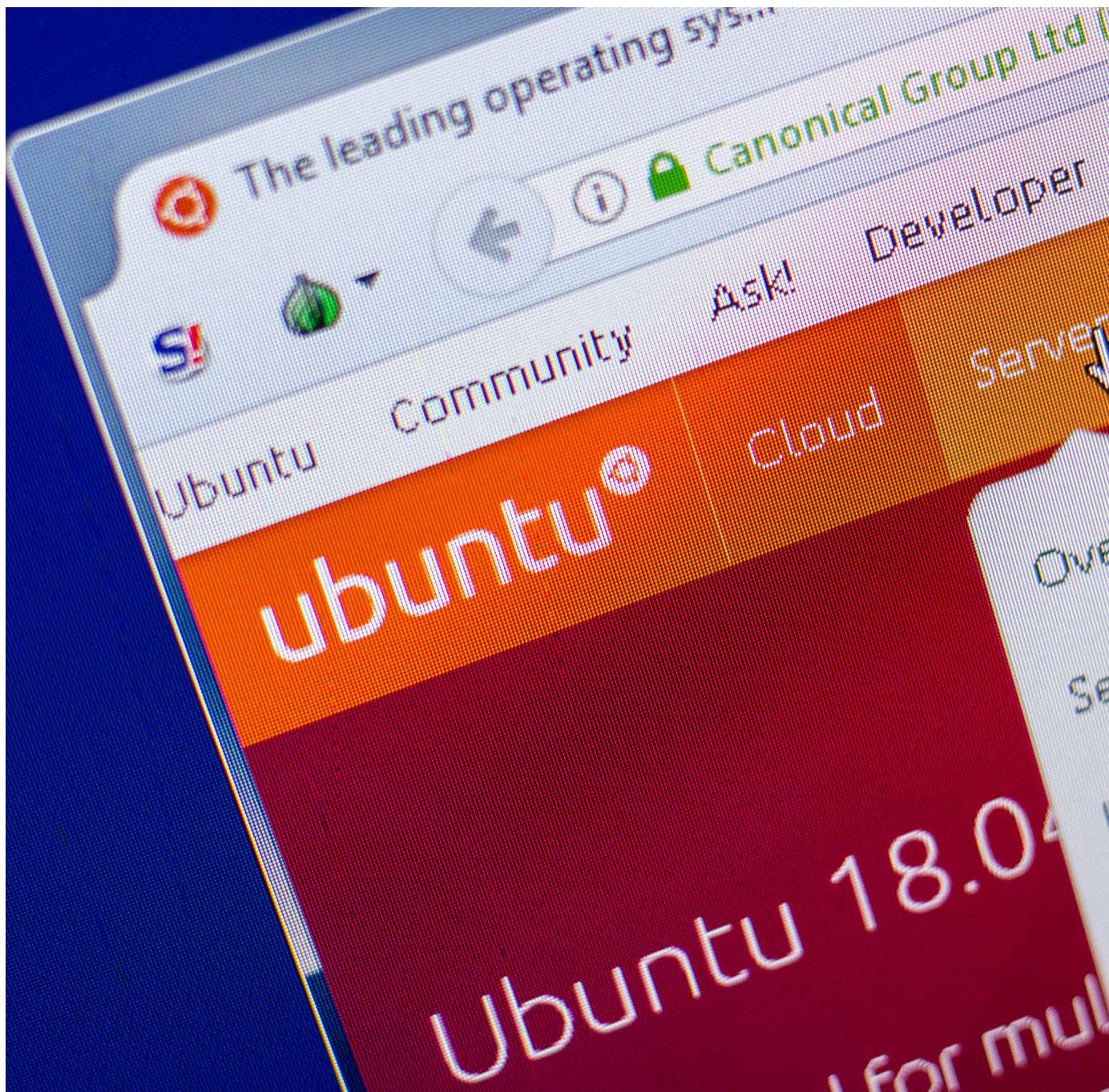
A modo de ejemplo, vamos a detallar los pasos esenciales para instalar sistemas operativos diseñados para ejercer de servidor.

Empecemos por Windows Server 2019:

1. Configuramos la BIOS para que se inicie desde el DVD.
2. Insertamos el disco de instalación de Windows Server 2019 y reiniciamos el PC.
3. Al iniciar, seleccionamos el idioma de la instalación.
4. Elegimos *Instalar*.
5. Elegimos la edición de Windows 2019.
6. Aceptamos la licencia del contrato.
7. Llegado este momento, podemos elegir entre *Modo Recomendado* o *Modo Avanzado*. Elegimos **Modo Avanzado**.
8. A continuación, llega el momento de elegir la partición del disco donde instalar el sistema operativo. Si queremos hacer la partición, entonces elegimos *Nuevo*, *Tamaño de la partición* y *Formatear*.
9. A partir de este paso, se instalará el sistema operativo y por último tendremos que reiniciar.
10. Escribimos la contraseña para el usuario administrador. Una vez iniciada la sesión, ya podemos empezar con la configuración básica de la administración del servidor.

En el caso de **Ubuntu Server 16**, los pasos serán los que detallamos a continuación:

1. Configuramos la BIOS para que se inicie desde el DVD.
2. Insertamos el disco de instalación y reiniciamos el PC.
3. Al iniciar, seleccionamos el idioma, país y la zona horaria.
4. Elegimos el *Hostname*.
5. Creamos la cuenta para usuario y su contraseña.
6. Elegimos el cifrado de la carpeta.
7. Ahora llega el momento de elegir el particionado del disco.
8. Le damos a *Instalar*.
9. Elegimos la configuración de las instalaciones.
10. Configuramos el gestor de arranque.



11. Hecho esto, GRUB se instalará en el sector de arranque de la partición.
12. Tras reiniciar el PC y entrar por primera vez con la cuenta administrativa, actualizamos el sistema tecleando lo siguiente:

`"sudo apt-get update"`

`"sudo apt-get upgrade"`

Hecho esto, el sistema habrá quedado instalado y podremos empezar a usarlo. Ya podemos modificar el archivo /etc/hosts para configurar Ubuntu Server como servidor.



5

ADMINISTRACIÓN DEL ACCESO AL DOMINIO

En este apartado vamos a seguir ampliando las distintas posibilidades que ofrecen los dominios. Recordemos que un dominio unifica y centraliza la administración de conjuntos de servidores y clientes en diferentes organizaciones, independientemente de su tamaño. Veremos los equipos que lo componen y los permisos y derechos que se les pueden asignar o retirar, entre otras cosas.

Los administradores del dominio tienen derechos administrativos sobre la base de datos del directorio y sobre cada miembro del dominio.

Además, veremos algunas herramientas que nos van a permitir optimizar el acceso a los recursos, como **Samba** y **NFS**.

5.1. EQUIPOS DE DOMINIO

Como hemos visto, en el Active Directory de un determinado dominio es donde conservamos aquella información referente a las cuentas de usuarios y grupos globales.

Al crearnos un dominio de red podemos centralizar los recursos y administrarlos con más facilidad.

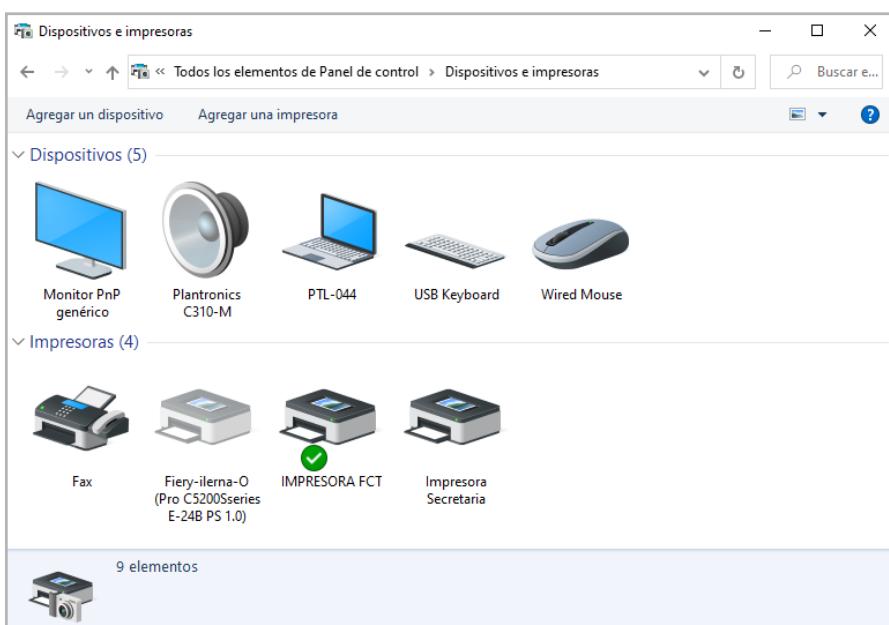
Hasta ahora, hemos utilizado una estructura cliente-servidor constituida por un ordenador (servidor) al que se conectan otros (clientes).

Sin embargo, esta estructura se puede complicar bastante si, por ejemplo, se tiene que sincronizar entre dos servidores.

Vamos a verlo de forma más amplia, estableciendo las siguientes categorías:

- **Equipos y recursos físicos:** forman parte del hardware. Pueden ser los distintos ordenadores, impresoras, escáner, monitores, etc.
- **Recursos lógicos:** todo elemento lógico administrado por el dominio. Podemos hablar, por ejemplo, de los directorios de trabajo compartidos a través de la red.
- **Usuarios y grupos:** los usuarios y grupos van a ser las personas que se gestionan a través del dominio. Estos son parte del sistema.
- **Servicios:** un dominio también nos permite administrar servicios como, por ejemplo, el correo electrónico, el acceso a FTP, etc.

Resumiendo, en un dominio cada elemento se representa como una entidad individual a la que se le pueden asignar unos atributos. Por otra parte, los elementos pueden tener otros elementos. La unión de todo esto va a definir el esquema de dominio y formará parte de su equipamiento.



Los periféricos que administremos a través del dominio también se consideran parte del equipo.



ponte a prueba

Los recursos lógicos son elementos administrados por el dominio.

- a) Verdadero
- b) Falso

En un dominio no tenemos la posibilidad de administrar servicios como FTP o correo electrónico, donde necesitaremos obligatoriamente equipos externos para la gestión de los servicios.

- a) Verdadero
- b) Falso

5.2. PERMISOS Y DERECHOS

Un modelo como Active Directory deja establecido cómo va a acceder al sistema cada usuario y cada grupo y, además, lleva a cabo un control sobre aquellas características particulares de dicho acceso.

Por ejemplo, cualquier sistema, tanto si es independiente como si forma parte de un determinado dominio, tiene la opción de compartir carpetas. Para hacerlo basta con elegir la opción de *Compartir*. Debemos tener mucho cuidado a la hora de elegir los permisos y derechos que van a tener todos los usuarios que puedan acceder a esa determinada carpeta.

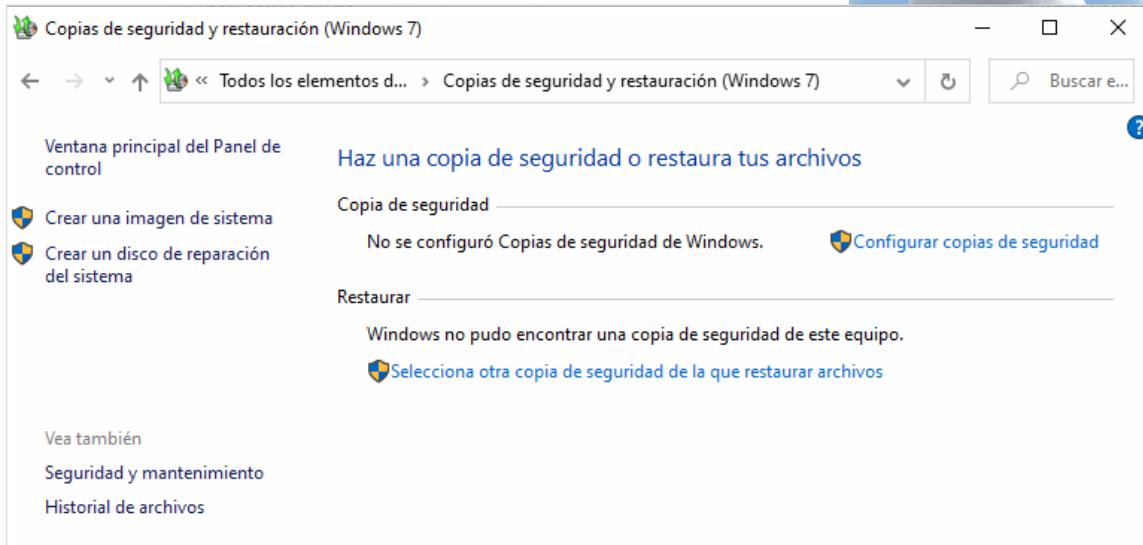
La estructura del dominio especifica qué acciones se autoriza a llevar a cabo a los usuarios y grupos:

- **Derechos (Privilegios)**

Son los atributos, tanto de usuarios como de grupos, que se les asignan para que puedan acceder al sistema y, de esta forma, tener un control sobre aquellas características particulares de cada acceso.

Podríamos resumirlo diciendo que **la estructura del dominio especifica qué acciones se autorizan a llevar a cabo por los usuarios y los grupos**.

Aquí podemos englobar acciones tan básicas como, por ejemplo, el inicio de sesión, la ejecución de copias de seguridad, etc.



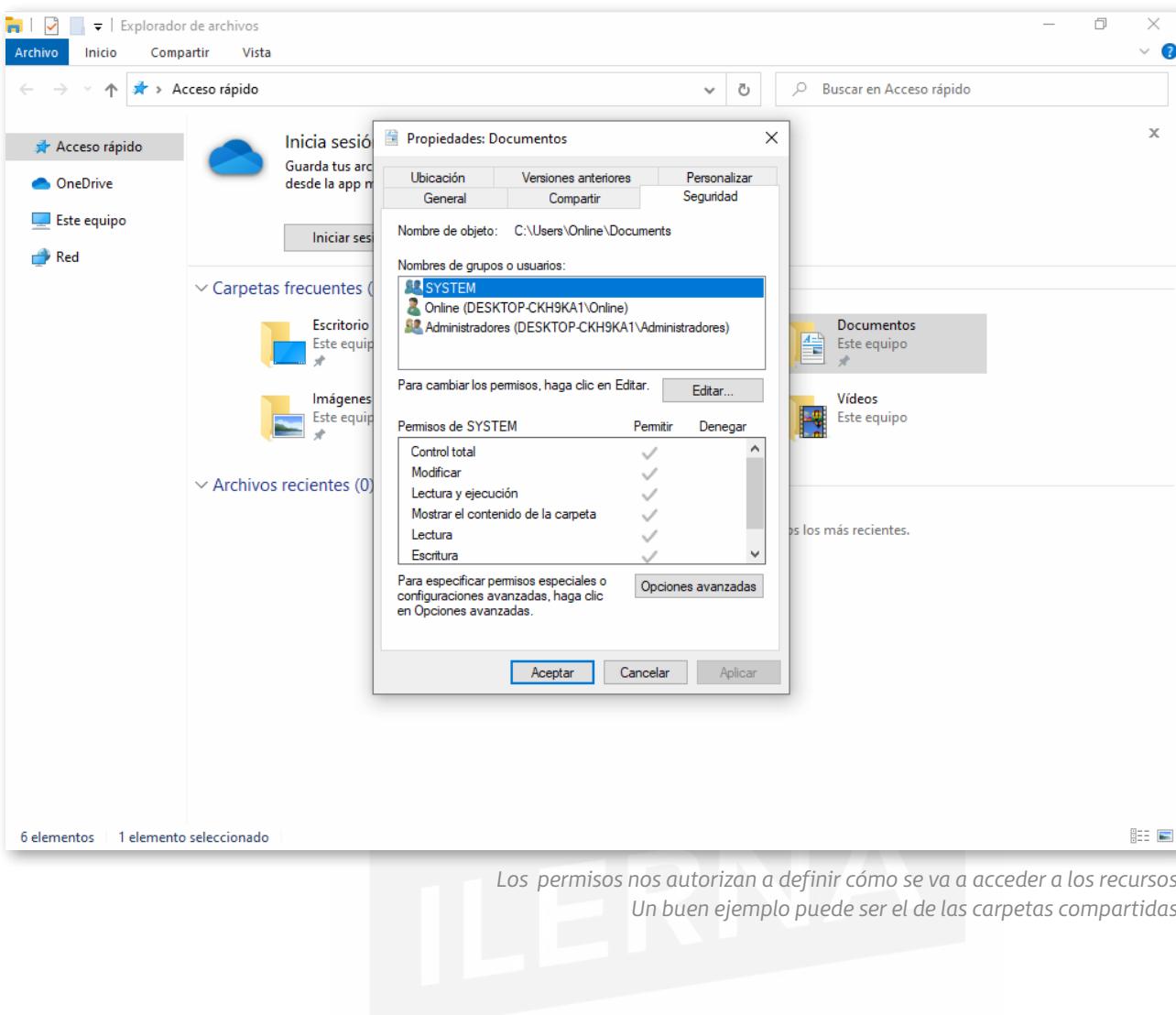
Los derechos pueden hacer referencia a acciones como realizar copias de seguridad.

En Active Directory aparece etiquetado como *Derecho de usuario* o *Userright*.

- **Permisos**

Podemos definir los permisos como el derecho o las características con las que podemos acceder a un recurso dependiendo del usuario o grupo de usuarios al que pertenezca. En el caso de recursos como las carpetas o ficheros compartidos, el dominio concederá o denegará el acceso a ellos y, además, establecerá cómo ha de llevarse a cabo.

Por tanto, cada usuario o grupo va a tener sus propios permisos referentes a un mismo recurso. Algunos podrán realizar una lectura de los datos, mientras que otros tendrán, además, permisos de modificación, ejecución, eliminación, etc.



5.3. ADMINISTRACIÓN DEL ACCESO A RECURSOS. SAMBA. NFS

Para administrar el acceso a recursos hemos estado utilizando algunas de las herramientas que nos ofrece el Active Directory. Concretamente, la aplicación *Usuarios y equipos*, que se encarga de centralizar la gestión.

De todas formas, debemos saber que existen otras posibilidades. Una de las más importantes y más utilizada es Samba.

Samba

Samba es un programa de libre implementación, y suele utilizarse en sistemas de tipo Unix. Los sistemas basados en Linux, como por ejemplo Ubuntu, ofrecen la posibilidad de instalar y utilizar este programa para proporcionar sus servicios a clientes basados en Windows.



Samba resulta ideal si administramos un dominio desde un servidor Linux en el que los clientes ejecutan Windows.

Mediante Samba podemos llevar a cabo una administración completa de los servicios de archivos y de impresión. Debido a que soporta listas de control de acceso, podemos especificar los derechos y permisos de los usuarios a través de dos vías:

- **Linux:** a través del propio servidor Linux.
- **Windows:** en equipos basados en Windows podemos utilizar una interfaz gráfica. La herramienta Winbindd permite también definir permisos.

CONCEPTO

Samba es ideal si administramos un dominio desde un servidor Linux en el que los clientes ejecutan Windows.

En resumen, podemos decir que **Samba** es el **software que permite que equipos Linux se muestren como servidores o ejerzan de clientes en redes Windows**. Este software permite también la administración de usuarios y la gestión de sus permisos.

En la mayoría de casos, lo normal es que el usuario administrador disponga de todos los permisos. Aunque, si no se conecta como administrador, adoptará las distintas formas del usuario.

Para hacer efectiva la seguridad, Samba dispone de una base de datos propia de usuarios. Pero como estos utilizan recursos del servidor (impresoras, carpetas, etc.) es

necesario que estén dados de alta en Linux. En definitiva, para poder ser usuario de Samba es preciso disponer, tanto de una cuenta de usuario en Linux como de una cuenta de usuario en Samba.

La gestión de usuarios de Samba se lleva a cabo mediante el comando **smbpasswd**. Este nos permite crear y borrar usuarios, modificar su contraseña, etc.

Veamos algunos ejemplos:

- **Creación de un usuario Samba**

"*sudo useradd<nombre de usuario>*"

- **Eliminar un usuario Samba**

"*sudo smbpasswd -x <nombre de usuario>*"

- **Deshabilitar un usuario**

"*sudo smbpasswd -d <nombre de usuario>*"

- **Habilitar un usuario**

"*sudo smbpasswd -e <nombre de usuario>*"

Para obtener más información sobre Samba puedes teclear lo siguiente:

"mansmbpasswd"

Por último, debemos tener presente que podemos usar SWAT. Su nombre proviene del acrónimo *Samba Web Administration Tool*, es decir, herramienta de administración web de Samba. Gracias a esta herramienta podemos configurar Samba en modo gráfico. Generalmente, resulta más sencillo hacerlo así que mediante el programa **Webmin** o editando el fichero **smb.conf**.

NFS

El **sistema de archivos de red** es un protocolo cuyas siglas se corresponden con *Network File System*. Podemos definirlo como una herramienta que se utiliza habitualmente a la hora de configurar redes basadas en un servidor de dominio cuando empleamos Linux.

El sistema NFS consta de dos partes principales: un servidor y uno o más clientes. Gracias a este sistema podemos conseguir que los ordenadores pertenecientes a una red local accedan a archivos remotos de manera transparente, de tal modo que, a nivel de usuario, se perciban como si fueran archivos locales.

NFS participa de la estructura cliente-servidor: tendremos equipos cliente que van a acceder de forma remota y a través de la red a la información que se encuentra almacenada en el equipo servidor.

Linux NFS Overview, FAQ and HOWTO Documents

This document provides an introduction to NFS as implemented in the Linux kernel. It links to developers' sites, mailing list archives, and relevant RFCs, and provides guidance for quickly configuring and getting started with NFS on Linux. A Frequently Asked Questions section is also included. This document assumes the reader is already familiar with generic NFS terminology.

NFS Links

- Linux NFS-HOWTO
- NFS-related kernel patches supported by Trond Myklebust
- NFS-related kernel patches supported by Neil Brown
- CITI's NFSv4 project
- SourceForge NFS Project Page
- The nfs-utils tarballs

Avoid applying experimental patches to your kernels unless there is a very good reason to do so.

General Information

Quick Overview

- NFS Versions 2, 3, and 4 are supported on 2.6 and later kernels.
- NFS over UDP and TCP on IPv4 are supported on the latest 2.4 and 2.6 kernels.
- Linux NFS clients and servers have been tested against many non-Linux implementations.
- Since version 1.0.1 of the NFS utilities tarball has changed the server export default to "sync", then, if no behavior is specified in the export list (thus assuming the default behavior), a warning will be generated at export time.
- If you plan to deploy NFS extensively, consider subscribing to one of these mailing lists: [NFS Mailing List](#). Before reporting problems, you should search for similar issues in the [searchable mail archive](#).
- A useful set of generic NFS references includes the following:
 - "[NFS Illustrated](#)," by Brent Callaghan; Addison-Wesley, 2000.
 - "[Managing NFS and NIS, 2nd edition](#)," by Hal Stern, Mike Eisler, Ricardo Labiaga; O'Reilly, 2001.
 - "[Linux NFS and Automounter Administration](#)," by Erez Zadok; Sybex, 2001.
 - "[Using the Linux NFS Client with Network Appliance Filers](#)," by Charles Lever; Netapp TR-3183, 2004.

Gracias a NFS podemos conseguir que los ordenadores pertenecientes a una red local accedan a archivos remotos de manera transparente.



ponte a prueba

Samba es un software de licencia comercial y suele implementarse en equipos Windows. Este ofrece la posibilidad de proporcionar servicios a clientes basados en sistemas operativos con licencia.

- a) Verdadero
- b) Falso

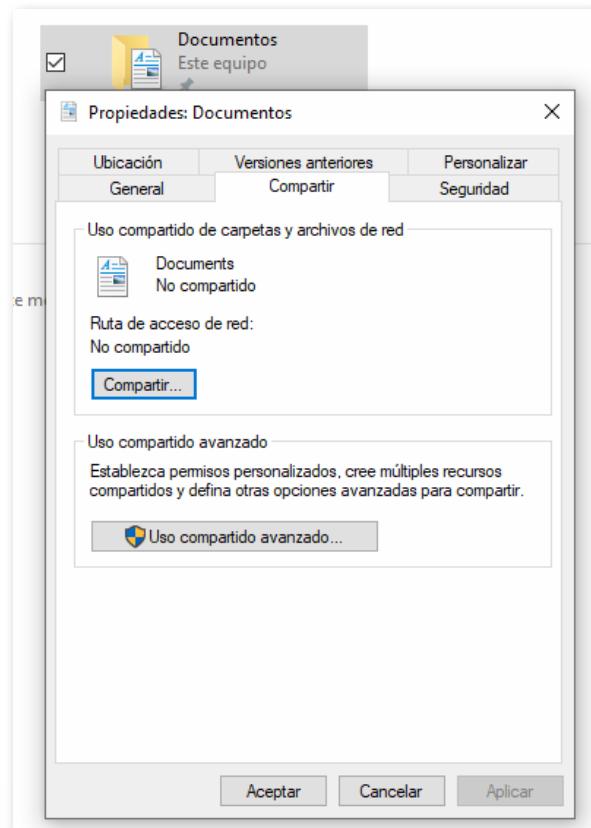
¿Qué comando utilizaremos para gestionar los usuarios en Samba?

- a) smbpasswd
- b) adduser
- c) addsmbuser
- d) smbuserpass

5.4. PERMISOS DE RED. PERMISOS LOCALES. HERENCIA. PERMISOS EFECTIVOS

Los equipos que administramos a través de la red pueden compartir sus recursos con los demás ordenadores, tanto si se trata del propio servidor, como si son clientes o estaciones de trabajo.

No solo desde el servidor podemos asignar permisos. También desde las estaciones de trabajo contamos con la posibilidad de definirlos localmente. Para poder compartir un directorio en un cliente que ejecute Windows, por ejemplo, bastará con desplegar el menú contextual que se muestra al pulsar el botón derecho del ratón sobre él desde el Explorador y escoger la opción **Compartir**.



Ventana “Compartir” en una estación de trabajo.

En esta nueva ventana se nos permite definir las diversas características del nuevo recurso compartido:

- **Nombre:** es el nombre que vamos a asignar al recurso elegido. No tiene que coincidir necesariamente con el de la propia carpeta.
- **Usuarios:** podemos especificar qué usuarios van a poder acceder al recurso.
- **Permisos:** donde vamos a asignar los permisos de lectura, escritura, etc. que se brindan a cada usuario.

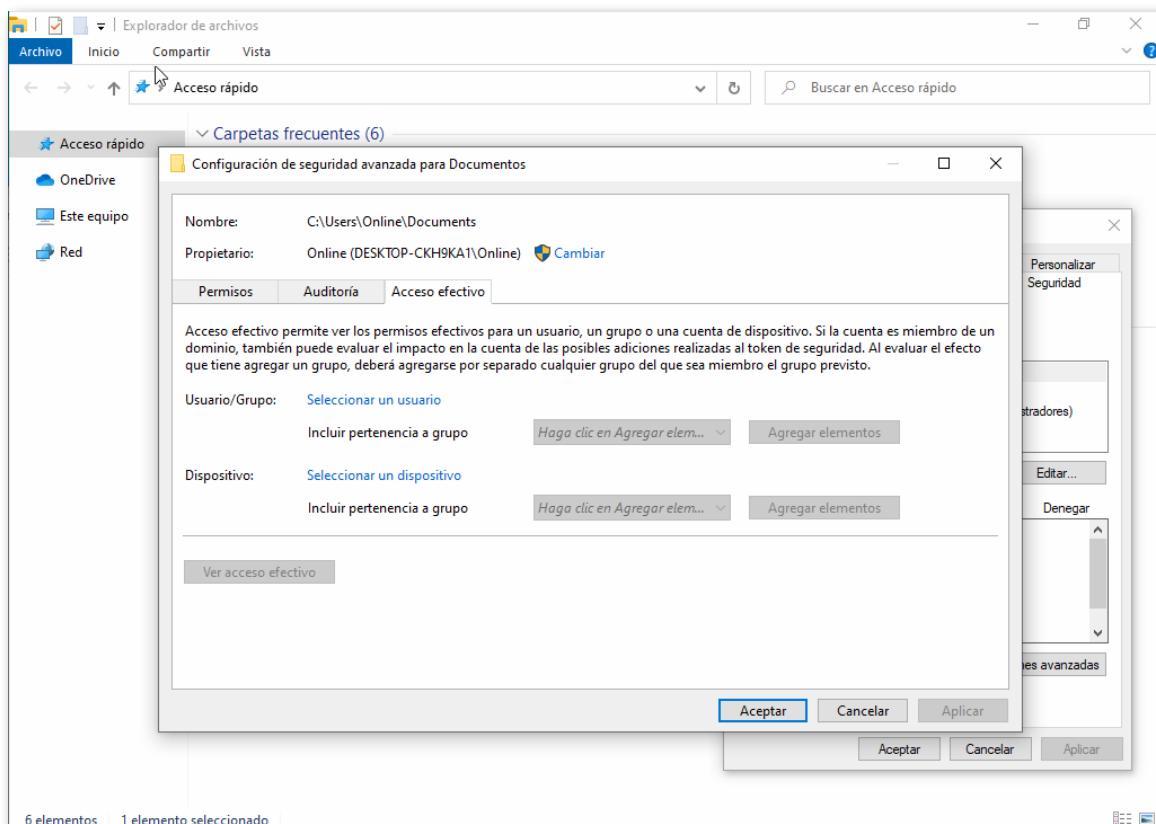
Cuando trabajamos con una red basada en dominio, como Active Directory, posiblemente habremos definido permisos desde el servidor y los habremos asignado a los distintos usuarios que van a acceder a la red. Recordemos que, a nivel interno, podemos considerar que estamos trabajando con una base de datos de directorios a los que se les asignan una serie de identificadores y características.

¿Qué sucede entonces cuando tenemos, por un lado, los permisos que se definen a través del servidor (por ejemplo, en Active Directory) y, por otro, los que se definen en los equipos cliente? ¿Cuáles son los permisos efectivos?

En dicho caso, solo los usuarios que cumplan los requisitos definidos en el servidor y los requisitos definidos en el

cliente tendrán acceso a la carpeta compartida y podrán realizar acciones sobre su contenido. En definitiva, deberán pasar ambos filtros.

La sección *Permisos efectivos* de las propiedades de **Configuración Avanzada** nos lista los permisos que se concederán al grupo o usuario seleccionado, atendiendo solamente a los permisos concedidos directamente a través de la pertenencia a un grupo.



Permisos efectivos de un directorio en Windows 10.

Así, para determinar cuáles serán los permisos más efectivos, tendremos en cuenta los siguientes factores:

- **Grupo general:** grupo general al que pertenece y nuestros permisos en él.
- **Grupo local:** grupo local al que pertenece y nuestros permisos en él.

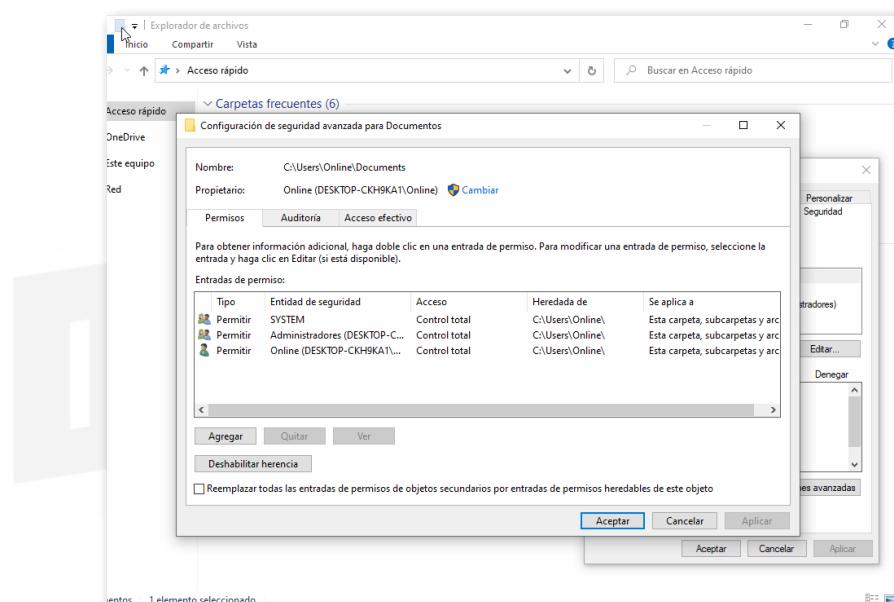
No obstante, es importante que tengamos presente que el acceso a los recursos compartidos se puede denegar mediante los permisos de recurso compartido.

Así, cuando utilizamos la sección *Permisos efectivos* para tratar de determinar qué permisos posee un usuario para acceder a un recurso determinado de nuestro dominio, tal vez los resultados que se muestren en la ventana no equivalgan a las autorizaciones reales con las que cuenta

el usuario para dicho recurso. Esta situación puede darse, generalmente, cuando ejecutamos herramientas administrativas de manera remota desde el servidor de recursos.

Para prevenir este tipo de incoherencias es importante comprobar de manera local cuáles son los permisos efectivos en el equipo que hospeda el recurso. Durante la comprobación tenemos que confirmar que la cuenta de administrador que usamos se encuentra en el mismo dominio que el recurso.

Otro factor para tener en cuenta es que los permisos se propagan desde los elementos que administramos, influyendo en sus elementos primarios. En tal caso hablamos de permisos heredados. Esta es otra característica que se debe tener en cuenta para que la asignación de permisos mantenga una coherencia.



Permisos heredados en Windows 10.

Por ejemplo, en Active Directory, los permisos heredados pueden distinguirse porque, a la hora de examinar los permisos de un elemento, sus casillas de verificación aparecen sombreadas. Esto significa que ha heredado permisos del elemento principal (recordemos que los directorios se estructuran en forma de árbol).

A partir de ahí, para ajustar los permisos y que se adecuen a nuestras necesidades, podemos emprender una de las siguientes acciones:

- **Cambios de configuración en el elemento principal:** si realizamos cambios de configuración en el elemento principal (el que brinda la herencia), el elemento secundario heredará sus permisos.

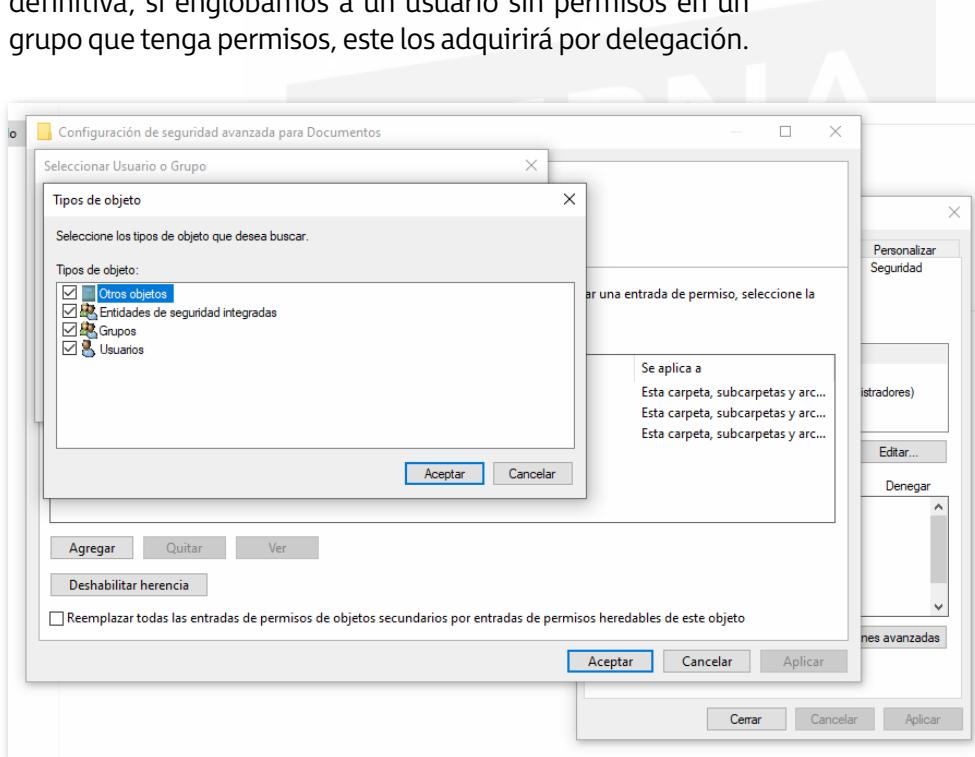
- **Configuración directa del permiso:** podemos elegir Permitir o Denegar para remplazar el permiso heredado.
- **Eliminar la herencia:** para ello desactivaremos la casilla de verificación etiquetada como *Heredar* del objeto principal y las entradas de permisos relativas a los objetos secundarios. En adelante, el elemento dejará de heredar los permisos del objeto principal.

5.5. DELEGACIÓN DE PERMISOS

Ahora que ya tenemos claro el significado de los permisos, cabe recordar que el administrador tiene permisos previos y que, a los usuarios, se les concederá solo parte de ellos: exclusivamente los que necesiten para completar sus tareas.

La **delegación de permisos** es un mecanismo mediante el cual concedemos a un usuario determinado o a un grupo completo el permiso para realizar una operación particular.

La delegación puede llevarse a cabo por distintas vías, pero la más habitual es la delegación por pertenencia al grupo. En definitiva, si englobamos a un usuario sin permisos en un grupo que tenga permisos, este los adquirirá por delegación.



La delegación puede llevarse a cabo por distintas vías, pero la más habitual es la delegación por pertenencia a un grupo.

La característica de delegación, no obstante, frecuentemente puede configurarse. En Windows Servers, sin ir más lejos, podemos hacerlo a través de la herramienta *Consola de administración de directivas de grupo (GPMC)*.

Tras desplegar *Objetos de directiva de grupo* en el dominio que contiene el elemento al que deseamos añadir o quitar permisos, haremos clic en **GPO**.

El apartado **Delegación** nos permitirá ajustar la característica.

5.6. LISTAS DE CONTROL DE ACCESO (ACL Access Control List)

Las listas de control de acceso suelen utilizarse para asignar los permisos de forma habitual. Gracias a ellas podemos asignar permisos a otros usuarios distintos al propietario y a grupos que no sean el propio grupo al que pertenece el propietario.

Además, también se utilizan para filtrar el tráfico en lo referente a la seguridad informática. Desde su propia configuración, es posible realizar tareas como:

- Aumentar el rendimiento de la red limitando el tráfico. Por ejemplo, una de las tareas que más tráfico de red abarca es la reproducción de vídeos. Es posible configurar una política corporativa que no permita la reproducción de estos.
- Es posible configurar el acceso de un host a una determinada área de la empresa y evitar que cualquier otro host acceda a ella.
- Bloquear el tráfico de las redes sociales y limitar únicamente al tráfico del correo electrónico.
- Permitir a diferentes usuarios acceder a determinados tipos de archivos.

En apartados anteriores hemos llegado a la conclusión de que hay definidos tres permisos para que los usuarios puedan acceder a los archivos:

- Lectura ("r")
- Escritura ("w")
- Ejecución ("x")

Sin embargo, en las redes que podemos habilitar en sistemas Linux tenemos tres figuras en relación con los archivos:

- *Owner*: propietario del archivo.
- *Group*: grupo al que pertenece el propietario del archivo.
- *Other*: se refiere al resto de usuarios que no son ni los propietarios ni el grupo.

Por regla general, si estructuramos los usuarios y los grupos de forma correcta desde el servidor, llevar a cabo las asignaciones pertinentes como administrador será suficiente para que cada usuario tenga el acceso que precisa y ninguno más. Sin embargo, ante escenarios más complejos, tenemos que recurrir a otras vías alternativas.

Una aplicación práctica de las listas de control de acceso

Imaginemos que disponemos de un servidor que ejecuta Windows Server y que deseamos sustituirlo por uno que ejecutará Ubuntu.

En nuestro supuesto, parte de los equipos clientes conectados a la red seguirán ejecutando Windows, pero en adelante será el servidor Linux el que les proporcione servicios de impresión, de servidor de archivos, etc. Este escenario complica las asignaciones.

Gracias a Samba podemos habilitar listas de control de acceso. De este modo, podemos asignar permisos de manera mucho más dinámica, porque a las tres figuras que hemos listado en relación con los archivos, se les agregan nuevas posibilidades:

Las que ya habíamos visto:

Owner

Group

Other

Se le pueden añadir:

Usuarios específicos: podemos agregar usuarios que tendrán acceso al recurso a nivel individualizado. Es más, podemos decidir qué permisos tendrán.

Grupos específicos: en esta sección podemos agregar un listado de grupos.

En definitiva, las listas de control de acceso amplían los elementos a los que asignamos permisos hasta cinco. No obstante, para poder utilizar las listas de control de acceso en Linux deben cumplirse las siguientes condiciones:

- **Soporte por parte del kernel:** el kernel de nuestra instalación de Linux soporta esta característica.
- **Soporte por parte del sistema de archivos:** el sistema de archivos debe montarse con el atributo ACL.

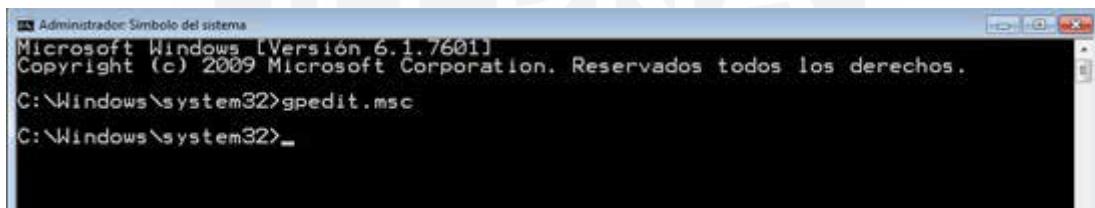
5.7. DIRECTIVAS DE GRUPO. DERECHOS DE USUARIOS. DIRECTIVAS DE SEGURIDAD. OBJETOS DE DIRECTIVA. ÁMBITO DE LAS DIRECTIVAS. PLANTILLAS

Las **directivas de grupo** son características propias de Windows Server y nos permiten especificar un conjunto de reglas que se van a aplicar de manera general a las cuentas de usuario y a las de equipo.

Nos encontramos con un mecanismo orientado a la simplificación de Active Directory y, gracias a él, podemos ejercer un control sobre lo que pueden y lo que no pueden hacer los usuarios. En resumen, nos permiten definir sus derechos y ampliar la seguridad.

Las directivas de grupo se utilizan con mayor frecuencia en las redes de dimensiones modestas que en las grandes redes y, de hecho, para usar esta función no precisamos necesariamente del uso de Active Directory.

En Windows 10, por ejemplo, podemos acceder a ellas tecleando *gpedit.msc* desde el **Símbolo del sistema**.



Tecleando “*gpedit.msc*” en el “Símbolo del sistema” de Windows 10 accedemos a la herramienta “Directivas de grupo local”.

Esto abrirá la herramienta *Editor de directivas de grupo local*. El panel izquierdo mostrará los elementos u objetos sobre los que podemos actuar para asignar o denegar derechos.

Tengamos presente que si escribimos:

{gpedit.msc /gpcomputer: “nombreDeEquipo”}

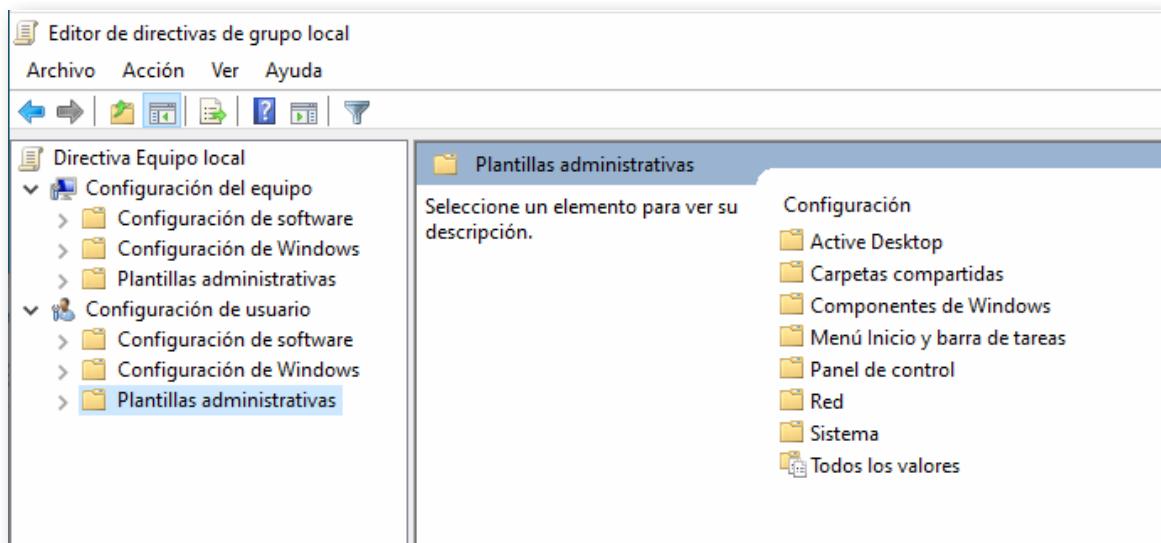
El objeto de la directiva de grupo local será *nombreDeEquipo*.

Por otra parte, si tecleamos lo siguiente:

{gpedit.msc /gpcomputer:“nombreDeEquipo.dominio.com”}

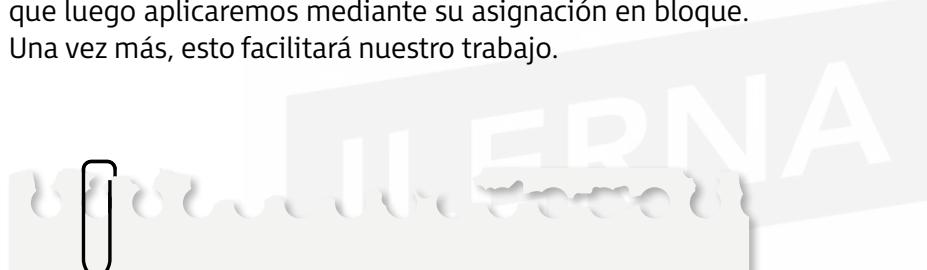
En tal caso haremos referencia a objetos de directiva de grupo almacenados en Active Directory.

Observemos que en las herramientas para editar directivas de grupo se nos permite crear y editar plantillas.



A la hora de especificar directivas de grupo podemos usar plantillas.

Gracias a las plantillas podemos compendiar características que luego aplicaremos mediante su asignación en bloque. Una vez más, esto facilitará nuestro trabajo.



ponte a prueba

Las directivas de grupo se utilizan con mayor frecuencia en las redes de dimensiones modestas que en las grandes redes.

- a) Verdadero
- b) Falso

Las plantillas nos permiten asignar directivas más estrictas, aunque tienen como desventaja su aplicación individual, donde tienen que asignarse usuario a usuario y no pueden realizar una asignación en bloque.

- a) Verdadero
- b) Falso



6 RESOLUCIÓN DE INCIDENCIAS Y ASISTENCIA TÉCNICA

La documentación técnica resulta clave en el ámbito que nos ocupa. En el presente apartado analizaremos cómo elaborarla.

Aunque hagamos una organización cuidadosa, es probable que a veces se produzcan incidencias y problemas técnicos, por lo que tendremos que prestar asistencia a los usuarios. A continuación, lo veremos de forma más detallada.

6.1. INTERPRETACIÓN, ANÁLISIS Y ELABORACIÓN DE DOCUMENTACIÓN TÉCNICA. INTERPRETACIÓN, ANÁLISIS Y ELABORACIÓN DE MANUALES DE INSTALACIÓN

Tanto a la hora de documentarnos sobre las tareas a realizar, como a la de ofrecer información a colaboradores y usuarios, debemos elaborar documentación técnica. Dado lo fundamental que resulta, analizaremos con mucho detenimiento lo que pretendemos detallar antes de volcarnos en la tarea, independientemente de si el soporte de la documentación es el papel o si va a distribuirse en formato digital.

Repasemos las principales características que deberá contemplar la documentación técnica:

Guía de referencia rápida

Una buena idea puede ser incluir una guía rápida que, a modo de esquema, recopile las características o funciones más imprescindibles o que se utilicen con mayor frecuencia.

Por ejemplo, en aplicaciones web encontramos muchas veces la opción de Ayuda, donde aparte del contacto con la atención de la plataforma suele haber pequeñas guías rápidas para orientar de una forma más concreta a los usuarios de los aplicativos.

Adecuación al nivel de los destinatarios

Es muy importante que tengamos presente a quién va dirigida la documentación. Si se trata de usuarios, el material debe ser entendido por todos ellos. En el caso de los usuarios avanzados debemos ser conscientes de su nivel.

← Ayuda →

Calendario escolar

En Calendario escolar, disponible en [Campus Virtual](#), podrás ver los **eventos y entregas** de las diferentes asignaturas, así como los **eventos globales** del centro. Haciendo clic en cada uno de los eventos, podrás verlos en detalle. Podrás también **personalizar** cada asignatura **con colores diferentes**, para identificar mejor los diferentes calendarios de las asignaturas.

No te pierdas detalle, con el Calendario Escolar de Campus Virtual ;).

¿Responde la pregunta este artículo?

Sí **No, necesito ayuda**

The screenshot shows the 'Documentación de Windows Server' (Windows Server Documentation) page. It features a grid of eight cards, each representing a different topic or guide:

- NOVEDADES**: Novedades de Windows Server 2019
- INFORMACIÓN GENERAL**: Introducción a Windows Server 2019
- GUÍA PASO A PASO**: Windows Admin Center
- INFORMACIÓN GENERAL**: Infraestructura hiperconvergida
- GUÍA PASO A PASO**: Conexión a los servicios híbridos de Azure
- GUÍA PASO A PASO**: Introducción a Windows Server 2016
- GUÍA PASO A PASO**: Usar las actualizaciones de seguridad extendida de Windows Server 2008 y 2008 R2
- INFORMACIÓN GENERAL**: Programa Windows Insider para servidores

Un exceso de información puede ser tan perjudicial para los usuarios que ya conocen el funcionamiento del programa como una escasez de la misma para quienes lo desconocen por completo.

Características específicas del paquete de software

Si el manual se centra en el software, no solo debe constar su nombre, sino también su versión. No olvidemos que las nuevas versiones del programa pueden variar sus características, tanto a nivel de licencias como de propiedades.

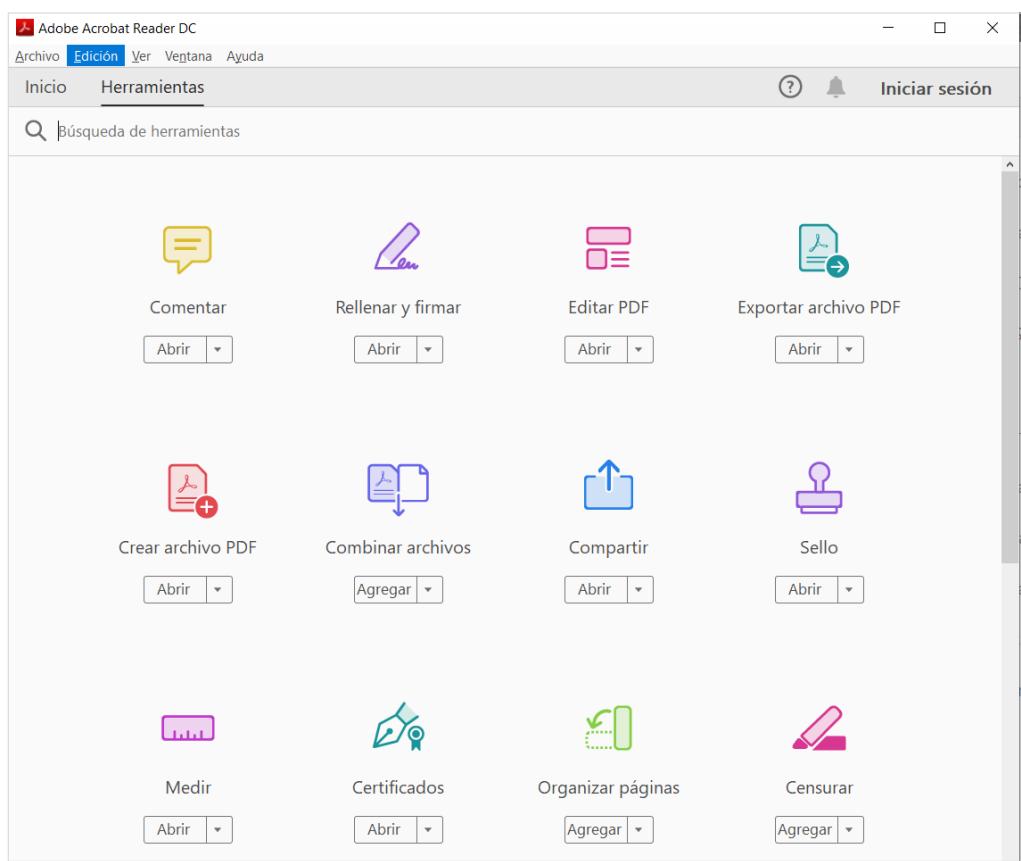
Como podemos ver en esta comparativa de la aplicación de Acrobat, la versión Pro cuenta con más características y un orden distinto que la versión Reader.

The screenshot shows the Adobe Acrobat Pro DC application window. The top menu bar includes Archivo, Edición, Ver, Ventana, Ayuda, Inicio, and Herramientas. The main interface has a search bar labeled 'Búsqueda de herramientas'. On the left, there's a 'Crear y editar' (Create and edit) panel with several tools:

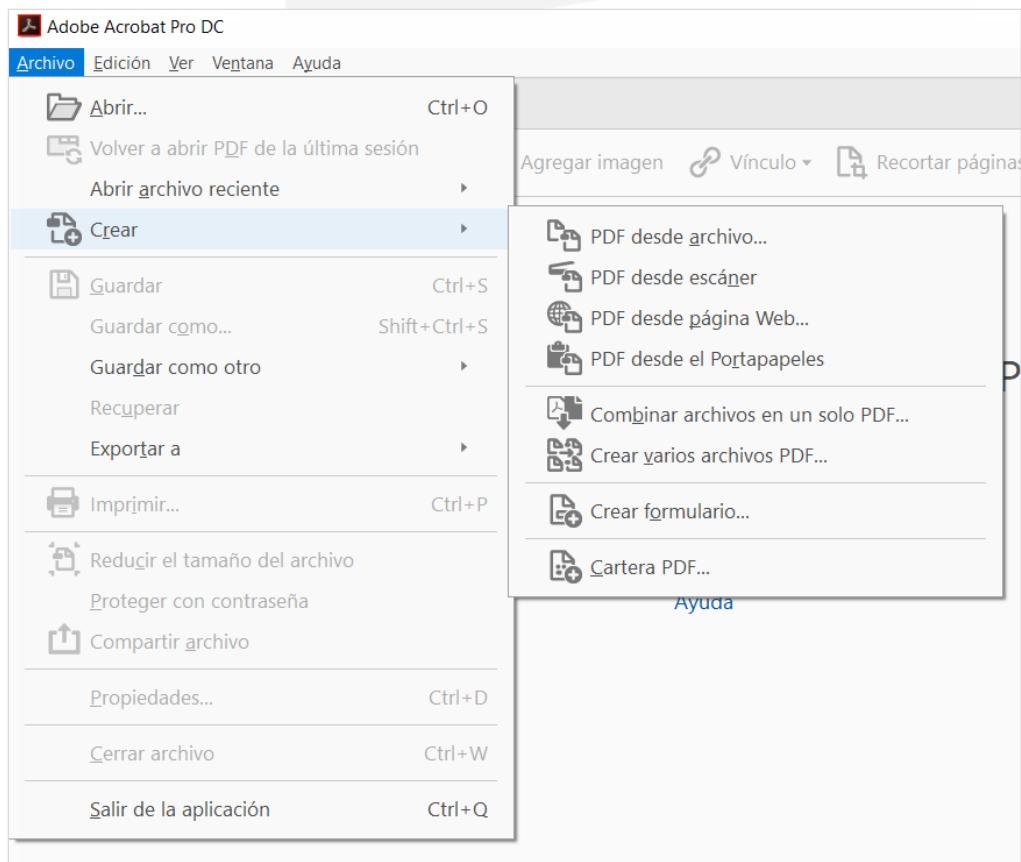
- Crear archivo PDF**: Includes 'Abrir' (Open) button.
- Combinar archivos**: Includes 'Abrir' (Open) button.
- Organizar páginas**: Includes 'Abrir' (Open) button.
- Editar PDF**: Includes 'Abrir' (Open) button.
- Exportar archivo PDF**: Includes 'Abrir' (Open) button.
- Digitalizar y OCR**: Includes 'Abrir' (Open) button.
- Medios enriquecidos**: Includes 'Agregar' (Add) button.

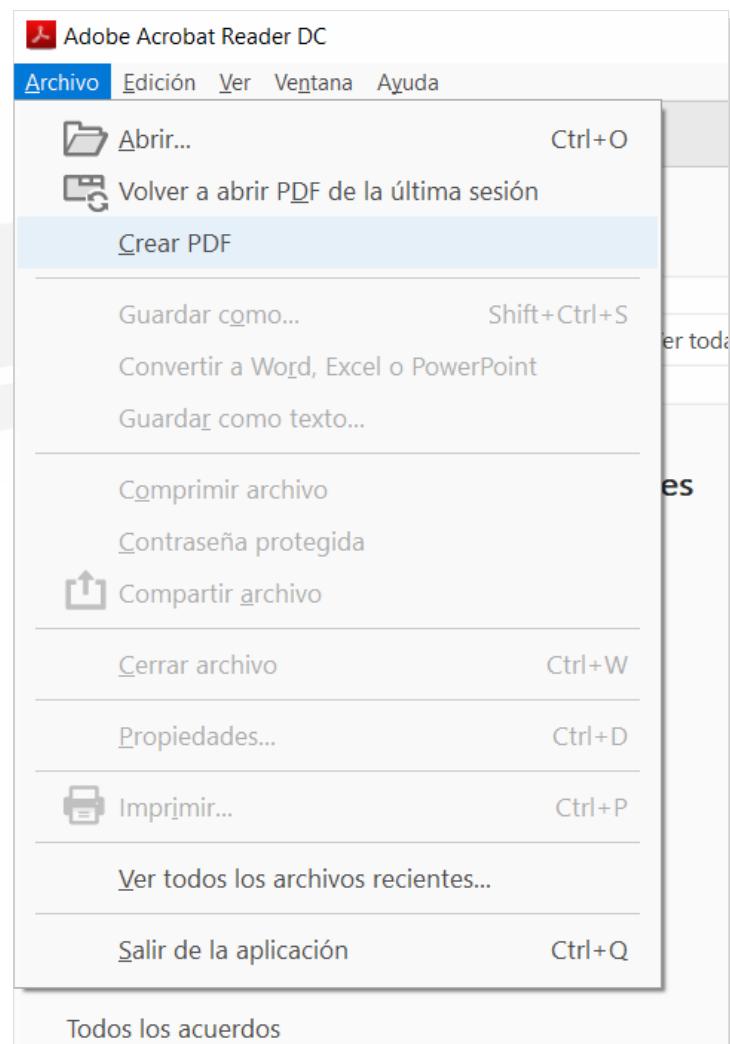
To the right of the main area is a sidebar listing additional features:

- Crear archivo PDF
- Combinar archivos
- Editar PDF
- Adobe Sign
- Rellenar y firmar
- Exportar archivo PDF
- Organizar páginas
- Enviar para comentarios
- Comentar
- Digitalizar y OCR
- Proteger



Aunque estas aplicaciones mantienen un formato visual muy similar, las opciones internas varían según las necesidades que tengamos.

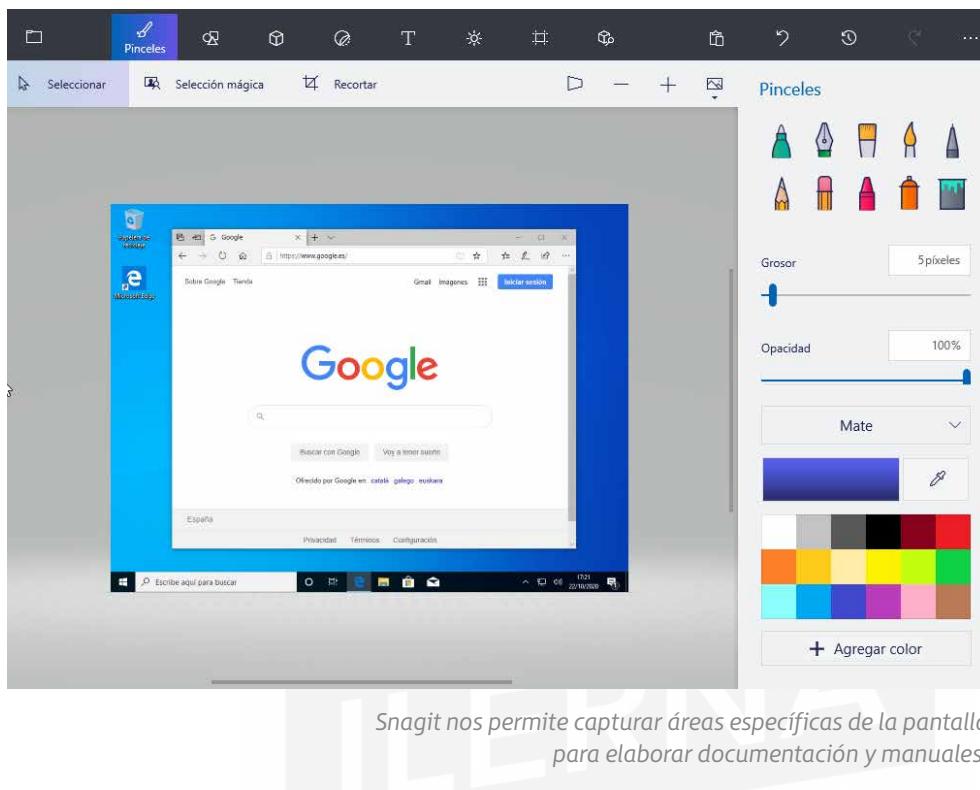




Cabe destacar que, en este caso, la licencia de la versión Pro conlleva costes económicos (comercial), en cambio la versión Reader es gratuita.

Capturas de pantalla

Lo ideal es que incluyamos imágenes que documenten el uso y manejo del sistema o de la aplicación a la que nos referimos. Podemos capturarlas con la tecla *Impr. Pant* o bien utilizando aplicaciones como Snagit (www.techsmith.com/snagit.html).



Actualmente aplicaciones como Gyazo se utilizan más debido a que nos ofrecen varias opciones para compartir estas imágenes, de tal forma que no quedan almacenadas en nuestro equipo físico y alivian de carga los discos duros.

Posibles problemas y errores

Es conveniente que la documentación incorpore una lista de posibles problemas y errores que puede encontrar el usuario y, a continuación, su posible solución.

Estas listas siempre están en constante actualización con los errores que van surgiendo entre versiones o actualizaciones que podamos realizar. Por este motivo, debemos tener en cuenta la escalabilidad de esta parte de la documentación.

Glosario

En caso de que utilicemos términos con los que el destinatario de la documentación no esté familiarizado, un glosario le facilitará bastante la tarea, ya que contiene la definición o explicación de las palabras técnicas.

Glosario de Windows IoT

28/08/2017 • Tiempo de lectura: 2 minutos • ● ●

Interfaz avanzada de configuración y energía (ACPI) ACPI es una especificación abierta del sector desarrollada de forma conjunta por Hewlett-Packard, Intel, Microsoft, Phoenix y Toshiba. ACPI establece interfaces estándar del sector que permiten la configuración dirigida al sistema operativo, la administración de energía y la administración térmica de plataformas de dispositivos móviles, de escritorio y servidor.

Sistema básico de entrada y salida (BIOS) El conjunto de rutinas de software fundamentales que prueban el hardware al inicio, inician el sistema operativo y permiten la transferencia de datos entre dispositivos de hardware.

Comercializar El desarrollo y la fabricación de un dispositivo con la intención de ofrecerlo comercialmente al público.

Entrada y salida de uso general (GPIO) GPIO es un pin genérico en un circuito integrado, cuyo comportamiento, incluido si se trata de un pin de entrada o salida, lo puede controlar el usuario en tiempo de ejecución. Puede usar el espacio de nombres Windows.Devices.Gpio en la aplicación para manipular los pines GPIO de la placa.

Con periféricos Windows IoT Core pueden estar en modo con periféricos o sin periféricos. La diferencia entre estos dos modos es la presencia o ausencia de cualquier forma de interfaz de usuario. De forma predeterminada, Windows 10 IoT Core está en modo con periféricos y muestra información del sistema, como el nombre del equipo y la dirección IP.

Sin periféricos En este modo, no hay ninguna pila de interfaz de usuario disponible y las aplicaciones no son interactivas. Las aplicaciones en modo "sin periféricos" se pueden considerar servicios.

Circuitos inter-integrados (I2C) Sencillos buses bidireccionales de datos en serie (SDA) y reloj en serie (SCL) de dos cables para el control de circuitos inter-integrados. Puede usar el espacio de nombres Windows.Devices.I2c en la aplicación para comunicarse con un dispositivo a través de I2C.

Diodo emisor de luz (LED) Un LED es una fuente de luz semiconductora de dos electrodos. Es un diodo de unión PN que emite luz cuando se activa.

Marco de controlador en modo kernel (KMDF) de Microsoft Windows Marco de desarrollo de Microsoft que permite a los desarrolladores de controladores exponer la funcionalidad del controlador en modo kernel, lo que permite al controlador acceder a la memoria y el hardware del sistema.

Prototipo El desarrollo de una versión más básica de una versión final del dispositivo que se pretende crear. Se recomienda encarecidamente la creación de prototipos, cuando no es un paso obligatorio del proceso de fabricación. Esta fase se debe usar para probar todas las características que espera usar para la versión final del dispositivo.

Glosario de Windows IoT.

Fuente: docs.microsoft.com


ponte a prueba

¿Cuáles de las siguientes características debería contemplar una guía didáctica?

- a) Guía de referencia rápida, errores y sus soluciones y capturas de pantalla.
- b) Nivel de los conceptos alto y capturas de pantalla, pensado solo para expertos.
- c) Bibliografía, guía de errores y soluciones y guía de referencia rápida.
- d) Capturas de pantalla y bibliografía.

6.2. INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS Y APLICACIONES. LICENCIAS DE CLIENTE Y LICENCIAS DE SERVIDOR

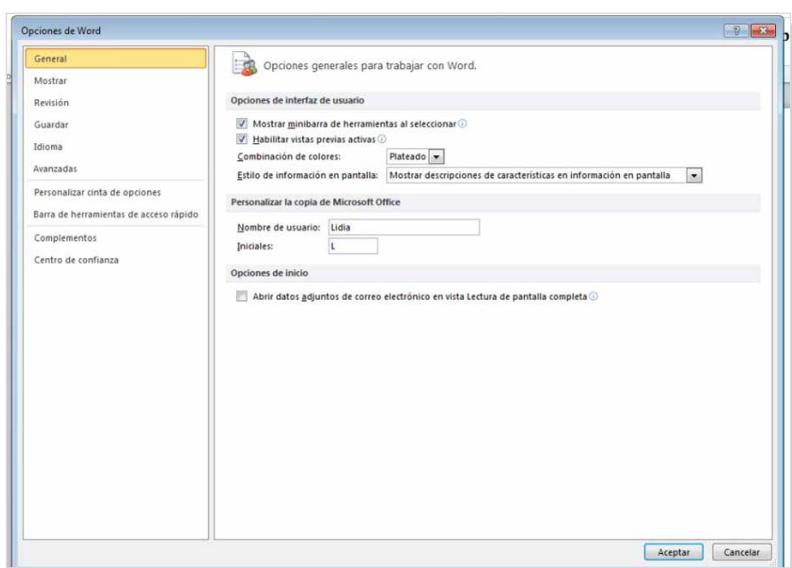
Cada usuario (o cada grupo) requerirá un sistema y unas aplicaciones específicas. Como administradores, debemos estar seguros de que todos ellos tienen acceso solamente al software que necesitan. También debemos asegurarnos de que este y su configuración cubren sus necesidades.

Para agregar o quitar aplicaciones, en Linux podemos recurrir al Centro de Software de Ubuntu y en Windows, al Panel de Control. En este último sistema, los archivos con extensión .exe abren los asistentes de instalación.



Instalación de una aplicación en Windows.

Tras la instalación debemos completarla, en la medida de lo posible, a través de la personalización que necesite cada usuario.



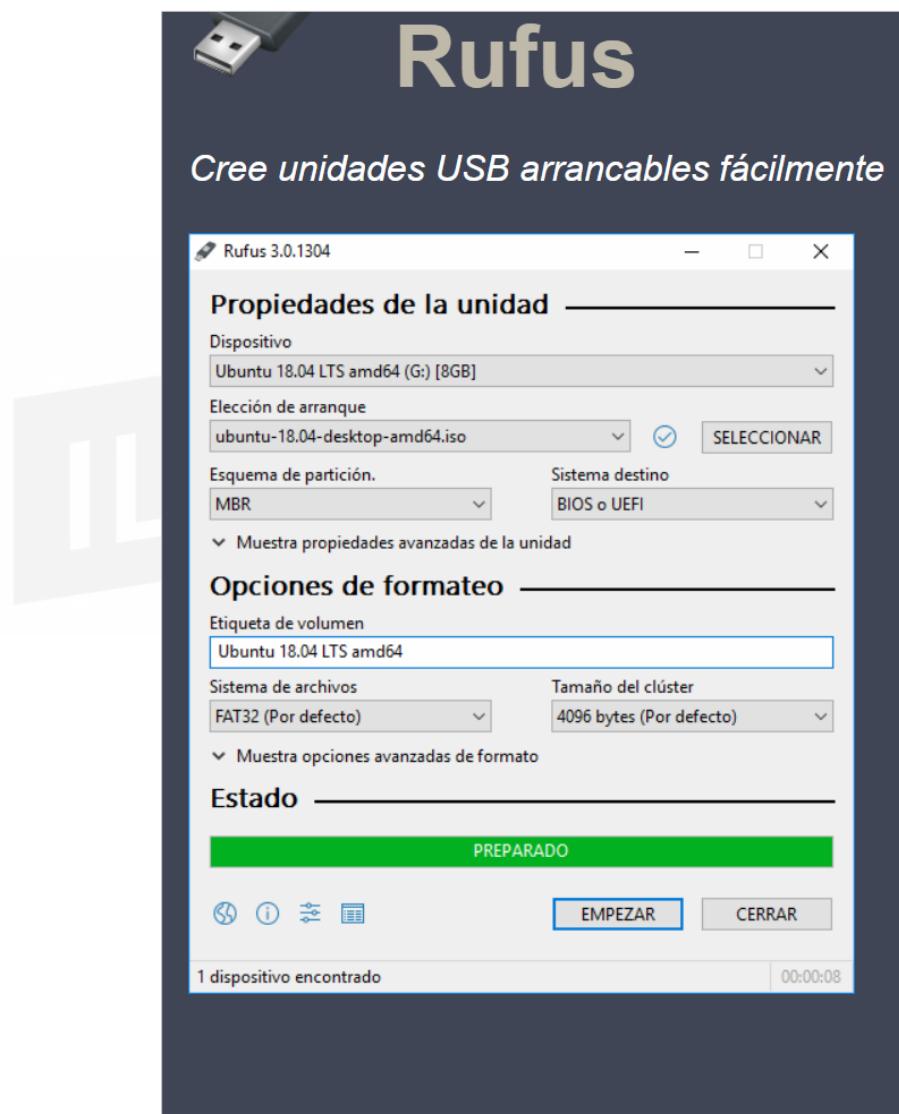
Configuración de una aplicación en Windows.

En el caso del sistema operativo, la instalación posee sus propias características:

Arranque desde el disco o pendrive de instalación

Con toda probabilidad, para iniciarla insertaremos un disco óptico o un pendrive en el ordenador. Una vez insertado, reiniciaremos el ordenador para que arranque desde el soporte elegido.

Programas como Nero BurningRoom, Daemon Tools, Rufus, Linux live u otros de este tipo pueden ayudarnos a crear discos o pendrive de instalación.

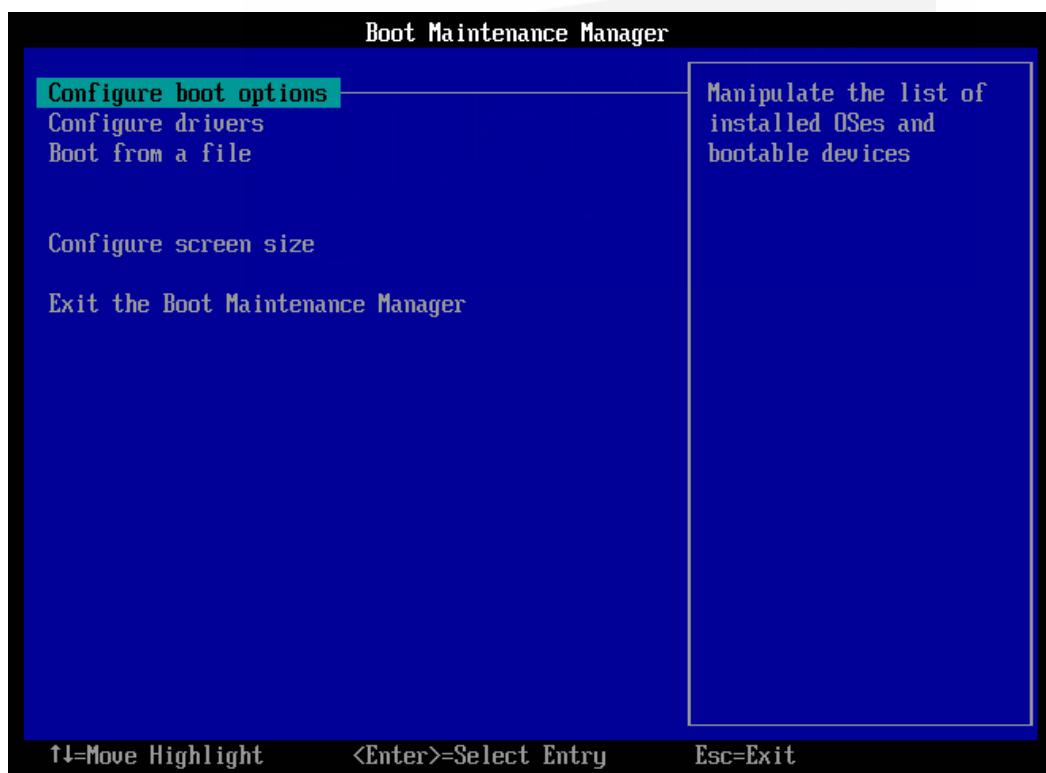


Actualmente, el recurso más utilizado para realizar las instalaciones es el pendrive o disco externo de instalación, debido a que muchos ordenadores portátiles no disponen de lector de discos para aliviar su tamaño y peso. Junto con las mejoras en las velocidades de transmisión de datos por USB, están dejando los discos (CD/DVD) obsoletos.

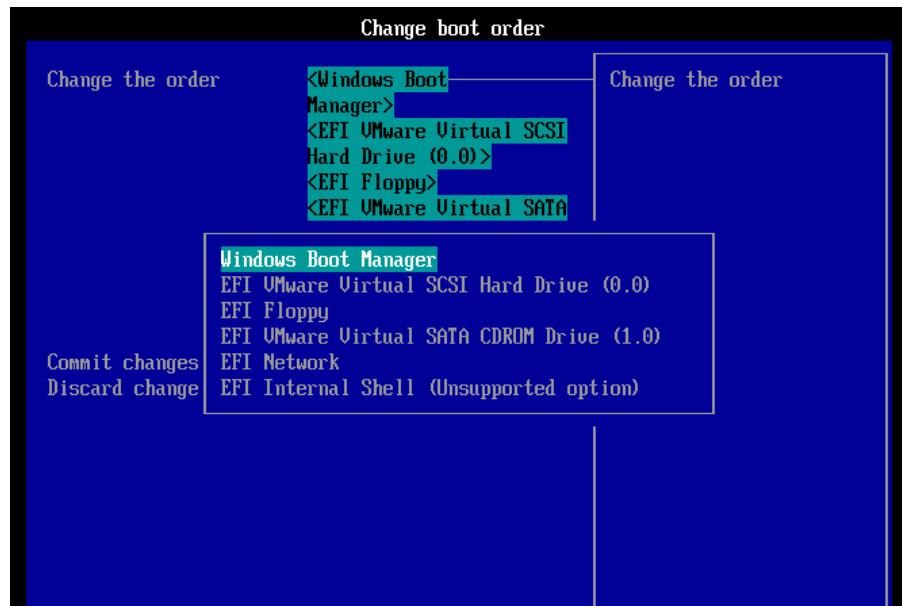


BIOS // UEFIBIOS

Para ello, previamente, tendremos que entrar en la BIOS o UEFIBIOS (según la placa base) del ordenador para cerciorarnos de que se da prioridad de arranque al soporte elegido sobre las demás unidades.



En determinadas placas base también encontramos la opción de modificar el dispositivo de arranque sin acceder a la BIOS, de tal forma que solo se utilizará esa vez, ya que, en el caso de la BIOS los cambios son permanentes y una vez instalado el sistema deberemos volver a modificar el dispositivo predeterminado para indicar que sea el disco duro.



Cada placa base tendrá sus configuraciones para los temas de arranque y en estas podremos ver las posibilidades que nos ofrece.



Los procesos de instalación de sistemas operativos y aplicaciones pueden resultar muy costosos si necesitamos llevarlos a cabo en un sinfín de equipos. Para facilitarnos la tarea, contamos con la alternativa de la instalación desatendida. En breve la analizaremos con detenimiento.

Por último, en el primer apartado hemos visto hasta qué punto son importantes las licencias. En los casos de software que se ofrece en versiones de cliente y de servidor es preciso tener claro cuál precisamos, pues sus características y su precio suelen variar entre sí.

6.3. INSTALACIONES DESATENDIDAS E IMPLEMENTACIÓN DE ARCHIVOS DE RESPUESTA

Si necesitamos instalar el sistema y otras aplicaciones en multitud de equipos, las instalaciones desatendidas representan una excelente opción.

Se trata de instalaciones que no nos solicitan que vayamos eligiendo opciones. Por el contrario, basta con unos pocos clics iniciales y la introducción de algún parámetro al principio para que la instalación se inicie y no pare hasta completarse.

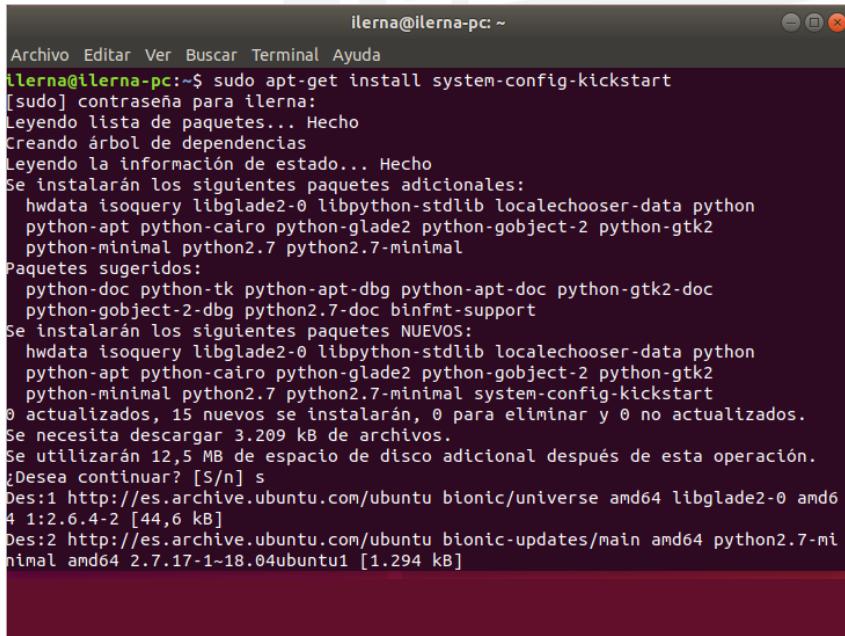
Para crear instalaciones desatendidas, contamos principalmente con dos opciones:

Crear la instalación desatendida a partir del propio software

Determinados sistemas y aplicaciones ofrecen esta posibilidad. Es el caso de Ubuntu, donde para crear la instalación podemos utilizar Kickstart.

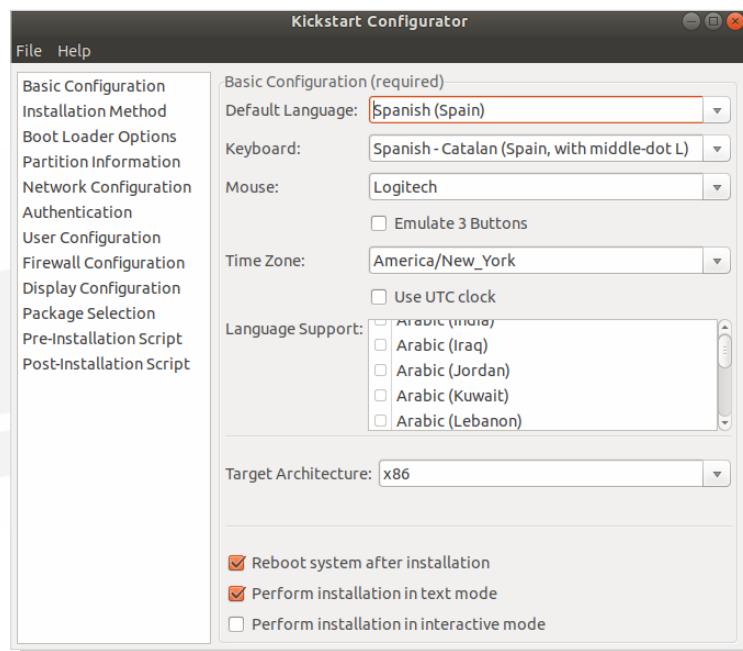
En primer lugar, lo añadimos tecleando:

"sudo apt-get install system-config-kickstart"



```
ilerna@ilerna-pc: ~
Archivo Editar Ver Buscar Terminal Ayuda
ilerna@ilerna-pc:~$ sudo apt-get install system-config-kickstart
[sudo] contraseña para ilerna:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  hwd Data isoquery libglade2-0 libpython-stdlib localechooser-data python
  python-apt python-cairo python-glade2 python-gobject-2 python-gtk2
  python-minimal python2.7 python2.7-minimal
Paquetes sugeridos:
  python-doc python-tk python-apt-dbg python-apt-doc python-gtk2-doc
  python-gobject-2-dbg python2.7-doc binfmt-support
Se instalarán los siguientes paquetes NUEVOS:
  hwd Data isoquery libglade2-0 libpython-stdlib localechooser-data python
  python-apt python-cairo python-glade2 python-gobject-2 python-gtk2
  python-minimal python2.7 python2.7-minimal system-config-kickstart
0 actualizados, 15 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 3.209 kB de archivos.
Se utilizarán 12,5 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Peso:1 http://es.archive.ubuntu.com/ubuntu bionic/universe amd64 libglade2-0 amd6
4 1:2.6.4-2 [44,6 kB]
Peso:2 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7-mi
nimal amd64 2.7.17-1~18.04ubuntu1 [1.294 kB]
```

Seguidamente, el programa figurará en *Herramientas* y a través de él podremos configurar las opciones de idioma, zona horaria y los demás detalles de la instalación en función de nuestros usuarios.



Crear una imagen de disco a partir de un sistema configurado

Otra práctica común es la de instalar y configurar a la perfección el sistema y las aplicaciones en un único equipo. Hecho esto, podemos replicar todos los contenidos del disco duro de dicho equipo en un pendrive, en un DVD o en una unidad de red.

A partir del pendrive, del DVD o la unidad de red podremos obtener copias idénticas al disco duro original volcando toda la información en otros equipos de manera desatendida.

Para realizar los procesos aquí descritos podemos emplear aplicaciones como Macrium Reflect.

Los **archivos de respuesta** son ficheros que contienen definiciones y valores de configuración y se utilizan como guía durante la instalación.

En Windows, por ejemplo, son archivos con extensión *.xml* y, en ellos, se pueden especificar diversas opciones que van desde cómo crear las particiones de disco, hasta cómo se realizará la configuración de pantalla o los favoritos de internet. Dichos archivos acostumbran a estar etiquetados como *unattend.xml*.

En Windows 8, por ejemplo, podemos usar archivos de respuesta con la herramienta Sysprep y también con la herramienta *Administración y mantenimiento de imágenes de implementación* (DISM).

ponte a prueba

¿Cuál de las siguientes opciones es un software válido para crear instalaciones desatendidas en Ubuntu?

- a) Kickstart
- b) InstallDes
- c) Brasero
- d) Wine

Las instalaciones desatendidas siempre tendrán que ser basadas en un sistema operativo nuevo y limpio (sin software instalado), ya que este tipo de instalación no permite generar una copia de un sistema con programas instalados.

- a) Verdadero
- b) Falso



6.4. SERVIDORES DE ACTUALIZACIONES AUTOMÁTICAS

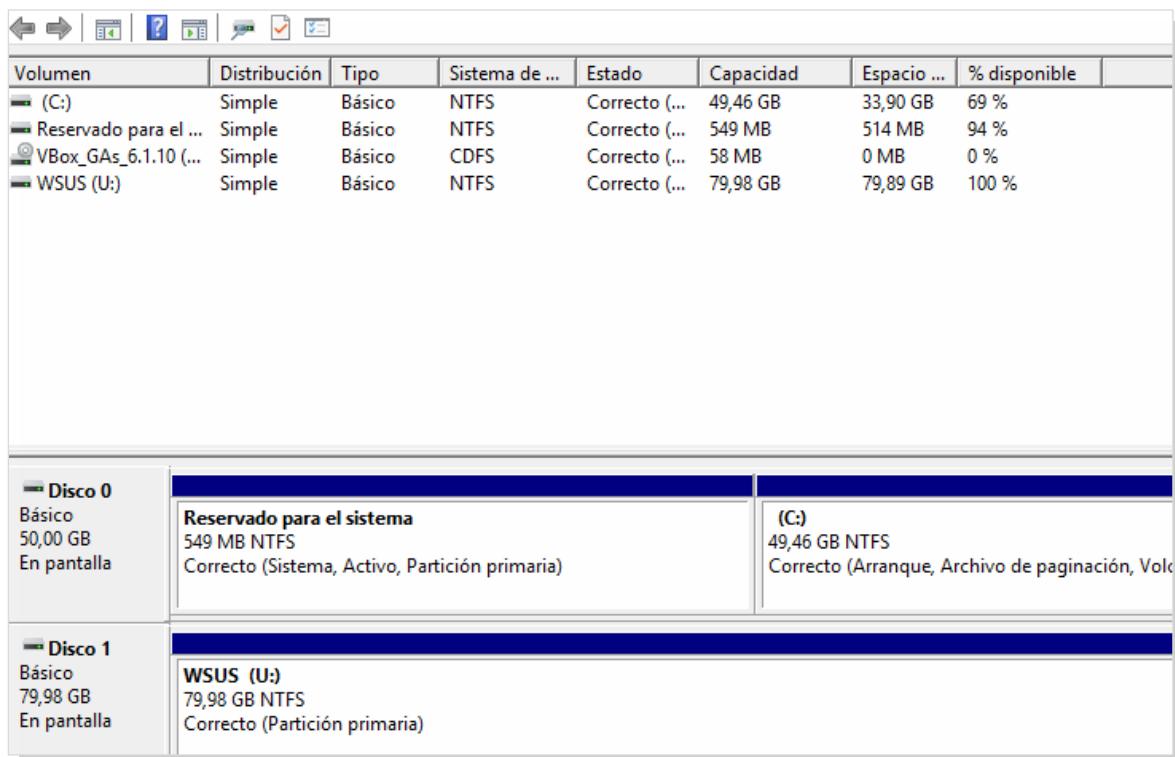
En el primer capítulo hemos visto la importancia de mantener actualizado el sistema operativo y las aplicaciones. Y es que, si como administradores de red no gestionamos las actualizaciones, las consecuencias pueden ser indeseadas.

Imaginemos que tenemos habilitada una red de cien ordenadores. Si programamos las actualizaciones automáticas para que estén activas y todos ellos se conectan y se ponen a descargarlas a la vez, la red podría llegar a colapsarse.

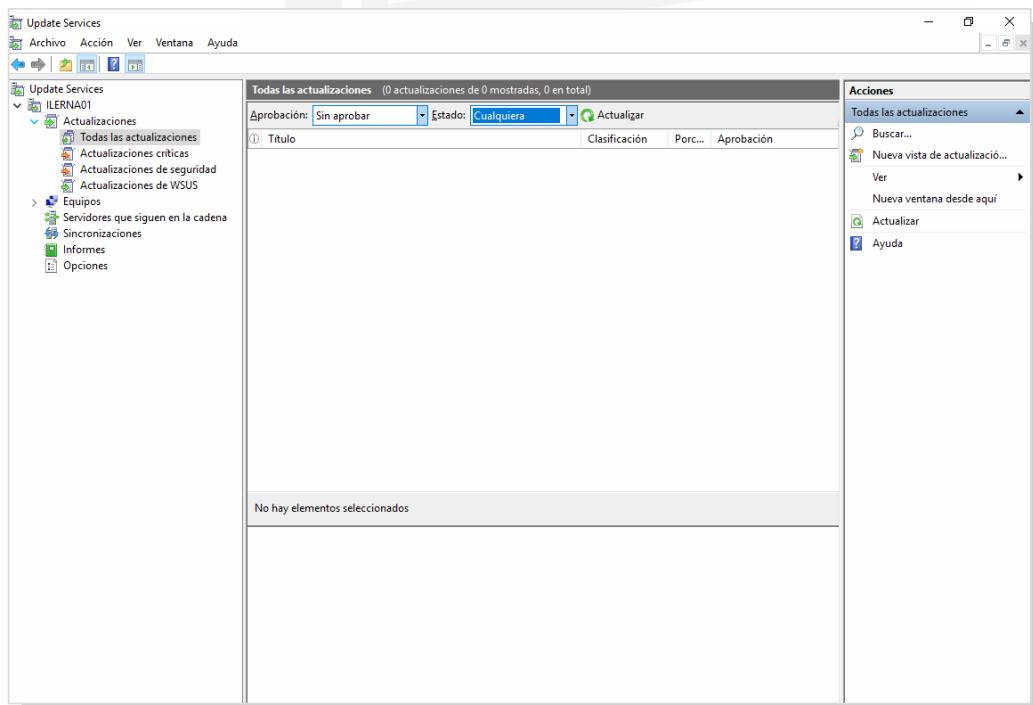
Para evitar que esto suceda, resulta más que recomendable instalar un servidor de actualizaciones. Gracias a este software, un solo equipo o unos pocos de ellos descargarán las actualizaciones. Posteriormente, el resto de los equipos del dominio accederán a ellas de forma local.

Un buen ejemplo de software ideado con este fin es Windows Server Update Services.

Para instalar este servicio debemos contar con un servidor con Windows Server donde podemos instalar el rol que nos permitirá realizar este servicio con el servidor elegido.

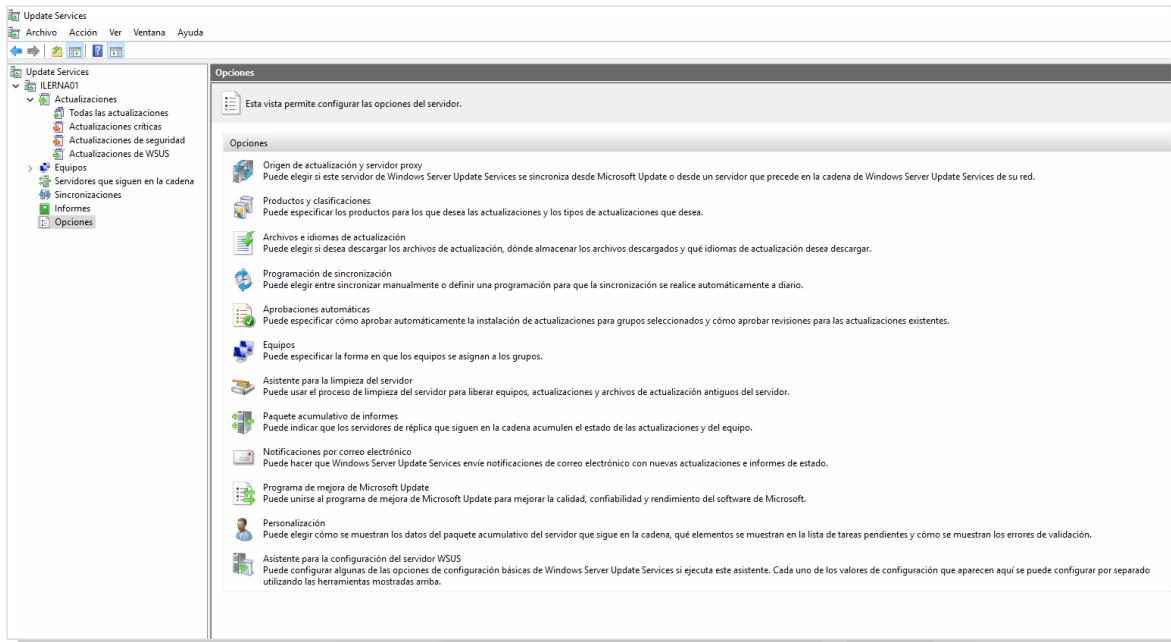


La instalación de este rol requiere un espacio de almacenamiento en un disco duro para almacenar las descargas de las actualizaciones. En este caso debemos tener en cuenta el tamaño y velocidad del disco, ya que este funcionará como almacén de consulta para los demás equipos de la red.



En la configuración del rol es donde podemos gestionar todos sus parámetros para que este proceso se pueda realizar sin colapsar la red de trabajo. En este punto es donde

configuraremos las horas en que queremos llevar a cabo el proceso de actualización y la forma de hacerla. Además, podemos gestionar el tipo de descarga de la instalación, pudiendo descartar instalaciones como las de Service Pack, que pueden ser más costosas y llevar cambios importantes en los equipos.



Cabe destacar que en sistemas operativos Windows como el del ejemplo, podemos encontrar herramientas para ver reportes y estadísticas de este servicio (<https://www.microsoft.com/es-es/download/details.aspx?id=45496>).

6.5. PARTES DE INCIDENCIAS Y PROTOCOLOS DE ACTUACIÓN

Entendemos por incidencias aquellos eventos que no forman parte de las operaciones habituales de los servicios, tanto de red como locales.

Estas pueden provocar ralentizaciones e incluso interrupciones en el ritmo de trabajo de la empresa u organización. Por lo que debemos contemplar dos necesidades vitales:

- **Reanudación de los servicios:** en primer lugar, debemos restaurar las operaciones lo más rápidamente posible para minimizar el impacto de la incidencia en la empresa u organización.
- **Prevención de futuras incidencias:** por otra parte, tenemos que poner en marcha mecanismos y herramientas para evitar, en la medida de lo posible, que la incidencia se vuelva a producir.

Llegados a este punto, podemos señalar **dos grupos** de incidencias:

- **Incidencias conocidas:** si una incidencia específica coincide con problemas habituales, buscaremos una solución temporal mientras indagamos sobre una medida definitiva. Es importante aplicarla inmediatamente.
- **Incidencias desconocidas:** si una incidencia no se ha producido con anterioridad, hay que registrarla.

Para el registro de incidencias y prevención de futuros fallos es fundamental que los usuarios y los colaboradores realicen partes. De este modo, podemos detectar y contar con un listado de incidencias que nos ayuden a solventarlas y prevenirlas.

Una vez hayamos recopilado las incidencias, los pasos serán los siguientes:

1. Clasificación de incidencias
2. Investigación, posibles diagnósticos y soluciones
3. Resolución de la incidencia y restablecimiento del servicio
4. La incidencia es archivada para futura referencia

Para una correcta gestión de las incidencias es fundamental contar con tanta información como sea posible. Así pues, el parte puede recoger datos tan significativos como los siguientes:

- **Fecha y hora de la incidencia**
- **Equipo físico en el que se ha producido**
- **Software y hardware instalado en el equipo**

A partir de ahí, debemos contar con un protocolo que dicte qué medidas tomar y qué debemos elaborar a partir de las experiencias previas.

Para generar la documentación de las incidencias podemos encontrar varios métodos, aunque, en este caso, destacaremos dos de ellos.

Incidencias en documentos

Las incidencias en documentos son utilizadas en entornos pequeños, con pocos usuarios y equipos, donde la gestión de esta infraestructura de red es más liviana.

No hay una aplicación o formato del documento fijo, aunque hay que recopilar, como mínimo, la información que hemos comentado anteriormente. Esta puede almacenarse con formatos diferentes.

Habitualmente se utilizan programas que facilitan la inserción y consulta de estos datos como, por ejemplo, la aplicación Microsoft Excel.

Nombre equipo	SER01	SER02
Instalación	12/05/2018	06/08/2019
Sistema Operativo	Windows Server 16	Windows Server 19
Versión	Datacenter	Datacenter
Arquitectura	x64	x64
IP1	192.168.1.10	192.168.1.11
MAC1	08-06-00-07-EC	08-88-00-17-AW
IP2		
MAC2		
IP3		
MAC3		
IP4		
MAC4		
CPU	intel i7	intel i5
RAM (gb)	32	16
RAM (tipo)	DDR4	DDR4
HDD1	150gb	1T
HDD1 (tipo)	SDD	SATA 3
HDD2	2 T	2T
HDD2 (tipo)	SATA 3	SATA 3
HDD3		
HDD3 (tipo)		
HDD4		
HDD4 (tipo)		

Servers Equipo cliente Hardware Técnicos +

Este tipo de aplicaciones son muy utilizadas para estos tipos de gestión, ya que nos permiten almacenar datos. Se pueden duplicar con gran facilidad y nos ofrecen diferentes herramientas para agilizar procesos repetitivos.

PARTES INCIDENCIAS														
Nombre equipo	Usuario	Sistema Operativo	Versión	Arquitectura	IP	MAC	CPU	RAM (gb)	RAM (tipo)	HDD1	HDD2	Responsable		
PC001	Pablo	Windows 10	Pro	x64	192.168.1.31	08-00-27-05-82-EB	i7	16	SATA 3			Marta García		
Resolución														
Incidencia														
El cargador de la máquina no funciona correctamente.							12/10/2019						El conector de la placa ha sido reparado ya que no conectaba de forma correcta	12/10/2019
PC002	Marta	Windows 10	Pro	x64	192.168.1.65	01-00-CC-08-82-EB	i7	8	DDR4	SDD		Pablo Pérez		
Resolución														
Incidencia														
Las licencias de Software de mis usuarios se están a punto de caducar y se necesita instalar nuevas aplicaciones.							25/11/2019						La máquina ha sido actualizada con nuevas aplicaciones con licencia informadas en el apartado de aplicaciones disponibles en la máquina.	28/11/2019
PC025	Martin	Windows 10	Pro	x64	192.168.1.84	48-00-27-EE-82-EE	i7	16	DDR4	SDD MM2		José García		
Resolución														
Incidencia														
Se necesitaría ampliar la capacidad de almacenamiento de la máquina para almacenar máquinas virtuales							05/04/2020						Se ha modificado el PC quitando la disquetera disponible para poner un disco de 2T SATA3 como almacenamiento interno de la máquina, el proceso ha sido informado en las	15/04/2020
PC033	Laura	Windows 10	Pro	x64	192.168.1.55	00-00-22-11-82-BB	i3	8	DDR4			Marta García		
Resolución														
Incidencia														
El ordenador hace mucho ruido.							09/07/2020						IDE SATA 1 SATA 2 PCI SOD SOD MM2	09/07/2020

Incidencias en aplicaciones

Las incidencias son gestionadas por aplicaciones en entornos grandes, donde la cantidad de máquinas y usuarios dentro de la red necesita ser gestionados para un correcto desempeño de sus funciones.

Hoy en día encontramos una gran variedad de aplicaciones de este tipo, tanto en aspecto web como en aplicaciones propias de escritorio, que debemos instalar en las máquinas.

Estas aplicaciones son un canal de comunicación entre los usuarios y los técnicos responsables, de tal modo que conseguimos transmitir la incidencia que se está produciendo en ese momento y almacenarla en sistemas de bases de datos para poder consultar esos datos.

Nueva petición

Proyecto * Helpdesk

Tipo * Incidencias

Asunto *

Descripción

Estado * Preautorización

Prioridad * Normal

Ficheros Elegir archivos Ningún archivo seleccionado (Tamaño máximo: 5 MB)

Crear Crear y continuar Previsualizar

La gran ventaja de este tipo de métodos es la escalabilidad que nos ofrecen las aplicaciones, pudiendo, de una forma muy sencilla, solventar la comunicación entre diferentes departamentos de una misma infraestructura y la gran recopilación de datos que podemos generar para obtener reportes de estos de una forma muy sencilla y visual.

6.6. ADMINISTRACIÓN REMOTA

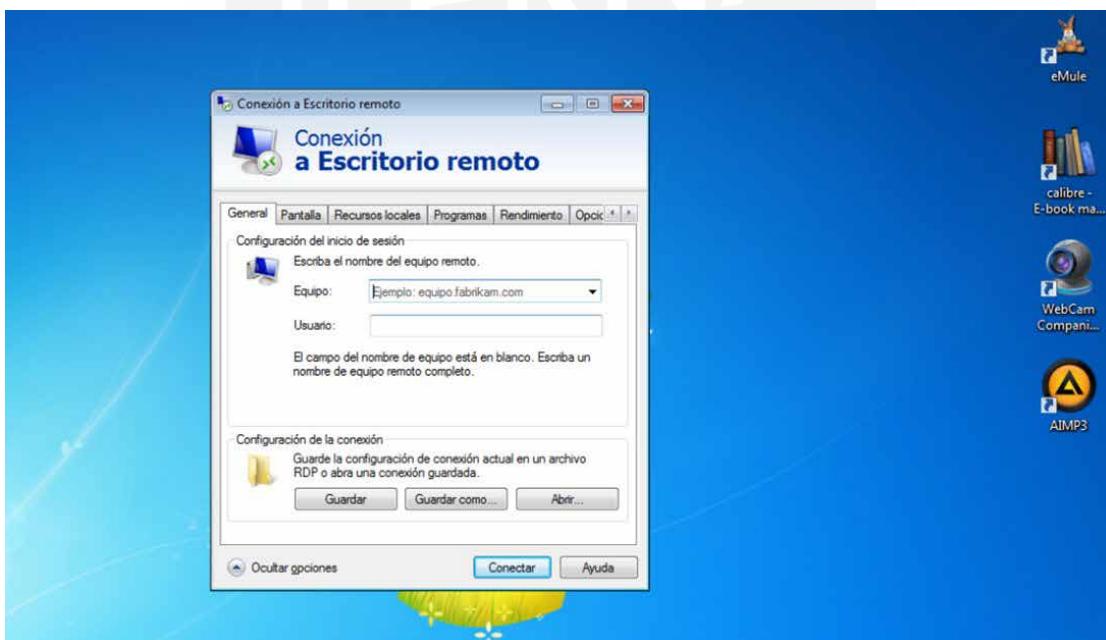
A menudo, tendremos que sentarnos frente a los equipos cliente para solventar incidencias y prestar asistencia a sus usuarios. Sin embargo, es posible que estos se encuentren en otro edificio, en otra ciudad o incluso en otro país.

Una descripción de los problemas vía telefónica tal vez no ayude a que nos hagamos una idea clara de qué está sucediendo al otro lado del cable y, a veces, desplazarnos físicamente para examinar el ordenador puede resultar muy costoso o inviable.

En tales casos, podemos utilizar herramientas de administración remota. Gracias a ellas, podemos tomar el control remoto de un ordenador a través de la conexión de red y solventar sus incidencias.

El administrador o la persona encargada de prestar asistencia ejecutará el software para tomar el control. En los clientes, a su vez, tendremos un servicio o aplicación que se va a ejecutar automáticamente cada vez que el sistema arranque. De modo que todo el equipo permanecerá siempre accesible remotamente.

Windows, sin ir más lejos, brinda herramientas de asistencia remota bajo el nombre de *Conexión a escritorio remoto*.



"Conexión a escritorio remoto" nos brinda la opción de trabajar remotamente con otro ordenador de la red como si estuviéramos frente a él.

No obstante, existen otras alternativas en este ámbito, desarrolladas por terceros como **TeamViewer**. Gracias a ella resulta relativamente sencillo llevar a cabo una administración remota entre sistemas Windows y Linux.



TeamViewer ofrece administración remota para Windows, Mac OS X y Linux.

Otra de las herramientas de asistencia más prácticas es UltraVNC (<http://www.uvnc.com/>), un programa de control remoto que también permite trabajar a través de la red local.

Está desarrollado en régimen de software libre y podemos visualizar el escritorio de otro ordenador y trabajar con él en todas sus facetas: desplegar el menú *Inicio*, ejecutar aplicaciones, editar documentos y, en definitiva, realizar todo tipo de operaciones.

Si en vez de optar por la instalación completa (*Full installation*) escogemos la personalizada, comprobaremos que nos encontramos frente a un paquete compuesto por dos aplicaciones independientes: un *Server* y un *Viewer*.

- **Server:** el primer paquete, el de servidor, es aquel que debemos agregar al equipo que deseamos controlar.
- **Viewer:** el segundo, el del visualizador, debe añadirse al ordenador desde el que deseamos ejercer el control remoto.

Así pues, en primer lugar, instalaremos UltraVNC Server en los ordenadores en red. Durante el proceso, se nos brindará la opción de descargar ficheros adicionales para Vista (*Download Vista addons files*) y un controlador que mejorará el rendimiento en sistemas operativos como Vista o Windows XP (*Download the mirror driver*). Si estamos

utilizando Windows 10 en ambos ordenadores, desmarcamos ambas opciones, pues no supondrá ninguna ventaja.

Por último, para que el software quede ejecutándose permanentemente en segundo plano y tomar sus riendas en cualquier momento, debemos agregarlo como servicio.

Tras completar el proceso, **ejecutaremos UltraVNC Server en el equipo que deseemos controlar** y lo configuraremos para que se ejecute automáticamente siempre que arranque.

Una vez hecho esto, ya podemos instalar el visualizador (UltraVNC Viewer) en el ordenador desde el que deseamos ejercer el control.

Otras herramientas interesantes para gestión remota si deseamos trabajar en modo texto son las siguientes:

- **SSH**: sus siglas corresponden a *Secure Shell*, es decir, *intérprete de órdenes seguro*. Puede descargarse desde www.openssh.com.
- **Putty**: otro software excelente dedicado a este fin. Puede descargarse desde www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

ponte a prueba

¿Cuál de las siguientes opciones son programas útiles para realizar administración remota?

- a) TeamViewer, Ultra VNC y Putty
- b) ConP2p, Putty y Gimp
- c) AR WP2, TeamViewer y Putty
- d) Gimp, Ultra VNC y ConP2p

BIBLIOGRAFÍA / WEBGRAFÍA

- ☒ Francisco Javier Muñoz, Juan Ignacio Benítez, Ángel Lozano (2005). *Sistemas Operativos en entornos Monousuario y Multiusuario*. Aravaca, Madrid.
- ☒ M.ª Jesús Ramos, Alicia Ramos, Sebastián Rubio (2005). *Instalación y mantenimiento de equipos informáticos*. Aravaca, Madrid.
- ☒ José Luis Raya Cabrera, Laura Raya González. (2011). *Sistemas Informáticos*. Grupo Editorial Ra-Ma.
- ☒ Isabel M.ª Jiménez Cumbreiras. (2017). *Sistemas Informáticos*. Garceta.
- ☒ Carlos Pes. *Recursos de Informática para Ciclos Formativos de Grado Superior*. Google Sites. Sitio web: <https://sites.google.com/site/carlospesrivas/recursos/informatica-ciclos-formativos-de-grado-superior>



solucionario

1.1. Estructura y componentes de un sistema informático. Periféricos y adaptadores para la conexión de dispositivos

¿Cuáles de las siguientes fases forman el ciclo de instrucción?

b) Fase de búsqueda y fase de ejecución.

La memoria principal es conocida como memoria central o memoria RAM.

a) Verdadero.

La memoria RAM es la memoria principal del sistema informático con la que gestionaremos todas las peticiones del sistema a la CPU.

1.2. Tipos y topologías de red

¿De qué tipo es una red de conexión bluetooth?

a) PAN.

1.3. Mapa físico y lógico de la red

El mapa lógico de la red nos mostrará una representación gráfica real de la situación de los componentes de la red dentro de un determinado espacio.

b) Falso.

El mapa lógico nos mostrará información sobre la red y sus aspectos internos, como las direcciones de los elementos, el grupo de los equipos, etc. La situación real de los elementos nos lo mostrará el mapa físico.

1.5. Funciones del sistema operativo

¿Cuáles de las siguientes opciones son funciones que desempeña un sistema operativo?

a) Administración de procesos, administración de recursos, administración de la memoria y recuperación de errores.

1.8. Licencias y tipos de licencias

¿Qué tipos de licencias se pueden adquirir de forma gratuita y con permisos para su redistribución?

d) Freeware y software libre.

1.10. Máquinas virtuales

Las máquinas virtuales nos permiten incrementar el hardware instalado en una máquina de forma que podremos mejorar

las prestaciones de un sistema informático e instalar más sistemas operativos en este.

b) Falso.

Las máquinas virtuales trabajarán con el hardware del que disponga el sistema informático y en ningún caso incrementará sus las prestaciones.

1.12. Instalación de sistemas operativos. Requisitos, versiones y licencias

¿En qué tipo de partición instalaremos un sistema operativo?

a) Primaria.

1.14. Actualización de sistemas operativos y aplicaciones

Tener el sistema operativo actualizado a sus últimas versiones mejorará y perfilará sus funcionalidades y nos ofrecerá una mayor seguridad.

a) Verdadero.

1.16. Registros del sistema

Para un funcionamiento óptimo de los registros, debemos realizar regularmente un mantenimiento y limpieza de estos.

a) Verdadero.

2.1. Administración de usuarios y grupos locales

En un sistema Linux, podemos representar los diferentes permisos con 9 caracteres que se dividen en grupos de tres caracteres. ¿A qué hace referencia el primer grupo de tres caracteres (empezando por la izquierda)?

a) El propietario de fichero.

2.3. Seguridad de contraseñas

En las cuentas de usuario de administrador, la seguridad en las contraseñas es muy importante. ¿Qué características deberíamos aplicar en las contraseñas para ofrecer una mayor seguridad?

b) Usar 8 caracteres como mínimo, no usar términos obvios, renovar la contraseña periódicamente y usar diferentes símbolos.

solucionario

2.4. Configuración del protocolo TCP/IP. Direcciones IP y máscaras de subred

¿Qué clase de red tiene como mascara el valor 255.255.0.0?

b) Clase B.

En las direcciones de clase A, ¿cuántos bloques de enteros de 4 bytes dedicaremos a identificar los equipos?

d) 3.

2.6. Archivos de configuración de red

¿En qué directorio de Linux encontraremos la configuración de la red?

a) etc/network/interfaces.

2.8. Principales comandos

¿Qué información muestra el comando “dir” en Windows?

a) Mostrar el contenido del directorio.

¿Qué acción realiza la palabra reservada “ls” en una sentencia de comandos en Linux?

a) Mostrar el contenido del directorio.

3.2. Tipos de sistemas de archivos

¿Qué sistema de archivos utiliza Windows 10?

b) NTFS.

Los directorios o también conocidos como ficheros son conjuntos de datos ordenados en los que almacenamos información.

b) Falso.

Los directorios o carpetas nos ofrecen la posibilidad de clasificar los datos, es decir, los archivos, y poner orden en el sistema.

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

¿Cuál de las siguientes opciones es utilizada como comando para desplazarnos por los directorios del sistema?

b) cd.

3.5. Estructura de directorios de sistemas operativos libres y propietarios

¿En qué carpeta del sistema almacena un sistema operativo Windows la instalación de los programas que tenga instalados?

b) Archivos de programa.

3.9. Montaje y desmontaje de dispositivos en sistemas operativos

¿Cuáles de las siguientes opciones son herramientas que nos brinda el sistema operativo Windows?

a) Administración de equipos, administrador de discos y programador de tareas.

El monitor de rendimiento de Windows permite generar informes a partir de los cuales es posible elaborar estadísticas.

a) Verdadero.

3.11. Herramientas de administración de discos. Particiones y volúmenes. Desfragmentación y revisión

Una unidad física de disco no se puede dividir en varias particiones, sino que siempre se verá como una sola partición completa y para obtener más particiones necesitaremos más discos.

b) Falso.

Una unidad física de disco puede dividirse en varias particiones. Cada partición puede tener su propio sistema de ficheros.

Los sistemas de ficheros están sometidos a constantes procesos de creación, borrado y modificación de archivos que, a la larga, provocará que los ficheros se fragmenten y surjan huecos sin información en nuestras particiones.

a) Verdadero.

La desfragmentación de discos es un proceso que elimina espacios de memoria vacíos que han sido utilizados con anterioridad.

4.1. Estructura cliente–servidor

¿En una estructura cliente-servidor quién proporciona los servicios?

b) El servidor.

solucionario

4.2. Protocolo LDAP

¿Cuál de las siguientes opciones agrupa las características que nos ofrece el protocolo LDAP?

- a) Acreditación de usuarios, búsqueda de datos, centralización de la información y posibilidad de replicar la base de datos.

4.4. Conceptos clave de Active Directory

¿Qué son las unidades organizativas en Active Directory?

- a) Contenedores de objetos que permiten organizarlos jerárquicamente en subgrupos dentro del dominio.

4.5. Administración de cuentas. Cuentas predeterminadas

En servicios de administración de usuarios como Active Directory de Windows, podemos generar diferentes usuarios para un dominio y asignarles diferentes permisos y roles de usuarios para obtener un mayor control dentro de la red.

- a) Verdadero.

4.9. Plantillas de usuario. Variables de entorno

Las variables de entorno nos permiten definir características comunes que podremos aplicar a diferentes usuarios.

- a) Verdadero.

¿Cuál de las siguientes opciones son variables de entorno (por defecto) en un sistema operativo Windows?

- a) %TMP%.

5.1. Equipos de dominio

Los recursos lógicos son elementos administrados por el dominio.

- a) Verdadero.

En un dominio no tenemos la posibilidad de administrar servicios como FTP o correo electrónico, donde necesitaremos obligatoriamente equipos externos para la gestión de los servicios.

- b) Falso.

5.3. Administración del acceso a recursos.

Samba. NFS

Samba es un software de licencia comercial y suele implementarse en equipos Windows. Este ofrece la posibilidad de proporcionar servicios a clientes basados en sistemas operativos con licencia.

- b) Falso.

Samba es un programa de libre implementación y suele utilizarse en sistemas de tipo Unix. Los sistemas basados en Linux, como Ubuntu, ofrecen la posibilidad de instalar y utilizar este programa para conseguir proporcionar a clientes basados en Windows sus servicios.

¿Qué comando utilizaremos para gestionar los usuarios en Samba?

- a) smbpasswd.

5.7. Directivas de grupo. Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbito de las directivas. Plantillas

Las directivas de grupo se utilizan con mayor frecuencia en las redes de dimensiones modestas que en las grandes redes.

- a) Verdadero.

Las plantillas nos permiten asignar directivas más estrictas, aunque tienen como desventaja su aplicación individual, donde tienen que asignarse usuario a usuario y no pueden realizar una asignación en bloque.

- b) Falso.

Las plantillas nos permiten compendiar características que luego podremos asignar en bloque, esto facilitara el trabajo.

6.1. Interpretación, análisis y elaboración de documentación técnica. Interpretación, análisis y elaboración de manuales de instalación

¿Cuáles de las siguientes características debería contemplar una guía didáctica?

- a) Guía de referencia rápida, errores y sus soluciones y capturas de pantalla.



solucionario

6.3. Instalaciones desatendidas e implementación de archivos de respuesta

¿Cuál de las siguientes opciones es un software válido para crear instalaciones desatendidas en Ubuntu?

- a) Kickstart.

Las instalaciones desatendidas siempre tendrán que ser basadas en un sistema operativo nuevo y limpio (sin software instalado), ya que este tipo de instalación no permite generar una copia de un sistema con programas instalados.

- b) Falso.

Las instalaciones desatendidas se pueden realizar a partir de una imagen de disco de un sistema configurado, esto nos ahorrará tiempo en instalaciones repetitivas.

6.6. Administración remota

¿Cuál de las siguientes opciones son programas útiles para realizar administración remota?

- a) TeamViewer, Ultra VNC y Putty.