

Unidad 2



Administración de software de base

Implantación de sistemas operativos





Índice

2.1. Administración de usuarios y grupos locales

- 2.1.1. Crear, modificar y editar usuarios y grupos
- 2.1.2. Cambiar la ruta del perfil del usuario

2.2. Seguridad de cuentas de usuario

- 2.2.1. Establecer la contraseña
- 2.2.2. Habilitar y deshabilitar cuentas de usuario

2.3. Seguridad de las contraseñas

- 2.3.1. Algoritmos para la elección de contraseñas seguras
- 2.3.2. Opciones de la contraseña: obligar a cambiar la contraseña, caducidad, etc
- 2.3.3. Cambiar la directiva de expiración de las contraseñas

2.4. Configuración del protocolo TCP/IP en un cliente de red

2.5. Configuración de la resolución de nombres

2.6. Lista de Comandos en terminales

- 2.6.1. Windows Powershell
- 2.6.2. Terminal de Linux



Introducción

En la unidad anterior vimos lo que era y cómo funcionaba un sistema operativo, pero esto no solo se limita a las aplicaciones o programas que el usuario final conoce.

A lo largo de los tiempos se ha ido implementando el software necesario en un sistema operativo para que se pueda realizar una mejor gestión de este y proteger todo lo posible este.

A todas estas herramientas que van de manera nativa en el sistema se le llama software de base, y como iremos viendo a lo largo de la unidad engloba multitud de términos y herramientas para la gestión de nuestro sistema y de nuestro equipo.

Cabe destacar que se verá durante toda la unidad distintos escenarios dependiendo del sistema que se use y que se usarán máquinas virtuales para cada prueba, ya que, en un equipo final, ciertas tareas no se pueden llevar a cabo porque cambiaría la correcta gestión del administrador.

Al finalizar esta unidad

- + Conoceremos los principales tipos de usuarios y grupos en los sistemas operativos.
- + Veremos cuales son los métodos más eficaces para fortalecer las cuentas de usuario.
- + Comprenderemos los distintos tipos de dotación de seguridad a las contraseñas de usuario.
- + Seremos capaz de configurar la red en un equipo cliente.
- + Habremos estudiado acerca de la configuración de la resolución de nombres en los equipos finales.
- + Conoceremos los comandos básicos de Windows y Linux y como se usan.



2.1.

Administración de usuarios y grupos locales

Lo primero que debemos hacer es definir dos conceptos principales:

Usuarios

Los usuarios son los ejecutores de las aplicaciones informáticas de un equipo en última instancia y necesitan de cuentas de acceso para poder identificarse en los equipos y poder trabajar en el sistema operativo en cuestión.

Si hablamos de tipos de usuarios, tenemos dos grandes grupos:

- > **Usuarios locales:** son cuentas de usuario que se crean en el mismo equipo y sin acceso a un dominio de red, se suele dar este caso en equipos domésticos.
- > **Usuarios globales:** estas son las cuentas que se crean en dominios o servidores y que tienen como función que se pueda conectar al dominio e iniciar sesión en distintos equipos unidos a este mismo dominio. Son los más usados en grandes empresas.

Sea un usuario local o un usuario global, siempre se guarda un registro de este usuario en el equipo de manera local.

Hemos de decir también, que en cuanto a usuarios globales nos referimos tenemos dos grupos que veremos más adelante en este mismo módulo: perfiles móviles y perfiles obligatorios.

Si hablamos de Windows, que es el principal software usado a nivel de sistema operativo, en cada perfil de usuario se almacena lo siguiente:

- > **Configuración inicial.** Son los datos de los programas instalados solo por el usuario, el historial de dicho usuario y sus archivos temporales.
- > **Información sobre preferencias de usuario.**
- > **Datos de programa.** Almacena los datos específicos de un programa, tanto si es de 32 como de 64 bits (se suele almacenar en sitios distintos).
- > **Entorno de red.** Accesos directos de red del usuario en cuestión.
- > **Elementos del escritorio.**
- > **Acceso directo a las impresoras configuradas.**
- > **Menú de Inicio.** Esto realmente es un acceso directo a las aplicaciones o programas definidos en el inicio.
- > **Mis documentos.** Documentos de sonido, video o simplemente de texto de pertenencia propia del usuario.



Grupos

Un grupo consiste en un grupo de usuarios que se encuentran categorizados en una misma clase para facilitar la gestión de estos. Un mismo usuario podrá pertenecer a varios grupos o a uno solo, pero siempre a uno. Normalmente estos grupos se usan para gestionar permisos y accesos a las distintas funciones de los sistemas.

De manera lógica, en un grupo puede haber varios usuarios, pero también puede haber uno solo, incluso ninguno.

Tenemos **dos tipos principales de grupos en los sistemas operativos:**

- > **Grupos de seguridad.** Son usados principalmente para asignar privilegios y permisos, son los más comunes e los grupos.
- > **Grupos de distribución.** Se suelen usar en entornos cloud o aplicaciones de correo para que la información llegue a varios usuarios al mismo tiempo, no suelen llevar consigo permisos ni privilegios especiales.

Vamos a hablar más específicamente de los grupos locales dentro de los grupos de seguridad, que al igual que pasaba con los usuarios son grupos que se crean en un equipo sin conexión al dominio y solo gestionan ese equipo en concreto, por lo que se añadirán a dichos grupos usuarios locales de manera general.

De manera principal, en Windows se crean 4 grupos locales principales, que son los siguientes:

- > **Administradores:** son los que pertenecen a este grupo los usuarios que tienen el control sobre el sistema y se encargan de su gestión., cuentan con todo tipo de permisos.
- > **Invitados:** es un grupo para usuarios que iniciarán sesión en el equipo de manera ocasional y cuentan con los permisos justos para poder trabajar en el equipo de manera temporal.
- > **Usuarios:** el principal de los grupos y donde suelen encontrarse la mayoría de los usuarios, o al menos deberían. Los usuarios comprendidos en este grupo pueden hacer un uso completo del equipo a falta de funciones de instalación de aplicaciones o de gestión de permisos y recursos ya que eso se encuentra a cargo del administrador.
- > **Usuarios avanzados:** estos usuarios realizan las mismas tareas que los usuarios normales en un principio per se le añade además el permiso para crear usuarios y grupos locales, pero solo podrán eliminar o modificar los de su propia creación.



2.1.1. Crear, modificar y editar usuarios y grupos

CREAR UNA CUENTA DE USUARIO LOCAL (WINDOWS 10):

1. Nos vamos a **Inicio** → **Configuración** → **Cuentas** → **Familia y otros usuarios**
2. Una vez aquí vemos que tenemos la opción **Otros usuarios** y aquí tenemos que seleccionar 'Agregar otra persona para este equipo'

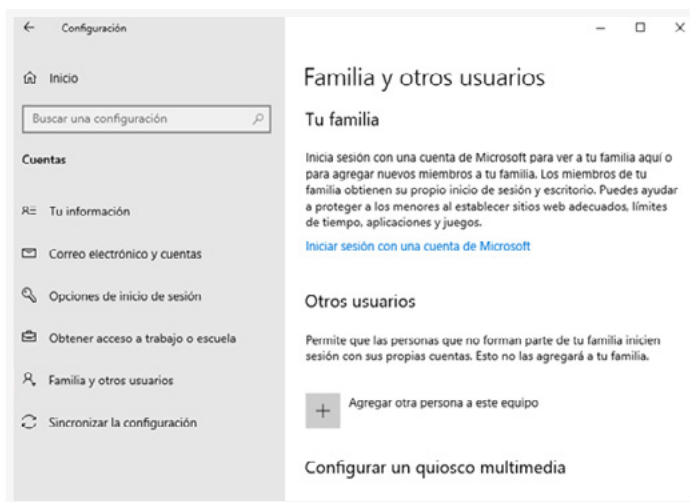


Imagen 31. Crear un usuario en Windows 10 1.

3. Nos pedirá que iniciemos con su cuenta de Microsoft y tendremos que seleccionar que no disponemos de inicio de sesión de Microsoft.
4. Después nos dirá que creamos una cuenta Microsoft y seleccionamos la opción de crear cuenta sin cuenta de Microsoft.
5. Nos aparecerá una ventana donde habrá que rellenar los datos del nuevo usuario.

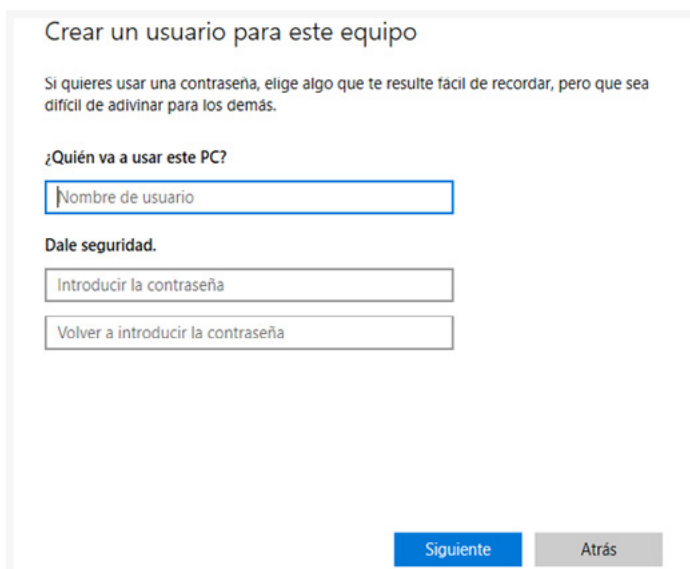


Imagen 32. Crear un usuario en Windows 10 2.



6. Ahora nos pedirá que, una vez puesta la contraseña, respondamos a unas preguntas de seguridad.
7. Ya estaría nuestro usuario creado y se vería de la siguiente forma:



Imagen 33. Crear un usuario en Windows 10 3.

EDITAR DATOS DE UNA CUENTA DE USUARIO (WINDOWS 10)

1. Seguimos los siguientes pasos: **Inicio** → **Panel de control** → **Cuentas de Usuario** → **Cuentas de usuario**.
2. Una vez aquí, seleccionaremos la opción '**Administrar otra cuenta**'.

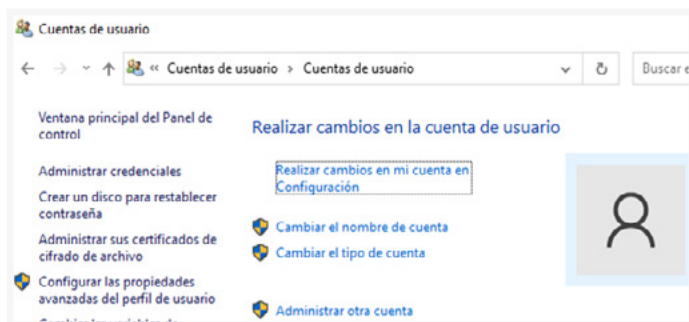


Imagen 34. Editar cuentas de usuario en Windows 10 1.

3. Aquí nos aparecerán diversas opciones de las principales del usuario, entre las que destaca 'Cambiar el tipo de cuenta'.

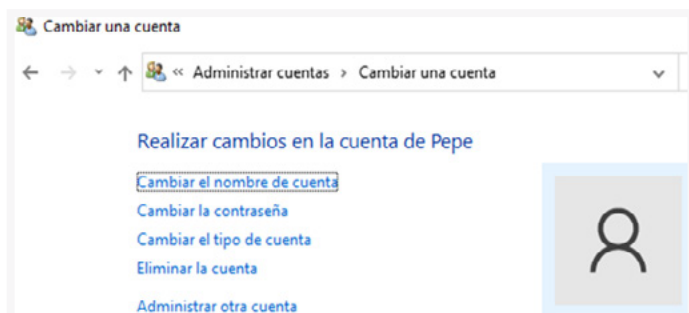


Imagen 35. Editar cuentas de usuario en Windows 10 2.



4. Con esta opción, lo que haremos será elegir si se trata de un usuario estándar o de un usuario administrador,

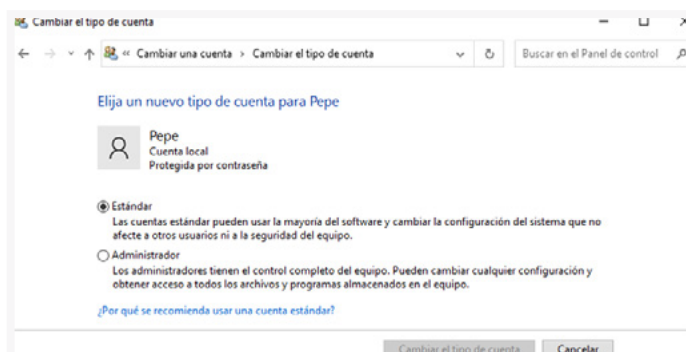


Imagen 36. Editar cuentas de usuario en Windows 10 3.

Debemos de tener en cuenta que este es solo uno de los métodos para tanto crear cuentas como editarlas en Windows 10, ya que hay numerosos.

ADMINISTRACIÓN LOCAL DE USUARIOS Y GRUPOS EN WINDOWS 10 CON POWERSHELL o POR CONSOLA

Windows 10 nos ofrece una herramienta moderna, llamada `lusrmgr.msc` o Administración local de usuarios y grupos.

Esta herramienta nos ayuda a que se haga una gestión de los usuarios de una manera aún más eficiente si se puede porque permite que se administren los usuarios y grupos locales.

Hay que tener en cuenta que esta función solo está disponible en Windows 10 Pro.

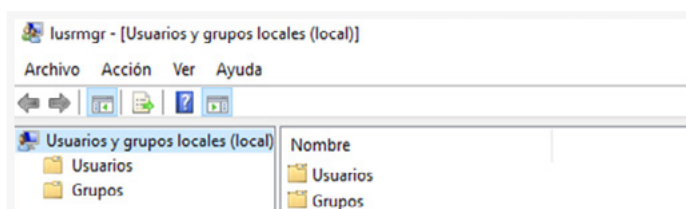


Imagen 37. Usuarios y grupos locales.

Además, para administrar los usuarios desde comandos, Windows nos ofrece dos comandos adicionales, para crear usuarios, `Net User` y para crear grupos, `Net LocalGroup`.



Como usar Net User

Para crear un usuario se usa el siguiente comando:

```
net user usuario contraseña /add
```

Para ver los usuarios que hay en una máquina local:

```
net user
```

Para modificar la contraseña de un usuario:

```
net user usuario nueva_contraseña
```

Para eliminar un usuario:

```
net user usuario /delete (/del)
```

Para desactivar un usuario:

```
net user usuario /active: no
```

Para activar un usuario:

```
net user usuario /active: yes
```

Cómo usar Net LocalGroup

Para agregar un grupo local:

```
net localgroup nombre_grupo /add
```

Para ver los grupos que hay en el equipo:

```
net localgroup
```

Para eliminar un grupo:

```
net localgroup nombre_grupo /del
```

Para añadir un comentario a un grupo:

```
net localgroup nombre_grupo /comment: "Implantación  
de Sistemas Operativos"
```

Para añadir un usuario a un grupo:

```
net localgroup nombre_grupo usuario /add
```

Para eliminar un usuario de un grupo:

```
net localgroup nombre_grupo usuario /delete
```



2.1.2. Cambiar la ruta del perfil del usuario

Windows 10 nos da por defecto acceso a una serie de carpetas personalizadas para el usuario que ayudan a que haya un mejor manejo de la información.

Estas carpetas se crean en la unidad C: y son Descargas, Documentos, Música, etc. El que se almacenen en el disco principal hace que de manera común se vaya acumulando ahí todo el rastro de estos archivos.

Es para solucionar esto por lo que se propone que haya una modificación de la ruta de dichas carpetas.

Para cambiar estas carpetas de ubicación debemos realizar lo siguiente:

Cambiar ubicación carpeta usuarios Windows 10

1. Lo primero que haremos será abrir el Explorador de Archivos de Windows 10 y nos iremos a la ruta que queremos como nueva ubicación de la carpeta.
2. Después, nos desplazamos hasta el menú de Inicio y donde pone "Nuevo2, seleccionamos la opción de "nueva carpeta".

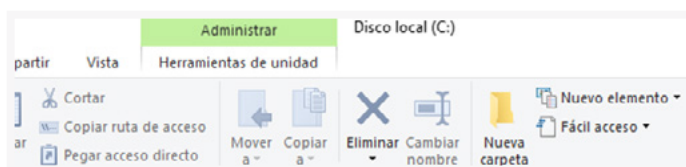


Imagen 38. Explorador de archivos de Windows 10.

También podemos usar la combinación de teclas Ctrl+Shift+N para crear esta carpeta nueva.

3. Ponemos a esta carpeta el nombre que deseamos.
4. Procedemos ahora a buscar en Inicio la opción Ejecutar.
5. Una vez dentro de ella escribimos lo siguiente: %HOMEPATH%.

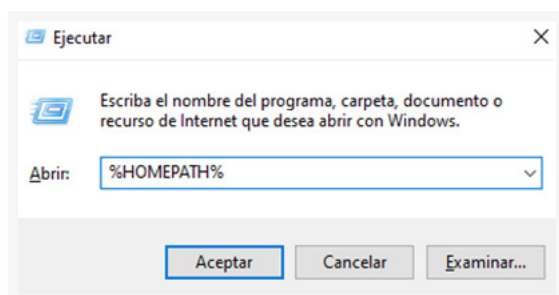


Imagen 39. Ejecutar.

6. Esta acción nos llevará a la carpeta raíz de usuario donde se almacenan todas las que hemos nombrado antes, y una vez aquí haremos click derecho sobre la que deseamos cambiar de ubicación y elegimos "Propiedades"

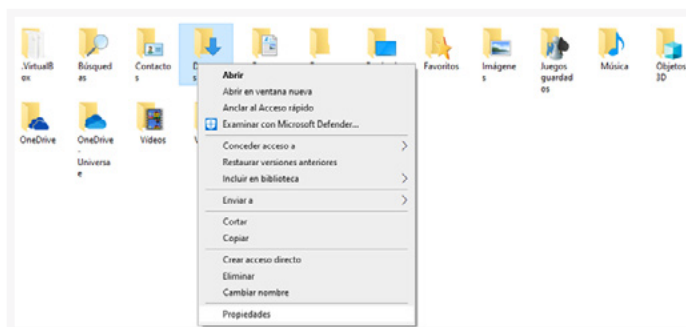


Imagen 40. Seleccionar la carpeta a mover.

7. Se nos abrirá una ventana emergente y tendremos que ir hasta la opción "Ubicación" y seleccionar dentro de esta la opción "mover".

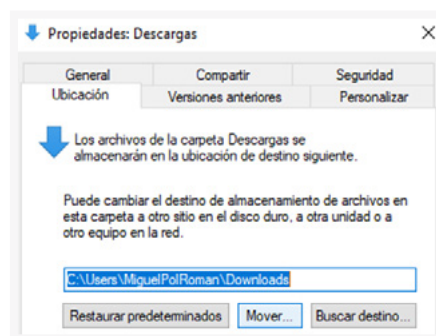


Imagen 41. Cambio de ruta.

8. Se nos abrirá otra ventana en la cual deberemos dirigirnos a la ruta donde se halla la nueva carpeta que queremos que sea la nueva ubicación de la nuestra.
9. Seleccionamos la carpeta, y damos en "Seleccionar carpeta", cuando retrocedamos veremos que se ha cambiado la ruta.
10. Damos en "Aplicar" y nos mostrará un mensaje advirtiéndonos de que se van a mover todos los archivos, habrá que decir que sí.
11. Entonces empezará a gestionar el cambio de todos los documentos de la carpeta y ya tendríamos modificada la ruta de la carpeta en cuestión para futuros objetos.



2.2.

Seguridad de cuentas de usuario

Para poder administrar la seguridad en las distintas cuentas de usuario, tenemos una herramienta en Windows que se llama Control de cuentas de usuario.

Esta herramienta nos ayuda a que haya una mayor protección frente a distintos malware y ataques de usuarios maliciosos. Un ejemplo que puede hacer UAC (acrónimo de Control de Cuentas de usuario) es que bloquea la instalación automática de aplicaciones que no estén autorizadas por el administrador además de bloquear cambios no autorizados en la configuración de nuestro sistema.

UAC permite que los usuarios se puedan loguear en el equipo como usuarios estándar a no ser que se definan también como administrador. Esta acción impide que durante la sesión se pueda ejecutar nada que necesite de las credenciales del administrador.

Hay ciertas aplicaciones que requerirán de permisos específicos para su ejecución, sobre todo las que no son nativas del sistema operativo en cuestión y son llamadas aplicaciones heredadas.

Para cualquier acción que requiera del permiso expreso del administrador, UAC nos dará la opción de añadir las credenciales de administrador, pero solo para esa acción, teniendo que volver a solicitarlas si necesitamos realizar cualquier otra función de administrador.

Esto nos lleva a plantear que salvo en casos específicos, incluso el administrador debería iniciar sesión en una cuenta estándar y funcionar así para no causar problemas en el equipo, ya que conoce las credenciales para poder realizar cualquier acción.

2.2.1. Establecer la contraseña

Como en prácticamente todos los sistemas, Windows nos da la opción de administrar la seguridad de sus contraseñas, para esto habrá que dirigirnos a:

Inicio → Configuración → Cuentas → Opciones de inicio de sesión

Una vez aquí, tenemos las distintas opciones de configuración de inicio de sesión en el equipo, las cuales podemos cambiar para nosotros y para los demás usuarios.



2.2.2. Habilitar y deshabilitar cuentas de usuario

Como hemos visto antes, las cuentas de usuario pueden deshabilitarse y volver a habilitarse dependiendo de las necesidades que tengamos, pero esta es una tarea que solo pueden ejecutar los administradores o en su defecto los usuarios avanzados con los usuarios que ellos mismos hayan creado.

Deshabilitar una cuenta significa que por mucho que se introduzcan credenciales, no se podrá acceder a la sesión.

Para deshabilitar una cuenta de usuario podemos o realizar por comandos como vimos anteriormente o realizar lo siguiente:

1. Volver a entrar en `lusrmgr.msc`.
2. Seleccionar el usuario en cuestión
3. Seleccionar "Propiedades".
4. Una vez dentro de propiedades, seleccionar la opción "La cuenta está deshabilitada".

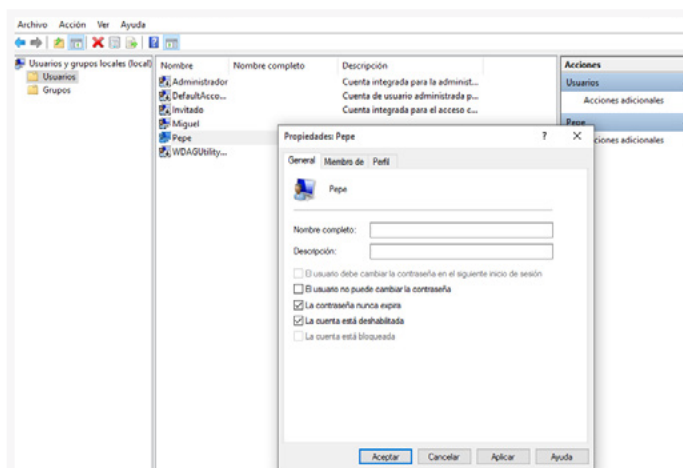


Imagen 42. Deshabilitar una cuenta de usuario.

Cabe destacar que esto tomará cabida para el próximo inicio de sesión y que ara volver a habilitar dicha cuenta solo tendremos que desmarcar esta opción.



2.3.

Seguridad de las contraseñas

Una de las principales razones por las que los usuarios quedan expuestos a ataques de otros usuarios es la poca seguridad recogida en sus contraseñas.

Para poder garantizar que las contraseñas sean seguras debemos de ver distintas medidas.

2.3.1. Algoritmos para la elección de contraseñas seguras

Existen una serie de algoritmos que nos ayudan a generar contraseñas robustas y eficientes. Para poder generar una contraseña segura de manera automática hay que tener en cuenta muchos factores porque si se establece un patrón, se podría predecir.

Lo lógico es que estos algoritmos creen una serie de contraseñas al azar que luego recibirán una pequeña modificación por parte del usuario con tal de que no sea exactamente igual a la generada.

Hay veces en las que los niveles de seguridad requeridos son muy altos y se usan unos algoritmos muy potentes que de hecho renuevan la contraseña de manera automática.

2.3.2. Opciones de la contraseña: obligar a cambiar la contraseña, caducidad, etc

Como ya se ha dicho anteriormente, las contraseñas son unos de los principales pilares de la seguridad informática y, además, se necesitan para acceder a equipos o plataformas, por lo que también debemos de poder modificarlas.

Lo más común en el día a día de un usuario es que esta contraseña se cambie cuando ya no es segura o cuando por la razón que sea, ha sido olvidada.

Es habitual que se establezcan ciertos protocolos de seguridad con la idea de que se mantenga una seguridad mínima en la creación de contraseñas, por ejemplo,

Windows requiere cuando son usuarios de dominio que la contraseña cumpla con estos requisitos:

- > No haberse usado en las últimas 5 contraseñas
- > Tener mínimo 8 caracteres
- > Uso de mayúsculas
- > Uso de minúsculas
- > Uso de números
- > Uso de caracteres alfanuméricos

2.3.3. Cambiar la directiva de expiración de las contraseñas

Una de las principales medidas que se usa como protocolo de seguridad de contraseñas es la caducidad de las contraseñas para obligarles a cambiarlas, por lo general suele ser cada 3 meses y es una práctica muy común en grandes empresas.



2.4.

Configuración del protocolo TCP/IP en un cliente de red

Con el fin de establecer una comunicación entre dos equipos, debemos tener en cuenta que los equipos llevan una configuración de red predefinida que habrá que cambiar en caso de querer tener una conexión específica.

A la hora de conectar equipos, el protocolo más usado es el TCP/IP, como ya se verá en la asignatura 'Planificación y Administración de Redes'. Para poder llevar a cabo una configuración lógica y que la red funcione mediante este protocolo necesita de los siguientes valores:

- > Una dirección IP válida que de manera general estará formada por 32 bits (IPv4) que se dividirán en cuatro grupos de decimales desde el 0 hasta el 255 y separados por puntos. Esta dirección hace la función de identificador de un equipo en la red. Un ejemplo de dirección IP es 198.10.20.54.
- > La máscara de subred que hace referencia a que parte de la dirección IP nos va a identificar la red donde se encuentra el equipo y a que parte hace referencia al propio equipo. Estos vuelven a ser valores de 32 bits de nuevo escritos en formato decimal donde la parte que no sea 0 indica lo que corresponde a la red y la parte que sea 0 indica qué corresponde al equipo.
- > Una puerta de enlace o Gateway para indicar al equipo hacia donde tiene que dirigirse para tener salida al exterior de la red, en una red domestica suele ser el router.
- > La identificación de que servidores DNS usará para conectarse. Estos servidores identificarán los nombres de una interfaz de red en sustitución de su IP, y es por esto por lo que podemos realizar búsqueda online sin tener que ir poniendo direcciones IP.

Hay tres tipos de direcciones IP que se configuran de manera normal:

- > **Estática:** la dirección IP es asignada de manera manual, ya sea por un administrador de toda la red o del equipo local.
- > **Dinámica:** la dirección IP viene designada por un servidor DHCP nada más haya conexión a red.
- > **Alternativa:** si no se cumple ninguna de las anteriores, se asigna una por el equipo de manera aleatoria.



Configuración TCP/IP y DNS en Windows

Windows instala por defecto los protocolos TCP/IP del tipo IPV4 e IPV6 la primera vez que detecte una interfaz de red activa.

Esto hará que se cree una conexión local que es configurable en cada adaptador de red disponible en el equipo, y para realizar dicha configuración debemos de seguir los siguientes pasos:

1. Primero vamos hasta **Inicio → Panel de control → Redes e Internet → Centro de redes y recursos compartidos**
2. Seleccionamos a la izquierda la opción "Cambiar configuración del adaptador"

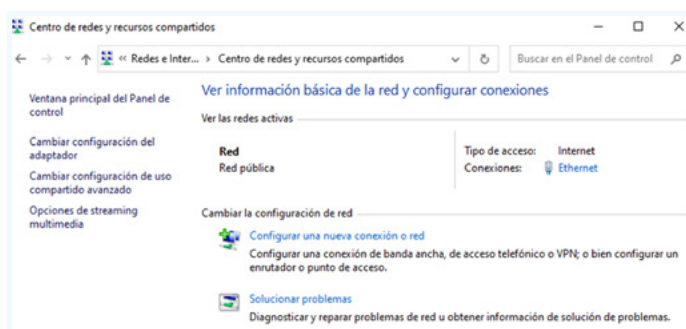


Imagen 8. Configuración de red en Windows 1.

3. Lo siguiente que haremos será seleccionar el adaptador que deseamos, realizar click derecho y seleccionar "Propiedades".

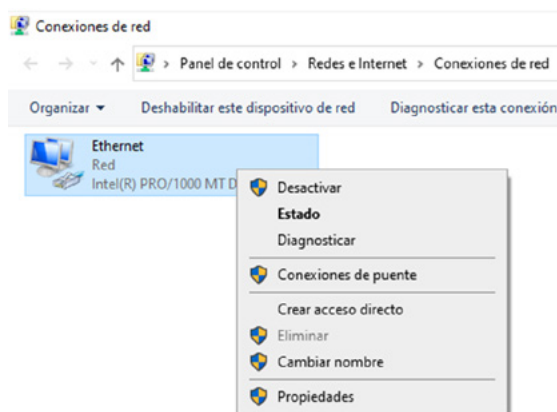


Imagen 9. Configuración de red en Windows 2.

4. Veremos que entonces aparecen un listado con todos los protocolos de red que registra dicho adaptador de red y los que están marcados quiere decir que están desinstalados.

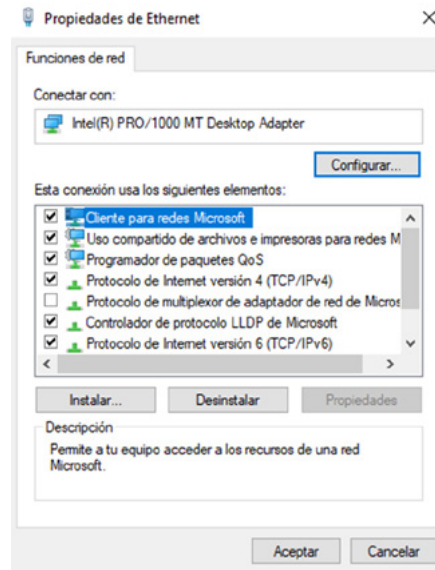


Imagen 10. Configuración de red en Windows 3.

5. El protocolo que a nosotros nos interesa es IPv4, que como podemos ver pone "Protocolo de Internet versión 4 (TCP/IPv4)".
6. Lo seleccionamos y veremos que tiene dos secciones principales, una para la IP y otra para la dirección DNS.
7. Por defecto, como podremos ver, Windows tiene de manera general activada la opción de DHCP, es decir, obtener tanto la dirección IP como los servidores DNS de manera automática.

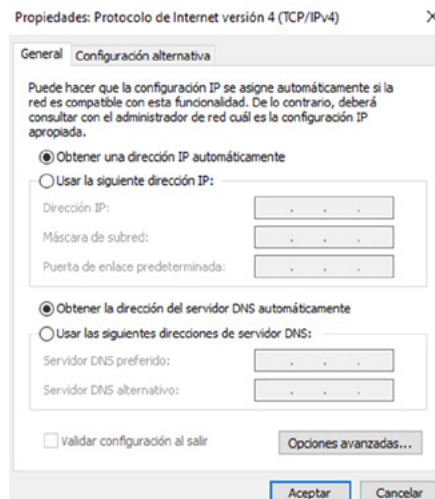


Imagen 11. Configuración de red en Windows 4.

8. Para realizar una configuración manual de las direcciones IP del equipo y servidores DNS, deberíamos seleccionar la opción "Usar la siguiente dirección IP" y "Usar las siguientes direcciones de servidor DNS". Pero para realizar esta acción, debemos de tener un conocimiento de las IPs y su funcionamiento, que aún no tenemos, es por esto por lo que, de momento, lo dejaremos automático.



9. Por último, tenemos la opción de "Opciones avanzadas", que nos muestra lo siguiente:

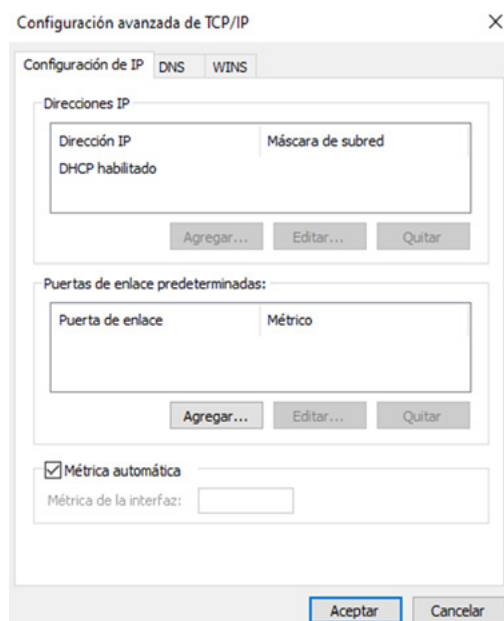


Imagen 12. Configuración de red en Windows 5.

10. Estas opciones sirven para que pueda haber más de una dirección IP a la vez, para una configuración más específica del DNS y para habilitar dominios de Windows respectivamente.

Vamos ahora a comprobar que tenemos conexión a internet, para eso lo primero que vamos a hacer es comprobar si tenemos realmente IP.

Nos vamos a:

Inicio → Símbolo del Sistema

Una vez aquí ejecutamos el siguiente comando:

`ipconfig /all`

Y debe de mostrarnos una serie de atributos como podemos ver a continuación:

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

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-ERDMQUM
Sufrido DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Sufrido DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-F8-19-F6
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::8183:19cb:11c6:f0ba%6(Preferido)
Dirección IPv4. . . . . : 10.0.2.15(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 25 de enero de 2022 7:05:47
La concesión expira . . . . . : miércoles, 26 de enero de 2022 7:05:49
Puerta de enlace predeterminada . . . . . : 10.0.2.2
Servidor DHCP . . . . . : 10.0.2.2
IAID DHCPv6 . . . . . : 101187623
DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-80-22-18-08-00-27-F8-19-F6
Servidores DNS. . . . . : 10.10.30.1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Imagen 13. `ipconfig /all`.



Aquí podemos observar que nos da un detalle más amplio de lo que realmente tenemos en red, ya que nos dice la IP, la MAC, la Máscara de red, la puerta de enlace predeterminada, etc.

Como podemos ver en la imagen anterior nuestra IP es 10.0.2.15, entonces, ahora vamos a otro equipo y realizaremos la acción ping para comprobarlo.

Ping es una herramienta provista por el 90% de los equipos con sistema operativo y red que lanza una serie de paquetes a una dirección en concreto, ya sea IP o DNS y nos avisa de la pérdida que hay, el tiempo que tarda y si está disponible dicha dirección, es decir, si tenemos conexión con esa dirección. Lógicamente, la comprobación la haremos desde otro equipo y queda tal que así:

```
C:\Users\Miguel>ping 10.0.2.15

Haciendo ping a 10.0.2.15 con 32 bytes de datos:
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.2.15: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.0.2.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Imagen 14. ping.

Como podemos ver, hay conexión y llegamos a este equipo, por lo que ya podríamos decir que tenemos el equipo listo para conectarse a la red y trabajar.

Configuración TCP/IP y DNS en Linux

Para la configuración de la red TCP/IP en Linux y del DNS tenemos varias opciones, una gráfica y otra por la línea de comandos o Terminal.

Vamos a ver la primera, en nuestro ejemplo usaremos Debian, que es una distro de Linux de las más usadas. Vamos a ver el proceso:

11. Lo primero que haremos será desplazarnos a la esquina superior derecha donde vemos que se encuentra el icono de red y nos da acceso a sus preferencias.

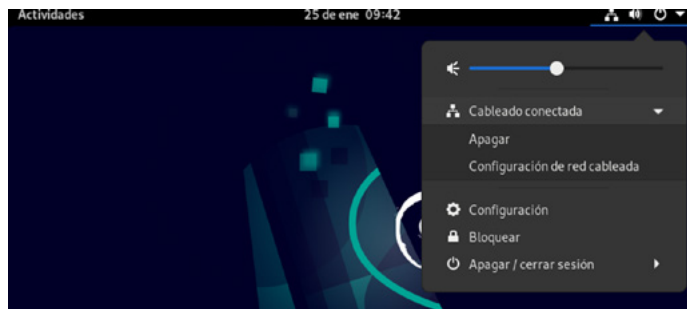


Imagen 1. Configuración de red en Debian 1



12. Una vez que estemos en la configuración de red veremos que tenemos varias opciones, entre ellas destaca la que nosotros queremos, que es la de red y que vemos en la siguiente imagen que nos aparece para configurar la conexión cableada (aparece la velocidad), la VPN, y el Proxy de red.

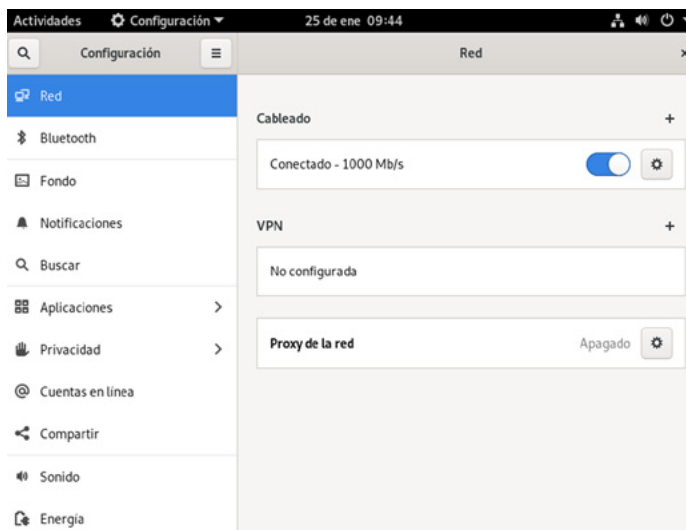


Imagen 2. Configuración de red en Debian 2

Aquí hay que destacar que en nuestro equipo no tenemos conexión Wifi, pero también aparecería ahí.

13. Si lo abrimos veremos que hay varias pestañas, relativas: Detalles, Identidad, IPv4, IPv6 y Seguridad.
14. En la primera pestaña podemos ver que nos dice la dirección IPv4 e IPv6 que nos corresponde, la MAC, el Gateway y el DNS predefinido además tres opciones que a la hora de la verdad no se suelen usar mucho. Sí que hay que poner ímpetu en que como podemos ver, podríamos eliminar el perfil de conexión, pero nos quedaríamos sin red.

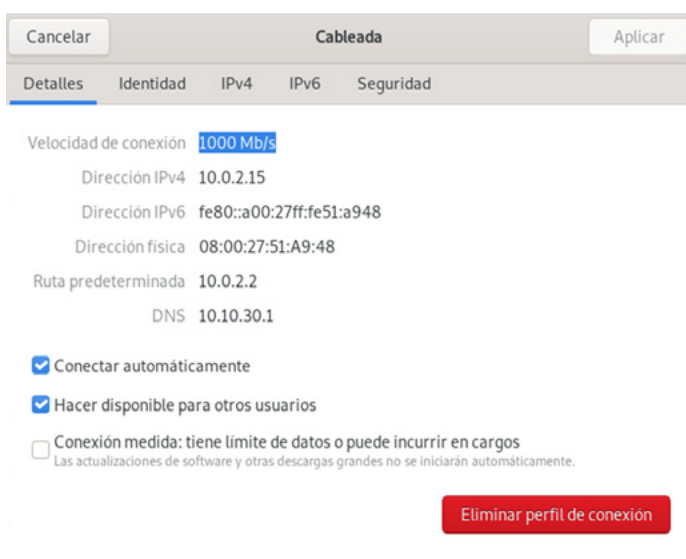


Imagen 3. Configuración de red en Debian 3.



15. Vamos a fijarnos simplemente en la pestaña IPv4, que es la que nos interesa ahora mismo, como podemos ver, de momento tenemos como pasaba con Windows, la opción de DHCP activada, y podríamos cambiarla a manual. Además, también tenemos una opción adicional que es desactivarla, activar solo enlace local y compartir la IP con otros equipos, pero de momento, no nos interesan, al igual que las rutas, que se verán en el módulo de Redes de este ciclo. La pestaña se ve tal que así:

Imagen 4. Configuración de red en Debian 4.

Ahora, para configurar la red por la línea de comandos se debería de hacer lo siguiente:

1. Vamos a abrir el terminal, nos vamos a **Actividades** y buscamos "Terminal".
2. Una vez abierto, tenemos que loguearnos como root, que es el usuario administrador de los sistemas Linux por excelencia, para eso, ejecutamos el comando:

su root

3. Ahora nos pedirá la contraseña de este usuario, la metemos y ya estaríamos logueados como root para poder realizar tareas administrativas en el equipo.

```
root@debian:/home/miguel#
```

Imagen 5. Configuración de red en Debian 5.

4. Una vez aquí, tenemos que conocer como se llama nuestra tarjeta de red, para eso lo que haremos será ejecutar el siguiente comando: `ip a`. Este comando nos dirá las interfaces de red disponibles en el equipo:

```
root@debian:/home/miguel# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:51:a9:48 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 81341sec preferred_lft 81341sec
    inet6 fe80:a00:27ff:fe51:a948/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Imagen 6. Configuración de red en Debian 6.

5. Como vemos, la interfaz de red activa ahora mismo se llama `enp0s3`.
6. Vale, ahora lo que tenemos que hacer es dirigirnos a la siguiente ruta, `/etc/network/interfaces.d`, y esto lo hacemos con el comando `cd`:

```
root@debian:/home/miguel# cd /etc/network/interfaces.d/
root@debian:/etc/network/interfaces.d#
```

Imagen 7. Configuración de red en Debian 7.

7. Aquí, si lanzamos el comando `ls`, veremos que no tenemos ahora mismo ningún fichero, pero en un principio, si quisiéramos realizar la configuración específica, deberíamos de crear un fichero con el nombre de la interfaz y realizar una cierta configuración.
8. Esta configuración es muy avanzada sintácticamente y se necesita conocer muy bien el entorno de una red para poder realizarla, por lo que, de momento, no lo veremos en esta unidad.



2.5.

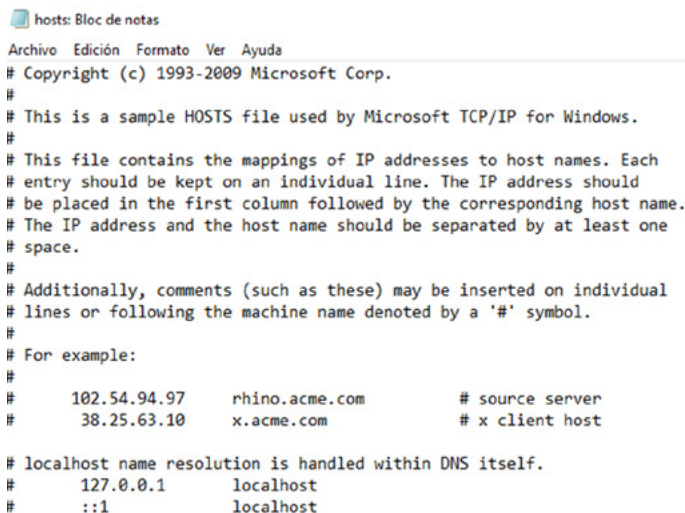
Configuración de la resolución de nombres

Si no disponemos de un servidor DNS activo en nuestra red, tendremos problemas a la hora de la configuración de red, por lo que tenemos que saber cómo se gestiona la resolución de nombres para un solo equipo en estas situaciones extraordinarias.

Windows

Para realizar la configuración de la resolución de nombres en Windows debemos de saber que esta se realiza en el siguiente fichero:

C:\Windows\System32\drivers\etc\hosts. El fichero solo puede ser editado por un administrador y tiene el siguiente aspecto:



```

hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
    
```

Imagen 27. Archivo hosts de Windows.

Este archivo funciona del siguiente modo: el sistema consulta aquí antes de realizar cualquier búsqueda, ve si hay una combinación de IP y nombre y si es así, realiza la búsqueda. En caso contrario, no sabrá llegar.

Para que varios equipos en red se puedan comunicar entre sí, deben de tener las mismas entradas.

Como hemos dicho antes, para poder editarlo es necesario ser administrador, pero no se puede realizar directamente, por lo que habrá que ir a Inicio, buscar el "Bloc de Notas" o cualquier editor de texto y abrirlo como Administrador.

Una vez que se realice esto deberemos de desplazarnos hasta el archivo con la opción de "Abrir" que traen todos los editores.

Cuando estemos en el propio archivo, para añadir una línea debemos de hacerlo con la combinación:

Ip nombre_equipo

Linux

Al igual que pasaba con Windows, tenemos un fichero en el cual se almacenan las direcciones de debe de tomar el equipo, este fichero se encuentra en la ruta /etc y es el fichero hosts.

Si lanzamos en esta ruta el comando `cat hosts`, nos mostrará el contenido del fichero, que es este:



```

miguel@debian: ~
root@debian:/etc# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      debian

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
    
```

Imagen 28. Archivo hosts de Linux.

Podemos editarlo lanzando como root, el comando `nano /etc/hosts` y su estructura sería la misma que en Windows.



2.6.

Lista de Comandos en terminales

2.6.1. Windows Powershell

- > **cd** → Para movernos entre directorios.
- > **dir** → Para listar el contenido de una carpeta.
- > **Tree** → Para mostrar la estructura en árbol de una carpeta.
- > **Cls** → Para limpiar la ventana de la consola.
- > **Move** → Para mover archivos.
- > **Rename** → Para renombrar archivos o directorios.
- > **MD** → Para crear una carpeta.
- > **Type** → Para crear un archivo.
- > **Get-Command** → Conocemos todos los cmdlets y comandos disponibles en PowerShell.
- > **Get-Host** → Nos da a conocer la versión de Powershell que está usando el sistema.
- > **Get-History** → Nos muestra un historial de todos los comandos de una misma sesión de Powershell.
- > **Get-Random** → Nos muestra un número aleatorio entre 0 y 2.147.483.646.
- > **Get-Service** → Nos dice que servicios están instalados en el sistema.
- > **Get-Help** → Nos muestra ayuda sobre los cmdlets y cómo usarlos.
- > **Get-Date** → Nos dice la fecha y hora actuales.
- > **Copy-Item** → Para copiar archivos o directorios.
- > **Invoke-Command** → Para ejecutar un script o un comando concretos.
- > **Invoke-WebRequest** → Se hace un inicio de sesión, un scraping o la descarga de información de un sitio web concreto
- > **Set-ExecutionPolicy** → Para cambiar políticas de seguridad a script o programas.
- > **Get-Item** → Para buscar información sobre un elemento en concreto.
- > **Remove-Item** → Para borrar elementos concretos.
- > **Get-Content** → Examina y muestra el contenido de un archivo.
- > **Set-Content** → Para almacenar texto en un archivo.
- > **Get-Variable** → Para ver en contenido de una variable.
- > **Set-Variable** → Para modificar o crear el contenido de una variable.
- > **Get-Process** → Para ver información acerca de los procesos en ejecución.
- > **Start-Process** → Para iniciar procesos.
- > **Stop-Process** → Para parar procesos.
- > **Start-Service** → Para iniciar servicios.
- > **Stop-Service** → Para parar servicios.
- > **Exit** → Para salir de PowerShell.

Cabe destacar que algunos comandos ya estaban disponibles en el símbolo del Sistema de Windows, pero la gran mayoría son nuevos de Powershell.

Además, todos estos comandos se pueden escribir tanto en mayúscula como en minúscula.



2.6.2. Terminal de Linux

- > **pwd** → Te da a conocer el directorio actual de trabajo.
- > **cd** → Nos ayuda a movernos entre rutas.
- > **ls** → Lista los contenidos de un directorio.
- > **cat** → Muestra el contenido de un archivo.
- > **cp** → Copia un archivo o directorio.
- > **mv** → Mueve un archivo o directorio.
- > **mkdir** → Para crear un directorio.
- > **rmdir** → Para borrar un directorio.
- > **rm** → Para borrar un archivo.
- > **touch** → Para crear un nuevo archivo sin contenido.
- > **locate** → Para localizar un archivo.
- > **find** → Para buscar un archivo más profundamente.
- > **grep** → Para filtrar en un mismo archivo.
- > **sudo** → Para elevarnos de privilegios.
- > **df** → Para conocer el estado del espacio en disco.
- > **du** → Para comprobar cuanto ocupa un archivo o un directorio.
- > **head** → Para ver las primeras líneas de un archivo cualquiera.
- > **tail** → Para ver las últimas líneas de un archivo de texto.
- > **diff** → Para comparar dos archivos línea por línea.
- > **tar** → Para comprimir una carpeta o varios archivos.
- > **chmod** → Para cambiar los permisos de archivos y directorios.
- > **chown** → Para cambiar el propietario de un archivo o directorio.
- > **jobs** → Muestra todos los trabajos en ejecución y en qué estado se encuentran.
- > **kill** → Para matar procesos.
- > **wget** → Para descargar archivos de internet.
- > **top** → Para mostrar los procesos en ejecución y el consumo de recursos de cada uno.
- > **history** → Para ver los comandos que se han usado en un periodo de tiempo definido.
- > **man** → Muestra el manual de un comando.
- > **echo** → Añade datos a un archivo.
- > **zip** → Para comprimir archivos.
- > **unzip** → Para descomprimir archivos.
- > **hostname** → Para ver el nombre de nuestro equipo.
- > **useradd** → Para añadir un usuario.
- > **userdel** → Para eliminar un usuario.

Cabe destacar que todos los comandos en Linux diferencian entre mayúsculas y minúsculas, por lo que el uso de estas puede generar que no se obtenga el resultado esperado.

Además, para finalizar, muchos de estos comandos necesitarán de permisos de superusuario para poder ejecutarse.



 www.universae.com

