

# UNIDAD 4

Páginas: 245 - 318

## Uso del sistema operativo Windows

Las versiones más extendidas actualmente son Windows 10 (W10) y Windows 11 (W11)

### Interfaz gráfica GUI

Gracias a la interfaz gráfica de usuario podemos ver distintos elementos útiles (barra de tareas, iconos del escritorio, aplicaciones predeterminadas...) nada más iniciar la sesión. Entre las dos versiones de Windows podemos ver algunos cambios de diseño, pero no de funcionalidad. En W11 se pueden aplicar plantillas para organizar las ventanas con el comando Windows+Z.

- Barra de tareas: aquí se pueden añadir las aplicaciones más usadas, personalizar los elementos que aparecen o configurar el comportamiento.
- Botón de inicio: encontramos el botón para apagar/suspender/reiniciar, las aplicaciones ancladas, la barra de búsquedas...
- Escritorio: es el área de trabajo de la pantalla (totalmente personalizable). Haciendo click derecho sobre el escritorio podemos ver las distintas acciones posibles. Se pueden añadir aplicaciones en Acceso directo para que sean más accesibles.
- Iconos del sistema: indican ciertos estado y acceso rápido a aplicaciones activas.
- Centro de actividades: acciones rápidas del sistema (conexiones red, bluetooth, accesibilidad, modo avión...)
- Otros botones: Fecha y hora. Notificaciones. Mostrar escritorio (parte derecha)

### Interfaces en modo texto (CLI): Símbolo del sistema y PowerShell

#### ❖ Símbolo del sistema

Se usa para ejecutar ciertas operaciones desde la terminal de comandos. Se puede abrir con el usuario conectado o ejecutar como administrador. El comando "help" muestra todos los comandos que se pueden usar

- cls: borra la pantalla
- color: configura los colores de primer plano y segundo plano de la consola
- date: muestra o establece la fecha
- exit: abandona el programa
- shutdown: apaga o reinicia el equipo
- time: muestra o establece la hora
- title: establece el título de la ventana
- ver: muestra la versión de Windows
- vol: muestra la etiqueta del volumen y el número de serie
- label: permite cambiar la etiqueta
- help + comando: información del comando

#### ❖ PowerShell

Es una interfaz más completa con comandos propios y otras ventajas.

#### ❖ Terminal de Windows

Desde aquí se puede abrir PowerShell, Símbolo de sistema y cualquier otra utilidad de comandos. Existen muchas combinaciones de tecla que permiten moverse por las terminales

## Introducción a la administración de Windows

- ❖ Panel de control: se pueden realizar ciertas tareas de configuración y administración del sistema, así como ajustar las propiedades de configuración del equipo.
- ❖ Configuración: Se pueden gestionar y administrar todas las opciones relativas al sistema, las cuentas, aplicaciones, dispositivos... (muchas funciones comunes con el panel de control)
- ❖ Herramientas administrativas/Windows: herramientas para los administradores del sistema.

## Variables del sistema

- Path: lista de las rutas donde el sistema buscará los ejecutables
- TEMP/TMP: ruta a los ficheros de archivos temporales
- PATHEXT: lista de las extensiones de archivos ejecutables del sistema
- ComSpec: ruta al intérprete de comandos de Windows
- USERNAME: nombre de usuario
- windir/systemroot: ruta donde se encuentra la carpeta de Windows y la unidad del sistema
- SystemDrive: unidad que contiene el sistema de Windows
- COMPUTERNAME: nombre del equipo
- ProgramFiles: ruta hacia las aplicaciones instaladas
- userprofile: acceso a la carpeta de perfil del usuario

Para ver estas variables en Símbolo de sistema se usa el comando “echo %variable%” y en PowerShell se usa el comando “echo \$env:variable”.

## Inicio y fin de sesión

Las acciones de fin de sesión y apagado se pueden ejecutar de manera gráfica o mediante comandos:

- Símbolo del sistema: shutdown → /s apaga, /p apaga sin espera, /r /t num reinicia a los num segundos, /l sale de la sesión
- PowerShell: Stop-Computer y Restart-Computer

## Gestión de archivos y directorios

El sistema de archivos de windows se estructura de manera jerárquica, todos los directorios cuelgan del directorio raíz (“\”). También se almacena en diferentes unidades identificadas por letras (“C:”).

## Explorador de archivos

Permite ver y gestionar todos los archivos y directorios. Las diferentes acciones que se pueden hacer son: Ver, Ordenar por, Agrupar por, Nuevo, Propiedades, Abrir en Terminal y Más opciones.

## Tipos de archivos

Se diferencian los tipos de archivo según su extensión, por defecto están ocultas pero se pueden mostrar desde Opciones de carpeta o Vista→Mostrar u ocultar→Extensiones de nombre de archivo.

Existen distintos tipos de extensiones:

- exe: archivos ejecutables
- bat: ficheros de script Símbolo del sistema
- ps1: fichero de script PowerShell

Las carpetas más utilizadas por el SO son:

- Users: carpetas personales de cada usuario
- Program files, archivos de programa: archivos de programas instalados
- Windows: mayoría de archivos y carpetas del SO
- System32: mayoría de programas necesarios para el funcionamiento del SO
- Temp: archivos temporales del sistema
- Logs: archivos de registro de las aplicaciones

Archivos que se almacenan en el directorio raíz:

- pagefile.sys: contiene parte del contenido de los ficheros que están en memoria RAM, para poder ir desocupándola y así poder tener más almacenamiento del real.
- swapfile.sys: contiene los elementos que acaban de salir de la memoria.
- hiberfil.sys: se usa para las opciones de hibernación de Windows, guarda información del núcleo, el estado de las aplicaciones y el estado del sistema para que se vuelva a arrancar en el mismo estado.

## Atributos

Los archivos pueden tener los siguientes atributos:

- H: Oculto
- R: Solo lectura
- S: Sistema (el archivo es del SO y solo lo puede usar este)
- A: Archivo (indica si un archivo se ha modificado)
- I: Indizado (en NTFS indica que el archivo/directorio se indexará para realizar búsquedas más rápidas)
- C: Compresión (en NTFS indica que el archivo/directorio se comprimirá automáticamente).
- E: Cifrado (archivo cifrado, se pueden conceder permisos)
- D: Directorio (indica que es un directorio)

## Trabajar con archivos y carpetas

Se puede trabajar de manera gráfica o mediante comandos.

- Comprimir: click derecho sobre el archivo/directorio y seleccionar Comprimir en un archivo ZIP (enviar a → Carpeta comprimida)
- Cifrar: Click derecho sobre el archivo y seleccionar Propiedades → Opciones avanzadas → Cifrar contenido para proteger datos. Solo el usuario que lo ha cifrado puede acceder a este archivo.

Comandos básicos:

- path: muestra la ruta de búsqueda para archivos ejecutables
- attrib: muestra los atributos del archivo

- cd/chdir: cambia de directorio
- copy: copia uno o más archivos
- del/erase: elimina uno o más archivos
- dir: muestra una lista de archivos y directorios
- md/mkdir: crea un directorio
- more: muestra la información de forma paginada por pantalla
- move: mueve archivos y directorios
- popd: cambia el directorio guardado por pushd
- pushd: guarda el directorio actual y después lo cambia
- rd/rmdir: elimina un directorio
- ren/rename: cambia el nombre de uno o más archivos
- sort: ordena la salida
- tree: muestra la estructura de directorios de una unidad o ruta
- type: muestra el contenido de un archivo de texto
- xcopy: copia archivos y árboles de directorios

## Gestión de usuarios y grupos locales

Los usuarios y grupos se pueden gestionar desde tres aplicaciones: Administración de equipo, Ejecutar lusrmgr.msc y Panel de control.

### Usuarios

Existen dos tipos de usuarios:

- Estándar: puede cambiar la configuración y archivos del propio usuario.
- Administrador: tiene todos los privilegios y control sobre el equipo. Hay que pertenecer al grupo Administradores y siempre tiene que existir uno

Desde Cuentas de usuarios se puede cambiar el nombre, cambiar el tipo de cuenta, administrar otra cuenta (añadir/eliminar usuario).

El usuario Administrador tiene los más altos privilegios en el sistema. La cuenta viene por defecto deshabilitada, pero se puede habilitar.

### Grupos

Un usuario puede pertenecer a más de un grupo, se pueden añadir más grupos al sistema desde Usuarios y grupos locales. Dentro de cada grupo podemos agregar más usuarios. Cualquier usuario que pertenezca al grupo Administradores tiene todos los privilegios.

## Permisos locales

Para modificar los permisos de un elemento, click derecho y seleccionar Propiedades → Seguridad → Editar.

Hay varios tipos de permisos posibles: Control total, Modificar, Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura y Escritura.

Seleccionando sobre Opciones avanzadas se pueden agregar usuarios o grupos con diferentes tipos de permisos. En caso de conflicto la denegación prevalece.

Si se crea una carpeta dentro de otra, los permisos se pasan de una a otra por herencia. Si queremos permisos diferentes hay que deshabilitar la herencia.

Se pueden compartir carpetas entre el sistema anfitrión y la máquina virtual desde la pestaña Dispositivos → Carpetas compartidas → Preferencias de las carpetas compartidas → Añadir nueva carpeta compartida.

## Gestión de procesos y servicios

### Procesos

Un proceso es un programa que está cargado en la memoria principal del ordenador y que se está ejecutando. Cada proceso tiene un número de PID que lo identifica.

Los procesos se pueden administrar desde el Administrador de tareas (pestaña Procesos). Aquí aparecen las aplicaciones abiertas, los procesos en segundo plano y los procesos del SO. En la pestaña Detalles se pueden ver las características de los procesos y finalizarlos. Se pueden habilitar o deshabilitar programas para que se ejecute al arrancar el sistema (desde Administrador de tarea o Configuración del sistema, Ejecutar → msconfig.exe).

### Servicios

Los servicios son procesos que pueden estar ejecutándose en segundo plano. Los servicios se pueden ver desde Configuración del sistema (Ejecutar → msconfig.exe) o desde Panel de control (Herramientas administrativas/Windows → Servicios). Un servicio se puede Iniciar, Detener, Pausar, Reanudar, Actualizar y ver las Propiedades.

Hay distintos tipos de inicio del servicio:

- Automático: se ejecuta en el inicio del sistema, puede tener la opción de Inicio retrasado (cuando el SO está totalmente iniciado) o Desencadenar inicio (cuando no hay muchos servicios ejecutándose).
- Manual: se ejecuta cuando el usuario lo inicia, puede tener la opción Desencadenar Inicio.
- Deshabilitado: no puede iniciarse hasta que no se cambie el tipo de inicio.

## Copias de seguridad

Las copias de seguridad se pueden realizar en un dispositivo externo, en una carpeta en la nube o en una carpeta local. Tanto para W10 y W11 se realizan desde Panel de Control → Historial de archivos, hay que seleccionar la ubicación donde vamos a guardar esa copia de seguridad y los directorios/archivos que queremos incluir. En Configuración avanzada se puede seleccionar la frecuencia con la que realizar las copias y el tiempo que se deseen tener las versiones almacenadas. También se puede usar la utilidad Copias de seguridad y restauración → Configurar copias de seguridad.

## Programación de tareas

Se pueden crear tareas programadas para ejecutarse en cierto momento. Desde Herramientas administrativas/Windows → Programador de tareas, se puede agregar una tarea (Acción → Crear tarea básica) asignando un nombre, el instante/frecuencia con que se va a ejecutar y elegir el comando o script que se va a ejecutar.

## Monitorización del sistema

Se puede monitorizar el funcionamiento del sistema a través del Administrador de tareas → Rendimiento y a través de este también se puede acceder al Monitor de recursos. En estas dos aplicaciones veremos información en tiempo real de forma gráfica sobre el funcionamiento del sistema. El Administrador de tareas ofrece información sobre más dispositivos y el Monitor de recursos una información más detallada.

El visor de eventos proporciona información sobre los eventos que han ocurrido en el sistema. Se encuentra en Herramientas administrativas → Visor de eventos o Ejecutar → eventvwr.exe. Se pueden diferenciar varios niveles de eventos: crítico, advertencia, detallado, error e información.

## Directivas de seguridad

Las directivas definen el comportamiento del sistema informático y sus elementos en cuestiones de seguridad.

### Directiva de equipo local

Para acceder al Editor de directivas de grupo local se accede desde Ejecutar → gpedit.msc. Desde aquí se puede configurar el equipo o el usuario. Dentro de cada configuración se encuentra lo siguiente:

- Configuración de software: sobre instalación y gestión de software
- Configuración de Windows: con los scripts de inicio y fin y la configuración de seguridad.
- Plantillas administrativas: modifican el comportamiento de componentes de Windows y del sistema.

### Directiva de seguridad local

Se puede acceder desde Ejecutar → secpol.msc. Permite definir directivas de seguridad para los equipos de un dominio. Es posible definir directivas de seguridad y cambiar aspectos como los siguientes:

- Directivas de cuenta
- Directivas locales
- Firewall de Windows con seguridad avanzada
- Directivas de administrador de listas de redes
- Directivas de clave pública
- Directivas de restricción de software
- Directivas de control de aplicaciones
- Directivas de seguridad IP en el equipo local
- Configuración de directivas de auditoría avanzada

### Directiva de grupo

Dentro de las directivas de grupo están las de grupo local (LGPO) y las de grupo de dominio (GPO). Para acceder Ejecutar → gpedit.msc

El LGPO se utiliza para configurar el sistema local. La consola de administración de políticas de grupo (gpmc.msc) se utiliza para administrar servidores.

## Registro de Windows

Es una base de datos formada por una serie de archivos donde se almacena información sobre el sistema, el SO, los programas instalados y cualquier dato necesario para la configuración del equipo. Cada vez que se modifica cualquier elemento del sistema, se modifica el Registro.

Los archivos del Registro se encuentran en la carpeta %SystemRoot%\System32\config y para cada usuario en %UserProfile%, dentro del fichero oculto NTUSER.DAT

Se puede acceder buscando Editor de Registro en las Herramientas administrativas/Windows o desde Ejecutar → regedit. Esta aplicación hace cambios en el dispositivo.

Para realizar una copia de seguridad del Registro, seleccionar Archivo → Exportar adjudicar la ruta y el nombre del fichero (tipo .reg) que se quiere asignar a la copia, se puede exportar todo el Registro o solo una rama. Para restaurar la copia se puede ir a Archivo → Importar y seleccionar el archivo (no modificar el Registro si no se está seguro de los cambios).

Para buscar información en el Registro, seleccionar Edición → Buscar y Buscar siguiente (por clave o valor)

## Introducción a los scripts de Windows

Permiten automatizar tareas en un SO para no tener que repetirlas. En Windows se pueden crear scripts desde dos aplicaciones: Símbolo del sistema con extensión .bat y PowerShell con extensión .ps1

Scripts de PowerShell (siempre arrancar como administrador)

Comandos típicos de PowerShell

- Se pueden crear alias (un comando o un conjunto a los que se les cambia el nombre para facilitar la ejecución)
- Redirecciones y tuberías: misma escritura que en Linux
- Cmdlets: combinación verbo-sustantivo (cmdlet get-help), los verbos mas usados son Get, Set, Copy, Move, New, Start, Stop, ForEach, Write, Read y entre los sustantivos más usados encontramos Host, Object, Item, Command, Computer

Existen 4 niveles de restricción:

- Restricted: no permite ejecutar scripts, modo interactivo.
- Allsigned: solo puede ejecutar scripts autenticados.
- Remotesigned: puede ejecutar scripts, solo deben estar autenticados los de procedencia remota.
- Unrestricted: se ejecuta cualquier script sin importar su origen.

Para ver el valor se puede usar el comando "Get-ExecutionPolicy" y para modificarlo "Set-ExecutionPolicy - ExecutionPolicy Unrestricted -scope LocalMachine"

Para crear un script lo primero es crear el fichero de texto donde vamos a introducir las instrucciones con el comando "notepad nombre\_script.ps1"

Los Cmdlets más usados son Write-Host "Frase" para mostrar una frase por pantalla y \$variable = Read-Host "Frase" para que el usuario introduzca datos en una variable. Las variables se pueden definir de forma implícita (\$variable) o de forma explícita (New-Variable variable), cuando se utilizan se escriben siempre con el símbolo \$. Se puede establecer el tipo de dato de la variable con "[tipo] \$variable = valor" o "\$variable = [tipo] valor". Existen

operadores matemáticos (+,-,\*,/,%), lógicos (eq, ieq, ceq, ne, lt, le, gt, ge, like, notlike, contains, notcontains, and, or, not/!) y de tipo (is, isnot)

La programación es muy parecida a java, con el uso de if, elseif, else, switch, while, do while, do until, for, foreach.

## Gestión de almacenamiento

Las unidades físicas se pueden dividir en unidades lógicas mediante las particiones. Discos dinámicos: varios discos pueden organizarse en un volumen que se comporte como una única unidad lógica. Los volúmenes pueden ser simples (una o varias particiones de un disco), distribuidos (varios discos o particiones de varios discos), seccionados (particiones del mismo tamaño de varios discos) y reflejados (varios discos con la misma información). Las letras que identifican las unidades lógicas se pueden cambiar o quitar desde la Administración de discos.

La herramienta BitLocker sirve para el cifrado de unidades (en Panel de control). Este cifrado se puede hacer al instalar el sistema o desde el Explorador de archivos seleccionando Activar BitLocker.

Los volúmenes RAID se pueden implementar mediante hardware y software. Tipos de RAID:

- RAID 0: volumen distribuido o striping, utiliza como mínimo dos discos y reparte los datos entre ambos. No tiene redundancia ni tolerancia a fallos.
- RAID 1: volumen reflejado o mirroring, utiliza dos discos físicos como mínimo y tiene redundancia (información duplicada). Tiene tolerancia a fallos.
- RAID 5: utiliza striping con paridad. Necesita como mínimo tres discos físicos.

## Integración de Linux en Windows. Subsistema de Windows para Linux