Sistemas y Aplicaciones Informáticas

Sistemas Operativos Microsoft

1. MS-DOS.

1.1. Características y estructura.

- Es un sistema operativo de 16 bits **monousuario** y **monotarea** diseñado para la gestión de los datos de disco, que además se encarga de coordinar las operaciones de entrada/salida y la gestión de la memoria. Está estructurado de la siguiente manera:
  - **Procesador de órdenes**. El archivo COMMAND.COM se encarga de interpretar los comandos introducidos por el usuario. Consta de:
    - Sección residente. Se encuentra permanentemente en memoria, gestiona la carga de la sección transitoria del procesador de órdenes, la terminación de la ejecución de programas y la gestión de errores críticos.
    - Sección transitoria. Ejecuta todas las órdenes del DOS, cargando en memoria las órdenes externas y liberando después la memoria que éstas ocupan.
    - Sección de arranque. Ejecuta el archivo por lotes de arranque AUTOEXEC.BAT, liberando después la memoria ocupada.
  - **Núcleo**. Formado por el archivo MSDOS.SYS, que se carga en memoria durante el arranque. Se encarga de la gestión de los archivos y la memoria, y proporciona una conexión con el hardware.
  - **BIOS**. Al arrancar el ordenador utiliza las rutinas de la ROM y el archivo IO.SYS para crear un área de memoria que se encarga de la entrada/salida. El DOS se comunica con dichas rutinas mediante paquetes de información traducidos por un controlador de dispositivo.
- Las aplicaciones que corren bajo DOS tienen todos los privilegios del sistema. Ellas pueden acceder a cualquier almacenamiento, cambiar las funciones de control de la CPU, y utilizar cualquier dispositivo de hardware. Los servicios de DOS son solicitados cuando una aplicación llama a la interrupción INT 21. Esta instrucción busca un punto de entrada del administrador de servicios de DOS en una tabla de hardware y salta a la rutina en el módulo MSDOS.SYS.

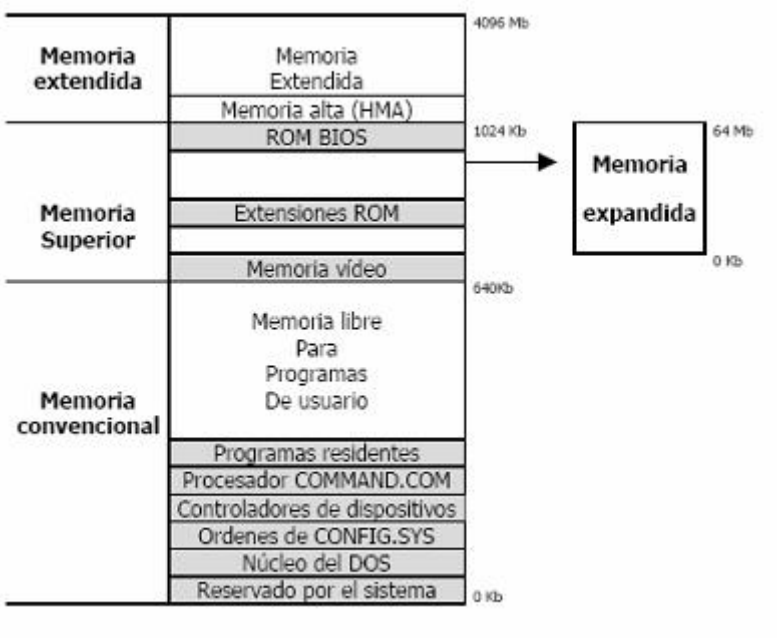
1.2. Zonas de memoria.

- **Memoria convencional**. Formada por los primeros 640 KB de la memoria RAM del ordenador. Es donde se cargan y ejecutan todos los programas de MS-DOS. Suele estar formada por:
  - Zona reservada por el sistema. Ocupa 2 KB y almacena la tabla de interrupciones, la tabla de características del ordenador, etc. Es imprescindible para que el ordenador funcione.
  - Núcleo del DOS. Formado por dos programas, IO.SYS y MSDOS.SYS, cuyo tamaño depende de la versión del sistema operativo.
  - Órdenes de archivos. Se cargan con el fichero CONFIG.SYS, estas órdenes son BUFFERS, FCBS, FILES, LASTDRIVE y STACKS.
  - Controladores de dispositivos. Se cargan con la orden DEVICE del fichero CONFIG.SYS, son el software necesario para la gestión de los dispositivos de entrada/salida (ANSI.SYS, HIMEM.SYS, EMM386.EXE, RAMDRIVE.SYS). Es opcional, pero a veces es necesaria.
  - Procesador de órdenes. Se encuentra en el fichero COMMAND.COM, es obligatorio y se carga después de los ficheros del sistema y de CONFIG.SYS.

- Programas residentes de usuario. Zona en la que se cargan los programas invocados desde el fichero AUTOEXEC.BAT, por ejemplo KEYB, DOSKEY, FASTOPEN, PRINT, etc.
- Memoria para programas de usuario. Zona libre para aplicaciones.

– **Memoria superior**. Comprende desde los 640 KB hasta los 1024 KB máximos que puede manejar directamente MS-DOS. Parte de ella es memoria ROM, pero entra dentro del espacio de direcciones del procesador. Está dividida en seis segmentos de 64 KB y se utiliza para almacenar programas del sistema y rutinas de inicialización y control. Suele contener lo siguiente:
  - Memoria de vídeo. Compuesta por dos segmentos, desde los 640 KB hasta los 768 KB, que almacena los caracteres y atributos que se visualizan en pantalla. Suele ir en la tarjeta gráfica que incorpora el equipo.
  - ROM BIOS. Formada por un segmento situado al final de la memoria superior, contiene un conjunto de rutinas básicas que gestionan las operaciones de entrada/salida. Se almacenan en memoria ROM y se encargan de varias funciones, como la transformación de las pulsaciones en el teclado en código ASCII, y del pase de los caracteres pulsados a la memoria de vídeo.
  - Extensiones de la ROM. Se encuentran entre la memoria de vídeo y la ROM BIOS. Gestionan los dispositivos del sistema como los controladores de disco, los controladores gráficos, etc.
  - Acceso a memoria EMS (Expanded Memory Specification). Es una parte de la memoria superior formada por un segmento (desde los 832 KB hasta los 896 KB) y situada entre la ROM BIOS y las extensiones de la ROM. Utilizada de la siguiente manera:
    - La memoria expandida está formada por bancos de memoria RAM hasta 64 MB, configurados como memoria EMS y divididos en páginas de 16 KB. En la zona de acceso a memoria expandida se crea un marco de página de cuatro páginas de 16 KB.
    - Como MS-DOS no puede acceder directamente por encima de los 1024 KB, se utiliza la zona de acceso a memoria expandida como lugar de intercambio con la memoria EMS mediante la técnica de conmutación de bancos de memoria.
  - Bloques de memoria superior (UMB). A partir de la versión 5.0 los huecos libres en la memoria superior pueden utilizarse para cargar los controladores de dispositivos (con DEVICEHIGH) y algunos programas residentes de DOS.

– **Memoria extendida**. Utilizada por los procesadores 386 y posteriores, ya que disponen de 32 bits. Comprende desde los 1024 KB hasta un máximo de 4096 MB, y está formada por:
  - Memoria alta (HMA). Es una zona de memoria extendida formada por 64 KB (desde los 1024 KB hasta los 1088 KB) que se utiliza para alojar programas residentes. Puede ser utilizada por un único programa al mismo tiempo.
  - Acceso a memoria XMS (eXtended Memory Specification). Utilizada por los 286 y posteriores, comprende desde los 1088 KB hasta el resto de la memoria RAM. Para ello necesita el controlador de dispositivo RAMDRIVE.SYS, que crea un disco virtual en memoria extendida y funciona como si el procesador accediera a un disco real. Para acceder a memoria XMS, el procesador tiene que trabajar en modo protegido y no en modo real.



- Otras zonas de memoria disponibles para MS-DOS son las siguientes:
  - Memoria CMOS RAM. Son 64 bytes a los que accede el sistema a través de determinados puertos. No entran dentro del rango de memoria direccionable.
  - Shadow RAM. Es un área de memoria perteneciente a la memoria superior en la que se crea una copia de las rutinas de la ROM, acelerando de este modo el proceso de manejo de dichas rutinas. Es posible activar y desactivar este tipo de memoria desde el menú de configuración de la BIOS.
  - Memoria caché. Permite acelerar el manejo de datos de uso frecuente en las unidades de disco. Es posible crear un área de memoria (convencional, expandida o extendida) donde se pueden almacenar dichos datos mediante la orden SMARTDRV.

1.3. Organización lógica del disco.

- Las particiones son divisiones lógicas efectuadas en un disco duro. Responden a la necesidad de compartir un mismo disco duro para varios sistemas operativos. Cada partición tiene la estructura lógica correspondiente a su sistema operativo.
- En el primer sector de todo disco duro se sitúa una tabla de particiones (Master Boot Record o MBR). Puede haber un sector de arranque por cada partición, por lo que es posible que en un disco duro existan cuatro sectores de arranque.
- Esta tabla de particiones incluye una tabla donde definimos las cuatro particiones que pueden estar presentes en nuestro disco duro y un pequeño programa que permite localizar la partición activa, leer su sector de arranque y usarlo para arrancar nuestro sistema informático.
- La MBR está situada en el primer sector del disco duro, de modo que su tamaño es de 512 bytes. Existe un programa al principio conocido como programa MBR o gestor de arranque que ocupa 445 bytes. Un programa MBR estándar, leerá la tabla de particiones y escogerá la partición primaria que esta marcada como activa. El MBR lee el primer sector de esa partición, y le cede el control de la CPU a ese programa (Boot Sector).

- No existe un programa MBR estándar. En realidad, el código que se encuentra aquí, puede ser muy variado, aunque normalmente todos son compatibles. Cada una de las cuatro entradas de 16 bytes que tiene la MBR se guardan campos que indican lo siguiente:

Dirección.	Contenido.	Tipo.
+00h	Estado de la partición: 00h – Inactiva 80h – arranque (activa)	1 Byte
+01h	Cabeza de lectura / escritura donde comienza la partición.	1 Byte
+02h	Sector y cilindro donde comienza la partición.	2 Bytes
+04h	Tipo de partición: 00h – Libre 01h – DOS con la vieja FAT de 12 bits. 02h – XENIX 03h – XENIX 04h – DOS con FAT 16 05h – Partición extendida. 06h – Partición DOS > 32 Megas. 0Bh – Windows FAT32 0Ch – Windows FAT 32 LBA 0Eh – VFAT 16h – Hidden FAT 16 (Oculta) 63h – Unix 65h – Novell Netware Etc.....	1 Byte
+05h	Cabeza de lectura / escritura donde termina la partición.	1 Byte
+06h	Sector y cilindro donde termina la partición.	2 Bytes
+08h	Dirección del primer sector de la partición. (Sector de arranque).	4 Bytes
+0Ch	Número de sectores en esta partición.	4 Bytes

Contenido de cada una de las 4 entradas de la tabla de particiones.
Longitud = 10h = 16 Bytes.

- Las particiones de un disco duro pueden ser de dos tipos:
  - Primarias. Puede haber un máximo de cuatro en un disco duro. Cada partición primaria tiene su propio sector de arranque y forma un volumen. Sólo el sector de arranque de la partición primaria es válido para arrancar el sistema operativo.
  - Extendidas. No puede haber más de una partición extendida en un disco. Una partición extendida no forma ningún volumen, ni tiene un sector de arranque como tal, en realidad es un contenedor de unidades lógicas. El sector de arranque de la partición extendida solo contiene información sobre las unidades lógicas que se encuentran dentro de ella, y los sectores de arranque de las unidades lógicas contienen información especifica.
- En un disco duro podemos tener hasta cuatro particiones como máximo. De las cuatro, solo una puede estar definida como activa al mismo tiempo, que será la que arranque el sistema.
- La tabla del MBR identifica la localización y tamaño de la partición extendida, pero no contiene información sobre las unidades lógicas creadas dentro de esta partición extendida. Ninguna de estas unidades lógicas pueden ser marcadas como activas, Si instalamos un sistema operativo en alguna de estas particiones lógicas, pero nunca podrá ser cargado, ya que no podemos marcar esa partición como activa, y por lo tanto no podemos indicar que sea el disco de arranque.
- Existen unos programas especiales conocidos como gestores de arranque que, instalados en el MBR, permiten indicar en el momento del arranque, de qué volumen vamos a cargar el boot sector, sin importar si dicho volumen es una partición primaria o una unidad lógica.
- El MBR es creado por primera vez en un disco mediante el comando FDISK. El sector de arranque de las particiones primarias y el sistema de archivos se crean ejecutando el comando FORMAT. Las reglas de numeración de las particiones de cara al MS-DOS son:

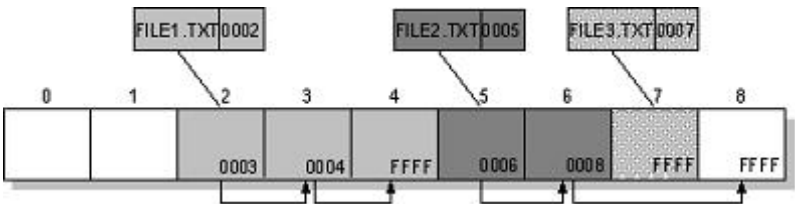
- Se enumeran y se asignan letras de disco consecutivas a la partición primaria activa o a la primera partición primaria de cada disco del sistema.
- Se localizan si existen particiones extendidas y se asignan consecutivamente las letras a las unidades lógicas empezando por el primer disco y continuando por los siguientes.
- Una vez recorridos todos los discos del sistema, se empieza de nuevo por el primer disco y si quedasen particiones primarias sin enumerar se enumeran una a una hasta finalizar el primer disco. A continuación, el resto de discos si existiesen.
- A continuación se enumeran las unidades de medios removibles.

– Esta enumeración bajo MS-DOS de las particiones es cierta para los controladores IDE en placa base y para los posibles controladores añadidos (IDE o SCSI) a nuestro sistema y que se carguen en memoria interceptando la INT 13 de la BIOS. Existe además un limite de ocho discos duros que la BIOS de una maquina puede ver.

– MS-DOS no trabaja directamente con los sectores físicos del disco, sino con clusters, que son agrupaciones de 2, 4, 8 ó 16 sectores. De esta manera, en cada operación de entrada/salida se accede a más información. Tiene el inconveniente del desaprovechamiento del espacio en disco, por lo que hay que desfragmentar a menudo. Los clusters en los que se almacenan los ficheros no tiene por qué ser contiguos. MS-DOS referencia los clusters por un número olvidándose de caras, pistas y sectores.

– La estructura lógica del sistema de archivos MS-DOS es la siguiente:

- Sector de arranque (boot). Se localiza siempre en el primer sector de la partición activa del disco y ocupa 512 bytes. Contiene un pequeño programa que se ejecuta al arrancar el ordenador y que carga el sistema operativo en memoria, y una tabla con información de la estructura física del disco (BIOS Parameter Block).
- Tabla de asignación de archivos (File Allocation Table). Organiza la información en forma de archivos dentro de la zona de datos. MS-DOS utiliza FAT16, que es una versión del sistema de archivos **FAT** que soporta hasta 65.535 unidades de asignación (direccionables con 16 bits, de ahí el nombre) de hasta 32 KB cada una. De todas las unidades de asignación, 18 están reservadas para el sistema. Por lo tanto, el tamaño máximo de una partición que use FAT16 es de unos 2 GB (65.535-18 x 32 KB). La FAT indica a MS-DOS en qué clusters está grabado un archivo. Debido a la importancia de la FAT, se crean dos iguales una detrás de otra como medida de seguridad.



Cada uno de sus elementos puede contener una de las siguientes informaciones:

- Un cero, significa cluster libre.

- Marca de último cluster del archivo.
- Número del siguiente cluster del archivo.
- Marca de cluster defectuoso.

* Directorio raíz. Se crea a continuación del último sector que ocupa la FAT y ocupa un número fijo de sectores. Contiene una entrada de 32 bytes por cada elemento que posee el directorio, en la que se almacena lo siguiente:

DESCRIPCIÓN	BYTES
Nombre	8
Extensión	3
Atributos	1
Reservado	10
Hora	2
Fecha	2
Entrada FAT de comienzo	2
Tamaño de archivo	4

* Área de datos. Se sitúa después del directorio raíz, es donde se almacenan los datos.

1.4. Arranque de MS-DOS.

- Se enciende el ordenador. La BIOS se instala de forma automática en un área de la memoria RAM denominada memoria sombra, ya que almacena una copia de las rutinas de la BIOS manteniéndose la copia original en la ROM.
- La CPU ejecuta el programa de autochequeo de hardware POST contenido en la BIOS. El POST carga en la memoria RAM el programa MBR del primer disco duro accesible y le cede el control. Al ejecutarse, el MBR lee de la tabla de particiones cuál es la partición activa. Una vez localizada lee el primer sector de dicha partición, lo carga en memoria y le cede el control.
- En este momento, en memoria está el programa correspondiente al sector de arranque de una partición formateada MS-DOS. Este programa es ligeramente diferente al del MBR. En su interior, tiene las instrucciones para localizar el archivo **IO.SYS**. Una vez localizado, lo carga en memoria y le cede el control, leyendo a su vez el archivo **MSDOS.SYS**.
- Gracias a estos ficheros se busca en el directorio raíz el archivo **CONFIG.SYS** de configuración del sistema y se carga. Este archivo guarda los datos correspondientes a la configuración de los periféricos, de la memoria RAM y de determinados parámetros del DOS. Su contenido puede ser modificado por el usuario para adaptar la configuración del sistema a sus necesidades; y si este no se encuentra el DOS asume unos valores por omisión para los parámetros.
- Después se carga el archivo **COMMAND.COM** o interprete de comandos. Es imprescindible que se encuentre en el directorio raíz para cargar en la memoria principal una copia de él.
- Por último, cada vez que se pone en marcha el sistema, y una vez finalizado el proceso anterior, el DOS ejecuta los comandos contenidos en un archivo denominado **AUTOEXEC.BAT**, lo que permitirá ejecutar de forma automática los procedimientos de iniciación del sistema sin necesidad de tener que teclear cada vez los mismos comandos. Además fija determinados parámetros para utilizar el DOS eficientemente. Este fichero puede ser modificado por el usuario y deberá hallarse en el directorio principal del disco de arranque. Si no se encuentra el sistema funcionará, aunque con limitaciones, pues en este caso el DOS tomará unos valores por defecto.

1.5. Configuración de MS-DOS.

1.5.1. Variables de entorno.

- El entorno es un área de memoria RAM en la que el sistema guarda información en forma de variables de tipo alfanumérico. Todos los programas pueden acceder a dichas variables y modificar sus valores, lo que permite la comunicación entre aplicaciones de usuario.
- **SET [variable=[cadena]]**. Comando que permite crear, modificar y eliminar las variables de entorno. Este comando se usa en AUTOEXEC.BAT o CONFIG.SYS para establecer variables de entorno cada vez que se inicie MS-DOS (**variable** especifica la variable que se desea crear o modificar; **cadena** especifica la cadena de caracteres que se desea asociar a la variable).
- Se manejan las siguientes variables de entorno:
  - Variables del sistema. MS-DOS las crea automáticamente y se encarga de mantenerlas y modificar sus valores según sus necesidades.
    - **CONFIG**. Permite utilizar configuraciones múltiples en el fichero CONFIG.SYS. Su valor corresponde al nombre de la opción elegida en el menú situado bajo la etiqueta [MENU] en CONFIG.SYS, y este nombre es el que se utiliza como primer parámetro del comando MENUITEM, que define las distintas opciones posibles.
    - **PATH [directorio]**. Obligatoria, contiene algún valor por defecto. Sirve para definir la ruta a tener en cuenta en la búsqueda de archivos ejecutables. El sistema busca primero el archivo en el directorio actual, y si no lo encuentra lo busca en los directorios especificados. Sólo busca archivos con extensión COM, EXE o BAT. Sin parámetros muestra el contenido de la variable. Ejemplo: PATH C:\; C:\DOS; C:\WINDOWS.
    - **APPEND [directorio]**. Sirve para definir los directorios donde el sistema busca automáticamente los archivos de datos si no los encuentra en el directorio actual. Es similar a PATH, pero APPEND es para archivos de datos. No es automática, es necesario crearla antes de asignarle un valor ejecutando previamente el comando APPEND /E. Ejemplo: APPEND C:\WINDOWS;C:\DOS.
    - **PROMPT**. Obligatoria, contiene algún valor por defecto. Permite cambiar el indicador del sistema. La opción más común es PG, que muestra la unidad en la que nos encontramos y toda la trayectoria de directorios seguido del símbolo >.
    - **COMSPEC**. Obligatoria, contiene algún valor por defecto. Le indica al sistema la ruta al archivo COMMAND.COM si no se encuentra en el directorio raíz. Esto ocurre cuando se borra la parte transitoria del intérprete de comandos para cargar algún programa de usuario. Ejemplo: COMSPEC=C:\ COMMAND.COM.
  - Variables del usuario. Son creadas y modificadas por el usuario mediante el comando SET.
    - **TEMP**. Indica el directorio donde se almacenarán los ficheros temporales creados durante la ejecución de programas. Ejemplo: SET TEMP= C:\DOS.
    - **DIRCMD**. Indica los parámetros del comando DIR. Ejemplo: SET DIRCMD= /P /O.
    - **MSDOSDATA**. Utilizado por los programas antivirus de WINDOWS para saber dónde están los archivos MSAV.INI y MWAV.INI.

1.5.2. Archivos de proceso por lotes.

- Un archivo de proceso por lotes es un archivo de texto con órdenes dirigidas al sistema operativo o con archivos ejecutables de aplicaciones, que se ejecutan secuencialmente. Llevan la extensión BAT y puede ser creados con cualquier editor de texto. Cada línea del archivo debe poseer una orden, y se puede detener la ejecución en cualquier momento pulsando Ctrl+Pausa.
- Los símbolos empleados exclusivamente en los archivos por lotes son:
  - **:etiqueta**. Nombre de una etiqueta. Deben ir precedidas de dos puntos (:) para diferenciarse de las órdenes. Admiten hasta ocho caracteres significativos.
  - **%número**. Parámetro del archivo por lotes, se trata de información adicional introducida detrás del nombre del archivo. Los parámetros deben estar separados entre sí por un espacio en blanco, y se numeran según el orden en que son introducidos. Se pueden gestionar hasta nueve parámetros y se referencian mediante el símbolo % seguido del número de parámetro.
  - **%variable%**. Recupera el valor de una variable de entorno.
  - **%%variable**. Variable de la orden FOR.
- Los comandos utilizados en estos archivos son:
  - **ECHO**. Controla la visualización de las órdenes y muestra mensajes:
    - **ECHO ON/OFF**. Activa/desactiva la visualización de todos los comandos que le siguen. Para eliminar la visualización de la propia orden ECHO o cualquier otra, debe ir precedida del símbolo @. Ejemplo: @ECHO OFF.
    - **ECHO mensaje**. Presenta en pantalla el mensaje, esté o no activado el echo.
  - **REM**. Permite introducir comentarios en el archivo por lotes. Las líneas precedidas por la palabra REM serán ignoradas.
  - **PAUSE**. Detiene temporalmente el desarrollo de un programa, visualizando un mensaje en pantalla a la espera de la pulsación de cualquier tecla. Si no se desea ver este mensaje, se puede redireccionar al dispositivo ficticio NUL (PAUSE >NUL).
  - **GOTO etiqueta**. Desvía sin condición el flujo del proceso hasta la etiqueta especificada.
  - **IF**. Desvía condicionalmente la ejecución de un archivo por lotes. Admite estas sintaxis:
    - **IF [NOT] EXIST archivo comando**. Si existe el archivo se ejecuta el comando. Con NOT, el comando se ejecuta si no existe el archivo.
    - **IF [NOT] cadena1==cadena2 comando**. Si ambas cadenas son iguales se ejecuta el comando. Una cadena se expresa entre comillas dobles. Por ejemplo, para comprobar si se ha introducido o no un parámetro se puede expresar con IF "%1" == "" ECHO Parámetro vacío. Con NOT, el comando se ejecuta si ambas cadenas son diferentes.
    - **IF [NOT] ERRORLEVEL número comando**. ERRORLEVEL es una variable que recoge el código de salida de cada orden externa que se ejecuta. Generalmente el código 0 indica ausencia de errores y otros códigos superiores hacen referencia a diferentes errores. Si el código de salida del último programa es igual o mayor al número, se ejecuta el comando. Con NOT, el comando se ejecuta si el código de salida es menor al número. Por tanto, para cumplirse exclusivamente si el código de salida es n podemos usar lo siguiente: IF ERRORLEVEL n IF NOT ERRORLEVEL (n+1) comando.

- **CHOICE [mensaje] [/C:opciones] [/N] [/S] [/T:opción,segundos]**. Permite elegir entre una serie de opciones, y dependiendo de la opción elegida devuelve un código de salida:
  - **mensaje**. Contiene el mensaje pidiendo introducir una de las opciones admitidas.
  - **/C:opciones**. Especifica las opciones posibles. Si el usuario pulsa la primera de las opciones, CHOICE devolverá un código de salida 1; si pulsa la segunda opción, CHOICE devuelve el código 2 y así sucesivamente. Si no se especifica este parámetro se asumen las opciones por defecto (SN).
  - **/N**. No muestra las opciones admitidas detrás del mensaje.
  - **/S**. Hace distinción entre mayúsculas y minúsculas. Si no se especifica este parámetro se toman como la misma opción.
  - **/T:opción,segundos**. Toma la opción indicada si no se pulsa ninguna otra tecla en los segundos especificados.

  Por ejemplo, con CHOICE `Introduzca opción /C:ABDES /N /T:S,15` el modificador /C indica las opciones admitidas. Si se pulsa la 'A' se generará un código de salida 1 y así sucesivamente hasta la 'S' que corresponde a un código 5. Gracias al modificador /N no muestra las teclas admitidas detrás del mensaje. El modificador /T toma como opción por defecto la 'S' si pasan 15 segundos sin pulsar ninguna tecla. El código de salida 0 se obtiene si el usuario responde con Ctrl+Pausa al mensaje de CHOICE.
- **FOR %%variable IN (conjunto) DO comando**. Esta orden repite el comando especificado para cada valor del conjunto. Conjunto es una lista de nombres de ficheros. En ella, se pueden establecer varios nombres separados por espacios y también se pueden utilizar comodines. Por ejemplo FOR `%%I IN (juan.txt maria.txt *.dat) DO TYPE %%I.`
- **SHIFT**. Desplaza el valor de los parámetros disminuyendo en uno su número de orden. Se mueve el valor de cada parámetro al parámetro anterior. El primer parámetro se pierde.
- **CALL archivo [parámetros]**. Llama a un archivo por lotes desde otro. Cuando la ejecución del archivo llamado finaliza, el archivo que lo llamó continúa su ejecución en la línea siguiente.

1.5.3. Configuración del arranque.

- Durante el arranque del sistema se leen el archivo de configuración CONFIG.SYS y el archivo por lotes AUTOEXEC.BAT, por este orden, que indican la configuración de cada ordenador.
- **AUTOEXEC.BAT** es un archivo por lotes que tiene las siguientes características:
  - Debe situarse en el directorio raíz de la unidad de arranque.
  - No es obligatoria su existencia. Si no existe MS-DOS ejecuta las órdenes TIME, DATE y VER y hace aparecer el PROMPT.
  - Permite definir una serie de variables de entorno (PATH, PROMPT, TEMP, DIRCMD) en cada arranque del ordenador. PATH y PROMPT se pueden definir con la orden SET o con unas órdenes diseñadas al efecto con el mismo nombre.
  - Contiene además órdenes para configurar el idioma del usuario y órdenes cuya misión es cargar programas residentes en memoria.

- **CONFIG.SYS** es un archivo de texto situado en el directorio raíz que contiene todas las órdenes de configuración del sistema. Dentro puede contener las siguientes órdenes:
  - **?** especifica que MS-DOS debe solicitar confirmación antes de su ejecución. Se inserta delante del signo =. Por ejemplo, BUFFERS?=30.
  - **BREAK=ON/OFF**. Especifica si MS-DOS debe verificar periódicamente la combinación de teclas CTRL+C.
  - **BUFFERS=número**. Son zonas de almacenamiento provisional empleadas para agilizar los procesos de lectura y escritura, el número debe estar entre 1 y 99. Un número de buffers alto hace más rápido el intercambio de información entre memoria y disco o pantalla.
  - **DEVICE=archivo**. Orden del sistema operativo que se utiliza para controlar los elementos hardware del ordenador. Algunos de estos ficheros son:
    - **ANSI.SYS**. Controlador del teclado, permite realizar configuraciones especiales como programar las teclas de función, etc.
    - **MOUSE.SYS**. Controlador del ratón.
    - **DISPLAY.SYS**. Controlador de la pantalla.
    - **DBLSPACE.SYS**. Hace que MS-DOS mueva DBLSPACE.BIN a la memoria superior.
    - **DRIVER.SYS**. Crea una unidad lógica para referirse a una unidad física.
    - **EGA.SYS**. Guarda y restaura la presentación cuando se usa el MS-DOS shell o Windows con un monitor EGA.
    - **HIMEM.SYS**. Es el controlador de memoria extendida. Debe preceder a todos los controladores que utilicen la memoria extendida.
    - **EMM386.EXE [NOEMS] [RAM]**. Es el controlador de memoria expandida para procesadores 386 y superiores, que se encarga de convertir memoria extendida en memoria EMS. También permite cargar controladores y programas residentes en el área de memoria superior para liberar memoria convencional. El parámetro NOEMS da acceso a la memoria superior, y RAM permite acceder tanto a memoria superior como memoria EMS. Debe estar precedido por la carga del controlador HIMEM.SYS.
    - **RAMDRIVE.SYS**. Simula una unidad de disco duro creando una unidad virtual en la memoria RAM.
    - **SETVER.EXE**. Carga la tabla de versión de MS-DOS en la memoria.
    - **SMARTDRV.EXE**. Programa que reserva un bloque de memoria expandida o extendida y lo utiliza como caché para lectura/escritura del disco.
  - **DOS=HIGH**. Permite que parte del núcleo de MS-DOS se cargue en la zona de memoria alta (HMA). Debe estar precedido por la carga del controlador HIMEM.SYS.
  - **DOS=UMB**. Permite que controladores y programas residentes puedan cargarse en los bloques de memoria superior (UMB) del área de memoria superior. Debe estar precedido por la carga del controlador HIMEM.SYS y el controlador de memoria expandida EMM386.EXE. Esta instrucción puede ser combinada con la anterior: DOS=HIGH,UMB.

- **LOADHIGH archivo**. Carga un programa en el área de memoria superior en procesadores 386 y superiores. Debe estar precedido por la carga de los controladores HIMEM.SYS y EMM386.EXE, y por la instrucción DOS=UMB.
- **DEVICEHIGH=archivo**. Carga un controlador de dispositivo en la memoria superior.
- **DRIVPARM**. Establece las características de una unidad de disco.
- **FILES=número**. Fija el número máximo de archivos que pueden estar abiertos simultáneamente, debe estar comprendido entre 8 y 255.
- **INSTALL**. Carga un programa residente en memoria.
- **LASTDRIVE=Z**. Establece el número de letras de unidad válidas.
- **NUMLOCK=ON/OFF**. Especifica si la configuración BLOCK NUM del teclado numérico está inicialmente activa o inactiva.
- **SHELL=intérprete**. Configura COMMAND.COM o especifica otro intérprete diferente.
- **STACKS**. Especifica opciones especiales de MS-DOS.
- **SWITCHES=[/K] [/W] [/N] [/F]**. Configura opciones especiales de MS-DOS:
  - **/K**. Hace que el teclado ampliado trabaje como uno normal.
  - **/W**. Permite cambiar la situación del fichero WINA20.386 para usuarios de Windows.
  - **/N**. Desactiva F5 y F8 que permiten controlar paso a paso la carga de CONFIG.SYS.
  - **/F**. Anula la pausa de dos segundos al comenzar la carga del sistema.

– La mayoría de los comandos de CONFIG.SYS pueden aparecer en cualquier orden. Sin embargo, el orden de los comandos DEVICE y DEVICEHIGH es importante puesto que algunos controladores de dispositivo activan dispositivos que otros controladores necesitan. El orden en que los controladores deberían aparecer en el archivo CONFIG.SYS es el siguiente:
  - HIMEM.SYS si el sistema tiene memoria extendida.
  - El administrador de memoria expandida.
  - EMM386.EXE si el procesador es un 386 con memoria extendida.
  - Cualquier otro controlador de dispositivo.
– Configuraciones múltiples. En versiones 6.0 o superiores es posible crear configuraciones múltiples a través de menús y submenús. El archivo CONFIG.SYS viene organizado en bloques con un encabezado. El bloque presenta el conjunto de órdenes que deben ejecutarse y el encabezado es un nombre entre corchetes. Los bloques terminan al comenzar uno nuevo o al finalizar el archivo. Hay que distinguir tres tipos de bloque:
  - **Bloques de menú**. Están encabezados por la palabra MENU entre corchetes. Las órdenes son del tipo MENUITEM que indican las distintas opciones del menú de configuración.

    ```
    [MENU]
    MENUITEM=COMPICOBOL, compilación COBOL
    MENUITEM=NORMAL, trabajo habitual
    ```

  - **Bloques de órdenes**. Encabezados por el MENUITEM que aparece en el bloque de menú.

    ```
    [COMPICOBOL]
    BUFFERS=50
    …
    ```

[NORMAL]

BUFFERS=25

…

- **Bloques comunes**. Cuando varios bloques presentan órdenes comunes, para evitar repetirlas se utilizan estos bloques con el encabezado [COMMON].

– Configuraciones de teclado, pantalla, idioma. Las páginas de códigos son diferentes tablas con los juegos de caracteres que usa el ordenador y que no son soportados por el código ASCII ampliado. Llevan un primer código que identifica a cada país, un número de página cuyos caracteres soportan los necesitados por cada país y un segundo código, también identificativo de cada país que se usa como parámetro en la orden KEYB. Las órdenes de configuración se reparten entre CONFIG.SYS y AUTOEXEC.BAT, y son las siguientes:

- **COUNTRY=número [, archivo COUNTRY.SYS]**. Permite fijar el formato de fecha y hora correspondiente al país elegido, siendo número el código numérico del país y fichero la ruta de acceso al fichero. Ejemplo: COUNTRY=034,850,C:\DOS\COUNTRY.SYS.
- **MODE**. Configura los dispositivos de MS-DOS y establece las páginas de códigos. Se ejecuta desde la línea de comandos o desde AUTOEXEC.BAT con varios formatos:
  - MODE dispositivo CODEPAGE PREPARE=(página (archivo CPI))
  - MODE dispositivo CODEPAGE SELECT=(página)
  - MODE dispositivo CODEPAGE [/STATUS]
  - MODE dispositivo CODEPAGE REFRESH

  siendo dispositivo en general CON, página corresponde a las páginas de códigos de los países y archivo CPI si existe alguno con información sobre páginas de códigos. Ejemplo: MODE CON CODEPAGE PREPARE=((850) C:\DOS\EGA.CPI).

País	Código	Páginas	Código
Alemania	049	850 437	GR
España	034	850 437	SP
Sudamérica	003	850 437	LA
EEUU	001	437 850	US
Francia	033	850 437	FR
Inglaterra	061	437 850	
Japón	081	932 437	JA

- **DISPLAY**. Controlador de CONFIG.SYS que, mediante DEVICE o DEVICEHIGH, proporciona soporte de códigos para la pantalla y la tarjeta gráfica. El formato es DEVICE=ruta\DISPLAY.SYS CON=([tipo] [,página] [,número_paginas]). Ejemplo: DEVICEHIGH /L:1,15872=C:\DOS\DISPLAY.SYS CON=(EGA,850,1).
- **KEYB**. Sirve para definir el teclado de cada país. Se ejecuta desde la línea de comandos o desde AUTOEXEC.BAT. El formato es KEYB código [,página] [,ruta\KEYBOARD.SYS]. Ejemplo: KEYB SP,850,C:\DOS\KEYBOARD.SYS.
- **NLSFUNC**. Su misión consiste en cargar información ampliada para que se pueda ejecutar la orden siguiente a NLSFUNC. Su formato es NLSFUNC ruta\fichero.
- **CHCP**. Cambia en una sola orden la página de códigos activa por la de otro país. Se ejecuta desde la línea de comandos o desde AUTOEXEC.BAT. El formato es CHCP página.

- Órdenes de configuración de memoria. La memoria convencional es la que utilizan todos los programas, lo cual implica que se debe tratar de liberar al máximo. Para ello hay que utilizar siempre que sea posible las órdenes DEVICEHIGH y LH (LOADHIGH).
  - **MEM**. Muestra la cantidad de memoria libre y de memoria utilizada.
  - **MEMMAKER.EXE**. Es una utilidad que se emplea después de modificar alguna línea de los archivos AUTOEXEC.BAT y/o CONFIG.SYS. Permite una optimización de la memoria realizando lo siguiente:
    - Comprueba el archivo CONFIG.SYS y las órdenes de gestión de memoria.
    - Añade en el CONFIG.SYS las órdenes DEVICE para HIMEM.SYS y EMM386.SYS.
    - Intenta cambiar la carga de programas residentes de AUTOEXEC.BAT mediante LH.
- Discos RAM. Son unidades lógicas de almacenamiento creadas en RAM. Por tanto, son volátiles y su acceso es rápido, pero están limitadas por la memoria disponible. Su creación se realiza mediante el controlador RAMDRIVE.SYS con la orden DEVICE=ruta\RAMDRIVE.SYS [tamaño] [/E] [/X], en memoria expandida (/E) o memoria extendida (/X).
- Otros comandos de interés.
  - **HELP**. Programa de ayuda que proporciona información de todos los comandos y utilidades de MS-DOS de forma interactiva.
  - **DOSKEY**. Programa residente en memoria que permite ir almacenando las últimas órdenes introducidas por teclado. Una vez instalado, se pueden recuperar las órdenes anteriores con las teclas de cursor arriba y abajo.
  - **SCANDISK [unidad:]**. Examina y repara opcionalmente posibles deficiencias de la superficie del disco. Las zonas dañadas se reparan automáticamente transfiriendo los datos a sectores en buen estado y marca la zona dañada para impedir su utilización.
  - **MSD**. Programa que facilita información técnica sobre el ordenador.

1.6. Explotación y administración de MS-DOS.

1.6.1. Comandos y dispositivos.

- El PROMPT es el indicador de mandatos del DOS. Define la unidad de disco activa y el directorio donde el DOS por omisión buscará los archivos, e indica que está preparado para recibir instrucciones. Normalmente la unidad por defecto es C: aunque puede cambiarse tecleando la nueva letra de identificación de la unidad seguida por dos puntos.
- El intérprete de comandos COMMAND.COM traduce las órdenes introducidas a código binario y realiza los pasos necesarios para realizar su ejecución. También se encarga de la ejecución de los archivos ejecutables con extensión COM, EXE o BAT por este orden:
  - Los archivos COM son más compactos y son cargados más rápidamente que sus equivalentes EXE, ya que no contienen información para la asignación de direcciones de memoria y siempre deben comenzar en la misma dirección. MS-DOS no sabe si un archivo con extensión COM es un programa ejecutable válido, simplemente lo carga en memoria y le transfiere el control. Aún cuando la longitud de un programa COM no puede exceder de los 64 KB y todo el código ejecutable está dentro del mismo segmento, las versiones actuales del MS-DOS reservan toda la memoria disponible. Si un programa COM debe

ejecutar otro proceso, es necesario que él mismo libere la memoria no usada para que pueda ser empleada por otra aplicación.

  - Los programas EXE son ilimitados en tamaño, el límite lo marca la memoria disponible del equipo, y construido a partir de varios módulos independientes. Además, los programas EXE pueden colocar el código, datos y pila en distintos segmentos de la memoria. La posibilidad de colocar las diversas partes de un programa en fragmentos diferentes de memoria, y de establecer segmentos de memoria con código que pudiera ser compartido por varias tareas, es apropiada para ambientes multitarea.

- MS-DOS tiene dos tipos de comandos:
  - **Internos**. Están incorporados en el código de COMMAND.COM y por tanto son residentes en memoria. Se agrupan según su uso atendiendo a la siguiente clasificación:
    - Archivos de proceso por lotes. CALL, PAUSE, ECHO, FOR, GOTO, CHOICE.
    - Manejo de directorios. CD, MD, RD.
    - Manejo de archivos. COPY, DEL, DIR, REN, TYPE, UNDELETE.
    - Otros. BREAK, VOL, PROMPT, CLS, DATE, TIME, VER.
  - **Externos**. El sistema tiene que leerlos del disco para cargarlos en memoria en cada ejecución. Cada orden se almacena en un archivo independiente con extensión COM o EXE. Existen diversos tipos de órdenes externas:
    - Manejo de discos. DISKCOMP, DISKCOPY, FORMAT, UNFORMAT, SYS, LABEL, CHKDSK, SCANDISK.
    - Copias de seguridad. MSBACKUP, RESTORE.
    - Configuración. APPEND, DOSKEY, KEYB.
    - Archivos. ATTRIB, MIRROR, COMP, FC, MOVE, XCOPY.
    - Especiales. ASSIGN, MORE, TREE.
    - Utilidades. DEBUG, HELP, LINK, MSAV, MSD, MEM.
- Dispositivos. Por omisión MS-DOS trabaja directamente con cuatro dispositivos y sus rutinas de gestión se encuentran en IO.SYS y MSDOS.SYS. Cada uno de estos dispositivos lleva asociado un nombre invariable y único:
  - **CON**. Identifica al teclado en las operaciones de entrada y al monitor en las operaciones de salida, puesto que ambos son dispositivos unidireccionales.
  - **LPT1 o PRN, LPT2 y LPT3**. Corresponden a puertos bidireccionales paralelo, se asocian a la conexión con impresoras.
  - **NUL**. Dispositivo ficticio que se crea para simular el envío o recepción de información.
  - **COM1 o AUX, COM2, COM3 y COM4**. Identifican puertos bidireccionales serie, se asocian a la conexión con el resto de periféricos.
- Redireccionamiento. MS-DOS permite cambiar la salida de algunos comandos hacia otro dispositivo o hacia un archivo mediante el símbolo >, que indica al sistema a dónde debe enviar el resultado de la orden. Con >> la nueva salida se escribe a continuación de la existente. El símbolo < indica que los datos deben tomarse desde el archivo o el dispositivo que se indique, en lugar de tomarlos del teclado.

- Filtros. Son órdenes del sistema operativo que leen los datos de un dispositivo de entrada, los modifican y los envían a un dispositivo de salida:
  - **MORE**. Divide la información que le llega en bloques de 24 líneas.
  - **SORT [/R] [/+N]**. Ordena alfabéticamente la información que le llega (**/R** ordena inversamente; **/+N** ordena por el carácter de la columna N).
  - **FIND cadena archivo [/C] [/V]**. Permite localizar en un archivo las líneas que contienen una cadena de caracteres expresada entre comillas (**/C** cuenta las veces que aparece la cadena buscada; **/V** muestra las líneas en las que no aparece la cadena).
- Tuberías. Son conexiones de órdenes que encadenan la salida de un comando con la entrada de otro. Se representan por el símbolo |.

1.6.2. Directorios y archivos.

- Los nombres de los archivos están formados por el **nombre** y la **extensión** separados por un punto. El nombre puede tener de uno a ocho caracteres sin espacios en blanco ni caracteres especiales, no se distingue entre mayúsculas y minúsculas. La extensión puede tener de cero a tres caracteres y sirve para indicar el tipo de archivo.
- Los archivos se organizan mediante una estructura jerárquica en forma de árbol invertido que parte del directorio raíz (\) que se crea al formatear el disco. Un **directorio** es un índice en el que se guarda el nombre de los archivos que se almacenan en él, el día y la hora de creación, su tamaño y el lugar donde se encuentra almacenado en el disco. Los directorios pueden contener a su vez otros directorios, y su nombre puede tener de uno a ocho caracteres. El directorio actual del sistema se indica con un punto y el directorio padre con dos puntos seguidos.
- Los archivos se almacenan en los directorios. Para acceder a ellos es necesario situarse en el directorio en el que se encuentran o bien indicar la ruta que hay que seguir a través del árbol de directorios para llegar a ellos. La especificación puede hacerse mediante:
  - Rutas absolutas. Parten siempre desde el directorio raíz y desde él se indica el camino a seguir hasta el archivo, ignorando el directorio actual en el que se encuentre el sistema.
  - Rutas relativas. Parten del directorio en el que se encuentre el sistema.
- Para referenciar un archivos hay que indicar su nombre y su extensión. Para referenciar a varios archivos a la vez se utilizan los **caracteres comodín** tanto en el nombre como en la extensión:
  - Asterisco (*). Cada uno sustituye a un grupo de caracteres.
  - Interrogación (?). Cada una sustituye a un único carácter.

1.6.3. Órdenes más comunes.

- Las órdenes básicas del sistema son las siguientes:
  - **CLS**. Borra la pantalla.
  - **VER**. Muestra la versión de MS-DOS instalada.
  - **DATE**. Muestra la fecha del sistema y permite modificarla.
  - **TIME**. Muestra la hora del sistema y permite modificarla.
  - **LABEL [unidad:] [etiqueta]**. Asigna una etiqueta al disco o cambia la existente.
  - **VOL [unidad:]**. Muestra el nombre interno de la unidad especificada.
- Las órdenes relacionadas con directorios y archivos son las siguientes:

- **TYPE [unidad:] archivo**. Muestra el contenido de un archivo de texto. No está permitido utilizar los comodines.
- **PRINT archivo [/T]**. Envía a la impresora una archivo o conjunto de archivos de texto (/**T** anula el proceso de impresión).
- **DEL [unidad:] archivo [/P]**. Borra archivos del disco excepto los ocultos o los de sólo lectura. Están permitidos los comodines (/**P** hace que se pida confirmación antes de borrar).
- **UNDELETE**. Permite recuperar algunos archivos borrados.
- **REN nom_antiguo nom_nuevo**. Cambia de nombre a los ficheros, admite comodines.
- **COPY [unidad:] archivo [unidad:] [archivo] [/V]**. Copia archivos de una unidad a otra o en la misma unidad con nombres diferentes (/**V** verifica si se ha realizado correctamente).
- **MOVE unidad_origen: archivo unidad_destino:** Mueve archivos de una unidad a otra y archivos de un directorio a otro y renombra archivos y directorios. Admite comodines.
- **FC archivo1 archivo2**. Compara dos archivos o dos grupos de archivos y visualiza las diferencias entre ellos, admite comodines.
- **TREE [unidad:] [/F]**. Visualiza la estructura de directorios de una unidad de disco (/**F** también visualiza los nombres de los archivos de cada directorio).
- **DIR [unidad:\ruta\archivo] [/P /W /S /L /O /A]**. Muestra los archivos y directorios que se encuentran en el directorio indicado (/**P** muestra pantalla a pantalla; /**W** muestra en columnas; /**S** muestra los archivos de todos los subdirectorios; /**L** muestra los nombre en minúscula; /**O** los ordena según un determinado criterio; /**A** muestra sólo los que tiene el atributo especificado).
- **MD [\ruta]\directorio**. Crea un directorio al final de la ruta especificada.
- **CD [\ruta]\directorio**. Cambia el directorio actual por el de la ruta especificada.
- **RD [\ruta]\directorio**. Borra el directorio al final de la ruta especificada si está vacío.
- **DELTREE [\ruta]\directorio [/Y]**. Borra el directorio indicado con todos sus archivos y subdirectorios, incluidos ocultos y de sólo lectura (/**Y** anula la confirmación de borrado).

– Las órdenes relacionadas con discos son las siguientes:

- **FORMAT [unidad:] [/S /B /Q /U /F:tamaño /V:etiqueta]**. Crea un sistema de archivos en la unidad indicada (/**S** prepara un disco de arranque, es decir, formatea y copia COMMAND.COM, IO.SYS y MSDOS.SYS; /**B** deja espacio en el disco para poder copiar el sistema con SYS; /**Q** formateo sin comprobación de sectores defectuosos; /**U** formateo incondicional sin posibilidad de reconstrucción del disco; /**F:tamaño** especifica el tamaño del disco al que se dará formato; /**V:etiqueta** formatea y asigna una etiqueta al disco).
- **UNFORMAT unidad:** Recupera los datos de un disco previamente formateado.
- **SYS [unidad:]**. Transfiere a la unidad especificada los ficheros del sistema COMMAND.COM, IO.SYS y MSDOS.SYS.
- **CHKDSK [unidad:]**. Emite un informe y repara el disco.
- **DISKCOPY [unidad_origen:] [unidad_destino:]**. Copia el contenido de un disco a otro.
- **XCOPY archivo [unidad_destino:] [/S /E /V]**. Copia archivos y directorios con los subdirectorios cargando en memoria los archivos a copiar y transfiriéndolos al destino. No

puede copiar archivos de sólo lectura o archivos ocultos. Se diferencia de COPY en que ésta copia de archivo en archivo (**/S** copia también los archivos incluidos en los subdirectorios; **/E** copia los directorios vacíos; **/V** comprueba que la copia se ha hecho correctamente).

- **DISKCOMP unidad1: unidad2:** Compara el contenido de dos discos sector a sector.

– Las órdenes relacionadas con la seguridad de la información son las siguientes:

- **ATTRIB [archivo][+R –R +H –H +S –S]**. Visualiza y modifica los atributos de un archivo, sin parámetros muestra los atributos de los archivos del directorio actual (**+R** hace al archivo de sólo lectura; **–R** quita el atributo de sólo lectura; **+H** hace al archivo oculto; **–H** quita el atributo de oculto; **+S** hace al archivo de sistema; **–S** quita el atributo de sistema).
- **MSBACKUP [archivo_especificaciones]**. Genera una copia de seguridad de todos o parte de los archivos del disco duro o de una unidad de red. Permite configurar y realizar copias de seguridad, así como comparar los archivos copiados con los originales.
- **RESTORE disco1: disco2: [arhivos] [/D /N /P]**. Restablece las copias de seguridad, es complementario de MSBACKUP (**/D** muestra una lista de los archivos de la copia de seguridad que coinciden con los nombres del disco destino; **/N** restablece los archivos que no existen en el disco destino; **/P** pide confirmación antes de restablecer los archivos).
- **MSAV [unidad:] [/S /C /R]**. Utilidad del sistema que permite detectar virus (**/S** examina la unidad sin eliminar los virus; **/C** examina la unidad y elimina los virus; **/R** crea el archivo MSAV.RPT con un informe de los virus detectados).

2. Windows XP.

2.1. Instalación.

2.1.1. Requisitos previos.

– Antes de instalar Windows XP, es conveniente asegurarnos de que los componentes de hardware cumplen los requisitos mínimos y que todo nuestro software y hardware es compatible con XP. Podemos consultar la Lista de Compatibilidad de Hardware (HCL) en el siguiente sitio Web de Microsoft: http://www.microsoft.com/hcl/

– Los requisitos de Hardware son los siguientes:

- *CPU*. Hasta dos Pentium II 233 MHz. Recomendado Pentium II 300 MHz o equivalente.
- *RAM*. 64 MB RAM es el mínimo y 4 GB RAM es el máximo. Se recomiendan 128 MB.
- *Disco duro*. Partición con un tamaño mínimo de 2GB, disponiendo al menos de 1,5 GB de espacio libre en el disco duro.
- *Monitor*. Resolución VGA o superior.
- *Accesorios*. Teclado y ratón Microsoft o compatible.
- *Dispositivos*. Unidad de CD-ROM o DVD.

2.1.2. Opciones de instalación.

– **Instalación nueva**. Sobre equipos nuevos o reemplazando el sistema operativo antiguo.

– **Actualización**. Sobre Windows 98 se realiza una doble instalación, sobre Windows 2000/NT4 se realiza una migración de componentes. Para actualizar desde la red, basta con copiar el directorio i386 del CD-ROM a una carpeta compartida e iniciar la actualización con

WINNT.EXE (16 bits) o WINNT32.EXE (32 bits). Con la opción /makelocalsource se hace una copia en local de los ficheros de instalación, para que no sea necesario el CD-ROM si se necesitan añadir componentes.

- **Instalación local**:
  - *Completa*. Con CD-ROM, desde el sistema operativo antiguo o el arranque.
  - *Clonación*. Utilizando la herramienta SYSPREP, interactivamente o mediante un fichero de respuestas creado con SETUPMGR.EXE.
- **Instalación remota**:
  - *Completa*. Mediante Remote Installation Services (RIS), de forma interactiva o con fichero de respuestas previamente creado.
  - *Clonación*. Utilizando la herramienta RIPREP, de forma interactiva o con fichero de respuestas previamente creado.

2.1.3. Proceso de instalación.

- **Selección de particiones**:
  - Una partición primaria es una unidad lógica y una partición extendida es aquella que puede alojar varias unidades lógicas. No es necesario que haya una partición primaria para crear una partición extendida. Puede haber hasta cuatro particiones primarias, o tres particiones primarias y una extendida en un disco básico. Sólo puede marcarse como activa una única partición primaria por disco. El sistema arrancará desde la partición primaria activa del primer disco físico. Es conveniente reservar todo el espacio existente en el disco ya que cuando se alcanza el límite de cuatro particiones, el espacio no asignado se pierde definitivamente. Para ello conviene crear una partición extendida.
  - Existen dos tipos de particiones:
    - **Partición del sistema**. El cargador NTLDR y el fichero de configuración BOOT.INI deben instalarse en esta partición, que debe ser la partición primaria activa del disco.
    - **Partición de inicio**. Contiene el núcleo NTOSKRNL.EXE y el resto de ficheros del sistema operativo. Puede estar en una partición extendida, diferente de la del sistema.
- **Selección de sistema de archivos**:
  - *FAT16 (File Allocation Table).* Basado en asignación no contigua de bloques por tabla de localización. Permite direccionar como máximo 2^{16} bloques de 32 KB (2 GB). El sector de arranque ocupa un sector (512 Bytes). El directorio raíz tiene un tamaño limitado y se encuentra en una posición fija del disco. Consume pocos recursos del sistema y es el mejor para discos y/o particiones de menos de 200MB. No pueden aplicarse permisos sobre archivos y directorios. Soportado por MS-DOS, Windows 3.x y Windows 95/98/ME/NT.
  - *FAT32*. Es una mejora de FAT16. Amplía el espacio de direccionamiento a 32 bits, aunque sólo se usan 28 y las 4 restantes están reservadas para el sistema. En la práctica permite crear particiones de unos 124 GB. El sector de arranque ocupa 32 sectores y el directorio raíz es un archivo más, permitiendo su crecimiento y evitando la limitación de archivos. Soportado por Windows 95 OSR2 y Windows 98/ME/2000/XP/Server.

    - *NTFS (New Techology File System)*. Utiliza direccionamiento de 64 bits y presenta características de seguridad (listas de control de acceso y cifrado de ficheros) y administración de cuotas de disco y compresión individual. No hay límite en el número de directorios y alcanza 16 EB como máximo. Soportado por Windows NT/2000/XP/Server.
- **Nombre de equipo y contraseña de administrador**. Es muy peligroso utilizar un nombre de equipo que coincida con el nombre de algún usuario. Por motivos de seguridad siempre se debe asignar una contraseña a la cuenta de administrador. Hay que asegurarse de recordar y proteger esta contraseña. Por regla general, nunca se debe dejar esa contraseña en blanco.
- **Grupo de trabajo o dominio**. Un determinado equipo se puede integrar en un:
    - *Grupo de trabajo*. Cada ordenador se gestiona de manera individual y cada usuario es administrador de su equipo. Todos pueden ser servidor y estación de trabajo a la vez. Windows XP no soporta más de diez conexiones entrantes como servidor de recursos compartidos, por eso es adecuada en una red de hasta diez equipos. Se utiliza la resolución de nombres NetBIOS para la comunicación entre ellos. Es recomendable que todo el grupo utilice un mismo nombre de grupo. Aunque vayamos a conectarnos a un dominio, es recomendable unirse a un grupo de trabajo durante la instalación y después, una vez finalizada la instalación de Windows XP, configurar la unión al dominio.
    - *Dominio*. El equipo necesita una cuenta de usuario de Active Directory, permite centralizar la administración de la seguridad. Cada dominio tiene un nombre único, se organizan en niveles y se administran como unidades con reglas y procedimientos comunes. Los usuarios tienen opciones limitadas sobre el equipo. Para trabajar en un dominio, es imprescindible que exista en algún punto de la red, un controlador principal de dominio. Este controlador debe estar montado con una versión servidor de Windows.

2.1.4. Pasos de arranque. NTLDR y BOOT.INI. Arranque dual.

- Los archivos que deben estar en el directorio raíz de la partición del sistema son los siguientes:
    - *NTLDR*. Programa cargador del sistema.
    - *BOOT.INI*. Archivo de configuración del arranque.
    - *BOOTSECT.DOS*. Copia del sector de arranque de MS-DOS.
    - *NTDETECT.COM*. Programa detector de hardware.
    - *NTBOOTDD.SYS*. Necesario solamente para los sistemas que arrancan desde un SCSI, en donde el BIOS en el adaptador SCSI se encuentra deshabilitado.
- Los pasos de arranque de Windows XP son los siguientes:
    - Verificación del hardware por parte del BIOS y ejecución del Master Boot Record (MBR).
    - Lectura de la tabla de particiones del MBR y búsqueda de la partición primaria activa.
    - Ejecución del cargador NTLDR, que se encuentra en el sector de inicio de dicha partición, y que hace saltar del modo real al protegido con memoria lineal de 32 bits.
    - El cargador NTLDR lee el archivo BOOT.INI, que contiene todos los sistemas operativos instalados disponibles, y muestra la selección del sistema operativo. Aunque el número de sistemas operativos que tengamos instalados en nuestra máquina no está limitado, el

cargador de Windows únicamente nos mostrará en la pantalla inicial de arranque del sistema las 10 primeras líneas especificadas en la sección [operating systems] del BOOT.INI.

  - Si se elige Windows XP, NTLDR ejecuta NTDETECT.COM para la detección del hardware y carga el núcleo del sistema operativo NTOSKRNL.EXE en memoria. Si se elige otro sistema operativo, NTLDR carga y ejecuta el BOOTSECT.DOS y le pasa el control.

- El archivo BOOT.INI tiene una estructura parecida a esta:

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="WinXP Pro" /fastdetect
C:\bootsect.dos="MS-DOS"
```

- Si el sistema operativo es de núcleo NT, el archivo BOOT.INI almacena la información referente al disco y a la partición en la que esta instalado. La sintaxis ARC se divide en cinco partes:
  - `multi(n)/scsi(n)`. Multi significa que el sistema usará la BIOS para acceder al disco duro mediante un controlador IDE. El valor que sigue a multi es siempre 0, porque sólo se puede arrancar desde el primer controlador IDE. Si tenemos un disco duro SCSI en lugar de IDE, ponemos `scsi` seguido del numero del adaptador SCSI del que queremos arrancar.
  - `disk(n)`. Si en la parte anterior hemos puesto `multi`, aquí siempre va un 0. Si hemos puesto `scsi` aquí ponemos el ID del dispositivo SCSI.
  - `rdisk(n)`. El número representa el número del disco duro dentro del controlador IDE. Va de 0 a 3, representando los cuatro discos duros que podemos tener en un controlador IDE.
  - `partition(n)`. El número indica en que partición esta instalado el sistema operativo. El número de partición comienza por 1, no por 0 como en las otras opciones.
  - `directorio="texto"`. Indicamos en que directorio se instaló Windows XP y ponemos un texto cualquiera que aparecerá en el menú al reiniciar el sistema.
- El número que aparece en `timeout` indica el tiempo que el menú se mostrará en pantalla. Si queremos que el menú permanezca en pantalla hasta que se seleccione una opción, sin importar el tiempo que transcurra, debemos escribir el valor -1 para la opción `timeout`. Algunos de los parámetros que se pueden añadir a la carga del sistema son los siguientes:
  - `/fastdetect`. No realiza la búsqueda del ratón en los puertos serie.
  - `/noguiboot`. No muestra la pantalla grafica de Windows durante el inicio del sistema.
  - `/sos`. Muestra los nombres de los drivers que va cargando, aparte de otras informaciones sobre el sistema.
- NTLDR lee las tablas de particiones de los discos del sistema y numera cada partición así:
  - Busca todas las particiones que no tengan como ID 00 (no usada) o 05 (extendida).
  - A cada partición encontrada le asigna un numero secuencial, comenzando por 1.
  - Busca la tabla de particiones de nuevo, y lee las particiones con ID 05 (extendidas).
  - Asigna números correlativos a las unidades lógicas de la primera partición extendida que encuentre, y continúa de la misma manera con el resto de particiones extendidas.

    - Esta búsqueda de particiones no sólo carga particiones Windows, sino que también funcionará con particiones de otros sistemas operativos como Linux.
- Si el sistema operativo es MS-DOS o Windows 9x, el archivo que se cargará es el sector de arranque BOOTSECT.DOS que esta en el directorio raíz de la partición activa del disco de arranque, que en estos sistemas siempre se nombra como C:
- Un sector de arranque de un sistema operativo no era mas que un pequeño programa de 512 bytes que se graba en el primer sector del disco duro o disquete desde donde queremos cargar el sistema operativo. Cuando se instala un sistema operativo de la familia NT en un disco duro donde ya exista MS-DOS o Windows 95/98, el proceso de instalación lee el sector de arranque de esos sistemas y los graba automáticamente en C:\ con el nombre BOOTSECT.DOS.
- Es posible conseguir que NTLDR cargue cualquier sistema operativo, incluido Linux. Todo lo que tenemos que hacer es obtener un fichero con el contenido del sector de arranque del sistema operativo que queramos arrancar. En Linux habría que utilizar la instrucción `dd`:

  ```
  dd if=/dev/hda1 of=/mnt/floppy/bootsect.lin bs=512 count=1
  ```

  donde *if=/dev/hda1* indica que se van a leer los datos de la partición de instalación de Linux, *of=/mnt/floppy/bootsect.lin* indica que se van a copiar a la disquetera con el nombre *bootsect.lin*, *bs=512* indica el tamaño en bytes de los bloques que se van a copiar y *count=1* el número de bloques que se van a copiar. Si tenemos Linux instalado en nuestro sistema y grabamos su sector de arranque en un fichero C:\BOOTSECT.LIN, con la siguiente línea:

  ```
  C:\bootsect.lin="Linux"
  ```

  conseguiríamos ejecutar el sector de arranque de Linux, donde podríamos tener un programa que se encargara de cargar el resto del sistema operativo, como LILO o GRUB.

2.1.5. Orden de instalación de los sistemas operativos.

- Si se instalan varios sistemas operativos en una máquina, hay que tener en cuenta lo siguiente:
    - MS-DOS y Windows 95/98/ME necesitan que la partición activa del disco de arranque, sea FAT o FAT 32. Al instalar Windows 95/98, este sobrescribe el sector de arranque de la partición, dejando un sector de arranque que únicamente puede arrancar el archivo IO.SYS.
    - En cambio, Windows ME respeta el sector de arranque de la partición.
    - Windows NT no puede arrancar de una partición FAT 32, porque no las maneja.
    - Windows XP puede arrancar todos los sistemas operativos previos.
    - El cargador de Windows NT no es capaz de arrancar Windows 2000 ni XP.
    - El cargador de Windows 2000 no es capaz de arrancar un sistema Windows XP/2003.
    - El cargador de Windows XP no puede arrancar un sistema Windows 2003.
- En conclusión, por regla general podemos decir que los sistemas operativos se instalan por orden de antigüedad, empezando por los más antiguos y terminando por los más modernos.

2.1.6. Recuperación de errores.

- **Instalación de Windows XP en un disco duro con una partición Windows 98**:
    - Al instalar Windows XP, va a sobrescribir el MBR del primer disco duro del sistema y va a escribir su propio sector de arranque en el sector de arranque de la partición activa de ese disco duro, borrando los que hubiese anteriormente (MBR y boot sector de Windows 98).

  - Windows 98 no es capaz de ejecutarse si no se carga el sector de arranque que llama al fichero IO.SYS. Windows XP detecta que se está instalando en un disco duro donde ya está instalado Windows 98, así que copia el sector de arranque de Windows 98 con el nombre de BOOTSECT.DOS en C:\ antes de instalar su propio sector de arranque y añade una línea en el BOOT.INI que permite cargar Windows 98.
  - Si en el menú de arranque se elige Windows 98, se cargará desde C:\ el archivo BOOTSECT.DOS y se le cederá el control, iniciándose Windows 98 sin ningún problema.
  - En este caso da lo mismo que hablemos de Windows 98, Windows 98 SE, Windows 95 o MS-DOS, ya que todos estos sistemas operativos operan del mismo modo. Asimismo, da igual hablar de Windows 2000, Windows XP o Windows 2003, dado que ambos respetan a los sistemas operativos anteriores de la misma manera.
  - Para volver a la situación anterior, habría que restaurar el MBR de Windows 98 con la orden FDISK /MBR y el sector de arranque de la partición activa con la orden SYS C: desde un disco de inicio de Windows 98.
- **Instalación de Windows XP en un disco duro con una partición Windows 2000**:
  - Este caso es muy semejante al anterior. Los arranques de Windows XP y de Windows 2000 son idénticos, con la salvedad de que el arranque de Windows 2000 no conoce ni respeta a Windows XP, debido a que tiene una versión distinta del fichero NTLDR.
  - Se diferencia del caso anterior en que no es necesario grabar el fichero BOOTSECT.DOS, ya que el arranque de Windows XP es compatible con el arranque de Windows 2000.
- **Instalación de Windows XP en un disco duro con una partición Windows 2003**:
  - Al instalar Windows XP, va a sobrescribir el MBR del primer disco duro del sistema y va a escribir su propio sector de arranque en el sector de arranque de la partición activa de ese disco duro, borrando los que hubiese anteriormente (MBR y boot sector de Windows 2003).
  - Puesto que arranque de Windows XP no reconoce a Windows 2003, será necesario usar la consola de recuperación de Windows 2003 y volver a instalar el MBR, el sector de arranque y el NTLDR de Windows 2003. Para ello se utilizarán los siguientes comandos:
    - **FIXMBR**. Instala el programa de MBR de Windows 2003 en el MBR del disco duro.
    - **FIXBOOT**. Instala el sector de arranque de Windows 2003, parecido al SYS de Windows 98. Para usar esta orden, debemos indicar la unidad a arreglar (FIXBOOT C:)

2.2. Configuración.

2.2.1. Añadir y eliminar componentes.

- En anteriores versiones de Windows, se podía elegir en el momento de la instalación que componentes deseábamos instalar. Esto ha cambiado en Windows XP que siempre se instala con una selección determinada de componentes.
- En Agregar o quitar componentes de Windows no aparecen todos los componentes de Windows, sino solo los más comunes. Si queremos ver todos los componentes, tendremos que realizar la siguiente operación:

- Desde el Windows Explorer ir a la carpeta **Inf** que cuelga del SystemRoot (donde instalamos Windows XP, normalmente X:\WINDOWS) y seleccionar el fichero **Sysoc.Inf** (se recomienda hacer una copia de seguridad de dicho fichero). Editar dicho fichero.
- Por cada componente de Windows, existe una línea en este fichero. Algunas de estas líneas contienen la palabra hide (oculto), lo que impide que dichos componentes se vean en agregar o quitar.
- Eliminar únicamente la palabra hide de las líneas, de modo que

  com=comsetup.dll,OcEntry,comnt5.inf,hide,7

  se convierta en

  com=comsetup.dll,OcEntry,comnt5.inf,,7

  Mucho cuidado con eliminar las comas, puesto que se trata de parámetros posicionales.
- Ahora ya aparecerán todos estos componentes cuando vayamos a Agregar o Quitar componentes de Windows, y podremos elegir instalar cualquiera de ellos.

2.2.2. Restauración del sistema.

- Cada punto de restauración de sistema que creemos, consume un espacio en disco. Cada cierto tiempo, Windows crea automáticamente sus propios puntos de restauración, y también son creados automáticamente cuando instalamos nuevo software o drivers siempre que estos sean considerados importantes por el sistema.
- El total del espacio en disco que pueden ocupar entre todos los puntos restauración, así como el funcionamiento general del programa de restauración, pueden ser ajustados desde la configuración de **Inicio → Ayuda y soporte técnico → Restaurar Sistema**.
- Cuando se crea un punto de restauración, y no existe espacio suficiente, Windows elimina el punto de restauración más antiguo que encuentre. No existe forma de salvaguardar un punto de restauración en concreto.

2.2.3. Inicio del sistema.

- Si no queremos usar la pantalla de bienvenida, se puede usar la pantalla de entrada al sistema de Windows 2000. Para ello debemos irnos a Panel de Control – Cuentas de Usuario y escoger la opción de “Cambiar la forma en la que los usuarios inician y cierran sesión”.
- Esta manera de entrar en el sistema fuerza a escribir el nombre de la cuenta de usuario, aunque esto refuerza la seguridad del sistema. Contamos con la ventaja en este método de que podemos usar la cuenta del Administrador para abrir sesión en Windows XP sin ningún problema.
- El cambio rápido de usuario nos permite cambiar del usuario de la sesión actual, a otra sesión de otro usuario sin tener que cerrar la misma. Esto es útil cuando otro usuario necesita usar la maquina, pero nosotros tenemos un programa en ejecución. Podemos usar el cambio rápido de usuario para abrir otra sesión en nuestra maquina, sin tener que cerrar la nuestra y por lo tanto, detener el programa. El cambio rápido de usuarios, se hace con las teclas **WINDOWS + L**.

2.2.4. Obtener información sobre el sistema.

- Si buscamos información sobre el arranque de nuestro sistema, que programas se cargan, desde donde, etc., podemos acceder a este tipo de información y modificar algunos aspectos desde Inicio – Ejecutar – MsConfig.

- Desde esta herramienta, podemos ver que procesos se cargan en el inicio de nuestro sistema, ya sea desde el SYSTEM.INI, el WIN.INI y el BOOT.INI (archivos de arranque que se utilizan en Windows XP para permitir la compatibilidad con anteriores versiones de Windows) o desde los procesos de inicio de Windows XP (Registro). Si queremos saber que se ejecuta en nuestro sistema, debemos prestar atención a todas las pestañas, y no sólo a la última de inicio.

2.2.5. Escritorio remoto.

- Podemos controlar nuestro PC situado en nuestra casa desde nuestro PC del instituto, pudiendo realizar casi las mismas acciones como si estuviéramos sentados delante de nuestra maquina.
- Para realizar esto, primero debemos configurar el equipo a controlar para que utilice escritorio remoto. Para ello, si el equipo trabaja con Windows XP debemos abrir **Sistema** en **Panel de Control**. En la pestaña **Remoto** debemos activar la casilla de verificación **Permitir a los usuarios conectarse remotamente a este equipo**.
- Para que podamos activar esta opción, debemos haber entrado en el sistema como un usuario con permisos de administración. Vemos también como desde aquí podemos seleccionar los usuarios de nuestro sistema que podrán acceder a el desde el exterior, y se nos informa que es imposible acceder desde el exterior con una cuenta de usuario que no tenga contraseña.
- Si el equipo que queremos controlar no es Windows XP, debemos introducir el CD de Windows XP y cuando aparezca la página de bienvenida, hacemos clic en **Realizar tareas adicionales** y, a continuación, clic en **Configurar conexión a Escritorio remoto**.
- Una vez que hemos activado en la maquina a controlar el acceso remoto a la misma, ya podemos controlarla remotamente. Para ello, nos situamos en la maquina desde la que queremos controlar nuestro PC y ejecutamos el asistente “Conexión a Escritorio Remoto”.
- En el formulario que nos aparece, indicamos a que equipo nos queremos conectar (podemos usar el nombre del equipo o su dirección IP). Una vez conectado al equipo, nos pedirá que iniciemos sesión (para lo que necesitaremos un nombre de usuario y contraseña usado en la maquina a controlar). Si en la maquina a controlar existe alguna sesión abierta, se cerrará para permitir abrir nuestra sesión.

2.3. Administración.

2.3.1. Cuentas de usuario.

2.3.1.1. Gestión de cuentas de usuario.

- Podemos gestionar las cuentas de usuario, usando un programa gestor con estilo Windows 2000. Si estamos conectados a un dominio, este es el gestor de usuarios que usaremos por defecto. Para acceder a dicho gestor, hay que ejecutar la siguiente orden desde Inicio – Ejecutar, o bien desde una ventana del intérprete de comandos CONTROL USERPASSWORDS2.
- La primera opción que vemos en pantalla, la de **Los usuarios deben escribir su nombre y contraseña para usar el equipo** nos permite indicar si queremos usar el sistema de usuarios y contraseñas o no. Si lo desactivamos, obtendremos un XP que se iniciará automáticamente con la cuenta que indiquemos sin mostrarnos siquiera la pantalla de bienvenida.

- Desde esta pantalla, podemos observar como podemos incluir al usuario en algún grupo de usuarios, bien uno de los dos incluidos en el gestor (usuarios estándar y usuarios restringidos) o bien seleccionando otro grupo como puede ser el de administradores, etc.
- La opción más interesante de todas las que nos ofrece XP es el gestor avanzado de cuentas de usuario, o consola de usuarios y grupos. podemos llegar a este gestor mediante Panel de Control – Herramientas Administrativas – Administración de Equipos y en ella escogemos la carpeta de usuarios locales y grupos. Podemos tanto asignar a un usuario varios grupos, como asignar a un grupo varios usuarios.
- Existen dos cuentas de usuario especiales en Windows XP, ya creadas y que no pueden (no deben) ser modificadas o eliminadas:
  - *La cuenta del Administrador del sistema (Administrador o Administrator).* Todos los sistemas XP tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitados para que solo puedan ser ejecutadas por el Administrador. Es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador, aunque Administrador solo puede haber uno. Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema.
  - *La cuenta de Invitado (Guest o Invitado).* Por defecto, en Windows XP Profesional esta cuenta esta desactivada y hagamos lo que hagamos no podremos asignarle una contraseña.
- Si nuestro sistema funciona bajo un grupo de trabajo, toda la información sobre estas cuentas se guarda en nuestro equipo con Windows XP, por lo que se dice que esta configurado con cuentas de usuario locales. Sin embargo existe otra forma de trabajar. Si en nuestra red se encuentra instalado un ordenador con Windows .Net Server, Windows 2000 Server o Windows NT Server, podemos indicar que la información de las cuentas se almacenen en dicho servidor, y no en nuestra maquina. Esta manera de trabajar nos permite obtener cuentas de usuario globales, y se suele conocer como trabajar en un dominio.

2.3.1.2. Tipos de cuentas y grupos.

- Una cuenta puede pertenecer a un determinado grupo, lo que permite al administrador simplificar enormemente la gestión de permisos y derechos en el sistema. Una cuenta de usuario puede pertenecer a un grupo, a varios grupos, o no estar vinculada a ningún grupo. Los permisos y derechos de los grupos son acumulativos, es decir, si un usuario pertenece a tres grupos, tendrá todos los derechos y permisos asignados a los tres grupos.
- Windows XP clasifica a las cuentas de usuario en varios grupos distintos que ya están creados en el momento de instalar el sistema. Aparte de estos grupos ya definidos, podemos crear todos los grupos que nos interesen.
- Si ejecutamos la orden NET USER desde una ventana del intérprete de comandos veremos una lista de los usuarios del sistema. Si ejecutamos NET USER (nombre del usuario) veremos variada información sobre dicha cuenta. La orden NET LOCALGROUP nos permite gestionar grupos locales también desde el intérprete de comandos.

2.3.1.3. Cuenta de administrador.

- Normalmente, la cuenta de Administrador no se muestra en la vista de la pantalla de bienvenida. Solo aparecerá en dicha pantalla, en las siguientes ocasiones:
  - No existe ninguna otra cuenta con derechos de administración.
  - Se ha iniciado el equipo en el modo a prueba de fallos (presionando F8 durante el inicio).
  - El Administrador tiene una sesión abierta y hemos usado cambio rápido de usuarios.
  - Para conseguir entrar en el sistema como Administrador, debemos pasar a la pantalla de bienvenida clásica (pulsando CTRL – ALT – SUPR al iniciar el sistema en la pantalla de bienvenida), escribir Administrador como nombre de usuario, e introducir su contraseña.
- Otra cosa que podemos hacer es cambiar el nombre de la cuenta administrador. Para ello, debemos abrir la consola SECPOL.MSC (Inicio – Ejecutar – SECPOLMSC) y en la opción de Políticas locales / Seguridad escoger la opción de Renombrar la cuenta del Administrador. No es nada recomendable cambiar de nombre esta cuenta, ya que existen muchos programas que esperan una cuenta con nombre Administrador.

2.3.1.4. Contraseñas en las cuentas de usuario.

- Si queremos forzar aun más el uso de contraseñas, podemos hacerlo ejecutando la consola de seguridad local SECPOL.MSC y desde allí colocar una serie de restricciones a las contraseñas. Si modificamos el valor de Longitud mínima de contraseña y ponemos algo mayor que cero, obligaremos a que cualquier cuenta de usuario nueva tenga que llevar contraseña, aunque sea de un único carácter.
- Al crear una contraseña, también se nos da opción de asignar una “pista” para dicha contraseña, de modo que si la olvidamos podamos recordarla leyendo esa pista. También es posible crear un disco para restablecer la contraseña, que nos crea un disco que inicia sesión en la maquina, aunque nos olvidemos de nuestra contraseña.
- Un administrador del sistema, podrá asignarnos una nueva contraseña, pero perderemos todos los archivos cifrados que tuviéramos en el equipo, y a todos los mensajes de correo electrónico que tuviéramos asociados a dicha cuenta.

2.3.1.5. Permisos y derechos locales.

- En Windows existen dos tipos de privilegios de acceso, los derechos y los permisos. Un permiso es el que nos permite acceder a un determinado recurso para realizar una acción en concreto. Un derecho es el que nos permite realizar una acción sobre todo el sistema, como puede ser iniciar sesión en el sistema, o cambiar la hora del reloj del sistema.
- El propietario de un recurso (o un Administrador) puede asignar permisos para ese recurso, mediante el cuadro de dialogo propiedades de dicho recurso. Un Administrador establece permisos usando las directivas de seguridad locales, a la que puede accederse mediante las opciones administrativas.
- Si no vemos la pestaña seguridad en las propiedades del recurso, debemos desactivar la opción Uso compartido simple de archivos (recomendado) a la que podemos llegar desde cualquier ventana de Mi PC, menú Herramientas – Opciones de carpeta – Ver y al final de la lista encontramos dicha opción Asimismo, esta pestaña de Seguridad solo puede activarse en carpetas

que estén grabadas en volúmenes que utilicen el sistema de ficheros NTFS, dado que FAT no presenta opciones de seguridad para los directorios.

- Gracias a la herencia de permisos, todos los recursos que creamos heredan los permisos que tenga establecidos el recurso padre que contiene a dichos recursos. Esto se realiza así para simplificar la vida de los Administradores. En realidad todas las nuevas carpetas que creamos heredan los permisos de la raíz de los volúmenes. Es decir, todas las carpetas que creamos en el volumen D: tienen los permisos de D:\
- ¿Y si alguna vez queremos interrumpir la herencia? Para ello, debemos crear la carpeta, y una vez creada entrar en las propiedades de la carpeta, ir a la pestaña Seguridad y pulsar el botón Opciones Avanzadas. Si desmarcamos la casilla “Heredar del objeto principal las entradas de permisos relativas a los objetos secundarios. Incluirlas juntos con las entradas indicadas aquí de forma explicita”, romperemos la herencia para esta carpeta, con lo que podremos eliminar y modificar permisos de la carpeta actual.
- Si activamos la casilla “Reemplazar las entradas de permisos en todos los objetos secundarios con aquellas entradas incluidas aquí y que sean relativas a los objetos secundarios”, conseguiremos que al modificar los permisos de esta carpeta, también se modifiquen automáticamente los permisos de todas las carpetas que están por debajo de la nuestra.
- Cuando deseleccionamos la primera casilla, la de “Heredar del objeto principal…” el sistema nos presentara un formulario de opciones, donde nos preguntará si queremos Copiar los permisos anteriores o Quitarlos. Si elegimos copiar, la carpeta quedará con los mismos permisos que heredó, aunque ya serán modificables. Si seleccionamos Quitar, se perderán todos los permisos de la carpeta heredados y empezaremos desde cero.
- Si tenemos una carpeta en la que solo tiene permisos un usuario y donde los Administradores no tienen ningún permiso, podemos acceder como Administrador a la pestaña Seguridad de la carpeta. saldrá un mensaje indicando que no podemos modificar directamente esta carpeta. Una vez en la pestaña **Seguridad** accederemos al botón de **Opciones Avanzadas**. La pestaña que nos interesa en este momento es **Propietario**. Veremos como en esta pestaña podemos cambiar el propietario actual de esta carpeta. Así, siendo administrador podemos quitar cualquier recurso a cualquier usuario y quedarnos con el como propietarios del mismo.
- De este modo, por mucho que un usuario intente modificar las opciones de seguridad de sus carpetas como propietario o creador de las mismas, siempre podemos como administrador tomar posesión de dichas carpetas. Una vez que hemos tomado el control de la carpeta, ya podemos acceder a la pestaña seguridad, y modificar los usuarios que pueden tener acceso a la misma, incluyéndonos nosotros en la lista de usuarios del recurso.
- Depende de los permisos que se le asignen a cada usuario, este podrá realizar o no determinadas acciones. A continuación se indican algunas acciones y el grupo de permisos que hay que otorgar para poder realizarlos:
  * El permiso **Recorrer carpeta** permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas). **Recorrer carpeta** sólo surte efecto cuando al

grupo o al usuario no se le ha concedido el permiso **Omitir comprobación de recorrido**, que comprueba los derechos de usuario en el complemento Directiva de grupo.

- El permiso **Atributos de lectura** permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.
- El permiso **Atributos extendidos de lectura** permite o impide que el usuario vea los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.
- El permiso **Atributos de escritura** permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.
- El permiso **Atributos extendidos de escritura** permite o impide que el usuario cambie los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.
- El permiso **Leer permisos** permite o impide que el usuario lea permisos del archivo o de la carpeta, como **Control total**, **Leer** y **Escribir**.
- El permiso **Tomar posesión** permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

2.3.1.6. Gestión de recursos compartidos en red.

- En Windows 98 esto se realiza mediante el **control de acceso a los recursos** mediante contraseñas. Podemos además crear dos contraseñas por cada recurso, una que permitirá a los usuarios leer la información del recurso pero no a escribir en el mismo, y otra contraseña que permitirá al usuario tener un control total del mismo. Este sistema presenta una serie de inconvenientes muy importantes:
  - Cada vez que comparto un recurso en la red si no quiero que sea accesible por todo el mundo, debo asignarle una contraseña. Posteriormente debo comunicar a todos los usuarios a los que quiero permitir el acceso la contraseña que he introducido.
  - Si además quiero que algunos usuarios tengan control total y otros no, debo comunicar dos contraseñas distintas.
- Windows XP no utiliza el **control de acceso a los recursos** mediante contraseña, sino que implementa el **control de acceso a los usuarios**. Esto significa que cuando creamos un recurso compartido no indicamos ninguna contraseña, sino que indicamos directamente a qué usuarios quiero dar permisos sobre dicho recurso, que permisos quiero asignar a cada usuario, etc.
- La gestión de los permisos en los recursos compartidos es muy parecida a la gestión de los permisos para los recursos locales. Debemos asignar los permisos para cada recurso compartido, indicando que usuarios o grupos tendrán acceso a dicho recurso, y limitando las posibilidades de uso de cada uno de ellos. También podemos modificar la gestión de la seguridad para cada recurso local.

- Antes de comenzar a compartir recursos, es aconsejable asegurarnos de que la cuenta de usuario "Invitado" esta desactivada, ya que podría ser usada por algunos usuarios para entrar en nuestras carpetas compartidas sin necesidad de contraseña. Aunque no tendrían ningún permiso sobre dichas carpetas, siempre es un riesgo innecesario.
- Para compartir recursos, debemos hacer clic en dicho recurso con el botón derecho, y en la opción "Propiedades" irnos a la pestaña Compartir. Si no nos aparece esta opción, debemos asegurarnos de que hemos activado el uso de recursos compartidos. Para ello, comprobamos que en el cuadro de dialogo de propiedades de la conexión de red esta activado el servicio **Compartir impresoras y archivos para redes Microsoft** (protocolo NetBEUI). En caso de que dicho servicio no este activo, debemos instalarlo desde el mismo formulario.
- Debemos tener cuidados a la hora de compartir carpetas, ya que por defecto se comparten las carpetas y las posibles subcarpetas que cuelguen de la misma. Nunca se debe compartir una carpeta de sistema (donde estén instaladas partes de Windows) y no es aconsejable compartir carpetas en las que existan programas ejecutables que se encuentren instalados en nuestra maquina (podrían tener archivos que se cargaran al inicio de nuestro sistema, con lo que los usuarios de nuestra red tendrían una opción de modificar nuestro inicio, introduciendo virus o errores en la carga). Tampoco se deben compartir los directorios raíz de las unidades, ya que es otorgar demasiado control a los usuarios de red.
- Podemos establecer también aquí el numero máximo de usuarios que queremos que usen el recurso. La opción por defecto (máximo permitido) va a permitir que hasta 10 usuarios estén conectados a este recurso al mismo tiempo. Si necesitamos que accedan más de 10 usuarios, debemos usar una versión servidora de Windows.
- Por defecto, un recurso se crea con permisos totales para todos los usuarios. **Esto es muy peligroso**. Debemos entrar en la opción de permisos, y establecer los permisos que nos interesen, y los usuarios a los que queremos darles esos permisos.
- Por defecto al compartir un recurso, Windows XP deja **Todos** (Everyone), con lo cual todos los usuarios que **estén dados de alta en nuestra maquina** podrán usar dicho recurso desde la red. Si un usuario intenta usar dicho recurso y no tiene una cuenta asociada en nuestro Windows XP con su nombre y contraseña no podrá.
- **Cualquier usuario** que quiera **acceder a un recurso** nuestro **desde la red**, debe usar un **nombre de usuario y una contraseña local de nuestro equipo**. Windows XP no permite el acceso ANONIMO a un recurso. Se denomina ANONIMO cuando nuestro equipo no reconoce el nombre y la contraseña del usuario que intenta acceder a nuestro equipo.

2.3.1.7. Perfiles de usuario.

- El perfil de usuario contiene todas las características y ficheros que forman parte de entorno de trabajo de un usuario. Esto incluye los parámetros especiales de ese usuario en el registro del sistema para multitud de aspectos, desde el aspecto del cursor del ratón, a la forma en que configura el Word, las cookies que utiliza, los favoritos de Internet, sus carpetas de documentos, accesos directos a carpetas de red, etc.

- Los perfiles de usuario locales se almacenan bajo la carpeta DOCUMENTS AND SETTINGS que se crea en el mismo volumen donde instalamos Windows XP, y en una carpeta con el nombre de la cuenta del usuario. Nuestro perfil estará almacenado en %SystemDrive%\Documents And Settings\%UserName%. Toda esta ruta esta también almacenada en una variable de entorno que es la de %UserProfile%.
- Dentro de cada perfil de usuario, encontramos una jerarquía de directorios o carpetas. El raíz de dicho perfil (es decir, la carpeta dentro de Documents And Settings que tiene como nombre el nombre del usuario) contiene un fichero NTUSER.DAT, que contiene la porción de información del registro del sistema inherente a dicho usuario. Si nuestro equipo forma parte de un dominio de Windows NT Server, también existirá un fichero NTUSER.POL, con las políticas de seguridad del sistema. En Windows 2000 se sustituyen estas políticas del sistema, por las políticas de grupo.

2.3.1.8. Perfiles comunes. Tipos de perfiles.

- Hay dos tipos de perfiles comunes:
  - Perfil **All Users**. El contenido de este perfil, se añade a los contenidos de los perfiles de cada usuario. Por defecto, solo los administradores pueden añadir objetos al escritorio y al menú inicio del perfil All Users.
  - Perfil **Default User**. Cuando un usuario inicia sesión en nuestro sistema por primera vez (y no tiene un perfil móvil u obligatorio), Windows crea un nuevo perfil local para dicho usuario, copiando el contenido de la carpeta Default User a una nueva carpeta con el nombre del usuario. Por lo tanto, podemos configurar los perfiles de nuestros nuevos usuarios, modificando el contenido de la carpeta Default User. Por defecto, solo los administradores pueden hacer cambios en esta carpeta.
- Hay que tener cuidado con un error que se suele cometer con los permisos de los ficheros al usar estos perfiles. Si ***copiamos*** un fichero a la carpeta de perfil para Default User, este fichero obtiene los permisos de la carpeta. Sin embargo, si ***movemos*** un fichero a la carpeta de perfil para Default User, este fichero conserva sus permisos propios. Esto hace que si como administrador creamos un fichero y lo movemos a la carpeta Default User (o a cualquier carpeta en realidad) este fichero nos pertenecerá a nosotros, y es muy probable que el usuario no tenga permiso ni siquiera para verlo.
- Windows admite tres tipos distintos de perfiles.
  - **Perfiles de usuarios locales**. Son los que se almacenan en %SystemDrive%\Documents And Settings en el disco duro local. Si un usuario cambia algo en su perfil, esos cambios solo se registran en nuestra maquina local, como es obvio. Es el único tipo de perfil usado si no estamos en un dominio.
  - **Perfiles de usuario móviles**. Estos perfiles no se almacenan en el disco duro local de la maquina, sino en un servidor de red. Esto implica que esos perfiles están disponibles para los usuarios sin importar en que maquina abran sesión, siempre que dichas maquinas tengan acceso a ese servidor. El perfil se encuentra almacenado en un servidor, de modo que al iniciar sesión se copia dicho perfil a la maquina en la que se encuentre el usuario. Si el

usuario modificar algo del perfil, dichos cambios son introducidos también en el servidor. Estos perfiles móviles pueden ser utilizados si contamos con un servidor en la red que cuente con Windows .NET Server o Windows 2000 Server.

- **Perfiles de usuario Obligatorios**. Estos perfiles solo pueden ser cambiados por los administradores. Inicialmente, es igual que un perfil de usuario móvil, pero a diferencia de éste, los cambios que el usuario efectué en su perfil no se copian en el servidor.

2.3.1.9. Gestión y asignación de perfiles.

- Salvo las carpetas escritorio y menú inicio, las demás carpetas no deben ser modificadas desde el explorador de archivos. Para gestionar estos perfiles, debemos usar el formulario de perfiles de usuario que XP incorpora. Para llegar a este formulario debemos ir al formulario Sistema (Panel de Control – Sistema o Propiedades de Mi PC) y allí Opciones Avanzadas – Perfiles de Usuario: Configuración.
- Los miembros que no sean miembros del grupo Administrador no podrán ver otros perfiles diferentes al suyo, y no pueden modificar ningún perfil. No se puede gestionar un perfil que tenga sesión abierta en el sistema.
- Como Administrador del sistema podemos asignar directamente un perfil a una cuenta de usuario. Para ello debemos usar la MMC (Microsoft Management Console) con el "snap-in" de Usuarios locales y Grupos. Si desde allí escogemos un usuario y hacemos doble clic, veremos como nos aparecen las propiedades de dicho usuario, y tenemos una pestaña para gestionar su perfil. Desde este formulario, podemos configurar lo siguiente:
  - **Ruta de acceso al perfil**. Si no queremos que el perfil este localizado en su ubicación por defecto, podemos indicar aquí donde queremos que se cree dicho perfil. Hay que tener en cuenta que el usuario que use el perfil debe tener derechos totales sobre dicha carpeta.
  - **Archivo de comandos de inicio de sesión**. Aquí podemos colocar el nombre y localización de un fichero de comandos (Script) que se ejecutará cada vez que el usuario inicie sesión. El Script de inicio de sesión, es un programa que se ejecuta automáticamente cada vez que el usuario inicia sesión en nuestra maquina. Cualquier fichero ejecutable (bat, cmd, vbs, js, wsf, exe, com,..) puede ser usado como Script de inicio.
  - **Carpeta particular (Home). Ruta de acceso local**. La carpeta particular (Home) es una carpeta en la que el usuario puede almacenar sus ficheros y programas. Aunque la mayoría de los programas usan la carpeta Mis Documentos para almacenar los ficheros del usuario, podemos necesitar crear una carpeta alternativa para dicho usuario. Si hemos creado un Script de inicio de sesión para el usuario, su directorio por defecto inicial es esta carpeta Home. Aquí indicamos en que directorio de nuestro sistema hemos creado la carpeta para dicho usuario.
  - **Carpeta particular (Home). Conectar**. Desde aquí podemos asignar una letra de unidad a un recurso compartido en red de otro equipo, de modo que creamos la carpeta Home del usuario en otro equipo de la red.

- Toda esta gestión de perfiles que hemos visto, **sólo** funciona adecuadamente si estamos unidos a un dominio. En un ámbito de grupo de trabajo, no es recomendable trabajar con perfiles que no sean locales.

2.3.1.10. Directivas de grupo locales.

- Las directivas de grupo forman parte de la estructura de Windows 2000, Windows XP y Windows .Net. En estos sistemas, las políticas de grupo son una herramienta muy poderosa que permite a los administradores configurar equipos de forma local o remota, instalando aplicaciones, restringiendo los derechos de los usuarios, eliminando aplicaciones, instalando y ejecutando scripts, y redirigiendo carpetas del sistema a red o viceversa. Pero también tienen utilidad las políticas de grupo en entornos pequeños, incluso en una sola máquina.
- Si estamos trabajando bajo un dominio (con un servidor en la red administrando dicho dominio) las políticas de grupo cobran mayor protagonismo. En un ambiente de grupo de trabajo, las políticas de grupo de cada maquina, controlan los aspectos únicamente de dicha maquina. Si nuestro equipo esta unido a un dominio, podemos configurar directivas del dominio completo, que afectarán a varias maquinas.
- El añadido (snap-in) de las consolas de Microsoft (MMC) que se encarga de las directivas de grupo es el **gpedit.msc**. (Inicio – Ejecutar – **gpedit.msc**).
- Dentro las directivas de grupo locales tenemos dos opciones:
  - *Configuración del equipo*. Los cambios que realicemos dentro de configuración del equipo se aplicarán al equipo local, y por lo tanto, afectarán a todos los usuarios del equipo local.
  - *Configuración del usuario*. Los cambios que realicemos dentro de la configuración del usuario, afectarán a usuarios, sin importar desde qué equipos se conecten.
- Algunas directivas aparecen tanto en la configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.
- Cuando activamos directivas de grupo, tanto desde configuración del equipo, como desde configuración del usuario, estas directivas se aplican a **todos** los usuarios, incluidos nosotros mismos. En una máquina que usamos normalmente, nos interesa buscar un método que nos permita “saltarnos” las directivas. Para conseguir esto, tenemos que tener en cuenta lo siguiente:
  - Las directivas de grupo se almacenan en una carpeta de nuestro sistema, concretamente en la carpeta %SystemRoot&\System32\GroupPolicy.
  - Cada vez que un usuario inicia sesión en nuestro equipo, el usuario lee automáticamente las directivas que encuentre en dicha carpeta
  - Todas las directivas que son leídas desde dicha carpeta se aplican al usuario que acaba de entrar en el sistema.
- El método consiste en impedir que los usuarios del grupo Administradores puedan leer dicha carpeta. Es decir, modificamos los permisos de seguridad de la carpeta donde están las directivas, %SystemRoot&\System32\GroupPolicy de modo que impidamos que los Administradores tengan permiso de lectura.

- De este modo, podemos conseguir que las directivas del sistema no se nos apliquen, pero si nos damos cuenta, al denegarnos a nosotros mismos los permisos sobre la carpeta GroupPolicy, estamos consiguiendo también que sea imposible que modifiquemos las directivas de grupo.
- Esto implica que siempre que vayamos a modificar una directiva de grupo tendremos que tomar el control sobre la carpeta GroupPolicy, para poder leer y escribir en ella antes de poder modificar la directiva, y una vez que hayamos modificado la directiva, volver a quitarnos el permiso de lectura sobre dicha carpeta. Todo esto lo tenemos que hacer sin cerrar sesión, ya que podemos correr importantes riesgos en caso contrario.
- Esta complejidad de los permisos sobre GroupPolicy vienen dados por que en cierta forma estamos "forzando" el uso de las directivas, que están pensadas para trabajar generalmente en un dominio, y no en un grupo de trabajo.

2.3.1.11. Asignación de derechos de usuario.

- Podemos asignar estos derechos en las directivas de grupo, en Configuración del equipo – Configuración de Windows – Configuración de seguridad – directivas locales – asignación de derechos de usuario. También podemos tomar un atajo, y ejecutar **SECPOL.MSC** que nos abrirá la consola con la asignación de derechos de usuario cargada por defecto.
- Unos derechos especialmente importantes son los derechos conocidos como derechos de inicio de sesión (logon rights) como denegar el acceso desde la red a este equipo, denegar el inicio de sesión localmente, etc. En estos derechos si podemos añadir los grupos o usuarios que queramos, y por lo tanto, podemos establecer que usuarios tendrán que iniciar sesión localmente, y cuales deberán hacerlo forzosamente desde la red, o al contrario.

2.3.1.12. El Administrador de equipos.

- Para ejecutar la consola del Administrador de equipos, podemos bien acceder a Herramientas Administrativas – Administrador de Equipos, o podemos ejecutar la orden COMPMGMT.MSC que nos trae directamente la consola de administrador de equipos. Una función interesante de esta consola, es que permite conectarnos para administrar otros equipos.
- Si nuestra cuenta de usuario actual (en el equipo local) es reconocida en el equipo a administrar como una cuenta del grupo Administradores, o si introducimos un nombre de usuario y contraseña reconocidos como del grupo Administradores por el equipo a controlar veremos que pasamos a administrar el equipo de la red remotamente.
- Así, es posible para un Administrador controlar una red completa de equipos siempre que tenga cuentas del grupo de administrador creadas en todos los equipos. Esto es una aproximación al control total que ejercemos cuando estamos trabajando en un dominio, en lugar de en un grupo de trabajo.

2.3.2. El registro del sistema.

2.3.2.1. Descripción. Claves del registro.

- En las versiones anteriores a Windows 95, cada programa que se instalaba, incluyendo los propios programas de Windows, contaba con una serie de ficheros donde se almacenaban las configuraciones de dichos programas. Estos ficheros solían tener la extensión .ini.

- A partir de Windows 95, aunque no se prohibieron los ficheros .ini, se creó una base de datos jerarquica central donde se guardan todas las configuraciones de todos los programas, incluidas las configuraciones del sistema operativo. Esta base de datos es el Registro de Windows.
- Cualquier opción que escojamos en el panel de control, en un menú de Word, una preferencia que escojamos en un juego que instalemos, cualquier directiva de grupo que activemos, etc., en realidad hace referencia a un cambio que se produce en una clave del Registro.
- El registro del sistema esta estructurado en forma arborescente (como los directorios de un volumen). En primer lugar tenemos las carpetas principales que cuelgan del raíz del registro. Estas carpetas principales son:
  - *HKEY_CURRENT_USER*. Contiene la raíz de la información de configuración del usuario que ha iniciado la sesión (el usuario actual). Aquí se almacenan las carpetas de usuario, los colores de pantalla y la configuración del Panel de control. Esta información se conoce como perfil de usuario.
  - *HKEY_USERS*. Contiene todos los perfiles de usuario del equipo. HKEY_CURRENT_USER es una subclave (un directorio) de HKEY_USERS.
  - *HKEY_LOCAL_MACHINE*. Contiene información de configuración específica del equipo local. Por lo que se aplican estas configuraciones a todos los usuarios del equipo local.
  - *HKEY_CLASSES_ROOT*. Es una subclave (subdirectorio) de la clave principal HKEY_LOCAL_MACHINE\Software. En esta entrada se almacena la información de la asociación de las extensiones. Aquí se indica que un .doc se abre con el winword.exe, etc.
  - *HKEY_CURRENT_CONFIG*. Contiene información acerca del perfil de hardware que utiliza el equipo local al iniciar el sistema. Es la configuración actual que se está usando para algunos puntos muy concretos.

2.3.2.2. Edición del registro.

- Es conveniente exportar a un sitio seguro la rama del registro que vamos a modificar, de modo que siempre podamos restaurarla en caso de necesidad desde el menú Archivo con la opción Importar. Hay que tener en cuenta una cosa a la hora de importar y exportar partes del registro. Si exportamos un archivo .reg (archivo de registro) realizamos una copia parcial únicamente, de modo que si exportamos, añadimos una clave nueva al registro, y luego importamos, nuestra clave nueva seguirá existiendo. Sin embargo, un archivo de subárbol realiza una copia total, de modo que si exportamos, añadimos una clave nueva al registro, y luego importamos, veremos como nuestra nueva clave desaparece dejando el registro tal y como estaba a la hora de realizar la exportación.
- Windows XP presenta un comportamiento anómalo cuando se importan subárboles grandes, llegando a presentar problemas de memoria baja e incluso llegando a corromper partes del registro. Se recomienda no utilizar subárboles siempre que sea posible.
- Cualquier cambio que se hace en el registro es automáticamente ejecutado por el sistema, sin tener siquiera que cerrar el editor del registro. Un método muy simple de modificar valores del registro es escribir un fichero con la cabecera arriba indicada, escribir la ruta completa del valor a modificar entre corchetes, y posteriormente, y entre comillas la entrada a cambiar y el valor al

que se va a cambiar. Las claves del registro (en el panel izquierdo) tienen también permisos para usuarios, al igual que las carpetas.

2.3.2.3. Modificación de un registro.

- Podemos modificar el registro de otro ordenador, por ejemplo, para repararlo o hacerle algún tipo de mantenimiento. Es parecido a la administración remota de otra equipo que hacemos desde Administración de equipos, aunque podemos perfilar algo más la administración directamente desde el registro.
- Para ello, veremos que en el programa Regedit.exe tenemos una opción en el menú para conectar a un registro de red. Solo podemos modificar las ramas HKEY_USERS y HKEY_LOCAL_MACHINE remotamente, que suelen ser las más interesantes.

2.3.3. El visor de sucesos.

- Windows XP permite llevar un registro de los sucesos que se producen en el sistema. Estos registros son almacenados automáticamente en tres ficheros:
  - Seguridad (Secevent.evt).
  - Aplicación (Appevent.evt).
  - Sistema (Sysevent.evt).
- El visor de sucesos, es un añadido de consola que se instala conjuntamente con el Windows XP y que nos permite visualizar estos tres archivos. La principal utilidad del visor de sucesos es la de auditar nuestros propios sucesos. el archivo de sucesos seguridad no tiene ninguna entrada. Este archivo se reserva para las auditorias que nosotros establezcamos.
- Para comenzar a utilizar estas auditorias de seguridad:
  - Nos vamos a Herramientas Administrativas – Directivas de seguridad local.
  - Nos vamos a Directivas Locales – Directivas de Auditoria.
  - Aquí veremos los posibles sucesos que podemos auditar. Por cada suceso, podemos habilitar que se auditen tanto los intentos correctos como los erróneos.
- Si creamos una carpeta en el systemdrive y accedemos a las propiedades de dicha carpeta, pestaña Seguridad – Opciones Avanzadas, veremos que también tenemos aquí una pestaña Auditoria. En dicha opción de auditoria, podemos indicar si queremos auditar el acceso a este recurso u objeto, e incluso indicar a que usuarios queremos auditar.
- Tenemos que tener mucho cuidado a la hora de auditar sucesos, pues es muy fácil que acabemos con una cantidad tal de sucesos auditados que sea casi imposible buscar el que realmente queremos ver.

2.3.4. Servicios en Windows XP.

- Para gestionar los servicios, usamos la consola services.msc (como siempre, podemos ejecutar directamente la consola, o llegar a ella desde Herramientas Administrativas – Servicios. Desde esta consola podemos parar, iniciar, detener y reiniciar cualquier servicio. No todos los servicios permiten que los iniciemos o paremos manualmente, esto suele ser debido a que existen servicios que dependen de otros servicios.

- Otra manera de iniciar o detener un servicio, es utilizar los comandos NET START y NET STOP desde el símbolo de sistema. El modo de usar estos comandos es NET START/STOP nombre del servicio.
- Para revisar o modificar la forma en que un servicio se inicia, o que sucede cuando no funciona correctamente, podemos acceder a las propiedades de dicho servicio (doble clic sobre el servicio en la consola de servicios). En la pestaña general del formulario, podemos especificar las opciones de inicio del servicio. La más interesante es la que se refiere al tipo de inicio.
- Desde la pestaña Iniciar sesión, podemos indicar que el servicio se inicie desde una cuenta de usuario y no desde la cuenta del sistema. En caso de usar esta opción, debemos asegurarnos de que el usuario indicado tiene derecho para iniciar dicho servicio.
- Desde la pestaña recuperación, podemos indicar que queremos que se realice si dicho servicio deja de funcionar.
- La ultima pestaña, de Dependencias, nos indica si este servicio depende de otro, de modo que podamos ver la jerarquía de servicios, y sepamos que ocurrirá si paramos dicho servicio.
- También podemos gestionar los servicios desde el símbolo del sistema, mediante las órdenes NET START, NET STOP, NET PAUSE y NET CONTINUE. Como ejemplo, para que la orden NET SEND mensaje funcione, debemos tener activo el servicio MENSAJERO. Podemos activar dicho servicio desde la consola de servicios o directamente con la orden NET START MENSAJERO. De igual modo, podemos pararlo desde la consola o con NET STOP MENSAJERO.
- Existen determinados programas, como puede el ICS (Conexión compartida a Internet) que corren como servicios automáticos. Esto permite, que baste con encender nuestro equipo para que dichos programas funcionen, sin que sea necesario que abramos ninguna sesión en la maquina. Esto es una ventaja de Windows 2000 sobre otros sistemas como Windows 98, donde no se ejecuta ningún programa hasta que no comencemos a utilizar directamente el sistema.
- Podría ser ventajoso poder transformar un programa normal y corriente en un servicio. La propia Microsoft si incluye dicha utilidad (srvany) “Kit de recursos de Windows 2000”. También necesitamos para este fin la utilidad instsrv que nos permite instalar un servicio mediante srvany.
- Para ello, copiamos en un directorio (por ejemplo C:\SERV) los archivos necesarios, que podemos bajarnos directamente de Internet realizando una búsqueda sobre srvany download. Estos archivos son: srvany.exe, srvany.wri e instsrv.exe.
- Desde un símbolo de comandos, nos vamos al directorio anterior (C:\SERV) y escribimos la orden

  INSTSRV *MISERVICIO* C:\SERV\SRVANY.EXE

- Con esto, hemos creado un nuevo servicio, con el nombre que le hayamos indicado (MISERVICIO en este ejemplo, pero puede ser cualquiera) para comprobarlo, ejecutamos la consola services.msc y veremos como efectivamente se ha creado un servicio con el nombre que le hayamos dado. Desde aquí, podemos indicar el tipo de inicio que deseamos para nuestro servicio, la cuenta a la que vamos a asociarlo, etc.

- Bien, ahora tenemos que indicar a dicho servicio que es programa es el que queremos que se ejecute como servicio. Para ello, nos vamos al editor del registro del sistema (Regedit) y nos vamos a la ruta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services y veremos como se ha creado una carpeta con el nombre que le hayamos dado al servicio.
- Bajo esta carpeta MISERVICIO, tenemos que crear una clave con nombres **Parameters**, y en dicha clave tenemos que crear un nuevo valor alfanumérico con nombre **Application**. El valor de Application debe ser el nombre del programa que queremos ejecutar como un servicio, utilizando la RUTA COMPLETA del ejecutable.
- Podemos crear también aparte del valor Application, los valores AppParameters y AppDirectory para indicar los parámetros que va a usar el programa y el directorio donde se va a ejecutar el programa. Ambos valores también son alfanuméricos.
- Si queremos desinstalar un servicio que hayamos instalado con instsrv podemos utilizar el formato:

  INSTSRV *MISERVICIO* remove
- Podemos instalar tantas instancias de srvany como queramos, siempre que utilicemos un nuevo nombre para cada servicio distinto que instalemos.

3. Windows Server 2003.

3.1. Requisitos previos de instalación.

- Antes de instalar Windows Server 2003, es conveniente asegurarnos de que los componentes de hardware cumplen los requisitos mínimos y que todo nuestro software y hardware es compatible con Windows Server 2003. Podemos consultar la Lista de Compatibilidad de Hardware (HCL) en el siguiente sitio Web de Microsoft: http://www.microsoft.com/hcl/
- Los requisitos de Hardware para la versión Standard en plataforma x86 son los siguientes:
  - *CPU*. Hasta cuatro Pentium II 233 MHz. Recomendado Pentium II 550 MHz o equivalente.
  - *RAM*. 128 MB RAM es el mínimo y 4 GB RAM es el máximo. Se recomiendan 256 MB.
  - *Disco duro*. Partición con un tamaño mínimo de 2GB, disponiendo al menos de 1,5 GB de espacio libre en el disco duro.
  - *Monitor*. Resolución VGA o superior.
  - *Accesorios*. Teclado y ratón Microsoft o compatible.
  - *Dispositivos*. Unidad de CD-ROM o DVD.
- Particularidades en la instalación:
  - Se denomina servidor autónomo a un servidor que funciona dentro de un grupo de trabajo, y un servidor miembro a un servidor que funciona dentro de un dominio.
  - Si se configura el servidor como controlador de dominio es obligatorio disponer de una partición formateada en NTFS para almacenar el volumen de sistema compartido.
  - Modos de licencia. Se aplican a un ordenador determinado que establezca varias conexiones simultáneas a través del servicio Service Message Block (SMB), que está basado en NetBIOS. Pueden ser:

- **Por servidor**. El número de licencias es el número máximo de clientes distintos que permite conectarse a la vez, es modificable después de la instalación del sistema.
- **Por puesto**. No hay límite de conexiones siempre que cada cliente disponga de un puesto con licencia.

3.2. Técnicas de red.

3.2.1. Servicios individuales.

- En las primeras redes todo estaba situado en el servidor central, y los equipos individuales no podían compartir absolutamente nada con el resto de la red. NetWare 2.x y 3.x han sido los sistemas operativos para redes dominantes en redes pequeñas que incluyen sólo un servidor y 30 o menos estaciones de trabajo. Con tal arreglo no se requiere un sofisticado servicio de administración de recursos.
- Sin embargo, agregar un segundo servidor puede complicar las cosas de manera significativa. El problema surge porque cada servidor individual mantiene su propia lista de usuarios y recursos. Cada una de esas cuentas de usuarios debe ser creada y mantenida de manera separada.
- Los usuarios también tienen un problema con los diversos servidores individuales. Para usar una impresora, el usuario debe saber cuál servidor tiene la impresora. Para tener acceso a un archivo o programa, el usuario debe conocer cuál servidor lo aloja.
- Este tipo de redes siguen siendo muy adecuadas en situaciones simples, donde solo existe un servidor y tiene unas funciones muy delimitadas, aunque es una solución no valida para la mayoría de las situaciones actuales.

3.2.2. Directorio de red.

- Bajo este sistema, los recursos pueden estar situados en varios servidores, pero se recogen todos en una única lista o directorio. Los recursos pueden agruparse de manera lógica en este directorio para hacerlos más fáciles de ubicar. Los usuarios pueden buscar en el directorio la información que desean, ya sea buscando por tipos de impresoras, capacidades de volúmenes compartidos, etc.
- Un servicio de directorio es una especie de guía telefónica exhaustiva que permite a usuarios, administradores y aplicaciones acceder a la información existente de todos y cada uno de los usuarios y sistemas de una red con tan sólo pulsar un botón o a través de programas muy simples.
- Como servicios de directorios de red, podemos citar:
  - X.500 es un estándar internacional para servicios de directorio, aunque su función se centra en la creación de directorios a nivel global y no en redes locales.
  - NetWare Directory Services (NDS, Servicios de directorio NetWare) está incorporado dentro de la línea de productos Novell NetWare 4.x. NDS está basada en X.500, aunque no es totalmente compatible con el estándar.
  - LDAP. Es el estándar creado por Microsoft para usarlo como base de su directorio. Aunque se integró parcialmente en unos añadidos a Windows NT, su uso principal se realiza en Windows 2000.

- En lugar de conectarse a diversos servidores, el usuario se conecta a una red y tiene acceso a los recursos de la red a través del servicio de directorio, sin importar cuál servidor ofrezca el servicio. El usuario ve el directorio de la red sin indicación de cuál servidor tiene la cuenta del usuario.
- Un servicio de directorio es una manera extremadamente formal de organizar los recursos en red. La configuración de tal servicio implica una cuidadosa planeación que involucra a todos los departamentos de la organización. Los servicios de directorio funcionan mejor cuando una organización (como un departamento de sistemas) es responsable del mantenimiento del directorio.

3.2.3. Grupos de trabajo.

- Los grupos de trabajo son conceptualmente opuestos a los servicios de directorio. Los directorios son formales y están administrados centralmente; los grupos de trabajo son informales y operados por los usuarios que comparten sus propios recursos locales.
- Después de que alguien se anexa a un grupo de trabajo, tiene acceso a todos los recursos compartidos en ese grupo. Para localizar los recursos en una red, Microsoft utiliza un servicio de explorador. En Windows NT o Windows 9x, el Entorno de Red o el Explorador de Windows puede ser utilizado para explorar la red e identificar los recursos para conectarse.
- Los grupos de trabajo hacen que el compartir recursos sea una operación muy simple, pero no organizan los servicios en ningún directorio. Tampoco facilitan la administración de los recursos compartidos de manera eficiente. Las contraseñas pueden ser utilizadas para restringir el acceso a los recursos, pero con una contraseña para cada recurso, éstas proliferan con rapidez.
- Si utilizamos Windows 2000 o Windows XP, también podemos usar los grupos de trabajo, sin tener que establecer contraseñas a los recursos. En su lugar, podemos indicar por cada recurso que usuarios pueden acceder al mismo, pero tenemos el problema que sólo podremos escoger usuarios desde nuestra lista de usuarios locales. Esto implica que si queremos acceder desde la red a un recurso compartido en una maquina XP, tenemos que conocer (o usar) el nombre de usuario y la contraseña de un usuario local de dicha maquina XP.

3.2.4. Dominios.

- Si estamos usando un grupo de trabajo, y compartimos un recurso, al acceder a la lista de usuarios que pueden acceder a dicho recurso desde la red local podemos elegirlos de una lista donde aparecen todos los usuarios **locales** de nuestro sistema. Esto quiere decir que no podemos compartir uno de nuestros recursos para un usuario que no sea **local** en nuestro sistema.
- Esto es así por que todas las cuentas de usuario son **locales** y son almacenadas en cada equipo individual. Una solución para este problema es que tengamos la opción de crear cuentas **globales**, es decir que podamos crear cuentas que no solo sean reconocidas en una maquina, sino que sean reconocidas en todas las maquinas de la red. Para hacer esto, necesitamos establecer un ordenador especial que va a ser el encargado de almacenar todas estas cuentas **globales**, mientras que las cuentas locales seguirán estando almacenadas en cada equipo local. Este ordenador pasa a ser un servidor, y nuestro grupo de trabajo se convierte en un **dominio**.

- Si queremos trabajar en un dominio, hay que indicar en todos los equipos que dejamos de trabajar en un grupo de trabajo, y queremos conectarnos a un dominio.
- Los dominios toman conceptos de los grupos de trabajo y servicios de directorio. Al igual que los grupos de trabajo, los dominios son bastante informales y pueden ser administrados utilizando una mezcla de controles locales y centrales. Los dominios pueden desarrollarse con relativa facilidad y establecerse con menos complejidad que la requerida normalmente para un directorio.
- Al igual que un directorio, un dominio organiza los recursos de diversos servidores en una estructura administrativa. Los usuarios reciben privilegios de conexión a un dominio más que a un servidor individual. Debido a que un dominio controla los recursos de varios servidores, es más fácil de administrar que una red con muchos servidores individuales.
- Los servidores, dentro del dominio, anuncian sus servicios a los usuarios. Los usuarios que se conectan en un dominio obtienen acceso a todos los recursos del dominio para el cual han recibido autorización de acceso. Pueden explorar los recursos en un dominio como lo harían en un grupo de trabajo, sin embargo, los dominios son alojados por servidores Windows NT y son más seguros que los grupos de trabajo.
- Cuando las redes se vuelven lo suficientemente amplias como para requerir varios dominios, los administradores pueden establecer relaciones de confianza (trust) entre los dominios. Estas relaciones simplifican la administración, ya que un usuario sólo requiere una cuenta en uno de los dominios. Los otros dominios que confían en el dominio de conexión del usuario pueden depender de que el dominio de conexión autentifique dicha conexión. Los dominios Windows NT Server no son lo mismo que los dominios encontrados en las redes TCP/IP.

3.3. Dominios y relaciones de confianza.

3.3.1. Dominios, tipos de servidores y sincronización.

- Esencialmente, los dominios son grupos de trabajo mejorados. El acceso a los recursos del dominio está controlado por un controlador de dominio. Al usuario se le asigna una cuenta única y una contraseña que es utilizada para controlar el acceso a todos los recursos del dominio. Los dominios también admiten el uso de grupos que permitan a los administradores asignar y cambiar los permisos de grandes cantidades de usuarios de manera más eficiente.
- Un servidor en un dominio tiene una de las siguientes tres funciones:
  - *Controlador primario del dominio (PDC, Primary Domain Controler).* Un servidor guarda la copia maestra de la base de datos de usuarios y grupos del dominio. El PDC es responsable de sincronizar la base de datos de cuentas con todos los BDC. El primer servidor en el dominio es configurado como controlador primario del dominio (PDC). Por cada dominio debe existir forzosamente un PDC, y por cada PDC que se monte, debe montarse también un dominio.
  - *Controlador de respaldo del dominio (BDC, Backup Domain Controler).* Otros servidores pueden guardar copias de respaldo de la base de datos de usuarios y grupos del dominio. Cada controlador de respaldo del dominio almacena una réplica de la base de datos contenida en el PDC, que se replica periódicamente para distribuir los cambios hechos a la

base de datos principal de éste. Si el controlador primario sufre un fallo de hardware, uno de los controladores de respaldo pasa a funcionar como si fuera el PDC (con algunas limitaciones). Cada dominio deberá tener por lo menos un BDC.

- *Servidor individual*. Los servidores pueden participar en un dominio sin ser designados como controladores primarios o de respaldo del dominio. Las computadoras que ejecutan el sistema operativo servidor (Windows NT, Windows 2000, Windows 2003) también pueden funcionar como servidores independientes o individuales, que pueden o no participar en los dominios. Estos servidores no funcionan como controladores primarios o de respaldo del dominio. Sin embargo, pueden aprovechar las bases de datos del usuario y los grupos que son mantenidos para el dominio, y se pueden asignar permisos de usuario y grupos para el servidor utilizando el Administrador de usuarios para dominio. El servidor también puede mantener su propia base de datos de usuarios como cualquier otra maquina con Windows XP Professional que exista en la red.

- Todos los cambios efectuados al directorio de la base de datos del dominio se realizan primero en el PDC, luego se distribuyen a los BDC en un proceso denominado "sincronización". Cuando un BDC solicita una actualización de base de datos, los cambios que tuvieron lugar desde la última actualización son copiados a la base de datos del BDC. Una actualización que sólo consiste en los cambios recientes se llama "sincronización parcial".
- El cambio en la base de datos del PDC tiene una capacidad limitada. Opera como un buffer circular, lo que significa que los cambios viejos serán purgados para hacer lugar a los nuevos cambios. En consecuencia, un BDC que está fuera de línea por un período largo puede haberse perdido de los cambios purgados en la base de datos. En este caso es necesario realizar una "sincronización total" en la que el BDC recibe del PDC una copia completa del directorio de la base de datos del dominio. Cuando las BDC están separadas del PDC por un vínculo WAN lento, la sincronización total es inadecuada.

3.3.2. Relaciones de confianza.

- Hay varias razones por las que una organización pudiera necesitar establecer dos o más dominios, por ejemplo:
  - Si se ponen demasiados servidores en un dominio, se reduce el desempeño.
  - Para lograr un mejor desempeño, la base de datos del dominio debe restringirse a 40 MB, limitando el número de estaciones de trabajo, usuarios y grupos que pueden ser definidos en un dominio dado.
  - Algunos departamentos prefieren manejar sus propios recursos, resulta más fácil si tienen sus propios dominios.
- Por suerte, los servidores Windows permiten establecer relaciones de confianza entre dominios. La figura anterior ilustra una relación de confianza simple entre dos dominios. Se ha configurado al dominio B para confiar en el dominio A. Entonces, si un usuario se ha conectado exitosamente en el dominio A, el dominio B asume que el usuario ha sido autentificado adecuadamente. Por ello, el dominio B acepta al usuario sin forzarlo a conectarse de manera explícita con ese

dominio. La confianza puede ser en un sentido o en ambos, es decir podemos hacer que A confié en B, que B confié en A, o bien que ambos confíen en el otro.

- Si A confía en B, y B confía en C…. ¿Quiere esto decir que A confía en C? Esto se conoce como propiedad transitiva y puede o no aplicarse en las relaciones de confianza entre dominios.:
  - En los dominios tradicionales (Windows NT) las relaciones de confianza no son transitivas.
  - En los dominios mixtos (donde existen servidores Windows 2000 o 2003 y servidores Windows NT) las relaciones de confianza no son transitivas.
  - En los dominios puros de Windows 2000 o 2003 las relaciones de confianza SI son transitivas.
- Una relación de confianza no autoriza de manera automática el acceso del usuario a los recursos en un dominio. Un dominio que confía otro, se apoya en éste para autentificar a los usuarios cuando se conectan pero el dominio que confía también debe autorizar el acceso del usuario a esos recursos.
- Imaginemos que queremos que TODOS los usuarios de la empresa cuenten con la posibilidad de acceder a cualquier recurso, sin importar en que dominio se encuentre dicho recurso. Como por cada uno de los dominios hay que establecer estas relaciones de confianza, tenemos que el numero de relaciones de confianza total será **N * (N-1)** relaciones de confianza. Este tipo de organización se conoce como **modelo de confianza total**.
- Este sistema presenta un problema derivado del alto número de relaciones de confianza que hay que crear. Para solucionar estos problemas, podemos usar el **modelo de dominio maestro**. Bajo este modelo, creamos un dominio especial (dominio maestro) que va a contener TODAS las cuentas de usuario de la empresa, de modo que ningún otro dominio tenga cuentas de usuario del dominio. Los demás dominios se limitarán a compartir sus recursos, gestionarlos, etc.
- De este modo, si nos damos cuenta, basta con que todos los dominios confíen en el dominio maestro, para que todos los usuarios puedan acceder a todos los recursos. A partir de este modelo de dominio maestro, podemos establecer otros modelos como el de doble dominio maestro (en donde hay dos dominios maestros que confían entre si), etc.
- Este tipo de organización de dominios, era la única opción posible cuando se instala Windows NT como sistema servidor, dado que las relaciones de confianza no son transitivas. Sin embargo, cuando montamos Windows 2000 o Windows 2003 como sistema operativo de red, aprovechando las propiedades transitivas de las relaciones y el uso de servidores DNS podemos simplificar bastante la organización de dominios.
- Podemos comprobar como el modelo de organización para la unión de dominios de Windows 2000 es mucho más lógico que el modelo usado por Windows NT (o por organizaciones mixtas, Windows 2000 y Windows NT). Sin embargo, para que este tipo de modelos puedan funcionar, se necesita que en los modelos de Windows 2000 se usen servidores DNS propios, cosa que no es necesaria en los modelos de Windows NT y todos estos conceptos se agrupan bajo el Directorio Activo, que es el protocolo de servicio de directorios usado por Windows 2000.

3.4. Usuarios y grupos.

- Así pues, cuando estamos trabajando en un dominio, existen dos tipos de cuentas de usuario:

    - **Locales.** Son cuentas de usuario que se crean en los equipos individuales del dominio y que son sólo visibles por el propio equipo que las crea.
    - **De Dominio.** Son cuentas de usuario que se crean en algún controlador del dominio y son visibles en todo el dominio (o árbol, o bosque).
- Cada vez que creamos una cuenta de usuario, se crea un identificador de seguridad (**Security ID. SID)**. Este SID es un número único que identifica una cuenta. El sistema no conoce a los usuarios por sus nombres, sino por sus SID. Los SID no se reutilizan nunca; cuando se borrar una cuenta, su SID se borra también con ella. Cada recurso (una carpeta, una impresora, etc.) cuenta con una **lista de control de acceso** (Access Control List, **ACL**) donde se integran los SID que tienen permiso a acceder a dicho recurso.
- En Windows Server 2003, los grupos de usuarios se dividen en dos tipos principales:
    - Grupos de seguridad.
    - Grupos de distribución.
- Los grupos de seguridad son los "auténticos" grupos de toda la vida, como los que usamos en Windows XP o Windows NT. La principal diferencia entre ellos, es que los grupos de seguridad cuentan con un SID, y los grupos de distribución no.
- En la ACL de un recurso, están almacenados los SID de los usuarios que pueden usar el recurso, y los SID de los grupos que pueden usar el recurso. Cuando un usuario accede al recurso, accede presentando su propio SID y los SID de todos los grupos a los que pertenece, de modo que posee varias posibilidades de usar el recurso.
- ¿Para que sirven entonces los grupos de distribución, que no cuentan con su propio SID? Prácticamente para nada. En realidad son útiles cuando queremos crear grupos, pero no los vamos a utilizar para conceder permisos de seguridad sobre recursos ni nada de esto, sino para cosas simples como enviarles correo electrónico a todos al mismo tiempo, etc.
- Los grupos de seguridad en Windows 2002, se dividen a su vez en cuatro grupos principales:
    - *Grupos de seguridad locales*. Son el equivalente en grupos a las cuentas de usuario locales, y solo pueden ser usados dentro de la maquina local donde se han creado, no siendo visibles fuera de la maquina local. Solo pueden contener cuentas de usuario locales de dicha maquina. Estos grupos de seguridad locales o grupos locales se almacenan en cada maquina local, y pueden contener si queremos cuentas de usuario y grupos del dominio.
    - *Grupos de seguridad locales de dominio*. Los grupos locales de dominio viven en los controladores de dominio Windows 2000 (Active Directory o Directorio Activo) y existen en un contexto diferente al de los locales que vimos anteriormente. Estos grupos locales de dominio pueden contener miembros de cualquier dominio del bosque del AD. Pueden contener usuarios de cualquier dominio del bosque, también pueden contener grupos globales y grupos universales. Estos grupos solo son validos dentro del propio dominio donde se han creado, que es por lo que se les llama grupos locales de dominio. Estos grupos suelen ser utilizados para controlar el acceso a los recursos locales del dominio.
    - *Grupos de seguridad globales*. Los grupos globales de Windows 2000, solo pueden contener cuentas de usuario locales del dominio donde se crean los grupos, y otros grupos

globales del propio dominio. No se pueden introducir en un grupo global otro grupo local o universal, ni cuentas de usuario del bosque. Estos grupos son la antitesis de los grupos locales de dominio; pueden contener únicamente cuentas del dominio local, pero son visibles en todo el bosque del Active Directory.

- *Grupos de seguridad universales*. Los grupos universales son nuevos en Windows 2000 y se pueden crear en cualquier controlador de dominio. Pueden contener miembros de cualquier dominio en el bosque y se pueden utilizar en cualquier ACL de los objetos del bosque. La afiliación a los grupos universales es infinitamente flexible y la pertenencia a uno de estos grupos es universalmente aceptada dentro del bosque. Estos grupos universales sólo funcionan en modo nativo (sin servidores Windows NT) y consumen muchos recursos, por lo que se recomienda utilizarlos tan poco como sea posible.

- Normalmente, el uso que se realiza de los grupos es el siguiente:
  - Utilizamos grupos locales para conceder privilegios y derechos de acceso a los recursos locales. Ponemos dentro de los grupos locales otros grupos del bosque y así tenemos control total sobre esos usuarios.
  - Utilizamos grupos globales para permitir que nuestros usuarios salgan fácilmente de nuestro dominio, de forma que en otros dominios se les pueda incluir en grupos locales.
  - No utilizamos grupos universales si es posible.
  - Y sobre todo, no es aconsejable realizar anidamientos de grupos (meter grupos dentro de grupos que están dentro de otros grupos….) ya que el rendimiento general del sistema bajará en gran medida, e incluso podemos llegar a desactivar el Active Directory.
- La cuenta Administrador en una máquina Windows 2000 Profesional, Windows XP, etc. extrae sus potencialidades de su pertenencia al grupo de Administradores locales. Si sacamos al Administrador de este grupo no tiene ninguna capacidad especial. Active Directory crea, automáticamente, el grupo global de Administradores del Dominio. Cuando una máquina Windows 2000 o XP se une a un dominio (o se convierte en controlador de dominio), el grupo global de Administradores del Dominio y el grupo Universal Administradores de Empresa se colocan automáticamente dentro del grupo local del dominio de Administradores. El efecto neto de este anidamiento es que un miembro de Administradores del Dominio o de Administradores de Empresa es un administrador local en cualquier maquina que pertenezca al dominio.
- Como resumen de los ámbitos y pertenencias de los grupos, podemos indicar lo siguiente:
  - **Grupos globales**: Los miembros de grupos globales pertenecen a un dominio pero tienen acceso a recursos en cualquier dominio para el que el grupo tenga permiso.
  - **Grupos locales**: Los miembros pertenecen a cualquier dominio pero los miembros sólo tienen acceso a recursos en el dominio local. Los grupos locales se usan para asignar permisos a recursos. A continuación podemos colocar los grupos globales dentro de grupos locales, de modo que a esos recursos puedan tener acceso los miembros del grupo global.
  - **Grupos universales**: Los miembros pueden pertenecer a cualquier dominio y pueden tener acceso a recursos en cualquier dominio. En Windows 2000, los grupos universales están disponibles sólo en modo nativo y no en modo mixto.

- Existen varios métodos de implementación de las cuentas de usuario en grupos:
  - **Usuario->grupo global<-permisos**. Para pocos usuarios y restricciones.
  - **Usuario->grupo local dominio<-permisos**. Poco recomendable.
  - **Usuario->grupo global->grupo local dominio<-permisos**. Bueno y complicado.
  - **Usuario->grupo global->grupo universal->grupo local dominio<-permisos**. Ídem.
  - **Usuario->grupo global->grupo local<-permisos**. Para pocos usuarios y servidores.
- Un esquema de los grupos sería el siguiente:
  - *Grupos locales*. Tienen alcance local y sirven para aplicar permisos de acceso locales respecto al bosque. Pueden incluir cuentas locales, cuentas de dominio del bosque y grupos globales del bosque.
  - *Grupos locales de dominio*. Tienen alcance de dominio y sirven para aplicar permisos de acceso al dominio respecto al bosque. Pueden incluir cuentas de dominio del bosque, grupos globales del bosque, grupos universales del bosque y grupos locales de dominio del propio dominio.
  - *Grupos globales*. Tienen alcance de bosque y sirven para agrupar las cuentas de un dominio respecto al bosque. Pueden incluir cuentas de dominio del propio dominio y grupos globales del propio dominio.
  - *Grupos universales*. Tienen alcance de bosque y sirven para agrupar las cuentas de un bosque respecto al bosque. Pueden incluir cuentas de dominio del bosque, grupos globales del bosque (principalmente) y grupos universales del bosque. Es mejor no utilizarlos, puesto que consumen muchos recursos.

3.5. Introducción al Active Directory.

- La seguridad en una red es algo imperativo, que típicamente se divide en dos partes; autentificación y autorización. Todo sistema de seguridad consta de uno o varios archivos que componen una base de datos con los nombres de los usuarios conocidos. En Windows NT se usaba un único archivo denominado SAM.
- Active Directory tiene las siguientes características:
  - *Directorio de usuarios y otros objetos de red*. Windows 2000 Server guarda la mayor parte de sus datos de usuario en un archivo denominado NTDS.DIT, diferente a SAM en algunos aspectos. En primer lugar, NTDS.DIT es una base de datos en Access modificada. En segundo lugar, NTDS.DIT almacena una variedad de información mucho mayor que la que guardaba SAM. No solo almacena usuarios, sino recursos de red de cualquier tipo. Los datos de NTDS.DIT y el programa que los gestiona conforman lo que se llama el servicio de directorio.
  - *Centralización de los directorios*. En una red con NT, Oracle, Netware y Notes, tenemos que cada usuario suma un total de cuatro cuentas de usuario diferentes. Podemos escribir esos nombres y contraseñas una sola vez en nuestro Windows 2000 Server y luego decirle a Oracle, Netware y Notes que se las pidan a la maquina Windows 2000 Server local que compruebe que efectivamente soy quien digo que soy, antes que triplicar toda esa información de seguridad Para verlo más claro: Si tenemos un ordenador central que actúa

como servidor de bases de datos, otro de servidor de correo electrónico, otro de servidor de impresión, etc., podemos tener uno que actúe de servidor de acceso, lo que podríamos llamar un servidor de autenticación.Esta capacidad de que programas distintos se comuniquen entre si, se conoce como interfaz de programación, y depende de que ambas partes se pongan de acuerdo en un "idioma común" para comunicarse. Microsoft optó por ofrecer para Active Directory una interfaz estándar en el mercado, llamada LDAP (Lighweight Directory Access Protocol. Protocolo de Acceso a Directorios Ligeros).

- *Resolución de nombres y DNS*. Existen en Internet muchos servidores DNS públicos que nos permiten conocer las direcciones IP de las páginas públicas a las que podemos querer acceder. Pero estos servidores públicos no serán capaces de darnos las direcciones IP de las páginas privadas que estén en nuestra propia red local. Tendremos que tener entonces una serie de servidores DNS privados en nuestra red local.
- *Subdivisión del control en un dominio*. Con Windows 2000 Server, el Ejército sólo tendría que crear un dominio y dividirlo según el concepto de **Unidades Organizativas**. Concretamente, resolvería el problema de esta manera:
  - Se crea un dominio llamado, por ejemplo, ARMADA.
  - Dentro de ARMADA, se crea una unidad organizativa denominada Blona, otra llamada Mdrid y una tercera llamada Svlla. Se configuran los servidores y luego se colocan dentro de su correspondiente unidad organizativa.
  - Análogamente, dentro de ARMADA se crea tres grupos de usuarios llamados Blona_Admin, Mdrid_Admin y Svlla_Admin. Se crean cuentas para sus respectivos usuarios y se ponen los administradores en sus correspondientes grupos.

  Hay que resaltar que en este punto, los Blona_Admin todavía no tienen ningún poder. Esa relación hay que crearla delegando el control de la UO (Unidad Organizativa) Blona al grupo de usuarios Blona_Admin. Veremos que las unidades organizativas constituyen una herramienta muy útil para construir grandes dominios. En otros sistemas operativos de red, como NT, tendríamos que dividir la empresa en dos dominios, y establecer relaciones de confianza entre ellos, lo que complicaría muchísimo la gestión de la red.
- *Conectividad y replicación*. Cada lugar, usualmente tendrá un controlador de dominio, (uno de esos servidores que albergan la base de datos de Active Directory). Pero esos controladores de dominio deben comunicarse entre ellos cuando algo cambia, como cuando un usuario cambia su contraseña o un administrador crea una cuenta de usuario. Es lo que se llama replicación de Active Directory. En particular, los servidores de AD de Windows 2000 comprimen los datos antes de enviarlos a través de una red lenta. Comprimir los datos implica un consumo considerable de CPU, pero merece la pena si tenemos en cuenta que la tasa de compresión de AD llega a ser de 10:1.
- *Escalabilidad.* Active Directory puede acomodar muchas más cuentas de usuario que la base de datos SAM de NT. Active Directory facilita el trabajo de creación de las cuentas, así como el mantenimiento de una red multi-dominio, sin necesidad de tener que crear complejas relaciones de seguridad, gracias a lo que se denominan bosques. La ventaja que

tienen los bosques es que dichas relaciones de confianza tienen lugar automáticamente, cosa que también ocurre con otras estructuras más pequeñas llamadas árboles.

* *Unificación del espacio de nombres*. Hay una parte de NT que identifica a los PC por su dirección IP (en caso que el PC tenga más de una tarjeta de red, tendrá una dirección IP y una dirección MAC por cada una) y otra parte que los identifica por la dirección MAC. Casi todas las empresas tienen una red interna o están conectadas a Internet. En ambos casos, la resolución de nombres se lleva a cabo siguiendo el sistema DNS (Domain Name System). Por el contrario, Microsoft ha usado durante años un sistema diferente e incompatible en sus sistemas operativos, llamado NetBIOS, que es más simple, sin puntos y con un máximo de 15 caracteres. Las redes basadas en NT que tengan software para Internet, no usan el sistema DNS para muchas cosas. Microsoft prefirió inventar sus propios servidores de nombres de alguna forma parecidos a DNS, pero empleando nombres NetBIOS; sus servidores se denominaron servidores WINS (Windows Internet Name Service, Servicio de Nombres de Internet de Windows). Cualquier empresa que quiera formar parte de Internet debe dar nombres DNS a sus maquinas. Pero si usan NT, tienen que darles nombres NetBIOS. Entonces surge el problema, ya que muchas veces los programas sólo entienden uno de los dos nombres. Windows 2000 emplea DNS para todas las búsquedas de nombres. Aunque el papel de WINS cada vez va siendo menor, todavía pasará algo de tiempo hasta que todos los sistemas dejen de usar WINS, como aún hacen los sistemas Windows 9x y NT. Tenemos que tener cuidado cuando montemos los servidores DNS. Una de las opciones que nos da Windows 2000 es la de montar un servidor DNS raíz, lo que indica que es un servidor DNS “real”, capaz de trabajar en Internet sin ayuda de ningún otro servidor.
* *Active Directory en empresas con un solo dominio*. En un sistema que este desarrollado sobre un solo dominio, o que trabaje sobre un grupo de trabajo sin dominio, AD es bastante fácil de implementar. Tendremos que instalar un servidor DNS, aunque una pequeña red se pude administrar sin preocuparse excesivamente por la configuración del DNS. Aunque en un sistema de este tipo, no se le va a sacar mucho provecho al Active Directory, si vamos a poder aprovechar las ventajas del propio Windows 2000. W2K nos ofrece cosas muy interesantes sobre NT, como el Plug and Play y la instalación centralizada de aplicaciones.
* *Active Directory en empresas con múltiples dominios*. En ambientes de este tipo, es donde Active Directory se muestra prácticamente imprescindible. W2K tiene una base de datos llamada catálogo global que sabe a qué dominio pertenece cada usuario. El catálogo global conoce a cada usuario por su nombre principal de usuario (UPN), cuyo formato es igual que el de una dirección de e-mail. Si utiliza el UPN podrá entrar desde cualquier ordenador de cualquier dominio y el catálogo global se encargará de redirigir la autorización del usuario hasta el CPD del dominio comerciales.ventas.acme.com. Podemos dividir los dominios en unidades organizativas, subdelegando el trabajo del administrador y del CPD en otros usuarios y equipos. El proceso de asignación del control de una UO a un grupo de usuarios se conoce como delegar, y W2K cuenta con un asistente para el proceso de delegación.

* *Árboles y bosques*. Otra característica interesante de W2K es que permite organizar múltiples dominios en bosques, que automatizan la generación de las relaciones de confianza. Los bosques de dominio se pueden subdividir en árboles, principalmente con el fin de facilitar la integración a DNS de su sistema de denominación de dominios. Los dominios en W2K son de tipo jerárquico, y pueden ser lo largos que se desee. W2K usa un sistema de nombres del tipo DNS, y tiene buenas razones para hacerlo: para seguir la pista a la estructura de dominios. Por defecto, uno de los controladores de dominios en acme.com es un servidor DNS. Se puede extender la estructura jerárquica de nombres tanto como se desee. W2K crea automáticamente relaciones de confianza entre acme.com, almacen.acme.com, etc. También hace todo el trabajo necesario para que los usuarios en ACME.COM se reconozcan como usuarios en los dominios hijos. Hay un grupo predefinido llamado Administración de empresas cuyos miembros son reconocidos como administradores por todo el bosque (todos los dominios) automáticamente.