

# Administración de Windows 10

---

Este capítulo trata sobre las tareas administrativas más comunes que suelen hacerse en un equipo con Windows 10. Comenzaremos con la gestión de las cuentas de usuario, las directivas de grupo local y los derechos de usuarios. Posteriormente veremos la configuración de la red y acabaremos con la gestión del sistema mediante comandos, tanto del cmd como del PowerShell.

---



*Administración en Windows 10* by Rafael Lozano is licensed under a [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 España License](https://creativecommons.org/licenses/by-nc-sa/3.0/es/).

## Tabla de contenido

1	Introducción .....	1
1.1	Usuario administradores .....	2
1.2	Control de cuentas de usuario .....	2
1.3	Configuración.....	2
1.4	El panel de control .....	3
1.5	El símbolo del sistema .....	6
2	Administración de cuentas de usuario .....	7
2.1	Cuentas de usuario .....	7
2.1.1	Administrador .....	8
2.1.2	Usuario estándar .....	8
2.1.3	Invitado .....	9
2.2	Gestión de cuentas de usuario del equipo.....	9
2.2.1	Crear cuentas de usuario del equipo .....	9
2.2.2	Eliminar usuario .....	11
2.2.3	Actualizar las propiedades de un usuario .....	13
2.2.4	Deshabilitar una cuenta de usuario.....	14
2.3	Perfil de usuario .....	15
2.4	Grupos .....	18
2.4.1	Crear un grupo nuevo .....	19
2.4.2	Agregar miembros al grupo .....	20
2.4.3	Eliminar un grupo local .....	21
2.5	Gestión de usuarios y grupos en símbolo del sistema .....	22
2.5.1	Gestión de usuarios. Comando net user.....	22
2.5.2	Gestión de grupos de usuarios. Comando net localgroup .....	23
2.6	Gestión de usuarios en WPS.....	24
2.6.1	Crear un usuario. New-LocalUser .....	24
2.6.2	Actualizar las propiedades de un usuario. Comando Set-LocalUser .....	25
2.6.3	Mostrar usuarios. Get-LocalUser.....	26
2.6.4	Habilitar usuarios. Enable-LocalUser.....	27
2.6.5	Deshabilitar usuarios. Disable-LocalUser .....	28
2.6.6	Cambiar nombre de usuario. Rename-LocalUser .....	28
2.6.7	Eliminar usuarios. Remove-LocalUser .....	29
2.7	Gestión de grupos en WPS.....	29
2.7.1	Crear grupos. New-LocalGroup .....	29
2.7.2	Actualizar grupos. Set-LocalGroup .....	30
2.7.3	Mostrar grupos. Get-LocalGroup .....	30
2.7.4	Gestionar miembros de grupos.....	31
2.7.5	Cambiar nombre de grupo. Rename-LocalGroup .....	34
2.7.6	Eliminar grupos. Remove-LocalGroup .....	34
3	Directivas de grupo local .....	35
3.1	Contraseñas seguras .....	37

3.2	Directiva de contraseñas.....	38
3.2.1	Definir las directivas de contraseña .....	40
3.3	Directiva de bloqueo de cuentas.....	41
3.3.1	Definir las directivas de bloqueo de cuenta .....	42
3.4	Derechos de usuarios .....	43
3.5	Gestión de directivas de grupo en el símbolo del sistema .....	44
3.5.1	Comando gpresult .....	44
3.5.2	Comando gpupdate .....	45
4	Gestión de procesos y servicios .....	45
4.1	Administrador de tareas .....	46
4.1.1	Inicio de programas .....	49
4.2	Programador de tareas .....	49
4.3	Servicios .....	51
4.3.1	Iniciar o parar un servicio .....	53
4.4	Gestión de procesos en el símbolo del sistema .....	55
4.4.1	Listado de procesos. Comando tasklist.....	55
4.4.2	Terminar un proceso. Comando taskkill.....	56
4.4.3	Tareas programadas. Comando schtasks .....	56
4.4.4	schtasks create .....	57
4.4.5	Apagado y reinicio del sistema. Comando shutdown .....	63
4.5	Gestión de servicios en el símbolo del sistema.....	64
4.5.1	Comando net .....	64
4.5.2	Comando sc .....	64
4.6	Gestión de procesos en WPS.....	65
4.6.1	Listar los procesos. Comando Get-Process .....	65
4.6.2	Parar un proceso. Comando Stop-Process .....	67
4.6.3	Comenzar un proceso. Comandos Start-Process.....	69
4.7	Gestión de servicios en WPS .....	71
4.7.1	Listar servicios. Comando Get-Service .....	71
4.7.2	Suspender un servicio. Comando Suspend-Service.....	73
4.7.3	Reanudar un servicio suspendido. Comando Resume-Service .....	75
4.7.4	Parar un servicio. Comando Stop-Service.....	75
4.7.5	Iniciar un servicio. Comando Start-Service .....	76
4.7.6	Reiniciar un servicio. Comando Restart-Service .....	78
4.7.7	Gestionar un servicio. Comando Set-Service.....	79
5	Configuración de la red.....	80
5.1	Red e Internet.....	80
5.2	El centro de redes y recursos compartidos .....	82
5.2.1	Ubicación de red .....	83
5.3	Configuración parámetros IP .....	83
5.4	Nombre de equipo y grupo de trabajo .....	85
5.5	Resolución de nombres .....	87
5.5.1	NetBIOS .....	87
5.5.2	DNS 89	
5.6	Gestión de la red en el símbolo del sistema.....	90
5.6.1	Información de la conexión de red. Comando ipconfig .....	90

5.6.2	Información de la conexión de red física. Comando getmac .....	92
5.6.3	Información de las conexiones y rutas de red. Comando netstat .....	92
5.6.4	Comprobación de conexión de red. Comando tracert.....	94
5.6.5	Comprobación de conectividad con un equipo. Comando ping .....	95
5.6.6	Comprobación de ruta. Comando pathping .....	96
5.6.7	Resolución de nombres. Comando nslookup .....	97
5.6.8	Caché ARP. Comando arp.....	99
5.6.9	Tabla de enrutamiento. Comando route .....	100
5.6.10	Configuración de red. Utilidad netsh.....	100
5.7	Gestión de la red en WPS .....	102
5.7.1	Ver las propiedades de los adaptadores de red. Función Get-NetAdapter .....	102
5.7.2	Desactivar un adaptador de red. Comando Disable-NetAdapter .....	103
5.7.3	Activar un adaptador de red. Función Enable-NetAdapter .....	103
5.7.4	Reiniciar un adaptador de red. Función Restart-NetAdapter .....	104
5.7.5	Ver la configuración IP. Comandos Get-NetIPConfiguration, Get-NetIPInterface y Get-NetIPAddress.....	105
5.7.6	Asignar propiedades a una interfaz de red. Comando Set-NetIPInterface .....	107
5.7.7	Asignar direcciones IP a interfaces. Comando New-NetIPAddress .....	108
5.7.8	Eliminar direcciones IP de interfaces. Comando Remove-NetIPAddress.....	109
5.7.9	Mostrar los servidores DNS. Comando Get-DnsClientServerAddress .....	110
5.7.10	Asignar un servidor DNS. Comando Set-DnsClientServerAddress .....	111
5.7.11	Comprobar la conectividad de red. Comando Test-NetConnection .....	112
5.7.12	Resolución de nombres. Comando Resolve-DnsName .....	114
5.7.13	Mostrar la tabla de enrutamiento. Comando Get-NetRoute.....	116
5.7.14	Crear una ruta. Comando New-NetRoute .....	118
5.7.15	Eliminar una ruta. Comando Remove-NetRoute .....	119
6	Bibliografía .....	124

# Administración de Windows 10

## 1 Introducción

La administración de Windows es una tarea muy amplia para centralizarla en una sola herramienta o utilidad. Prácticamente, cualquier tarea administrativa puede realizarse desde alguno de los sitios siguientes:

- ✓ *Configuración*, con Windows 10 se están centralizando tareas administrativas en un nuevo componente llamado *Configuración* al cual se accede directamente desde el botón *Inicio*. En la última versión, *aniversary update*, incorpora una potente herramienta de búsqueda para encontrar las consolas de administración que incorpora.
- ✓ *Panel de control*, desde el que podremos fácilmente administrar dispositivos, configurar el entorno, solucionar problemas, etc. Aquí el administrador del sistema puede encontrar las herramientas que le permitirán mantener en todo momento su sistema operativo funcionando a pleno rendimiento; además de poder solucionar la mayoría de problemas.
- ✓ *Administración de equipos*.- Nos da acceso a la consola de administración de Windows. Aquí encontraremos herramientas para gestionar usuarios, carpetas compartidas, administración de discos, etc.
- ✓ *Herramientas Administrativas*.- Es un grupo de programas del menú *Inicio* con un conjunto de aplicaciones para tareas de administración del equipo y servicios.
- ✓ *Símbolo del sistema*.- Es el intérprete de comandos tradicional de Windows el cuál incluye un conjunto de comandos específicos de administración del sistema operativo.

- ✓ *Windows PowerShell*.- Es un intérprete de comandos muy potente y versátil que incluye un completo lenguaje de scripting para automatización de tareas administrativas.

## 1.1 Usuario administradores

Las tareas de administración en Windows 10 no puede hacerlas cualquier usuario. Muchas operaciones administrativas son muy delicadas y por tanto solamente aquellos usuarios con el perfil de administrador pueden hacerla. Como mínimo existen dos usuarios con este perfil:

- ✓ *Administrador*.- Esta cuenta de usuario está por defecto deshabilitada. Puede habilitarse y abrir sesión con ella para realizar tareas administrativas, pero no se recomienda.
- ✓ La cuenta que se creó durante la instalación. El nombre de esta cuenta varía en cada equipo ya que se introduce al hacer la instalación.

Más adelante veremos las cuentas de usuarios y los tipos de cuenta que existen, pero por ahora solamente necesitamos saber que los usuarios administradores son los únicos que pueden realizar tareas administrativas.

## 1.2 Control de cuentas de usuario

Control de cuentas de usuario (UAC) es una característica de Windows que ayuda a controlar el equipo informando cuando un programa hace un cambio que requiera permiso de nivel de administrador. UAC funciona ajustando el nivel de permiso de su cuenta de usuario. Si realiza tareas que se pueden llevar a cabo como usuario estándar (por ejemplo, leer correo electrónico, escuchar música o crear documentos), tendrá los permisos de un usuario estándar, aunque haya iniciado sesión como administrador.

Cuando se vayan a realizar cambios en el equipo que requieran permiso de nivel de administrador, UAC lo notificará. Si es administrador, hacer clic en el botón *Sí* para continuar. Si no es administrador, alguien con cuenta de administrador en el equipo tendrá que escribir su contraseña para continuar. Si da permiso, se le concederán temporalmente los derechos de un administrador para llevar a cabo la tarea y posteriormente sus permisos volverán a ser los de un usuario estándar. Esto se hace de tal forma que incluso si utiliza una cuenta de administrador, no se podrán realizar cambios en el equipo sin que usted lo sepa, lo que ayuda a impedir que se instale software malintencionado (malware) y spyware, o que estos programas realicen cambios en el equipo.

## 1.3 Configuración

Windows 10 incorpora un nuevo componente desde el cual accedemos a tareas administrativas habituales en el equipo. Accedemos a él mediante el icono *Configuración* del botón *Inicio*. Algunas de estas tareas administrativas se podrán realizar directamente aquí, pero también incluyen enlaces que acceden directamente a componentes del *Panel de Control*.

Se puede utilizar *Configuración* para gestionar las cuentas de usuario, la configuración de la red, los dispositivos conectados al equipo, las actualizaciones de seguridad, etc.

Aunque poco a poco conforme Microsoft libera nuevas versiones y actualizaciones, se incluyen más tareas administrativas en este componente, todavía, en el momento de escribir este documento, la mayoría de ellas se realizan desde el panel de control.

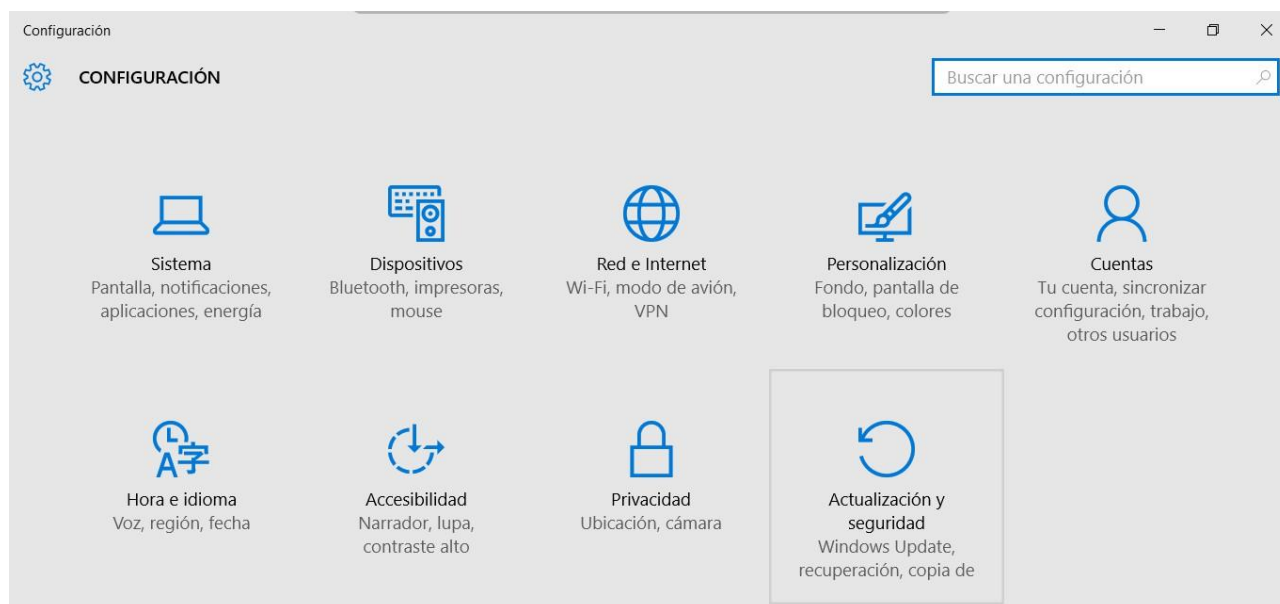


Figura 1.- Configuración

## 1.4 El panel de control

Anteriormente hemos hablado del Panel de control como el autentico centro neurálgico desde donde podemos administrar el sistema. Debido a que existen una gran cantidad de herramientas y aplicaciones para hacer la administración del sistema, estas se encuentran por defecto visualizadas agrupadas por categorías.

Podemos acceder al *Panel de control* haciendo una búsqueda en la barra de tareas. También lo podemos añadir como icono en el escritorio. Para ello seguir los siguientes pasos:

1. Clic derecho sobre el escritorio.
2. En el menú contextual que aparece hacer clic en la opción *Personalización*.
3. Hacer clic en *Temas*.
4. Hacer clic en *Configuración de icono de escritorio*.
5. Activar los iconos que se deseen ver en el escritorio, entre ellos el del *Panel de control*.

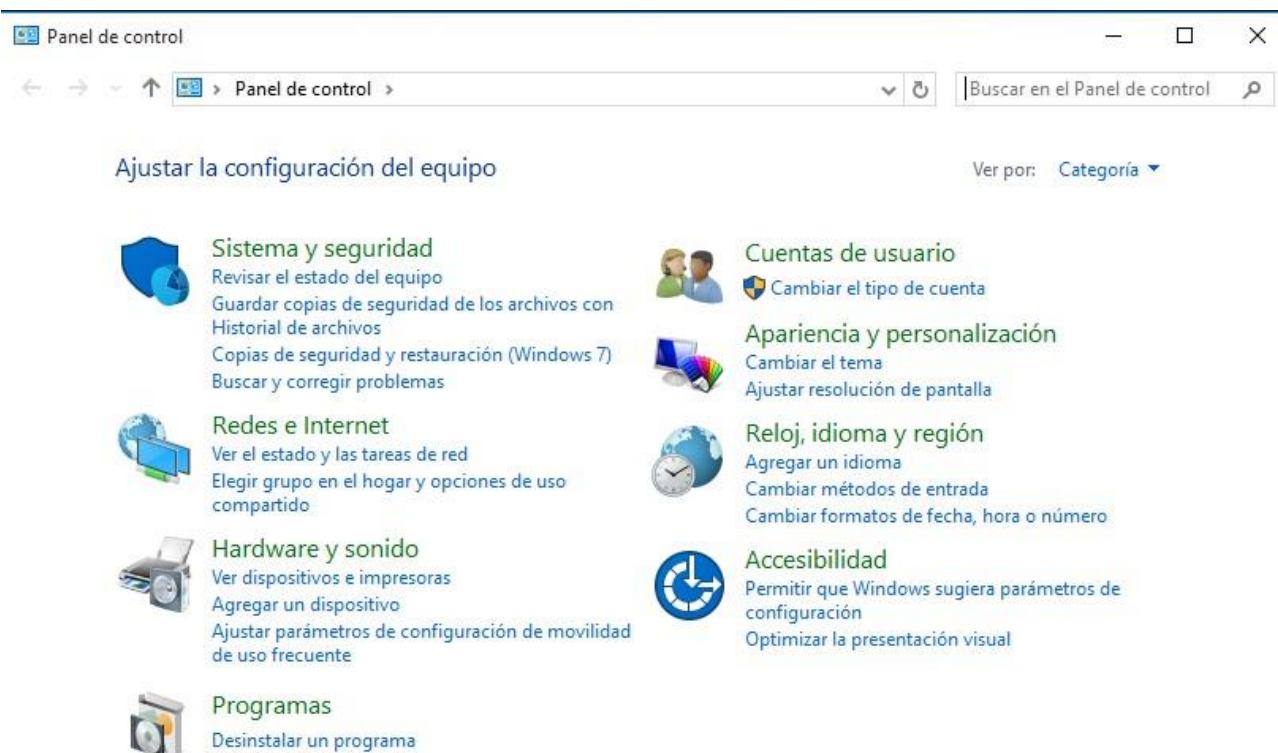


Figura 2.- Panel de Control

Se puede usar el *Panel de control* para cambiar la configuración de Windows. Esta configuración controla casi todas las cuestiones de aspecto y funcionamiento de Windows y permite configurar Windows para que se adapte a las preferencias del usuario.

Podemos ver todas las herramientas disponibles para la administración del equipo si elegimos otra forma de visualización. En la parte superior de la ventana tenemos la lista *Ver por:* donde podremos elegir *Categoría*, *Iconos grandes* e *Iconos pequeños*. El primero caso es la visualización por defecto, mientras que los dos siguientes muestran todas las herramientas y aplicaciones del *Panel de control*, cada uno con un tamaño de icono diferente.

Conforme vayamos viendo las tareas de administración y configuración del equipo iremos utilizando diferentes herramientas del panel de control. Algunas de ellas se encuentran en las *Herramientas Administrativas* que es una carpeta del *Panel de control* que contiene herramientas para los administradores del sistema y para usuarios avanzados.





Figura 3.- Panel de Control

*Herramientas Administrativas* se encuentran en la categoría *Sistema y Seguridad* del *Panel de Control*, pero también están disponibles como elemento del menú *Inicio*.

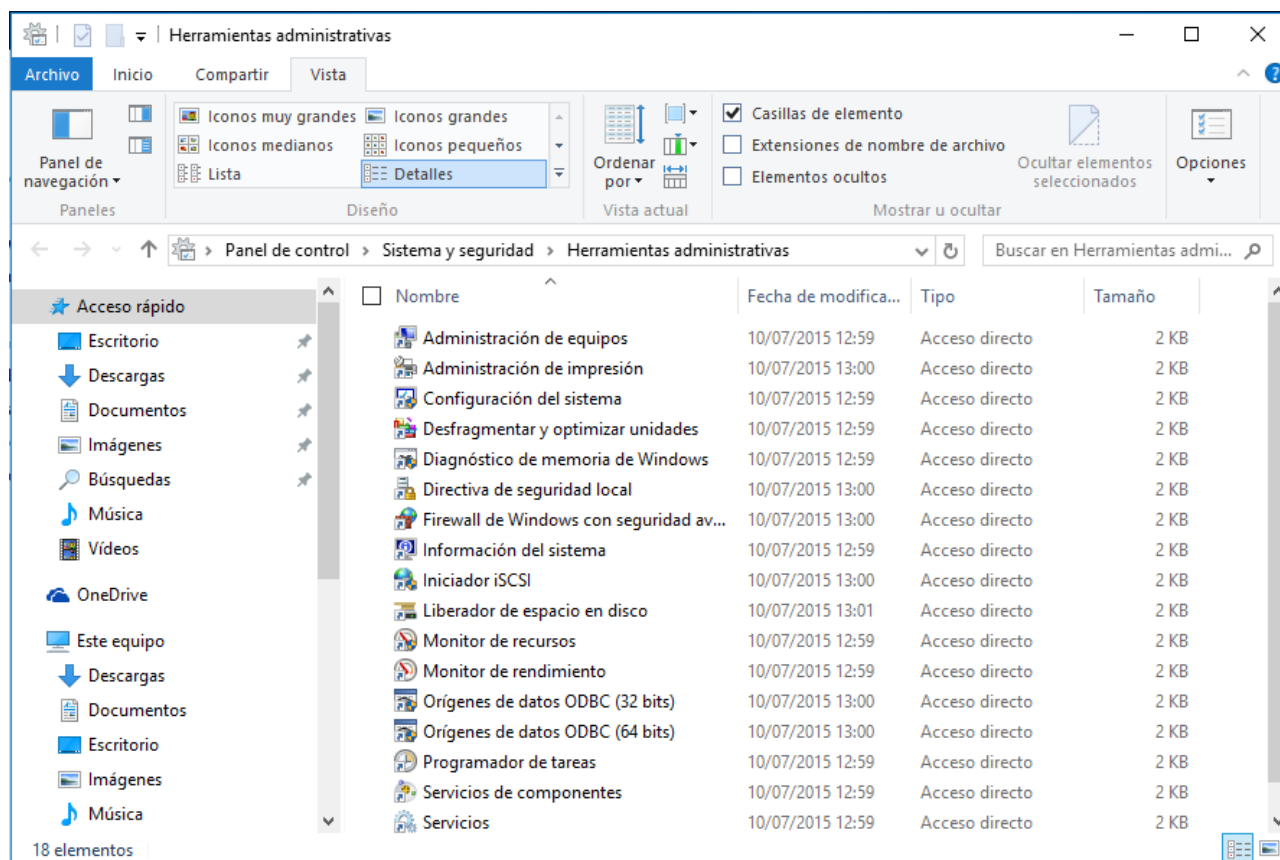


Figura 4.- Herramientas administrativas

## 1.5 El símbolo del sistema

El símbolo del sistema (`cmd.exe`) es la aplicación utilizada en sistemas basados en Windows para ejecutar comandos y otros como scripts con formato `.bat` y `.sys`.

Esta intérprete de comandos permite comunicarnos directamente con el sistema operativo y realizar una serie de tareas. El usuario escribe el comando ajustándose a la sintaxis del mismo y al pulsar la tecla Intro el intérprete lo ejecuta. La mayoría de comandos disponibles pueden ejecutarse también desde la interfaz gráfica de usuario, un método mucho más sencillo e intuitivo por lo que es la opción recomendada para la mayoría de usuarios.

Sin embargo, la línea de comandos muestra su potencia por ejemplo para ejecutar tareas repetitivas, en ocasiones donde se bloquea la interfaz gráfica o incluso para acceder a cierta información que no está disponible de ninguna otra manera. Windows también tiene otro intérprete de comandos, el PowerShell, destinada a administradores de sistemas lo que aumenta enormemente su potencial.

Podemos acceder a la interfaz en línea de comandos de Windows en modo usuario y en modo administrador, la primera limitada y la segunda más potente y con acceso a todo el equipo.

En Windows podemos acceder mediante *Inicio* → *Sistema de Windows* → *Símbolo del sistema*. También mediante la barra de búsqueda o archivos del menú de inicio introduciendo “cmd” o “símbolo del sistema”. Pulsando en ellos con el botón derecho del ratón podemos elegir el acceso en modo usuario o administrador.

La interfaz de texto del CMD la podemos personalizar en diseño, colores o fuentes accediendo a su propiedades mediante un clic secundario en el marco de la ventana.

Una buena forma de comenzar es mediante el comando `help` que nos mostrará una lista con todos los comandos disponibles. `help <nombre de comando>` nos mostrará información sobre un comando específico mientras que `<nombre de comando> /?` nos mostrará la ayuda del comando con todos sus argumentos y opciones.

## 2 Administración de cuentas de usuario

Windows es un sistema operativo multiusuario en el que varios usuarios pueden hacer uso del equipo. Para que cada usuario mantenga sus datos y personalice el equipo según sus preferencias existen las cuentas de usuario. Para facilitar la concesión de permisos y derechos a los usuarios, estos suelen estar agrupados en grupos de usuarios.

### 2.1 Cuentas de usuario

Una cuenta de usuario es una colección de información referente a un usuario del equipo que indica a Windows los archivos y carpetas a los que puede obtener acceso, los cambios que puede realizar en el equipo y las preferencias personales, como el fondo de escritorio o el protector de pantalla. Las cuentas de usuario permiten compartir un equipo con varias personas pero manteniendo sus propios archivos y configuraciones. Cada persona obtiene acceso a su propia cuenta de usuario con un nombre de usuario y una contraseña.

En versiones anteriores las cuentas de usuario se creaban en el propio equipo y podían usarse en este y en el acceso a los recursos de red compartidos por otros equipos. En esta versión de Windows disponemos también de las cuentas Microsoft, las cuales están enfocadas al acceso de los servicios en la nube.

Con una cuenta Microsoft solamente necesito abrir sesión en mi ordenador para acceder a todos los servicios que Microsoft ofrece.



Figura 5.- Servicios de Microsoft

Además puede acceder a estos servicios desde cualquier dispositivo: PC, tablet o teléfono móvil.

Si por el contrario vamos a usar cuentas de usuario local del equipo, tenemos tres tipos de cuentas. Cada tipo proporciona al usuario un nivel diferente de control sobre el equipo:

- ✓ Las cuentas estándar son para el trabajo diario con el equipo.
- ✓ Las cuentas de administrador proporcionan el máximo control sobre un equipo y sólo se deben usar cuando sea necesario.
- ✓ Las cuentas de invitado se destinan principalmente a personas que necesitan usar temporalmente un equipo.

### 2.1.1 Administrador

Una cuenta de administrador es una cuenta de usuario que permite realizar cambios que afectan a otros usuarios. Los administradores pueden cambiar la configuración de seguridad, instalar software y hardware, y obtener acceso a todos los archivos en un equipo. Los administradores también pueden realizar cambios en otras cuentas de usuario.

Cuando se instala Windows, se crea una cuenta de usuario. Esta cuenta es una cuenta de administrador que permite configurar el equipo e instalar cualquier programa que desee usar. Cuando se termine de configurar el equipo, se recomienda usar una cuenta de usuario estándar para el trabajo diario. Es más seguro usar una cuenta de usuario estándar en lugar de una cuenta de administrador porque puede evitar que se realicen cambios que afecten a todos los usuarios del equipo.

### 2.1.2 Usuario estándar

Una cuenta de usuario estándar permite usar la mayoría de capacidades del equipo. Se puede usar la mayoría de programas instalados en el equipo y cambiar las opciones de configuración que afecten a su cuenta de usuario. No obstante, una cuenta de usuario estándar no puede realizar lo siguiente:

- ✓ Instalar o desinstalar software y hardware.
- ✓ Eliminar archivos necesarios para el funcionamiento del equipo.
- ✓ Cambiar las opciones de configuración que afecten a la seguridad del equipo.

Si se usa una cuenta estándar, es posible que Windows solicite una contraseña de administrador para poder ejecutar determinadas tareas.

¿Por qué es recomendable utilizar una cuenta de usuario estándar en lugar de cuenta de administrador? La cuenta estándar puede ayudar a proteger el equipo, dado que evita que los usuarios realicen cambios que afecten a todos los que usen el equipo, como eliminar archivos que son necesarios para que el equipo funcione. Por ello, se recomienda que cada usuario tenga una cuenta estándar.

Con una cuenta estándar, se puede hacer prácticamente todo lo que se puede hacer con una cuenta de administrador, pero si se desea hacer algo que afecte a los demás usuarios del equipo, como instalar software o cambiar la configuración de seguridad, Windows pedirá que se le proporcione una contraseña para una cuenta de administrador.

### 2.1.3 Invitado

Una cuenta de invitado permite a los usuarios obtener acceso temporalmente al equipo. Quienes usen la cuenta de invitado no pueden instalar software o hardware, cambiar la configuración ni crear una contraseña. Es necesario activar la cuenta de invitado antes de que pueda usarse.

## 2.2 Gestión de cuentas de usuario del equipo

Crear, modificar, eliminar o bloquear cuentas de usuario son tareas que pueden realizarse desde el Panel de Control o desde Herramientas Administrativas. Vamos a ver con detalle estas operaciones de ambas formas.

### 2.2.1 Crear cuentas de usuario del equipo

Para crear una cuenta de usuario nueva realizar los siguientes pasos:

1. Hacer clic en el menú *Inicio*.
2. Hacer clic en *Configuración*.
3. Hacer clic en *Cuentas*.
4. Hacer clic en *Familia y otros usuarios*.
5. Hacer clic en *Agregar otra persona a este equipo*.
6. Nos pide una dirección de correo electrónico de una cuenta de Microsoft. Hacer clic en *No tengo los datos de inicio de sesión de esta persona*. Esto nos llevará a un formulario de creación de cuenta Microsoft.
7. Hacer clic en *Agregar un usuario sin cuenta Microsoft*.
8. Nos aparece un formulario para introducir el nombre del usuario y la contraseña. Lo rellenamos y hacemos clic en *Siguiente*.

# Crear una cuenta para este equipo

Si quieres usar una contraseña, elige algo que te resulte fácil de recordar, pero que sea difícil de adivinar para los demás.

¿Quién va a usar este PC?

Dale seguridad.

Figura 6.- Crear cuenta de usuario del equipo

Una vez la cuenta está creada aparecerá en la lista de usuarios. Si hacemos clic sobre ella aparecerá el menú de gestión de la cuenta de usuario. Desde aquí podemos quitarla o cambiar el tipo de cuenta.

Desde *Administración de Equipos* en las *Herramientas Administrativas* se tiene un mayor control sobre la creación de las cuentas de usuario. Para crear una cuenta de usuario en *Administración de Equipos* seguir los siguientes pasos:

1. Abrir *Herramientas Administrativas* en el *Panel de Control*.
2. Abrir *Administración de Equipos*.
3. Desplegar el árbol de la consola y hacer clic en *Usuarios y grupos*. Una vez aquí hacemos clic en la carpeta *Usuarios* y en el panel central aparecerá la lista de usuarios actuales que hay en el equipo.
4. En la carpeta *Usuarios* hacer clic con el botón derecho del ratón o desplegar *Acciones adicionales*.
5. Seleccionar *Usuario nuevo...*
6. Rellenar los datos del nuevo usuario.
7. Si activamos la casilla *El usuario tiene que cambiar su contraseña en el siguiente inicio de sesión* Windows obligará a que el usuario actualice su contraseña cuando abra sesión por primera vez.
8. Si activamos la casilla *La contraseña nunca caduca* entonces el usuario no podrá

cambiar la contraseña.

9. Si activamos la casilla *La contraseña nunca expira* significa que no se le aplicarán las directivas de contraseña referentes a vigencia máxima de la contraseña.
10. Una vez rellenados los datos hacer clic en el botón *Crear*.

Un nombre de usuario no puede tener más de 20 caracteres, componerse en su totalidad de puntos o espacios, ni contener ninguno de los siguientes caracteres: \ / " [ ] : | < > + = ; , \$ \* @

Una vez la cuenta se ha creado se puede abrir sesión con ella y comenzar a trabajar en el equipo.

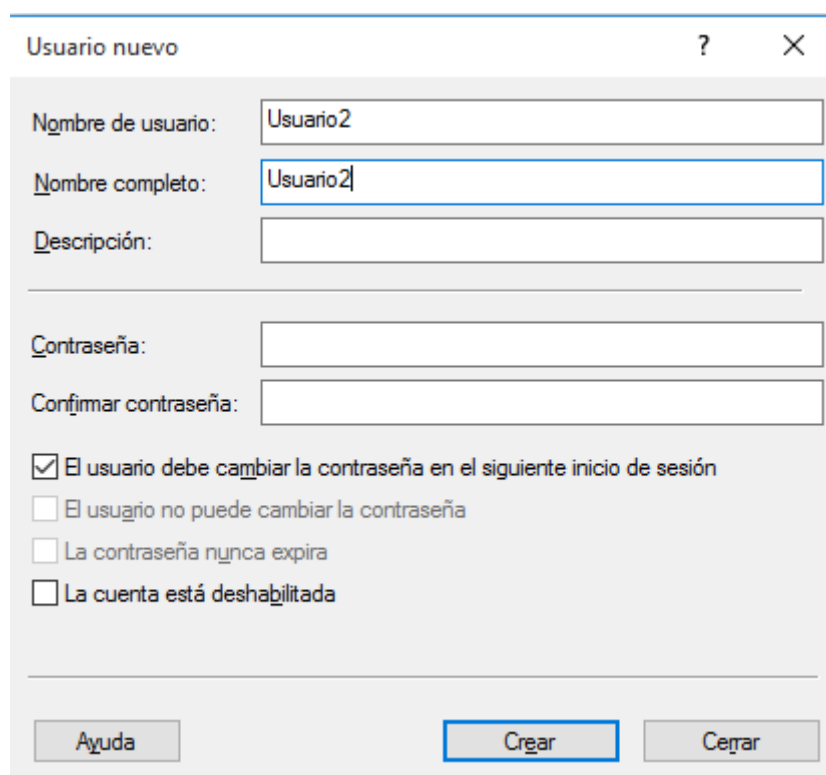


Figura 7.- Crear usuario en Administración de Equipos

### 2.2.2 Eliminar usuario

Cuando una cuenta de usuario deja de usarse es recomendable eliminarla. Para eliminar una cuenta desde el Panel de Control seguir los siguientes pasos:

1. Abrir el *Panel de Control*.
2. Hacer clic en *Cuentas de usuario*.
3. Hacer clic en *Cuentas de usuario*.
4. Hacer clic en *Administrar otra cuenta*.
5. Hacer clic sobre la cuenta de usuario que se va a modificar.

6. Hacer clic en *Eliminar la cuenta*.
7. Nos aparece un cuadro de diálogo en el que nos pide si queremos conservar los archivos del usuario.

### ¿Desea conservar los archivos de Usuario1?

Antes de eliminar la cuenta de Usuario1, Windows puede guardar automáticamente el contenido del escritorio de Usuario1 y las carpetas Documentos, Favoritos, Música, Imágenes y Vídeos en una nueva carpeta llamada "Usuario1" en el escritorio. Pero Windows no puede guardar los mensajes de correo electrónico ni otras configuraciones de Usuario1.

Eliminar archivos

Conservar archivos

Cancelar

Figura 8.- Conservar archivos de usuario eliminado

8. Hacemos clic en *Eliminar archivos* o en *Conservar archivos* según la decisión que tomemos al respecto.

Para eliminar la cuenta desde *Configuración*:

9. Hacer clic en el menú *Inicio*.
10. Hacer clic en *Configuración*.
11. Hacer clic en *Cuentas*.
12. Debajo del icono de la cuenta de usuario a borrar hacer clic en *Quitar*.
13. Nos mostrará un mensaje de advertencia de que vamos a perder todos los datos del usuario que eliminamos. Si estamos seguros hacer en el botón *Eliminar cuenta y datos* para confirmar el borrado del usuario.

¿Quieres eliminar cuenta y datos?

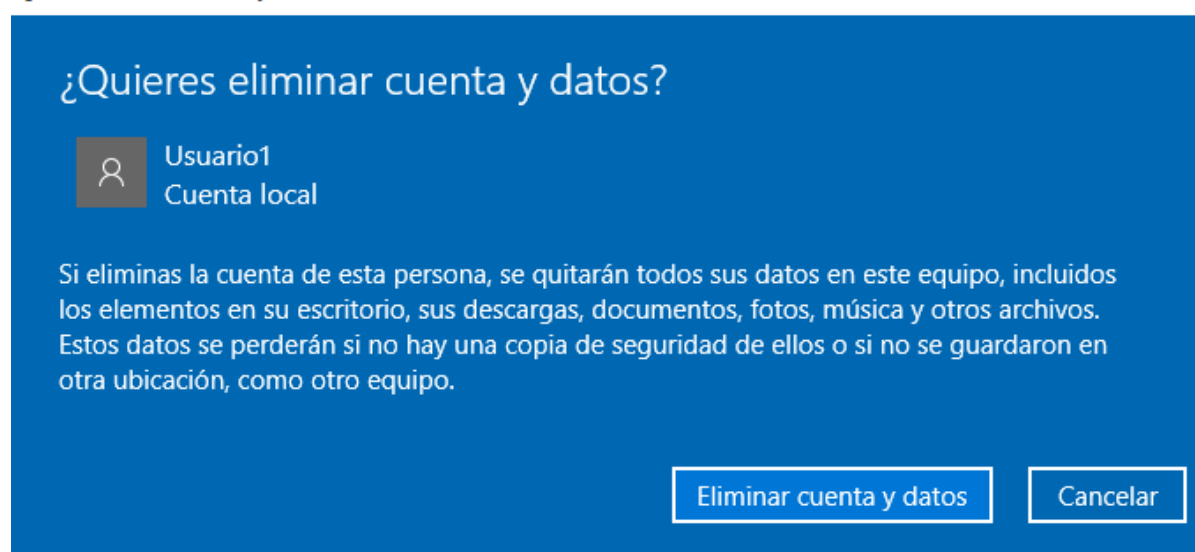


Figura 9.- Eliminación de cuenta de usuario



Para eliminar un usuario en Administrador de equipos seguir los siguientes pasos:

1. Abrir *Herramientas Administrativas* en el *Panel de Control*.
2. Abrir *Administración de Equipos*.
3. Desplegar el árbol de la consola y hacer clic en *Usuarios y grupos*. Una vez aquí hacemos clic en la carpeta usuarios y en el panel central aparecerá la lista de usuarios actuales que hay en el equipo.
4. Seleccionar el usuario que queremos dar de baja.
5. Hacer clic sobre *Acciones adicionales del usuario* en el panel derecho y seleccionar la opción *Eliminar*.
6. Hacer clic en el botón *Sí* para confirmar el borrado de la cuenta de usuario.

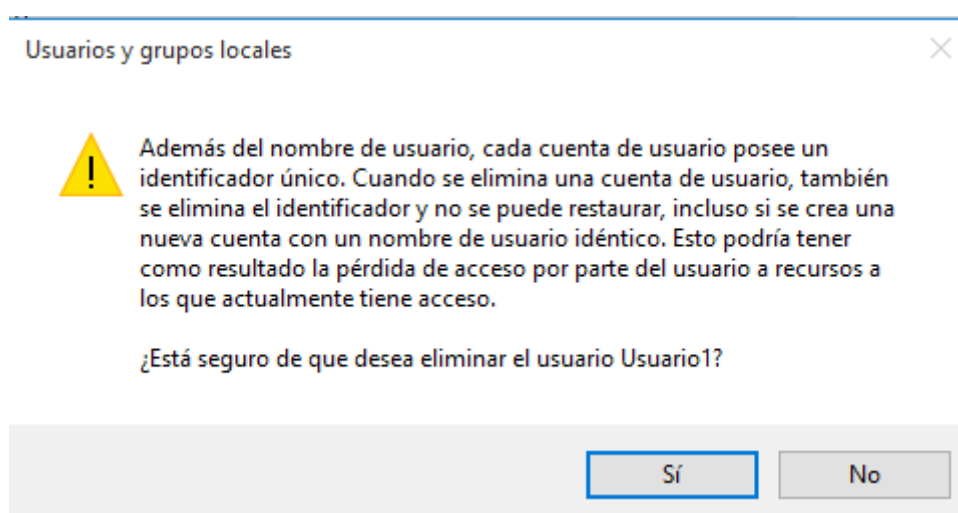


Figura 10.- Eliminación de usuario en Administración de Equipos

En la confirmación del borrado nos avisa de que cada usuario tiene un identificador único que, en el caso de borrarlo, impide volver a recuperar la información de configuración del equipo que afecta al usuario, como los permisos, derechos o pertenencias a grupos.

### 2.2.3 Actualizar las propiedades de un usuario

Desde el *Panel de control* podemos actualizar la mayoría de las propiedades de la cuenta de usuario. En *Administración de equipos* solamente es posible cambiar algunas de ellas.

Para actualizar una cuenta de usuario desde el *Panel de control* seguir los siguientes pasos:

1. Abrir el *Panel de Control*.
2. Hacer clic en *Cuentas de usuario*.
3. Hacer clic en *Cuentas de usuario*.

4. Hacer clic en *Administrar otra cuenta*.
5. Hacer clic sobre la cuenta de usuario que se va a modificar.
6. Hacer clic en *Cambiar el nombre de la cuenta* en el menú de gestión del usuario para modificar el nombre de inicio de sesión.
7. Hacer clic en *Cambiar la contraseña* para modificar la clave de acceso.
8. Hacer clic en *Cambiar el tipo de cuenta* para pasar de una cuenta estándar a administrador o viceversa.
9. Introducir los datos necesarios en cada caso y aceptar.

Para cambiar las propiedades de un usuario en *Administrador de equipos* seguir los siguientes pasos:

1. Abrir *Herramientas Administrativas* en el *Panel de Control*.
2. Abrir *Administración de Equipos*.
3. Desplegar el árbol de la consola y hacer clic en *Usuarios y grupos*. Una vez aquí hacemos clic en la carpeta usuarios y en el panel central aparecerá la lista de usuarios actuales que hay en el equipo.
4. Seleccionar el usuario que queremos actualizar.
5. Hacer clic sobre *Acciones adicionales del usuario* en el panel derecho y seleccionar la opción *Establecer la contraseña...* para poner una nueva contraseña.
6. Hacer clic sobre *Acciones adicionales del usuario* en el panel derecho y seleccionar la opción *Propiedades* para editar sus propiedades.
7. Introducir los datos necesarios en cada caso y aceptar.

#### 2.2.4 Deshabilitar una cuenta de usuario

Si se desea que una cuenta de usuario no esté disponible, se puede deshabilitar. Una cuenta deshabilitada se puede volver a habilitar más adelante. Deshabilitar una cuenta no es lo mismo que eliminarla. Cuando se elimina una cuenta, no se puede restaurar. Para deshabilitar una cuenta de usuario seguir los siguientes pasos:

1. Abrir *Herramientas Administrativas* en el *Panel de Control*.
2. Abrir *Administración de Equipos*.
3. Desplegar el árbol de la consola y hacer clic en *Usuarios y grupos*. Una vez aquí hacemos clic en la carpeta usuarios.
4. Seleccionar el usuario que queremos bloquear.
5. Hacer clic sobre *Acciones adicionales del usuario* en el panel derecho y seleccionar la opción *Propiedades* para editar sus propiedades.

6. Activar la casilla *La cuenta está deshabilitada*.
7. Hacer clic en *Aceptar*.

Mientras la cuenta esté deshabilitada el usuario no puede abrir sesión. Se tienen que repetir los mismos pasos para habilitarla, pero en esta ocasión hay que desactivar la casilla *La cuenta está deshabilitada*.

## 2.3 Perfil de usuario

El perfil de usuario es toda la información relativa a una cuenta de usuario. Esto incluye sus datos, vídeos, música, opciones de configuración y personalización del equipo, favoritos, etc. Contiene la configuración para fondos de escritorio, protectores de pantalla, preferencias de puntero, configuración de sonido y otras características. Los perfiles de usuario permiten que se usen sus preferencias personales siempre que inicie sesión en Windows.

Un perfil de usuario no es lo mismo que una cuenta de usuario, que se usa para iniciar sesión en Windows. Cada cuenta de usuario tiene por lo menos un perfil de usuario asociado.

Los perfiles de usuario se almacenan por defecto en la carpeta `C:\Usuarios` donde habrá una carpeta por cada usuario con su mismo nombre. Este es el contenido de un perfil de usuario.













Nombre	Fecha de modifica...	Tipo
 Búsquedas	05/08/2016 18:04	Carpeta de archivos
 Contactos	14/07/2016 18:50	Carpeta de archivos
 Descargas	04/08/2016 13:44	Carpeta de archivos
 Documentos	05/08/2016 18:36	Carpeta de archivos
 Escritorio	04/08/2016 13:43	Carpeta de archivos
 Favoritos	14/07/2016 18:50	Carpeta de archivos
 Imágenes	04/08/2016 13:44	Carpeta de archivos
 Juegos guardados	14/07/2016 18:50	Carpeta de archivos
 Música	04/08/2016 13:45	Carpeta de archivos
 OneDrive	14/07/2016 18:51	Carpeta de archivos
 Vídeos	04/08/2016 13:45	Carpeta de archivos
 Vínculos	05/08/2016 18:04	Carpeta de archivos

Figura 11.- Perfil de usuario

Como se puede observar aquí se guardan también los archivos del usuario que están organizados en las diferentes bibliotecas, junto con los datos de configuración y personalización del entorno del usuario.

Como se puede observar el perfil de usuario se almacena en la misma partición que el sistema operativo. Esto significa que si un día el sistema operativo queda inutilizado, y hay

que formatear, los datos de los usuarios corren riesgo de perderse, por lo que parece bastante lógico mantener los perfiles de usuario en una partición aparte.

Existe la posibilidad de cambiar la ubicación de cada carpeta. Cada usuario podría editar las propiedades de una carpeta en particular, como *Mis documentos* o *Mis vídeos* y cambiarla por otra. Para ello seguir los siguientes pasos:

1. Abrir el *Explorador de Windows*.
2. Navegar hasta la carpeta que almacena el perfil de usuario.
3. Hacer clic con el botón derecho del ratón sobre la carpeta a la que vamos a cambiar su ubicación.
4. Hacer clic en la pestaña *Ubicación*.
5. Hacer clic en el botón *Mover...* y navegar hasta la nueva carpeta.
6. Hacer clic en *Aceptar*. Los archivos que se encuentran actualmente en la carpeta anterior se mueven a la nueva carpeta.

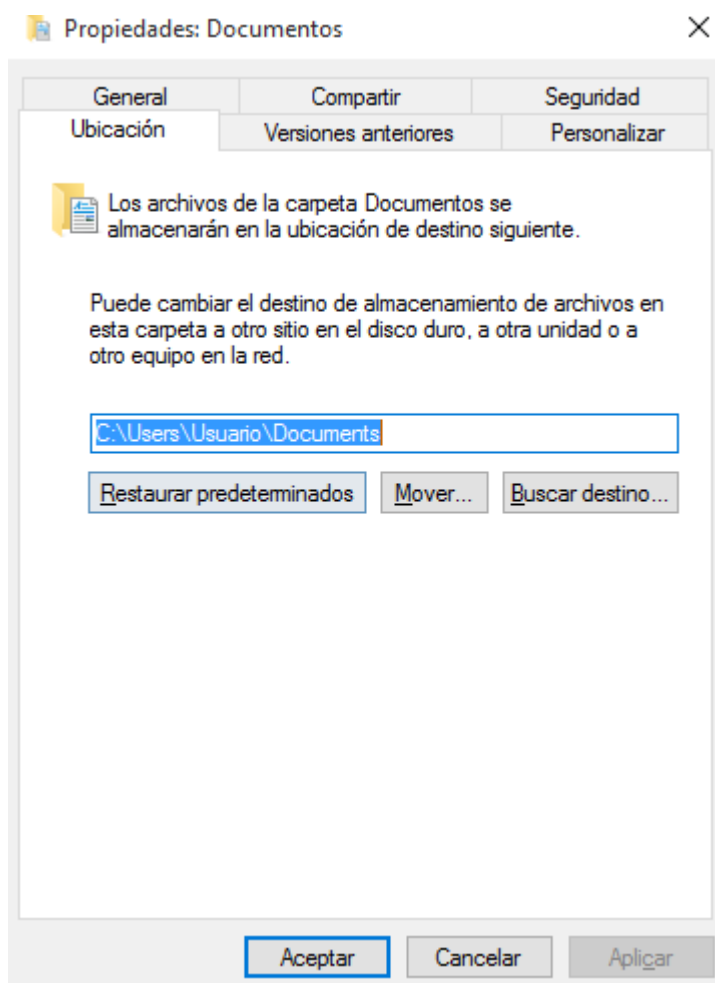


Figura 12.- Cambiar la ubicación del Mis documentos

Aunque tal vez resulte más conveniente cambiar la ubicación del perfil de un usuario

completo editando sus propiedades en el *Administrador de equipos*. Para ello seguir los siguientes pasos:

1. Abrir el *Explorador de Windows*.
2. Copiar la carpeta `C:\Usuarios\login` con el perfil actual del usuario con cuenta `login` en la nueva ubicación, por ejemplo `D:\Usuarios`. Sustituir `login` por el nombre de la cuenta de usuario. Debemos tener preparada esta nueva ubicación con antelación. Supuestamente será otra partición del disco duro diferente a la partición de Windows y con sistema de archivos NTFS.
3. Abrimos el editor de registro escribiendo `regedit` en el cuadro de búsqueda de la barra de tareas y nos vamos a la clave `HKEY_LOCAL_MACHINE → SOFTWARE → MICROSOFT → Windows NT → CurrentVersion → ProfileList`.
4. Dentro de `ProfileList` veremos una serie de carpetas con unas numeraciones muy largas. Son identificadores de usuario. Debemos buscar la que pertenece al usuario al que vamos a cambiar la ubicación del perfil. Se reconoce fácilmente porque dentro de la carpeta existe una entrada denominada `ProfileImagePath` con el valor `C:\Users\login`.

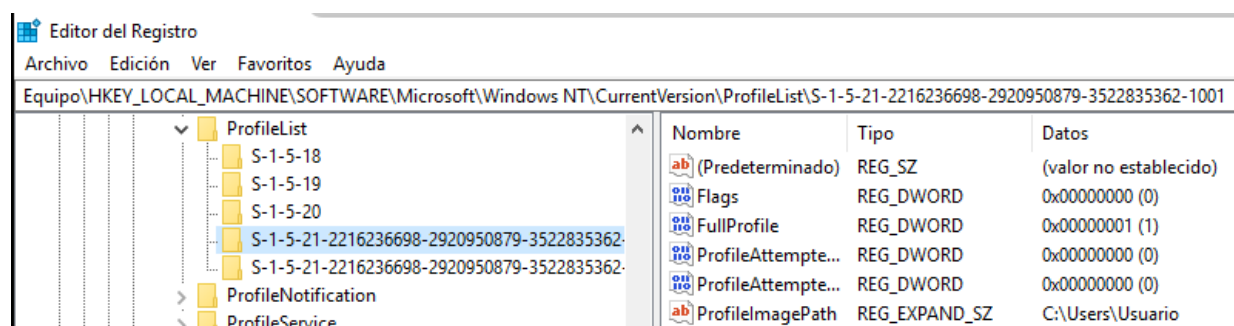


Figura 13.- Editor de registro. Perfil de usuario

5. Cambiamos el valor de la entrada `ProfileImagePath` por su valor actual al de la nueva ubicación. Por ejemplo, si lo vamos a mover a la unidad D: el perfil del usuario `Usuario` debemos establecer el valor `D:\Usuarios\Usuario`. Para cambiar cada entrada hay que hacer doble clic sobre ella y rellenar el campo *Información del valor*.
6. Cerrar el registro. Cuando el nuevo usuario abra sesión tendrá su perfil colocado en otra unidad.

Sin embargo, es posible que si el equipo va a ser utilizado por muchos usuarios y la información de sus perfiles ocupa mucho espacio, tal vez es preferible que todos los usuarios tengan sus perfiles en una carpeta diferente a `C:\Usuarios` en una partición diferente. Para ello seguir los siguientes pasos:

1. Abrir el *Explorador de Windows*.
2. La carpeta que almacena los perfiles de usuario tiene subcarpetas ocultas que deberemos visualizar. Para mostrar carpetas ocultas hacemos clic en el menú *Vista* y activamos la casilla *Elementos ocultos*.

3. Copiamos la carpeta C:\Usuarios\Default en la nueva ubicación, por ejemplo D:\Usuarios. Debemos tener preparada esta nueva ubicación con antelación. Supuestamente será otra partición del disco duro diferente a la partición de Windows y con sistema de archivos NTFS.
4. Hacemos lo mismo con la carpeta C:\Usuarios\Acceso Público.
5. Abrimos el editor de registro escribiendo regedit en el cuadro de búsqueda de la barra de tareas y nos vamos a la clave HKEY\_LOCAL\_MACHINE → SOFTWARE → MICROSOFT → Windows NT → CurrentVersion → ProfileList.
6. Cambiamos el valor de las entradas Default, ProfilesDirectory y Public por las nuevas ubicaciones. Para cambiar cada entrada hay que hacer doble clic sobre ella y rellenar el campo *Información del valor*.

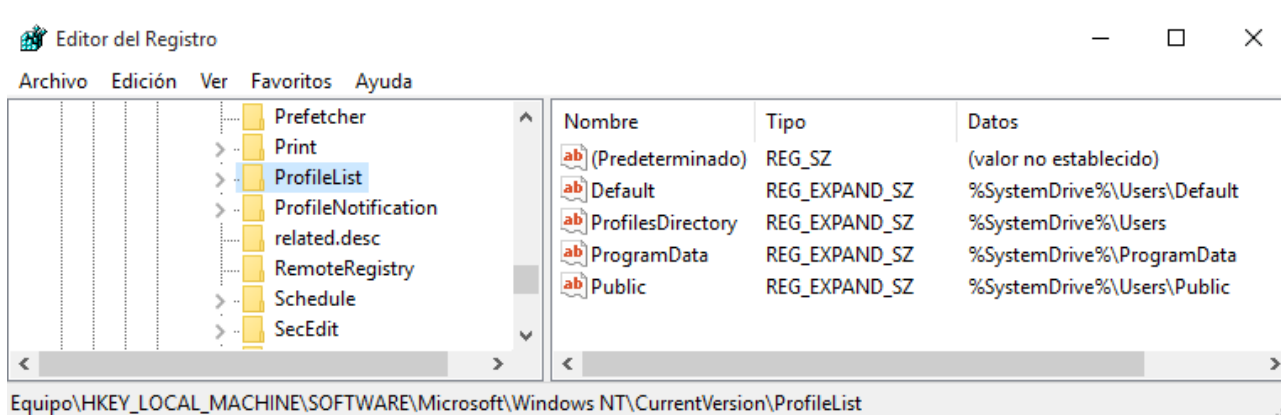


Figura 14.- Propiedades de perfil de usuario en el editor de registro

Por defecto el valor de las claves anteriores que hacen referencia a los perfiles de registro comienzan por %SystemDrive% que es una variable de entorno cuyo valor es C:, es decir, la partición de Windows. Para cada entrada de registro hay que establecer los siguientes valores:

Clave	Valor antiguo	Nuevo valor
Default	%SystemDrive%\Users\Default	D:\Usuarios\Default
ProfilesDirectory	%SystemDrive%\Users	D:\Usuarios\
Public	%SystemDrive%\Users\Public	D:\Usuarios\Public

A partir de ahora cuando creamos un nuevo usuario su perfil se creará en la nueva ubicación. Para los usuarios que ya existieran previamente siguen conservando su perfil en el lugar que estaba.

## 2.4 Grupos

Un grupo es un conjunto de cuentas de usuario y/o grupos a los que se les realiza un mismo tratamiento en la gestión de los permisos, es decir, se les concede o deniega permiso sobre un archivo o carpeta. La agrupación de varios usuarios en un grupo tiene como objetivo facilitar la administración de los permisos a los usuarios. Si se crea una carpeta

compartida a la que tienen que acceder varios usuarios, en lugar de dar permisos individualmente a cada usuario, se agrupan estos en un grupo y posteriormente se concede el permiso al grupo sobre la carpeta. Cualquier usuario que pertenezca al grupo tiene el permiso concedido al grupo. Se dice que un usuario es miembro de un grupo cuando esta asignado al grupo. Un usuario puede pertenecer a varios grupos y un grupo puede tener varios miembros.

La gestión de grupos incluye la creación del grupo, eliminación y asignación de miembros. Estas tareas se realizan desde *Administrador de Equipos* → *Usuarios locales y grupos* → *Grupos*. Desde aquí se puede hacer:

#### 2.4.1 Crear un grupo nuevo

Para crear un nuevo grupo seguiremos los siguientes pasos:

1. Abrir *Administración de equipos*.
2. En el árbol de la consola, desplegar *Administración del equipo* → *Herramientas del sistema* → , *Usuarios locales y grupos* → *Grupos*.
3. Hacer clic en *Acción* → *Grupo nuevo*.
4. En *Nombre de grupo*, escribir un nombre para el nuevo grupo.
5. En *Descripción*, escribir la descripción del nuevo grupo.
6. Hacer clic en *Crear* y, después, en *Cerrar*.

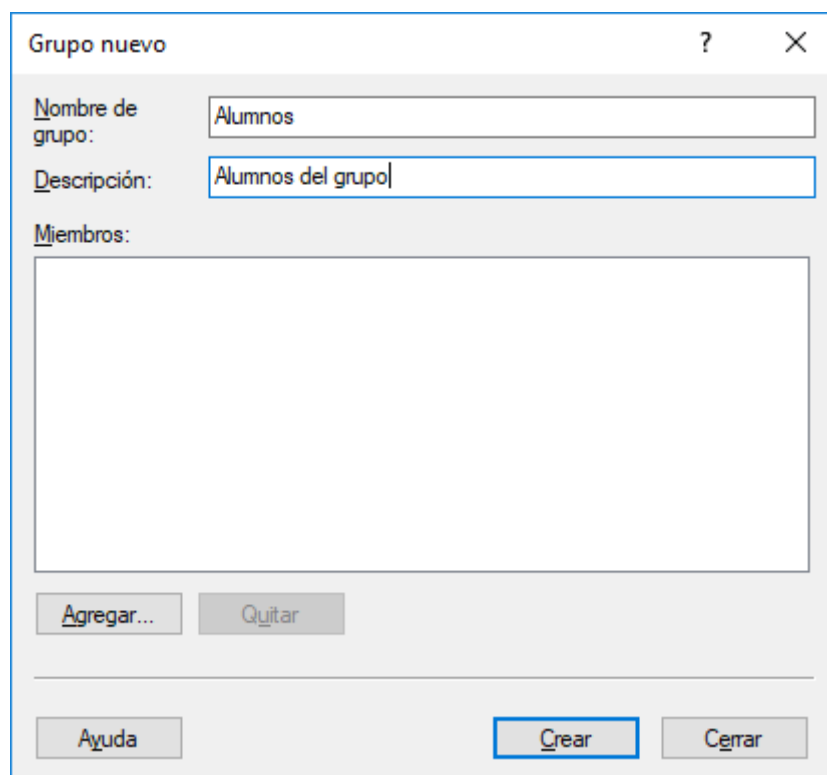


Figura 15.- Creación de un grupo nuevo

El nombre de un grupo no puede coincidir con ningún otro nombre de grupo o de usuario del equipo que se está administrando. Puede contener hasta 256 caracteres, en mayúsculas o minúsculas, excepto " / \ [ ] : ; | = , + \$ < > . Un nombre de grupo no puede contener sólo puntos (.) o espacios en blanco.

### 2.4.2 Agregar miembros al grupo

Durante la creación del grupo disponíamos del botón *Agregar...* para añadir miembros al grupo. El proceso para agregar miembros al grupo es similar cuando se edita el grupo que cuando se crea nuevo. Para ello seguimos los siguientes pasos

1. Abrir Administración de equipos.
2. En el árbol de la consola, desplegar *Administración del equipo* → *Herramientas del sistema* → *Usuarios locales y grupos* → *Grupos*.
3. Hacer clic con el botón derecho del ratón en el grupo al que queremos agregar miembros, y seleccionar *Agregar a grupo...*
4. Para indicar los miembros del grupo se hace clic en el botón *Agregar...* y aparecerá un cuadro de diálogo para introducir los usuarios que pertenecen al grupo en el campo *Nombre*. La nomenclatura a utilizar para cada uno de ellos es `HOSTNAME\USUARIO` que habrá que escribir en el cuadro de texto inferior. Después, hacer clic en *Aceptar*. Podemos validar los nombres de los usuarios o grupos que vamos a agregar haciendo clic en *Comprobar nombres*.
5. Si no sabemos con exactitud el nombre podemos hacer clic en *Opciones avanzadas* para abrir el cuadro de diálogo *Seleccionar usuarios*. Una vez aquí podemos hacer clic en el botón *Buscar ahora* para que muestre la lista de usuarios y grupos. Seleccionamos los que necesitemos y hacemos clic en *Aceptar*.



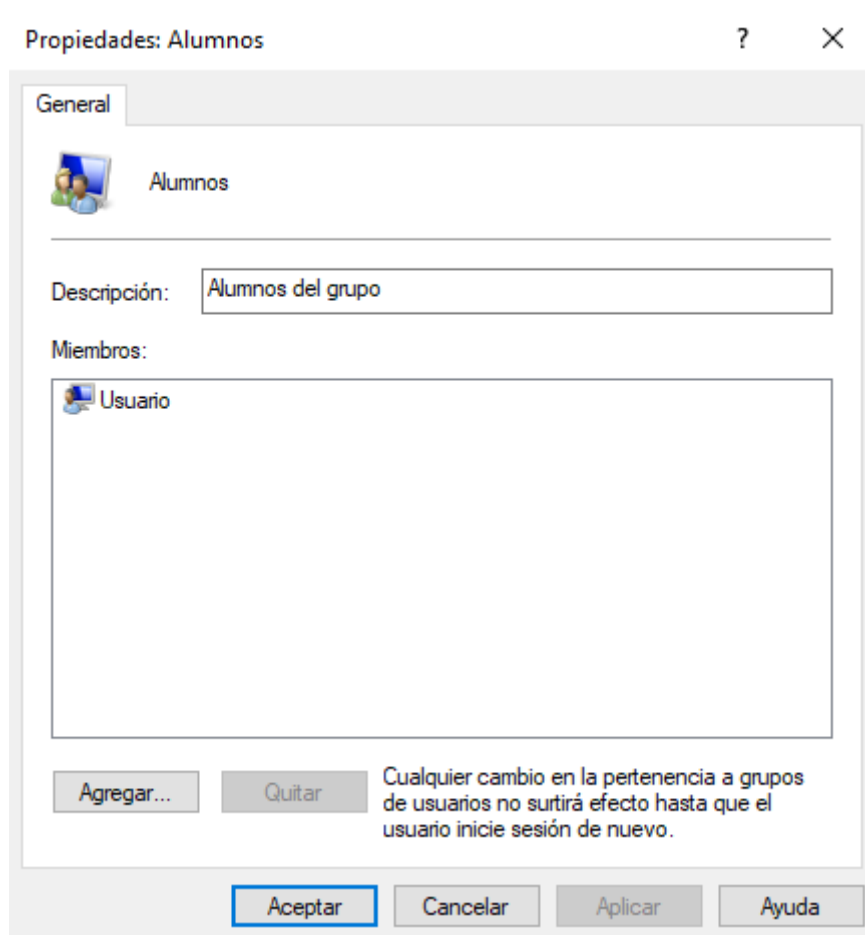


Figura 16.- Miembros del grupo

También se puede introducir una lista de nombres de usuarios y grupos separados por punto y coma. Haciendo clic en el botón *Comprobar nombres* buscaría en el equipo para verificar que los nombres introducidos son correctos.

Para quitar un usuario de un grupo local, seleccionamos el usuario en *Miembros* y, a continuación, hacemos clic en *Quitar*.

Un usuario que pertenece a un grupo tiene todos los derechos y permisos concedidos a ese grupo. Si un usuario es miembro de varios grupos, tiene todos los derechos y permisos concedidos a cada grupo al que pertenece.

No debemos agregar un usuario nuevo al grupo Administradores a menos que el usuario vaya a realizar únicamente tareas administrativas.

También se pueden introducir como miembros del grupo a usuarios individuales. Desde la ventana de propiedades del usuario se pincha en la pestaña *Miembro de* y se accede a la lista de grupos a los que pertenece el usuario. Haciendo click en el botón *Agregar* se pueden añadir nuevos grupos del usuario.

### 2.4.3 Eliminar un grupo local

Cuando ya no se necesita un grupo se puede eliminar. Seguiremos el siguiente proceso:

1. Abrir Administración de equipos.
2. En el árbol de la consola, desplegar *Administración del equipo* → *Herramientas del sistema* → *Usuarios locales y grupos* → *Grupos*.
3. Hacer clic con el botón derecho del ratón en el grupo al que queremos agregar miembros, y seleccionar *Eliminar*.

No se pueden eliminar los grupos integrados (*Administradores*, *Operadores de copia*, *Usuarios avanzados*, *Usuarios*, *Invitados* y *Replicador*). No se puede recuperar un grupo eliminado. Eliminar un grupo local sólo elimina el grupo, pero no las cuentas de usuario ni los grupos que eran miembros de dicho grupo. Si eliminamos un grupo y creamos otro con el mismo nombre, deberemos establecer nuevos permisos para el grupo nuevo, ya que éste no heredará los permisos concedidos al grupo antiguo.

## 2.5 Gestión de usuarios y grupos en símbolo del sistema

Podemos gestionar los usuarios y grupos con los siguientes comandos.

### 2.5.1 Gestión de usuarios. Comando net user

El comando net user añade una cuenta de usuario o visualiza su información.

<pre>net user [&lt;usuario&gt; {&lt;Password&gt;   *} /add [&lt;opciones&gt;] net user [&lt;usuario&gt; [/delete] ]</pre>	
Parámetro	Descripción
<usuario>	Especifica el nombre de la cuenta de usuario a añadir, borrar, modificar o ver. El nombre de usuario tiene como máximo 20 caracteres.
<password>	Asigna una clave a la cuenta de usuario. Teclear un asterisco provoca que el intérprete solicite la clave. Esta no se visualiza cuando se teclea.
<opciones>	Especifica opciones. La siguiente tabla las muestra

El parámetro <opciones> incluye las siguientes

Opción	Descripción
/active:{no   yes}	Habilita o deshabilita la cuenta de usuario.
/comment:"<Texto>"	Añade un comentario descriptivo de hasta 48 caracteres a la cuenta de usuario. Debe estar entrecomillado doble.
/countrycode:<NNN>	Utiliza el código de país/región para establecer el idioma por defecto de la ayuda y mensajes de error para el usuario. Un valor 0 indica el código de país/región por defecto.
/expires:{<DD/MM/YYYY>   never}	Provoca que la cuenta de usuario expire si se indica una fecha de expiración. El formato de fecha puede estar en [MM/DD/YYYY], [DD/MM/YYYY], o [mmm,dd,YYYY],

	dependiendo del código de país/región. Para el nombre del mes podemos usar números o abreviaturas de tres letras. Para el año podemos usar dos o cuatro dígitos. Si se omite el año se toma el de la fecha del sistema.
/fullname:"<Nombre>"	Especifica el nombre de usuario completo en lugar de un nombre de usuario. Debe encerrarse entre comillas dobles.
/homedir:<Path>	Establece la carpeta personal del usuario.
/passwordchg:{yes no}	Especifica si los usuarios pueden cambiar sus contraseñas. Por defecto es yes.
/passwordreq:{yes no}	Especifica si una cuenta de usuario debe tener una contraseña. Por defecto es yes.
/profilepath:[<Path>]	Establece el path para el perfil del usuario.
/scriptpath:<Path>	Establece el path para el script de inicio de sesión del usuario. El path es relativo a %systemroot%\System32\Repl\Import\Scripts.
/usercomment:"<Texto>"	Comentario de una cuenta de usuario entrecomillado doble.
/active:{yes no}	Habilita o deshabilita una cuenta de usuario. Por defecto la cuenta está activa

## 2.5.2 Gestión de grupos de usuarios. Comando net localgroup

Añade, visualiza o modifica grupos locales. Usado sin parámetros visualiza los nombres de los grupos locales.

<pre>net localgroup [&lt;grupo&gt; {/add [/comment:"&lt;Texto&gt;"]   /delete} ] net localgroup [&lt;grupo&gt; &lt;nombre&gt; [...] {/add   /delete} ]</pre>	
Parámetro	Descripción
<grupo>	Especifica el nombre del grupo a añadir, expandir o borrar. Usado sin parámetros adicionales visualiza la lista de usuarios o grupos en el grupo local.
/comment:"<Texto>"	Añade un comentario de hasta 256 caracteres para el grupo. El texto debe estar entrecomillado doble.
<nombre>[ ...]	Lista de uno o más nombres de usuarios o grupos para añadir o quitar de un grupo local
/add	Añade un nombre de grupo o nombre de usuario al grupo.
/delete	Quita el nombre de grupo o usuario de un grupo local.

## 2.6 Gestión de usuarios en WPS

Vamos a ver un conjunto de cmdlets para la gestión completa de usuarios y grupos. Para todos ellos veremos su sintaxis y una explicación de los parámetros obligatorios. Para una referencia completa del comando hay un enlace debajo de cada uno de ellos que direcciona la referencia completa del cmdlet en la web de WPS.

### 2.6.1 Crear un usuario. New-LocalUser

El cmdlet New-LocalUser crea una nueva cuenta de usuario.

```
New-LocalUser
[-AccountExpires <DateTime>]
[-AccountNeverExpires]
[-Description <String>]
[-Disabled]
[-FullName <String>]
[-Name] <String>
{-Password <SecureString> | [-NoPassword] }
[-PasswordNeverExpires]
[-UserMayNotChangePassword]
[-whatIf]
[-Confirm]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String>	Nombre del usuario
-Password <SecureString>	Asigna una contraseña al nuevo usuario
-NoPassword	Indica que el nuevo usuario no tendrá una contraseña.

[Haz clic para obtener la referencia completa.](#)

Por ejemplo, si creamos un usuario sin clave podríamos poner lo siguiente

```
PS C:\> New-LocalUser -Name "Usuario2" -NoPassword -FullName "Manuel
Gómez Benítez"

Name           Enabled Description
-----
Usuario2 True
```

Si queremos crear el usuario con una clave tendremos que leer la clave desde teclado sin mostrarla con Read-Host, y posteriormente asignársela al nuevo usuario.

```
PS C:\> $clave = Read-Host -AsSecureString
*****
PS C:\> New-LocalUser -Name "Usuario3" -Password $clave -FullName "Laura
```

```
Sánchez García" -Description "Usuario con clave"
```

```
Name      Enabled Description
-----
Usuario3  True      Usuario con clave
```

```
PS C:\>
```

También podíamos haber creado el usuario sin clave y nos la solicitará por teclado.

```
PS C:\> New-LocalUser -Name Jgarcia -FullName "Juan García Pérez"
```

```
cmdlet New-LocalUser en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Password: *****
```

```
Name      Enabled Description
-----
Jgarcia    True
```

## 2.6.2 Actualizar las propiedades de un usuario. Comando Set-LocalUser

El cmdlet Set-LocalUser permite modificar las propiedades de un usuario.

```
Set-LocalUser
  [-AccountExpires <DateTime>]
  [-AccountNeverExpires]
  [-Description <String>]
  [-FullName <String>]
  { [-Name] <String> | [-InputObject] <LocalUser> | [-SID]
  <SecurityIdentifier> }
  [-Password <SecureString>]
  [-PasswordNeverExpires <Boolean>]
  [-UserMayChangePassword <Boolean>]
  [-WhatIf]
  [-Confirm]
  [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalUser>	Cuenta de usuario a modificar
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.

[Haz clic para obtener la referencia completa.](#)

Por ejemplo, podemos hacer que la contraseña del usuario 2 nunca caduque.

```
Set-LocalUser -Name "Usuario2" -PasswordNeverExpires $true
```

También podemos hacer que el usuario 3 no pueda cambiar su clave.

```
PS C:\> Set-LocalUser -Name "Usuario3" -UserMayChangePassword $false
```

En el siguiente ejemplo vamos a obtener un usuario para posteriormente cambiar su descripción.

```
PS C:\> $usuario2 = Get-LocalUser -Name "Usuario2"
PS C:\> Set-LocalUser -InputObject $usuario2 -Description "Usuario nº2"
```

### 2.6.3 Mostrar usuarios. Get-LocalUser

Muestra los usuarios del sistema.

<pre>Get-LocalUser { [[-Name] &lt;String[]&gt;]   [[-SID] &lt;SecurityIdentifier[]&gt;] } [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.

[Haz clic para obtener la referencia completa.](#)

Por ejemplo, si queremos un listado completo de todos los usuarios del sistema.

```
PS C:\> Get-LocalUser

Name                               Enabled Description
----                               -
Administrador                     False  Cuenta integrada para la administración del
equipo o dominio
DefaultAccount                    False  Cuenta de usuario administrada por el
sistema.
Invitado                           False  Cuenta integrada para el acceso como invitado
al equipo o dominio
Usuario                           True
Usuario2                          True
Usuario3                          True  Usuario con clave
WDAGUtilityAccount                False  Una cuenta de usuario que el sistema
administra y usa para escenarios de Protección de a...
```

Si solamente queremos ver información de un único usuario podemos utilizar el parámetro -Name.

```
PS C:\> Get-LocalUser -Name Usuario3
```

```
Name      Enabled Description
-----
Usuario3  True      Usuario con clave
```

Podemos emplear metacaracteres para listar varios usuarios con parte del nombre común.

```
PS C:\> Get-LocalUser -Name Usuario*

Name      Enabled Description
-----
Usuario   True
Usuario2  True      Usuario n°2
Usuario3  True      Usuario con clave
```

Mediante este cmdlet podemos consultar también las propiedades de una cuenta de usuario.

```
PS C:\> $usuario3 = Get-LocalUser Usuario3
PS C:\> $usuario3.Enabled
False
PS C:\> $usuario3.FullName
Laura Sánchez García
PS C:\> $usuario3.Description
Usuario con clave
PS C:\>
```

#### 2.6.4 Habilitar usuarios. Enable-LocalUser

Podemos habilitar usuarios locales con Enable-LocalUser. Un usuario habilitado puede abrir sesión y acceder a los recursos publicados en la red.

```
Enable-LocalUser
    { [-Name] <String> | [-InputObject] <LocalUser> | [-SID]
    <SecurityIdentifier> }
    [-whatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalUser>	Cuenta de usuario a modificar
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.

[Haz clic para obtener referencia completa.](#)

Por ejemplo, para habilitar el usuario n.º 2 ejecutamos el siguiente cmdlet.

```
PS C:\> Enable-LocalUser -Name Usuario2
```

### 2.6.5 Deshabilitar usuarios. Disable-LocalUser

Podemos deshabilitar usuarios locales con `Disable-LocalUser`. Un usuario deshabilitado no puede abrir sesión.

```
Disable-LocalUser
    { [-Name] <String> | [-InputObject] <LocalUser> | [-SID]
  <SecurityIdentifier> }
    [-whatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalUser>	Cuenta de usuario a modificar
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.

[Haz clic para obtener referencia completa.](#)

Por ejemplo, para deshabilitar el usuario n.º 3 ejecutamos el siguiente cmdlet.

```
PS C:\> Disable-LocalUser -Name Usuario3
```

### 2.6.6 Cambiar nombre de usuario. Rename-LocalUser

Podemos cambiar el nombre de una cuenta de usuario con `Rename-LocalUser`.

```
Rename-LocalUser
    { [-Name] <String> | [-InputObject] <LocalUser> | [-SID]
  <SecurityIdentifier> }
    [-NewName] <String>
    [-whatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalUser>	Cuenta de usuario a modificar
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.
-NewName <String>	Nuevo nombre de la cuenta.

[Haz clic para obtener la referencia completa.](#)



Por ejemplo, vamos a cambiar el nombre de la cuenta usuario3 por uno más amigable y acorde a la persona a la que pertenece.

```
PS C:\> $usuario2 = Get-LocalUser -Name Usuario2
PS C:\> Rename-LocalUser -InputObject $usuario2 -NewName "Mgomez"
PS C:\> (Get-LocalUser -Name Mgomez).FullName
Manuel Gómez Benítez
```

### 2.6.7 Eliminar usuarios. Remove-LocalUser

El cmdlet Remove-LocalUser se emplea para eliminar usuarios del sistema.

```
Remove-LocalUser
    { [-Name] <String> | [-InputObject] <LocalUser> | [-SID]
    <SecurityIdentifier> }
    [-whatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalUser>	Cuenta de usuario a modificar
-Name <String>	Nombre del usuario a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del usuario a modificar.

[Haz clic para obtener la referencia completa.](#)

Por ejemplo, eliminamos al usuario n.º 3.

```
PS C:\> Remove-LocalUser -Name Usuario3
```

## 2.7 Gestión de grupos en WPS

A continuación vamos a ver el conjunto de cmdlets para la gestión de grupos locales.

### 2.7.1 Crear grupos. New-LocalGroup

El cmdlet New-LocalGroup crea un nuevo grupo local.

```
New-LocalGroup
    [-Description <String>]
    [-Name] <String>
    [-whatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-Name <String>	Nombre del grupo

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para crear el grupo becarios ejecutamos el siguiente cmdlet.

```
PS C:\> New-LocalGroup -Name becarios -Description "Los alumnos en prácticas"
```

## 2.7.2 Actualizar grupos. Set-LocalGroup

Para actualizar un grupo local tenemos el cmdlet Set-LocalGroup.

<pre>Set-LocalGroup   -Description &lt;String&gt;   { [-InputObject] &lt;LocalGroup&gt;   -Name &lt;String&gt;   -SID &lt;SecurityIdentifier&gt; }   [-whatIf]   [-Confirm]   [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-InputObject <LocalGroup>	Grupo a modificar
-Name <String>	Nombre del grupo a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a modificar.

[Haz clic para obtener una referencia completa.](#)

A modo de ejemplo podemos cambiar la descripción del grupo anterior.

```
PS C:\> Set-LocalGroup -Name becarios -Description "Trabajadores en prácticas"
```

## 2.7.3 Mostrar grupos. Get-LocalGroup

Para visualizar información del grupo u obtener un grupo para un uso posterior en una variable disponemos del cmdlet Get-LocalGroup.

<pre>Get-LocalGroup   [[-Name] &lt;String[]&gt;]   [[-SID] &lt;SecurityIdentifier[]&gt;]   [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-Name <String>	Nombre del grupo a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a modificar.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. Para ver un listado de todos los grupos en el sistema

```
PS C:\> Get-LocalGroup
```

Name	Description
----	-----
becarios	Trabajadores en prácticas
Administradores	Los administradores tienen
acceso completo y sin restricciones al equipo ...	
Administradores de Hyper-V	Los miembros de este grupo
tienen acceso completo y sin restricciones a t...	
Duplicadores	Pueden replicar archivos
en un dominio	
...	

Para ver información del grupo `becarios`.

```
PS C:\> Get-LocalGroup becarios
```

Name	Description
----	-----
becarios	Trabajadores en prácticas

Podemos también utilizar metacaracteres para obtener un conjunto de grupos.

```
PS C:\> Get-LocalGroup Operador*
```

Name	Description
----	-----
Operadores criptográficos	Los miembros tienen
autorización para realizar operaciones criptográficas.	
Operadores de asistencia de control de acceso	Los miembros de este
grupo pueden consultar de forma remota los atributos...	
Operadores de configuración de red	Los miembros en este
equipo pueden tener algunos privilegios administrati...	
Operadores de copia de seguridad	Los operadores de copia de
seguridad pueden invalidar restricciones de se...	

## 2.7.4 Gestionar miembros de grupos.

Los grupos son conjuntos de usuarios. Con los siguientes cmdlets podemos añadir, mostrar o eliminar miembros de grupos.

### 2.7.4.1 Añadir miembros al grupo. *Add-LocalGroupMember*

Para añadir un conjunto de usuarios como miembros de un grupo empleamos el cmdlet `Add-LocalGroupMember`. Los nuevos miembros pueden ser usuarios o grupos. Todos los derechos y permiso que se asignen al grupo se asignan a todos los miembros del grupo. Los miembros del grupo `Administradores` tienen control total en el PC.

```
Add-LocalGroupMember
{ [-Group] <LocalGroup> | -Name <String> | -SID
<SecurityIdentifier> }
[-Member] <LocalPrincipal[]>
[-whatIf]
[-Confirm]
[<CommonParameters>]
```

Parámetro	Descripción
-Group <LocalGroup>	Grupo a modificar
-Name <String>	Nombre del grupo a modificar
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a modificar.
-Member <LocalPrincipal[]>	Array con los miembros del grupo. Puede ser una lista de miembros (usuarios y/o grupos) separados por coma.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para añadir varios usuarios al grupo creado en apartados anteriores ejecutamos el siguiente cmdlet.

```
PS C:\> Add-LocalGroupMember -Name becarios -Member Mgomez, Jgarcia,
CNuñez
```

#### 2.7.4.2 *Mostrar miembros de grupo. Get-LocalGroupMember*

Si queremos comprobar los miembros de un grupo local empleamos `Get-LocalGroupMember`.

```
Get-LocalGroupMember
[[[-Member] <String>]
{ [-Name] <String> | [-Group] <LocalGroup> | [-SID]
<SecurityIdentifier> }
[<CommonParameters>]
```

Parámetro	Descripción
-Group <LocalGroup>	Grupo con los miembros que queremos listar
-Name <String>	Nombre del grupo para listar sus miembros
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a listar sus miembros.
-Member <LocalPrincipal[]>	Array con los miembros del grupo que queremos listar. Se pueden emplear metacaracteres.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para ver los miembros del grupo becarios.

```
PS C:\> Get-LocalGroupMember -Name becarios
```

ObjectClass	Name	PrincipalSource
Usuario	PCW10\CNuñez	Local
Usuario	PCW10\Jgarcia	Local
Usuario	PCW10\Mgomez	Local

```
PS C:\> Get-LocalGroupMember -Group becarios
```

ObjectClass	Name	PrincipalSource
Usuario	PCW10\CNuñez	Local
Usuario	PCW10\Jgarcia	Local
Usuario	PCW10\Mgomez	Local

Para ver los miembros del grupo Administradores.

```
PS C:\> Get-LocalGroupMember -Group Administradores
```

ObjectClass	Name	PrincipalSource
Usuario	PCW10\Administrador	Local
Usuario	PCW10\Usuario	Local

Si queremos restringir el listado anterior a los miembros cuyo nombre comienza por Admin.

```
PS C:\> Get-LocalGroupMember -Group Administradores -Member Admin*
```

ObjectClass	Name	PrincipalSource
Usuario	PCW10\Administrador	Local

#### 2.7.4.3 Quitar miembros de grupo. *Remove-LocalGroupMember*

El cmdlet `Remove-LocalGroupMember` quita usuarios o grupos como miembros de un grupo local.

```
Remove-LocalGroupMember
    { [-Name] <String> | [-Group] <LocalGroup> | [-SID]
  <SecurityIdentifier> }
    [-Member] <LocalPrincipal[]>
    [-WhatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-Group <LocalGroup>	Grupo con los miembros que queremos quitar
-Name <String>	Nombre del grupo para quitar a los miembros
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a quitar miembros.
-Member <LocalPrincipal[]>	Array con los miembros del grupo que queremos quitar. Se pueden emplear metacaracteres.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, si queremos quitar los usuarios Mgomez y Jgarcia del grupo becarios.

```
PS C:\> Remove-LocalGroupMember -Name becarios -Member Mgomez, Jgarcia
```

## 2.7.5 Cambiar nombre de grupo. Rename-LocalGroup

Para cambiar el nombre de un grupo utilizamos el cmdlet Rename-LocalGroup.

<pre>Rename-LocalGroup { [-Name] &lt;String&gt;   [-InputObject] &lt;LocalGroup&gt;   [-SID] &lt;SecurityIdentifier&gt; } [-NewName] &lt;String&gt; [-WhatIf] [-Confirm] [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-InputObject <LocalGroup>	Grupo a cambiar el nombre.
-Name <String>	Nombre del grupo para cambiar su nombre.
-SID <SecurityIdentifier>	Especifica el identificador de seguridad del grupo a cambiar su nombre.
-NewName <String>	Nuevo nombre del grupo

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para cambiar el nombre del grupo becarios por usuarios\_practicas ejecutaríamos el siguiente cmdlet.

```
PS C:\> Rename-LocalGroup -Name becarios -NewName usuarios_practicas
```

## 2.7.6 Eliminar grupos. Remove-LocalGroup

Para eliminar un grupo disponemos del cmdlet Remove-LocalGroup.

<pre>Remove-LocalGroup { [-Name] &lt;String[]&gt;   [-InputObject] &lt;LocalGroup[]&gt;   [-</pre>	
--	--

```
SID] <SecurityIdentifier[]> }  
    [-whatIf]  
    [-Confirm]  
    [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <LocalGroup[]>	Array de grupos a eliminar. Puede ser una lista de grupos separados por comas.
-Name <String[]>	Array de nombres de grupo para eliminar.
-SID <SecurityIdentifier[]>	Array de identificadores de seguridad de los grupos a eliminar.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, vamos a eliminar el grupo usuarios\_practicas.

```
PS C:\> Remove-LocalGroup -Name usuarios_practicas
```

### 3 Directivas de grupo local

Directiva de grupo o GPOs (*Group Policy Object*) es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo en un entorno de red con un dominio Active Directory. La directiva de grupo proporciona la gestión centralizada y configuración del sistema operativo, aplicaciones y configuración de los usuarios. En otras palabras, la Directiva de Grupo, en parte, controla lo que los usuarios pueden y no pueden hacer en un sistema informático.

Directiva de grupo a menudo se utiliza para restringir ciertas acciones que pueden presentar riesgos de seguridad potenciales, por ejemplo: Bloquear el acceso al Administrador de tareas, restringir el acceso a determinadas carpetas, deshabilitar la descarga de archivos ejecutables, etc.

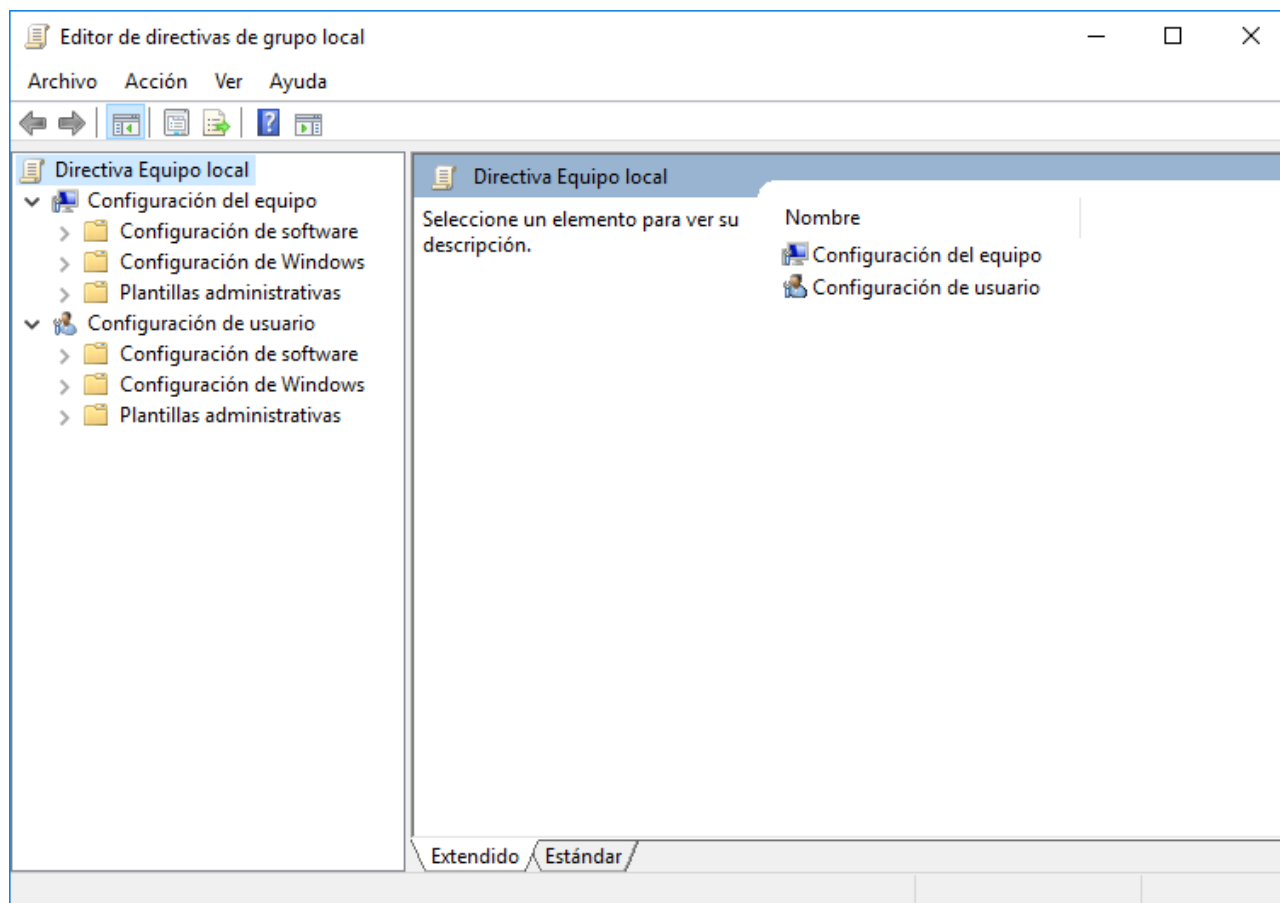


Figura 17.- Editor GPO

Directiva de Grupo Local (LGP) es una versión más básica de la directiva de grupo utilizado por Active Directory. En las versiones de Windows anteriores a Windows Vista, se puede configurar la directiva de grupo para un equipo local único, pero a diferencia de la Directiva de Grupo de Active Directory, no se pueden hacer políticas para usuarios individuales o grupos.

Windows dispone de un editor de directiva de grupo local para gestionar la GPO. Para abrirlo pulsamos la combinación de teclas Win+R y ejecutamos `gpedit.msc`. Como vemos en la ventana del editor de GPOs contamos con dos opciones:

- ✓ Configuración del equipo.- Nos permite realizar y establecer ajustes a los parámetros de la máquina local.
- ✓ Configuración de usuario.- Nos brinda la posibilidad de establecer los parámetros para el usuario que ha de usar la máquina.

Cada una de las opciones antes mencionadas está subdividida en tres categorías:

- ✓ Configuración de software.- Esta opción nos permite establecer la configuración necesaria para el software instalado en la máquina local.
- ✓ Configuración de Windows.- Usando esta opción podremos establecer los parámetros relacionados con el entorno de Windows, por ejemplo, directivas de seguridad, scripts, resolución de nombres, etc; En esta categoría hay que poner



mucho cuidado ya que algún ajuste mal establecido puede afectar el rendimiento del sistema.

- ✓ Plantillas administrativas. - Esta es sin lugar a dudas la opción que más usaremos ya que desde aquí está prácticamente todos los ajustes del equipo, panel de control, inicio de sesión, apagado, etc.

Es importante recordar que cuando trabajamos con una GPO local la configuración que más hemos de usar es la del usuario, ya que la configuración del sistema trata temas muy delicados sobre todo en temas de seguridad, redes, scripts, ya que la mayoría de estos parámetros son usados cuando la máquina está en un dominio.

### 3.1 Contraseñas seguras

A menudo se subestima y se pasa por alto la función de las contraseñas en la protección de la red de una organización. Las contraseñas ofrecen la primera línea defensiva contra el acceso no autorizado.

Las contraseñas vulnerables ofrecen a los intrusos una forma de acceso sencilla a los equipos y la red, mientras que las contraseñas seguras son considerablemente más difíciles de averiguar, incluso si se utiliza el software para averiguar contraseñas que existe actualmente. Las herramientas para averiguar contraseñas son cada vez mejores y los equipos utilizados son más eficaces. El software para averiguar contraseñas utiliza uno de los tres métodos siguientes: suposiciones inteligentes, ataques de diccionario y ataques físicos automatizados que intentan todas las combinaciones de caracteres posibles. Con tiempo suficiente, mediante esta automatización se puede averiguar cualquier contraseña. Sin embargo, las contraseñas seguras son mucho más difíciles de averiguar que las vulnerables. Para obtener seguridad, un equipo debe tener contraseñas seguras para todas las cuentas de usuario.

Una contraseña vulnerable:

- ✓ no es una contraseña.
- ✓ contiene el nombre de usuario, el nombre real o el nombre de la empresa.
- ✓ contiene una palabra exacta del diccionario. Por ejemplo, *Contraseña* es una contraseña vulnerable.

Una contraseña segura:

- ✓ tiene seis caracteres como mínimo.
- ✓ no contiene el nombre de usuario, el nombre real o el nombre de la empresa.
- ✓ no contiene una palabra exacta del diccionario.
- ✓ es significativamente diferente de otras contraseñas anteriores. Las contraseñas que utilizan incrementos (Contraseña1, Contraseña2, Contraseña3, etc.) no son seguras.

- ✓ está compuesta por caracteres de cada uno de los siguientes cuatro grupos:

Grupo	Ejemplo
Letras mayúsculas	A, B, C...
Letras minúsculas	a, b, c ...
Numéricos	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números)	` ~ ! @ # \$ % ^ & * ( ) _ + - = { }   [ ] \ : " ; ' < > ? , . /

Un ejemplo de una contraseña segura es J\*p2l e04>F.

Una contraseña puede cumplir la mayoría de los criterios de una contraseña segura y, aún así, seguir siendo vulnerable. Por ejemplo, ¡Ho1aAto2! es una contraseña relativamente insegura, aunque cumple la mayoría de los criterios de una contraseña segura y cumple también los requisitos de complejidad de la directiva de contraseñas. H!o1Z¡2a es una contraseña segura porque la palabra del diccionario está intercalada con símbolos, números y otras letras. Es importante informar a los usuarios acerca de las ventajas de utilizar contraseñas seguras y enseñarles cómo crear contraseñas que ofrezcan verdadera seguridad.

Las contraseñas de Windows pueden incluir hasta 127 caracteres. Windows cuenta con un conjunto de directivas de grupo que comprueba la complejidad de la contraseña de la cuenta de usuario cuando se establece.

## 3.2 Directiva de contraseñas

Con la directiva de contraseña se puede establecer la política de contraseñas de la empresa u organización. Para ello hay que definir y establecer unos criterios representados por cada directiva que indican su obligatoriedad y ciclo de vida. Estos son:

- ✓ Almacenar la contraseña usando cifrado reversible.- Esta configuración de seguridad determina si el sistema operativo almacena las contraseñas con cifrado reversible. Esta directiva aporta compatibilidad para las aplicaciones que utilizan protocolos que requieren conocer la contraseña del usuario para la autenticación. El almacenamiento de contraseñas con cifrado reversible equivale, básicamente, al almacenamiento de versiones de texto simple de las contraseñas. Por este motivo, esta directiva no debe habilitarse nunca, a menos que los requisitos de la aplicación sean más importantes que la necesidad de proteger la información de las contraseñas.
- ✓ Exigir historial de contraseñas.- Esta configuración de seguridad determina el número de nuevas contraseñas únicas que hay que asociar con una cuenta de usuario para que se pueda volver a utilizar una contraseña antigua. El valor debe estar comprendido entre 0 y 24 contraseñas. Esta directiva permite a los administradores mejorar la seguridad, al garantizar que las contraseñas antiguas no

se vuelven a utilizar continuamente. El valor predeterminado en los controladores de dominio es de 24

- ✓ Las contraseñas deben cumplir los requisitos de complejidad.- Esta opción de configuración determina si las contraseñas deben cumplir los requerimientos de complejidad. Si está habilitada esta directiva (por defecto), las contraseñas deben cumplir los requisitos mínimos siguientes:
  - No deben contener parte o todo el nombre de la cuenta del usuario.
  - Tener seis caracteres de longitud, como mínimo.
  - Estar compuesta por caracteres de tres de las siguientes categorías:
    - Letras mayúsculas, de la A a la Z
    - Letras minúsculas, de la a a la z
    - Dígitos en base 10, de 0 a 9
    - Caracteres no alfabéticos (por ejemplo, !, \$, #, %)
- ✓ Longitud mínima de la contraseña.- Esta configuración de seguridad determina el número mínimo de caracteres que puede contener la contraseña de un usuario. Puede establecer un valor entre 1 y 14 caracteres, o que no se requiere contraseña si establece el número de caracteres como 0. El valor por defecto es 7.
- ✓ Vigencia máxima de la contraseña.- Esta configuración de seguridad determina el periodo (en días) que puede utilizarse una contraseña antes de que el sistema exija al usuario que la cambie. Puede configurar las contraseñas para que caduquen tras un número de días entre 1 y 999, o puede especificar que las contraseñas nunca caduquen estableciendo el número de días en 0. Si la vigencia máxima de la contraseña se encuentra entre 1 y 999 días, la *Vigencia mínima de la contraseña* deberá ser inferior a la vigencia máxima. Si la vigencia máxima de la contraseña está establecida en 0, la vigencia mínima puede ser cualquier valor entre 0 y 998 días.
- ✓ Vigencia mínima de la contraseña.- Esta configuración de seguridad determina el periodo (en días) que se debe utilizar una contraseña antes de que el usuario pueda cambiarla. Puede establecer un valor entre 1 y 998 días, o bien permitir que se efectúen cambios de forma inmediata si configura el número de días como 0. La vigencia mínima de la contraseña debe ser inferior a la *Vigencia máxima de la contraseña*, a menos que ésta se establezca en 0, valor que indica que la contraseña nunca caduca. Si la vigencia máxima de la contraseña está establecida en 0, la vigencia mínima puede ser cualquier valor entre 0 y 998.

Configurar la vigencia mínima de la contraseña con un valor mayor que 0 si desea que *Exigir historial de contraseñas* entre en vigor. Sin una vigencia mínima de la contraseña, los usuarios pueden probar las distintas contraseñas de forma repetida hasta obtener una contraseña favorita antigua. La configuración predeterminada no sigue esta recomendación,

de forma que un administrador puede especificar una contraseña para un usuario y solicitarle que cambie la contraseña definida cuando inicie sesión. Si el historial de la contraseña se establece como 0, el usuario no tendrá que elegir una contraseña nueva. Por este motivo, *Exigir historial de contraseñas* se establece como 1 de forma predeterminada.

### 3.2.1 Definir las directivas de contraseña

Las directivas de contraseña se establecen en las directivas de grupo. Por tanto, pueden establecerse en una unidad organizacional o en todo el dominio. Para aplicar o modificar la directiva de contraseña siga los siguientes pasos:

1. Abrir el editor de GPO.
2. Desplegar el árbol de la consola en *Configuración de Equipo* → *Configuración de Windows* → *Configuración de Seguridad* → *Directivas de cuenta* → *Directivas de contraseña*.

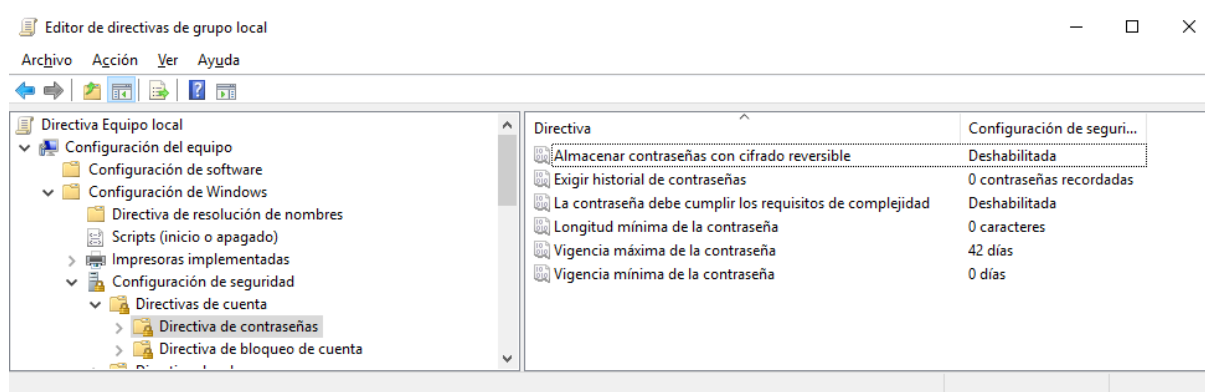


Figura 18.- Directivas de contraseña

3. En el panel de detalles, hacer clic con el botón derecho del ratón en la configuración de directiva en cuestión y seleccionar *Propiedades*.
4. Si va a definir esta configuración de directiva por primera vez, active la casilla de verificación *Definir esta configuración de directiva*.
5. Establecer las opciones que se deseen y, después, hacer clic en Aceptar.

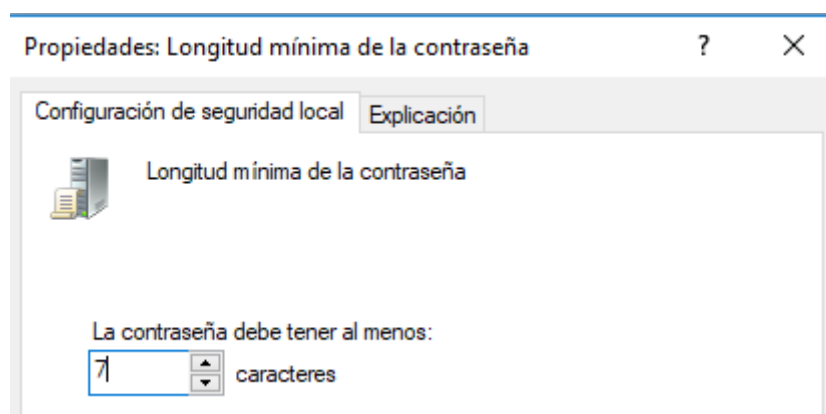


Figura 19.- Directiva Longitud mínima de la contraseña

### 3.3 Directiva de bloqueo de cuentas

La directiva de bloqueo de cuentas deshabilita una cuenta de usuario si se escribe una contraseña incorrecta un número de veces especificado durante un período de tiempo dado. Esta configuración de directiva ayuda a impedir que los intrusos averigüen las contraseñas de los usuarios y reducen la probabilidad de que los ataques a la red tengan éxito.

Los usuarios bloqueados no pueden tener acceso a sus cuentas hasta que éstas se desbloqueen automáticamente al cabo de un período de tiempo especificado o hasta que se desbloqueen manualmente.

Las cuentas de los usuarios autorizados pueden quedar bloqueadas si no escriben la contraseña correcta o si se cambia su contraseña en un equipo mientras están conectados en otro equipo. El equipo que utiliza la contraseña incorrecta intenta repetidamente autenticar al usuario y, como la contraseña que utiliza para la autenticación es incorrecta, la cuenta de usuario acaba por bloquearse. Para evitar el bloqueo de usuarios autorizados, configure el umbral de bloqueo de cuentas en un valor alto. No obstante, el caso de un equipo que intenta autenticar a un usuario repetidamente con una contraseña incorrecta es muy parecido al comportamiento que se emplea en el software utilizado para averiguar contraseñas. Configurar el umbral de bloqueo de cuentas en un valor alto para que los usuarios autorizados no queden bloqueados también puede permitir de forma inadvertida el acceso no autorizado a la red por parte de los intrusos.

Las directivas de bloqueo de cuenta que se pueden definir son:

- ✓ Duración del bloqueo de cuenta.- Esta configuración de seguridad determina el número de minutos que una cuenta bloqueada permanece en este estado antes de desbloquearse automáticamente. El intervalo disponible oscila entre 0 y 99.999 minutos. Si la duración del bloqueo de cuenta se establece en 0, la cuenta se bloquea hasta que un administrador la desbloquea explícitamente. Si no se define ningún umbral de bloqueo de cuenta, la duración del bloqueo de cuenta será mayor o igual al tiempo de restablecimiento. No tiene valor por defecto, ya que esta configuración de directiva sólo tiene significado cuando se especifica *Umbral de bloqueo de cuenta*.

- ✓ Restablecer la cuenta de bloqueos después de.- Esta configuración de seguridad determina el número de minutos que deben transcurrir tras un intento de inicio de sesión incorrecto para que el contador de intentos de inicio de sesión incorrectos se restablezca en 0. El intervalo disponible oscila entre 1 y 99.999 minutos. Si se define un umbral de bloqueo de cuenta, este tiempo de restablecimiento debe ser menor o igual a *Duración del bloqueo de cuenta*. No tiene valor por defecto, ya que esta configuración de directiva sólo tiene significado cuando se especifica *Umbral de bloqueo de cuenta*.
- ✓ Umbral de bloqueos de cuenta.- Esta configuración de seguridad determina el número de intentos de inicio de sesión incorrectos que hacen que una cuenta de usuario se bloquee. Una cuenta bloqueada no puede usarse hasta que un administrador la restablezca o hasta que expire su duración de bloqueo. Puede establecer un valor comprendido entre 0 y 999 intentos de inicio de sesión incorrectos. Si establece el valor en 0, la cuenta no se bloqueará nunca. Los intentos incorrectos de escribir una contraseña en estaciones de trabajo o servidores miembro bloqueados mediante Ctrl+Alt+Supr o protectores de pantalla protegidos por contraseña se contabilizan como intentos de inicio de sesión incorrectos. Valor por defecto: 0.

### 3.3.1 Definir las directivas de bloqueo de cuenta

Aunque las directivas de bloqueo de cuenta se pueden definir para el equipo local, el siguiente proceso es para las cuentas del dominio.

1. Abrir el editor de GPO.
2. Desplegar el árbol de la consola en *Configuración de Equipo* → *Configuración de Windows* → *Configuración de Seguridad* → *Directivas de cuenta* → *Directivas de bloqueo de cuenta*.

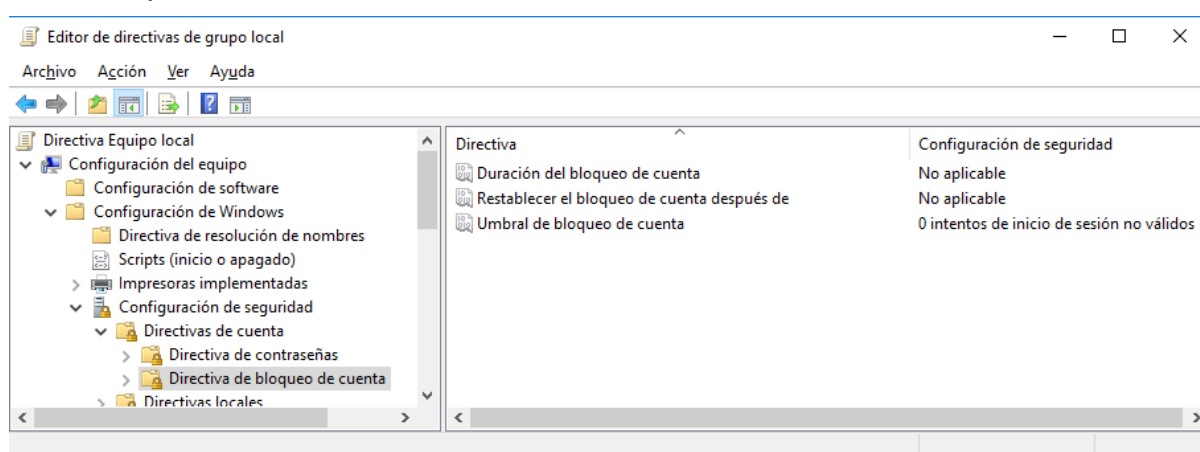


Figura 20.- Directivas de bloqueo de cuenta

3. En el panel de detalles, hacer doble clic en la directiva de bloqueo de cuenta que se desea modificar.
4. Si la opción de seguridad no se ha definido todavía, activar la casilla de verificación *Definir esta configuración de directiva*.

### 3.4 Derechos de usuarios

Los derechos de usuario conceden determinados privilegios a los usuarios y grupos del sistema. Los administradores pueden asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales. Estos derechos autorizan a los usuarios a realizar acciones específicas, como iniciar una sesión en el sistema de forma interactiva o realizar copias de seguridad de archivos y directorios.

Los derechos de usuario se diferencian de los permisos en que se aplican a las cuentas de usuario, mientras que los permisos se asignan a los objetos como carpetas, archivos e impresoras.

La lista de derechos de usuario es muy larga. Si se desea información concreta sobre alguno de ellos se recomienda consultar *Derechos y privilegios de usuario* de la documentación de Windows.

Para gestionar los derechos de usuario tenemos *Directiva de seguridad local*. Seguir los siguientes pasos:

1. Abrir el editor de GPO.
2. Desplegar el árbol de la consola en *Configuración de Equipo* → *Configuración de Windows* → *Configuración de Seguridad* → *Directivas locales* → *Asignación de derechos de usuario*.
3. En la lista de directivas hacer doble clic en el derecho de usuario que vamos a definir.
4. Para asignar un usuario o grupo hacer clic en *Agregar usuario o grupo...* Buscar un usuario y hacer clic en *Aceptar*.
5. Para eliminar un usuario o grupo seleccionarlo en la lista de usuarios y grupos y posteriormente hacer clic en el botón *Quitar*.
6. Cuando se haya terminado de agregar usuarios y grupos, o de eliminar usuarios y grupos hacer clic en el botón *Aceptar*.

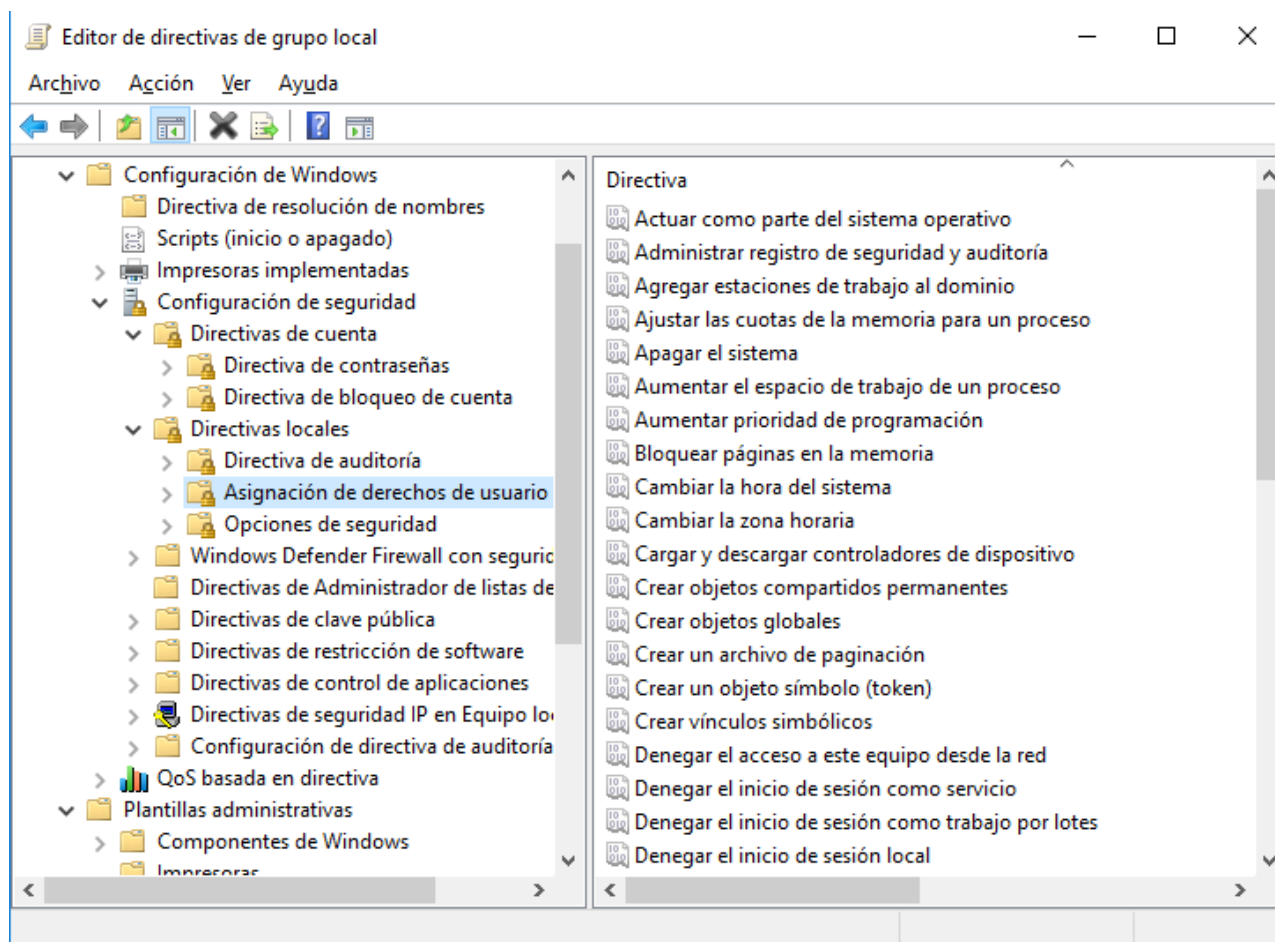


Figura 21.- Asignación de derechos de usuario

7. Repetir los pasos anteriores para los derechos de usuario que se desean gestionar.

Si queremos ver que privilegios tenemos como usuario podemos ejecutar el comando `whoami /priv` en el símbolo del sistema.

### 3.5 Gestión de directivas de grupo en el símbolo del sistema

Los siguientes comandos permiten gestionar las directivas de grupo local o de dominio.

#### 3.5.1 Comando `gpresult`

Esta herramienta de línea de comandos muestra información del conjunto resultante de directivas (RSOP) para un usuario y equipo de destino.

```
gpresult [/S sistema [/U usuario [/P [contraseña]]] [/SCOPE
ámbito]
[/USER usuarioDestino] [/R | /V | /Z] [(/X | /H) <archivo> [/F]]
```

Parámetro	Descripción
/S sistema	Especifica el sistema remoto al que se conecta.



/U [dominio\]usuario /P [contraseña]	Especifica las credenciales de usuario con las que se realiza la consulta del conjunto de directivas.
/SCOPE ámbito	Especifica si se muestra la configuración de equipo (COMPUTER) o la de usuario (USER).
/USER usuarioDestino	Usuario del cual se consulta el conjunto de directivas.
/R	Muestra datos resumidos
/V	Muestra información detallada
/Z	Muestra información con mayor nivel de detalle.
/X <archivo>	Guarda la información en un archivo con formato XML.
/H <archivo>	Guarda la información en un archivo con formato HTML.
/F	Sobreescribe el archivo generado en las dos opciones anteriores.

### 3.5.2 Comando gpupdate

El comando gpupdate actualiza opciones de la directiva de grupo.

gpupdate [/Target:{Computer   User}] [/Force] [/wait:<valor>] [/Logoff] [/Boot] [/Sync]	
Parámetro	Descripción
/Target:{Computer   User}	Especifica si se actualizan las directivas de usuario o de equipo. Por defecto se actualizan ambas.
/Force	Vuelve a aplicar toda la configuración de directivas. De forma predeterminada solo se aplicarán las directivas que cambiaron.
/wait:<valor>	Indica una espera en segundos para aplicar las directivas.
/Logoff	Después de actualizar las directivas de grupo se cierra la sesión. Se utiliza cuando las directivas solamente se aplican cuando se abre sesión de nuevo.
/Boot	Produce un reinicio después de actualizar las directivas. Se emplea cuando las directivas solamente pueden aplicarse al reiniciar el sistema
/Sync	Aplica las directivas en segundo plano.

## 4 Gestión de procesos y servicios

A continuación vamos a describir algunas herramientas y técnicas para realizar un mantenimiento de los procesos y servicios de Windows que nos permite obtener un rendimiento adecuado.

## 4.1 Administrador de tareas

Cada uno de los programas que se ejecutan en el equipo tiene un proceso asociado a él que inicia el programa. Con el *Administrador de tareas* podemos ver los procesos que se están ejecutando en el equipo en ese momento.

Para ver los procesos en ejecución realizar los siguientes pasos:

1. Abrir el *Administrador de tareas* pulsando la combinación de teclas Ctrl+Alt+Supr y en el menú de pantalla que aparece se hace clic sobre *Iniciar el Administrador de Tareas*.
2. Hacer clic en *Más detalles*. Aparece la lista completa de procesos en ejecución en esos momentos. Los procesos se dividen varias categorías que están rotuladas con un nombre y un número entre paréntesis que indica el número de procesos en dicha categoría. Estas son:
  - a) Aplicaciones.- Aplicaciones que está ejecutando el usuario.
  - b) Procesos en segundo plano.- Generalmente son servicios en espera de algún evento que los despierte para atender una petición. Por ejemplo, el subsistema de impresión está esperando a que le llegue un documento a imprimir desde cualquier aplicación.
  - c) Procesos de Windows.- Procesos del SO.

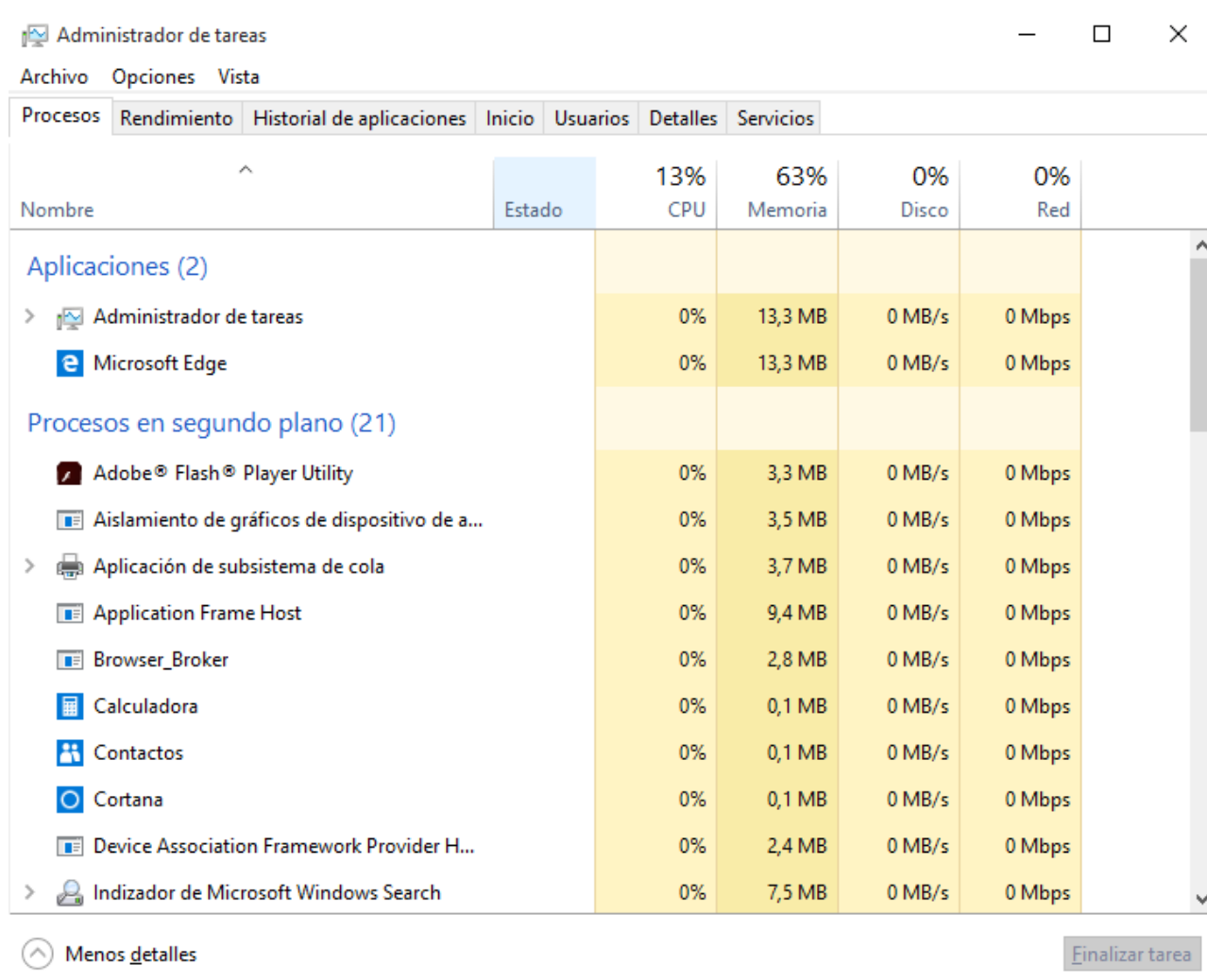


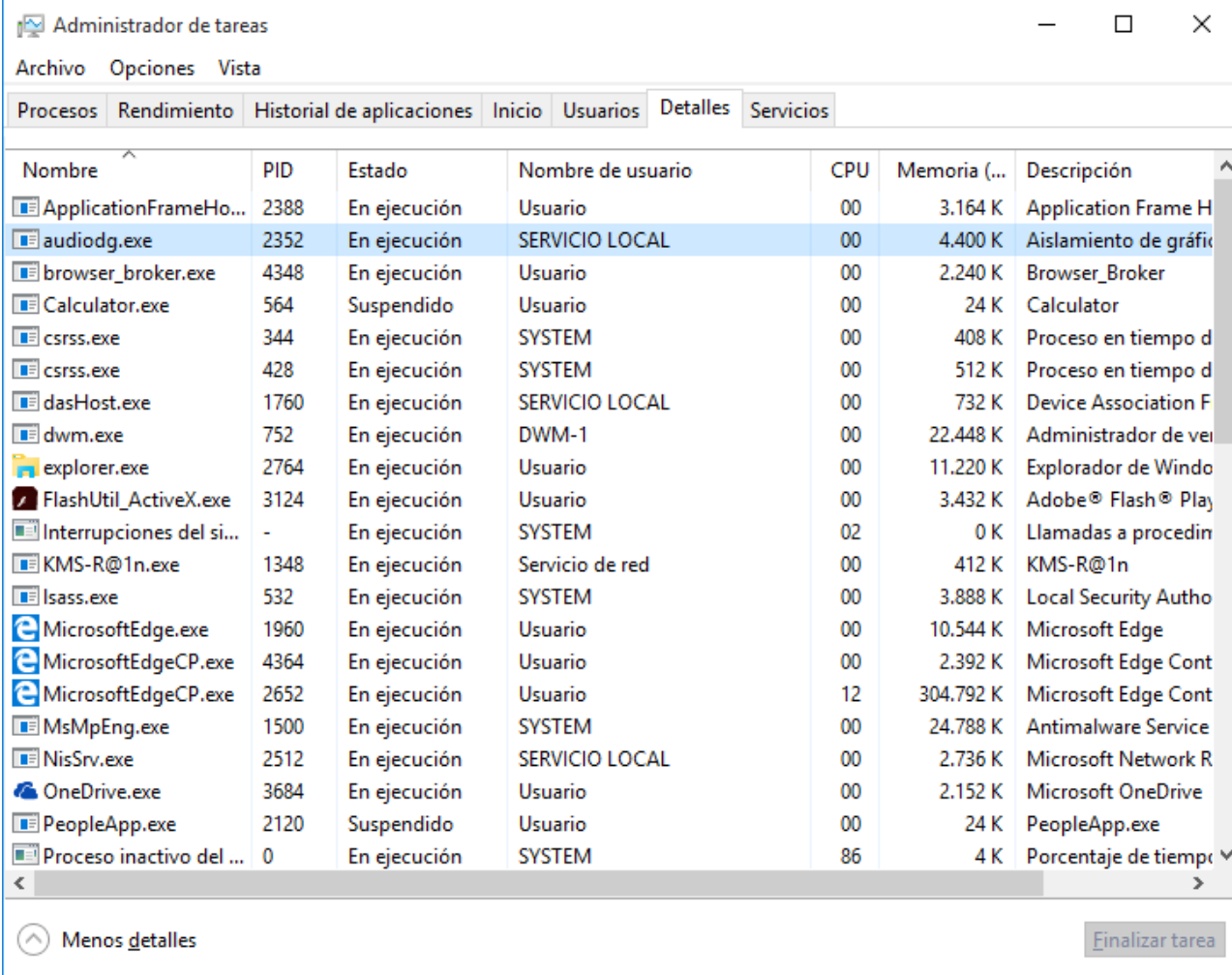
Figura 22.- Procesos en ejecución

La lista incluye el nombre del proceso, su estado y porcentajes de ocupación o uso de la CPU, memoria RAM, Disco y Red.

3. Para obtener más información podemos hacer clic en la pestaña *Detalles*, realizar una de las siguientes acciones:
  - a) En la pestaña *Detalles* se puede ver información añadida de los procesos. Aquí nos muestra el PID de los procesos. Es necesario haber abierto sesión como administrador o autenticarse como tal.
  - b) Para ver más información acerca de alguno de los procesos que se ejecutan en el *Administrador de tareas*, hacer clic con el botón derecho del ratón en el proceso y, a continuación, hacer clic en *Propiedades*. En el cuadro de diálogo *Propiedades*, se puede ver información general acerca del proceso, incluidos la ubicación y el tamaño. Hacer clic en la ficha *Detalles* para ver información detallada acerca del proceso.

También se puede ver qué servicios están asociados a un proceso. Para ver qué servicios se están ejecutando en un proceso determinado, haga clic con el botón derecho

del ratón en un proceso y, a continuación, hacer clic en *Ir al servicio*. Los servicios asociados al proceso aparecen resaltados en la ficha *Servicios*.



Nombre	PID	Estado	Nombre de usuario	CPU	Memoria (...)	Descripción
ApplicationFrameHo...	2388	En ejecución	Usuario	00	3.164 K	Application Frame H
audiodg.exe	2352	En ejecución	SERVICIO LOCAL	00	4.400 K	Aislamiento de gráfic
browser_broker.exe	4348	En ejecución	Usuario	00	2.240 K	Browser_Broker
Calculator.exe	564	Suspendido	Usuario	00	24 K	Calculator
csrss.exe	344	En ejecución	SYSTEM	00	408 K	Proceso en tiempo d
csrss.exe	428	En ejecución	SYSTEM	00	512 K	Proceso en tiempo d
dasHost.exe	1760	En ejecución	SERVICIO LOCAL	00	732 K	Device Association F
dwm.exe	752	En ejecución	DWM-1	00	22.448 K	Administrador de ve
explorer.exe	2764	En ejecución	Usuario	00	11.220 K	Explorador de Windo
FlashUtil_ActiveX.exe	3124	En ejecución	Usuario	00	3.432 K	Adobe® Flash® Play
Interrupciones del si...	-	En ejecución	SYSTEM	02	0 K	Llamadas a procedin
KMS-R@1n.exe	1348	En ejecución	Servicio de red	00	412 K	KMS-R@1n
lsass.exe	532	En ejecución	SYSTEM	00	3.888 K	Local Security Autho
MicrosoftEdge.exe	1960	En ejecución	Usuario	00	10.544 K	Microsoft Edge
MicrosoftEdgeCP.exe	4364	En ejecución	Usuario	00	2.392 K	Microsoft Edge Cont
MicrosoftEdgeCP.exe	2652	En ejecución	Usuario	12	304.792 K	Microsoft Edge Cont
MsMpEng.exe	1500	En ejecución	SYSTEM	00	24.788 K	Antimalware Service
NisSrv.exe	2512	En ejecución	SERVICIO LOCAL	00	2.736 K	Microsoft Network R
OneDrive.exe	3684	En ejecución	Usuario	00	2.152 K	Microsoft OneDrive
PeopleApp.exe	2120	Suspendido	Usuario	00	24 K	PeopleApp.exe
Proceso inactivo del ...	0	En ejecución	SYSTEM	86	4 K	Porcentaje de tiempo

Figura 23.- Lista de procesos en la ficha Detalle

Si un programa que se ejecuta en el equipo deja de responder, Windows trata de identificar el problema y corregirlo automáticamente. Si no se quiere esperar, se puede finalizar el programa con el *Administrador de tareas*.

El uso del Administrador de tareas para finalizar un programa manualmente puede ser más rápido que esperar, pero se pierden todos los cambios que no se hayan guardado. Si tiene trabajo importante que se desea conservar, esperar unos minutos y deje que Windows trate de corregir el problema.

Para finalizar un programa que no responde:

1. Abrir el *Administrador de tareas*.
2. Hacer clic en *Mas detalles*.
3. Hacer clic en el proceso que no responde y, a continuación, en el botón *Finalizar tarea*.

### 4.1.1 Inicio de programas

Desde el *Administrador de tareas* podemos ver los programas que se cargan durante el arranque del sistema. Podemos acelerar el arranque del PC si eliminamos aquellos que tienen un impacto alto sobre

Seguir los siguiente pasos:

1. Abrir el *Administrador de Tareas*.
2. Hacer clic en la ficha *Inicio* para ver los programas que se ponen en marcha automáticamente cuando arranca Windows.
3. En la columna *Impacto de Inicio*, buscan los programas marcados como Alto o Medio. Esto significa que tardan en ponerse en marcha y ralentizan el arranque. Aquellos que no uses a menudo, puedes desactivarlos. No necesitas que arranquen cada vez que se pone en marcha el ordenador. Por ejemplo, iTunes, Adobe Reader o el escáner de documentos.
4. Para desactivarlos, hacer clic con el botón derecho sobre la aplicación y selecciona *Deshabilitar* o hacer clic en el botón *Deshabilitar* en la parte inferior. No te preocupes, cuando los necesites funcionarán sin problemas.

## 4.2 Programador de tareas

Si se usa un programa específico con una frecuencia determinada, se puede usar el programador de tareas para crear una tarea que abra el programa automáticamente de acuerdo con la programación que se elija. Por ejemplo, podríamos programar una tarea para que cada quince días se ejecutara el desfragmentador de disco. También podemos programar un apagado automático todos los días a determinada hora. Estos programas generalmente no tienen interactividad con el usuario.

1. Abrir el *Programador de tareas* en el menú *Inicio* → *Todos los programas* → *Herramientas administrativas*.
2. Hacer clic en el menú *Acción* y luego en *Crear tarea básica*.
3. Escribir un nombre para la tarea y, si se desea, una descripción y hacer clic en el botón *Siguiente*.
4. Realizar una de estas acciones:
  - a) Para seleccionar una programación basándose en el calendario, hacer clic en *Diariamente*, *Semanalmente*, *Mensualmente* o *Una vez*, hacer clic en *Siguiente*, especificar la programación que se desea usar y hacer clic en el botón *Siguiente*.
  - b) Para seleccionar una programación basándose en eventos repetitivos, hacer clic en *Al iniciarse el equipo* o *Al iniciar la sesión* y, a continuación, hacer clic en el botón *Siguiente*.
  - c) Para seleccionar una programación basándose en eventos específicos, hacer clic

en *Cuando se registre un evento específico*, hacer clic en el botón *Siguiente*, especificar el registro de eventos y otros datos mediante las listas desplegables y, a continuación, hacer clic en el botón *Siguiente*.

5. Para programar una aplicación para que se inicie automáticamente, hacer clic en *Iniciar un programa* y, a continuación, en el botón *Siguiente*.
6. Hacer clic en el botón *Examinar* para buscar el programa que se desea iniciar. Si conocemos el nombre del ejecutable podemos escribirlo directamente. Si el programa recibe argumentos tenemos que rellenar el cuadro *Agregar argumentos (opcional)* y después hacer clic en el botón *Siguiente*.
7. Hacer clic en el botón *Finalizar*.

El ejemplo siguiente ejecuta el comando `shutdown` para apagar el equipo a las 15:00 horas de cada día.

Asistente para crear tareas básicas

Resumen

Crear una tarea básica

Desencadenar

Diariamente

Acción

Iniciar un programa

Finalizar

Nombre: Apagado automático

Descripción:

Desencadenador: Diariamente; A las 15:00 todos los días

Acción: Iniciar un programa; shutdown /s /t 120 /c "Apagado de equipo. Guada

☐ Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar

Al hacer clic en Finalizar, la nueva tarea se creará y se agregará a su programación de Windows.

< Atrás Finalizar Cancelar

Figura 24.- Apagado automático

Una vez hemos programado una tarea podemos visualizarla en la lista de tareas programadas.

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora última ejecución	Resultado de última ejecución
Apagado automático	Listo	A las 15:00 todos los días	20/08/2016 15:00:00	30/11/1999 0:00:00	La tarea no se ha ejecutado todavía.
OneDrive Standalone Update Task	Listo	A las 4:00 el 01/05/1992 - Tras...	20/08/2016 11:46:37	30/11/1999 0:00:00	La tarea no se ha ejecutado todavía.

Figura 25.- Lista de tareas programadas

En cualquier momento podemos editar las propiedades de la tarea programada haciendo doble clic sobre ella. Aparecerá una ventana en la que podremos modificar la configuración de la tarea. Podemos cambiar la frecuencia, hora de ejecución, usuario que ejecuta la tarea, etc.

Propiedades de Apagado automático (Equipo local)

General | Desencadenadores | Acciones | Condiciones | Configuración | Historial (deshabilitado)

Nombre: Apagado automático

Ubicación: \

Autor: PC00\Usuario

Descripción:

Opciones de seguridad

Al ejecutar la tarea, usar esta cuenta de usuario:

Usuario Cambiar usuario o grupo...

☒ Ejecutar solo cuando el usuario haya iniciado sesión

☐ Ejecutar tanto si el usuario inició sesión como si no

☐ No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.

☐ Ejecutar con los privilegios más altos

☐ Oculta

Configurar para: Windows Vista™, Windows Server™ 2008

Aceptar Cancelar

Figura 26.- Propiedades de una tarea programada

Una vez se han modificado los datos de la tarea programada, hacemos clic en el botón *Aceptar*.

### 4.3 Servicios

Un servicio es un tipo de aplicación que se ejecuta en segundo plano en el sistema, sin interactividad con el usuario, y es similar a un proceso demonio de UNIX. Los servicios

proporcionan una funcionalidad a los usuarios, como servicios web, servicios de archivos, impresión, etc.

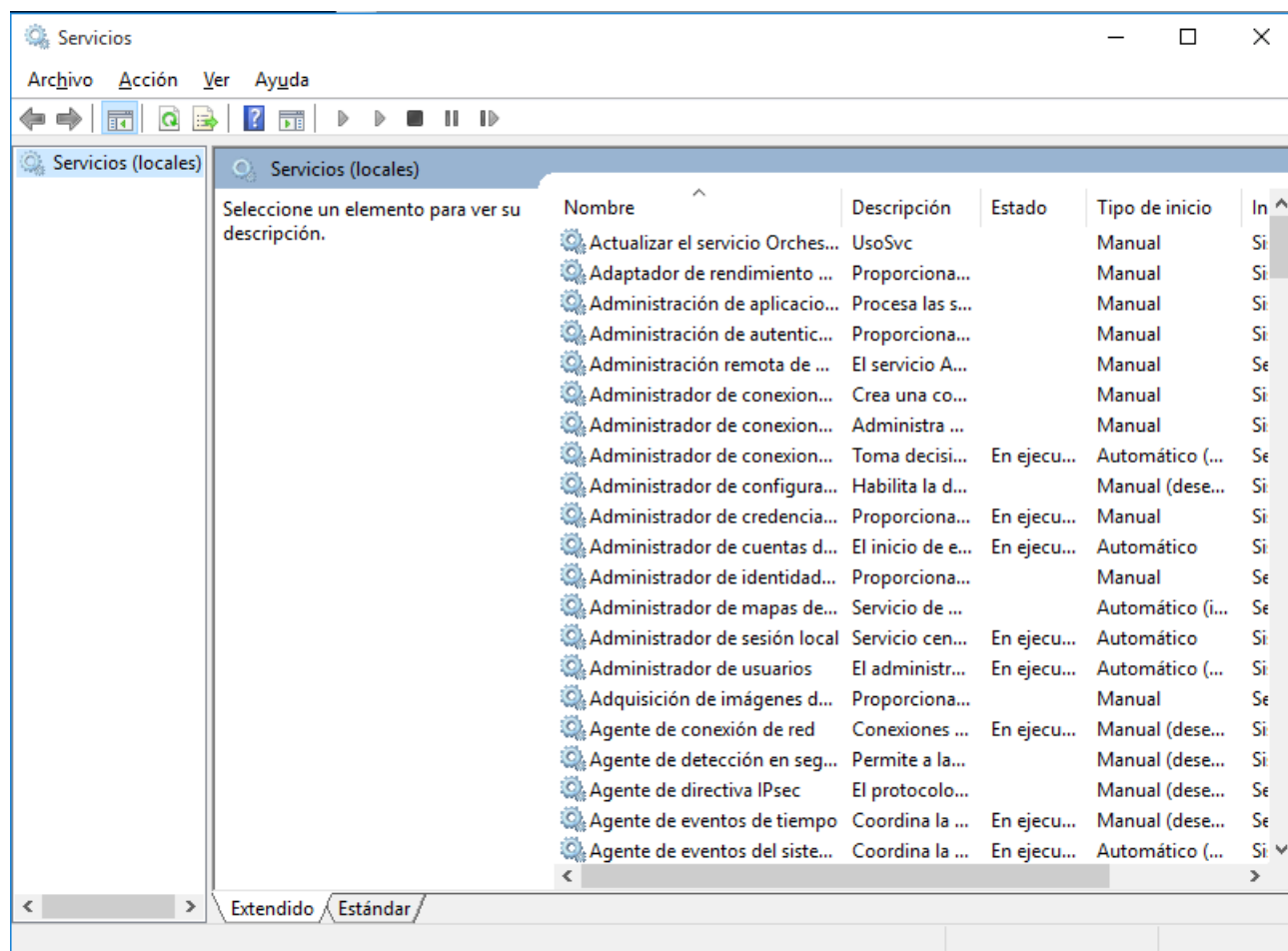


Figura 27.- Servicios

Para gestionar los servicios tenemos el complemento *Servicios* en las *Herramientas administrativas* del *Panel de control*. Con esta herramienta podemos hacer lo siguiente:

- ✓ Iniciar, detener, pausar, reanudar o deshabilitar servicios.
- ✓ Configurar acciones de recuperación para llevar a cabo si se produce un error en un servicio; por ejemplo, reiniciar el servicio automáticamente o reiniciar el equipo.
- ✓ Ejecutar servicios en el contexto de seguridad de una cuenta de usuario distinta de la del usuario que ha iniciado sesión o de la cuenta de equipo predeterminada.
- ✓ Habilitar o deshabilitar servicios para un perfil de hardware específico.
- ✓ Exportar y guardar información de servicio en un archivo .txt o .csv.
- ✓ Ver el estado y la descripción de cada servicio.
- ✓ Ver las dependencias de servicios.



### 4.3.1 Iniciar o parar un servicio

Es posible que deseemos iniciar un servicio porque lo necesitamos y por defecto tiene un arranque manual. Por ejemplo, el servicio de compatibilidad de Bluetooth permite a Windows detectar y configurar dispositivos que emplean esta tecnología inalámbrica. Para ello seguir los siguientes pasos:

1. Hacer doble clic sobre el servicio para editar sus propiedades.
2. Hacer clic en el botón *Iniciar*.
3. Si queremos que a partir de ahora el servicio se ponga en marcha automáticamente cada vez que se inicie el equipo, en la lista *Tipo de inicio* elegimos *Automático* o *Automático (inicio retrasado)*.
4. Hacemos clic en el botón *Aceptar*.

Si queremos parar el servicio repetiremos los pasos pero haciendo clic en el botón *Detener* y poniendo el *Tipo de inicio* a *Deshabilitado* o *Manual*. Los servicios con inicio *Manual* pueden iniciarse o detenerse desde aquí cuando se necesitan.

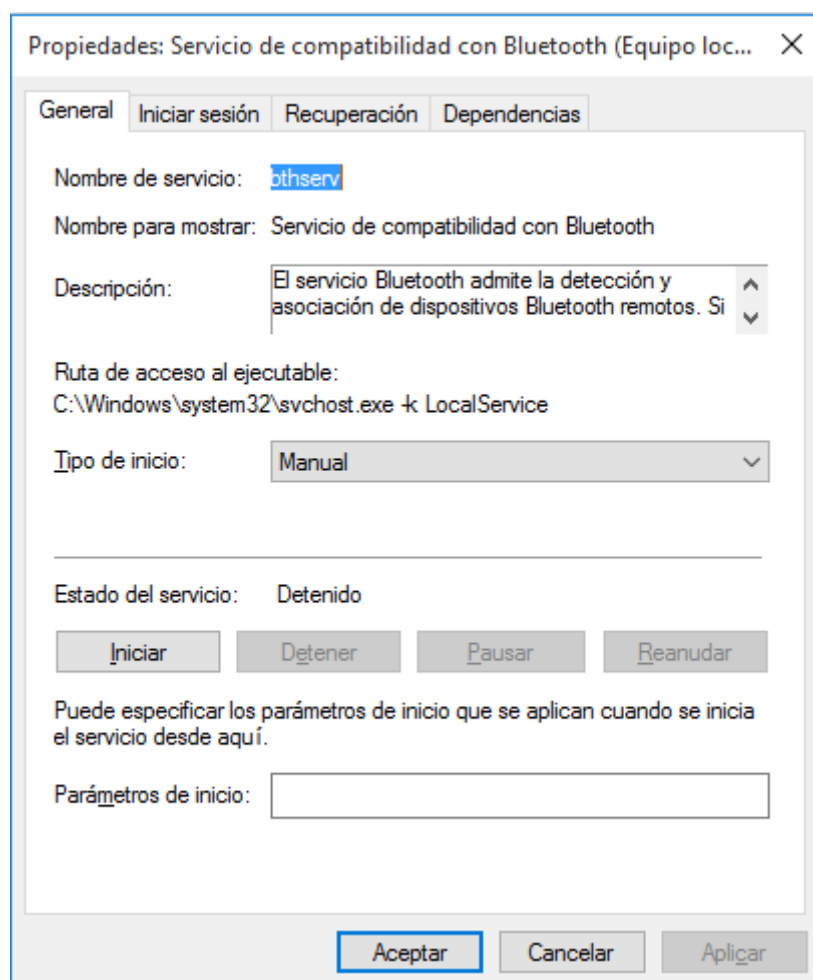


Figura 28.- Propiedades de servicio

Hay que tener mucho cuidado al detener o deshabilitar un servicio ya que puede tener

dependencias con otros. Un servicio depende de otro cuando para que el primero se inicie es necesario que el segundo esté iniciado.

En la ficha *Dependencias* de las propiedades del servicio podemos ver los servicios de los que depende y aquellos que dependen de él.

Por ejemplo en la siguiente imagen aparecen las dependencias del servicio *Servidor* el cual se encarga de gestionar las peticiones de recursos (archivos o impresión) desde la red.

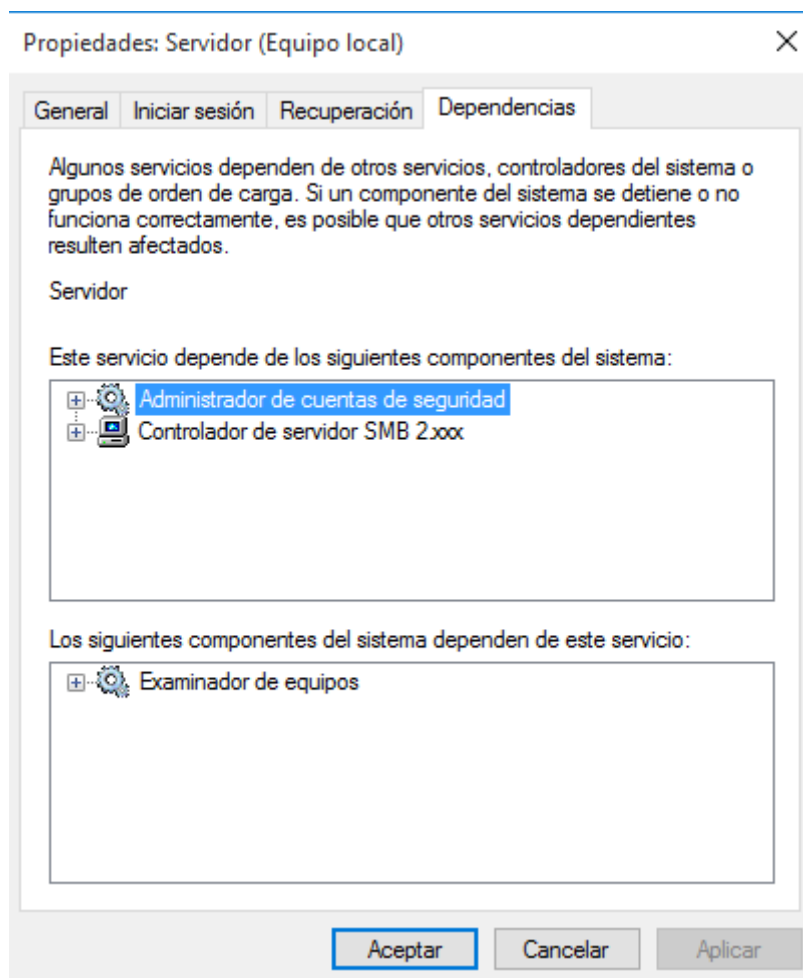


Figura 29.- Dependencias de servicios

## 4.4 Gestión de procesos en el símbolo del sistema

Los siguientes comandos se emplean para tareas generales de mantenimiento del sistema.

### 4.4.1 Listado de procesos. Comando tasklist

Visualiza un listado de los procesos actualmente en ejecución en el sistema.

```
tasklist [{/m <módulo> | /svc | /v}] [/fo {table | list | csv}]
[/fi <filtro> [/fi <filtro> [ ... ]]]
```

Parámetro	Descripción
/m <módulo>	Lista todas las tareas con los módulos DLL cargados que coinciden con el nombre dado. Si no se especifica un módulo, esta opción visualiza todos los módulos cargados por cada tarea.
/svc	Lista todos los servicios para cada proceso.
/v	Visualiza información adicional en el listado de tareas.
/fo {table   list   csv}	Especifica el formato de la salida. Por defecto es table.
/fi <filtro>	Especifica el tipo de proceso para incluir o excluir en la consulta. Ver la siguiente tabla para nombres, operadores y valores de filtros válidos.

Esta tabla establece los filtros a utilizar con la opción /fi.

Nombre de filtro	Operadores	Valores
STATUS	eq, ne	RUNNING   NOT RESPONDING   UNKNOWN
IMAGENAME	eq, ne	Nombre de imagen
PID	eq, ne, gt, lt, ge, le	Valor de PID
SESSION	eq, ne, gt, lt, ge, le	Número de sesión
SESSIONNAME	eq, ne	Nombre de sesión
CPUTIME	eq, ne, gt, lt, ge, le	Tiempo de la CPU en formato <i>HH:MM:SS</i>
MEMUSAGE	eq, ne, gt, lt, ge, le	Uso de memoria en KB
USERNAME	eq, ne	Nombre de usuario
SERVICES	eq, ne	Nombre de servicio
WINDOWTITLE	eq, ne	Título de ventana
MODULES	eq, ne	Nombre DLL

#### 4.4.2 Terminar un proceso. Comando taskkill

Termina con la ejecución de procesos o tareas, las cuales se pueden identificar mediante su PID o por su nombre.

```
taskkill [/fi <filtro>] [...] [/pid <ID de proceso> | /im <nombre>] [/f] [/t]
```

Parámetro	Descripción
/fi <filter>	Aplica un filtro para seleccionar un conjunto de tareas. Puede usar más de un filtro o usar el carácter comodín (*) para especificar todas las tareas o nombres de imagen. Los filtros válidos se enumeran en la sección <b>Nombres, operadores y valores de filtro</b> de este artículo.
/pid <processID>	Especifica el id. de proceso del proceso que se va a finalizar.
/im <imagename>	Especifica el nombre de imagen del proceso que se va a finalizar. Use el carácter comodín (*) para especificar todos los nombres de imagen.
/f	Especifica que los procesos se forzaron a finalizar. Este parámetro se omite para los procesos remotos; todos los procesos remotos se fuerzan a finalizar.
/t	Finaliza el proceso especificado y los procesos secundarios iniciados por él.

#### 4.4.3 Tareas programadas. Comando schtasks

La herramienta **schtasks.exe** realiza las mismas operaciones que las **tareas programadas** en el **panel de control**. Puede usar estas herramientas conjunta e indistintamente.

##### Permisos necesarios

- Para programar, ver y cambiar todas las tareas del equipo local, debe ser miembro del grupo Administradores.
- Para programar, ver y cambiar todas las tareas del equipo remoto, debe ser miembro del grupo Administradores en el equipo remoto, o bien debe usar el parámetro **/u** para proporcionar las credenciales de un administrador del equipo remoto.
- Puede usar el parámetro **/u** en una operación **/create** o **/change** si los equipos local y remoto están en el mismo dominio, o si el equipo local está en un dominio en el que confía el dominio del equipo remoto. De lo contrario, el equipo remoto no puede autenticar la cuenta de usuario especificada y no puede comprobar que la cuenta sea miembro del grupo Administradores.
- La tarea que tiene previsto ejecutar debe tener el permiso adecuado; estos permisos varían según la tarea. De forma predeterminada, las tareas se ejecutan con los permisos del usuario actual del equipo local o con los permisos del usuario especificado por el parámetro **/u**, si se incluye uno. Para ejecutar una tarea con permisos de una cuenta de usuario diferente o con permisos del sistema, use el parámetro **/ru**.

## Sintaxis

```
schtasks /change  
schtasks /create  
schtasks /delete  
schtasks /end  
schtasks /query  
schtasks /run
```

Parámetro	Descripción
<code>schtasks change</code>	Cambia una o varias de las siguientes propiedades de una tarea: <ul style="list-style-type: none"><li>• Programa que la tarea ejecuta (/tr)</li><li>• Cuenta de usuario con la que se ejecuta la tarea (/ru)</li><li>• Contraseña de la cuenta de usuario (/rp)</li><li>• Agrega la propiedad interactive-only a la tarea (/it)</li></ul>
<code>schtasks create</code>	Programa una nueva tarea.
<code>schtasks delete</code>	Elimina una tarea programada.
<code>schtasks end</code>	Detiene un programa iniciado por una tarea.
<code>schtasks query</code>	Muestra las tareas programadas para ejecutarse en el equipo.
<code>schtasks run</code>	Inicia inmediatamente una tarea programada. La operación <b>run</b> omite la programación, pero usa la ubicación del archivo de programa, la cuenta de usuario y la contraseña guardadas en la tarea para ejecutar la tarea inmediatamente.

### 4.4.4 schtasks create

```
schtasks /create /sc <scheduledtype> /tn <taskname> /tr <taskrun> [/s  
<computer> [/u [<domain>\]<user> [/p <password>]]] [/ru  
{[<domain>\]<user> | system}] [/rp <password>] [/mo <modifier>] [/d  
<day>[,<day>...] | *] [/m <month>[,<month>...]] [/i <idletime>] [/st  
<starttime>] [/ri <interval>] [{/et <endtime> | /du <duration>}  
[/k]] [/sd <startdate>] [/ed <enddate>] [/it] [/np] [/z] [/xml  
<xmlfile>] [/v1] [/f] [/rl <level>] [/delay <delaytime>] [/hresult]
```

## Parámetro

/SC <scheduletype>

## Descripción

Especifica el tipo de programación. Los valores válidos incluyen:

- **MINUTE:** especifica el número de minutos antes de que se ejecute la tarea.
- **HOURLY:** especifica el número de horas antes de que se ejecute la tarea.
- **DAILY:** especifica el número de días antes de que se ejecute la tarea.
- **WEEKLY:** especifica el número de semanas antes de que se ejecute la tarea.
- **MONTHLY:** especifica el número de meses antes de que se ejecute la tarea.
- **ONCE:** especifica que esa tarea se ejecuta una vez en una fecha y hora especificadas.
- **ONSTART:** especifica que la tarea se ejecuta cada vez que se inicia el sistema. Puede especificar una fecha de inicio o ejecutar la tarea la próxima vez que se inicie el sistema.
- **ONLOGON:** especifica que la tarea se ejecuta cada vez que un usuario (cualquier usuario) inicia sesión. Puede especificar una fecha o ejecutar la tarea la próxima vez que el usuario inicie sesión.
- **ONIDLE:** especifica que la tarea se ejecuta cada vez que el sistema permanece inactivo durante un período de tiempo especificado. Puede especificar una fecha o ejecutar la tarea la próxima vez que el sistema se quede inactivo.
- **ONEVENT:** especifica que la tarea se ejecuta en función de un evento que coincide con la información del registro de eventos del sistema, incluido EventID.

/tn <taskname>

Especifica un nombre para la tarea. Cada tarea del sistema debe tener un nombre único y debe cumplir las reglas para los nombres de archivo, sin superar los 238 caracteres. Use comillas para incluir nombres que incluyan espacios. Para almacenar la tarea programada en otra carpeta, ejecute **/tn**<folder name\task name>.

/tr <Taskrun>

Especifica el programa o comando que ejecuta la tarea. Escriba la ruta de acceso completa y el nombre de archivo de un archivo ejecutable, un archivo de script o un archivo por lotes. El nombre de la ruta de acceso no debe superar los 262 caracteres. Si no agrega la ruta de acceso, **schtasks** asume que

Parámetro	Descripción
<code>/ru</code> <code>{[&lt;domain&gt;]&lt;user&gt;   system}</code>	<p>el archivo está en el directorio <code>&lt;systemroot&gt;\System32</code>.</p> <p>Ejecuta la tarea con permisos de la cuenta de usuario especificada. De forma predeterminada, la tarea se ejecuta con los permisos del usuario actual del equipo local o con los permisos del usuario especificado por el parámetro <b>/u</b>, si se incluye uno. El parámetro <b>/ru</b> es válido al programar tareas en equipos locales o remotos. Las opciones válidas incluyen:</p> <ul style="list-style-type: none"><li>• <b>Domain</b>: especifica una cuenta de usuario alternativa.</li><li>• <b>System</b>: especifica la cuenta del sistema local, una cuenta con privilegios elevados que el sistema operativo y los servicios del sistema usan.</li></ul>
<code>/rp &lt;password&gt;</code>	<p>Especifica la contraseña para la cuenta de usuario existente o la cuenta de usuario especificada por el parámetro <b>/ru</b>. Si no usa este parámetro al especificar una cuenta de usuario, SchTasks.exe le pedirá la contraseña la próxima vez que inicie sesión. No use el parámetro <b>/rp</b> para las tareas que se ejecutan con credenciales de cuenta del sistema (<b>/ru System</b>). La cuenta del sistema no tiene una contraseña y SchTasks.exe no solicita una.</p>
<code>/mo &lt;modifiers&gt;</code>	<p>Especifica la frecuencia con la que se ejecuta la tarea dentro de su tipo de programación. Las opciones válidas incluyen:</p> <ul style="list-style-type: none"><li>• <b>MINUTE</b>: especifica que la tarea se ejecuta cada <code>&lt;n&gt;</code> minutos. Puede usar cualquier valor entre 1 y 1439 minutos. De forma predeterminada, es 1 minuto.</li><li>• <b>HOURLY</b>: especifica que la tarea se ejecuta cada <code>&lt;n&gt;</code> horas. Puede usar cualquier valor entre 1 y 23 minutos. De forma predeterminada, es 1 hora.</li><li>• <b>DAILY</b>: especifica que la tarea se ejecuta cada <code>&lt;n&gt;</code> días. Puede usar cualquier valor entre 1 y 365 días. De forma predeterminada, es 1 día.</li><li>• <b>WEEKLY</b>: especifica que la tarea se ejecuta cada <code>&lt;n&gt;</code> semanas. Puede usar cualquier valor entre 1 y 52 días. De forma predeterminada, es 1 semana.</li><li>• <b>MONTHLY</b>: especifica que la tarea se ejecuta cada <code>&lt;n&gt;</code> meses. Puede usar cualquiera de los valores siguientes:<ul style="list-style-type: none"><li>○ Un número entre 1 y 12 meses</li><li>○ <b>LASTDAY</b>: para ejecutar la tarea el último día del mes</li><li>○ <b>FIRST, SECOND, THIRD o FOURTH junto con el parámetro /d &lt;day&gt;</b>: especifica la semana y el día concretos para ejecutar la tarea. Por ejemplo, el tercer miércoles del mes.</li></ul></li><li>• <b>ONCE</b>: especifica que la tarea se ejecuta una vez.</li></ul>

Parámetro	Descripción
	<ul style="list-style-type: none"><li>• <b>ONSTART</b>: especifica que la tarea se ejecuta en el inicio.</li><li>• <b>ONLOGON</b>: especifica que la tarea se ejecuta cuando el usuario especificado por el parámetro <b>/ru</b> inicia sesión.</li><li>• <b>ONIDLE</b>: especifica que la tarea se ejecuta después de que el sistema se quede inactivo durante el número de minutos especificado por el parámetro <b>/i</b>.</li></ul>
<b>/d DAY[,DAY...]</b>	<p>Especifica la frecuencia con la que se ejecuta la tarea dentro de su tipo de programación. Las opciones válidas incluyen:</p> <ul style="list-style-type: none"><li>• <b>WEEKLY</b>: especifica que la tarea se ejecuta semanalmente proporcionando un valor entre 1 y 52 semanas. Opcionalmente, también puede agregar un día específico de la semana agregando un valor de MON a SUN o un intervalo de [MON a SUN...].</li><li>• <b>MONTHLY</b>: especifica que la tarea se ejecuta semanalmente cada mes proporcionando un valor entre FIRST, SECOND, THIRD, FOURTH y LAST. Opcionalmente, también puede agregar un día específico de la semana agregando un valor de MON a SUN o proporcionando un número entre 1 y 12 meses. Si usa esta opción, también puede agregar un día específico del mes proporcionando un número entre 1 y 31.</li></ul> <p><b>NOTA:</b> el valor de fecha de 1 a 31 solo es válido sin el parámetro <b>/mo</b> o si el parámetro <b>/mo</b> es mensual (de 1 a 12). El valor predeterminado es el día 1 (el primer día del mes).</p>
<b>/m MONTH[,MONTH...]</b>	<p>Especifica un mes o meses del año durante el cual se debe ejecutar la tarea programada. Las opciones válidas incluyen JAN - DEC y * (cada mes). El parámetro <b>/m</b> solo es válido con una programación de tipo MONTHLY. Es necesario cuando se usa el modificador LASTDAY. De lo contrario, es opcional y el valor predeterminado es * (cada mes).</p>
<b>/i &lt;Idletime&gt;</b>	<p>Especifica cuántos minutos está inactivo el equipo antes de que se inicie la tarea. Un valor válido es un número entero de 1 a 999. Este parámetro solo es válido con una programación de tipo ONIDLE y, a continuación, es necesario.</p>
<b>/st &lt;Starttime&gt;</b>	<p>Especifica la hora de inicio de la tarea, para lo que se utiliza el formato de hora de 24 horas, HH:mm. El valor predeterminado es la hora actual del equipo local. El parámetro <b>/st</b> es válido con las programaciones MINUTE, HOURLY, DAILY, WEEKLY, MONTHLY y ONCE. Es necesario para una programación ONCE.</p>
<b>/ri &lt;interval&gt;</b>	<p>Especifica el intervalo de repetición de la tarea programada, en</p>



Parámetro	Descripción
	minutos. Esto no es aplicable para los tipos de programación MINUTE, HOURLY, ONSTART, ONLOGON, ONIDLE y ONEVENT. El intervalo válido es de 1 a 599940 (599940 minutos = 9999 horas). Si se especifican los parámetros <b>/et</b> o <b>/du</b> , el valor predeterminado es <b>10 minutos</b> .
<b>/et</b> <endtime>	Especifica la hora del día a la que finaliza una programación de tareas por minuto u hora en formato de 24 horas <HH:MM>. Después de la hora de finalización especificada, schtasks no vuelve a iniciar la tarea hasta que se repite la hora de inicio. De forma predeterminada, las programaciones de tareas no tienen ninguna hora de finalización. Este parámetro es opcional y válido solo con una programación de tipo MINUTE u HOURLY.
<b>/du</b> <duration>	Especifica un período máximo de tiempo durante una programación por minuto o por hora en formato de 24 horas <HHHH:MM>. Una vez transcurrida la hora especificada, schtasks no vuelve a iniciar la tarea hasta que se repite la hora de inicio. De forma predeterminada, las programaciones de tareas no tienen duración máxima. Este parámetro es opcional y válido solo con una programación de tipo MINUTE u HOURLY.
<b>/k</b>	Detiene el programa que la tarea ejecuta en el momento especificado por <b>/et</b> o <b>/du</b> . Sin <b>/k</b> , schtasks no vuelve a iniciar el programa después de alcanzar la hora especificada por <b>/et</b> o <b>/du</b> , ni lo detiene si aún se está ejecutando. Este parámetro es opcional y válido solo con una programación de tipo MINUTE u HOURLY.
<b>/sd</b> <Startdate>	Especifica la fecha en la que se inicia la programación de la tarea. El valor predeterminado es la fecha actual del equipo local. El formato de <b>Startdate</b> varía con la configuración regional seleccionada para el equipo local en <b>Configuración regional y de idioma</b> . Solo un formato es válido para cada configuración regional. Los formatos de fecha válidos incluyen (asegúrese de elegir el formato más similar al formato seleccionado para <b>Fecha corta</b> en <b>Configuración regional y de idioma</b> en el equipo local): <ul style="list-style-type: none"> <li>• &lt;MM&gt;//: especifica el uso para formatos de mes primero, como inglés (Estados Unidos) y español (Panamá).</li> <li>• &lt;DD&gt;//: especifica el uso para formatos de día primero, como búlgaro y neerlandés (Países Bajos).</li> <li>• &lt;YYYY&gt;//: especifica el uso para formatos de año primero, como sueco y francés (Canadá).</li> </ul>
<b>/ed</b> <Enddate>	Especifica la fecha en la que finaliza la programación. Este parámetro es opcional. No es válido en una programación de

Parámetro	Descripción
	<p>tipo ONCE, ONSTART, ONLOGON, ONIDLE u ONEVENT. De forma predeterminada, las programaciones no tienen fecha de finalización. El valor predeterminado es la fecha actual del equipo local. El formato de <b>Enddate</b> varía con la configuración regional seleccionada para el equipo local en <b>Configuración regional y de idioma</b>. Solo un formato es válido para cada configuración regional. Los formatos de fecha válidos incluyen (asegúrese de elegir el formato más similar al formato seleccionado para <b>Fecha corta</b> en <b>Configuración regional y de idioma</b> en el equipo local):</p> <ul style="list-style-type: none"> <li>• &lt;MM&gt;//: especifica el uso para formatos de mes primero, como inglés (Estados Unidos) y español (Panamá).</li> <li>• &lt;DD&gt;//: especifica el uso para formatos de día primero, como búlgaro y neerlandés (Países Bajos).</li> <li>• &lt;YYYY&gt;//: especifica el uso para formatos de año primero, como sueco y francés (Canadá).</li> </ul>
/ec <channelname>	Especifica el nombre del canal de eventos desencadenado por el tipo de programación ONEVENT que coincide con los criterios de un registro de eventos del sistema.
/it	Especifica que se ejecute la tarea programada solo cuando Ejecutar como usuario (la cuenta de usuario en la que se ejecuta la tarea) haya iniciado sesión en el equipo. Este parámetro no tiene ningún efecto en las tareas que se ejecutan con permisos del sistema o en las tareas que ya tienen establecida la propiedad interactive-only. No se puede usar un comando change para quitar la propiedad interactive-only de una tarea. De forma predeterminada, Ejecutar como usuario es el usuario actual del equipo local cuando la tarea se programa o la cuenta se especifica mediante el parámetro <b>/u</b> , si se usa uno. Sin embargo, si el comando incluye el parámetro <b>/ru</b> , Ejecutar como usuario es la cuenta especificada por el parámetro <b>/ru</b> .
/np	No se almacena ninguna contraseña. La tarea se ejecuta de forma no interactiva como el usuario especificado. Solo están disponibles los recursos locales.
/z	Especifica la eliminación de la tarea tras la finalización de su programación.
/xml <xmlfile>	Crea una tarea especificada en el archivo XML. Se puede combinar con los parámetros <b>/ru</b> y <b>/rp</b> , o bien con el parámetro <b>/rp</b> por sí solo si el archivo XML ya contiene la información de la cuenta de usuario.
/v1	Crea una tarea visible para los sistemas operativos anteriores a Vista. Esto no es compatible con el parámetro <b>/XML</b> .

Parámetro	Descripción
/f	Especifica la creación de la tarea y la supresión de las advertencias si la tarea especificada ya existe.
/rl <level>	Especifica el nivel de ejecución del trabajo. Los valores aceptables son <b>LIMITED</b> (las tareas programadas se ejecutarán con el menor nivel de privilegios, como las cuentas de usuario estándar) y <b>HIGHEST</b> (las tareas programadas se ejecutarán con el nivel más alto de privilegios, como las cuentas de superusuario). El valor predeterminado es <b>Limited</b> .
/delay <delaytime>	Especifica el tiempo de espera para retrasar la ejecución de la tarea después de desencadenarse en formato mmmm:ss. Esto solo es válido para los tipos de programación ONSTART, ONLOGON y ONEVENT.
/hresult	Especifica que el código de salida del proceso esté en formato HRESULT.
/?	Muestra la ayuda en el símbolo del sistema.

### Ejemplos de creación de tareas

<https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/schtasks-create>

#### 4.4.5 Apagado y reinicio del sistema. Comando shutdown

Apaga, reinicia o hiberna el equipo local. Tiene argumentos para planificar en tiempo el apagado o reinicio, un cierre de sesión además de forzar el apagado de aplicaciones. También se usa para documentar un cierre inesperado del sistema.

```
shutdown [/i | /l | /s | /r | /a | /p | /h | /e] [/f] [/m \\<PC>] [/t <xxx>]
```

Parámetro	Descripción
/i	Visualiza el cuadro de diálogo de apagado remoto. Debe ser el primer parámetro. Si se especifica todas las demás opciones se ignoran.
/l	Cierra la sesión del usuario actual inmediatamente
/s	Apaga el ordenador.
/r	Reinicia el ordenador
/a	Aborta el apagado del sistema. Solamente efectivo durante el periodo de gracia.
/p	Apaga el ordenador sin periodo de gracia ni aviso.

/h	Hiberna el ordenador.
/e	Te permite documentar la razón inesperada por la que se apaga el ordenador.
/f	Fuerza a las aplicaciones en ejecución a cerrarse sin avisar al usuario. Podría provocar la pérdida de datos sin guardar.
/m \\<PC>	Indica el ordenador a apagar.
/t <XXX>	Establece un periodo de gracia de XXX segundos antes de apagar o reiniciar el ordenador. Se visualizará un mensaje de aviso en la consola local. Se puede especificar entre 0 y 600 segundos. Por defecto son 30 segundos.

## 4.5 Gestión de servicios en el símbolo del sistema

Para la gestión de los servicios del sistema disponemos de los siguientes comandos.

### 4.5.1 Comando net

El comando net se emplea para gestionar el funcionamiento de los servicios del sistema. Con este comando podemos listar, parar, iniciar, pausar, reanudar y reiniciar un servicio del sistema.

net { START   STOP   PAUSE   CONTINUE } [<servicio>]	
Parámetro	Descripción
START	Inicia el servicio
STOP	Para el servicio
PAUSE	Suspende un servicio.
CONTINUE	Reanuda un servicio.
<servicio>	Nombre del servicio. Si tiene espacios en blanco hay que encerrarlo entre comillas dobles.

### 4.5.2 Comando sc

El comando sc se emplea para comunicarse con el administrador de los servicios del sistema. Con este comando se pueden crear, borrar, consultar, arrancar y parar los servicios.

sc [\\<servidor>] [<comando>] [<servicio>] [<opciones>]	
Parámetro	Descripción
\\servidor	Servidor donde se realizará la operación.

comando	Operación que se realiza con el servicio. Los principales comandos son: ✓ query.- Muestra el estado del servicio. ✓ start.- Inicia el servicio. ✓ stop.- Para el servicio. ✓ config.- Cambia la configuración del servicio.
servicio	Nombre del servicio que se gestiona. Si tiene espacios en blanco tiene que encerrarse entre comillas dobles.
opciones	Opciones del comando empleado. Para ver una referencia podemos ejecutar <code>sc comando /?</code> .
<servicio>	Nombre del servicio. Si tiene espacios en blanco hay que encerrarlo entre comillas dobles.

## 4.6 Gestión de procesos en WPS

A continuación veremos un conjunto de cmdlets para gestionar los procesos del sistema.

### 4.6.1 Listar los procesos. Comando Get-Process

El cmdlet `Get-Process` muestra un listado con los procesos en ejecución del sistema.

<pre>Get-Process { [[-Name] &lt;String[]&gt;]   -Id &lt;Int32[]&gt;   -InputObject &lt;Process[]&gt; } [-Module] [-FileVersionInfo] [-IncludeUserName] [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
<code>-Name &lt;String[]&gt;</code>	Especifica uno o más procesos por su nombre. Pueden utilizarse metacaracteres.
<code>-Id &lt;Int32[]&gt;</code>	Especifica uno o más procesos por su ID.
<code>-InputObject &lt;Process[]&gt;</code>	Se especifica uno o más objetos de tipo proceso.

[Haz clic para obtener una referencia completa.](#)

Sin parámetros se listan todos los procesos. Podemos especificar un proceso en particular por su nombre o ID de proceso. Por defecto, este cmdlet devuelve un objeto proceso con información detallada acerca del mismo y soporta métodos que permiten comenzar y parar procesos. Podemos también usar los parámetros para obtener información de la versión del programa que lanza el proceso.

Los campos que lista son:

- ✓ Handles .- Número de manejadores asociados al proceso.

- ✓ NPM (K).- Cantidad de memoria no paginada en KB que emplea el proceso.
- ✓ PM (K).- Cantidad de memoria paginada en KB que emplea el proceso.
- ✓ WS (K).- Tamaño del conjunto de trabajo en KB del proceso.
- ✓ VM (M).- Cantidad de memoria virtual en MB que emplea el proceso.
- ✓ CPU(s).- Porcentaje de uso del tiempo de la CPU.
- ✓ Id.- Identificador del proceso
- ✓ SI.- Identificador de sesión. 0 para el sistema, 1 para el primer usuario logueado, ...
- ✓ ProcessName.- Nombre del proceso.

Veamos algunos ejemplos. Para obtener una lista completa de todos los procesos del sistema.

```
PS C:\> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
322	19	7484	22940	0,36	3896	1	ApplicationFrameHost
170	10	6320	11252	0,13	1916	0	audiodg
292	28	8888	24792	0,11	6032	1	backgroundTaskHost
...							

La lista es mucho más larga. Se ha cortado por razones de espacio. El siguiente cmdlet obtiene información sobre los procesos explorer y notepad.

```
PS C:\> Get-Process -Name explorer,notepad
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
2003	74	33540	82952	8,48	2728	1	explorer
234	14	2880	14032	0,08	4068	1	notepad

Podemos ver la versión de la aplicación que lanza el proceso.

```
PS C:\> Get-Process -Name notepad -FileVersionInfo
```

ProductVersion	FileVersion	FileName
10.0.17134.466	10.0.17134.46...	C:\Windows\system32\notepad.exe

Para ver todas las propiedades de un proceso tenemos que emplear el operador | para enviar el proceso al cmdlet Format-List que lista las propiedades de un objeto en formato de lista.

```
PS C:\> Get-Process -Name notepad | Format-List *
```

Name : notepad  
 Id : 4068  
 PriorityClass : Normal  
 FileVersion : 10.0.17134.466 (WinBuild.160101.0800)  
 HandleCount : 235  
 WorkingSet : 14159872  
 PagedMemorySize : 2768896  
 PrivateMemorySize : 2768896  
 VirtualMemorySize : 187875328  
 TotalProcessorTime : 00:00:00.0781250  
 SI : 1  
 Handles : 235  
 VM : 2203506098176  
 ...

También podemos listar un conjunto de procesos basándonos en los valores de alguna de sus propiedades. Para ello debemos combinar `Get-Process` con el cmdlet `Where-Object` el cual permite seleccionar objetos de una lista cuando cumple unas condiciones. Por ejemplo, vamos a listar los procesos que tienen una prioridad normal.

```
PS C:\> Get-Process | Where-Object -Property PriorityClass -eq -Value "Normal"
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
48	4	2224	2552	0,00	2908	1	cmd
236	13	7036	14452	0,17	2312	1	conhost
...							

En el siguiente ejemplo vemos las propiedades del proceso con la calculadora y usamos el argumento `-IncludeUserName` para que muestre el usuario que lo ha creado.

```
PS C:\> Get-Process -IncludeUserName calculator
```

Handles	WS(K)	CPU(s)	Id	UserName	ProcessName
523	44376	0,44	1112	PCW10\UsuarioCalculador	

#### 4.6.2 Parar un proceso. Comando Stop-Process

El cmdlet `Stop-Process` para uno o más procesos en ejecución. Podemos especificar el proceso por nombre, identificador de proceso (PID) o pasando un objeto proceso. `Stop-Process` solamente trabaja con procesos locales.

Los procesos que pueden pararse son los que ha lanzado el propio usuario que ejecuta `Stop-Process`. Para otros procesos hay que ejecutar PowerShell como

administrador. El proceso se para sin pedir confirmación salvo que se utilice el argumento -Confirm.

<pre>Stop-Process     { [-Id] &lt;Int32[]&gt;   -Name &lt;String[]&gt;   [-InputObject] &lt;Process[]&gt; }     [-PassThru]     [-Force]     [-whatIf]     [-Confirm]     [&lt;CommonParameters&gt;]</pre>	
--	--

Parámetro	Descripción
-Name <String[]>	Especifica uno o más procesos por su nombre. Pueden utilizarse metacaracteres.
-Id <Int32[]>	Especifica uno o más procesos por su ID.
-InputObject <Process[]>	Se especifica uno o más objetos de tipo proceso.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. Para parar el proceso asociado a la Calculadora.

```
PS C:\> Stop-Process -Name Calculator
```

Si una aplicación está bloqueada y queremos terminarla podemos usar el argumento -Force. Por ejemplo, el siguiente cmdlet finaliza el Administrador de Equipos.

```
PS C:\> Get-Process -Name mmc*
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
569	47	36648	14796	1,52	5804	1	mmc

```
PS C:\> Stop-Process -ID 5804
```

Si queremos ver previamente a su finalización el proceso que vamos a parar podemos emplear los argumentos -Confirm y -PassThru. El primero pide confirmación para finalizar el proceso mientras que el segundo visualiza las propiedades del proceso a parar. El siguiente ejemplo para el proceso del bloc de notas.

```
PS C:\> Stop-Process -Name notepad -Confirm -PassThru
```

Confirmar

¿Está seguro de que desea realizar esta acción?

Se está realizando la operación "Stop-Process" en el destino "notepad (4068)".

[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspende [?] Ayuda (el valor predeterminado es "S"):



Handles	NPM (K)	PM (K)	WS (K)	CPU (s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
229	13	2524	12916	0,08	4068	1	notepad

El siguiente ejemplo para el proceso cmd.exe.

```
PS C:\> $p = Get-Process -Name cmd
PS C:\> $p.Name
cmd
PS C:\> Stop-Process -InputObject $p
PS C:\> Get-Process | Where-Object {$_.hasExited}
PS C:\>
```

El primer comando usa `Get-Process` para obtener un objeto que representa al proceso `cmd` y luego lo almacena en la variable `$p`. Esta variable se pasa a `Stop-Process` que usa el parámetro `InputObject`. El último comando obtiene todos los procesos que se ejecutaron y se han parado. Para ello el resultado de `Get-Process` (todos los procesos) se pasa con el operador `|` al cmdlet `Where-Object` que selecciona los que tiene el valor de la propiedad `HasExited` a `$True`.

#### 4.6.3 Comenzar un proceso. Comandos `Start-Process`

El cmdlet `Start-Process` inicia uno o más procesos. Para especificar el programa que origina el proceso introduce un fichero ejecutable o un fichero de script. Si especificamos un archivo no ejecutable, `Start-Process` inicia el programa asociado al fichero.

Podemos usar los parámetros de `Start-Process` para especificar opciones, como la carga de un perfil de usuario, iniciar el proceso en una nueva ventana o utilizar credenciales de usuario diferentes a la del usuario que ha abierto sesión.

```
Start-Process
    [-FilePath] <String>
    [[-ArgumentList] <String[]>]
    [-Credential] <PSCredential>
```

```

[-WorkingDirectory <String>]
[-LoadUserProfile]
[-Verb <String>]
[-NoNewWindow]
[-PassThru]
[-RedirectStandardError <String>]
[-RedirectStandardInput <String>]
[-RedirectStandardOutput <String>]
[-windowStyle <ProcessWindowStyle>]
[-wait]
[-UseNewEnvironment]
[-whatIf]
[-Confirm]
[<CommonParameters>]

```

Parámetro	Descripción
-FilePath <String>	Especifica el path (opcional) y el archivo del programa que origina el proceso. Puede ser un archivo ejecutable o un documento que esté asociado a una aplicación.
-ArgumentList <String[]>	Especifica los valores de los parámetros. Si el valor de algún parámetro contiene un espacio en blanco se encierra entre comillas.
-WorkingDirectory <String>	Especifica la ubicación del archivo ejecutable o el documento.
-windowStyle <ProcessWindowStyle>	Especifica el estado de la ventana utilizada por el nuevo proceso. Los valores permitidos son Normal, Hidden, Minimized y Maximized.
-Verb <String>	Especifica el verbo a utilizar por el nuevo proceso. Los verbos disponibles dependen de la extensión del archivo que ejecuta el proceso. Consultar la referencia del comando para conocer los verbos y sus archivos asociados.

[Haz clic aquí para una referencia completa.](#)

Veamos algunos ejemplos. Para lanzar el bloc de notas podemos ejecutar el siguiente cmdlet.

```
PS C:\> Start-Process -FilePath notepad.exe
```

En este caso no ha sido necesario indicar el path completo del bloc de notas ya que se encuentra dentro de la variable de entorno PATH.

También podemos abrir un archivo de texto si lo pasamos como argumento

```
PS C:\> Start-Process -FilePath notepad.exe -ArgumentList "C:\Users\
Usuario\Documents\info.txt"
```

El mismo efecto hubiéramos conseguido si pasamos el archivo info.txt en el

argumento -FilePath.

```
PS C:\> Start-Process -FilePath "C:\Users\Usuario\Documents\info.txt"
```

Si queremos lanzar un proceso para una aplicación a la que tenemos que especificar su path completo podemos emplear el argumento -WorkingDirectory. En el siguiente ejemplo iniciamos Escáneres y Cámaras.

```
PS C:\> Start-Process -FilePath ImagingDevices.exe -WorkingDirectory
"C:\Program Files (x86)\Windows Photo Viewer"
```

Podemos iniciar el Internet Explorer en una ventana maximizada.

```
PS C:\> Start-Process -FilePath iexplore.exe -WindowStyle Maximized
```

## 4.7 Gestión de servicios en WPS

Para la gestión de servicios disponemos de un conjunto de cmdlets que permiten realizar las mismas operaciones que con el complemento Services en el escritorio gráfico. Son:

- ✓ Listar los servicios con Get-Service.
- ✓ Pausar un servicio con Suspend-Service.
- ✓ Reanudar servicios con Resume-Service.
- ✓ Parar un servicio con Stop-Service.
- ✓ Iniciar un servicio con Start-Service.
- ✓ Reiniciar un servicio con Restart-Service.
- ✓ Actualizar las propiedades de un servicio con Set-Service.

### 4.7.1 Listar servicios. Comando Get-Service

El cmdlet Get-Service obtiene objetos que representan los servicios en el sistema sin importar el estado en que se encuentren. Podemos listar estos servicios en pantalla o redirigirlos a otros cmdlets que gestionan servicios.

```
Get-Service
{ [[-Name] <String[]>] | -DisplayName <String[]> | [-
InputObject <ServiceController[]>] }
[-DependentServices]
[-RequiredServices]
[-Include <String[]>]
[-Exclude <String[]>]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de los servicios a recuperar. Admite caracteres comodín.

-DisplayName <String[]>	Especifica un array de cadenas con los nombres a visualizar de los servicios. Se admiten metacaracteres.
-InputObject <ServiceController[]>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. La forma más simple de este cmdlet es listar todos los servicios.

```
PS C:\> Get-Service
```

```
Status      Name      DisplayName
-----
Stopped     AJRouter  Servicio de enrutador de AllJoyn
Stopped     ALG       Servicio de puerta de enlace de niv...
Stopped     AppIDSvc  Identidad de aplicación
Running     Appinfo   Información de la aplicación
...
```

En el siguiente ejemplo listamos los servicios cuyo nombre comienza por un texto.

```
PS C:\> Get-Service -Name "Net*"
```

```
Status      Name      DisplayName
-----
Stopped     Netlogon  Net Logon
Stopped     Netman    Conexiones de red
Running     netprofm  Servicio de lista de redes
Stopped     NetSetupSvc Servicio de configuración de red
Stopped     NetTcpPortSharing Servicio de uso compartido de puert...
```

En este otro ejemplo obtenemos los servicios cuyo nombre visualizado contiene una cadena.

```
PS C:\> Get-Service -DisplayName "*red*"
```

```
Status      Name      DisplayName
-----
Stopped     dot3svc   Configuración automática de redes c...
Stopped     NcaSvc    Asistente para la conectividad de red
Running     NcbService Agente de conexión de red
Running     NcdAutoSetup Configuración automática de disposi...
Stopped     Netman    Conexiones de red
```

```
Running     netprofm  Servicio de lista de redes
Stopped     NetSetupSvc Servicio de configuración de red
Running     NlaSvc    Reconoc. ubicación de red
Running     nsi       Servicio Interfaz de almacenamiento...
```

Stopped	p2pimsvc	Administrador de identidad de redes...
Stopped	p2psvc	Agrupación de red del mismo nivel
Stopped	shpamsvc	Shared PC Account Manager
Stopped	UmRdpService	Redirector de puerto en modo usuari...
Running	VaultSvc	Administrador de credenciales
Running	WdNisSvc	Servicio de inspección de red de An...
Stopped	XboxNetApiSvc	Servicio de red de Xbox Live

Ahora utilizaremos el cmdlet Where-Object para listar los servicios que tienen una propiedad con un valor concreto. Por ejemplo, listamos los servicios cuyo estado es en ejecución (Running).

```
PS C:\> Get-Service | Where-Object -Property Status -eq "Running"
```

Status	Name	DisplayName
Running	Appinfo	Información de la aplicación
Running	AudioEndpointBu...	Compilador de extremo de audio de W...
...		

En el siguiente ejemplo vemos los servicios que el servicio cliente DHCP requiere para poder funcionar.

```
PS C:\> Get-Service dhcp -RequiredServices
```

Status	Name	DisplayName
Running	Afd	Controlador de función suplementari...
Running	NSI	Servicio Interfaz de almacenamiento...
Running	Tdx	Controlador de soporte TDI heredado...

Con el siguiente ejemplo obtenemos los servicios que dependen del cliente DHCP.

```
PS C:\> Get-Service dhcp -DependentServices
```

Status	Name	DisplayName
Stopped	NcaSvc	Asistente para la conectividad de red
Running	iphlpvc	Aplicación auxiliar IP
Running	WinHttpAutoProx...	Servicio de detección automática de...
Running	NcdAutoSetup	Configuración automática de disposi...
Stopped	AppVClient	Microsoft App-V Client
Running	netprofm	Servicio de lista de redes
Running	NlaSvc	Reconoc. ubicación de red

#### 4.7.2 Suspender un servicio. Comando Suspend-Service

El cmdlet Suspend-Service envía un mensaje de suspensión al controlador de servicios de Windows para cada uno de los servicios especificados. Mientras un servicio esté suspendido, estará todavía en ejecución, pero su acción es pausada hasta que se reanude utilizando el cmdlet Resume-Service. Podemos especificar servicios por su

nombre, su descripción corta o podemos usar el parámetro `-InputObject` para pasar un objeto servicio que representa el servicio que se desea pausar.

<pre>Suspend-Service { [[-Name] &lt;String[]&gt;]   -DisplayName &lt;String[]&gt;   [- InputObject &lt;ServiceController[]&gt;] } [-PassThru] [-Include &lt;String[]&gt;] [-Exclude &lt;String[]&gt;] [-WhatIf] [-Confirm] [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
<code>-Name &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres de los servicios a pausar. Admite caracteres comodín.
<code>-DisplayName &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres a visualizar de los servicios que se quieren pausar. Se admiten metacaracteres.
<code>-InputObject &lt;ServiceController[]&gt;</code>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, si queremos pausar el servicio cliente de red ejecutamos el siguiente comando.

```
Suspend-Service -Name LanmanWorkstation
```

Con el servicio anterior suspendido, el PC no puede acceder a recursos de red.

La mayoría de los servicios no pueden suspenderse. La propiedad `CanPauseAndResume` de un objeto servicio tiene el valor `True` si el servicio admite la suspensión y reanudación. Podemos ver una lista de estos servicios con el siguiente comando.

```
PS C:\> Get-Service | Where-Object -Property CanPauseAndContinue -eq $True
```

Status	Name	DisplayName
-----	----	-----
Paused	LanmanWorkstation	Estación de trabajo
Running	Winmgmt	Instrumental de administración de W...

Como podemos ver en el ejemplo anterior, solamente hay dos. Sin embargo, en versiones de Windows Server hay más.

La suspensión del servicio `Lanmanworkstation` podríamos haberla hecho también mediante el operador `|` como sigue.

```
PS C:\> Get-Service -Name LanmanWorkstation | Suspend-Service
```

### 4.7.3 Reanudar un servicio suspendido. Comando Resume-Service

El cmdlet `Resume-Service` envía un mensaje de reanudación al controlador de servicios de Windows para cada servicio especificado. Si un servicio está suspendido (pausado), lo reanuda. Si el servicio está actualmente en ejecución, el mensaje se ignora. Podemos especificar servicios por sus nombres, descripciones o empleando el parámetro `InputObject` para pasar un objeto servicio que queremos reanudar.

<pre>Resume-Service     { [[-Name] &lt;String[]&gt;]   -DisplayName &lt;String[]&gt;   [-InputObject &lt;ServiceController[]&gt;] }     [-PassThru]     [-Include &lt;String[]&gt;]     [-Exclude &lt;String[]&gt;]     [-WhatIf]     [-Confirm]     [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
<code>-Name &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres de los servicios a reanudar. Admite caracteres comodín.
<code>-DisplayName &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres a visualizar de los servicios que se quieren reanudar. Se admiten metacaracteres.
<code>-InputObject &lt;ServiceController[]&gt;</code>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

En el siguiente ejemplo reanudamos el servicio cliente de red que pausamos en el epígrafe anterior.

```
PS C:\> Resume-Service LanmanWorkstation
```

También podemos reanudar todos los servicios actualmente suspendidos.

```
PS C:\> Get-Service | Where-Object -Property Status -eq "Paused" | Resume-Service
```

### 4.7.4 Parar un servicio. Comando Stop-Service

El cmdlet `Stop-Service` envía un mensaje de parada al controlador de servicios de Windows para cada servicio especificado. La parada del servicio implica que deja de ejecutarse y ofrecer la funcionalidad del servicio. Podemos especificar los servicios por sus nombres, descripciones o con el parámetro `InputObject` para pasar un objeto servicio que representa el servicio que queremos parar.

```
Stop-Service
  [-Force]
  [-Nowait]
  { [[-Name] <String[]>] | -DisplayName <String[]> | [-
InputObject <ServiceController[]>] }
  [-PassThru]
  [-Include <String[]>]
  [-Exclude <String[]>]
  [-whatIf]
  [-Confirm]
  [<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de los servicios a parar. Admite caracteres comodín.
-DisplayName <String[]>	Especifica un array de cadenas con los nombres a visualizar de los servicios que se quieren parar. Se admiten metacaracteres.
-InputObject <ServiceController[]>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para parar el servicio de Audio de Windows.

```
PS C:\> Stop-Service -DisplayName "Audio de Windows"
```

La parada de un servicio implica la parada de los servicios de los que depende. Por ello resulta conveniente realizar un listado del servicio en el que se muestren los servicios que dependen de él antes de pararlo. Por ejemplo, a continuación vemos los servicios que dependen del centro de seguridad de Windows.

```
PS C:\> Get-Service -Name wscsvc | Format-List -Property Name,
DependentServices
```

```
Name           : wscsvc
DependentServices : {}
```

No hay ninguno, podemos entonces pararlo.

```
PS C:\> Get-Service -Name wscsvc | Stop-Service
```

#### 4.7.5 Iniciar un servicio. Comando Start-Service

El cmd-let Start-Service envía un mensaje de inicio de servicio al controlador de servicios de Windows para cada servicios especificado. Si un servicio está en ejecución, el



mensaje se ignora y no produce ningún error. Podemos especificar servicios por sus nombres, descripciones o con el parámetro `InputObject` que suministra un objeto servicio que representa el servicio a iniciar.

```
Start-Service
{ [[-Name] <String[]>] | -DisplayName <String[]> | [-
InputObject <ServiceController[]>] }
[-PassThru]
[-Include <String[]>]
[-Exclude <String[]>]
[-WhatIf]
[-Confirm]
[<CommonParameters>]
```

Parámetro	Descripción
<code>-Name &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres de los servicios a iniciar. Admite caracteres comodín.
<code>-DisplayName &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres a visualizar de los servicios que se quieren iniciar. Se admiten metacaracteres.
<code>-InputObject &lt;ServiceController[]&gt;</code>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. Iniciamos el servicio que paramos en el epígrafe anterior.

```
PS C:\> Start-Service -DisplayName "Audio de Windows"
```

Iniciamos ahora el centro de seguridad.

```
PS C:\> Get-Service wscsvc | Start-Service
```

Si iniciamos un servicio deshabilitado da un error. Por ejemplo

```
PS C:\> Start-Service tzautoupdate
Start-Service : No se puede iniciar el servicio 'Actualizador de zona horaria automática (tzautoupdate)' debido al error siguiente: No se
```

puede iniciar el servicio tzautoupdate en el equipo '.'.

Por tanto tendríamos primero que cambiar su tipo de inicio a Manual para poder iniciarlo. El cambio de las propiedades de un servicio se verá en un epígrafe posterior.

#### 4.7.6 Reiniciar un servicio. Comando Restart-Service

El cmdlet Restart-Service envía un mensaje de parada seguido de un mensaje de inicio al controlador de servicios de Windows para un servicio especificado. Si un servicio ya está parado, se inicia sin notificar un error. Podemos especificar servicios por sus nombres, descripciones o mediante el parámetro InputObject al que se le pasa el objeto servicio que queremos reiniciar.

```
Restart-Service
    [-Force]
    { [[-Name] <String[]>] | -DisplayName <String[]> | [-InputObject <ServiceController[]>] }
    [-PassThru]
    [-Include <String[]>]
    [-Exclude <String[]>]
    [-WhatIf]
    [-Confirm]
    [<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de los servicios a iniciar. Admite caracteres comodín.
-DisplayName <String[]>	Especifica un array de cadenas con los nombres a visualizar de los servicios que se quieren iniciar. Se admiten metacaracteres.
-InputObject <ServiceController[]>	Especifica un array de objetos servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. El siguiente comando reanuda el servicio de configuración automática de WLAN.

```
PS C:\> Restart-Service -Name Wlansvc
```

El siguiente comando reinicia todos los servicios de red que están parados.

```
PS C:\> Get-Service -DisplayName "*red*" | Where-Object -Property Status -eq "Stopped" | Restart-Service
```

### 4.7.7 Gestionar un servicio. Comando Set-Service

El cmdlet Set-Service cambia las propiedades de un servicio. Esto incluye el estado, descripción, nombre visualizado y modo de arranque. Podemos usar este servicio para iniciar, parar y pausar un servicio. Para identificar el servicio, podemos indicar su nombre o enviar un objeto servicio a través del operador |.

```
Set-Service
{ [-Name] <String> | [-InputObject] <ServiceController> }
[-DisplayName <String>]
[-Credential <PSCredential>]
[-Description <String>]
[-StartupType <ServiceStartupType>]
[-Status <String>]
[-PassThru]
[-WhatIf]
[-Confirm]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de los servicios a actualizar. Admite caracteres comodín.
-InputObject <ServiceController>	Especifica un objeto servicio. Podemos utilizar una variable objeto servicio, un comando que obtiene objetos servicio o redirigir la salida de un cmdlet.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. El siguiente servicio cambia el nombre visualizado del servicio LanmanWorkstation y lo establece a “Cliente de Red”.

```
PS C:\> Get-Service lanmanworkstation

Status  Name                DisplayName
-----  ---                -
Running lanmanworkstation Estación de trabajo

PS C:\> Set-Service -Name LanmanWorkstation -DisplayName "Cliente de
red"
PS C:\> Get-Service lanmanworkstation

Status  Name                DisplayName
-----  ---                -
Running lanmanworkstation Cliente de red
```

En el siguiente ejemplo cambiamos el modo de inicio del servicio de Audio de

Windows de Manual a Automático.

```
PS C:\> Set-Service -Name Audiosrv -StartupType Automatic
```

Con Set-Service podemos iniciar un servicio actualizando su propiedad Status. En el siguiente ejemplo iniciamos el servicio de conexiones de red.

```
PS C:\> Get-Service -Name Netman
```

Status	Name	DisplayName
Stopped	Netman	Conexiones de red

```
PS C:\> Set-Service -Name Netman -Status Running
PS C:\> Get-Service -Name Netman
```

Status	Name	DisplayName
Running	Netman	Conexiones de red

Para parar el servicio ponemos su estado a Stopped y si queremos suspenderlo lo pasamos a Paused.

## 5 Configuración de la red

Actualmente los ordenadores trabajan conectados en red. Una de las principales ventajas de los equipos informáticos es el poder compartir información y recursos. Conectándonos a otra red podremos intercambiar archivos, usar aplicaciones conjuntas, compartir impresoras, etc.

Para que un equipo conectado a una red pueda comunicarse con otros equipos de la red y acceder a Internet necesita tener configurado lo siguiente:

- ✓ Parámetros de red del protocolo IP.
- ✓ Nombre del equipo para acceso a otros equipos en la red local.
- ✓ Resolución de nombres para traducir nombres a direcciones IP.

Para configurar todos estos elementos disponemos de dos herramientas GUI y diversos comandos en línea que veremos a continuación

### 5.1 Red e Internet

Con la nueva versión de Windows parte de la configuración de la red se ha migrado al elemento *Red e Internet* del menú *Inicio* → *Configuración*.

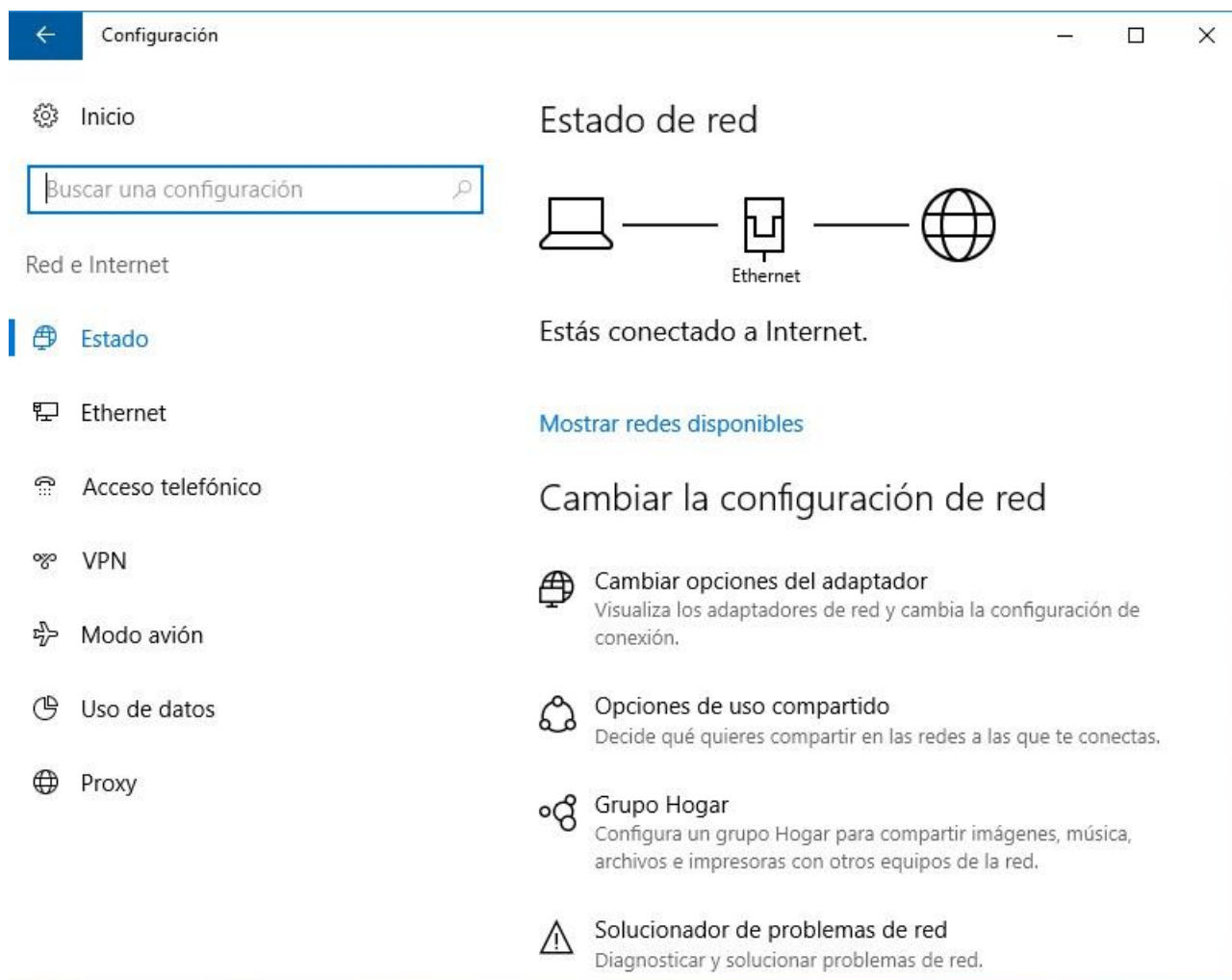


Figura 30.- Red e Internet

Como se aprecia en la figura anterior la gestión de la red está dividida en varias categorías que se disponen en la parte izquierda. Estas son:

- ✓ Estado.- Muestra el estado actual de la red. Aquí podemos comprobar si estamos conectados a Internet y en caso de que hubiera algún problema disponemos de la posibilidad de ejecutar un diagnóstico de la red para resolverlo.
- ✓ Ethernet.- Muestra las conexiones de red a las que podremos ver la configuración IP actual, definir un perfil de red y configurar el uso de datos medidos.
- ✓ Acceso telefónico.- Si disponemos en nuestro PC de una tarjeta de red lo más seguro es que no tengamos una conexión de red a través de una línea telefónica básica.
- ✓ VPN.- En este apartado podemos configurar las conexiones de redes privadas virtuales, las cuales nos permitirían estar conectados a la red local de nuestra organización sin tener el PC físicamente presente en dicha red, sino a través de una conexión VPN desde Internet.
- ✓ Modo avión.- Solamente es aplicable a las tarjetas de red inalámbricas. Desde aquí podemos poner una tarjeta inalámbrica en modo avión lo que supone su

desconexión de la red WLAN.

- ✓ **Uso de datos.**- Presenta una estadística de la cantidad de información transferida por las conexiones de red. En el caso de un dispositivo móvil con acceso a Internet a través de una red de telefonía móvil podemos saber que cantidad de datos hemos consumido.
- ✓ **Proxy.**- Aquí podemos configurar si estamos conectados a Internet a través de un servidor proxy en lugar de un router. En este caso habría que indicar la dirección IP del servidor proxy y el número de puerto empleado.

## 5.2 El centro de redes y recursos compartidos

El *Centro de redes y recursos compartidos* es la herramienta de Windows que apareció con Windows Vista y se ha mantenido hasta ahora. Se emplea para configurar las opciones de red del PC. Podemos acceder desde el *Panel de control* → *Redes e Internet*.

En la imagen inferior podemos el estado actual de la red. En *Ver las redes activas* tendremos una red por cada conexión de red, que normalmente coincidirá con cada interfaz de red que tenga instalada el equipo. En este caso tenemos una conexión de red, denominada *Red*, cuya ubicación es *Red privada*, está conectada a Internet y al grupo Hogar.

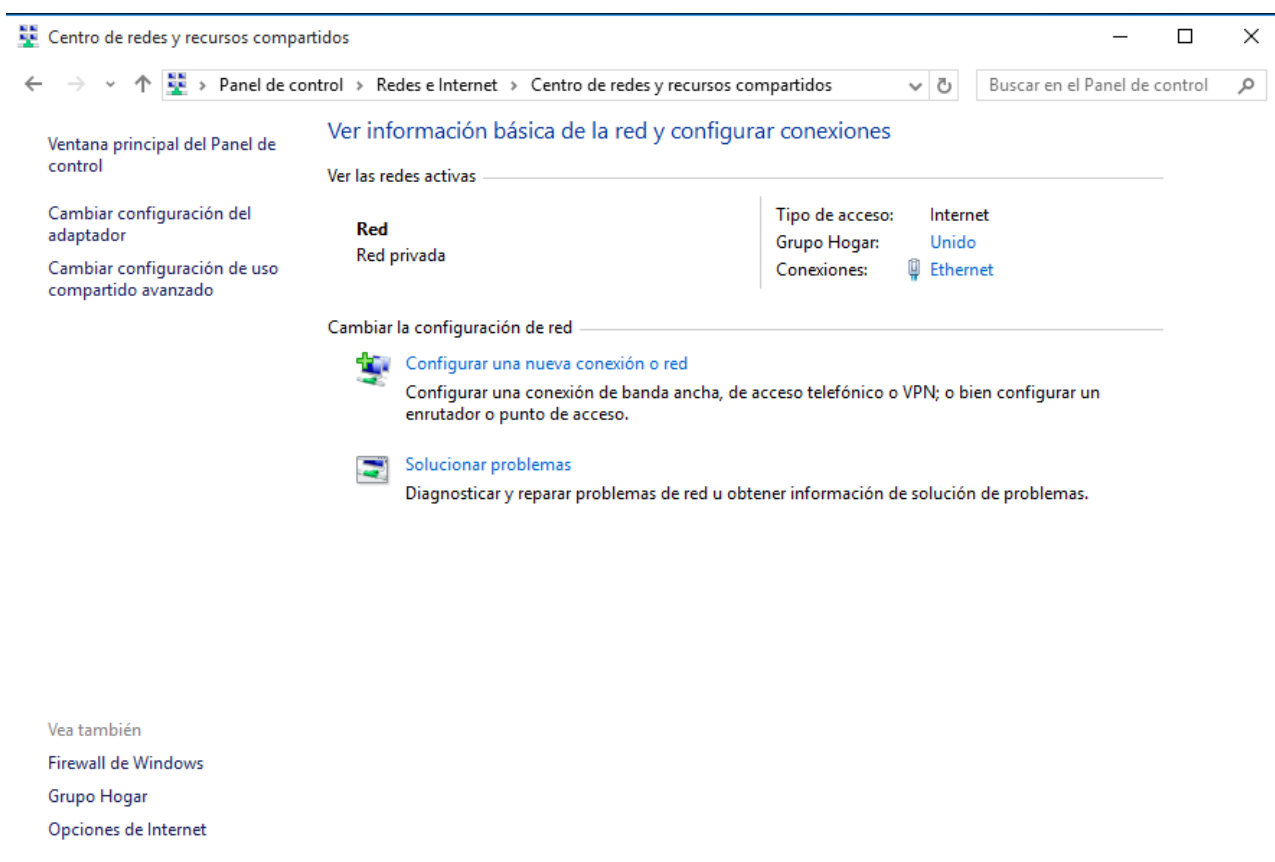


Figura 31.- Centro de redes y recursos compartidos

### 5.2.1 Ubicación de red

La primera vez que el equipo se conecta a una red, debemos elegir una ubicación de red. De esta forma, la configuración apropiada del cortafuegos y seguridad se define automáticamente para el tipo de red con la que hemos conectado. Cuando nos conectamos a redes en diversas ubicaciones (por ejemplo, a la red de nuestra casa, de la cafetería de al lado, a la del aeropuerto o la del trabajo), elegir una ubicación de red puede ser útil para asegurarnos de que el equipo tenga siempre el nivel de seguridad adecuado. Existen cuatro ubicaciones de red:

- ✓ Red privada.- Para redes privadas como la de casa o del trabajo o cuando conozca y confíe en los usuarios y dispositivos de la red. Los equipos de una red privada pueden pertenecer a un grupo en el hogar. La detección de redes está activada para las redes privadas, lo que permite ver otros equipos y dispositivos de la red y que otros usuarios de la red vean el equipo.
- ✓ Red pública.- Para las redes de lugares públicos (por ejemplo, cafeterías, hoteles o aeropuertos). Esta ubicación se ha diseñado para evitar que el equipo sea visible para otros equipos y te ayudará a proteger el equipo de software malintencionado de Internet. El Grupo Hogar no está disponible en redes públicas, y la detección de redes está desactivada. También debemos elegir esta opción si estamos conectado directamente a Internet sin usar un enrutador (como una conexión por modem cable), o si tenemos una conexión de banda ancha móvil.
- ✓ Dominio.- Se usa en redes de dominio dentro de entornos corporativos, como las de las empresas. Un administrador de red controla este tipo de ubicación de red, que no se puede seleccionar ni cambiar.

Dependiendo de la ubicación de red que escojamos tendremos configurado en nuestro PC una seguridad más o menos restrictiva. Se supone que en una red privada conocemos todos los PCs que hay conectados y tenemos plena confianza en ellos. Sin embargo, no se puede confiar en absoluto en los PCs conectados en una red pública y que son totalmente desconocidos.

En cualquier momento podemos cambiar la ubicación de red siguiendo estos pasos:

1. Hacer clic en *Inicio* → *Configuración* → *Red e Internet*.
2. Hacer clic en Wi-Fi o Ethernet, dependiendo de la interfaz de red a la que queremos cambiar su ubicación.
3. En la parte derecha hacer clic sobre la interfaz de red.
4. En *Perfil de Red* seleccionar *Público* o *Privado*.

## 5.3 Configuración parámetros IP

En Internet se utiliza como protocolo IP. El protocolo IP define una serie de parámetros que todo ordenador conectado a Internet tiene que tener configurados para poder

conectarse. Estos son:

- ✓ Dirección IP.
- ✓ Máscara de red.
- ✓ Puerta de enlace.
- ✓ Direcciones IP de los servidores de nombres de dominio.

Para configurar estos parámetros tenemos dos opciones:

- ✓ Configuración estática.- El administrador del sistema configura manualmente estos parámetros.
- ✓ Configuración automática.- El PC emplea un servidor DHCP. Un servidor ejecutando el servicio DHCP se encarga de configurar de manera automática los ordenadores de la red cuando estos arrancan. Esta es la forma habitual de configurar un PC en red.

Para configurar un PC con sus parámetros IP seguiremos los siguientes pasos:

1. Entrar en *Red e Internet* desde *Configuración*.
2. Hacer clic en *Ethernet*.
3. En *Configuración relacionada* hacer clic en *Cambiar opciones del adaptador*.
4. Hacer clic con el botón derecho del ratón sobre el icono de la interfaz de red y seleccionar la opción *Propiedades* y después seleccionar *Protocolo de Internet version 4 (TCP/IPv4)* y hacer clic en el botón *Propiedades*.

También podemos acceder desde el Centro de Redes y recursos compartidos.

1. Abrir el *Centro de Redes y recursos compartidos*.
2. Hacer clic en el enlace *Cambiar configuración del adaptador*.
3. Hacer clic con el botón derecho del ratón sobre el icono de la interfaz de red y seleccionar la opción *Propiedades*.
4. Seleccionar *Protocolo de Internet version 4 (TCP/IPv4)* y hacer clic en el botón *Propiedades*.
5. A partir de ahora los pasos son comunes



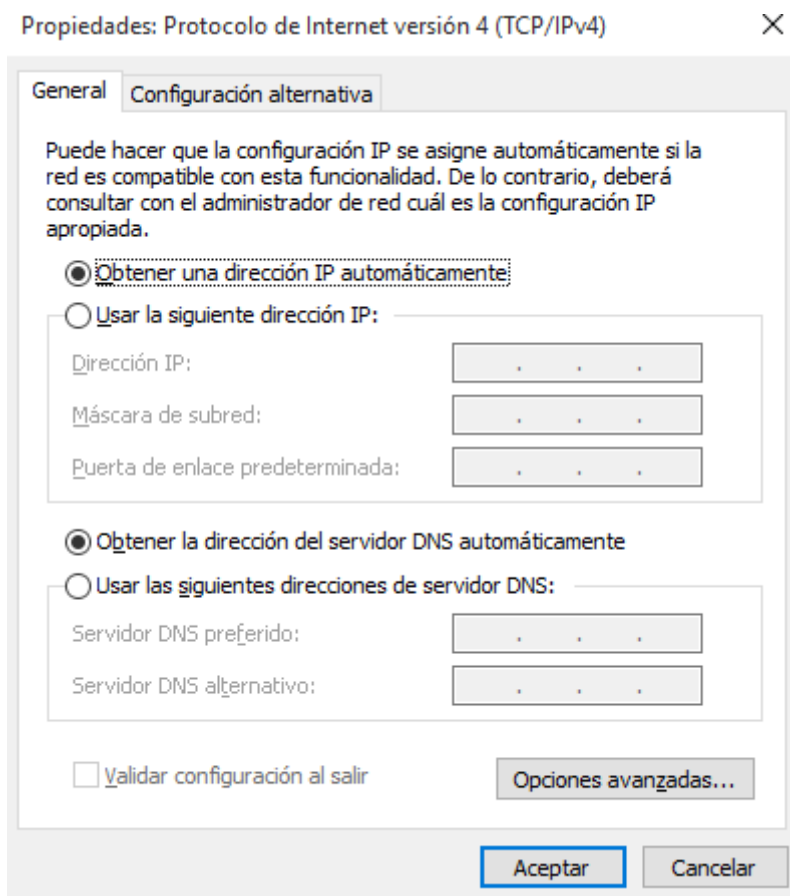


Figura 32.- Configuración TCP/IP

6. Si el PC se configura automáticamente hacer clic en *Obtener una dirección IP automáticamente* y en *Obtener la dirección del servidor DNS automáticamente*.
7. Si el PC se configura de forma estática hacer clic en *Usar la siguiente dirección IP* y en *Usar las siguientes direcciones de servidor DNS* y rellenar los siguientes campos:
  - a) *Dirección IP.*
  - b) *Máscara de subred.*
  - c) *Puerta de enlace.*
  - d) *Servidor DNS preferido.*
  - e) *Servidor DNS alternativo.*
8. Hacer clic en el botón *Aceptar*.

## 5.4 Nombre de equipo y grupo de trabajo

A los PCs se les asigna un nombre, ya a que resulta más fácil referirse a los equipos por un nombre que por la dirección IP. Por ejemplo: si en el navegador se escribe `http://www.google.es` o se hace accede a una carpeta compartida mediante un nombre UNC como `\\servidor\compartida` se está utilizando nombres de PC de alto nivel.

En todas las versiones de Windows los PC's tienen asignado un nombre que se emplea para identificarlos en la red. En versiones anteriores a Windows 2000/XP este nombre corresponde a lo que se conoce como nombre NetBIOS y es utilizado para la comunicación entre PCs dentro de la red local. Aunque la longitud máxima es de 16 caracteres, el sistema permite usar sólo 15 porque el último es utilizado para funciones reservadas al sistema.

Además, en redes TCP/IP se emplean nombres dentro del sistema DNS los cuales se conocen como *hostname*. Este nombre tiene unas características sintácticas muy distintas al NetBIOS: puede tener hasta 63 caracteres y sólo están permitidos letras, números y el signo menos (-); a diferencia del nombre NetBIOS que permite la utilización de algunos símbolos. Podemos ver el *hostname* del equipo ejecutando el comando del mismo nombre en una ventana de símbolo del sistema.

A partir de Windows 2000/XP, el nombre que colocamos al equipo es el *hostname*, no el nombre NetBIOS. Windows sigue utilizando el nombre NetBIOS por compatibilidad con los anteriores sistemas operativos y aplicaciones basadas en NetBIOS, haciéndolo coincidir con el *hostname*.

Para asignar un nombre al equipo seguir los siguientes pasos:

1. Hacer clic en *Inicio* → *Configuración* → *Sistema* → *Acerca de*. También podemos abrir las propiedades del equipo en *Panel de Control* → *Sistema y seguridad* → *Sistema*.
2. Si hemos utilizado la primera opción hacemos clic en el botón *Cambiar el nombre de este equipo*. Si hemos llegado a través del panel de control en *Configuración de nombre, dominio y grupo de trabajo* hacer clic en el enlace *Cambiar configuración*.
3. Escribir el nuevo nombre o en la pestaña *Nombre de equipo* hacer clic en el botón *Cambiar...* y escribir el nombre en el cuadro de texto *Nombre de equipo*.
4. Hacer clic en el botón *Siguiente* o *Aceptar*.

Después de cambiar el nombre del equipo tenemos que reiniciar el PC para que los cambios entren en vigor. A partir de entonces, cuando accedamos a la red aparecerán este equipo identificado con el nombre configurado aquí. Hay que recordar que este nombre solamente servirá para comunicar los PCs de la red local, nunca fuera de ella. Para comunicar el PC con una red de área extensa como Internet se emplea la dirección IP.

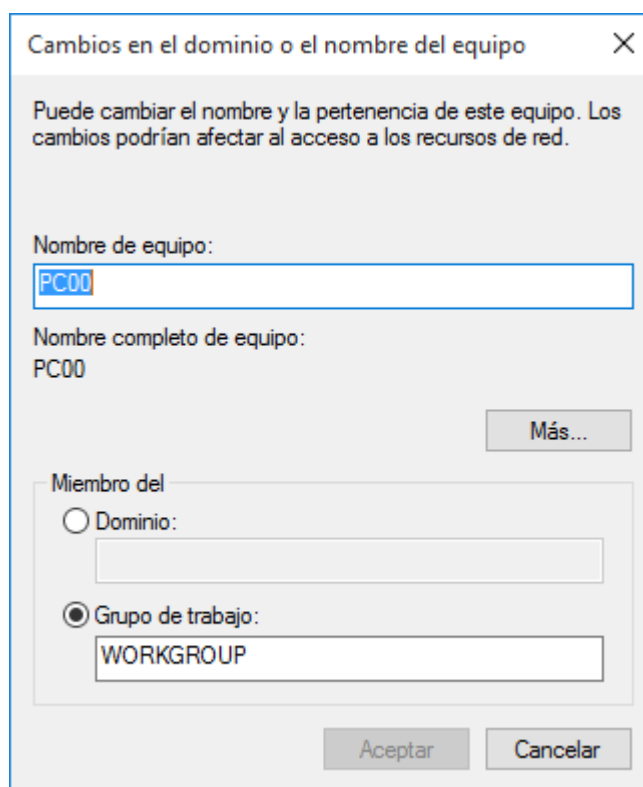


Figura 33.- Nombre de equipo

## 5.5 Resolución de nombres

Los PCs tienen una dirección IP para identificarse de forma única en una red. Sin embargo, resulta mucho más fácil acceder a un PC por un nombre en lugar de por una dirección IP. Hemos visto antes que los PCs de una red local Windows tienen el nombre NetBIOS para identificarse entre sí. Con este nombre los usuarios pueden buscar recursos compartidos en la red local. Sin embargo, cuando accedemos a otros ordenadores en Internet lo hacemos con su nombre DNS, el cual tiene que ser traducido a una dirección IP. A la traducción de un nombre a su correspondiente dirección IP se le conoce como resolución de nombres.

En una red Windows debemos resolver nombres NetBIOS y nombres DNS (*hostname*) y para ello se emplean métodos diferentes.

### 5.5.1 NetBIOS

Cuando un PC se vuelve activo en la red, quiere reclamar un nombre para sí; esto se denomina registro de nombre. Sin embargo, dos PCs en el mismo grupo de trabajo podrían solicitar el mismo nombre; lo que causaría problemas para cualquier PC que quiera comunicar con una de esos dos. Por tanto, antes de usar un nombre NetBIOS hay que registrarlo. Posteriormente, el PC necesitará traducir nombres NetBIOS a su correspondiente dirección IP. Para ello se disponen de los siguientes métodos:

- ✓ NetBIOS Cache.- Si en algún momento se resuelve un nombre, permanece durante un cierto tiempo en memoria la dirección IP del PC. Esta traducción sería la más

rápida ya que se dispone de la dirección IP.

- ✓ *NetBIOS Name Server.*- Servidor de nombres NetBios. Las versiones server de Windows disponen de un servicio denominado WINS (*Windows Internet Name Server*). Un servidor de la red ejecuta el servicio WINS y los clientes están configurados para usarlo. Para explicarlo en forma sencilla: cuando los clientes se inician, registran con el servidor WINS su nombre y su dirección IP. Con esta información el servidor construye una base de datos dinámica que incluye todos los clientes que se registraron. Luego cuando los clientes tienen que resolver una dirección IP le preguntan al servidor WINS, que si puede, responde adecuadamente.
- ✓ *Broadcast.*- Cuando un PC necesita saber la dirección IP de otro, y no hay disponible un servidor WINS, envía un mensaje por difusión a todos los equipos de la red preguntando por la dirección IP de un nombre. Esta información en la red dirigida a todos los equipos contiene algo así como “¿Qué dirección IP tiene el equipo que se llama SERVIDOR?” Todos los equipos lo escuchan, pero contesta sólo el que se llama SERVIDOR, devolviendo su dirección IP.
- ✓ *Archivo LMHOSTS.*- Es un archivo de texto, donde cada línea corresponde a un registro e incluye la dirección IP seguida de por lo menos un espacio y el nombre NetBIOS correspondiente. Este archivo debe estar disponible y mantenerse individualmente en cada PC. Por defecto este archivo no esta creado, se tendrá que crear para lo cual hay un archivo de ejemplo llamado `lmhosts.sam` que nos servirá de guía. La ubicación de este archivo es la siguiente: `C:\WINDOWS\system32\drivers\etc`. Este archivo es propio de Microsoft y es una adaptación del método del archivo `hosts` para traducción de nombres DNS.

El archivo `C:\windows\System32\drivers\etc\lmhosts` se emplea para resolver nombres NetBIOS localmente, lo que resulta más rápido que hacerlo mediante mensajes de broadcast. El formato de este archivo es similar al anterior. Es un archivo de texto donde se emplea una línea para cada equipo con el siguiente formato

```
dirección_IP nombre_NetBIOS
```

Como podemos ver hay diferentes formas de traducir un nombre NetBIOS a una dirección IP. El método de resolución del nombre empleado por un PC lo determina un parámetro de red del equipo denominado tipo de nodo. Existen 4 tipos de nodos:

- ✓ *Nodo B.*- Emplea exclusivamente mensajes de broadcast para resolver nombres.
- ✓ *Nodo H (híbrido).*- El PC se registra en un servidor WINS y lo utiliza para resolver otros nombres. Si el servidor no está disponible emplea mensajes de broadcast.
- ✓ *Nodo P.*- Emplea exclusivamente un servidor WINS para registrarse y resolver nombres.
- ✓ *Nodo M.*- Emplea mensajes de difusión para registrarse y resolver nombres. Si no tiene éxito la resolución de nombres entonces emplea el servidor WINS.

Si la configuración IP del equipo dispone de un servidor WINS el PC será un nodo tipo

H, de lo contrario será B. Se puede establecer también el tipo de nodo mediante una clave de registro.

Para configurar la dirección IP del servidor WINS seguimos los siguientes pasos:

1. Abrir las propiedades TCP/IP de la conexión de red como se vio anteriormente.
2. Hacer clic en el botón *Opciones avanzadas*.
3. Hacer clic en la pestaña WINS.

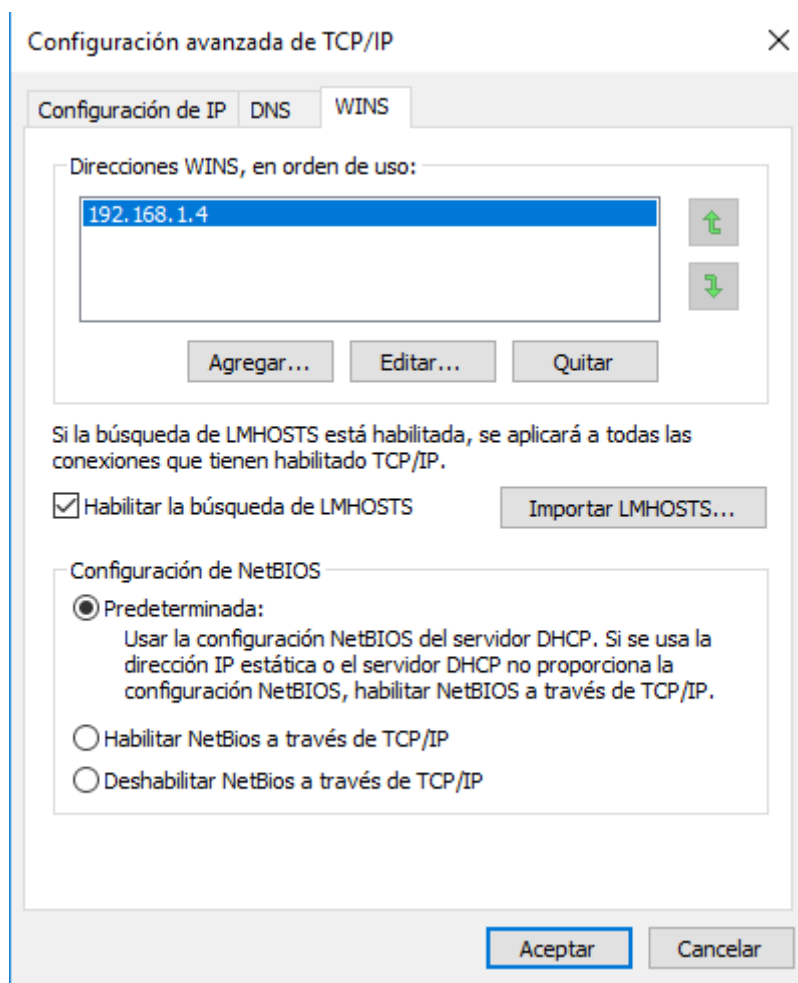


Figura 34.- Configuración del servidor WINS

4. Hacer clic en el botón *Agregar...*
5. Introducir la dirección IP del servidor WINS y hacer clic en el botón *Aceptar*.

### 5.5.2 DNS

El protocolo DNS (*Domain Name System*) suministra una base de datos global y jerárquica de nombres de hosts en Internet. Los servidores conectados a Internet proveyendo algún servicio utiliza un nombre DNS para acceder a ellos. Cuando un PC necesita acceder a un servidor en Internet tiene que hacer previamente una consulta a un servidor DNS para que le suministre la dirección IP correspondiente a ese nombre. Una vez

tiene la dirección IP del servidor ya puede acceder a él. Este proceso de traducción es transparente al usuario y los PCs hacen las consultas a los servidores DNS configurados en las propiedades TCP/IP de la interfaz de red.

En el apartado anterior hemos visto que uno de los parámetros de red son las direcciones IP de los servidores DNS. Sin embargo, la resolución de nombres DNS incluye más métodos que veremos a continuación:

- ✓ **Archivo Hosts.**- Es un archivo de texto, donde cada línea corresponde a un registro e incluye la dirección IP seguida de por lo menos un espacio y el hostname del equipo, este es un archivo que existe en cada ordenador. Este archivo se encuentra en la siguiente ubicación `C:\WINDOWS\system32\drivers\etc`.
- ✓ **DNS (Domain Name Server).**- Un servidor con el servicio de DNS instalado y configurado el cual se encargará de traducir un nombre a una dirección IP. Los clientes tienen configurado hasta dos servidores DNS (principal y secundario) mediante su dirección IP.
- ✓ **Hostname Cache.**- Cuando resuelven un nombre a una dirección IP, esta información permanece almacenada en memoria durante un tiempo.

El archivo `C:\windows\System32\drivers\etc\hosts` se emplea para resolver nombres DNS localmente, es decir, sin pasar la consulta a un servidor DNS. Consiste en un archivo de texto cuyas líneas corresponde a una dirección IP con un nombre DNS. El formato de cada línea es

```
dirección_IP nombre_DNS
```

## 5.6 Gestión de la red en el símbolo del sistema

A continuación se exponen diferentes utilidades en línea de comando para la gestión de la red.

### 5.6.1 Información de la conexión de red. Comando `ipconfig`

El comando `ipconfig` muestra los valores actuales de la configuración de la red TCP/IP y actualiza la configuración de DHCP (Protocolo de configuración dinámica de host) y DNS (Sistema de nombres de dominio). Si se utiliza sin parámetros, `ipconfig` muestra la dirección IP, máscara de subred y puerta de enlace predeterminada de todos los adaptadores.

```
ipconfig [/all] [/renew [<adaptador>]] [/release [<adaptador>]]
[/flushdns] [/displaydns] [/registerdns]
```

Parámetro	Descripción
/all	Muestra la configuración de TCP/IP completa de todos los adaptadores. Sin este parámetro, <code>ipconfig</code> sólo mostrará los valores de dirección IP, la máscara de subred y la puerta de enlace predeterminada para cada adaptador. Los adaptadores pueden

	representar a interfaces físicas, como los adaptadores de red instalados, o interfaces lógicas, como las conexiones de acceso telefónico a redes.
/renew [<adaptador>]	Renueva la configuración de DHCP de todos los adaptadores (si no se especificó un adaptador) o de un adaptador específico, si se incluyó el parámetro adaptador. Este parámetro sólo está disponible en equipos que dispone de adaptadores configurados para obtener una dirección IP automáticamente. Para especificar un nombre de adaptador, escriba el nombre de adaptador que aparece cuando se utiliza ipconfig sin parámetros.
/release [<adaptador>]	Envía el mensaje DHCPRELEASE al servidor DHCP para liberar la configuración actual de DHCP y descartar la configuración de dirección IP para todos los adaptadores (si no se especificó un adaptador) o para un adaptador específico si se incluyó el parámetro adaptador. Este parámetro deshabilita TCP/IP para los adaptadores configurados para obtener una dirección IP automáticamente. Para especificar un nombre de adaptador, escriba el nombre de adaptador que aparece cuando se utiliza ipconfig sin parámetros.
/flushdns	Vacía y restablece el contenido del servicio de resolución de la caché de clientes DNS. Durante la solución de problemas de DNS, puede utilizar este procedimiento para descartar entradas de resultados negativos en la caché y otras entradas agregadas dinámicamente.
/displaydns	Muestra el contenido del servicio de resolución de la caché del cliente DNS, que incluye las entradas cargadas previamente desde el archivo Hosts local y los registros de recursos que se hayan obtenido recientemente para consultas de nombre resueltas por el equipo. El servicio Cliente DNS utiliza esta información para resolver rápidamente los nombres consultados frecuentemente, antes de consultar a sus servidores DNS configurados.
/registerdns	Inicia el registro dinámico manual de los nombres DNS y direcciones IP configurados en un equipo. Puede usar este parámetro para solucionar problemas en el registro de nombres DNS o para resolver un problema de actualización dinámica entre un cliente y un servidor DNS sin tener que reiniciar el cliente. La configuración de DNS de las propiedades avanzadas del protocolo TCP/IP determina qué nombres se registran en DNS.

Este comando resulta más útil en equipos configurados para obtener una dirección IP automáticamente. Así se permite a los usuarios determinar los valores de la configuración de TCP/IP que ha configurado DHCP, APIPA (Direcciones IP privadas automáticas) o una configuración alternativa.

Si el nombre adaptador contiene espacios en blanco, hay que encerrar entre comillas el texto (por ejemplo, "nombre de adaptador").

En los nombres de adaptador, `ipconfig` admite la utilización del carácter comodín asterisco (\*) para especificar adaptadores cuyos nombres comienzan con la cadena especificada o adaptadores que contienen la cadena especificada. Por ejemplo, `Local*` busca todos los adaptadores que comienzan con la cadena `Local` y `*Con*` busca todos los adaptadores que contienen la cadena `Con`.

### 5.6.2 Información de la conexión de red física. Comando `getmac`

Muestra la dirección MAC de los adaptadores de red.

getmac [/FO <formato>] [/V]	
Parámetro	Descripción
/FO <formato>	Especifica en que formato se va a mostrar la salida. Valores válidos: "TABLE", "LIST" y "CSV".
/V	Especifica que se muestra la salida detallada.

### 5.6.3 Información de las conexiones y rutas de red. Comando `netstat`

`Netstat` (*network statistics*) es una herramienta de línea de comandos que muestra un listado de las conexiones activas de un ordenador, tanto entrantes como salientes.

Muestra las conexiones de TCP activas, los puertos en que el equipo escucha, las estadísticas de Ethernet, la tabla de enrutamiento IP, las estadísticas de IPv4 (para los protocolos IP, ICMP, TCP y UDP) y las estadísticas de IPv6 (para los protocolos IPv6, ICMPv6, TCP sobre IPv6 y UDP sobre IPv6). Cuando se utiliza sin parámetros, `netstat` muestra las conexiones de TCP activas.

netstat [-a] [-e] [-f] [-n] [-o] [-p <protocolo>] [-s] [-r] [ <intervalo>]	
Parámetro	Descripción
-a	Muestra todas las conexiones de TCP activas y los puertos TCP y UDP en que el equipo está escuchando.
-e	Muestra las estadísticas Ethernet, tales como el número de bytes y paquetes enviados y recibidos. Este parámetro se puede combinar con -s.
-f	Muestra nombres de dominio completos (FQDN) para direcciones externas.
-n	Muestra las conexiones de TCP activas, aunque las direcciones y los números de puerto se expresan numéricamente y no se intenta determinar los nombres..
-o	Muestra las conexiones de TCP activas e incluye el Id. de proceso (PID)



	de cada conexión. Puede encontrar la aplicación basándose en el PID de la ficha Procesos del Administrador de tareas de Windows. Este parámetro se puede combinar con -a, -n y -p.
-p <protocolo>	Muestra las conexiones del protocolo especificado en protocolo. En este caso, el protocolo puede ser tcp, udp, tcpv6 o udpv6. Si este parámetro se utiliza con -s para mostrar las estadísticas por protocolo, el protocolo puede ser tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6 o ipv6.
-s	Muestra las estadísticas por protocolo. De manera predeterminada, se muestran las estadísticas correspondientes a los protocolos TCP, UDP, ICMP e IP. Si el protocolo IPv6 está instalado, se muestran estadísticas de los protocolos TCP sobre IPv6, UDP sobre IPv6, ICMPv6 y IPv6. El parámetro -p puede utilizarse para especificar un conjunto de protocolos.
-r	Muestra el contenido de la tabla de enrutamiento IP. Es equivalente al comando route print.
<intervalo>	Presenta la información seleccionada cada intervalo segundos. Presione CTRL+C para detener la presentación de las estadísticas. Si omite este parámetro, netstat imprimirá una vez la información seleccionada.

La salida del comando netstat proporciona las siguientes estadísticas:

- ✓ Proto.- Nombre del protocolo (TCP o UDP).
- ✓ Dirección local.- La dirección IP del equipo local, así como el número de puerto que se está utilizando. El nombre del equipo local que corresponde a la dirección IP y el nombre del puerto se muestran a menos que se especifique el parámetro -n. Si el puerto no está aún establecido, el número se muestra como un asterisco (\*).
- ✓ Dirección remota.- La dirección IP y el número de puerto del equipo remoto al cual está conectado el socket. Los nombres que corresponden a la dirección IP y el puerto se muestran a menos que se especifique el parámetro -n. Si el puerto no está aún establecido, el número se muestra como un asterisco (\*).
- ✓ Estado.- Indica el estado de una conexión de TCP. Los estados posibles son los siguientes:
  - ESTABLISHED.- El socket tiene una conexión establecida
  - SYN\_SENT.- El socket está intentando iniciar una conexión
  - SYN\_RECV.- Una petición de conexión fue recibida por la red
  - FIN\_WAIT1.- El socket está cerrado, y la conexión esta finalizándose
  - FIN\_WAIT2.- La conexión está cerrada, y el socket está esperando que finalice la conexión remota
  - TIME\_WAIT.- El socket está esperando después de cerrarse que concluyan los

paquetes que siguen en la red

- CLOSED.- El socket no está siendo usado
- CLOSE\_WAIT.- La conexión remota ha finalizado, y se espera que se cierre el socket
- LAST\_ACK.- La conexión remota ha finalizado, y se espera que se cierre el socket. Esperando el acknowledgement.
- LISTEN.- El socket está esperando posibles conexiones entrantes
- CLOSING.- Ambos sockets han finalizado pero aún no fueron enviados todos los datos
- UNKNOWN.- El estado del socket no se conoce

#### 5.6.4 Comprobación de conexión de red. Comando tracert

El comando `tracert` determina la ruta tomada hacia un destino mediante el envío de mensajes de petición de eco del protocolo ICMP al destino con valores de campo de tiempo de vida (TTL) que crecen de forma incremental. La ruta muestra la lista de enrutadores entre el host de origen y un destino.

Por ejemplo, si queremos probar la conexión entre nuestro equipo y el host `www.google.es` tendríamos que ejecutar el siguiente comando que produciría la siguiente salida.

```
C:\Users\Usuario>tracert www.google.es

Traza a la dirección www.google.es [216.58.210.227]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2     3 ms     3 ms     2 ms    192.168.100.1
  3     4 ms     3 ms     3 ms    192.168.144.1
  4     *        5 ms     4 ms    129.red-81-41-226.staticip.rima-
t de.net [81.41.226.129]
  5     *        *        *        Tiempo de espera agotado ...
  6     *        *        *        Tiempo de espera agotado ...
  7     *        *        *        Tiempo de espera agotado ...
  8     *        12 ms    11 ms    84.16.8.59
  9    12 ms    13 ms    13 ms    216.239.43.159
 10   42 ms    26 ms    26 ms    216.239.56.37
 11   41 ms    26 ms    26 ms    66.249.94.47
 12   31 ms    26 ms    26 ms    mrs04s10-in-f227.1e100.net
[216.58.210.227]

Traza completa.
```

Básicamente, la salida muestra los nodos intermedios que hay que recorrer para llegar desde la máquina local hasta el host de destino, `www.google.es` en este ejemplo. Cada línea representa un salto, un enrutador con tres tiempos que indica lo que ha tardado el

paquete en llegar a él. Si aparece \* es que el paquete se ha perdido. Por defecto presentará la información de hasta 30 saltos y el tiempo de espera para cada uno de ellos es de 5 sg. Estos valores pueden modificarse con las opciones del comando. Si a partir de una línea solamente aparecen asteriscos es que no ha podido contactar con ese nodo.

### 5.6.5 Comprobación de conectividad con un equipo. Comando ping

Comprueba la conectividad de nivel IP en otro equipo TCP/IP al enviar mensajes de solicitud de eco del protocolo ICMP (*Protocolo de mensajes de control Internet*). Se muestra la recepción de los mensajes de solicitud de eco correspondientes, junto con sus tiempos de ida y vuelta. Ping es el principal comando de TCP/IP que se utiliza para solucionar problemas de conectividad, accesibilidad y resolución de nombres. Cuando se usa sin parámetros, ping muestra ayuda.

ping [-t] [-a] [-n <recuento>] [-w <espera>] {<nombre_destino>   <direcciónIP_destino>}	
Parámetro	Descripción
-t	Por defecto se envían 4 paquetes ICMP al destino para comprobar la conectividad. Con este parámetro se envían paquetes indefinidamente hasta que se detenga. Para ver estadísticas y continuar, presionar Ctrl-Interrumpir; para detener, presionar Ctrl+C.
-a	Especifica que la resolución de nombres inversa se realiza en la dirección IP de destino. Si es correcto, ping muestra el nombre de host correspondiente.
-n <recuento>	Especifica el número de mensajes de solicitud de eco enviados. El valor predeterminado es 4.
-w <espera>	Especifica el período de tiempo, en milisegundos, que se esperará a recibir el mensaje de respuesta de eco que corresponde a un mensaje de solicitud de eco. Si no se recibe el mensaje de respuesta de eco en el tiempo de espera, se muestra el mensaje de error "Tiempo de espera agotado para esta solicitud". El tiempo de espera predeterminado es 4000 ms (4 segundos).
<nombre_destino>   <direcciónIP_destino>	Especifica el destino, identificado por la dirección IP o el nombre de host.

Si una conexión de red de área local se ha configurado correctamente deberemos de tener acceso a los servicios de red disponibles. Si no es así, podemos realizar un conjunto de comprobaciones para detectar el error. Para ello seguir los siguientes pasos:

1. Para obtener rápidamente la configuración TCP/IP de un equipo, abrir Símbolo del sistema y, a continuación, ejecutar `ipconfig`. En los resultados del comando hay que asegurarse de que el adaptador de red de la configuración TCP/IP que está probando no se encuentra en el estado `Medios desconectados`.

2. En el símbolo del sistema, hacer ping a la dirección del bucle; para ello, escribir:  
ping 127.0.0.1.
3. Hacer ping a la dirección IP del equipo.
4. Hacer ping a la dirección IP de la puerta de enlace, o gateway, predeterminada. Si el comando ping no funciona, comprobar que la dirección IP de la puerta de enlace predeterminada es correcta y que la puerta de enlace (enrutador) está operativa.
5. Hacer ping a la dirección IP de un host remoto (que esté en una subred diferente). Si el comando ping no funciona, comprobar que la dirección IP del host remoto es correcta, que éste está operativo y que todas las puertas de enlace (enrutadores) que hay entre el equipo y el host remoto están en funcionamiento.
6. Hacer ping a la dirección IP del servidor DNS. Si el comando ping no funciona, compruebe que la dirección IP del servidor DNS es correcta, que éste está operativo y que todas las puertas de enlace (enrutadores) que hay entre el equipo y servidor DNS están en funcionamiento.
- 7.

#### 5.6.6 Comprobación de ruta. Comando pathping

El comando pathping proporciona información acerca de la latencia de red y pérdida de paquetes en saltos intermedios entre un origen y destino. Envía varios mensajes de solicitud de eco a cada enrutador entre un origen y destino durante un período de tiempo y, a continuación, calcula los resultados en función de los paquetes devueltos desde cada enrutador. Pathping realiza el equivalente del comando tracert mediante la identificación de los enrutadores que están en la ruta de acceso. Hace ping periódicamente a todos los enrutadores durante un período de tiempo especificado y calcula estadísticas en función del número que devuelve cada uno.

Este comando combina la funcionalidad de ping y tracert.

```
pathping [-g lista_host] [-h saltos_máx] [-i dirección] [-n]
[-p periodo] [-q núm_consultas] [-w tiempo_espera]
[-4] [-6] destino
```

Parámetro	Descripción
-g lista_host	Especifica que los mensajes de solicitud de eco utilizarán la opción ruta de origen no estricta en el encabezado IP con el conjunto de destinos intermedios especificados en lista_host. Con el enrutamiento de origen no estricto, destinos intermedios sucesivos pueden separarse por uno o varios enrutadores. El número máximo de direcciones o nombres en la lista de hosts es 9. lista_host es una serie de direcciones IP (en notación decimal con puntos) separadas por espacios.
-h saltos_máx	Especifica el número máximo de saltos en la ruta de acceso para buscar el destino (destino). El valor predeterminado es 30

	saltos.
-i dirección	Especifica la dirección de origen.
-n	No resuelve las direcciones IP de los enrutadores intermedios a sus nombres lo que acelera todo el proceso.
-p periodo	Especifica el número de milisegundos de espera entre pings consecutivos. El valor predeterminado es 250 milisegundos (1/4 de segundo).
-q num_consultas	Especifica el número de mensajes de solicitud de eco enviados a cada enrutador de la ruta de acceso. El valor predeterminado es 100 consultas.
-w tiempo_espera	Especifica el número de milisegundos para esperar cada respuesta. El valor predeterminado es 3.000 milisegundos (3 segundos).
-4   -6	Especifica que pathping solamente emplea IPv4 o IPv6
destino	Especifica el destino, que se identifica por el nombre de host o dirección IP.

### 5.6.7 Resolución de nombres. Comando nslookup

Nslookup.exe es una herramienta administrativa de la línea de comandos para probar y solucionar problemas de los servidores DNS. Muestra información que puede usarse para diagnosticar la infraestructura de DNS, es decir, nos permite comprobar si los servidores DNS de nuestro equipo resuelven correctamente las consultas que se le envían

Nslookup se puede ejecutar en dos modos: interactivo y no interactivo. El modo no interactivo es útil cuando sólo se necesita resolver una consulta. La sintaxis para el modo no interactivo es la siguiente:

nslookup [-opción] [nombre de host] [servidor]	
Parámetro	Descripción
-opción	<p>Especifica uno o varios comandos nslookup como una opción de la línea de comandos. Algunos de los subcomandos más habituales son:</p> <ul style="list-style-type: none"> <li>✓ -server direccionIP   nombreServidor.- Establece como servidor DNS predeterminado para realizar las consultas.</li> <li>✓ -retry=número.- Establece el número de reintentos para realizar una consulta DNS. Por defecto se utilizan 4 reintentos.</li> <li>✓ -timeout=milisegundos.- Especifica el número de milisegundos que se esperará por cada respuesta. El número predeterminado de segundos de espera es 5.</li> <li>✓ -type=tipoRecurso.- Especifica un tipo de registro de</li> </ul>

	<p>recursos DNS. El tipo de registro de recursos predeterminado es A. Más abajo hay una tabla que muestra los valores válidos para este comando.</p> <p>✓ <code>ls [opt] dominio [&gt; fichero].-</code> Muestra información sobre un dominio DNS. Esto es útil para ver todos los hosts que hay dentro de un dominio remoto. El resultado puede volcarse en un fichero. Las opciones que podemos usar son:</p> <ul style="list-style-type: none"> <li>-a Devuelve alias y nombres canónicos.</li> <li>-d Devuelve todos los datos del dominio</li> <li>-t Filtrará por tipo</li> </ul> <p>✓ <code>exit.</code>- Sale de nslookup.</p>
nombre_host	Busca información del host utilizando el servidor de nombres DNS predeterminado actualmente, si no se especifica otro servidor. Para buscar un equipo fuera del dominio DNS actual, cualificar completamente el nombre del host con un punto final.
servidor	Especifica que el servidor de nombres a enviar la consulta. Si se omite, se usará el servidor de nombres DNS predeterminado en la configuración IP.
-w <espera>	Especifica el período de tiempo, en milisegundos, que se esperará a recibir el mensaje de respuesta de eco que corresponde a un mensaje de solicitud de eco. Si no se recibe el mensaje de respuesta de eco en el tiempo de espera, se muestra el mensaje de error "Tiempo de espera agotado para esta solicitud". El tiempo de espera predeterminado es 4000 ms (4 segundos).
<nombre_destino>   <direccionIP_destino>	Especifica el destino, identificado por la dirección IP o el nombre de host.

Los tipos de recurso válidos para realizar consultas son los siguientes

Valor	Descripción
A	Especifica la dirección IP un equipo.
ANY	Especifica todos los tipos de datos.
CNAME	Especifica un nombre canónico para un alias.
GID	Especifica el identificador de grupo de un nombre de grupo.
HINFO	Especifica el tipo de CPU y sistema operativo de un equipo.
MB	Especifica un nombre de dominio de buzón
MG	Especifica un miembro de un grupo de correo.
MINFO	Especifica información del buzón o de la lista de correo.
MR	Especifica el nombre de dominio de correo cambiado.
MX	Especifica el intercambiador de correo.
NS	Especifica un servidor de nombres DNS de la zona con nombre.

PTR	Especifica un nombre del equipo si la consulta es una dirección IP. Si no, dirige el puntero a otra información.
SOA	Especifica el inicio de autoridad de una zona DNS.
TXT	Especifica la información de texto.
UID	Especifica el identificador de usuario.
UINFO	Especifica la información de usuario.
WKS	Describe un servicio conocido.

La sintaxis para el modo interactivo es la siguiente:

```
nslookup [-] [servidor]
```

Si queremos ejecutar nslookup en modo interactivo y utilizar un servidor DNS diferente al predeterminado deberemos utilizar el guión en lugar del nombre de host y a continuación indicar la dirección IP o el nombre del servidor DNS que queramos utilizar. Al entrar en modo interactivo mostrará un prompt. A partir de entonces solo hay que teclear la consulta a resolver para que muestre el resultado. Si queremos utilizar alguna opción de las anteriores, debemos anteponer set al nombre del comando y omitir el guión. La longitud de la línea de comandos debe ser menor de 256 caracteres.

### 5.6.8 Caché ARP. Comando arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones (ARP).

```
arp -s <dir_IP> <dir_MAC> [<interfaz>]
arp -d <dir_IP> [<interfaz>]
arp -a [<dir_IP>] [-N <interfaz>] [-v]
```

Parámetro	Descripción
-a <dir_IP>	Muestra las entradas ARP actuales. Si se especifica <dir_IP>, solo se muestran las direcciones IP y física del equipo especificado. Si existe más de una interfaz de red que utilice ARP, se muestran las entradas de cada tabla ARP. Se puede emplear también -g.
-v	Muestra las entradas ARP detalladas.
<dir_IP>	Especifica una dirección IP
-s <dir_IP> <dir_MAC>	Añade una entrada en la tabla ARP con la dirección IP y la dirección MAC asociada. Las direcciones MAC se especifican usando el guión medio - como separador de cada byte.
-d <dir_IP> [<interfaz>]	Elimina la entrada en la tabla ARP para el host especificado por <dir_IP> que puede incluir el carácter comodín * (asterisco) para eliminar todos los host.
-N <interfaz>	Muestra las entradas de la tabla ARP para la interfaz especificada.

### 5.6.9 Tabla de enrutamiento. Comando route

El comando route manipula la tabla de enrutamiento.

route [-f] [-p] [-4 -6] comando [destino] [MASK máscara_red] [puerta_enlace] [METRIC métrica] [IF interfaz]	
Parámetro	Descripción
-f	Borra las entradas de la tabla de enrutamiento.
-p	Crea una ruta persistente que se mantiene entre reinicios del sistema.
-4   -6	Especifica si es una ruta IPv4 o IPv6. Por defecto es IPv4
comando	Alguno de los siguientes: ✓ PRINT.- Imprime una ruta ✓ ADD.- Agrega una ruta ✓ DELETE.- Elimina una ruta ✓ CHANGE.- Modifica una ruta existente
destino	Dirección de red o host.
MASK máscara_red	Máscara de red en formato decimal punteada. Por defecto es 255.255.255.255
puerta_enlace	Dirección IP de siguiente salto.
METRIC metrica	Métrica de la ruta
IF interfaz	Interfaz de salida

### 5.6.10 Configuración de red. Utilidad netsh

Netsh es una utilidad de línea de comandos que permite mostrar y/o modificar la configuración de la red. Netsh interactúa con bibliotecas de enlace dinámico (dll) cada una de las cuales proporciona un conjunto de características denominado contexto. Un contexto proporciona un grupo de comandos específicos para un rol de servidor de red o característica concreta. Estos contextos amplían la funcionalidad de netsh al proporcionar la configuración y supervisión de uno o más servicios, utilidades o protocolos.

```
netsh [-a ArchAlias] [-c Contexto] [-r EquipoRemoto] [-u
[NombreDominio\]NombreUsuario] [-p Contraseña | *]
[Comando | -f ArchivoScript]
```

Si se ejecuta sin argumentos, se muestra el prompt netsh> para ejecutarse en modo interactivo. Si ejecutamos netsh /? veremos una lista de contextos y subcontextos disponibles. Si ejecutamos netsh contexto /? veremos una lista de comandos y subcontextos disponibles en un contexto concreto. Podemos ir aumentando argumentos a netsh y acabar con /\$ para ver la lista de comandos y contextos disponibles.

La cantidad de contextos, subcontextos y comandos dentro de un contexto aumenta exponencialmente las posibilidades de netsh. En este documento nos centraremos en la



configuración básica de red que incluye lo siguiente:

- ✓ Mostrar y cambiar la configuración de las interfaces de red. Contexto `interface`.
- ✓ Mostrar y/o cambiar la configuración DNS. Contexto `dns`.

Veamos algunos ejemplos. Para mostrar la configuración IP de las interfaces de red ejecutamos el siguiente comando `netsh`.

```
C:\> netsh interface ipv4 show config
C:\> netsh interface ipv4 show addresses
```

El segundo mostraría menos información que el primero. Si necesitamos asignar una configuración IP de forma estática a una interfaz de red debemos ejecutar el siguiente comando.

```
C:\> netsh interface ipv4 set address name="Ethernet"
source=static addr=192.168.0.10 mask=255.255.255.0
gateway=192.168.0.1
```

Vemos que estamos asignando la dirección IP 192.168.0.10/24 y puerta de enlace 192.168.0.1 a la interfaz de red con nombre Ethernet. A esta conexión de red faltaría asignar los servidores DNS para completar la configuración IP del ordenador. Lo haríamos con el siguiente comando `netsh`.

```
C:\> netsh interface ipv4 set dnsservers name="Ethernet"
source=static address=192.168.0.1
```

En este caso solamente podemos asignar un servidor DNS. Si queremos añadir más de uno tenemos que emplear el comando `add` en lugar de `set`, el cual nos permite gestionar entradas a una tabla. Para el ejemplo que nos ocupa sería una tabla de servidores DNS. Sería así

```
C:\> netsh interface ipv4 add dns "Ethernet" 192.168.0.1
C:\> netsh interface ipv4 add dns "Ethernet" 8.8.8.8 index=2
```

Vemos que `index=2` es para indicar que el segundo servidor DNS es secundario.

Para configurar una interfaz de red de forma dinámica tenemos también el comando `set` pero indicando un origen diferente.

```
C:\> netsh interface ip set address name="Ethernet" source=dhcp
C:\> netsh interface ipv4 set dnsserver name=Ethernet source=dhcp
```

Para desactivar o activar la interfaz de red tenemos los siguientes comandos

```
C:\> netsh interface set interface name=Ethernet admin=DISABLE
C:\> netsh interface set interface name=Ethernet admin=ENABLE
```

En lugar de usar nombres de las interfaces de red podemos emplear sus números de

índice. Con el siguiente comando listamos todas las interfaces de red.

```
C:\>netsh interface ipv4 show interfaces
```

El primer campo es el número de índice que podemos emplearlo en el argumento name visto en los comandos anteriores.

## 5.7 Gestión de la red en WPS

A continuación vamos a ver los cmdlets y funciones necesarios para realizar una gestión básica de la configuración de la red.

### 5.7.1 Ver las propiedades de los adaptadores de red. Función Get-NetAdapter

La función Get-NetAdapter obtiene las propiedades de las interfaces de red.

```
Get-NetAdapter
{ [-Name] <String[]> | -InterfaceDescription <String[]> |
-InterfaceIndex <UInt32[]> }
[-AsJob]
[-CimSession <CimSession[]>]
[-IncludeHidden] [-Physical]
[-ThrottleLimit <Int32>]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de las interfaces de red a mostrar. Admite caracteres comodín.
-InterfaceDescription <String[]>	Especifica un array de cadenas con las descripciones de las interfaces de red a mostrar. Admite caracteres comodín.
InterfaceIndex <UInt32[]>	Especifica un array con los números de índice de las interfaces de red a mostrar.

Para ver una referencia completa ejecutar el cmdlet Get-Help Get-NetAdapter -detailed.

Veamos algún ejemplo. Para mostrar todos los adaptadores de red del sistema ejecutaríamos el siguiente cmdlet.

```
PS C:\Windows\system32> Get-NetAdapter

Name      InterfaceDescription ifIndex Status MacAddress      LinkSpeed
-----
Ethernet  Intel(R) PRO...      11      Up      08-00-27-DC-D4-95 1 Gbps
```

Solo muestra un adaptador de red. Hubieramos conseguido el mismo efecto si ejecutamos el siguiente cmdlet.

```
PS C:\Windows\system32> Get-NetAdapter -Name Ethernet
```

### 5.7.2 Desactivar un adaptador de red. Comando Disable-NetAdapter

El cmdlet `Disable-NetAdapter` desactiva un adaptador de red. Esto provocará la pérdida de la conectividad de red en el especificado adaptador. Por defecto pedirá confirmación antes de desactivarlo.

```
Disable-NetAdapter
{ [[-Name] <String[]>] | -InterfaceDescription <String[]> |
-InputObject <CimInstance[]> }
[-AsJob]
[-CimSession <CimSession[]>]
[-IncludeHidden]
[-PassThru]
[-Confirm]
[-WhatIf]
[-ThrottleLimit <Int32>]
[<CommonParameters>]
```

Parámetro	Descripción
<code>-Name &lt;String[]&gt;</code>	Especifica un array de cadenas con los nombres de las interfaces de red a desactivar. Admite caracteres comodín.
<code>-InterfaceDescription &lt;String[]&gt;</code>	Especifica un array de cadenas con las descripciones de las interfaces de red a desactivar. Admite caracteres comodín.
<code>-InputObject &lt;CimInstance[]&gt;</code>	Especifica un array con objetos de tipo adaptador de red.

Para ver una referencia completa ejecutar el cmdlet `Get-Help Disable-NetAdapter -detailed`.

Veamos algún ejemplo. Para desactivar el adaptador de red Ethernet ejecutamos el siguiente cmdlet.

```
PS C:\Windows\system32> Disable-NetAdapter -Name Ethernet

Confirmar
¿Está seguro de que desea realizar esta acción?
Disable-NetAdapter 'Ethernet'
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspendir [?] Ayuda
(el valor predeterminado es "S"):
PS C:\Windows\system32>
```

### 5.7.3 Activar un adaptador de red. Función Enable-NetAdapter

El cmdlet `Enable-NetAdapter` activa un adaptador de red que está desactivado. De esta forma se recupera la conectividad de red en el adaptador.

```
Enable-NetAdapter
{ [[-Name] <String[]>] | -InterfaceDescription <String[]> |
-InputObject <CimInstance[]> }
[-AsJob]
[-CimSession <CimSession[]>]
[-IncludeHidden]
[-PassThru]
[-Confirm]
[-WhatIf]
[-ThrottleLimit <Int32>]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de las interfaces de red a activar. Admite caracteres comodín.
-InterfaceDescription <String[]>	Especifica un array de cadenas con las descripciones de las interfaces de red a activar. Admite caracteres comodín.
-InputObject <CimInstance[]>	Especifica un array con objetos de tipo adaptador de red.

Para ver una referencia completa ejecutar el cmdlet `Get-Help Disable-NetAdapter -detailed`.

Veamos algún ejemplo. Para activar el adaptador de red Ethernet que desactivamos en el ejemplo anterior ejecutamos el siguiente cmdlet.

```
PS C:\Windows\system32> Enable-NetAdapter -Name Ethernet
```

#### 5.7.4 Reiniciar un adaptador de red. Función Restart-NetAdapter

El cmdlet `Restart-NetAdapter` desactiva y vuelve a activar un adaptador de red.

```
Restart-NetAdapter
{ [[-Name] <String[]>] | -InterfaceDescription <String[]> |
-InputObject <CimInstance[]> }
[-AsJob]
[-CimSession <CimSession[]>]
[-IncludeHidden]
[-PassThru]
[-Confirm]
[-WhatIf]
[-ThrottleLimit <Int32>]
[<CommonParameters>]
```

Parámetro	Descripción
-Name <String[]>	Especifica un array de cadenas con los nombres de las

	interfaces de red a reiniciar. Admite caracteres comodín.
-InterfaceDescription <String[]>	Especifica un array de cadenas con las descripciones de las interfaces de red a reiniciar. Admite caracteres comodín.
-InputObject <CimInstance[]>	Especifica un array con objetos de tipo adaptador de red.

Para ver una referencia completa ejecutar el cmdlet `Get-Help Restart-NetAdapter -detailed`.

En el siguiente ejemplo se reinicia el adaptador de red Ethernet.

```
PS C:\Windows\system32> Restart-NetAdapter -Name Ethernet
```

### 5.7.5 Ver la configuración IP. Comandos `Get-NetIPConfiguration`, `Get-NetIPInterface` y `Get-NetIPAddress`

Para mostrar la configuración IP del sistema disponemos de tres comandos. El cmdlet `Get-NetIPConfiguration` muestra la configuración IP del equipo, lo que incluye interfaces, direcciones IP y servidores DNS.

<pre>Get-NetIPConfiguration     [{ -All   -InterfaceIndex &lt;Int32&gt; }]     [[-InterfaceAlias] &lt;String&gt;]     [-AllCompartments]     [-CimSession &lt;CimSession&gt;]     [-CompartmentId&lt;Int32&gt;]     [-Detailed]     [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-All	Obtiene la configuración de todas las interfaces, incluyendo las de bucle local, las virtuales y las desconectadas.
-InterfaceIndex <Int32>	Obtiene la configuración de la interfaz identificada por su número de índice.
-InterfaceAlias <String>	Obtiene la configuración de la interfaz identificada por su alias.

Para ver una referencia completa ejecutar el cmdlet `Get-Help Get-NetIPConfiguration -detailed`.

El siguiente ejemplo muestra la configuración IP de todas las interfaces.

```
PS C:\Windows\system32> Get-NetIPConfiguration
```

```
InterfaceAlias      : Ethernet
InterfaceIndex      : 11
```

```
InterfaceDescription : Intel(R) PRO/1000 MT Desktop Adapter
NetProfile.Name      : Red
IPv4Address          : 10.0.2.15
IPv6DefaultGateway   :
IPv4DefaultGateway   : 10.0.2.2
DNSServer            : 10.0.2.3
```

En este caso solamente disponemos de una interfaz de red activa. Vemos que las dos primeras propiedades son el alias y el índice de la interfaz. Con estos datos también podríamos obtener la configuración de la interfaz con los siguientes comandos

```
PS C:\Windows\system32> Get-NetIPConfiguration -InterfaceAlias Ethernet
PS C:\Windows\system32> Get-NetIPConfiguration -InterfaceIndex 11
```

Otro comando es `Get-NetIPInterface` que obtiene información de la configuración IP de las direcciones IP asociadas interfaces de red.

```
Get-NetIPInterface
[-InterfaceIndex <UInt32[]>]
[[-InterfaceAlias] <String[]>]
[-AddressFamily <AddressFamily[]>]
```

Parámetro	Descripción
-InterfaceIndex <Int32>	Obtiene la configuración IP de la interfaz identificada por su número de índice.
-InterfaceAlias <String>	Obtiene la configuración IP de la interfaz identificada por su alias.
- AddressFamily <AddressFamily[]>	Obtiene la configuración IP del protocolo especificado. Los valores aceptados son IPv4 e IPv6.

[Haz clic aquí para obtener la referencia completa.](#)

Por ejemplo, con el siguiente comando se muestran todas la configuración IP de todas las interfaces.

```
PS C:\Windows\system32> Get-NetIpInterface
```

Por último el comando `Get-NetIpAddress` muestra también la configuración IP.

```
Get-NetIpAddress
[[-IPAddress] <String[]>]
[-InterfaceIndex <UInt32[]>]
[-InterfaceAlias <String[]>]
[-AddressFamily <AddressFamily[]>]
```

Parámetro	Descripción
-IPAddress <String[]>	Especifica un array de direcciones IPv4 o IPv6.

-InterfaceIndex <UInt32>	Obtiene la configuración IP de la interfaz identificada por su número de índice.
-InterfaceAlias <String>	Obtiene la configuración IP de la interfaz identificada por su alias.
- AddressFamily <AddressFamily[]>	Obtiene la configuración IP del protocolo especificado. Los valores aceptados son IPv4 e IPv6.

[Haz clic para obtener una referencia completa.](#)

Con el siguiente ejemplo se obtiene la configuración IP de la interfaz Ethernet.

```
PS C:\Windows\system32> get-NetIPAddress -InterfaceAlias Ethernet

IPAddress      : fe80::4da3:5f90:846f:17f8%11
InterfaceIndex : 11
InterfaceAlias : Ethernet
AddressFamily  : IPv6
Type           : Unicast
PrefixLength   : 64
PrefixOrigin   : WellKnown
SuffixOrigin   : Link
AddressState   : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore

IPAddress      : 10.0.2.15
InterfaceIndex : 11
InterfaceAlias : Ethernet
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Dhcp
SuffixOrigin   : Dhcp
AddressState   : Preferred
ValidLifetime  : 19:31:50
PreferredLifetime : 19:31:50
SkipAsSource   : False
PolicyStore    : ActiveStore
```

### 5.7.6 Asignar propiedades a una interfaz de red. Comando Set-NetIpInterface

El cmdlet Set-NetIpInterface modifica una interfaz IP, incluyendo características DHCP, enrutamiento y Wake On LAN

```
Set-NetIPInterface
  [-InputObject <CimInstance[]>]
  [-InterfaceIndex <UInt32[]>]
  [[-InterfaceAlias] <String[]>]
  [-AddressFamily <AddressFamily[]>]
  [-Forwarding <Forwarding>]
  [-Dhcp <Dhcp>]
  [-PassThru]
  [-whatIf]
  [-Confirm]
  [<CommonParameters>]
```

Parámetro	Descripción
-InputObject <CimInstance[]>	Especifica un array de objetos de interfaz a los que se va a asignar propiedades.
-InterfaceIndex <UInt32>	Especifica la interfaz por su número de índice.
-InterfaceAlias <String>	Especifica la interfaz por su alias.
- AddressFamily <AddressFamily[]>	Especifica la versión del protocolo. Los valores aceptados son IPv4 e IPv6.
-Forwarding <Forwarding>	Especifica si se activa el enrutamiento en la interfaz. Valores admisibles son Enabled y Disabled
-Dhcp <Dhcp>	Especifica si la interfaz se configura mediante DHCP. Valores admisibles son Enabled y Disabled

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, activamos DHCP para la interfaz de red Ethernet

```
PS C:\Windows\system32> Set-NetIPInterface -InterfaceAlias Ethernet -
Dhcp Enabled
```

### 5.7.7 Asignar direcciones IP a interfaces. Comando New-NetIPAddress

El comando New-NetIPAddress crea y configura direcciones IP, IPv4 o IPv6 y se asigna a una interfaz de red. También se recomienda establecer una longitud de prefijo y una puerta de enlace.

Si ejecutamos este cmdlet y añadimos una dirección IP a una interfaz con DHCP habilitado, entonces DHCP es automáticamente deshabilitado. La nueva dirección IP no es utilizable hasta que finalice la detección de direcciones duplicadas.

```
New-NetIPAddress
  [-IPAddress] <String>
  -InterfaceAlias <String>
```



```

[-DefaultGateway <String>]
[-AddressFamily <AddressFamily>]
[-Type <Type>]
[-PrefixLength <Byte>]
[-ValidLifetime <TimeSpan>]
[-PreferredLifetime <TimeSpan>]
[-SkipAssSource <Boolean>]
[-PolicyStore <String>]
[-CimSession <CimSession[]>]
[-ThrottleLimit <Int32>]
[-AsJob]
[-WhatIf]
[-Confirm]
[<CommonParameters>]

```

Parámetro	Descripción
-InterfaceAlias <String>	Interfaz de red a la que se asocia la dirección IP
-IPAddress <String>	Dirección IP a crear.
[-PrefixLength <Byte>]	Longitud de prefijo (máscara de subred)
[-DefaultGateway <String>]	Puerta de enlace
- AddressFamily <AddressFamily[]>	Indica la versión del protocolo IP. Los valores aceptados son IPv4 e IPv6.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, el siguiente comando asigna la dirección IP 192.168.0.10/24 con puerta de enlace 192.168.0.1 a la interfaz de red Ethernet.

```

PS C:\Windows\system32> New-NetIPAddress -InterfaceAlias Ethernet -
IPAddress 192.168.0.10 -PrefixLength 24 -DefaultGateway 192.168.0.1

```

### 5.7.8 Eliminar direcciones IP de interfaces. Comando Remove-NetIPAddress

El cmdlet Remove-NetIPAddress eliminar una dirección IP de una interfaz. Si se omite la dirección IP a eliminar, se eliminan todas.

```

Remove-NetIPAddress
  [[-IPAddress] <String[]>]
  [-InterfaceIndex <UInt32[]>]
  [-InterfaceAlias <String[]>]
  [-AddressFamily <AddressFamily[]>]
  [-Type <Type[]>]
  [-PrefixLength <Byte[]>]

```

<pre>[-AddressState &lt;AddressState[]&gt;] [-DefaultGateway &lt;String&gt;] [-PassThru] [-WhatIf] [-Confirm] [&lt;CommonParameters&gt;]</pre>	
Parámetro	Descripción
-InterfaceAlias <String>	Interfaz de red especificada por su alias
-InterfaceIndex <Int32>	Interfaz de red especificada por su número de índice.
-IPAddress <String>	Dirección IP a eliminar.
[-PrefixLength <Byte>]	Longitud de prefijo (máscara de subred)
[-DefaultGateway <String>]	Puerta de enlace
- AddressFamily <AddressFamily[]>	Indica la versión del protocolo IP. Los valores aceptados son IPv4 e IPv6.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, podemos eliminar la dirección IP anterior mediante el siguiente comando

```
PS C:\Windows\system32> Remove-NetIPAddress -InterfaceAlias Ethernet -
IPAddress 192.168.0.10
```

```
Confirmar
¿Está seguro de que desea realizar esta acción?
Performing operation "Remove" on Target "NetIPAddress -IPv4Address
192.168.0.10 -InterfaceIndex 11 -Store Persistent"
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspendir [?] Ayuda
(el valor predeterminado es "S"):
```

### 5.7.9 Mostrar los servidores DNS. Comando Get-DnsClientServerAddress

El cmdlet Get-DnsClientServerAddress muestra las direcciones IP de los servidores de nombres asociados a una interfaz.

```
Get-DnsClientServerAddress
[-InterfaceIndex <UInt32[]>]
[[-InterfaceAlias] <String[]>]
[-AddressFamily <AddressFamily[]>]
[-CimSession <CimSession[]>]
[-ThrottleLimit <Int32>]
[-AsJob]
```

[<CommonParameters>]	
Parámetro	Descripción
-InterfaceAlias <String>	Interfaz de red especificada por su alias
-InterfaceIndex <Int32>	Interfaz de red especificada por su número de índice.
- AddressFamily <AddressFamily[]>	Indica la versión del protocolo IP. Los valores aceptados son IPv4 e IPv6.

[Haz clic para obtener una referencia completa.](#)

En el siguiente ejemplo se muestran los servidores DNS configurados en el equipo.

```
PS C:\Windows\system32> Get-DnsClientServerAddress

InterfaceAlias Interface Address ServerAddresses
              Index      Family
-----
Ethernet       11          IPv4      {10.0.2.3}
Ethernet       11          IPv6      {}
```

#### 5.7.10 Asignar un servidor DNS. Comando Set-DnsClientServerAddress

El cmdlet Set-DnsClientServerAddress establece uno o más servidores DNS asociados con una interfaz. Sobrescribe los servidores DNS obtenidos dinámicamente por DHCP.

Set-DnsClientServerAddress { [-InterfaceAlias] <String[]>   [-InterfaceIndex] <Int32[]>   -InputObject <CimInstance[]>} [-ServerAddresses <String[]>] [-validate] [-ResetServerAddresses] [-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [-AsJob] [-PassThru] [-whatIf] [-Confirm] [<CommonParameters>]	
Parámetro	Descripción
-InterfaceAlias <String[]>	Interfaces de red especificada por su alias
-InterfaceIndex <Int32[]>	Interfaces de red especificada por su número de índice.

-InputObject <CimInstance[]>]	Especifica un array de objetos de interfaz a los que se va a asignar los servidores DNS.
-ServerAddresses <String[]	Lista de direcciones de servidores DNS.
-Validate	Valida los servidores DNS antes de establecerlos.
-ResetServerAddresses	Restaura los servidores DNS a su valor por defecto.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para establecer en la interfaz Ethernet los servidores DNS 192.168.0.1 y 8.8.8.8.

```
PS C:\Windows\system32> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddress 192.168.0.1, 8.8.8.8
```

### 5.7.11 Comprobar las conectividad de red. Comando Test-NetConnection

El cmdle Test-NetConnection visualiza información de diagnóstico de una conexión de red. Realiza pruebas para ping, TCP, traza de ruta y diagnóstico de selección de ruta. Dependiendo de los parámetros de entrada la salida puede incluir resultados de búsquedas DNS, una lista de interfaces IP, resultados de selección de ruta y/o confirmación de establecimiento de conexión.

Test-NetConnection [[[-ComputerName] <String> { [-TraceRoute][-Hops <Int32>] [-CommonTCPPort] <String>   - Port <Int32> } [-InformationLevel] <String> [<CommonParameters>]	
Parámetro	Descripción
-ComputerName <String>	Nombre o dirección IP del ordenador con el que se quiere comprobar la conectividad.
-TraceRoute	Especifica que se haga una traza de rutas hasta el destino
-Hops <Int32>	Especifica el número de saltos máximo a atravesar en la traza de una ruta
-CommonTCPPort <String>	Especifica una lista de puertos TCP comunes. Valores aceptables son HTTP, RDP, SMB, WINRM
-Port <Int32>	Especifica el puerto remoto a comprobar
-InformationLevel <String>	Especifica el nivel de información a mostrar. Valores aceptables son Detailed y Quiet.

[Haz clic para obtener una referencia completa.](#)

Veamos algunos ejemplos. Si ejecutamos Test-NetConnection sin argumentos

realizará una prueba de conectividad con un servidor por defecto

```
PS C:\Windows\system32> Test-NetConnection

ComputerName           : internetbeacon.msedge.net
RemoteAddress          : 13.107.4.52
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.2.15
PingSucceeded          : True
PingReplyDetails (RTT) : 23 ms
```

Podemos repetir el cmdlet anterior pero con un nivel de información mayor.

```
PS C:\Windows\system32> Test-NetConnection -InformationLevel Detailed

ComputerName           : internetbeacon.msedge.net
RemoteAddress          : 13.107.4.52
NameResolutionResults  : 13.107.4.52
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.2.15
NetRoute (NextHop)     : 10.0.2.2
PingSucceeded          : True
PingReplyDetails (RTT) : 23 ms
```

Vamos a realizar la misma prueba pero indicando el servidor de destino.

```
PS C:\Windows\system32> Test-NetConnection -ComputerName www.google.com
-InformationLevel Detailed

ComputerName           : www.google.com
RemoteAddress          : 172.217.168.164
NameResolutionResults  : 172.217.168.164
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.2.15
NetRoute (NextHop)     : 10.0.2.2
PingSucceeded          : True
PingReplyDetails (RTT) : 44 ms
```

En el siguiente ejemplo vamos a comprobar el servidor web de Microsoft.

```
PS C:\Windows\system32> Test-NetConnection -ComputerName
www.microsoft.com -Port 80

ComputerName           : www.microsoft.com
```

```
RemoteAddress      : 23.211.9.92
RemotePort         : 80
InterfaceAlias     : Ethernet
SourceAddress      : 10.0.2.15
TcpTestSucceeded   : True
```

En el siguiente ejemplo obtenemos información de diagnóstico de ruta hasta el servidor de Google.

```
PS C:\Windows\system32> Test-NetConnection -ComputerName www.google.com
-Traceroute -InformationLevel Detailed
```

```
ComputerName       : www.google.com
RemoteAddress      : 172.217.168.164
NameResolutionResults : 172.217.168.164
InterfaceAlias     : Ethernet
SourceAddress      : 10.0.2.15
NetRoute (NextHop) : 10.0.2.2
PingSucceeded      : True
PingReplyDetails (RTT) : 31 ms
TraceRoute         : 10.0.2.2
                   : 0.0.0.0
                   : 10.195.84.1
                   : 0.0.0.0
                   : 62.42.228.62
                   : 74.125.242.161
                   : 74.125.253.201
                   : 172.217.168.164
```

#### 5.7.12 Resolución de nombres. Comando Resolve-DnsName

El cmdlet `Resolve-DnsName` realiza una búsqueda DNS. Su funcionalidad es similar al comando `nslookup`.

```
Resolve-DnsName
  [-Name] <String>
  [[-Type] <RecordType>]
  [-Server <String[]>]
  [<CommonParameters>]
```

Parámetro	Descripción
<code>-Name &lt;String&gt;</code>	Nombre que se quiere consultar a un servidor de nombres.
<code>[-Type] &lt;RecordType&gt;</code>	Especifica el tipo de registro DNS que se consulta. Por defecto es A
<code>-Server &lt;String[]&gt;</code>	Array de servidores DNS a los que se envía la consulta. Por

defecto la consulta se envía al servidor DNS configurado en la interfaz de red.

[Haz clic para obtener una referencia completa.](#)

En el siguiente ejemplo se consulta el nombre `www.microsoft.com`.

```
PS C:\Windows\system32> Resolve-DnsName -Name www.microsoft.com
```

Name	Type	TTL	Section	NameHost
----	----	---	-----	-----
www.microsoft.com	CNAME	17	Answer	
www.microsoft.com-c-3.edgekey.net				
www.microsoft.com-c-3.edgekey.net	CNAME	17	Answer	
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net				
www.microsoft.com-c-3.edgekey.net	CNAME	17	Answer	
e13678.dspb.akamaiedge.net				
net.globalredir.akadns.net				

Name : e13678.dspb.akamaiedge.net  
QueryType : AAAA  
TTL : 17  
Section : Answer  
IP6Address : 2a02:26f0:15:1:8100::356e

Name : e13678.dspb.akamaiedge.net  
QueryType : AAAA  
TTL : 17  
Section : Answer  
IP6Address : 2a02:26f0:15:1:9300::356e

Name : e13678.dspb.akamaiedge.net  
QueryType : A  
TTL : 17  
Section : Answer  
IP4Address : 23.211.9.92

Podemos consultar el servidor web de apple y enviar la consulta al servidor DNS de Google.

```
PS C:\Windows\system32> Resolve-DnsName -Name www.apple.com -Server 8.8.8.8
```

Name	Type	TTL	Section	NameHost
------	------	-----	---------	----------

```

www.apple.com CNAME 1055 Answer
www.apple.com.edgekey.net
www.apple.com.edgekey.net CNAME 1055 Answer
www.apple.com.edgekey.net.globalredir.akadns.net
www.apple.com.edgekey.net.glob CNAME 1055 Answer
e6858.dsce9.akamaiedge.net
alredir.akadns.net

```

```

Name       : e6858.dsce9.akamaiedge.net
QueryType  : AAAA
TTL        : 19
Section    : Answer
IP6Address : 2a02:26f0:b1:692::1aca

```

```

Name       : e6858.dsce9.akamaiedge.net
QueryType  : AAAA
TTL        : 19
Section    : Answer
IP6Address : 2a02:26f0:b1:6a0::1aca

```

```

Name       : e6858.dsce9.akamaiedge.net
QueryType  : A
TTL        : 6
Section    : Answer
IP4Address : 23.216.202.232

```

### 5.7.13 Mostrar la tabla de enrutamiento. Comando Get-NetRoute

El cmdlet Get-NetRoute obtiene información de la tabla de enrutamiento.

<b>Get-NetRoute</b> [[-DestinationPrefix] <String[]>] [-InterfaceIndex <UInt32[]>] [-InterfaceAlias <String[]>] [-AddressFamily <AddressFamily[]>] [<CommonParameters>]	
Parámetro	Descripción
[-DestinationPrefix] <String[]>	Especifica un array de redes de destino. Se obtendrán las rutas IP a las redes de destino indicadas. Una red de destino contiene una dirección IP y una longitud de prefijo separadas por barra /.



<code>[-InterfaceIndex &lt;UInt32[]&gt;]</code>	Obtiene la ruta asociadas a las interfaces indicadas por medio del array de números de índice de la interfaz de red.
<code>[-InterfaceAlias &lt;String[]&gt;]</code>	Obtiene la ruta asociadas a las interfaces indicadas por medio del array de nombres de interfaz de red.
<code>[-AddressFamily &lt;AddressFamily[]&gt;]</code>	Especifica la versión del protocolo IP. Valores aceptables son IPv4 e IPv6

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para mostrar toda la tabla de enrutamiento ejecutamos el siguiente cmd-let.

```
PS C:\Windows\system32> Get-NetRoute
```

```
ifIndex DestinationPrefix                                NextHop
RouteMetric ifMetric PolicyStore
-----
-----
```

```
256 25      ActiveStore
1      255.255.255.255/32                                0.0.0.0
256 75      ActiveStore
11     224.0.0.0/4                                        0.0.0.0
256 25      ActiveStore
1      224.0.0.0/4                                        0.0.0.0
256 75      ActiveStore
1      127.255.255.255/32                                0.0.0.0
256 75      ActiveStore
1      127.0.0.1/32                                       0.0.0.0
256 75      ActiveStore
1      127.0.0.0/8                                        0.0.0.0
256 75      ActiveStore
11     10.0.2.255/32                                      0.0.0.0
256 25      ActiveStore
11     10.0.2.15/32                                       0.0.0.0
256 25      ActiveStore
11     10.0.2.0/24                                        0.0.0.0
256 25      ActiveStore
11     0.0.0.0/0                                          10.0.2.2
0 25      ActiveStore
11     0.0.0.0/0                                          192.168.0.1
256 25      ActiveStore
11     ff00::/8                                          ::
256 25      ActiveStore
1      ff00::/8                                          ::
```

```
256 75      ActiveStore
11      fe80::4da3:5f90:846f:17f8/128      ::
256 25      ActiveStore
11      fe80::/64      ::
256 25      ActiveStore
1      ::1/128      ::
256 75      ActiveStore
```

Si restringimos la salida solamente a las rutas IPv6.

```
PS C:\Windows\system32> Get-NetRoute -AddressFamily IPv6

ifIndex DestinationPrefix      NextHop
RouteMetric ifMetric PolicyStore
-----
-----
```

```
256 25      ActiveStore
1      ff00::/8      ::
256 75      ActiveStore
11      fe80::4da3:5f90:846f:17f8/128      ::
256 25      ActiveStore
11      fe80::/64      ::
256 25      ActiveStore
1      ::1/128      ::
256 75      ActiveStore
```

#### 5.7.14 Crear una ruta. Comando New-NetRoute

El cmdlet New-NetRoute crea una ruta IP en la tabla de enrutamiento. Hay que especificar la red de destino y una interfaz de red de salida.

```
New-NetRoute
[-DestinationPrefix] <String>
{ -InterfaceAlias <String> | -InterfaceIndex <Int32> }
[-AddressFamily <AddressFamily>]
[-NextHop <String>]
[-RouteMetric <UInt16>]
[-whatIf]
[-Confirm]
[<CommonParameters>]
```

Parámetro	Descripción
[-DestinationPrefix] <String>	Especifica la red de destino. Una red de destino contiene una dirección IP y una longitud de prefijo separadas por barra /.
[-InterfaceIndex	Especifica el número de índice de la interfaz.

<UInt32>]	
[-InterfaceAlias <String>]	Especifica el nombre de la interfaz.
[-AddressFamily <AddressFamily[]>]	Especifica la versión del protocolo IP. Valores aceptables son IPv4 e IPv6
-NextHop <String>	Especifica la dirección IP de siguiente salto.
-RouteMetric <UInt16>	Indica la métrica de la ruta

[Haz clic para una referencia completa.](#)

En el siguiente ejemplo añade una ruta a la red 192.168.0.0/24.

```
PS C:\Windows\system32> New-NetRoute -DestinationPrefix 192.168.0.0/24 -
InterfaceAlias Ethernet -NextHop 10.0.2.2
```

ifIndex	DestinationPrefix	NextHop
RouteMetric	ifMetric	PolicyStore
-----	-----	-----
11	192.168.0.0/24	10.0.2.2
256	25	ActiveStore
11	192.168.0.0/24	10.0.2.2
256		Persiste...

### 5.7.15 Eliminar una ruta. Comando Remove-NetRoute

El cmdlet Remove-NetRoute elimina una ruta de la tabla de enrutamiento. Sin parámetros borra todas las rutas de la tabla de enrutamiento.

```
Remove-NetRoute
  [-DestinationPrefix] <String[]>
  [-InterfaceIndex <UInt32[]>]
  [-InterfaceAlias <String[]>]
  [-NextHop <String[]>]
  [-AddressFamily <AddressFamily[]>]
  [-RouteMetric <UInt16[]>]
  [-whatIf]
  [-Confirm]
  [<CommonParameters>]
```

```
Remove-NetRoute
  -InputObject <CimInstance[]>
  [-whatIf]
  [-Confirm]
  [<CommonParameters>]
```

Parámetro	Descripción
<code>[-DestinationPrefix] &lt;String&gt;</code>	Especifica la red de destino. Una red de destino contiene una dirección IP y una longitud de prefijo separadas por barra /.
<code>[-InterfaceIndex &lt;UInt32&gt;]</code>	Especifica el número de índice de la interfaz.
<code>[-InterfaceAlias &lt;String&gt;]</code>	Especifica el nombre de la interfaz.
<code>[-AddressFamily &lt;AddressFamily[]&gt;]</code>	Especifica la versión del protocolo IP. Valores aceptables son IPv4 e IPv6
<code>-NextHop &lt;String&gt;</code>	Especifica la dirección IP de siguiente salto.
<code>-RouteMetric &lt;UInt16&gt;</code>	Indica la métrica de la ruta
<code>-InputObject &lt;CimInstance[]&gt;</code>	Especifica un array de objetos de tipo ruta para eliminar.

[Haz clic para una referencia completa.](#)

Por ejemplo, para eliminar la ruta que hemos creado antes

```
PS C:\Windows\system32> Remove-NetRoute -DestinationPrefix
192.168.0.0/24 -NextHop 10.0.2.2

Confirmar
¿Está seguro de que desea realizar esta acción?
Performing operation "Remove" on Target "NetRoute -DestinationPrefix
192.168.0.0/24 -InterfaceIndex 11 -NextHop 10.0.2.2 -Store Active"
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspendir [?] Ayuda
(el valor predeterminado es "S"):
```

Si queremos eliminar todas las rutas asociadas a una interfaz.

```
PS C:\Windows\system32> Get-NetRoute -InterfaceAlias Ethernet | Remove-
NetRoute
```

#### 5.7.16 Mostrar las conexiones TCP. Comando Get-NetTCPConnection

El cmdlet Get-NetTCPConnection muestra las conexiones TCP actuales. Se emplea para ver las propiedades de una conexión TCP, que son: direcciones IP locales y remotas, puertos locales y remotos; y estado de la conexión.

```
Get-NetTCPConnection
[[-LocalAddress] <String[]>]
[[-LocalPort] <UInt16[]>]
[-RemoteAddress <String[]>]
[-RemotePort <UInt16[]>]
[-State <State[]>]
[<CommonParameters>]
```

Parámetro	Descripción
<code>[-LocalAddress]</code> <code>&lt;String[]&gt;</code>	Especifica dirección IP local de la conexión.
<code>[-LocalPort]</code> <code>&lt;UInt16[]&gt;</code>	Especifica el número de puerto local de la conexión
<code>-RemoteAddress</code> <code>&lt;String[]&gt;</code>	Especifica dirección IP remota de la conexión.
<code>-RemotePort</code> <code>&lt;UInt16[]&gt;</code>	Especifica el número de puerto remota de la conexión
<code>-State</code> <code>&lt;State[]&gt;</code>	Especifica el estado de la conexión.

[Haz clic para obtener una referencia completa.](#)

Por ejemplo, para ver un listado de todas las conexiones TCP ejecutamos el siguiente cmdlet.

```
PS C:\Windows\system32> Get-NetTCPConnection
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
::	49669	::				
0	596			Listen		
::	49668	::				
0	568			Listen		
::	49667	::				
0	1608			Listen		
::	49666	::				
0	980			Listen		
::	49665	::				
0	1016			Listen		
::	49664	::				
0	472			Listen		
::	445	::				
0	4			Listen		
::	135	::				
0	800			Listen		
0.0.0.0	50023	0.0.0.0		Bound		
0	980			Bound		
0.0.0.0	50021	0.0.0.0		Bound		
0	3424			Bound		
0.0.0.0	50020	0.0.0.0		Bound		
0	3424			Bound		
0.0.0.0	50019	0.0.0.0				

```

0          Bound          3424
0.0.0.0    50018          0.0.0.0
0          Bound          3424
0.0.0.0    50017          0.0.0.0
0          Bound          3424
0.0.0.0    49929          0.0.0.0
0          Bound          980
10.0.2.15  50023          40.67.254.36
443        Established Internet 980
10.0.2.15  50018          104.126.44.86
443        CloseWait  Internet 3424
10.0.2.15  49929          40.67.254.97 443
Established Internet      980
...

```

Si queremos ver las conexiones establecidas ejecutamos el siguiente cmdlet.

```

PS C:\Windows\system32> Get-NetTCPConnection -State Established

LocalAddress          LocalPort RemoteAddress
RemotePort State      AppliedSetting OwningProcess
-----
-----
10.0.2.15             50023    40.67.254.36
443                   Established Internet 980
10.0.2.15             49929    40.67.254.97
443                   Established Internet 980

```

Si queremos ver los servicios que hay operando en nuestro ordenador a través de los puertos de escucha ejecutamos el siguiente cmdlet.

```

PS C:\Windows\system32> Get-NetTCPConnection -State Listen

LocalAddress          LocalPort RemoteAddress
RemotePort State      AppliedSetting OwningProcess
-----
-----
::                  49669    ::
0                   Listen    596
::                  49668    ::
0                   Listen    568
::                  49667    ::
0                   Listen    1608
::                  49666    ::
0                   Listen    980
::                  49665    ::

```

```
0          Listen          1016
::          49664          ::
0          Listen          472
::          445           ::
0          Listen          4
::          135           ::
0          Listen          800
0.0.0.0     49669          0.0.0.0
0          Listen          596
0.0.0.0     49668          0.0.0.0
0          Listen          568
0.0.0.0     49667          0.0.0.0 0          Listen
1608
...
```

## 6 Bibliografía

---

BOTT, E. , *Introducing Windows 10 for IT Professionals Technical Overview*. 2016 Microsoft Press , ISBN 978-0-7356-9697-6

SOLVETIC SEGURIDAD, *Manual del editor de GPO local en Windows 10*. Junio 2016. [Accedido enero 2018]. Disponible en <<https://www.solvetic.com/tutoriales/article/2655-manual-del-editor-de-gpo-local-en-windows-10/>>

SS64, *Command line reference – Database and OS scripting*. [Accedido diciembre 2018]. Disponibles en <<https://ss64.com/nt/sc.html>>

POWERSHELL 5.1, 6, *PowerShell Documentation* [Accedido diciembre 2018]. Disponible en <<https://docs.microsoft.com/en-us/powershell/>>