Módulo 1
Sistemas informáticos

UF1: Instalación, configuración y explotación del Sistema Informático

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 apartados:

- **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.

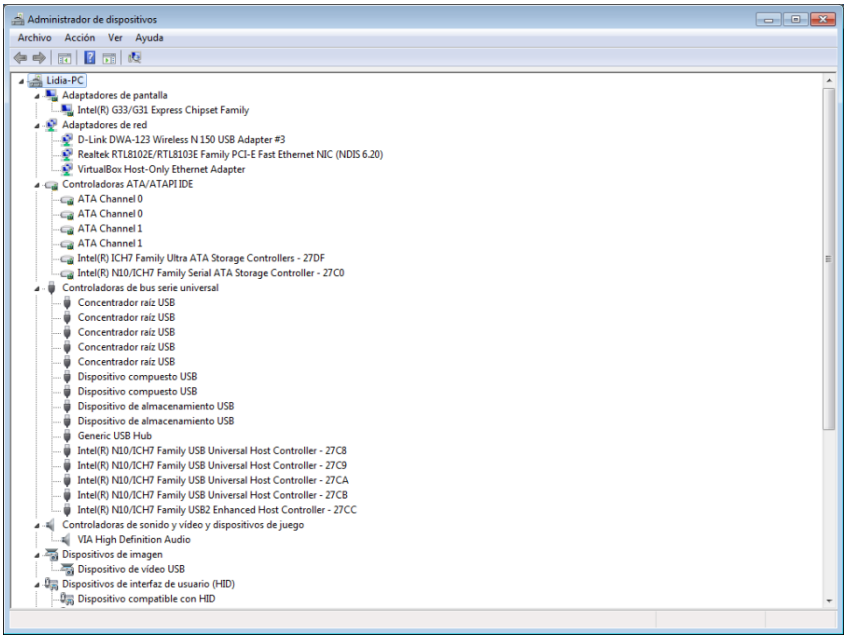
- **Conocer en profundidad el software**

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. Tipos de redes, cableado y conectores

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) que veremos a continuación:



- Caja
- Fuente de alimentación
- Placa madre
- CPU
- Disco duro
- Memoria RAM
- Tarjeta gráfica
- Tarjeta de sonido
- Tarjeta de red
- Unidades de almacenamiento adicionales (CD-ROM, discos secundarios, etcétera)
- Periféricos de entrada y salida (monitor, teclado, etcétera)

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, atendemos 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 formado 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)**

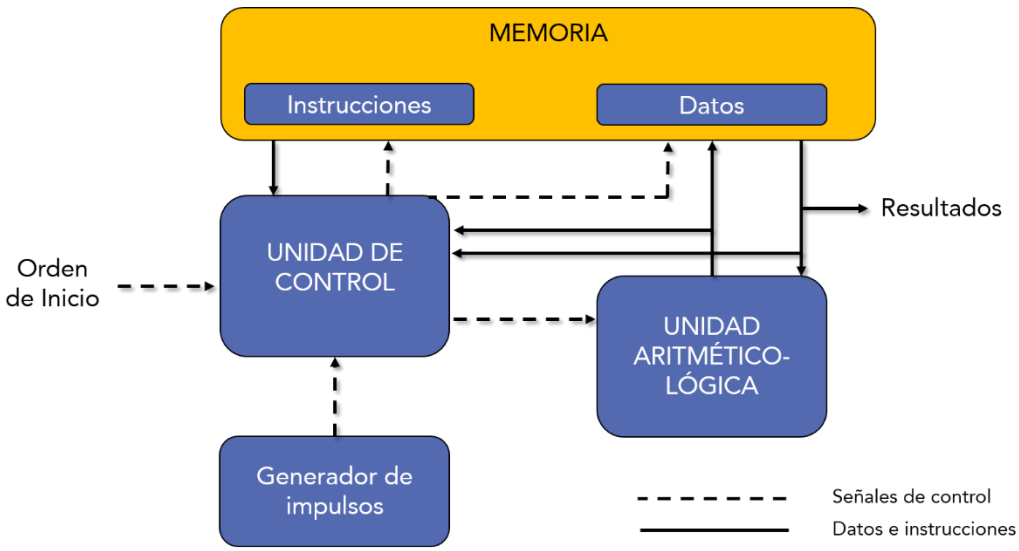
  Es la parte pensante del sistema informático. Su tarea fundamental es recibir información para interpretarla y procesarla mediante las órdenes que envía al resto de componentes del sistema.

- **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* o *or*-. Conforma uno de los tres bloques en los que se divide la CPU o unidad central de procesamiento central.

- **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 dispositivos. 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 unidades conectadas.

Funciones de un bus:

1. Soportar la información a transmitir.

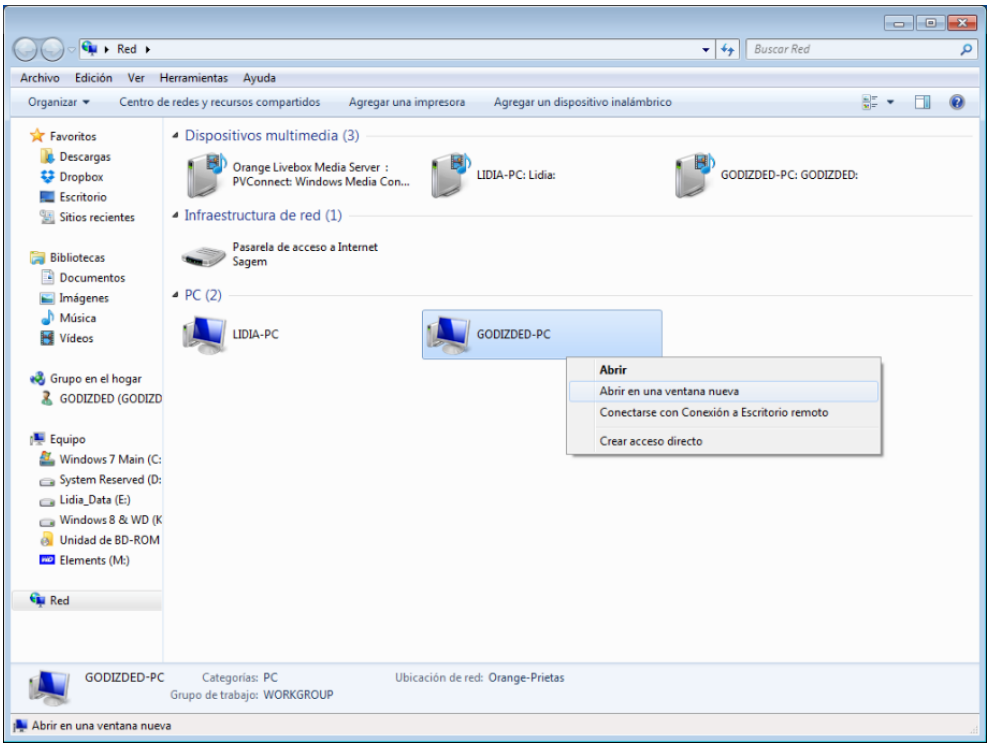
2. Garantizar la correcta comunicación entre los elementos que comparten el bus.

- **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 S.O. y de las aplicaciones.

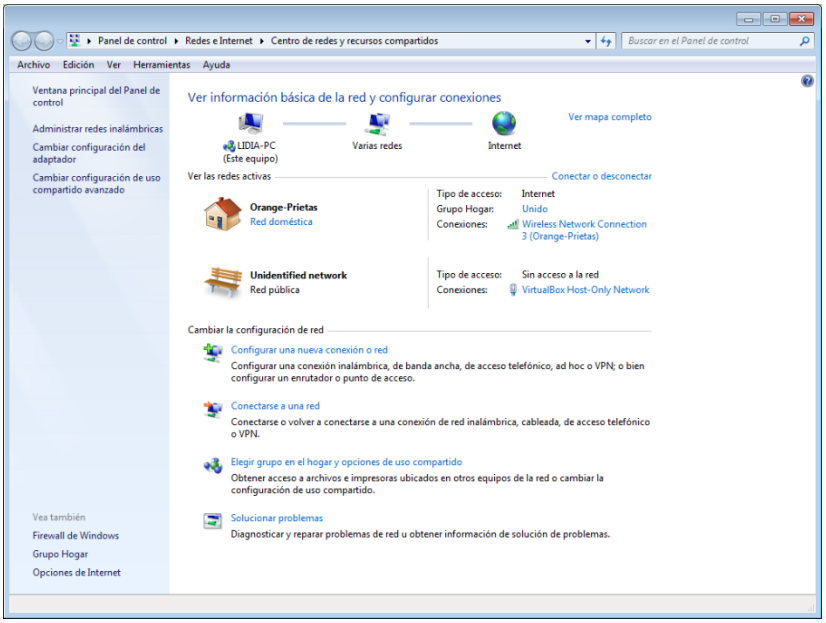
También se deberá tener en cuenta las características técnicas de la red que estemos empleando y su tipo de cableado.



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

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 Wi-Fi ha supuesto una revolución en este ámbito, pues nos permite habilitar redes sin necesidad de cablearlas físicamente.



La tecnología Wi-Fi nos permite habilitar redes sin necesidad de cablearlas físicamente.

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.

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 implementan tarjetas de red Wi-Fi 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 cabrá añadir a los usuarios (recursos humanos) y, por supuesto, la información.

1.2. 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 la estructura de la misma.

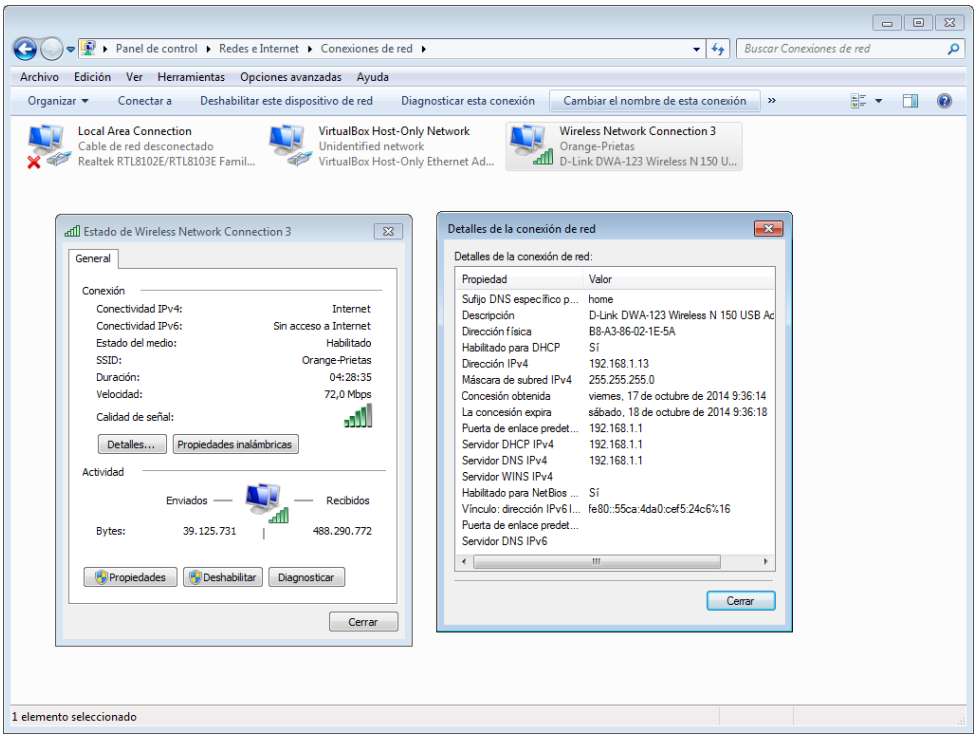
Dicha documentación deberá llevarse a cabo en dos frentes.

- **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 ser tenido en cuenta para garantizar que la señal de red llegue a cada equipo de la mejor forma posible.

- **Mapa lógico**

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



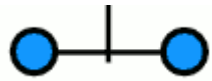
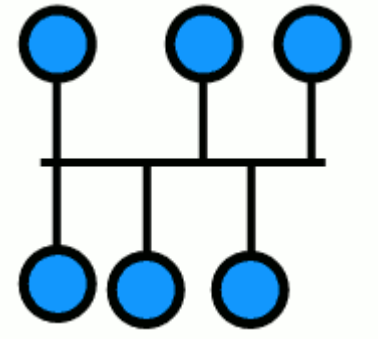
La dirección IP es uno de los datos que deberemos documentar a la hora de realizar un mapa físico de la red.

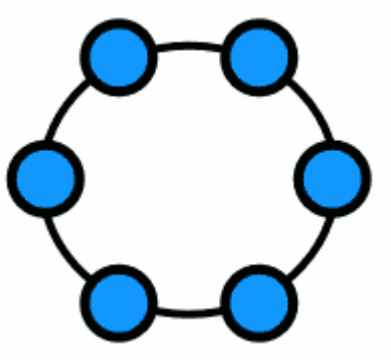
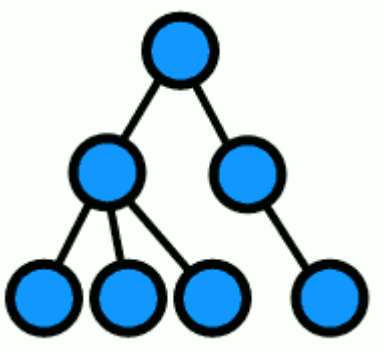
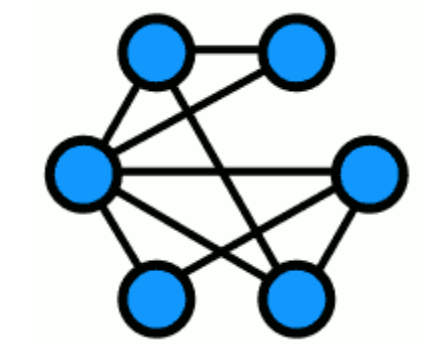
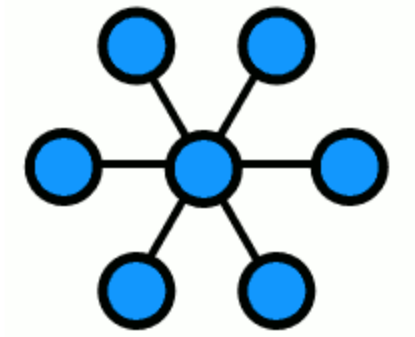
En lo referente a los tipos de redes, podemos establecer la siguiente clasificación:

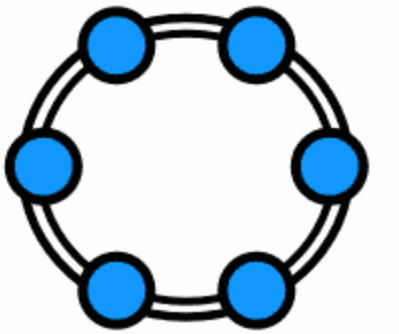
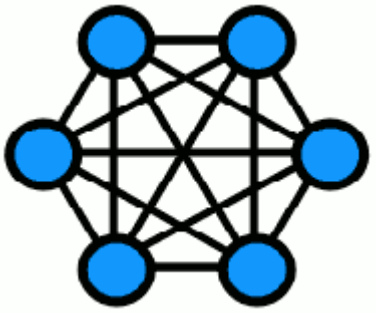
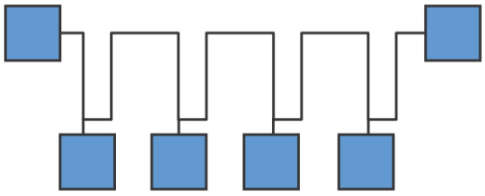
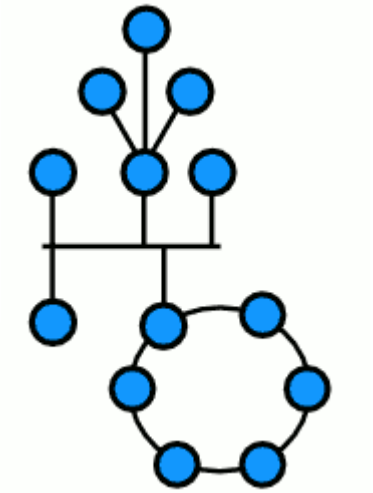
- **LAN.** Red de área local (*Local Area Network*) en la que uno o varios ordenadores están conectados entre sí, generalmente dentro de un mismo edificio. Permite compartir dispositivos de hardware, archivos, etc.
- **MAN.** Red de área metropolitana (*Metropolitan Area Network*) ubicada en una misma área geográfica, normalmente dentro de una misma ciudad. Utiliza dos buses unidireccionales independientes.
- **WAN.** Red de área amplia (*World Area Network*) que se expande por diversas áreas del mundo. Utiliza fibra óptica o satélites.
- **PAN.** Red de área personal (*Personal Area Network*) que su utiliza únicamente para uso personal y apenas cubre unos metros, como por ejemplo Por ejemplo, a través de una conexión Bluetooth.
- **WLAN.** Red LAN inalámbrica (*Wireless Local Area Network*) que transmite información de forma inalámbrica.

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.	
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.	
Estrella Los dispositivos están conectados siempre a un punto central y todas las comunicaciones se realizan a través de este nodo.	

Doble anillo Funciona igual que la topología en anillo. Además, posee un segundo anillo que conecta también todos los nodos.	
Totalmente conexa Cada nodo se conecta, a su vez, con todos los demás.	
Daisy chain Todos los nodos se encuentran conectados en cadena, de manera que el dispositivo 1 está conectado al 2, el 2 al 3 y así sucesivamente.	
Híbrida Combina varias de las anteriores.	

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, estas 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 encargada de que la información que se envía a la capa de aplicación pueda ser leída con éxito.
Sesión	Garantiza la comunicación entre dos puertos (*hosts)*.
Transporte	Transporta los datos del emisor hasta receptor.
Red	Responsable de que exista conectividad entre dos *hosts* diferentes.
Vínculo de datos	Acceso al medio.
Física	Transmite las señales.

1.3. Arquitectura de un sistema operativo

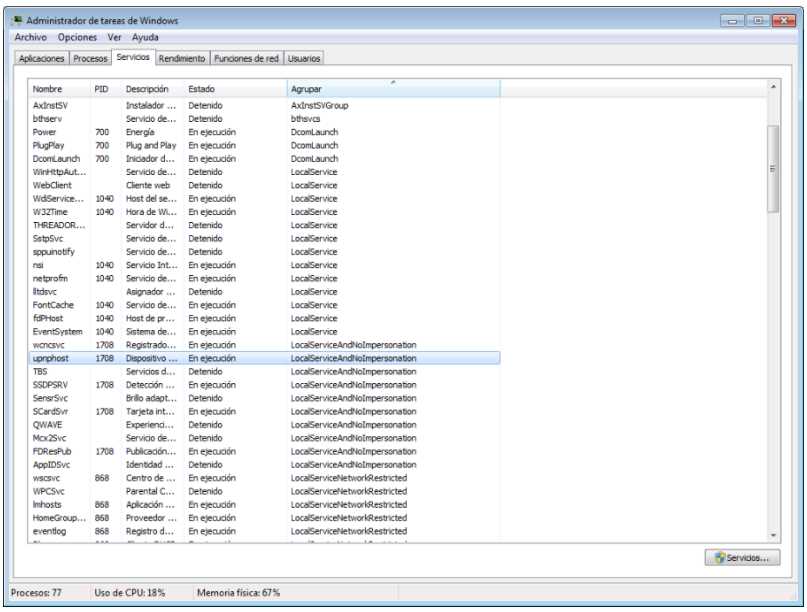
A lo largo de las últimas décadas los sistemas operativos han ido evolucionando de forma notable. Además, las consolas de tipo texto como DOS han dejado paso a interfaces más modernas de tipo gráfico como Windows o Mac OS X.

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 permanentemente ejecutándose en 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.



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.

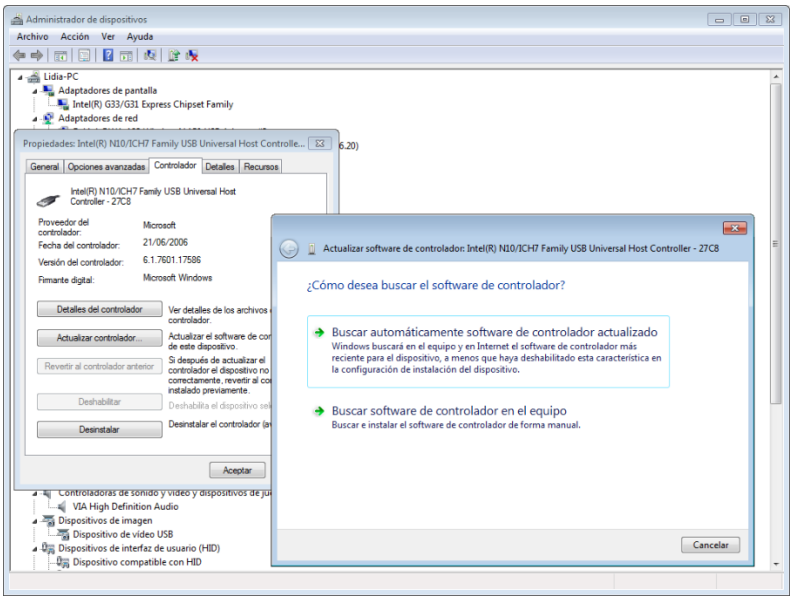
  Así, por ejemplo, mediante dichas llamadas el sistema puede efectuar operaciones básicas como abrir archivos, modificarlos, cerrarlos, etc. También puede efectuar instrucciones de entrada y salida para operaciones relacionadas con gráficos y sonido, comunicaciones, etc.

- **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.

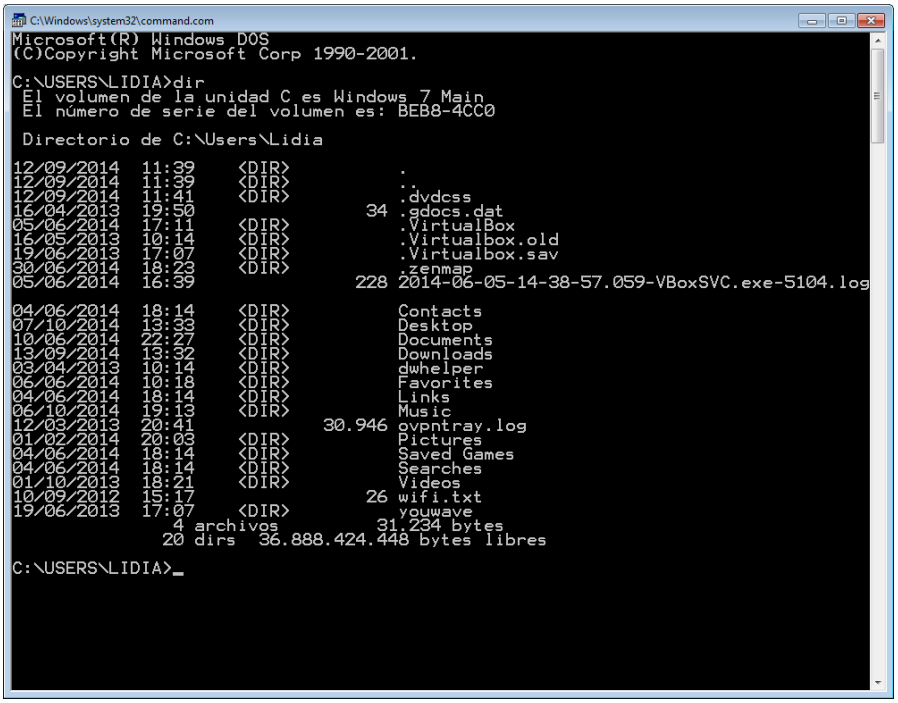
- **Controladores o *drivers***

  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 reciba. Para introducirlas podemos usar una interfaz gráfica o bien un intérprete de comandos tipo DOS.



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

1.4. 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:

- **Administración 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.

- **Administración 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**

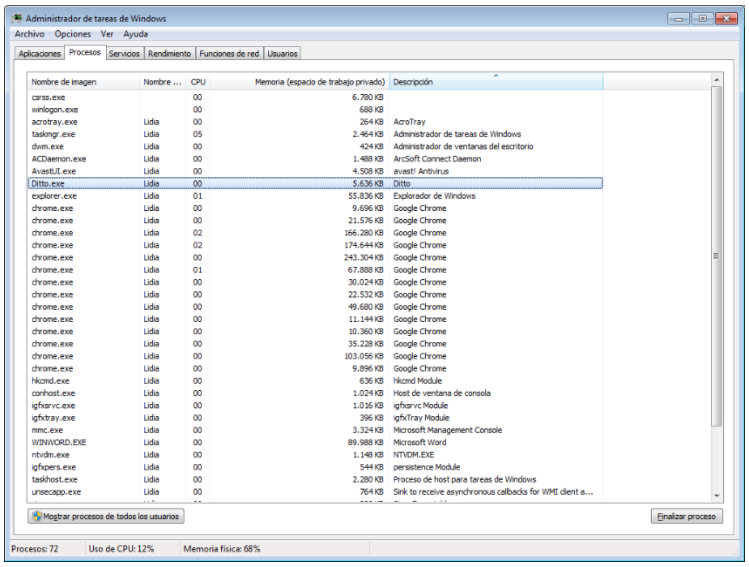
Supervisa qué áreas de memoria están en uso y cuáles están libres. Además, determina cuánta memoria asignará a un proceso y en qué momento. También libera la memoria cuando ya no es requerida para el proceso.

- **Recuperación de errores**

El sistema operativo contiene rutinas que intentan evitar perder el control de una tarea cuando se suscitan errores en la trasferencia 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*.

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.



1.5. 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:

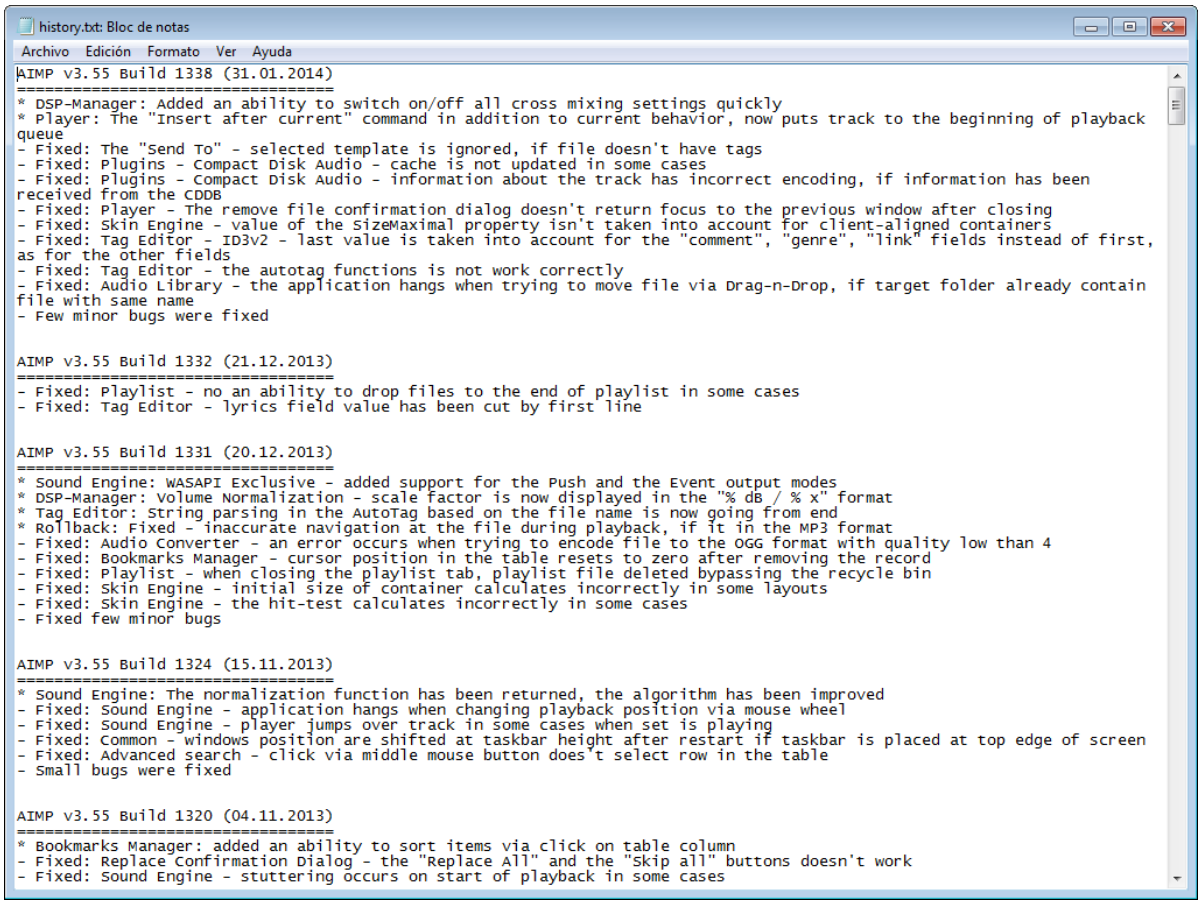
Según la cantidad de procesos que pueden gestionar, de forma simultánea	
Monotarea	- Solamente mantienen un proceso en ejecución. - Realiza tareas secuencialmente.
Multitarea	- Permite ejecutar varios procesos a la vez. - En algunos casos dos procesos pueden utilizar dos CPU diferentes.
Según el número 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.

1.6. Tipos de aplicaciones

Podríamos hacer una primera clasificación de aplicaciones en base a 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.



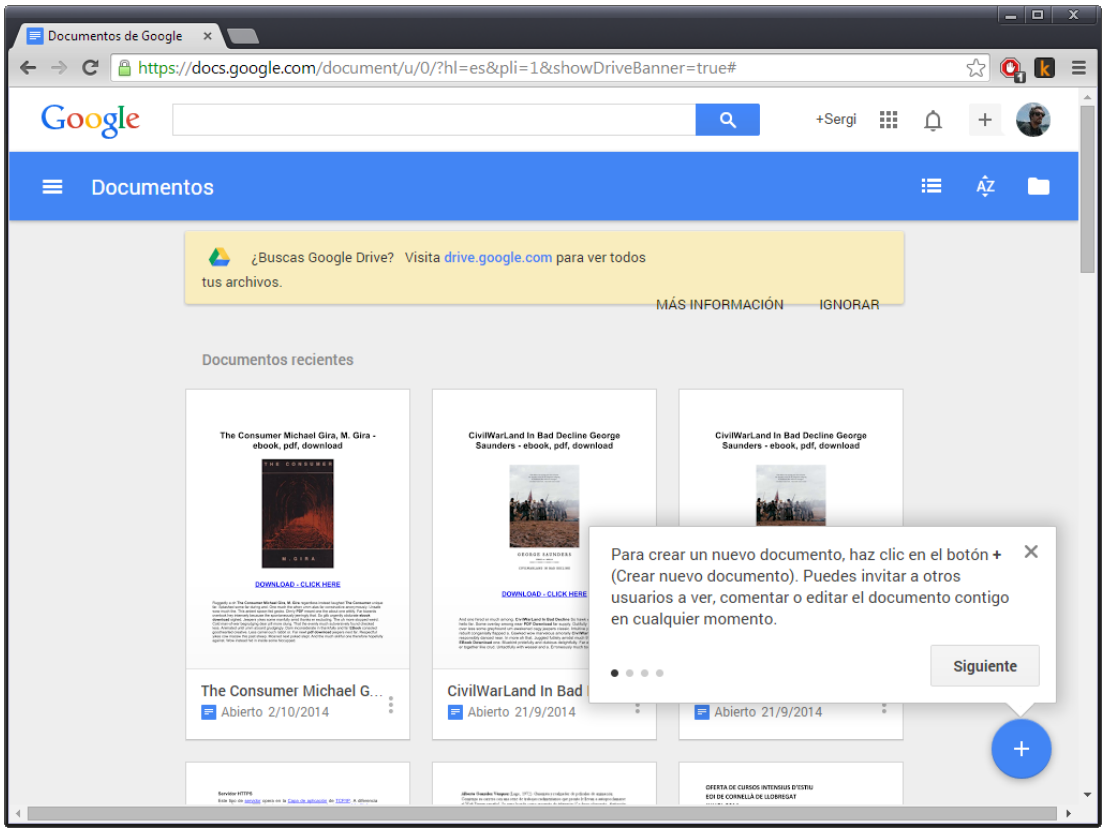
El famoso Bloc de notas de Windows es un buen ejemplo de aplicación local.

- **Aplicaciones en red**

  En este caso se ejecutan en un entorno de red local. En consecuencia, las aplicaciones suelen tener dos componentes: la primera se ejecuta de manera local y la segunda 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, estableceremos categorías como ofimática (Word, Excel, etc.), optimización del sistema (CCleaner, Defraggle, etc.), y así sucesivamente.

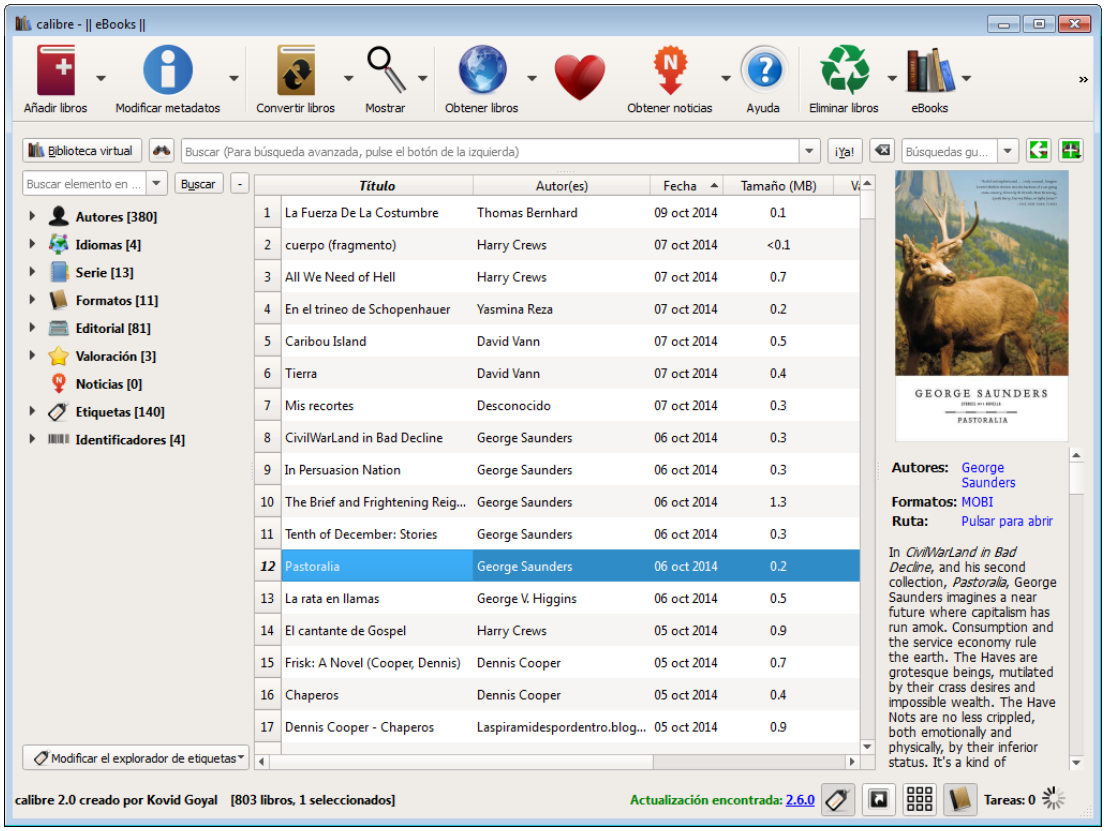
1.7. Licencias y tipos de licencias

A la hora de escoger el software de una aplicación o de un sistema operativo debemos tener muy presente la licencia bajo la que se distribuye.

Las licencias más frecuentes son las siguientes:

- **Licencia de software libre**

  El software distribuido bajo este régimen es gratuito y puede ejecutarse y distribuirse sin restricción. Gracias a que ofrece su código en abierto, los usuarios pueden estudiar su funcionamiento, adaptarlo a sus necesidades y mejorarlo. Después de modificarlo pueden ponerlo a disposición del público.



Aplicaciones como Calibre se distribuyen como software libre.

- **Licencia *freeware***

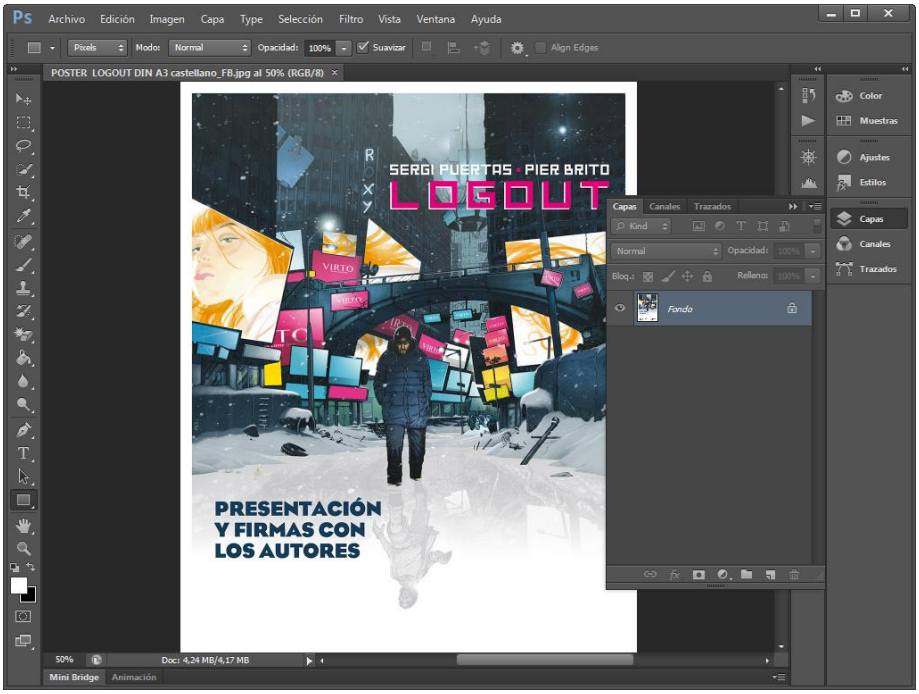
  El software que usa esta licencia también es gratuito y puede distribuirse sin restricción. La diferencia básica con el software libre es que no modificarse ya que su código fuente no es público.

- **Licencia *shareware***

  Se trata de software que puede redistribuirse gratuitamente, pero llegado cierto momento y tras un determinado período de uso, para poder utilizarlo se debe realizar un pago. A menudo tiene funcionalidades bloqueadas que no se desbloquearán hasta que dicho pago se haya efectuado.

- **Licencia comercial**

  Bajo esta licencia englobamos aquellos softwares desarrollados por individuos o empresas con el objetivo de ganar dinero. No se puede redistribuir y su utilización está sujeta al pago de la licencia.



Adobe Photoshop es un buen ejemplo de software comercial.

1.8. Gestores de arranque

Los gestores de arranque son programas muy básicos que, aunque no ofrecen las funcionalidades que nos brindan los sistemas operativos, resultan muy sencillos.

Su función es preparar los elementos más básicos que precisa el sistema operativo para funcionar y, a veces, nos brindan 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 permitirá elegir el que deseemos.

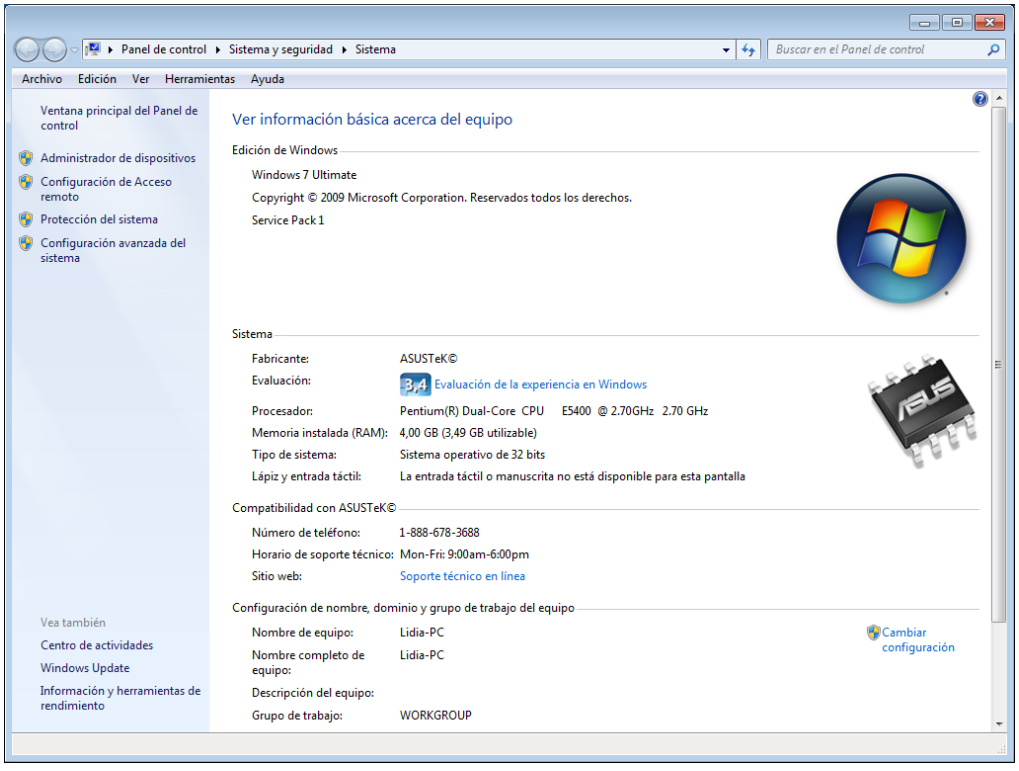
1.9. Consideraciones previas a la instalación de sistemas operativos libres y propietarios

Además del tipo de licencia del sistema operativo que elijamos, hay otra serie de factores que deberemos 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 nuestro siguiente apartado.



El procesador y la memoria RAM resultarán clave a la hora de garantizar que el sistema operativo se ejecute con fluidez.

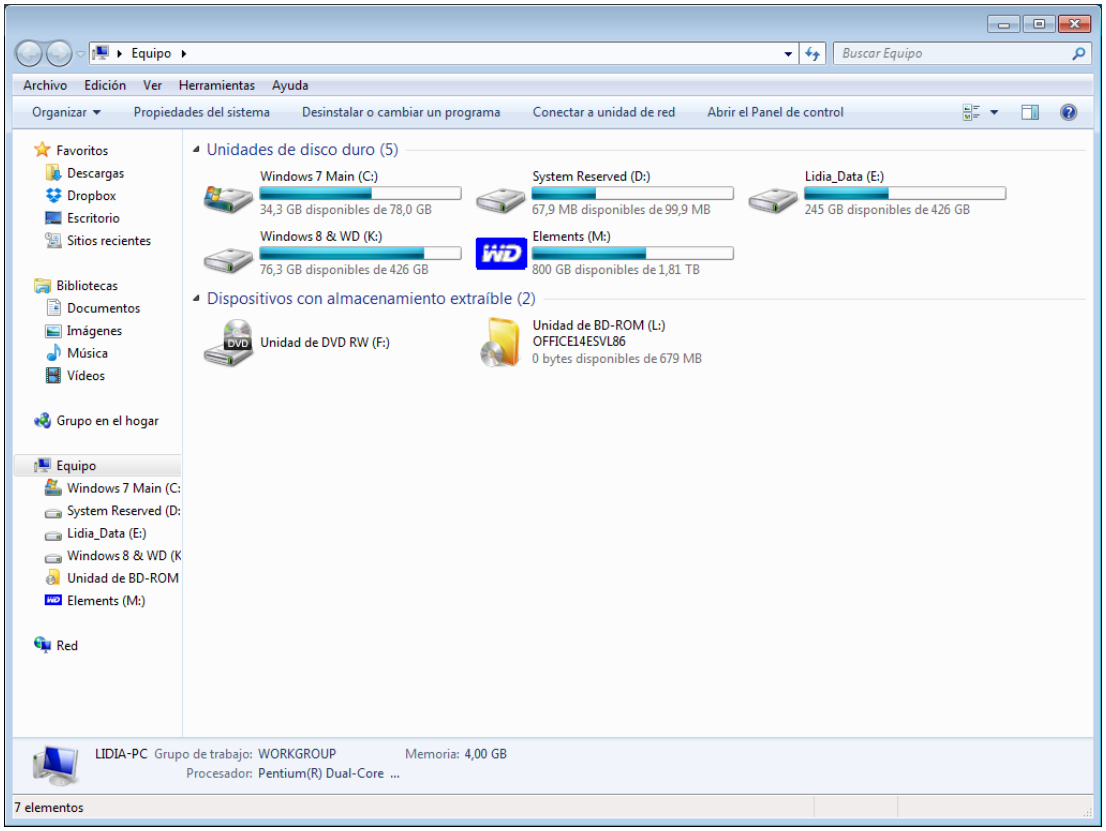
- **Medios desde los que llevaremos a cabo la instalación del sistema operativo**

  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**

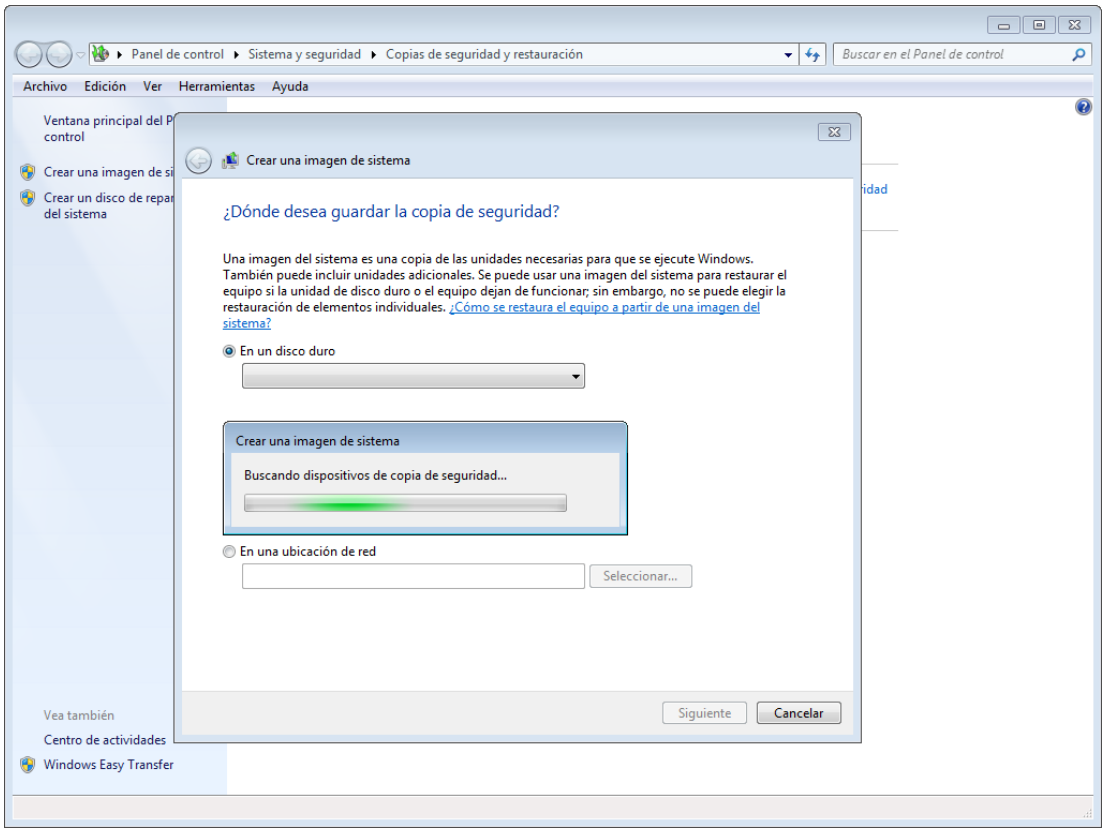
  ¿Qué disco o partición es la óptima para instalar el sistema? En líneas generales, siempre será el que brinde mayor rapidez en la lectura y escritura de datos.

  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.



Elegir adecuadamente la partición de destino del sistema operativo mejorará el rendimiento y nos ahorrará futuros quebraderos de cabeza.

Por otra parte, 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 los mismos.



Antes de instalar el sistema operativo en una partición, es vital realizar una copia de seguridad de la misma.

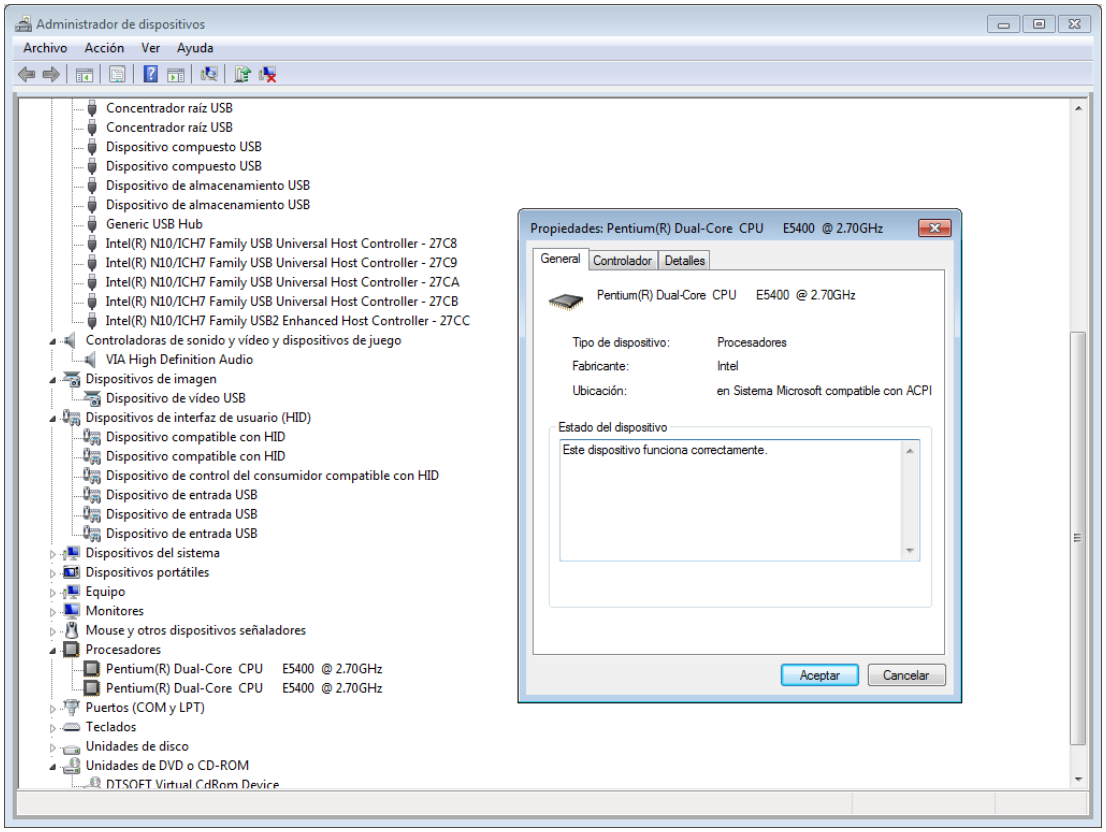
1.10. Instalación de sistemas operativos. Requisitos, versiones y licencias

Un sistema operativo es un programa que grabamos en el disco duro de nuestro ordenador y que, al iniciarse, se cargará una parte de él 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 que soporten su ejecución.

La inmensa mayoría de los sistemas operativos especifican unos requisitos mínimos que deberemos 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.).

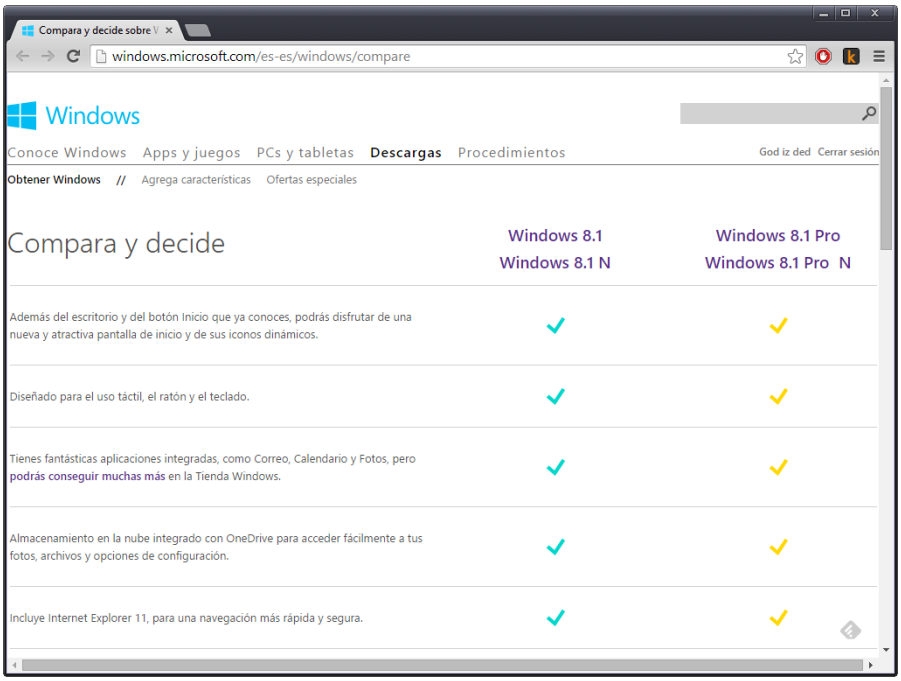


El Administrador de dispositivos nos ilustra acerca del tipo de CPU con el que está equipado nuestro ordenador.

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 contamos con la posibilidad de decantarnos por una versión más antigua del sistema operativo. Windows XP tendrá unos requisitos más bajos que Windows 8, por ejemplo.

Dado que sistemas como Windows ofrecen distintas modalidades, otro factor a considerar será qué modalidad precisamos. Así, por ejemplo, Windows 7 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 y así poder personalizar las funcionalidades del sistema operativo. Si por el contrario no 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 distintas funcionalidades.

Si vamos a instalar un sistema en régimen de propietario será imprescindible que adquiramos una licencia. Por norma general, cada versión precisará 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*** (http://www.vmware.com/es/products/workstation/).

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.
2. **Introducir el DVD** original en la bandeja.
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.

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, distingamos 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***.
10. Se **iniciará el proceso de instalación** de Windows 10 propiamente dicho. El sistema se reiniciará.
11. Definiremos un **nombre de usuario y de equipo** y pulsaremos en *Siguiente*.
12. Introduciremos la **clave de producto**.
13. Activaremos las **actualizaciones de seguridad**.
14. Definiremos la **fecha y hora** del sistema y la zona horaria.
15. 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. Configuraremos la BIOS para que **arranque desde el DVD o el pendrive.**
2. **Reiniciaremos el PC** con el DVD o el pendrive insertado.
3. Entraremos 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 iniciará el **asistente**. Elegiremos el idioma.
5. Confirmaremos que reunimos los requisitos mínimos de instalación pulsando en ***Continuar***.
6. Elegiremos si vamos a **descargar las actualizaciones del sistema** y otras características.
7. Definiremos las **particiones de disco**. Aquí se nos presentan tres opciones:
    - Eliminar el sistema operativo anterior e instalar.
    - Instalar Ubuntu conjuntamente con Windows.
    - Particionar el disco manualmente. Esta opción nos permite crear particiones, lo ideal es definir tres: En la partición *root*, instalaremos el sistema con un formato de archivos EXT4. En la partición *home* almacenaremos los documentos. La partición *swap* se usará para grabar archivos temporales cuando se acabe la memoria RAM.
8. Haremos clic en ***Instalar ahora***.
9. Definiremos la **zona horaria**.
10. Configuraremos el **teclado**.
11. Daremos de alta un **nombre de usuario y una contraseña**.

Con esto, accederemos al escritorio de Ubuntu.

Como hemos apuntado ya, contamos con la posibilidad de **instalar sistemas operativos en una máquina virtual**.

Veamos ahora cómo hacerlo en **VirtualBox**:

1. Descargaremos e instalaremos VirtualBox (https://www.virtualbox.org/).
2. **Ejecutaremos el software**: la interfaz de VirtualBox se divide en tres áreas: en la izquierda, aparecerán nuestras máquinas virtuales ya creadas. En la derecha, veremos el estado de nuestra máquina. El área superior nos permite controlar la máquina virtual.
3. **Crearemos la máquina virtual** pulsando en *Nueva*.
4. En el asistente, elegiremos el **sistema operativo** que vamos a instalar.
5. **Definiremos la memoria RAM** que le asignaremos al sistema operativo.
6. **Configuraremos el disco duro virtual**: establecemos su nombre, su tamaño y el resto de opciones. En este caso escogeremos Dinámico y así su tamaño irá aumentando conforme aumente el espacio que precisa la máquina virtual.
7. Haremos clic en ***Crear*** y la máquina virtual quedará creada y lista.
8. **Introduciremos el disco de instalación del sistema operativo**. En el menú de configuración entraremos en Almacenamiento y seleccionaremos la unidad escogida anteriormente.
9. **Iniciaremos la máquina** que hemos creado haciendo clic en el botón Iniciar. El proceso de instalación del sistema operativo dará comienzo.

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.

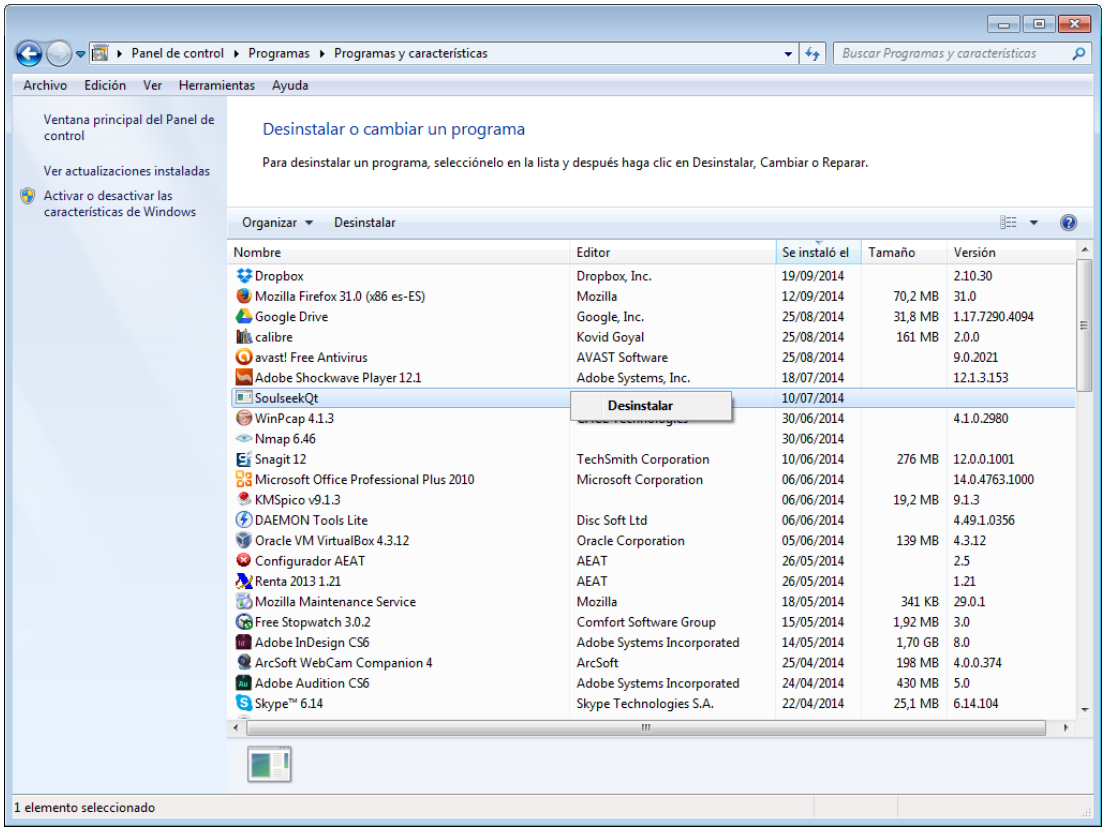
1.11. Instalación y desinstalación de aplicaciones. Requisitos, versiones y licencias

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 nuestro sistema operativo son aptos para la ejecución de las aplicaciones.
- **Versiones.** La versión más reciente, más completa y más 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.



El Panel de control nos brinda la posibilidad de agregar y eliminar aplicaciones de nuestro equipo.

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 ese 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 **Revo Uninstaller**.

http://www.revouninstaller.com/

1.12. 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:

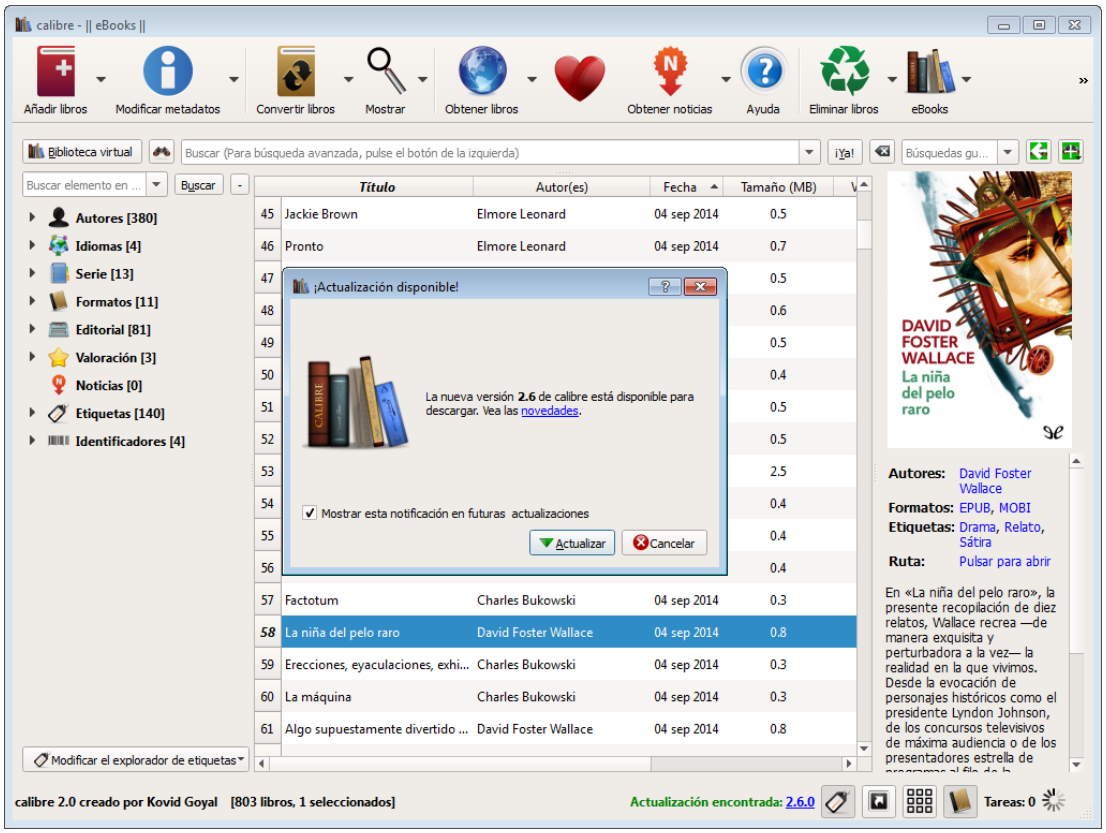
- **Actualización**

  Basta con instalar la nueva versión sin desinstalar la previa para que el software se actualice.

- **Instalación en limpio**

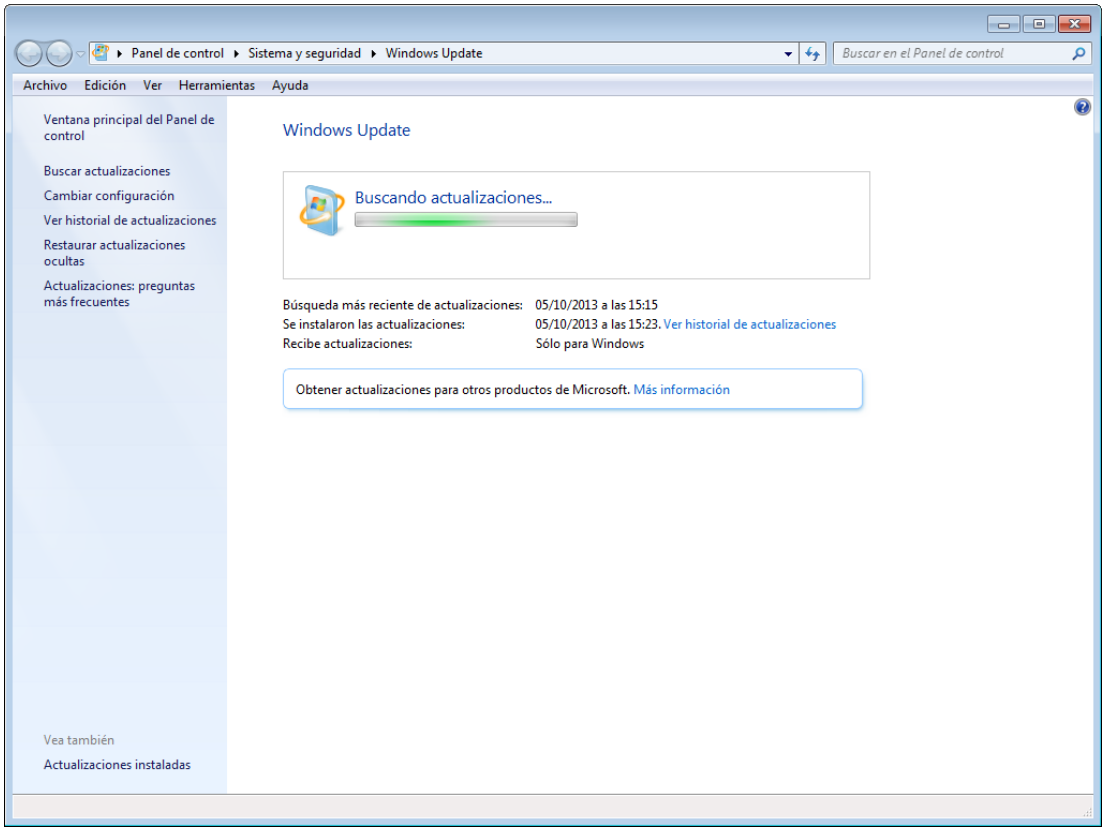
  Algunas veces debemos desinstalar la versión previa antes de instalar la nueva.

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.

También los sistemas operativos 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 ese motivo es importante descargarlas e instalarlas. En el caso de Windows contamos con el módulo denominado Windows Update.



Las actualizaciones del sistema operativo redundarán en beneficio de una mayor seguridad y es importante instalarlas.

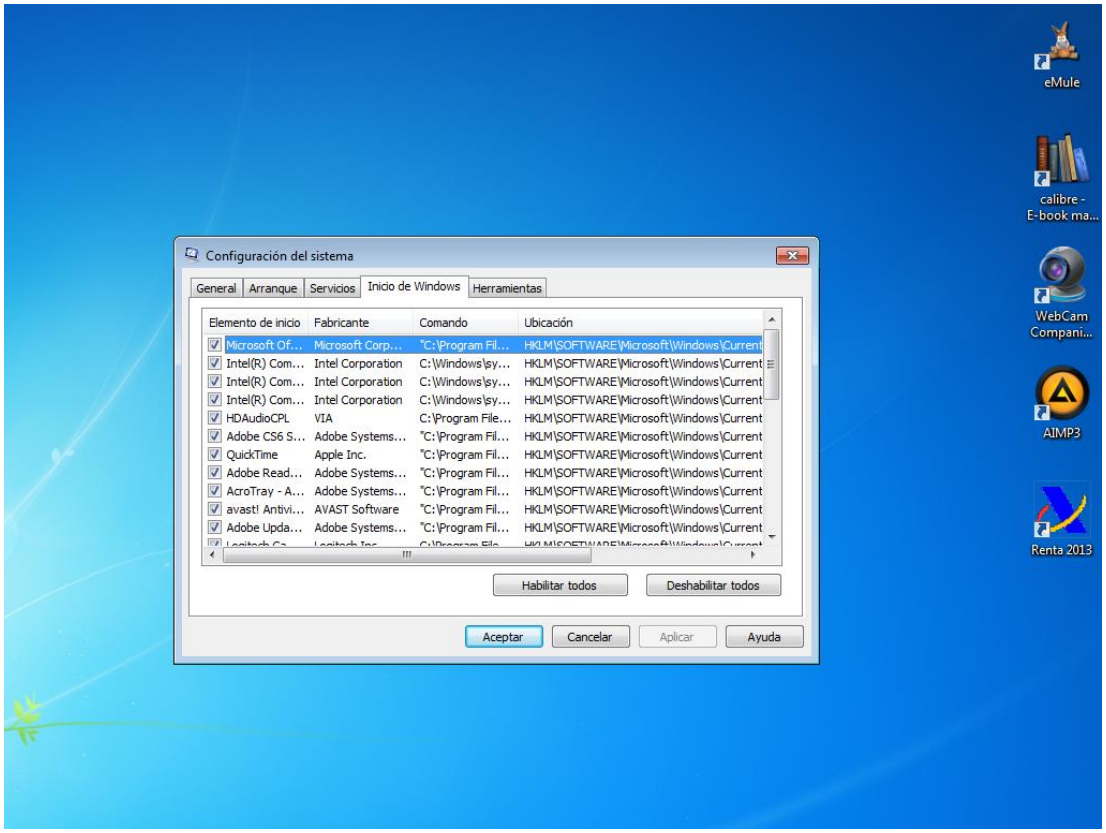
1.13. Archivos de inicio de sistemas operativos

Los pasos al iniciar un ordenador pueden variar dependiendo de diversos factores tales como el dispositivo de arranque o la existencia de particiones en éste, 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 será 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, para este fin podemos emplear ***MSConfig***. Para ello pulsaremos ***Win+R*** y, en el cuadro de diálogo que se mostrará, teclearemos ***MSConfig***.

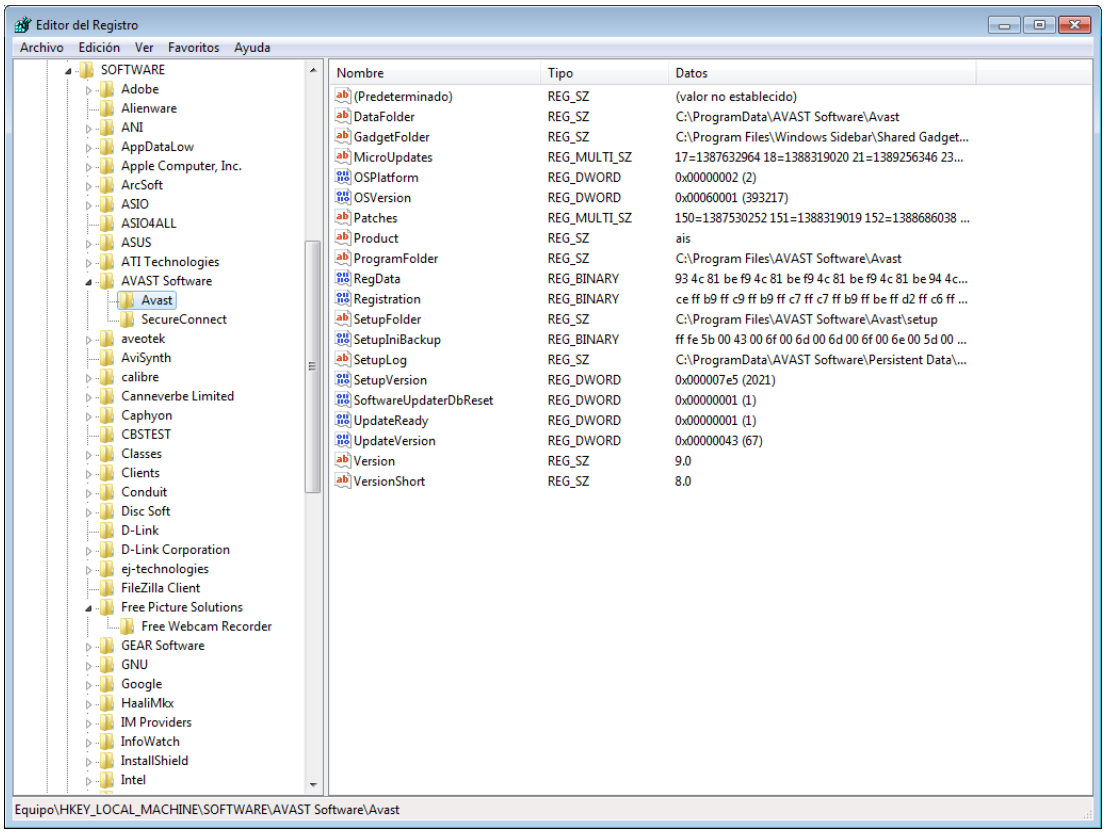


MSConfig nos permite modificar los archivos de inicio del equipo.

1.14. 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***.



El registro de Windows centraliza la configuración del sistema operativo, sus servicios y las aplicaciones que tenemos instaladas.

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

https://www.piriform.com/ccleaner/download

1.15. Actualización y mantenimiento de controladores de dispositivos

Cuando adquirimos equipos o dispositivos, los fabricantes de hardware acostumbran a incluir *drivers* o controladores que permitirán que el sistema operativo pueda trabajar con ellos. Es muy habitual que vayan apareciendo nuevas versiones de dichos *drivers* que optimicen el rendimiento del hardware, corrijan los 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.

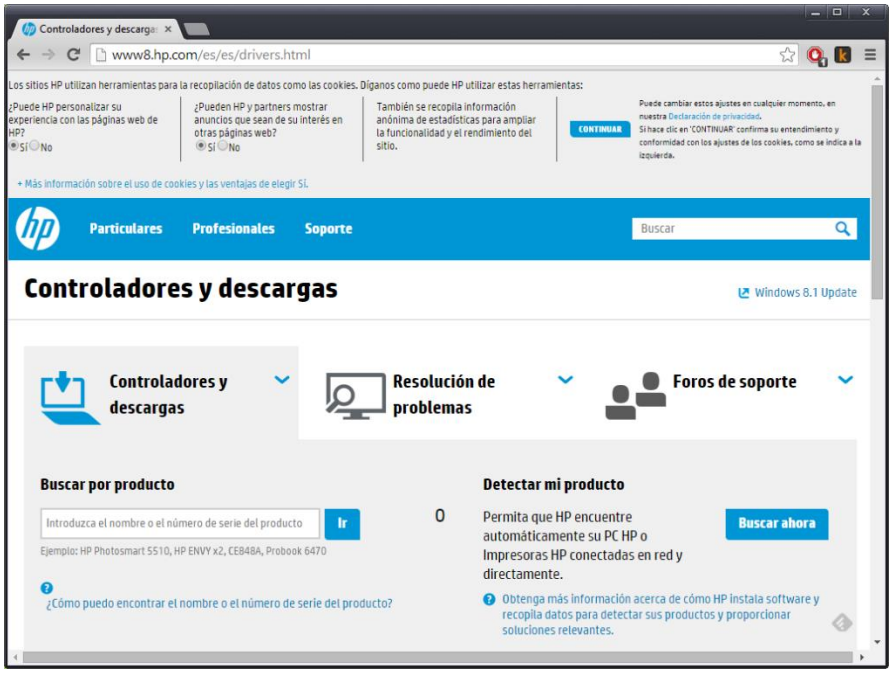
Para ello contamos con diversas opciones:

- **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 llevarse a cabo desde el Administrador de dispositivos.

- **Descarga online**

  Casi todos los fabricantes disponen de una web desde la que nos podemos descargar las nuevas versiones.



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. Para ello podemos emplear aplicaciones como **Double Driver**.

http://www.boozet.org/dd.htm

2. Administración de software de base

Cuando hablamos de **software** nos referimos al conjunto de instrucciones que se van a desarrollar 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 varios tipos de 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 pueden utilizar un ordenador en las aulas como son: los profesores, los alumnos o un trabajador del departamento de informática. Por seguridad, cada grupo tendrá 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.

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.

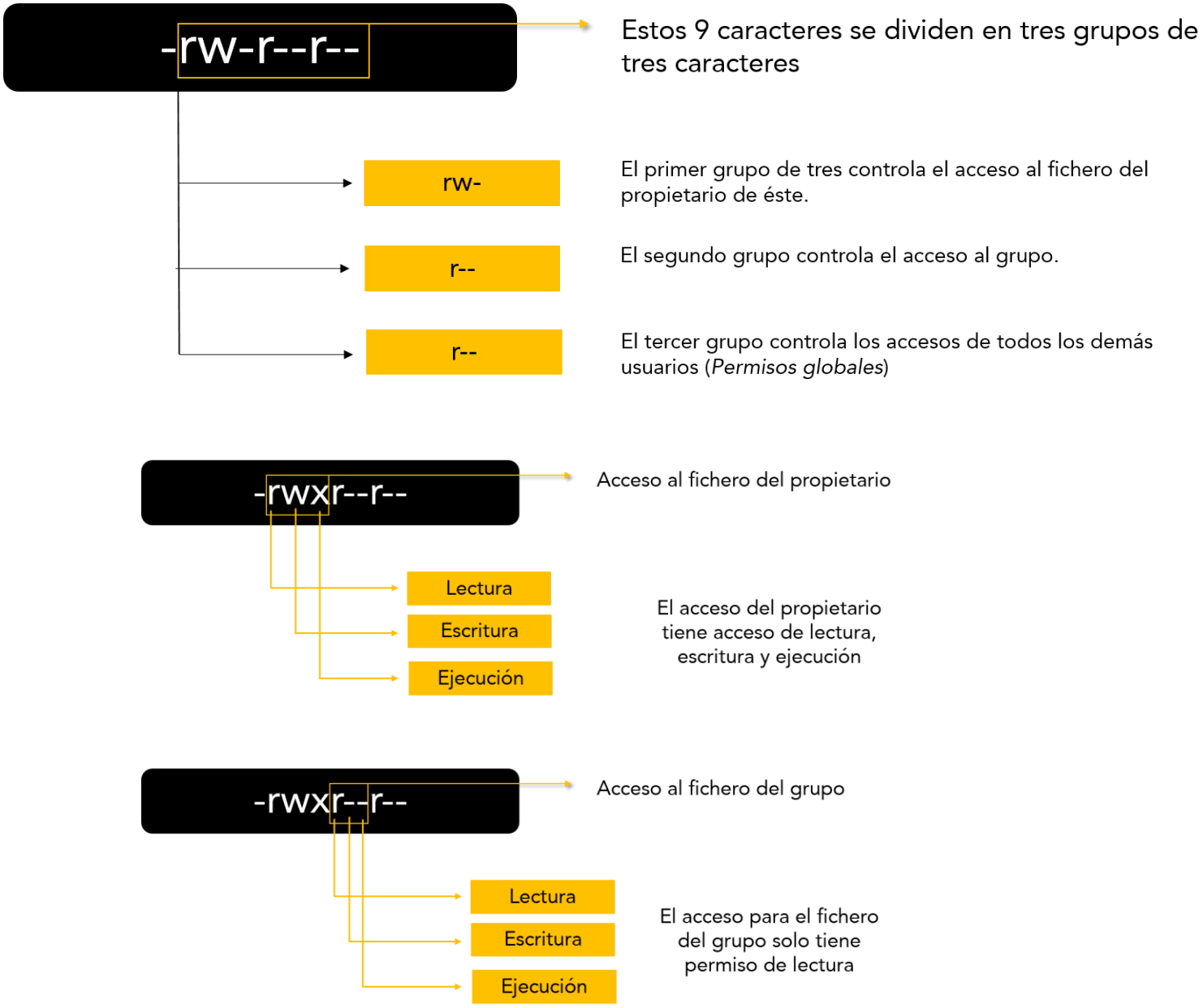
Por ejemplo, a la hora de trabajar con ficheros, podemos establecer diferentes permisos en función del usuario:

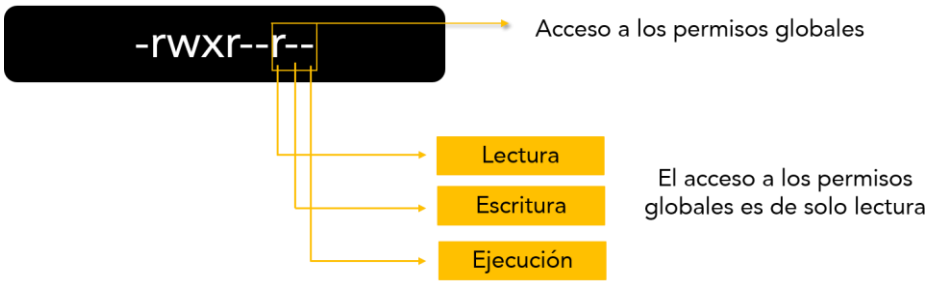
- **Lectura** (*read*)
  El usuario tiene la posibilidad de abrir y leer los contenidos del fichero

- **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.

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.

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.

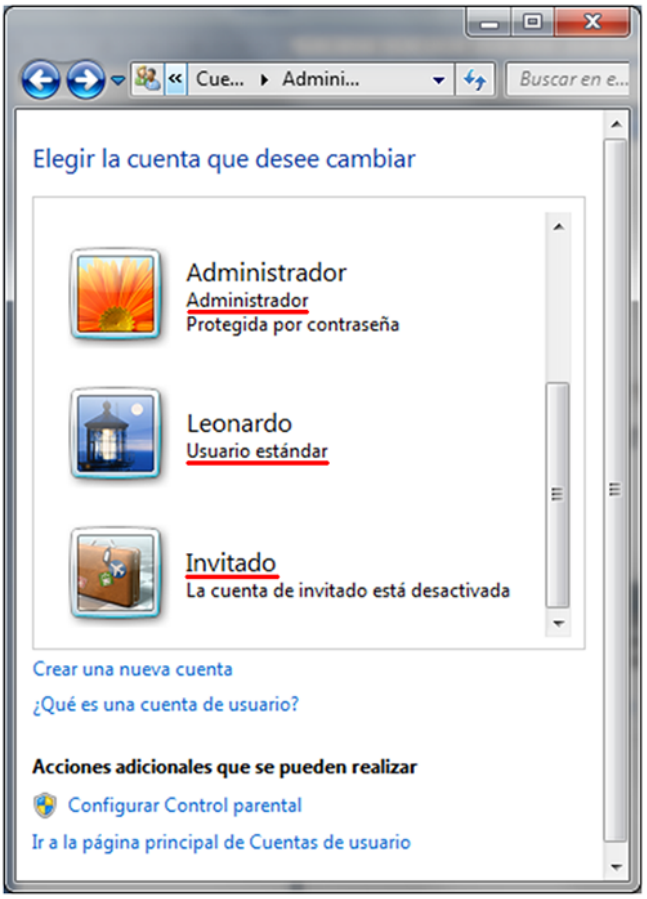
Además, para maximizar la seguridad, siempre que nos sea posible, debemos tener en cuenta las siguientes pautas:

- **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.



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 utilizar nuestra máquina.

2.3. Seguridad de contraseñas

En el caso de las cuentas de usuario de administrador la seguridad en las contraseñas es muy importante, ya estos tienen poderes sobre otras cuentas y sobre la configuración del equipo. Para el resto de 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 éstas 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, haremos 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.

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.

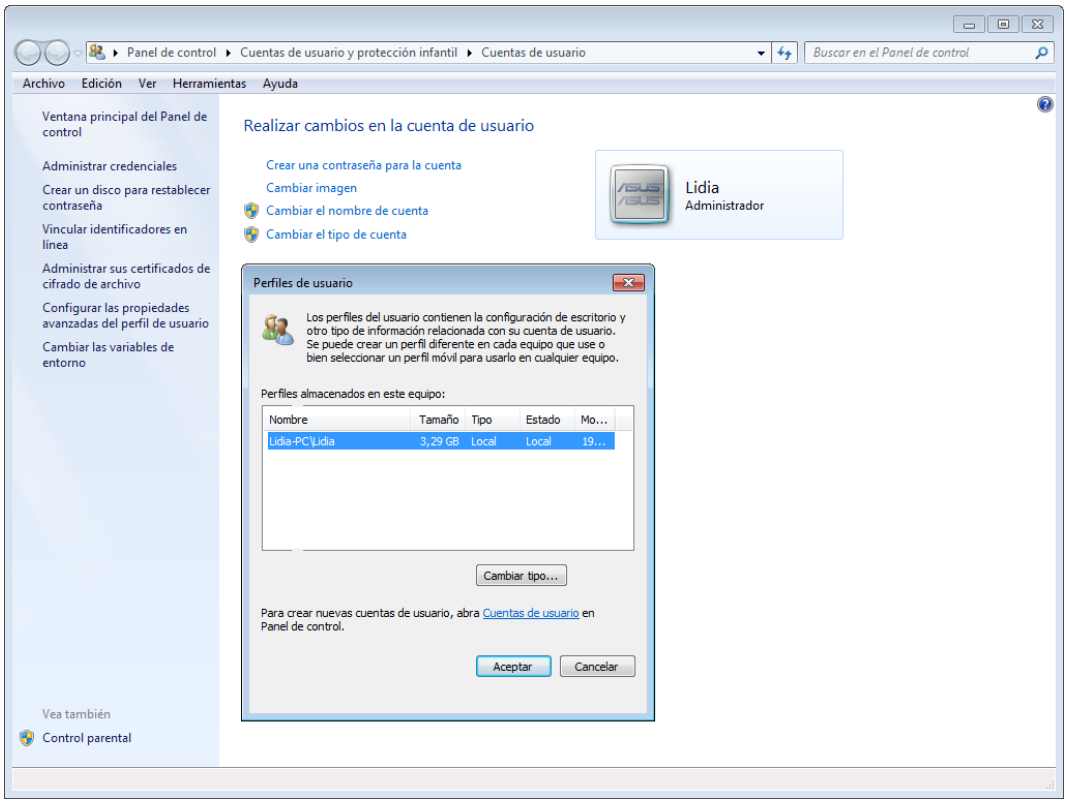
2.4. Administración de perfiles locales de usuario

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 perfiles idóneos y de asignarlos a las cuentas.



La creación de perfiles de usuario en Windows 7 se realiza a través del Panel de control.

2.5. Configuración del protocolo TCP/IP. Direcciones IP y máscaras de subred

Para configurar debidamente el servidor de red 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 a 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 puede, en ningún caso, haber 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**

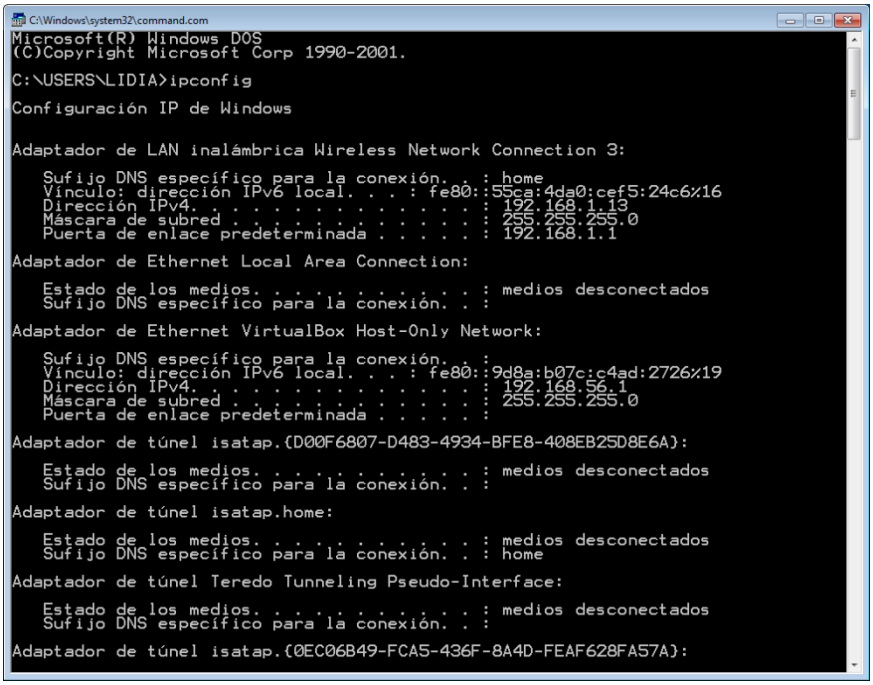
  Los últimos bits de la dirección IP constituyen la dirección del equipo en la red, y deben ser distintos para cada equipo.

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 comprendido entre 0 y 255, y 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.



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 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.

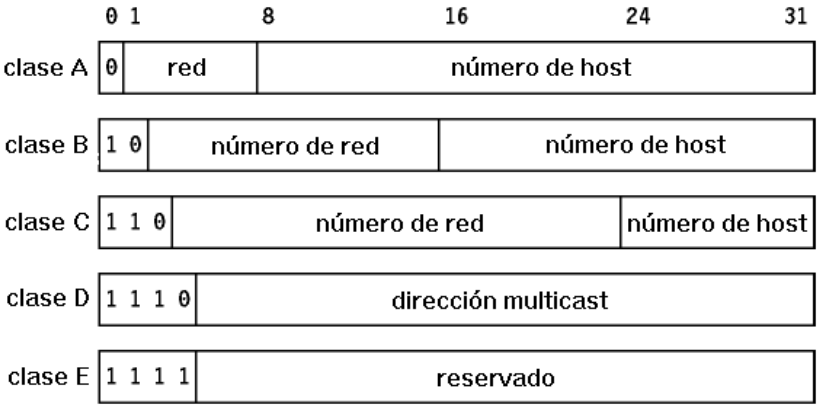
Así, en una dirección W.X.Y.Z de clase C, X.Y.Z identifican la red. Únicamente Z se refiere a los ordenadores.

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.



- **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

- **Cantidad de *hosts* por cada red de cada clase:**

2n-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)

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, 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 del mismo que permite muchas más direcciones.

2.6. Servicio de Nombres de Dominio (DNS).

Dentro del dns tenemos los reenviadores, la zona directa, la zona inversa y la sugerencia raíz (son los más importantes, pero hay más.
Si nuestro servidor tiene salida a internet pero no nuestros clientes, puede ser que tengamos mal configurados cualquier punto del dns.

ipconfig /all: para ver todas las ip, tanto la de red, la máscara de subred, la puerta de enlace predeterminada. Luego los servidores con los que estamos saliendo.

ipconfig /release: para liberar nuestra ip de nuestra tarjeta de red.

Después de liberar:

ipconfig /renew: para renovarla.

release y renew son para ip dinámicas.

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.

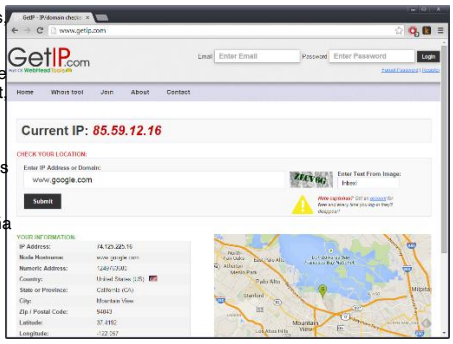
Compruébalo escribiendo 74.125.225.16 en tu navegador. Esta es la IP actual de Google. La página ***GetIP*** (http://www.getip.com/) consulta el DNS de los nombres de dominio que escribimos y nos permite obtener su dirección IP equivalente.

Puedo quitar la ip de facebook para que mis trabajadores no puedan entrar.

La cache es una memoria que almacena nuestros datos más recurrentes, todas las búsquedas que hemos ido realizando (tiene un espacio de memoria limitado). He ido 3 veces a youtube hoy, estará entonces en la memoria cache, de tal forma que cuando busque esa url, me va a salir de la memoria cache y no voy a tener que realizar una búsqueda en internet, porque ya tengo esa búsqueda almacenada en memoria, con lo cuál va ser más rápido.

Si por ejemplo solo tuviésemos espacio para 5 páginas, guardaríamos las 5 url más buscadas. Si tuviésemos una sexta que acaba siendo la más buscada, subiria.
La cache es del mismo tipo que la memoria ram, pero al ser más pequeña es también más rápido. Un disco duro de 512 siempre será mucho más rápido que uno de 1 tb del mismo tipo.

La cache nos agilizan la búsqueda de información, y solo se borrará cuando la borremos nosotros, sin embargo las cookies son datos que almacenamos en nuestro navegador de forma temporal, pero no agiliza nuestra navegación. Guardan datos de usuario y de conexión (gps para los lugares…).



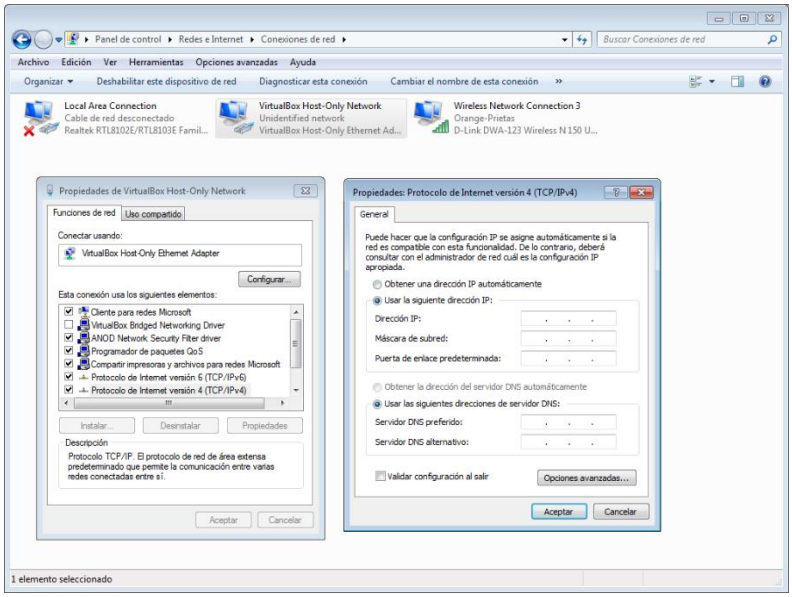
No solo basta con escoger los servidores más rápidos, sino que además es necesario configurar nuestro sistema operativo correctamente. Aprenderemos más adelante cómo hacerlo.

con ping www.google.es obtenemos su ip.

2.7. Archivos de configuración de red

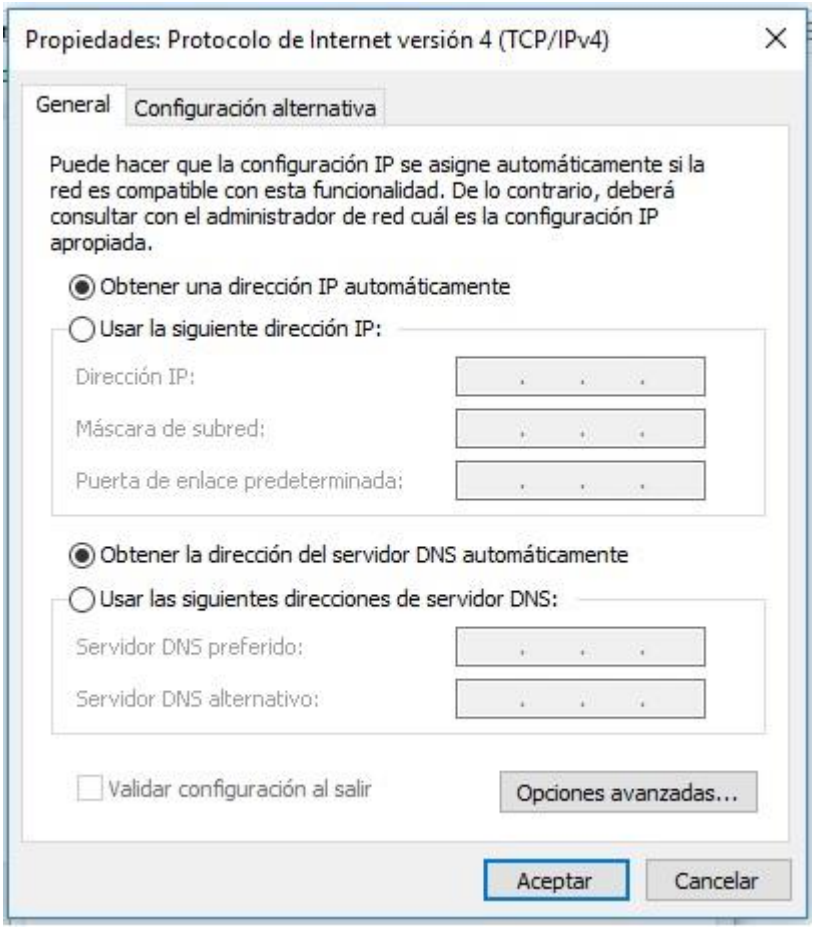
Toda comunicación en red sigue el modelo TCP/IP. Como protocolo rige las normas al realizar este proceso de comunicación. La configuración de nuestro equipo forma parte de la red y sigue una serie de pasos que a continuación vamos a detallar.

A través del Panel de control vamos a configurar tanto 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 de 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, 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.

En el caso de Linux, no obstante, la configuración de red se almacena en */etc/network/interfaces*.

2.8. Optimización de sistemas para ordenadores portátiles. Archivos de red sin conexión

Los ordenadores portátiles poseen unas características propias que deberemos 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 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**

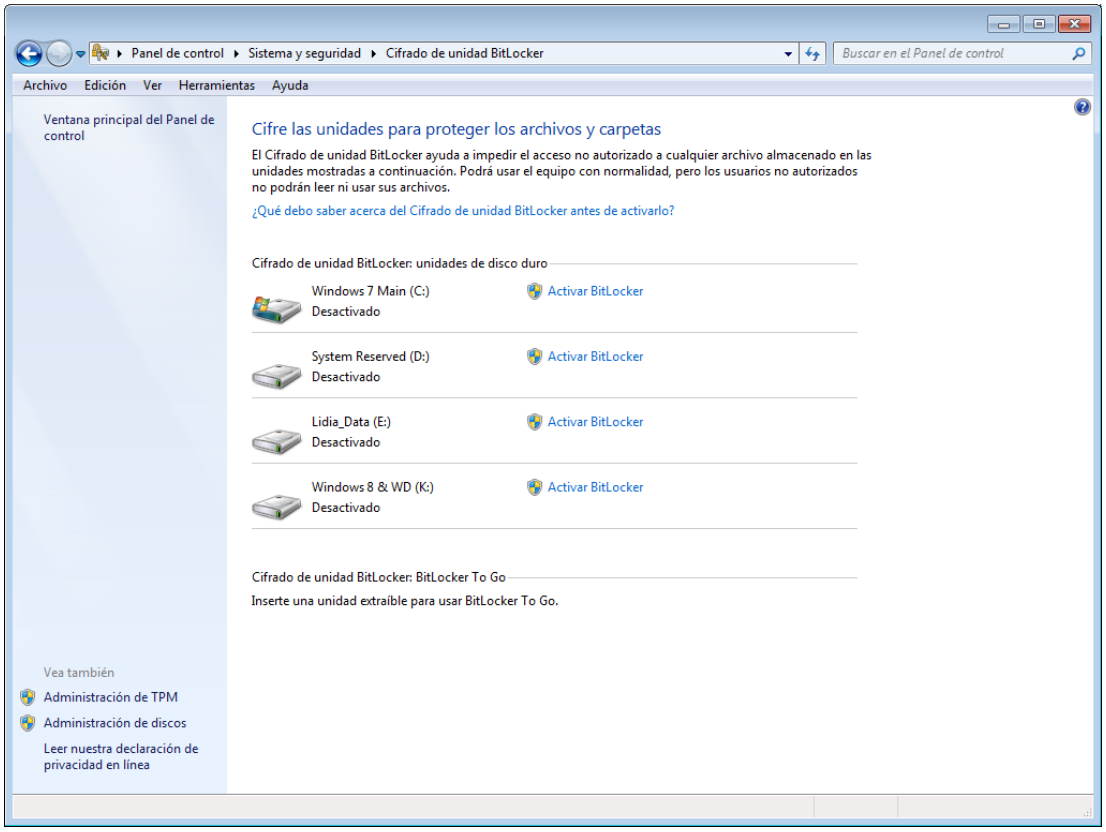
  Además de la contraseña de inicio de sesión, podemos habilitar la de la BIOS e instalar software adicional para proteger archivos y carpetas.

- **Sistemas de autenticación fuertes**

  Los lectores de huellas dactilares o de tarjetas inteligentes son cada vez más utilizados 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 la 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 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**

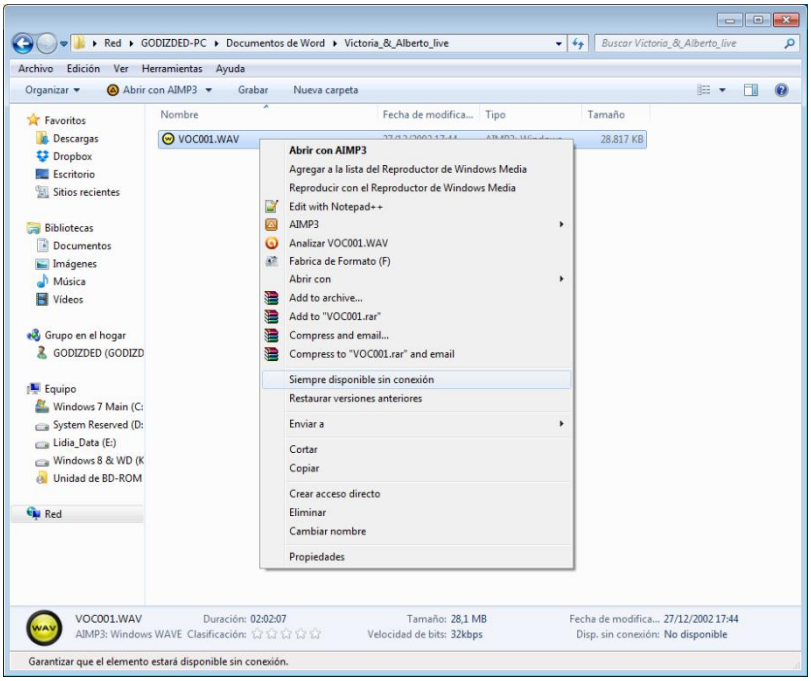
  En Windows 10 esta acción puede realizarse a través del Panel de control, en Agregar o quitar programas.

- **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, bastará con pulsar sobre el archivo o sobre la carpeta con el botón secundario del ratón y, en el menú contextual, elegiremos el comando ***Siempre disponible sin conexión***.

2.9. Principales comandos de Linux

Existen una serie de comandos en Linux que nos ofrecen la posibilidad de movernos y gestionar dicho sistema operativo.

Podemos obtener una versión actualizada de esta información a través de la página de Ubuntu y ver un listado de los comandos disponibles en *doc.ubuntu-es.org/Comandos_de_uso_frecuente*.

Al explorador de windows se le llama ventana gráfica.

UF2: Gestión de la información y de recursos en una red

La raíz sería una partición del disco duro, como por ejemplo C: en windows.
En este caso, sería una partición primaria porque es la que ha instalado el S.O.
Dentro, sistema de carpetas, y dentro también puede haber sistema de ficheros.
Estructura básica de windows: tenemos archivos de programa

1. 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.

1.1 Sistema de archivos

Al hablar de **sistema de archivos** nos referimos al 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.

A nivel interno es habitual que los datos se estructuren en bloques que tendrán siempre un mismo tamaño, se les denomina sectores. No obstante, como usuarios, gracias a las aplicaciones para gestionar archivos, los datos se pueden presentar como:

- **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

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

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)

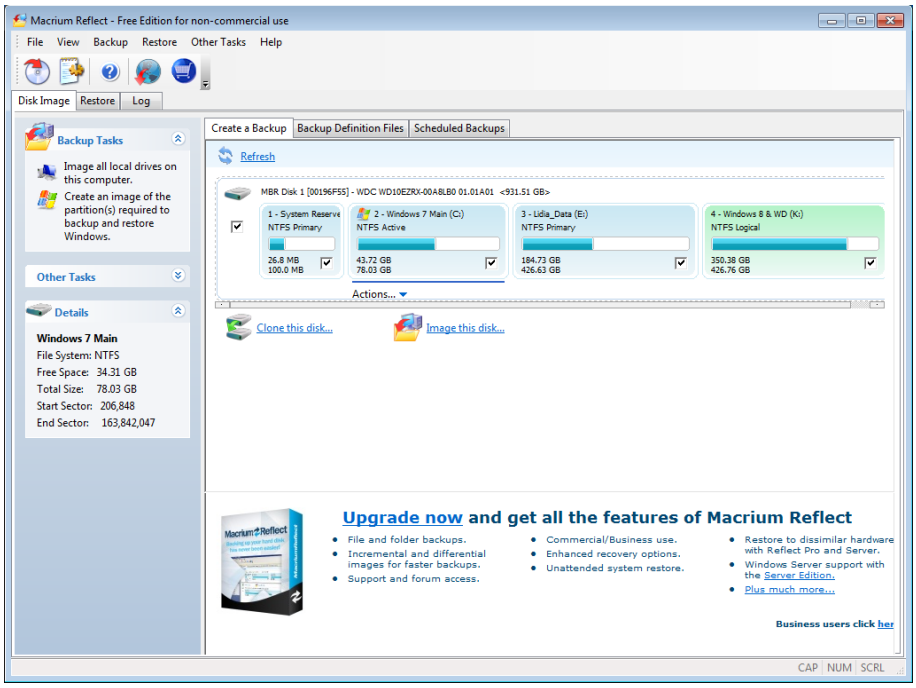
  Sistema de archivos heredado de MS-DOS que podemos encontrar en las primeras versiones de Windows. Debido a esto, se considera un sistema universal y, pese a su antigüedad, aún se utiliza con cierta frecuencia.

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

  Sistema de archivos diseñado para versiones más recientes de Windows. Gracias a él se consigue 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 Macrium Reflect.

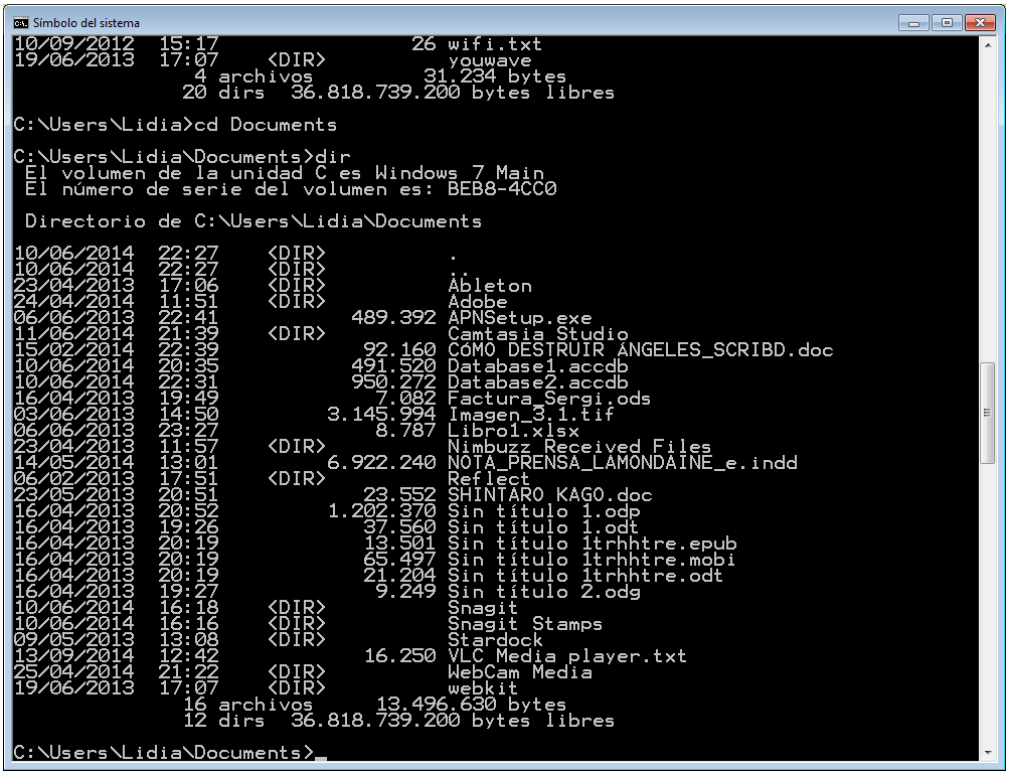
La elección del tipo de sistema de archivos suele realizarse tras particionar el disco, en el momento de formatearlo. Pero, como veremos más adelante, podemos crear, eliminar y modificar las particiones usando herramientas del propio sistema operativo. Recordemos que un mismo disco físico puede tener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

1.2 Gestión de sistemas de archivos mediante comandos y entornos gráficos

En windows se llama cmd

Tanto en Linux como en Windows, los sistemas de archivos se pueden administrar desde la consola o símbolo del sistema, tecleando los diferentes comandos.

En Windows debemos ejecutar el símbolo del sistema desde el menú Inicio. De esta forma nos aparecerá una ventana donde podremos teclear las instrucciones.



Particiones NTFS vistas a través de la aplicación Macrium Reflect.

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

con cd .. volvemos atrás

si ponemos cd, la inicial de donde queremos ir, y tabulador, nos marca las distintitas opciones que comienzan por d

cd / sin escribir nada más para ir a la raíz del sistema (C:\)

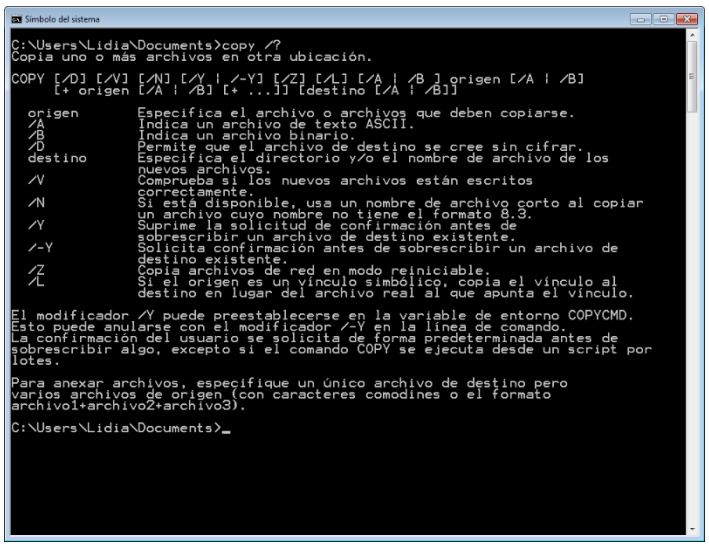
Ejecutando como administrador elevamos permisos. Nos aparecería C:\Windows\system32> en lugar de C:\Users\AEO>

directorios ocultos se muestra como [.] [. .] o simplemente los puntos solo.

cls limpiar

MD	Crea el directorio especificado.	MD Juegos
RD	Elimina el directorio especificado.	RD Juegos
COPY	Copia ficheros	
DEL	Borra ficheros	Con rename, ponemos el nombre viejo entre comillas, y el nuevo nombre también entre comillas.
REN	Renombra ficheros	
MOVE	Mueve ficheros	Con move ponemos el nombre del fichero que queremos mover, y el nuevo directorio al que queremos mover entre comillas / y nombre del fichero. Si ponemos otro nombre, se le cambia el nombre. Ej: move Doc1.txt "Nueva carpeta/doc1.txt"

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



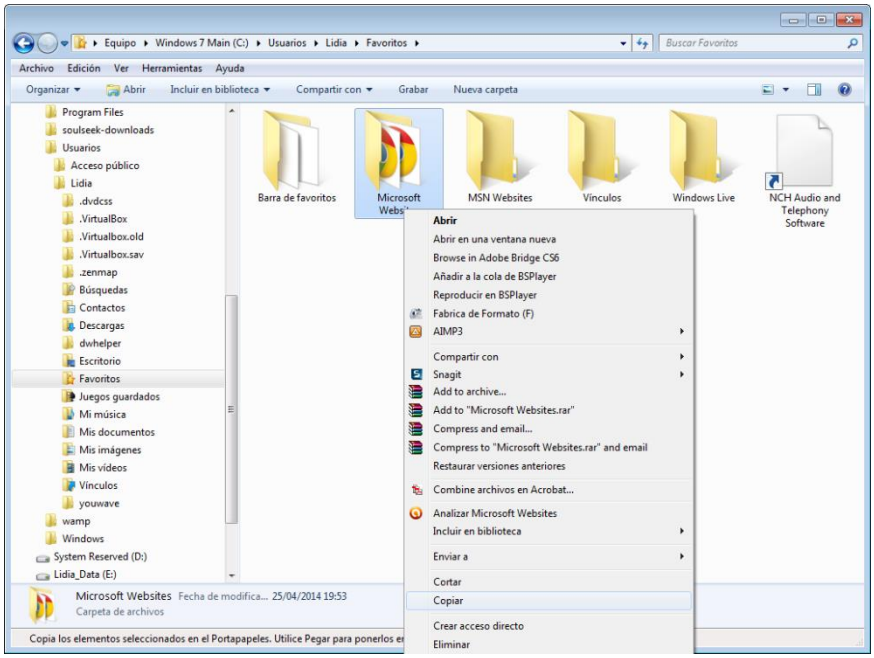
No obstante, los sistemas operativos actuales incorporan herramientas específicas que muestran los datos en un entorno gráfico para que el tratamiento de la información sea más intuitivo.

Algunos de los principales gestores de archivos en formato gráfico para Linux son los siguientes:

- **Nautilus**
- **Krusader**
- **Konqueror**

En Windows también se nos brindan múltiples opciones en este ámbito, como ***FreeCommander*** (*http://www.freecommander.com/*) o ***Unreal Commander***

(*http://x-diesel.com/*). No obstante, el Explorador de Windows, accesible a través del menú Inicio, es perfectamente apto para el fin que nos ocupa.



El Explorador de archivos de Windows.

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**.

En administrador de dispositivos le sale dos veces el mismo procesador porque en la máquina virtual marcó que tenía dos cpu.

Panel de control > Programas > Programas y características > Actualizaciones instaladas para borrar alguna, o la misma ruta para desinstalar un programa.

En windows update también tenemos opciones para volver atrás.

Activar o desactivar las características de Windows, está Hyper-V, máquina virtual que viene con windows.

https://ionicons.com/ para descargar fuentes. Panel de control > Apariencia y personalización > Fuentes

Administración de discos: Particiones primarias, particiones extendidas, unidades lógicas. Solo podemos tener 4 particiones primarias (4 .S.O sin virtualizar).
Podemos tener muchas particiones extendidas (o secundarias), se crearon con la curiosidad de que pueden contener una infinidad de unidades lógicas.
Podemos tener más de 4 particiones primarias, es decir, podemos instalar más de 4 S.O siempre que sea dentro de una partición secundaria, con lo cual me va a requerir que estas particiones primarias sean de máquinas virtuales, que podemos instalar en un disco duro externo (no es necesario que ese disco duro sea un disco duro primario). Estas máquinas virtuales me van a crear pequeñas particiones primarias dentro de esta partición secundaria e infinitas.

Con windows server instalar al menos AD DS, DHCP, DNS

El administrador debe tener una contraseña segura en windows server. Windows nos crea automáticamente un usuario administrador si usamos wmplayer. Automáticamente entraríamos con el usuario que creamos durante la instalación (no administrador) y nos daría error por contraseña no segura, refiriéndose a la de administrador. Cerramos sesión, accedemos a la cuenta de administrador y establecemos contraseña segura.

Lo mejor es que los servidores tengan las IP's estáticas ya que este normalmente no se apaga. Muchos servicios nos pedirán que sea estática. Con dinámica deberíamos entrar a configurarla cada vez que configuremos un servicio.

Importante mantener los servidores actualizados, configurar hora automática.

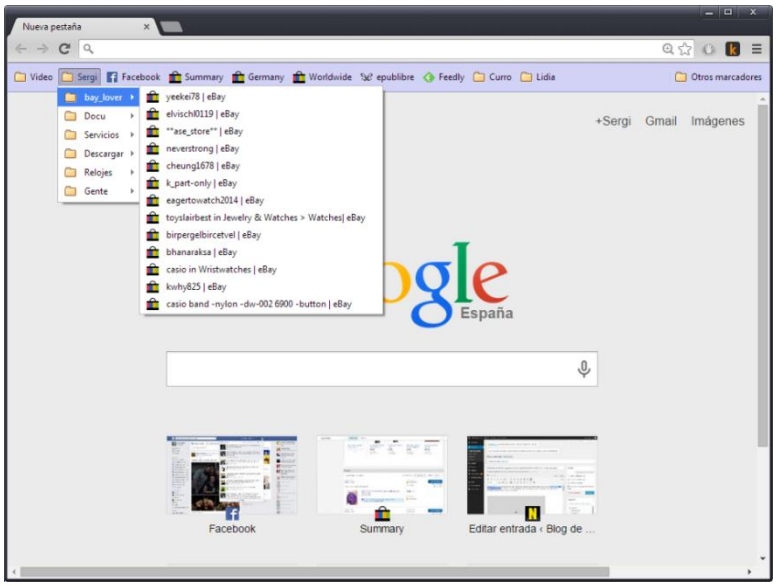
Configuración de seguridad mejorada de IE -> Si queremos navegar por internet, desactivarlo. Normalmente lo dejaríamos activado, ya que los servidores no están hechos para navegar por internet.

Empezar instalando Servicios de dominio de Active Directory.
Instalar dns, empezar por los bosques. Si me salta una alerta amarilla, darle a promover. El DNS sirve para transformar una IP en un dominio.

1.3 Gestión de enlaces

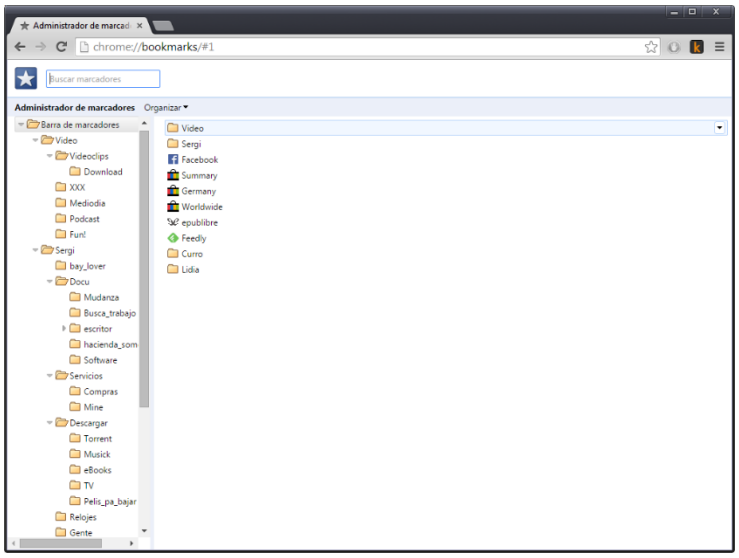
Los navegadores web nos brindan una opción extremadamente interesante: la posibilidad de guardar el enlace a una página que nos interesa de tal modo que, en adelante, podamos acceder a ella con un solo clic.

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.



Desplegable de enlaces guardados en Google Chrome.

Haciendo clic con el botón derecho sobre la barra inmediatamente inferior y eligiendo el comando ***Administrador de marcadores***, podremos gestionar los enlaces.



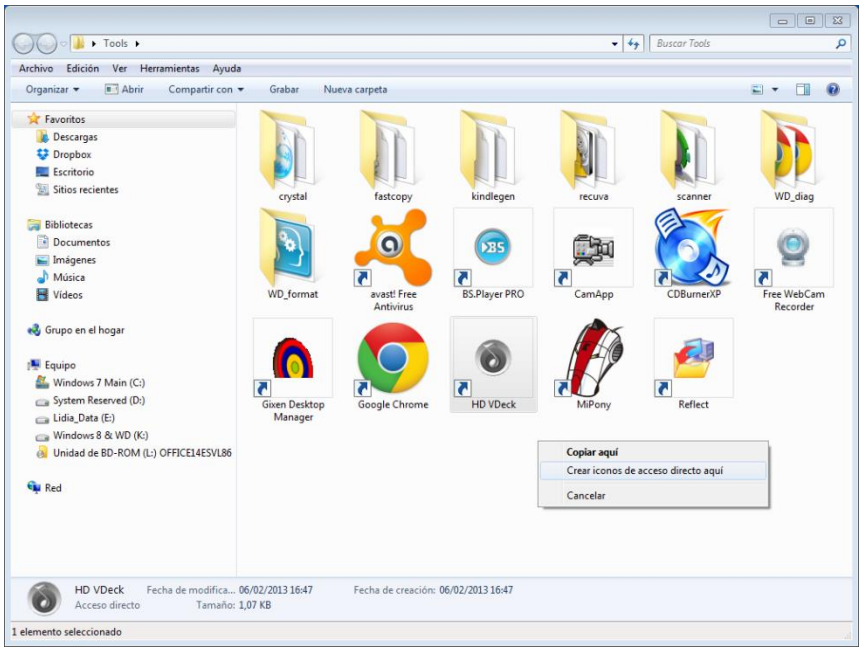
El Administrador de marcadores de Chrome nos permite gestionar los enlaces.

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 dejará 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, dejaremos 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 desplegará, elegiremos Crear acceso directo aquí.



Creación de accesos directos en Windows 7.

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

- *ln -s nom_archivo nom_enlace*

1.4 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:

Directorios Linux	Almacenan.
/bin	Comandos esenciales que usará el usuario.
/boot	Archivos de arranque de Linux.
/dev	Archivos que corresponden al hardware (ratón, teclado, disco duro, etc.).
/etc	Configuración del sistema.
/home	Estructura de árbol en la que cada usuario tiene su propio subdirectorio. Equivalente a la carpeta *Documents and Settings* de Windows.
/lib	Librerías y módulos del núcleo.
/media	Información para medios extraíbles.
/mnt	Monta los sistemas de archivos temporalmente.
/opt	Paquetes de software independientes de otros paquetes.
/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 *home* del administrador.
/proc	Documentación del sistema.

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**

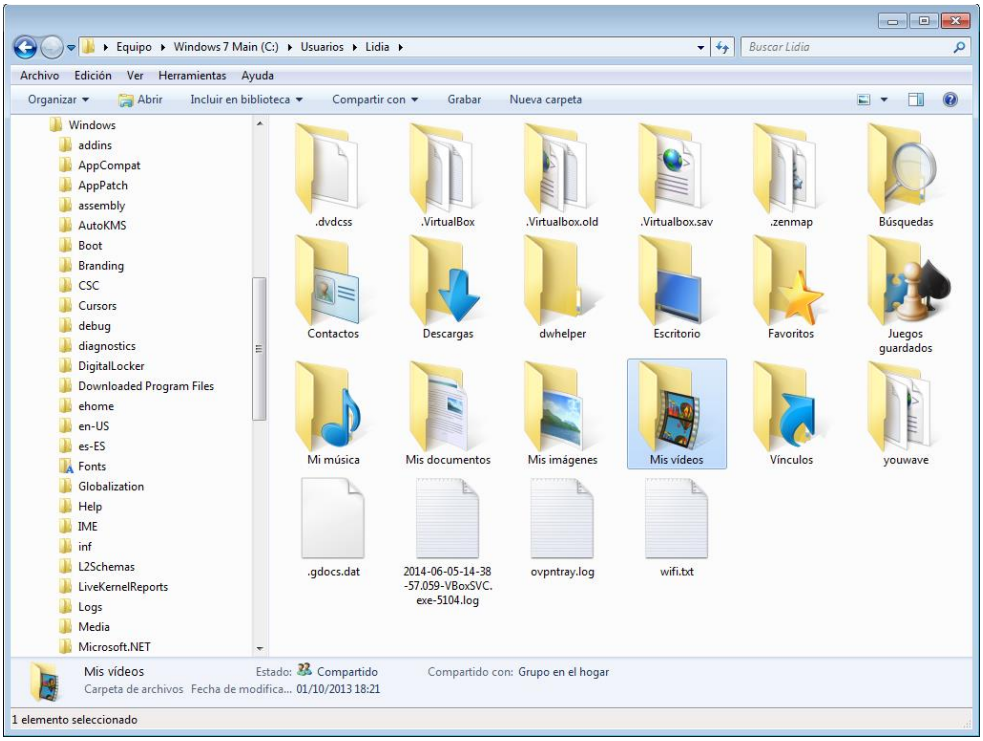
      Páginas web agregadas como favoritas.

- **Menú inicio**

  Accesos directos del menú inicio del usuario en cuestión.

- **Mis documentos**

  Archivos personales del usuario.



Subcarpetas de un usuario en Windows 7.

Por último, 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 de los mismos.

1.5 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 esto, 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 reemplazar el nombre completo o alguna parte del nombre de cualquier archivo. También puede reemplazar 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 (?)**
  Reemplaza un solo carácter, aunque se pueden poner varios símbolos de interrogación según cuáles sean 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.

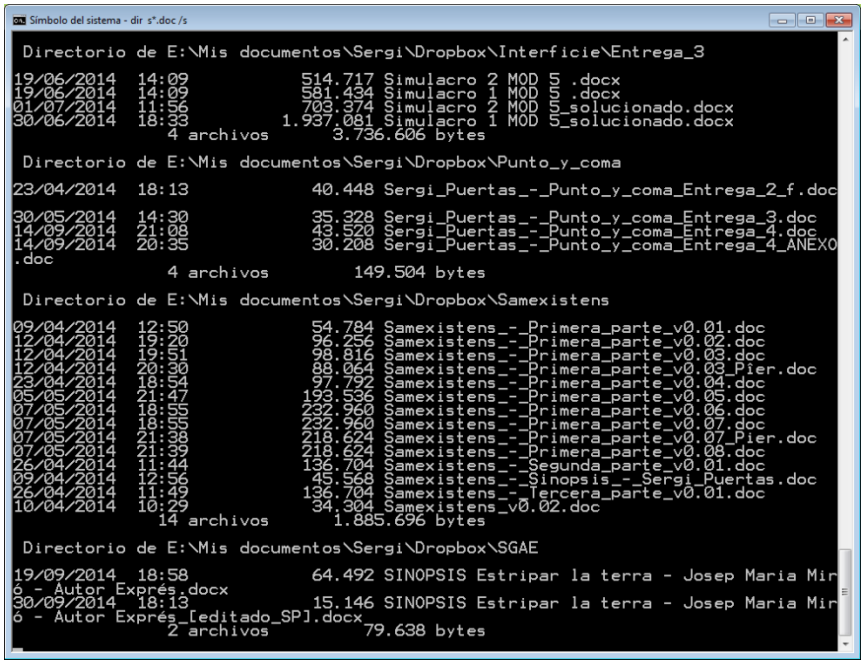
  Si tecleamos ***DEL d??.txt*** solamente borraremos aquellos archivos con esta extensión, que cumplan este requisito (d03.txt, dat.txt, etc.).

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:

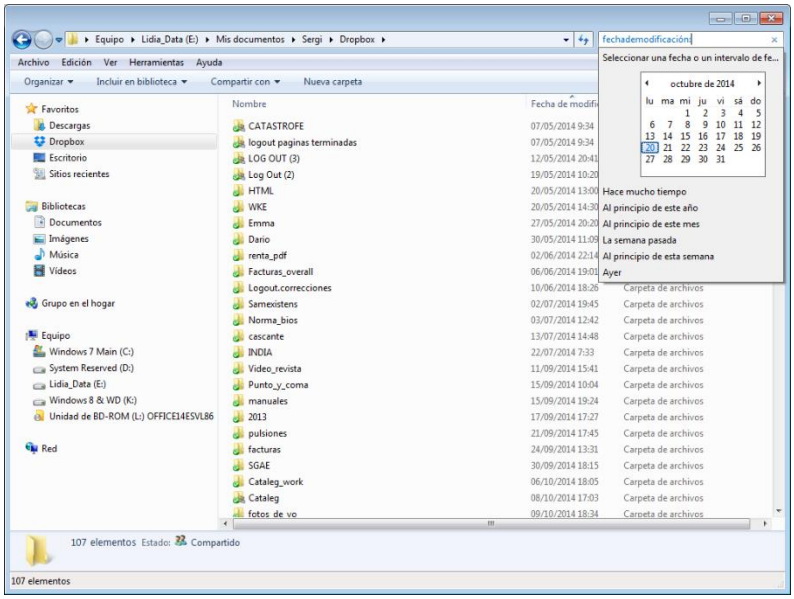
- El parámetro /s buscará en los subdirectorios.
- En el nombre del fichero a buscar podemos teclear comodines.
- Ejemplo: DIR s*.doc* buscará los archivos y directorios que empiecen con la letra s y cuya extensión sea DOC, DOCX, etc.



Búsqueda de archivos desde la línea de comando.

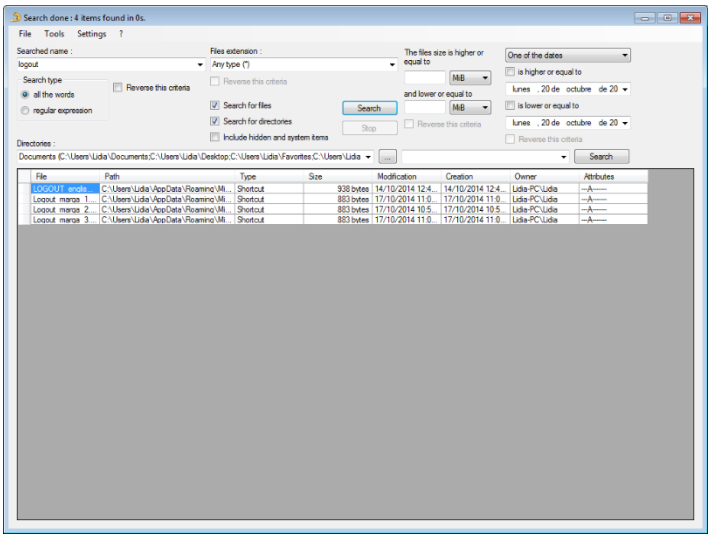
Si preferimos usar una herramienta gráfica, en Windows 10, podemos emplear la casilla que se halla en el área superior derecha del Explorador de Windows.

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



Búsqueda de archivos desde Windows.

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.

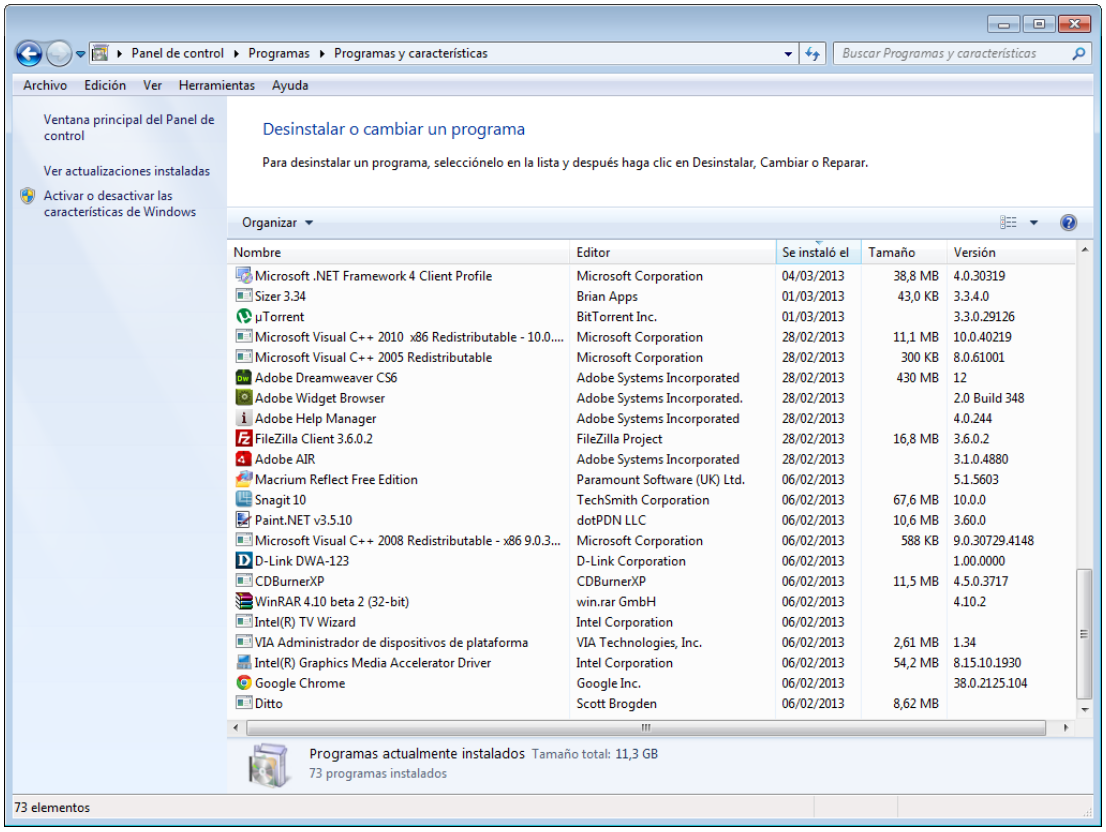


Búsqueda de archivos desde FileSearch.

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.

1.6 Identificación del software instalado mediante comandos y herramientas gráficas

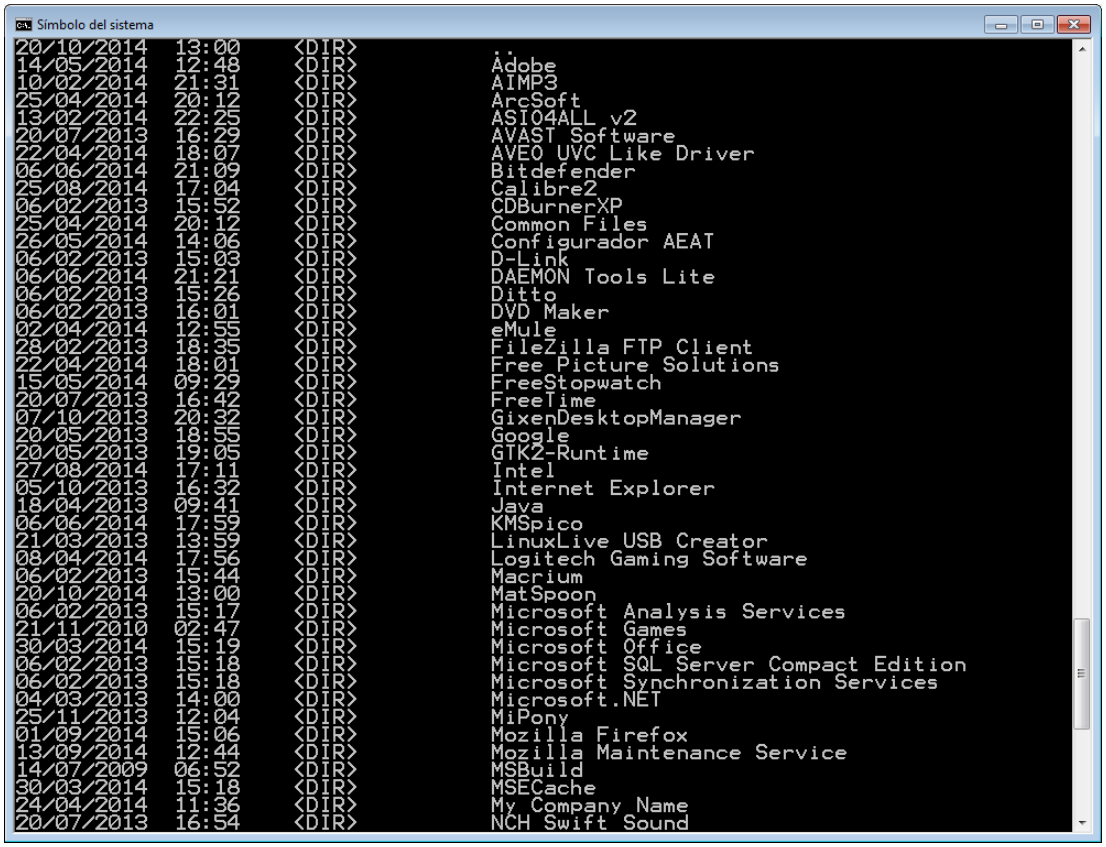
A la hora de determinar qué software tenemos instalado en un equipo lo más sencillo es remitirse al área del sistema orientada a este fin. En Windows 7, por ejemplo, para esta acción podemos acceder al ***Panel de control***, entrar en ***Programas*** y hacer clic en ***Programas y características***.



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, así pues, deberemos usar el ***Símbolo del sistema*** para desplazarnos a la carpeta ***Archivos de programa***. Una vez allí, teclearemos ***DIR*** para listar el directorio y ver qué programas hay en el equipo.



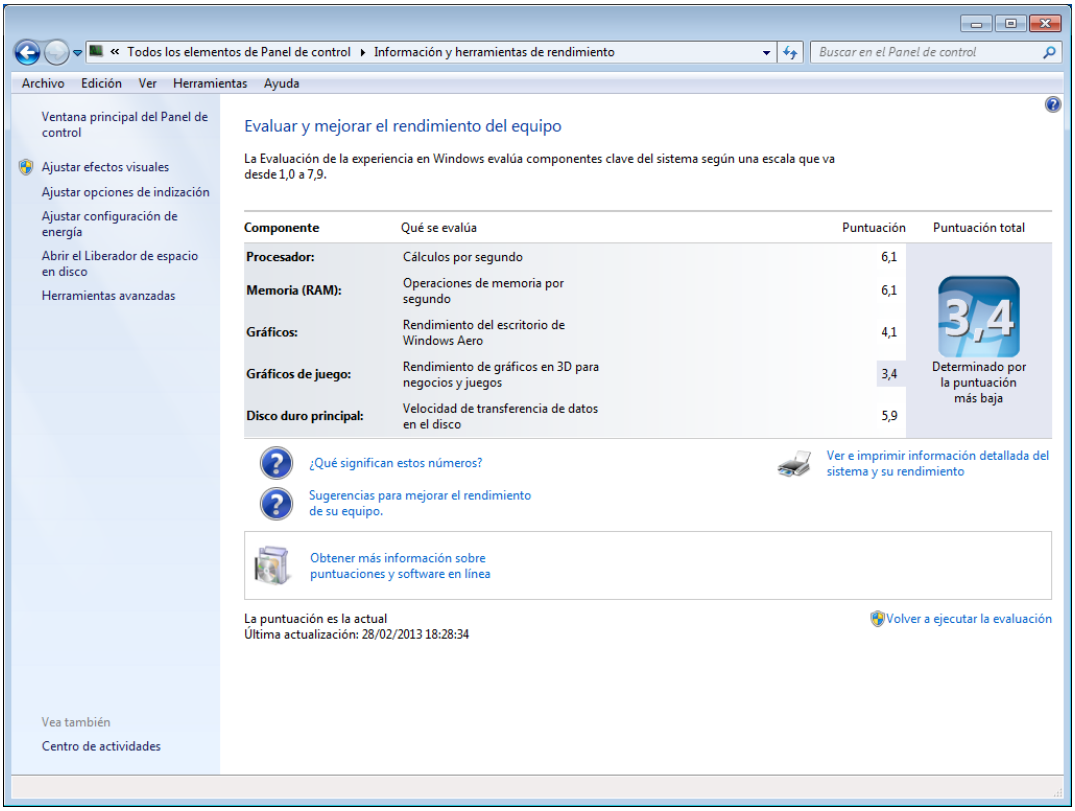
También podemos identificar el software instalado mediante el comando DIR.

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

1.7 Gestión de la información del sistema. Rendimiento. Estadísticas

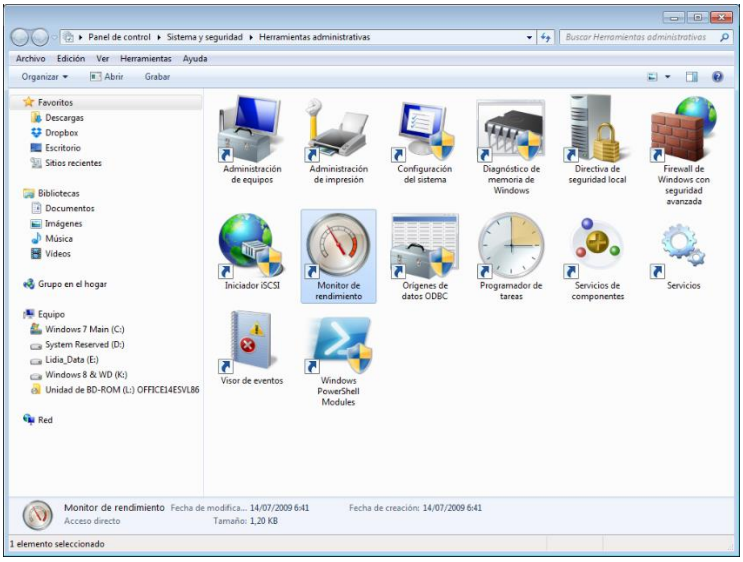
A menudo deseamos obtener datos cuantificables del rendimiento de nuestro equipo más allá de nuestras percepciones subjetivas acerca del mismo. En Windows podemos acceder a un área dedicada a este fin accediendo a las Propiedades de Equipo.

En la ventana que se abrirá deberemos 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).



Rendimiento de un equipo Dual Core ejecutando Windows 7.

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.

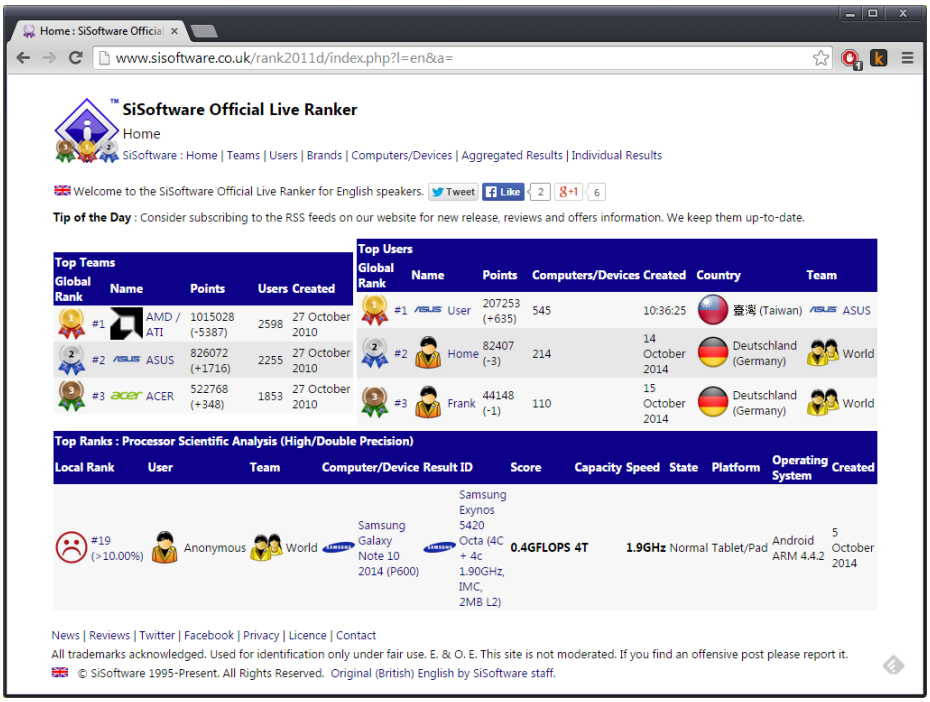


Las Herramientas administrativas de Windows 10 nos amplían información acerca del rendimiento del equipo.

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

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

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



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 dedicadas a este fin.

1.8 Montaje y desmontaje de dispositivos en sistemas operativos

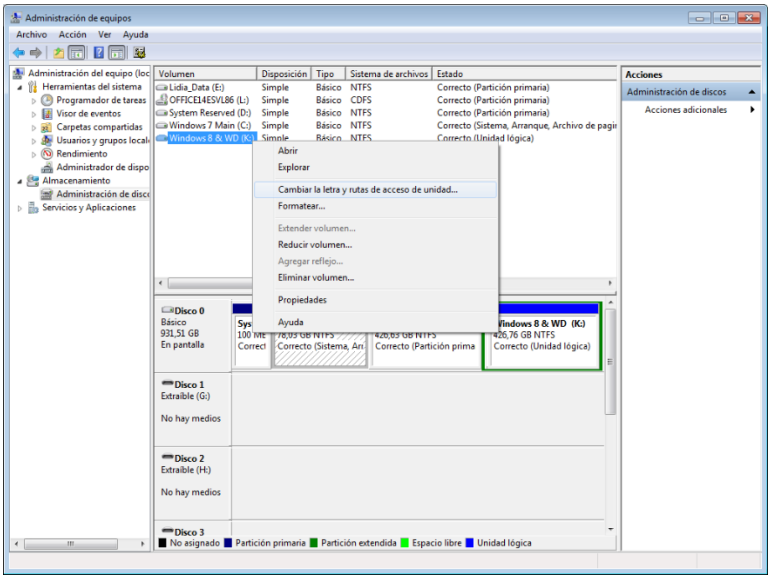
El montaje y el desmontaje de dispositivos es una técnica de administración de discos que generalmente se utiliza en Linux, pero que está también disponible en las versiones más recientes de Windows. Una unidad montada es, en definitiva, una partición asignada a una carpeta vacía de otra partición. Generalmente, 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 guardan la información y se está llenando y 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 deberemos 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 mostrará, accederemos al panel izquierdo y, en Almacenamiento, abriremos el apartado Administración de disco.



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

Una vez se listen las particiones, haremos clic con el botón derecho del ratón en la unidad que queremos montar. En el menú contextual pulsaremos sobre la opción Cambiar la letra y rutas de acceso de unidad.

Seguidamente, pulsaremos sobre Agregar en Montar en la siguiente carpeta NTFS vacía y, a continuación, escribiremos 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, haremos clic en Cambiar la letra y rutas de acceso de unidad. Esto nos permitirá seleccionar el comando Quitar.

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

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*.

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

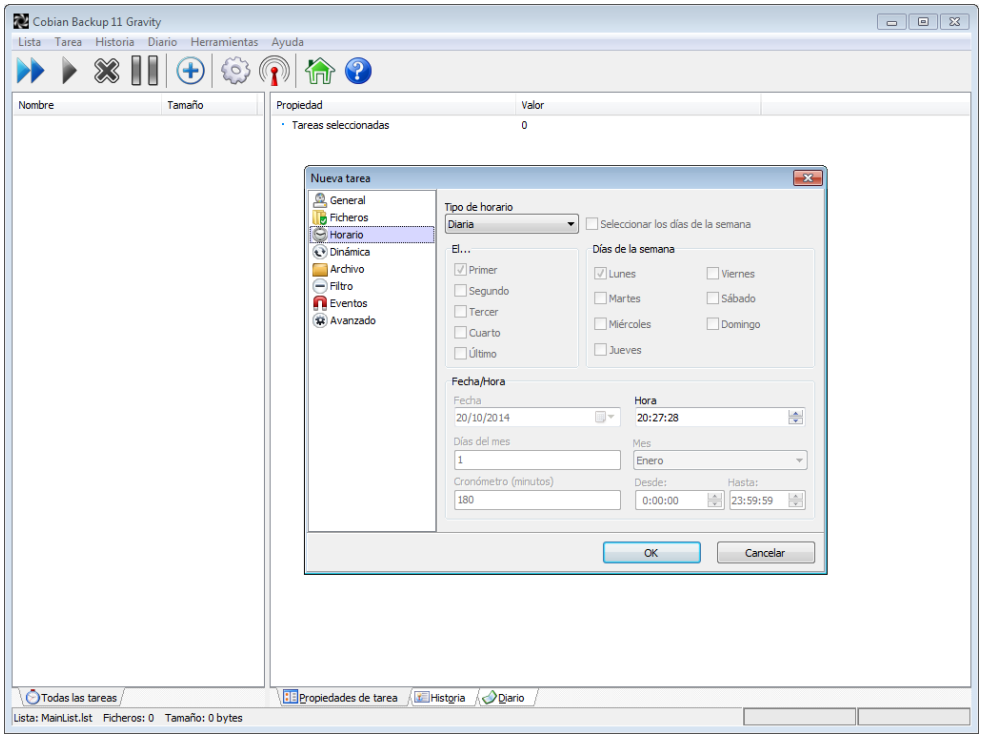
1.9 Automatización

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**

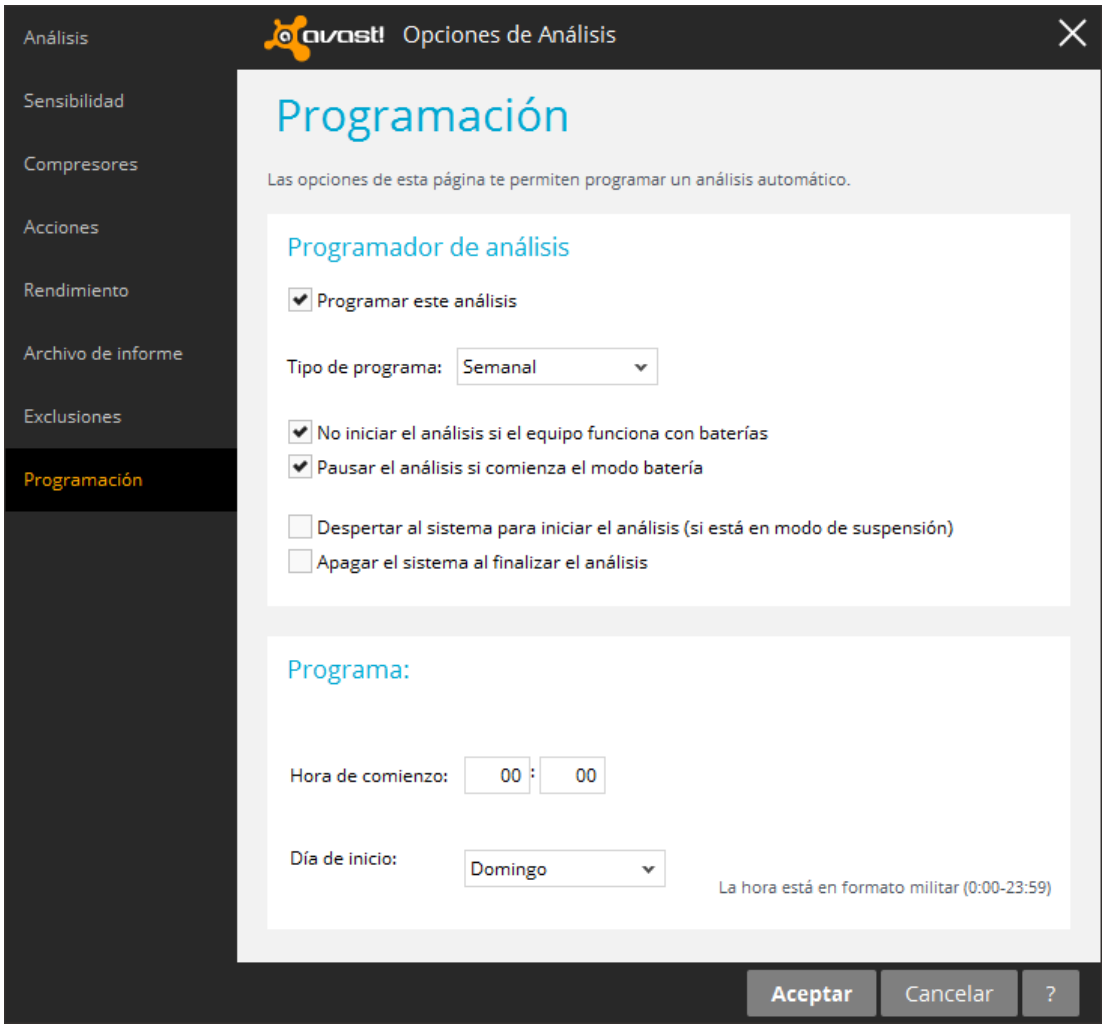
  Es muy habitual que el software para copias de seguridad, como ***Cobian Backup*** (http://www.cobiansoft.com/cobianbackup.htm), permita automatizar los respaldos.



Automatización de una copia de seguridad.

- **Antivirus**

  Prácticamente todos los antivirus, ofrecen la opción de automatizar los análisis. Es el caso de **Avast!** ***Free*** (http://www.avast.com/es-ww/index).



El Administrador dispone de todos los permisos sin ninguna limitación.

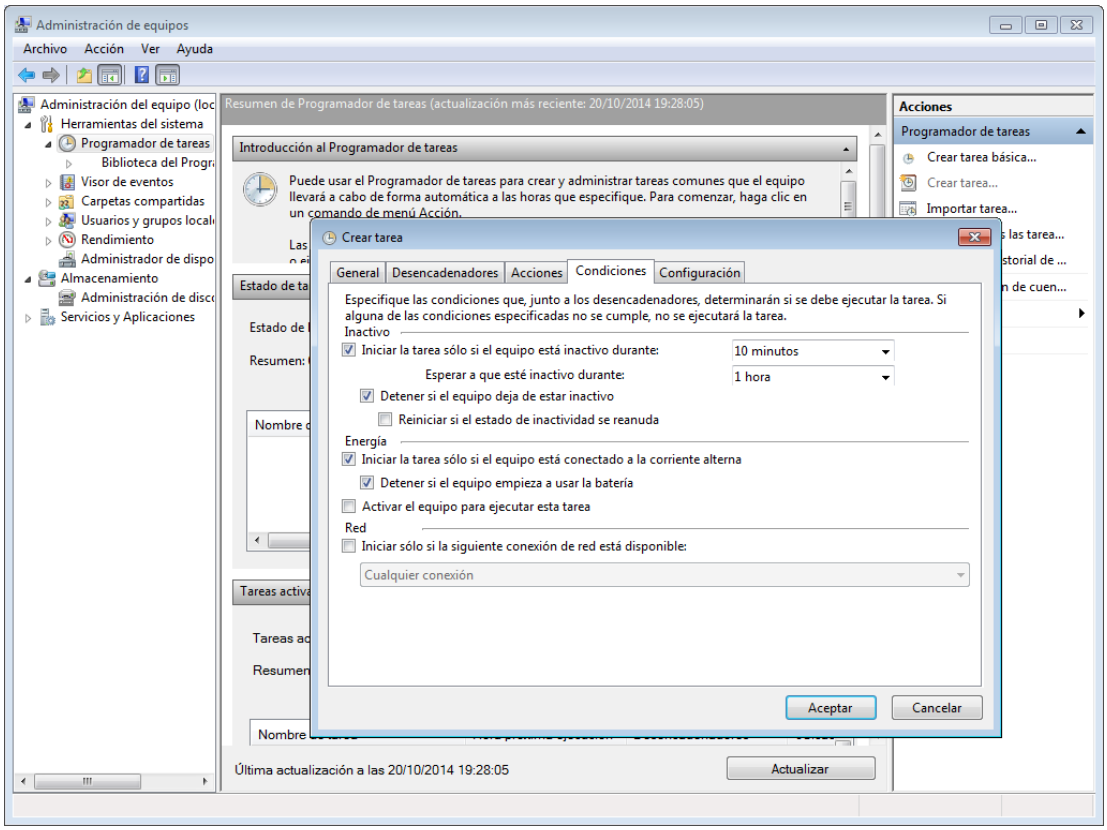
Gracias a la automatización de estos procesos, podemos programar estas acciones de modo que se ejecuten durante la hora de comer, durante la noche o en aquellas horas que no consumirán recursos de sistema que en otras horas nos serán precisos para trabajar.

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, haremos clic 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 sobre ella podemos definir, entre otras cosas, qué tarea se va a ejecutar y en qué condiciones.



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

En ocasiones las tareas rutinarias que deberemos realizar con regularidad podrán completarse mediante comandos. Por supuesto, contamos con la posibilidad de escribirlas una a una mediante la ventana de Símbolo del sistema de Windows 7. Pero existe la opción de simplificar significativamente este proceso gracias a los ficheros de proceso de lotes.

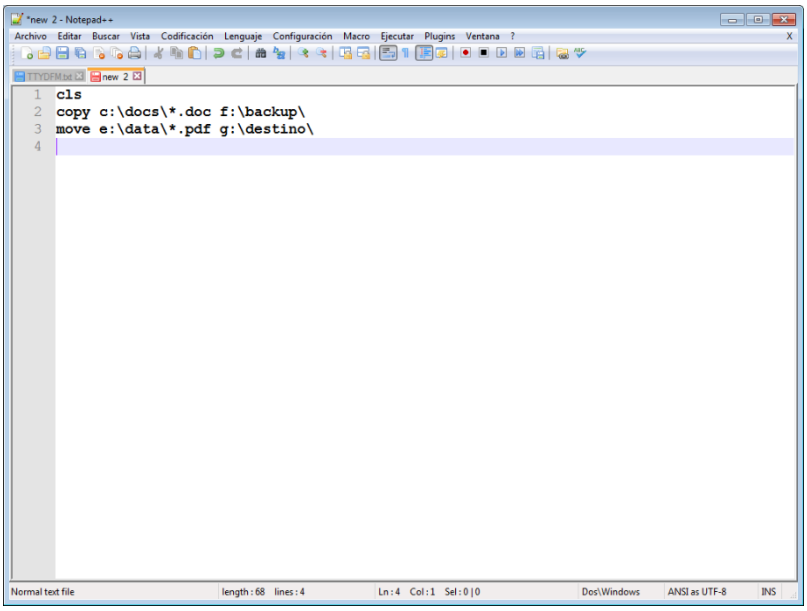
Este tipo de archivos nos brindan la opción de procesar una secuencia de comandos a partir de un archivo de texto sin formato. Si hacemos doble clic sobre él, todas las tareas que contiene se ejecutarán, una tras otra, de manera automatizada.

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

Para la automatización, deberemos proceder del siguiente modo:

- **Elección de las tareas a automatizar**

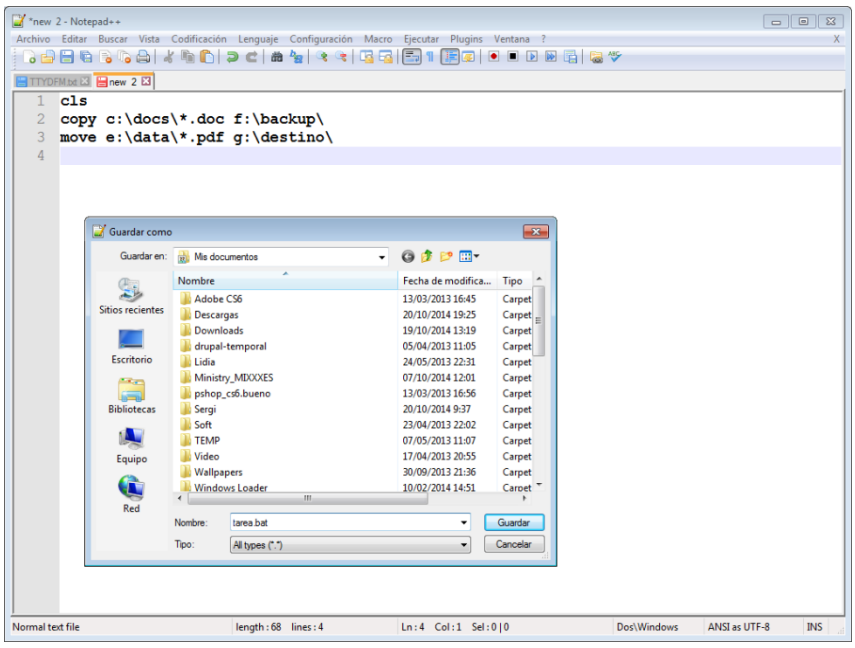
  En un documento en blanco, teclearemos los comandos correspondientes a las tareas que deseamos automatizar, pulsando *Intro* tras escribir cada una de ellas.



Escribimos los comandos.

- **Nombre del archivo**

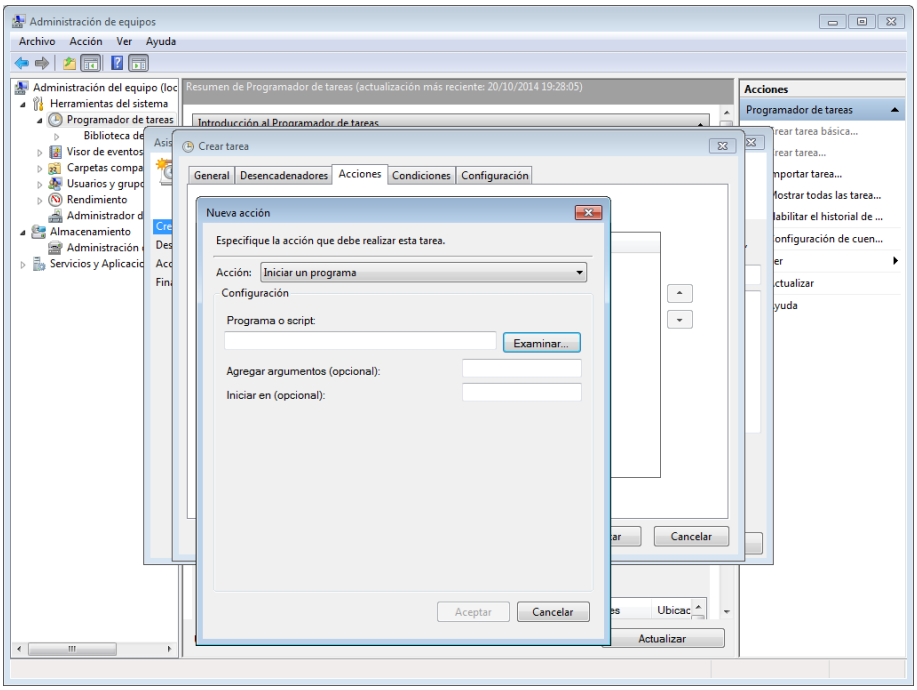
  Al guardar el archivo, es muy importante que le asignemos la extensión *.bat*. Solo así, más adelante, cuando hagamos doble clic sobre él, todos los comandos que hayamos incluido en él se ejecutarán de forma secuencial.



Guardamos el archivo con extensión BAT.

- **Programación de las tareas automatizadas**

  Hecho esto, podremos 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.battoexeconverter.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.

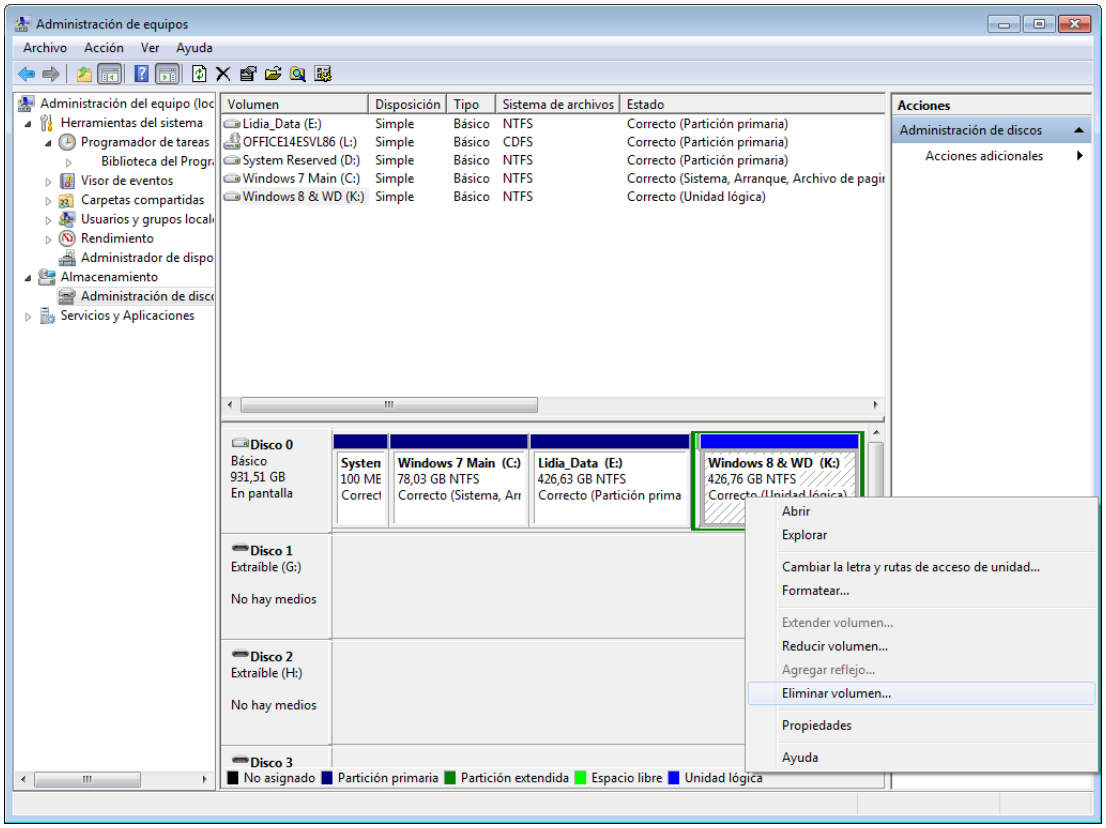
1.10 Herramientas de administración de discos. Particiones y volúmenes. Desfragmentación y revisión

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, deberemos 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 mostrará, accederemos al panel izquierdo y, en Almacenamiento, abriremos el apartado ***Administración de discos***. El área inferior de la ventana nos permitirá crear nuevas particiones si hay espacio disponible, eliminar particiones, y redimensionar las que tenemos creadas.



La Administración de discos en Windows 7 permite crear y eliminar particiones de disco.

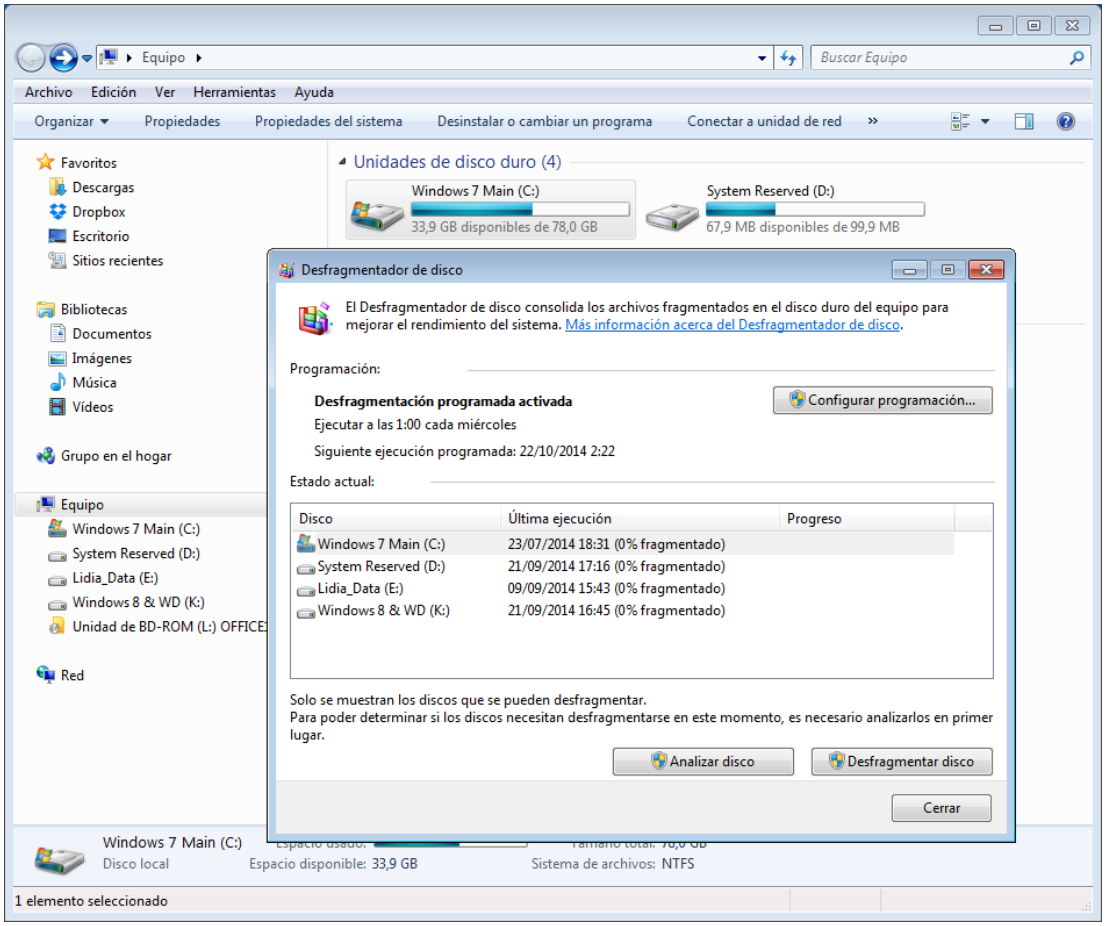
Por supuesto, para hacer uso de las herramientas que permiten administrar particiones es necesario disponer de privilegios de administrador, dado que eliminar una partición borra todos los datos que contiene la misma.

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

- **Gparted**
- **Pysdm**
- **Partitionmanager**

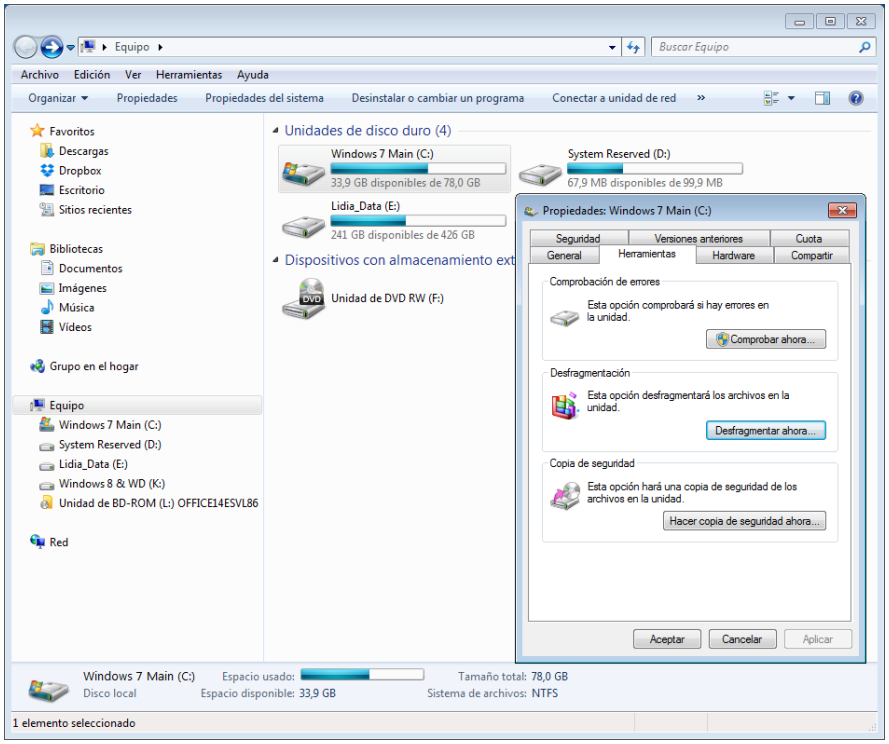
Por otra parte, cabe tener en cuenta que los sistemas de ficheros están sometidos a constantes procesos de creación, borrado y modificación de archivos que, a la larga, provocará que los ficheros se fragmenten y surjan huecos sin información en nuestras particiones. Esto origina una ralentización del 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 accederemos a las Propiedades de la misma a través de Equipo. En la pestaña Herramientas haremos clic en Desfragmentar ahora.



Desfragmentación de particiones en Windows 7.

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 7.

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*.

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

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

2. 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 conectarán 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.

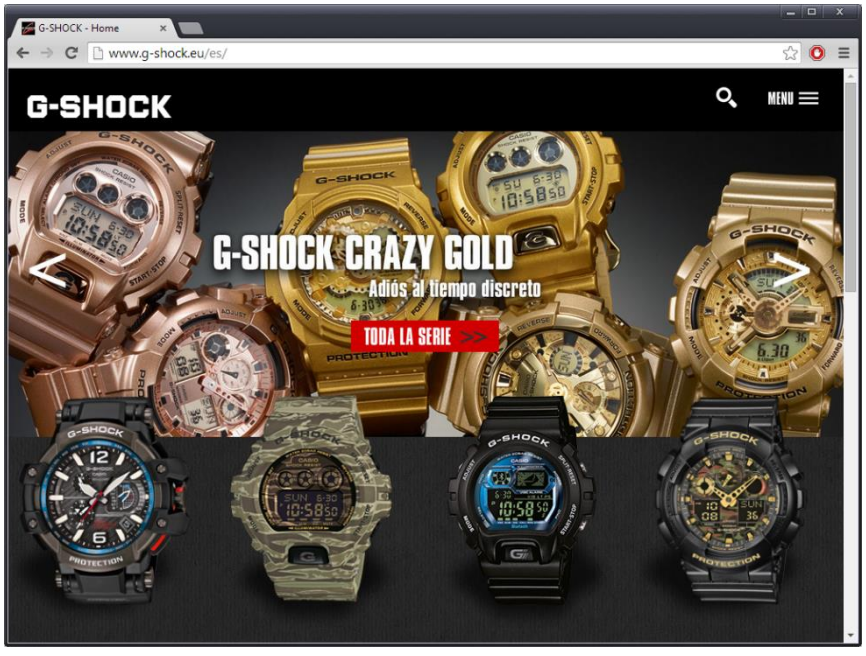
2.1. Estructura cliente – servidor

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, quizá 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.

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.

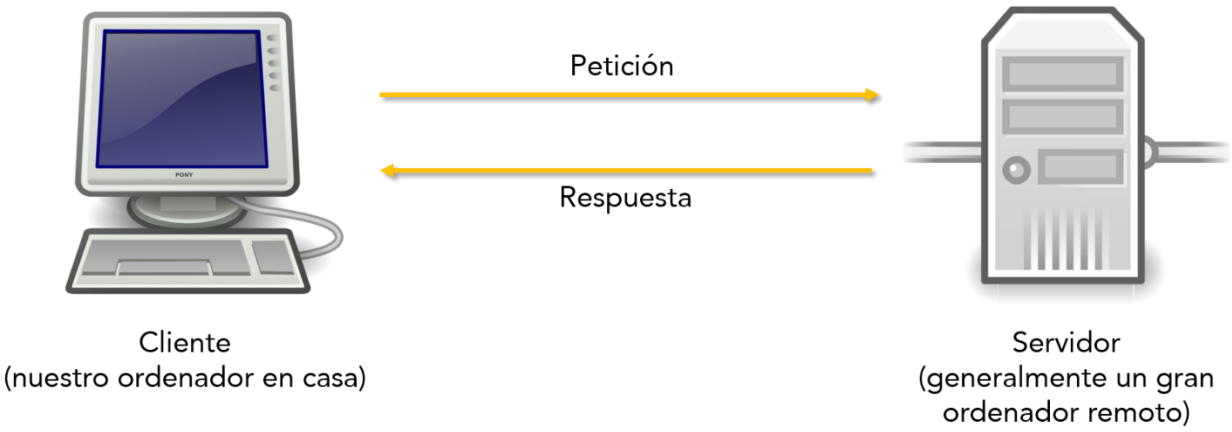
- **Cliente.** Es el sistema que precisa de servicios.
- **Servidor.** Es el sistema que proporciona servicios.



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

Desde el punto de vista lógico, cliente y servidor son elementos separados que establecen su comunicación mediante la red de comunicaciones y que 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 quien 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.



2.2 Protocolo LDAP

Consideramos el **LDAP** (*Lightweight Directory Access Protocol*) como un protocolo ligero de acceso a directorios. 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 siguientes son las más destacables:

- **Acreditación de usuarios**

  Los usuarios pueden acceder a sus respectivas cuentas desde cualquier equipo en red acreditado mediante LDAP.

- **Búsqueda de datos**

  Los usuarios pueden también 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**

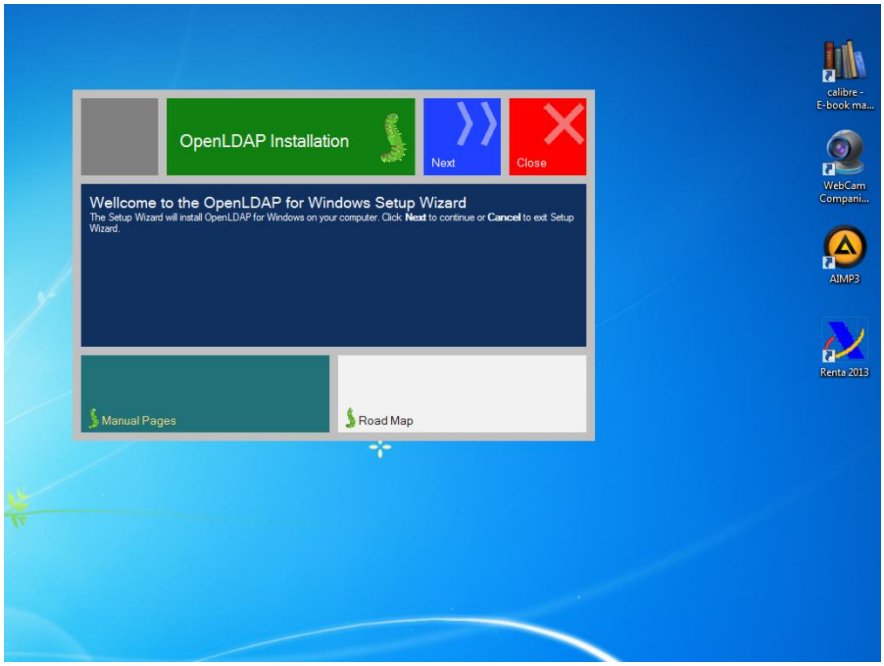
  De hecho, una vez hayamos configurado la base de datos LDAP podremos replicarla. Gracias a eso, se nos brinda la opción de configurar diversos servidores LDAP sincronizados. Cuando la red y cantidad de usuarios crecen rápidamente, la red puede balancear la carga entre varios servidores.

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 verificará que el usuario cuente 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 slapd ldap-utils"

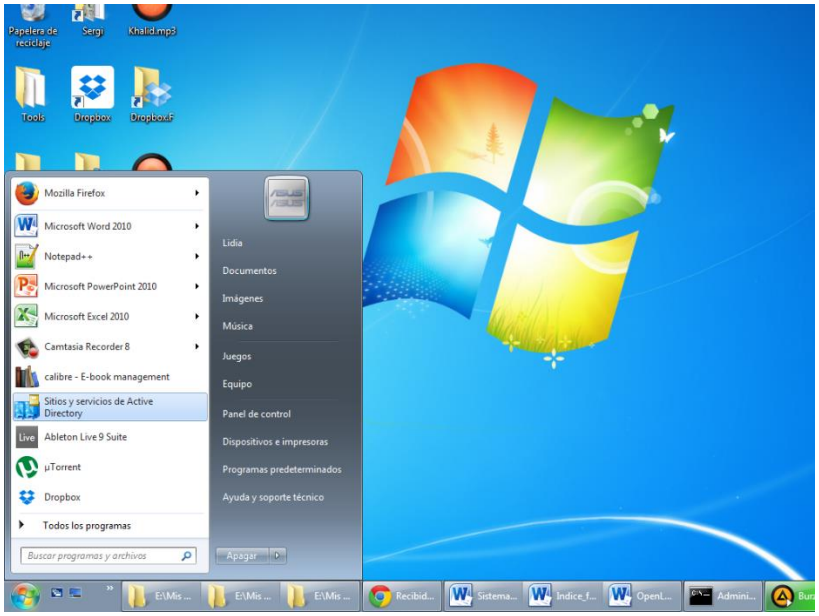
En Windows, para tal fin podemos utilizar *OpenLDAP for Windows* (http://www.userbooster.de/en/download/openldap-for-windows.aspx).



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 7 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.



Gestión remota de Active Directory desde Windows 7.

2.3. 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:

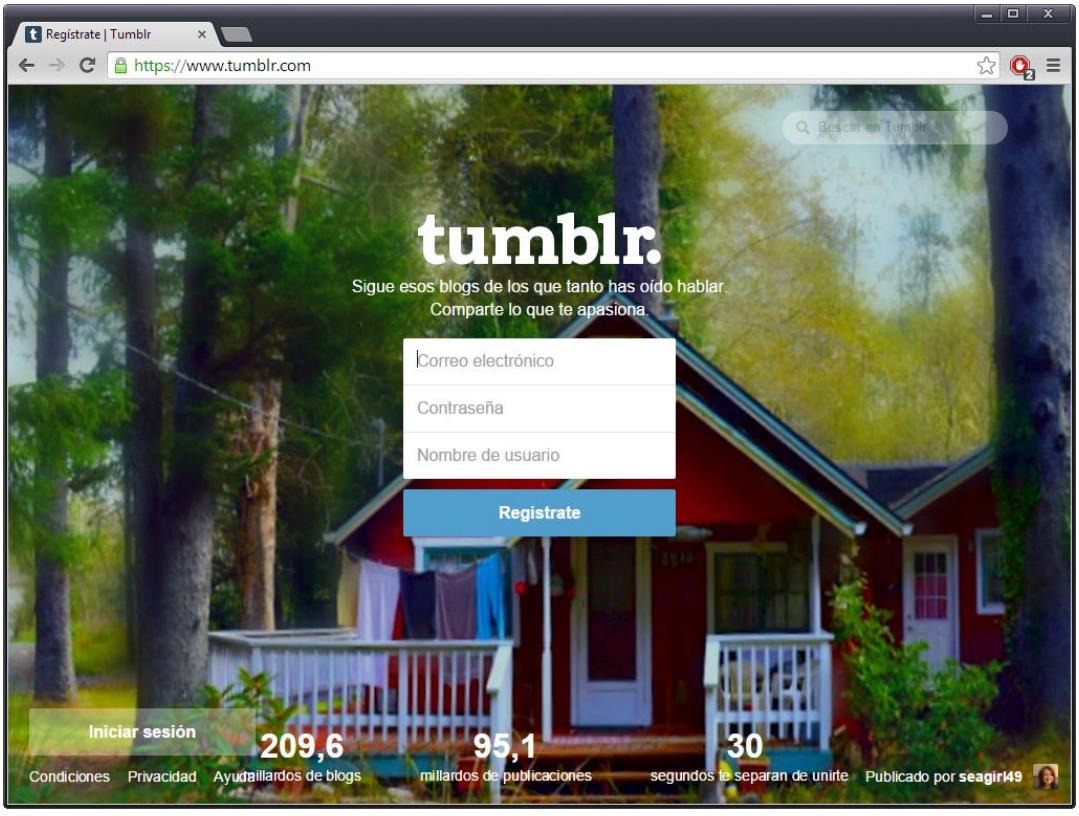
- **Dominios en redes**

  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, Tumblr.com sería un dominio válido. El dominio, en este caso, hospeda imágenes de todos sus usuarios.

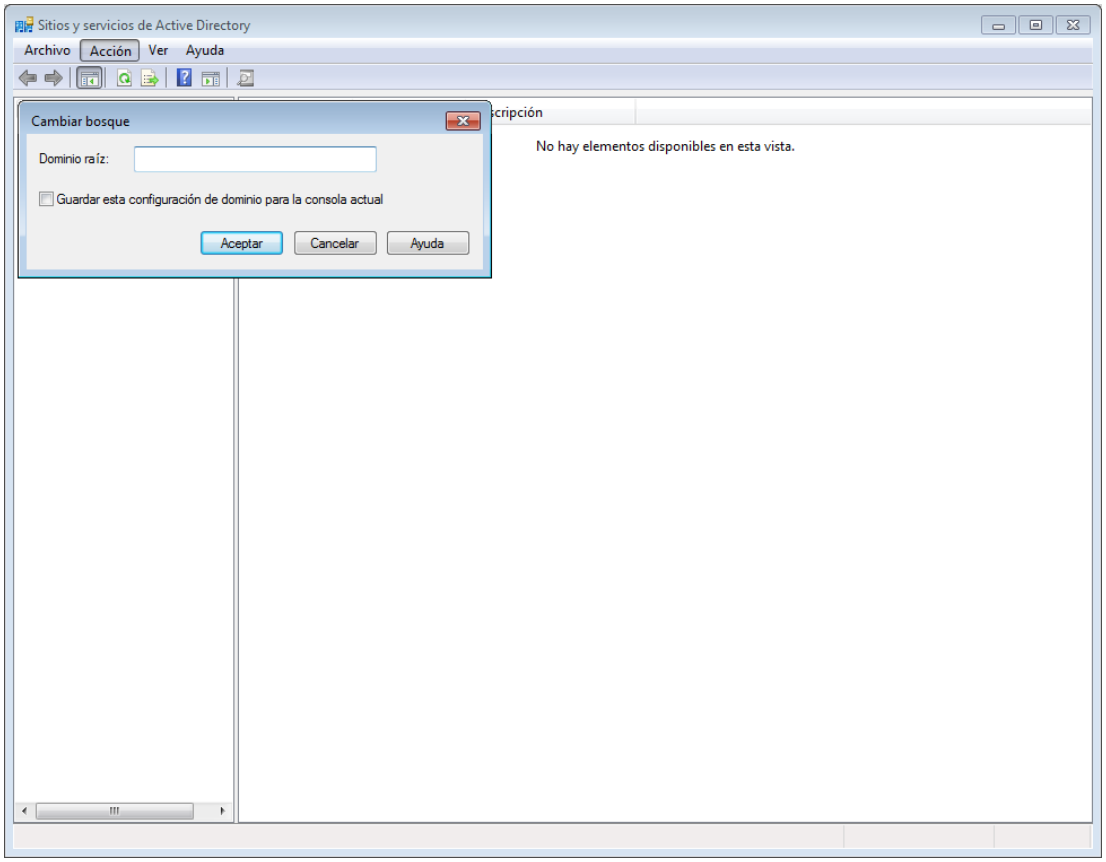


En Internet, los nombres de dominio suelen hacer referencia a la empresa u organización que gestiona el sitio.

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 estará relacionada con la primera, pero contará con características propias.



Conexión a un dominio de Active Directory desde Windows 7.

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, Xcascantex.tumblr.com sería un subdominio válido. El subdominio hospeda solamente imágenes del usuario Xcascantex.

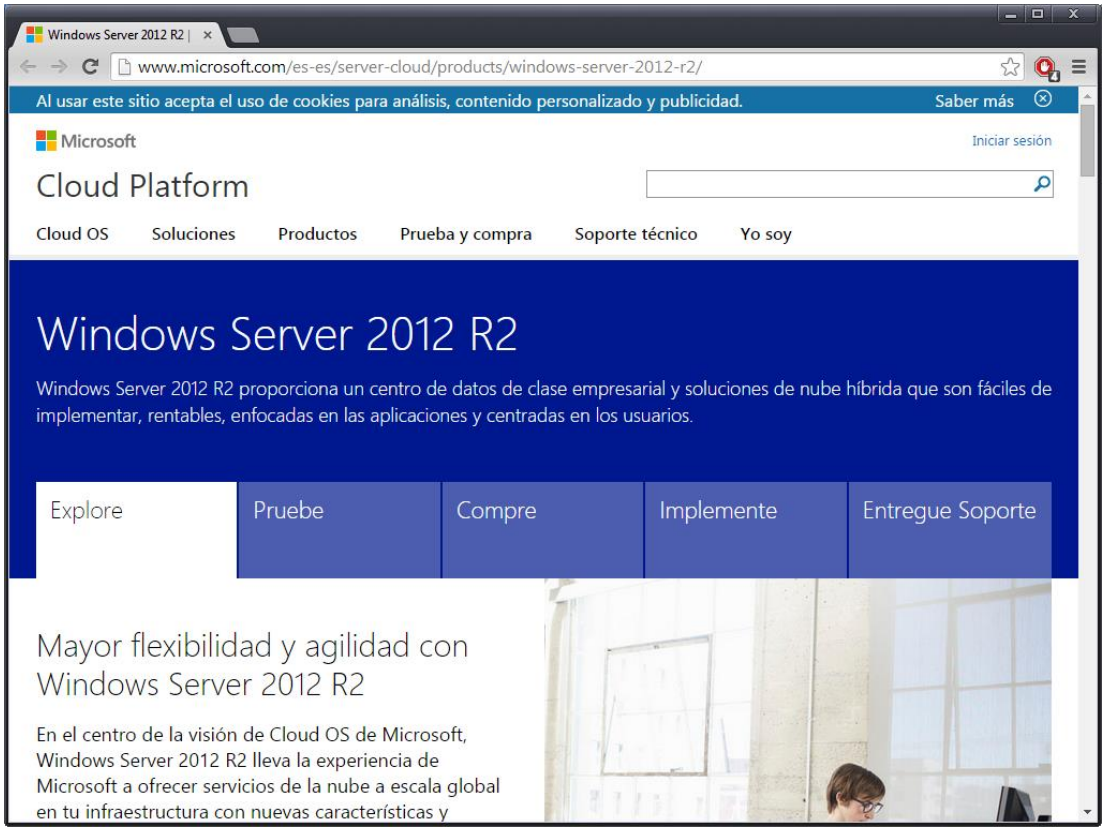
Las cuentas de usuario de Tumblr son un buen ejemplo de subdominio en Internet.

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

- **Requisitos para la creación de un dominio de red**

  En este caso, el principal requisito será 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.



El sistema operativo Windows Server nos brinda la opción de crear dominios y subdominios.

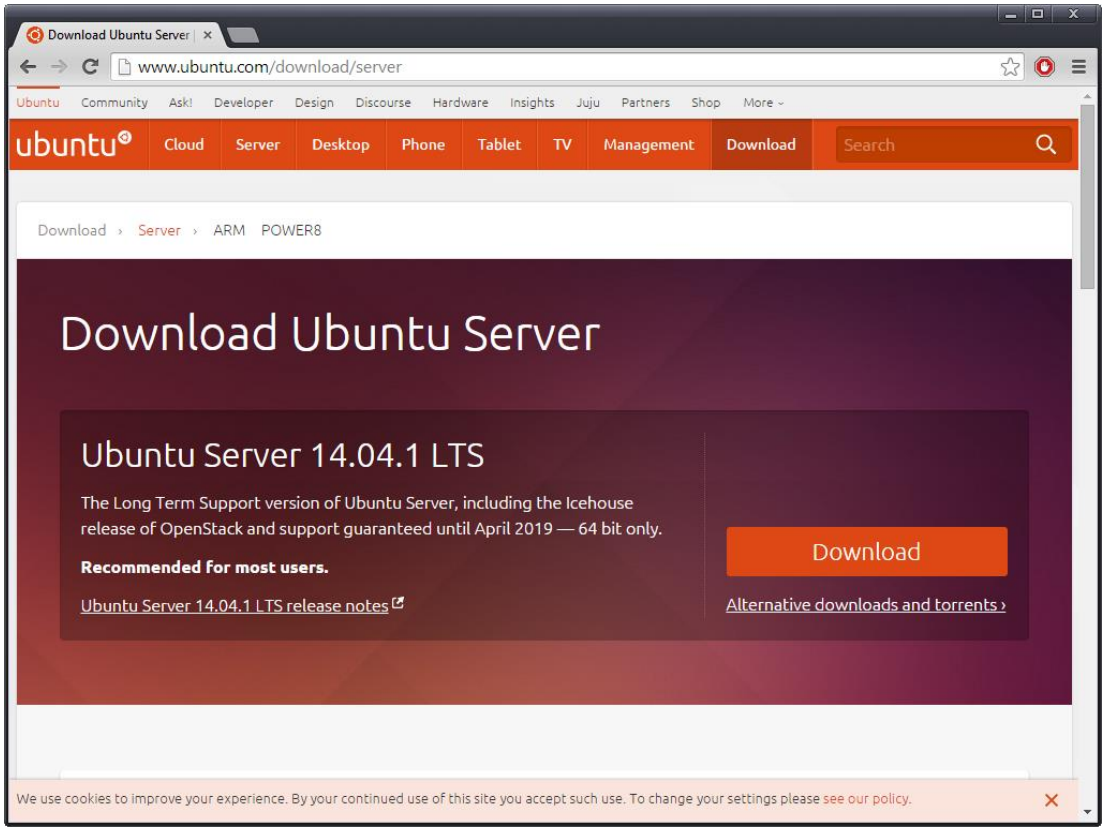
Para configurar el dominio desplegamos el menú Inicio y ejecutamos el comando ***dcpromo***. Seguidamente, se mostrará un cuadro de diálogo que nos informará de que se está instalando el software que nos brinda los servicios de dominio *de* ***Active Directory***.

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

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

"sudo aptitude install bind9"

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



En régimen de software libre podemos utilizar Ubuntu Server para crear un 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 poder alojar nuestras páginas online para darles difusión a través de la Red de redes.

  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/).

Son muchas empresas nos permiten adquirir dominios en Internet.

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.

2.4. 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 podrán 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 Directory Users and Computers*.

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***

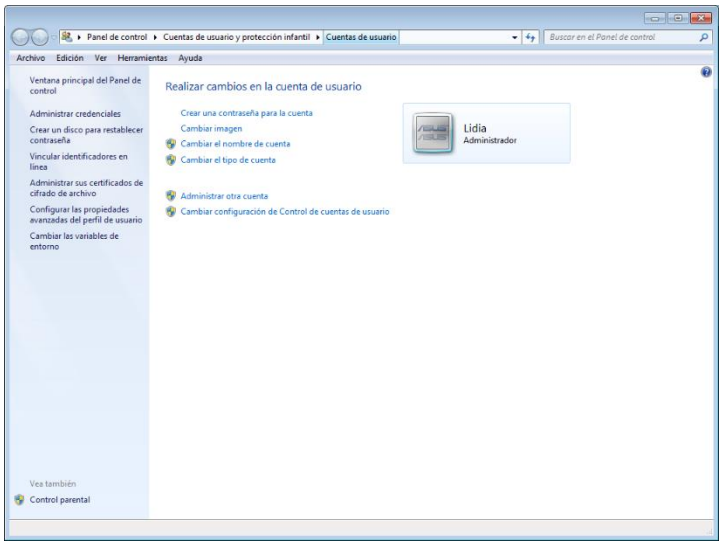
  Elimina una cuenta de usuario.

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. Recordemos 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.

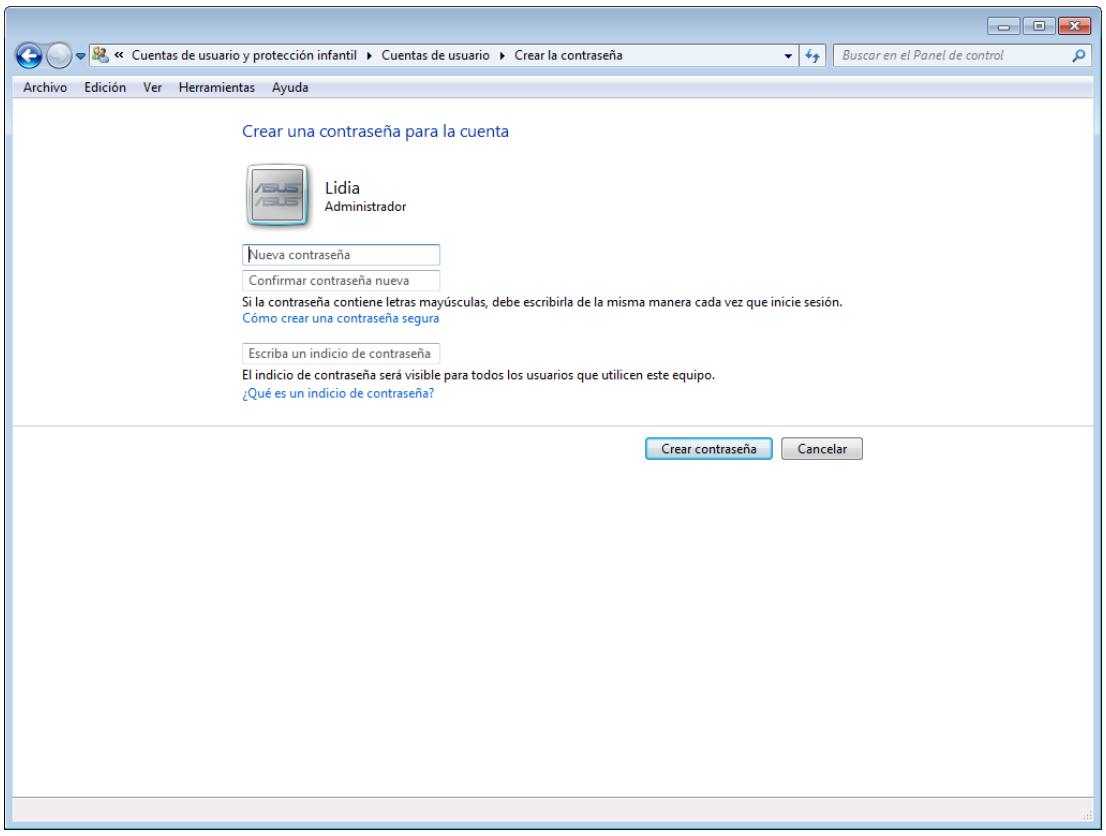


Al igual que sucede en Windows 7, la cuenta de Administrador de dominio en Windows Server tendrá plenos privilegios.

2.5. 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 autentificar 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 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 podrán acceder a ellos si estos son correctos. En caso contrario, se les denegará 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 cuenta.

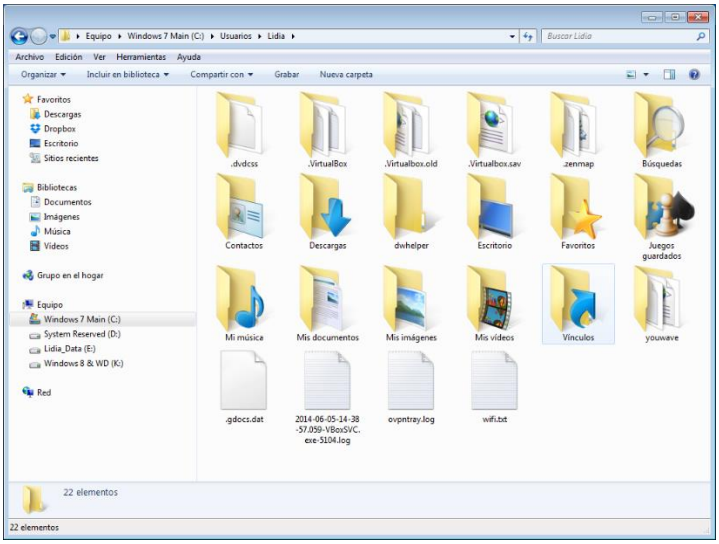
Asimismo, los bloqueos de cuenta pueden ir en función no solo del inicio de sesión con datos incorrectos, sino también de otros parámetros. Así, podemos definir bloqueos de cuentas si un usuario mantiene su sesión iniciada durante demasiado tiempo, etc.

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

2.6. 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 tendrá que configurar aplicaciones, dispondrá de sus documentos, etc.

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

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

Los perfiles obligatorios, por su parte, 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 agregaremos la extensión *.man*. Para convertir un perfil móvil en un perfil obligatorio accederemos al archivo *ntuser.dat*, donde se almacena la información referente al perfil, y le cambiaremos la extensión por *ntuser.man*.

2.7. Carpetas personales

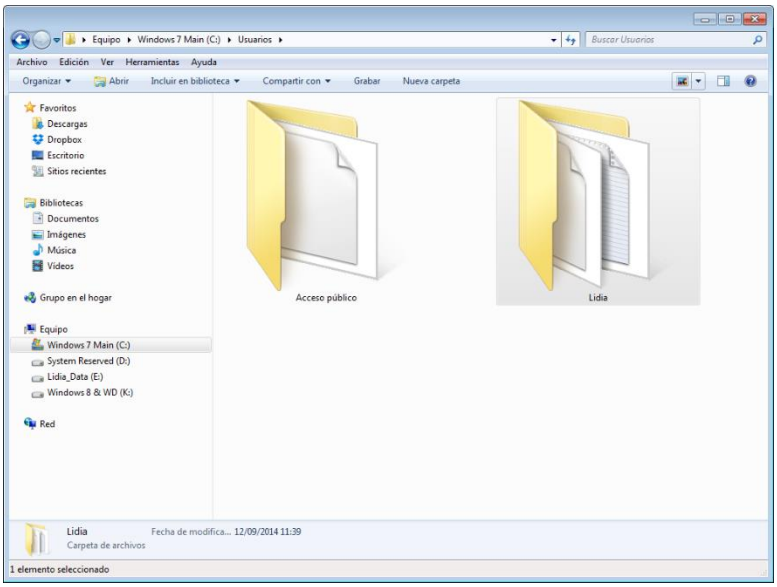
Una vez que ya hemos puesto en marcha nuestro dominio en red, se nos ofrece la posibilidad de crear en el servidor un directorio general en el que cada usuario podrá almacenar su información personal en su propia subcarpeta.

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 necesitaremos la herramienta ***Usuarios y equipos*** de Active Directory.

En el *Perfil* de los usuarios, activaremos 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, haremos clic en ***Conectar*** y seleccionaremos una letra de unidad, por ejemplo "*Z:*".



Subcarpetas de usuario en la carpeta "Users" de Windows 10.

2.8. Plantillas de usuario. Variables de entorno

Las plantillas de usuario se utilizan para ahorrarnos gran cantidad de trabajo.

Nos permiten, en definitiva, **definir una serie de características comunes que posteriormente podremos aplicar a un gran número de usuarios**. Imaginemos, por ejemplo, que queremos definirlas para todos los usuarios del departamento de marketing.

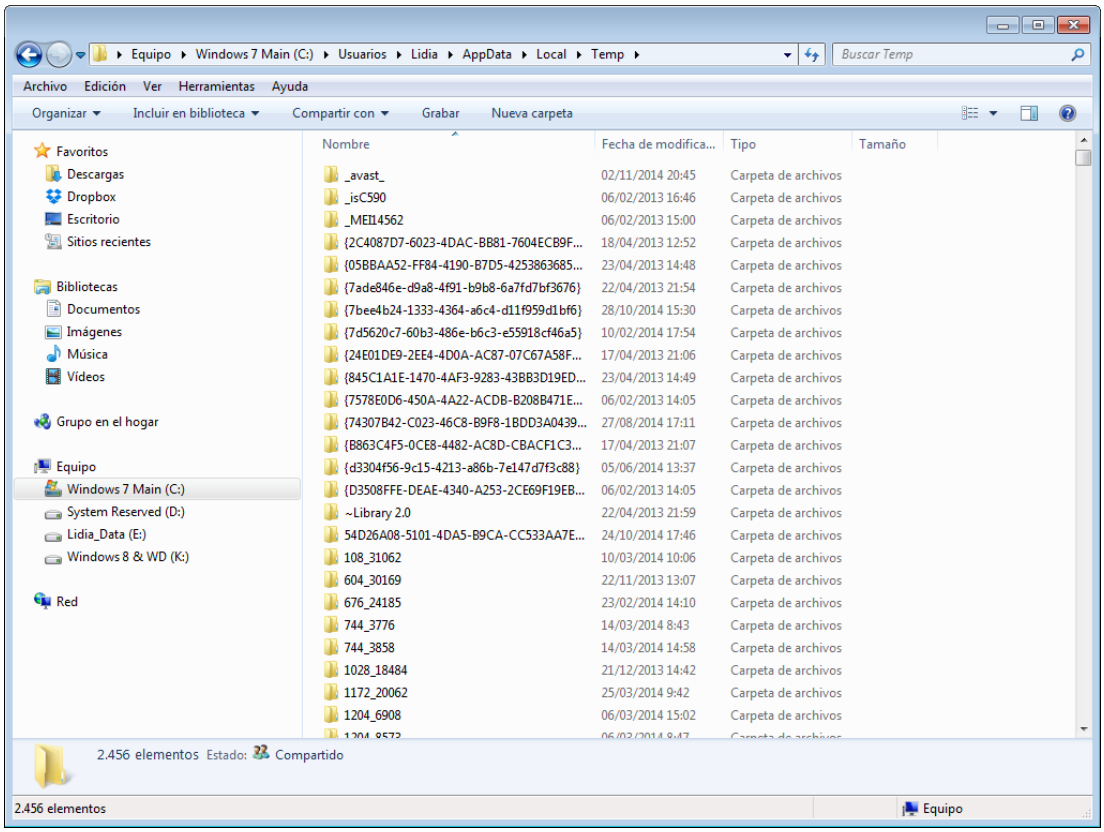
En este caso, crearemos una plantilla de usuario etiquetada como *Marketing*, rellenaremos sus datos y luego la aplicaremos a todos los usuarios de dicho departamento.

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

Posteriormente cuando creemos los usuarios, accederemos a sus **propiedades** y le asignaremos el perfil que hemos definido.

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

Si por ejemplo tecleamos ***%TMP%*** en la barra de direcciones del Explorador de Windows, accederemos a la carpeta temporal del usuario con el que hayamos 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, accederemos a la carpeta temporal del usuario con el que hayamos iniciado sesión.

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

2.9. 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.

En dicho entorno, por ejemplo, tenemos dos tipos de grupos:

- **Grupos de distribución.** Generalmente se utilizan para crear listas de distribución de e-mail.
- **Grupos de seguridad.** Estos son los que nos interesan, puesto que nos permiten asignar permisos a los recursos compartidos.

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

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

2.10. 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 ejercerá 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, su *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.

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 él pueden realizar acciones en cualquier dominio, pero sus permisos son efectivos únicamente para recursos del dominio en el que fue creado el grupo.

2.10. Instalación de Windows Server y Ubuntu Server

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

Empecemos por Windows Server 2016:

1. Configuramos la BIOS para que se inicie desde el DVD.
2. Insertamos el disco de instalación de Windows Server 2016 y reiniciamos el PC.
3. Al iniciar, seleccionamos el idioma de la instalación.
4. Elegimos Instalar.
5. Elegimos la edición de Windows 2016.
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. Finalizamos con la configuración básica de la admiración del sistema operativo.

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.

3 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**.

3.1 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:

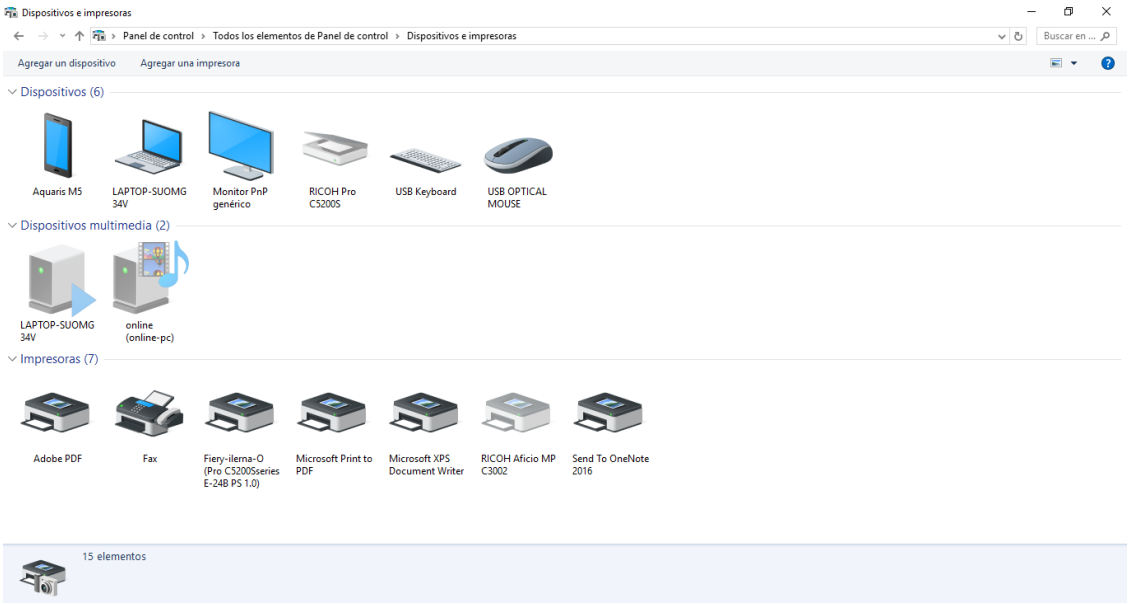
- **Equipos y recursos físicos**
  Forman parte del hardware. Pueden ser los distintos ordenadores, impresoras, escáner, monitores, etc.

- **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 contener 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.

3.2 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.

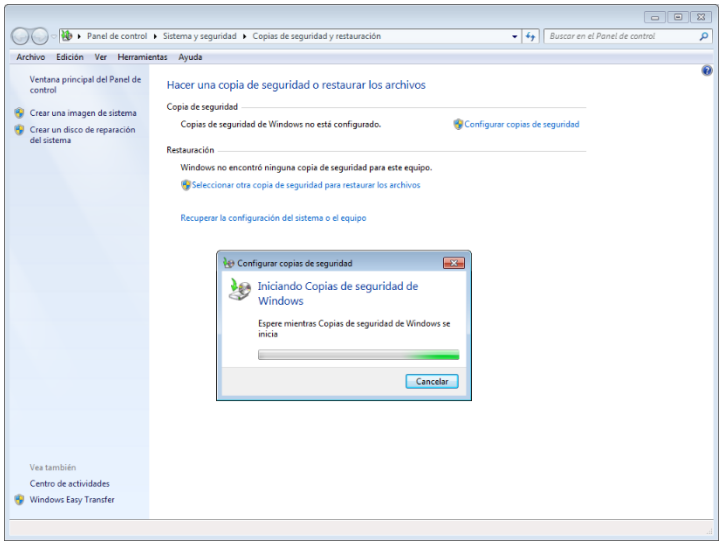
La estructura del dominio especifica qué acciones se autoriza a llevar a cabo a los usuarios y grupos:

- **Derechos (Pirvilegios)**

Son los atributos, tanto de usuarios como de los 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.



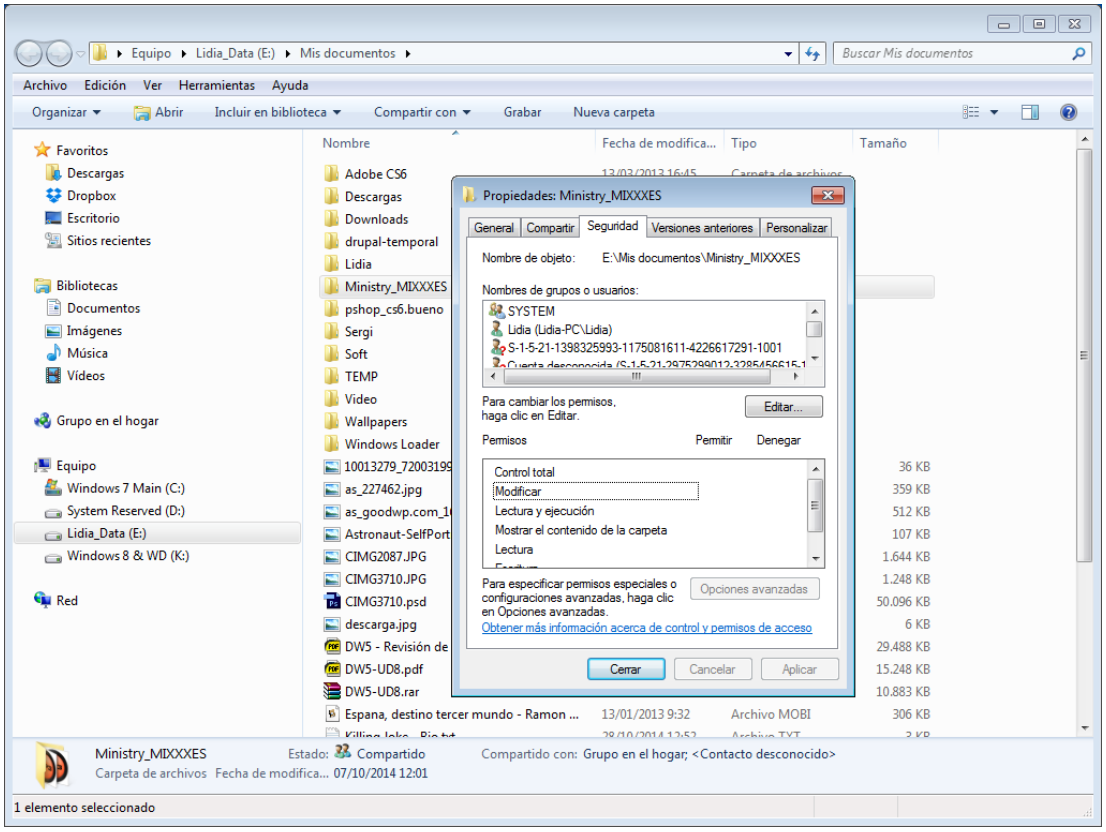
Los derechos pueden hacer referencia a acciones como realizar copias de seguridad.

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

- **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.



Los permisos nos autorizan a definir cómo se va a acceder a los recursos. Un buen ejemplo puede ser las carpetas compartidas.

3.3 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 conseguir proporcionar a clientes basados en Windows sus servicios.

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.

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 los casos, lo normal es que el usuario administrador disponga de todos los permisos. Aunque, si no nos conectamos 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:

"man smbpasswd"

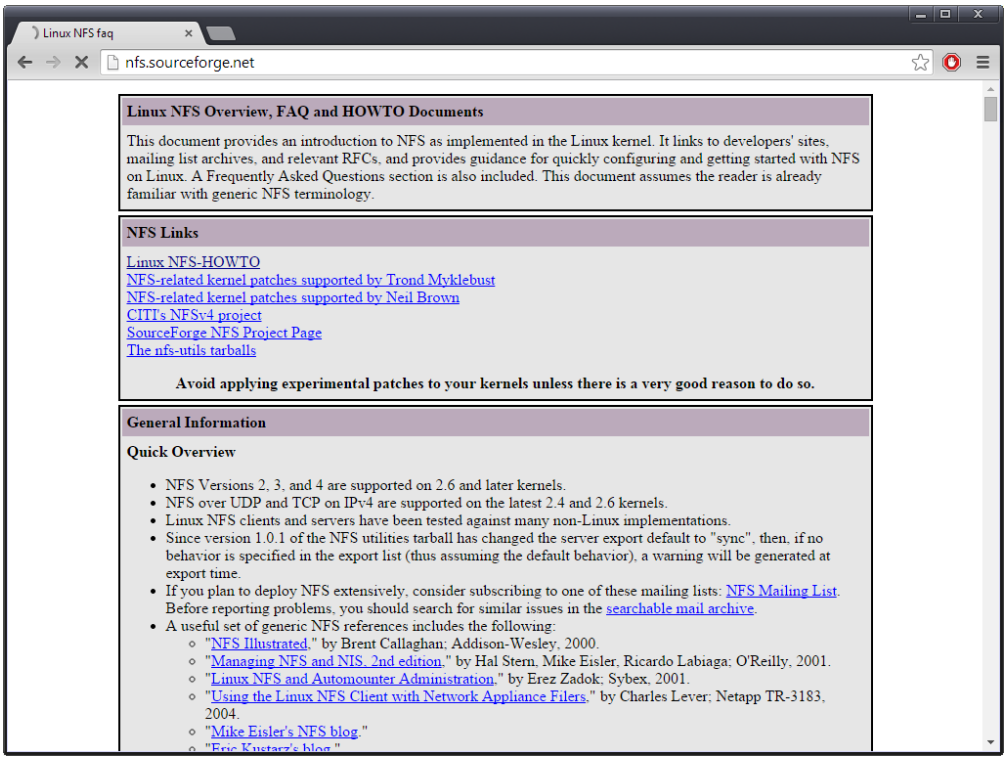
Por último, debemos tener presente que podemos usar SWAT. Su nombre proviene del acrónimo *Samba Web Administration Tool*, es decir, herramienta de administración web de Samba. Gracias a esta herramienta podemos configurar Samba en modo gráfico. Generalmente resulta más sencillo hacerlo así que mediante 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 percibirán como su 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.

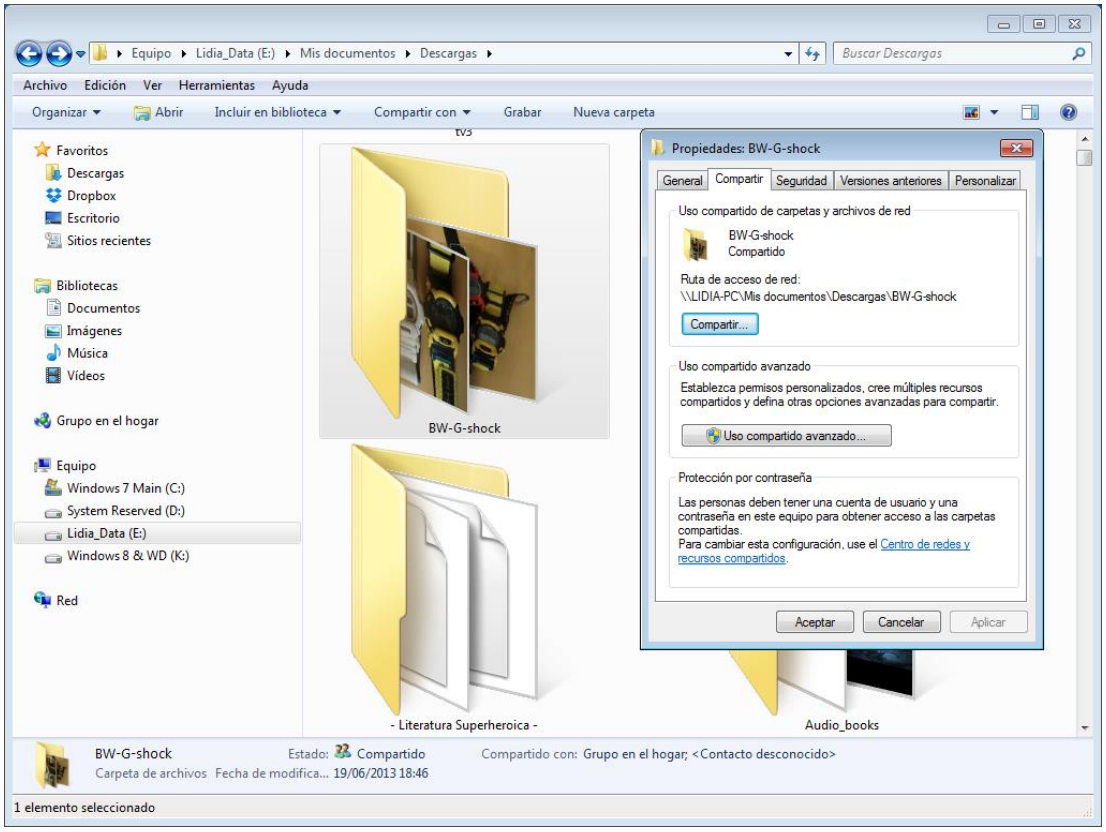


Gracias a NFS podemos conseguir que los ordenadores pertenecientes a una red local accedan a archivos remotos de manera transparente.

3.4 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 con 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:

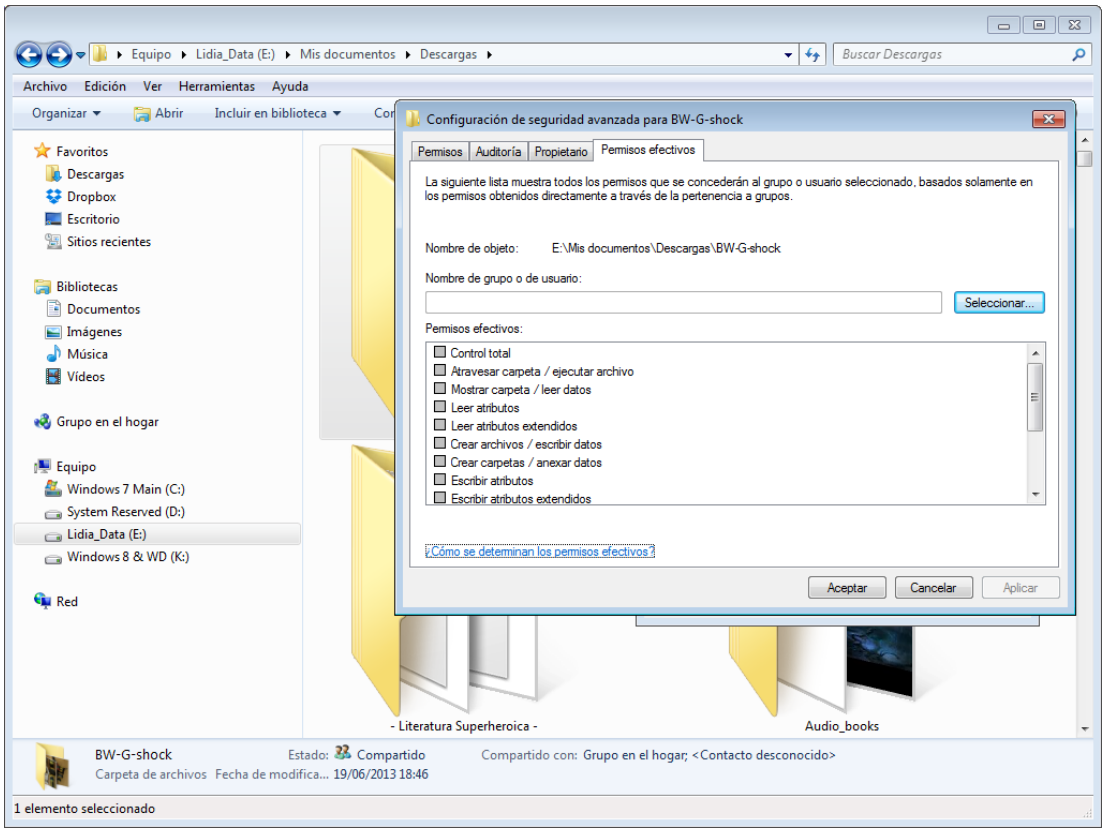
- **Nombre.** Es el nombre que vamos a asignar al recurso elegido. No tiene que coincidir necesariamente con el de la propia carpeta.
- **Usuarios.** Podemos especificar qué usuarios van a poder acceder al recurso.
- **Permisos.** Dónde vamos a asignar los permisos de lectura, escritura, etc. que se brindarán 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 7.

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**

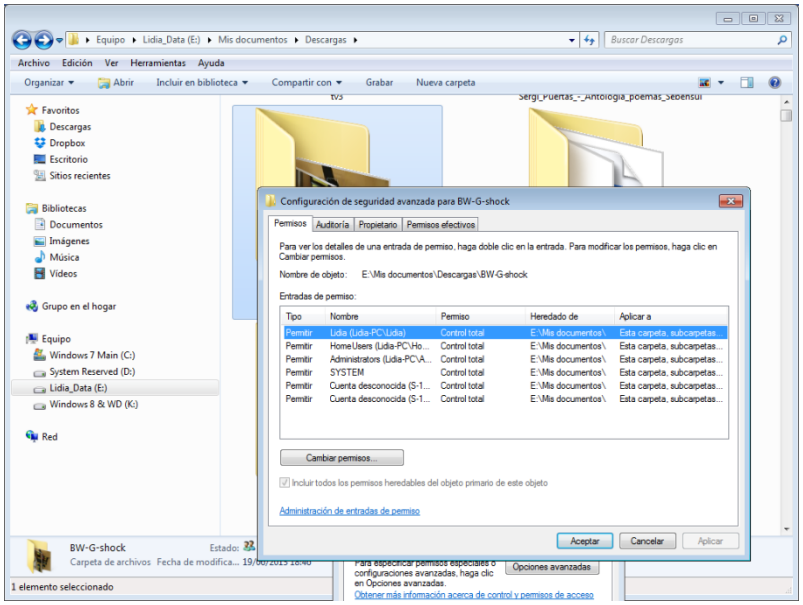
  Grupo local al que pertenece y nuestros permisos en él.

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 para 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 reemplazar 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.

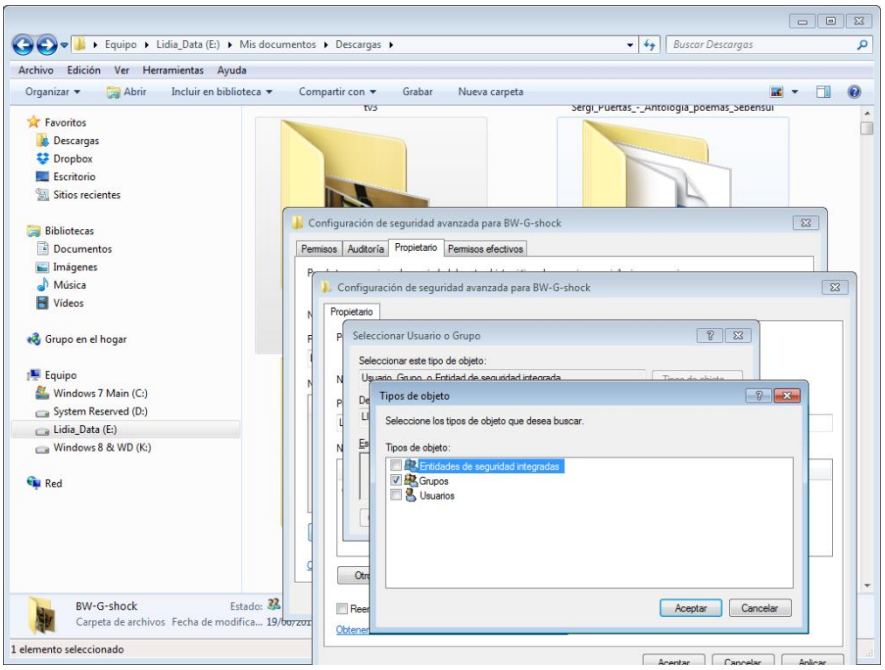
  En adelante, el elemento dejará de heredar los permisos del objeto principal.

3.5 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 a 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.

3.6 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.

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 quien 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*.

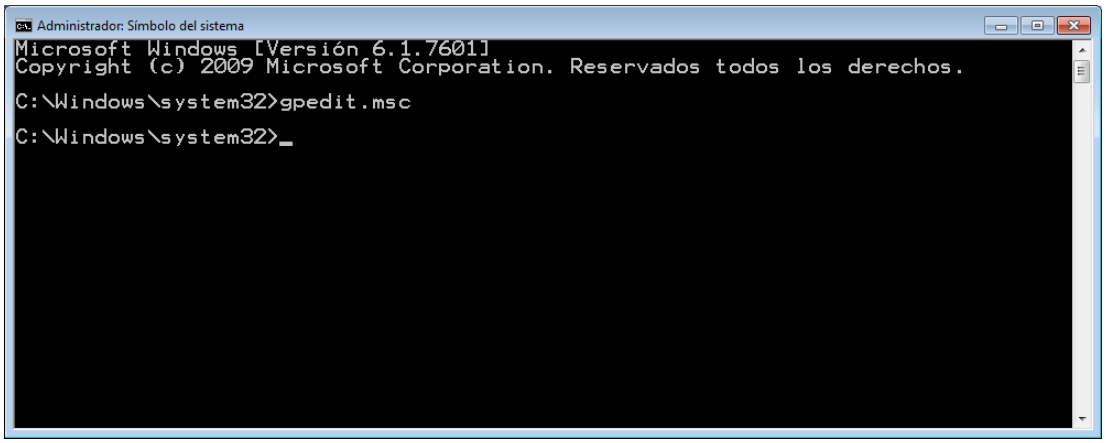
3.7 Directivas de grupo. Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbito de las directivas. Plantillas

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



Tecleando "gpedit.msc" en el "Símbolo del sistema" de Windows 7 accederemos 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"}

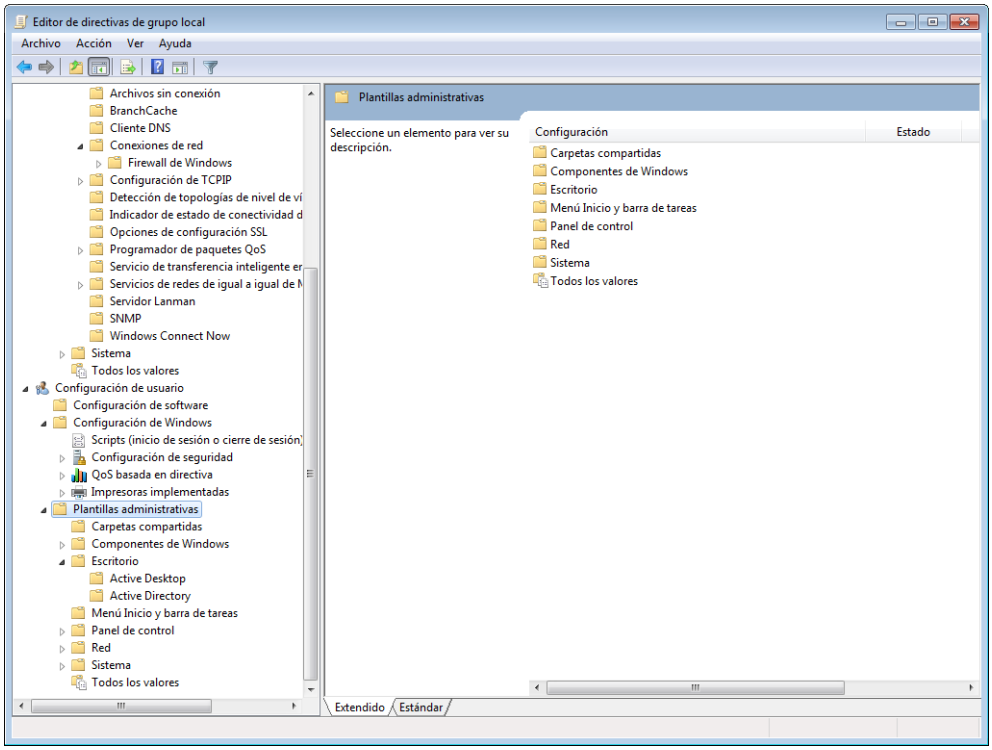
El objeto de la directiva de grupo local será *nombreDeEquipo*.

Por otra parte, si tecleamos lo siguiente:

{gpedit.msc /gpcomputer:"nombreDeEquipo.dominio.com"}

En tal caso haremos referencia a objetos de directiva de grupo almacenadas 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.

La imagen que se descarga del S.O desde su web (la ISO), viene sin configurar y sin apps (solo viene software básico). Sin embargo, desde nuestro S.O podemos crear una ISO que contenga ya determinadas apps. También guarda documentos y demás, así que se suele hacer sobretodo al principio, para que solo guarde las apps instaladas. Práctica muy usada en el mundo laboral. Con programas de licencia se suele hacer aparte, aunque como las licencias van por inicio de sesión con nuestro usuario, no debería haber problemas.

UF3: Implantación de software específico

1 Resolución de incidencias y asistencia técnica

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

A veces, es probable que se produzcan incidencias y problemas técnicos a pesar del cuidado con el que organicemos, por lo que tendremos que prestar asistencia a los usuarios. A continuación, lo veremos de forma más detallada.

1.1. 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 resultará 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.

- **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.

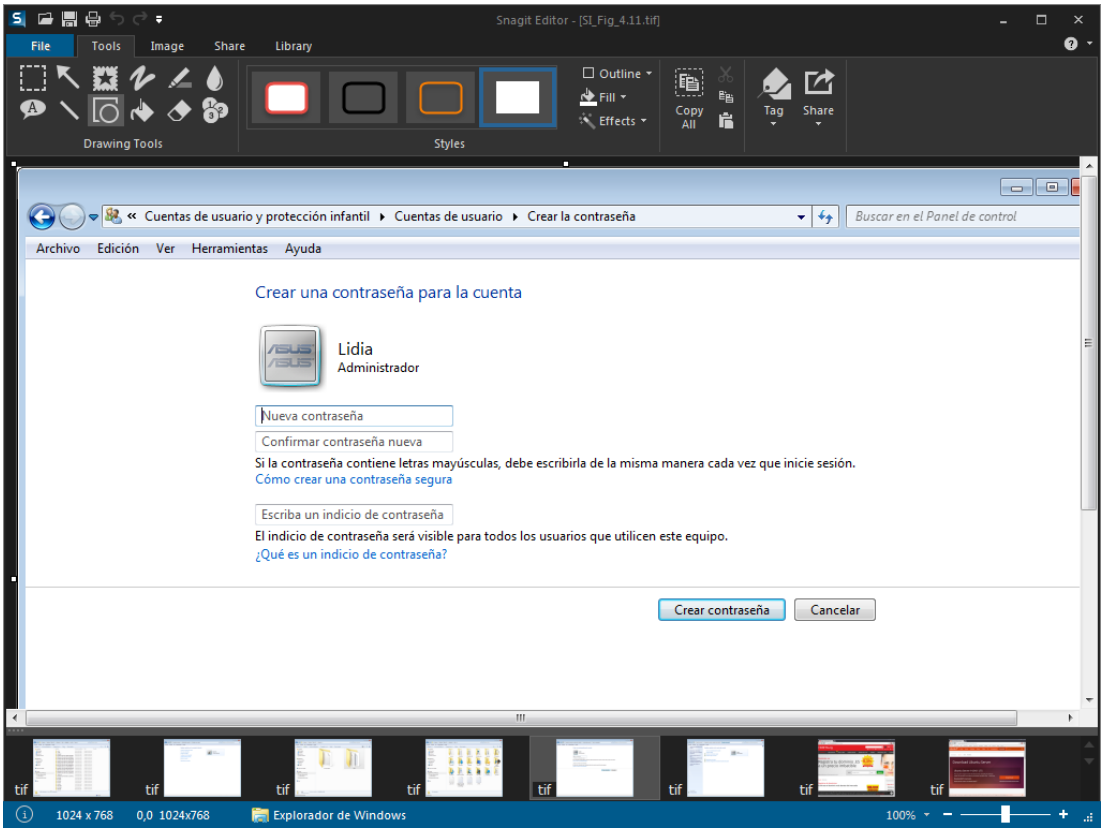
  Un exceso de información puede ser tan perjudicial para los usuarios que ya conocen el funcionamiento del programa como la falta de esta para quienes lo desconocen.

- **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 nuevas versiones del programa pueden variar sus características.

- **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*).



Snagit nos permite capturar áreas específicas de la pantalla para elaborar documentación y manuales.

- **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.

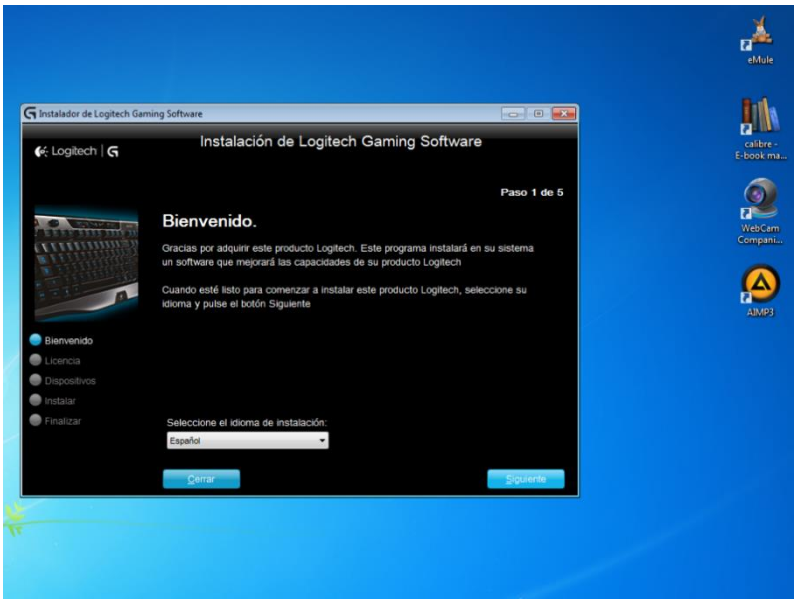
- **Glosario**

  En caso de que utilicemos términos con los que el destinatario de la documentación no esté familiarizado, un glosario le facilitará bastante la tarea.

1.2. Instalación y configuración de sistemas operativos y aplicaciones. Licencias de cliente y licencias de servidor

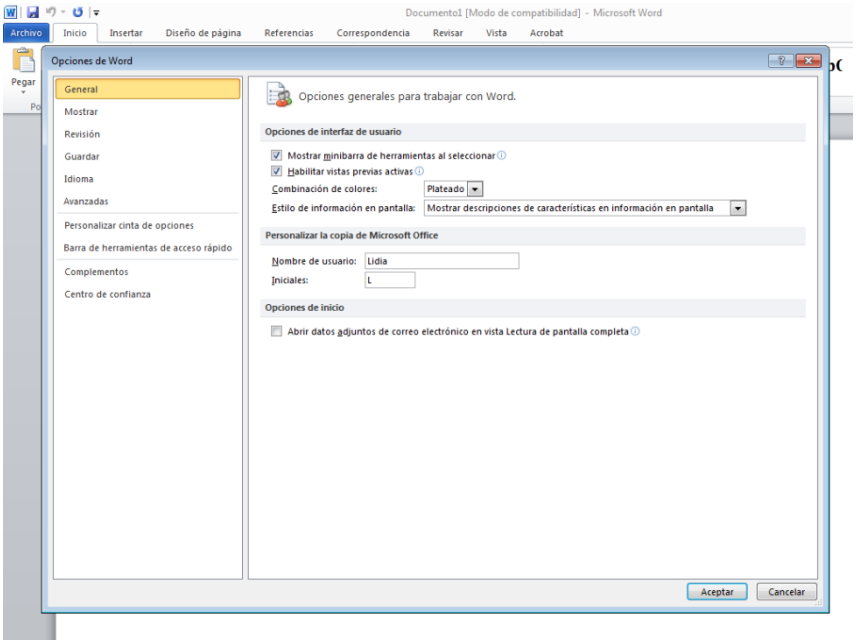
Cada usuario –o cada grupo– requerirá un sistema y unas aplicaciones específicas. Como administradores debemos estar seguros de que todos ellos tienen acceso solamente al software que necesitan. También debemos asegurarnos de que este y su configuración cubren sus necesidades.

Para agregar o quitar aplicaciones podemos recurrir en Linux al *Centro de Software* de Ubuntu, y en Windows al *Panel de Control*. En este último sistema, los archivos con extensión *.exe* abrirán los asistentes de instalación.



Instalación de una aplicación en Windows.

Tras la instalación debemos completar la instalación, personalizándola para cada usuario en la medida de lo posible.



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.

- **BIOS**

  Para ello, previamente, tendremos que entrar en la BIOS del ordenador para cerciorarnos de que se da prioridad de arranque al soporte elegido sobre las demás unidades.

Los procesos de instalación de sistemas operativos y aplicaciones pueden resultar muy trabajosos 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 nuestro primer apartado vimos hasta qué punto eran 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.

1.3. 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 solicitarán que vayamos eligiendo opciones. Por el contrario, bastará 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"

  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.

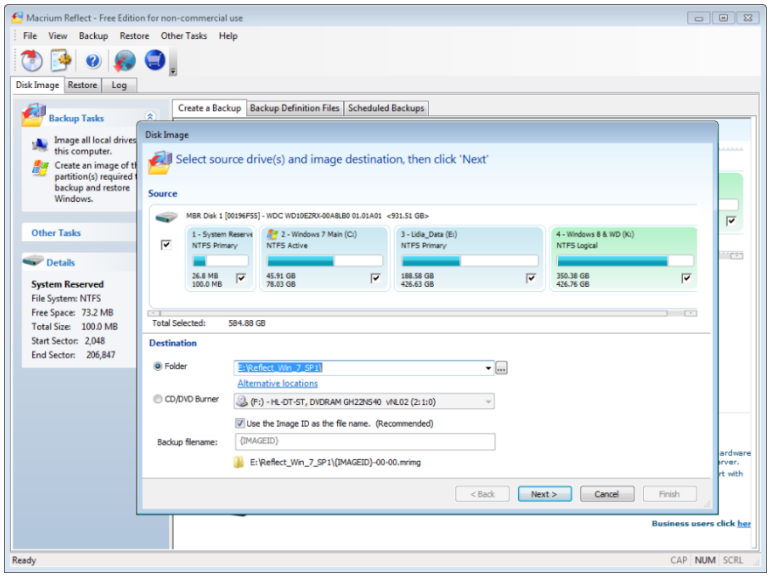
- **Crear una imagen de disco a partir de un sistema configurado**

  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 del 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.

(*www.macrium.com/reflectfree.aspx*)



Macrium Reflect nos permite replicar el sistema operativo y las aplicaciones de un equipo en muchos otros.

Los **archivos de respuesta** son ficheros que contienen definiciones y valores de configuración y que 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)*.

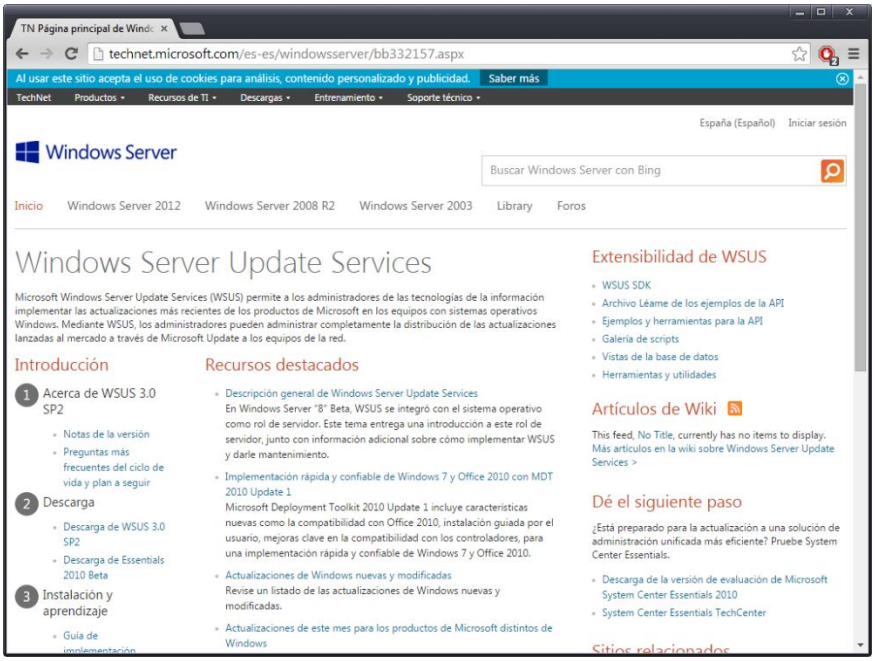
1.4. Servidores de actualizaciones automáticas

En nuestro primer capítulo vimos la importancia de mantener actualizado el sistema operativo y las aplicaciones. No obstante, si como administradores de red no gestionamos las actualizaciones, estas pueden tener consecuencias 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 situación podría llegar a colapsar la red.

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 equipos del dominio accederán a ellas de forma local.

Un buen ejemplo de software dedicado a este fin lo constituye Windows Server Update Services.



Windows Server Update Services nos servirá para habilitar un servidor de actualizaciones automáticas.

1.5. 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.

Estos 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, tendremos que poner en marcha mecanismos y herramientas para intentar evitar, en la medida de lo posible, que la incidencia se vuelva a producir.

Llegados a este punto, podemos tener **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.** Por otra parte, 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 podremos detectar y contar con un listado de incidencias que nos ayudarán 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 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 dictamine qué medidas tomar y qué debemos elaborar a partir de las experiencias previas.

Si nuestra conexión es limitada podemos no conectarnos al servidor y solo realizar transferencias de archivos.

1.6. Administración remota

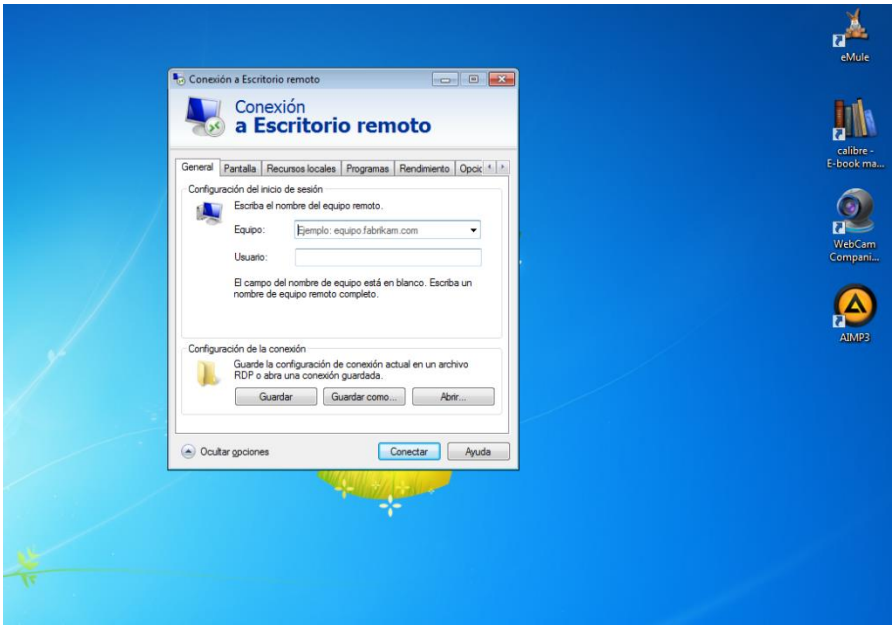
A menudo, tendremos que sentarnos frente a los equipos cliente para solventar incidencias y prestar asistencia a sus usuarios. Sin embargo, es posible que estos se encuentren en otro edificio, en otra ciudad o incluso en otro país.

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 e 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 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 levar 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 permite también 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, llevar a cabo 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, deberá 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 drive*r). Si estamos utilizando Windows 7 u 8 en ambos ordenadores desmarcaremos ambas opciones, pues no supondrá ninguna ventaja.

Por último, para que el software quede ejecutándose permanentemente en segundo plano, para que podamos 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 excelente software dedicado a este fin. Puede descargarse desde www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Bibliografía

https://sites.google.com/site/carlospesrivas/recursos/informatica-ciclos-formativos-de-grado-superior

http://apuntes-fp.blogspot.com.es/p/apuntes.html

https://ardillan.xyz/dam-desarrollo-de-aplicaciones-multiplataforma/

Francisco Javier Muñoz, Juan Ignacio Benítez, Ángel Lozano (2005). *Sistemas Operativos en entornos Monousuario y Multiusuario*. Aravaca, Madrid.

Mª Jesús Ramos, Alicia Ramos, Sebastián Rubio (2005). *Instalación y mantenimiento de equipos informáticos.* Aravaca, Madrid

ILERNA Online