

Comandos de cmd avanzados

1. Verificar la integridad del sistema: ejecuta "sfc /scannow" para buscar y reparar archivos del sistema dañados o corruptos.

```
C:\Windows\System32>sfc /scannow

Iniciando examen en el sistema. Este proceso tardará algún tiempo.

Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 100%.

Protección de recursos de Windows no encontró ninguna infracción
de integridad.

C:\Windows\System32>
```

2. Verificar si hay actualizaciones de seguridad: ejecuta "wmic qfe list" para ver una lista de todas las actualizaciones instaladas, incluidas las actualizaciones de seguridad.

```
C:\Windows\System32>wmic qfe list
Caption
InstalledOn Name ServicePackInEffect Status
http://support.microsoft.com/?kbid=5056579 ANIBAL Update
4/25/2025
https://support.microsoft.com/help/5058499 ANIBAL Update
5/30/2025
5/14/2025
5/30/2025
CSName Description FixComments HotFixID InstallDate InstalledBy
ANIBAL Security Update KB5058523 NT AUTHORITY\SYSTEM
ANIBAL Update KB5059502 NT AUTHORITY\SYSTEM

C:\Windows\System32>
```

3. Verificar los permisos de archivos y carpetas: ejecuta "icacls [ruta del archivo o carpeta]" para verificar los permisos y la propiedad de los archivos y carpetas.

```
C:\Windows\System32>icacls C:\Users\aniba\Downloads\Ironhack
C:\Users\aniba\Downloads\Ironhack NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administradores:(OI)(CI)(F)
ANIBAL\aniba:(OI)(CI)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos

C:\Windows\System32>
```

4. Escanear en busca de virus y malware: ejecuta "sfc /scanfile=[ruta del archivo]" para escanear un archivo específico en busca de virus y malware.

```
C:\Windows\System32>sfc /verifyfile=C:\Windows\System32\kernel32.dll
```

```
Protección de recursos de Windows no encontró ninguna infracción de integridad.
```

```
C:\Windows\System32>
```

5. Verificar la configuración de Firewall: ejecuta "netsh advfirewall show allprofiles" para ver la configuración del Firewall de Windows.

```
C:\Windows\System32>netsh advfirewall show allprofiles
```

```
Configuración de Perfil de dominio:  
-----
```

6. Bloquear un puerto específico: ejecuta "netsh advfirewall firewall add rule name="[nombre de la regla]" dir=in action=block protocol=TCP localport=[número de puerto] enable=yes" para bloquear el tráfico en un puerto específico.

```
C:\Windows\System32>netsh advfirewall firewall add rule name="Bloquear puerto 445" dir=in action=block protocol=TCP localport=445 enable=yes  
Aceptar
```

```
C:\Windows\System32>
```

7. Verificar la configuración de red: ejecuta "ipconfig /all" para ver la configuración de red de tu PC, incluyendo la dirección IP, la puerta de enlace predeterminada y el servidor DNS.

```
C:\Windows\System32>ipconfig /all
```

```
Configuración IP de Windows
```

8. Cambiar la contraseña de administrador: ejecuta "net user administrator *[nueva contraseña]" para cambiar la contraseña de la cuenta de administrador.

```
C:\Windows\System32>net user administrator *
```

```
No se ha encontrado el nombre de usuario.
```

```
Puede obtener más ayuda con el comando NET HELPMSG 2221.
```

```
C:\Windows\System32>
```

9. Cambiar el tiempo de espera de la pantalla de inicio de sesión: ejecuta "net accounts /maxpwage:[número de días]" para cambiar el tiempo de espera de la pantalla de inicio de sesión.

```
C:\Windows\System32>net accounts /maxpwage:90
Se ha completado el comando correctamente.
```

```
C:\Windows\System32>
```

10.Verificar las cuentas de usuario: ejecuta "net user" para ver una lista de todas las cuentas de usuario del sistema.

```
C:\Windows\System32>net user

Cuentas de usuario de \\ANIBAL
```

11.Verificar las conexiones de red activas: ejecuta "netstat -a" para ver una lista de todas las conexiones de red activas en tu PC.

```
C:\Windows\System32>netstat -a
```

Conexiones activas

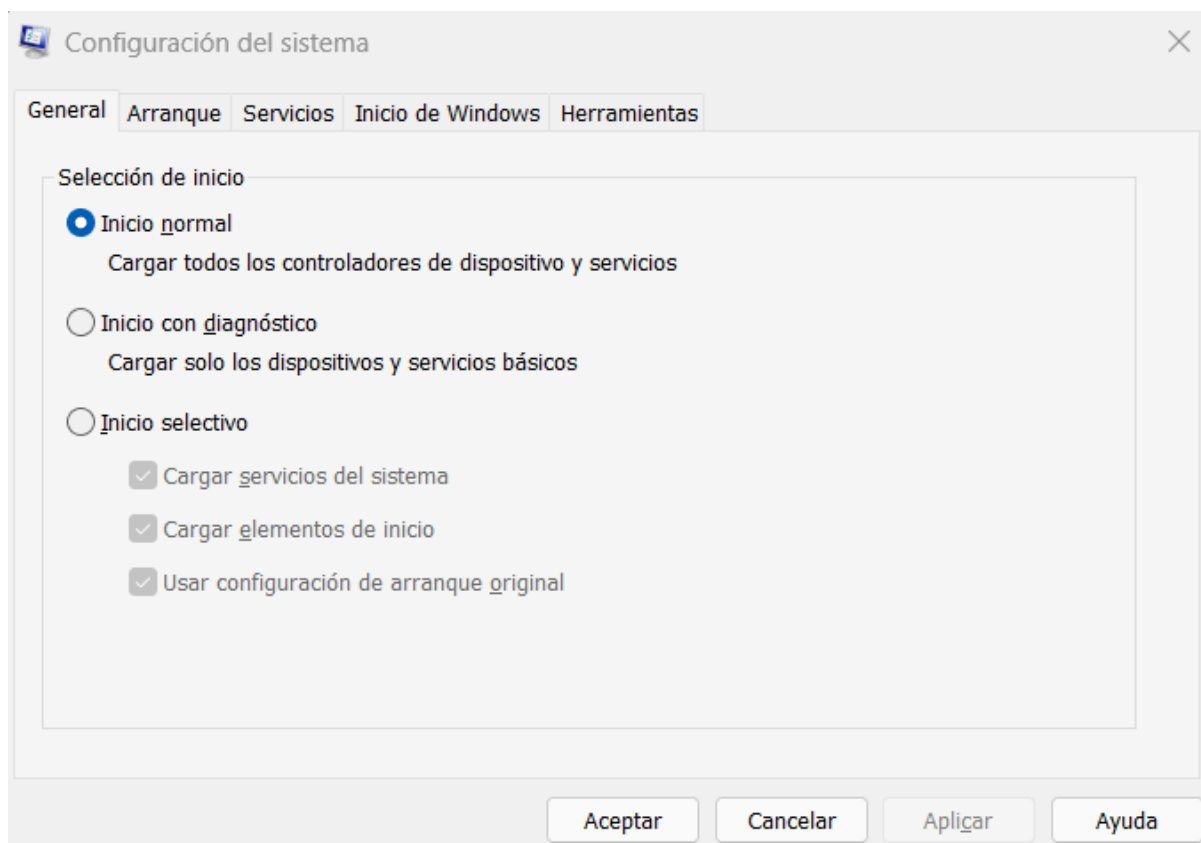
Proto	Dirección local	Dirección remota	Estado
-------	-----------------	------------------	--------

12.Verificar los servicios en ejecución: ejecuta "sc query" para ver una lista de todos los servicios en ejecución en tu PC.

```
C:\Windows\System32>sc query
```

```
NOMBRE_SERVICIO: AdobeARMservice
NOMBRE_MOSTRAR : Adobe Acrobat Update Service
```

13.Verificar los programas de inicio: ejecuta "msconfig" para ver una lista de los programas que se ejecutan automáticamente al iniciar el sistema.



14. Verificar la configuración de seguridad de Internet Explorer: ejecuta "reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" para ver la configuración de seguridad de Internet Explorer.

```
C:\Windows\System32>reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
ActiveXCache REG_SZ C:\Windows\Downloaded Program Files
CodeBaseSearchPath REG_SZ CODEBASE
EnablePunycode REG_DWORD 0x1
MinorVersion REG_SZ 0
WarnOnIntranet REG_DWORD 0x1

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents
```

15. Verificar la configuración de BitLocker: ejecuta "manage-bde -status" para ver el estado de BitLocker en tu PC.

```
C:\Windows\System32>manage-bde -status
Cifrado de unidad BitLocker: versión de la herramienta de configuración 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.
```

16. Verificar las políticas de seguridad local: ejecuta "secedit /export /areas securitypolicy /cfg C:\security.cfg" para exportar las políticas de seguridad local.

```
C:\Windows\System32>secedit /export /areas securitypolicy /cfg C:\security.cfg

La tarea se ha completado correctamente.
Consultar el registro %windir%\security\logs\scesrv.log para obtener información detallada.

C:\Windows\System32>
```

17. Verificar la configuración de las actualizaciones automáticas: ejecuta "reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" para ver la configuración de las actualizaciones automáticas.

```
C:\Windows\System32>reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update
    AcceleratedInstallRequired REG_DWORD    0x1
    IsOOBEInProgress          REG_DWORD    0x1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\LastOnlineScanTimeForAppCategory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Power
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RequestedAppCategories

C:\Windows\System32>
```

18. Verificar la configuración de Directiva de seguridad local: ejecuta "secedit /analyze /db C:\Windows\security\local.sdb /cfg C:\security.cfg /quiet" para analizar la Directiva de seguridad local.

```
C:\Windows\System32>secedit /analyze /db C:\Windows\security\local.sdb /cfg C:\security.cfg /quiet

C:\Windows\System32>
```

19. Verificar la integridad del sistema: El comando "sfc /scannow" escanea el sistema en busca de archivos dañados y los repara automáticamente si es posible.

```
C:\Windows\System32>sfc /scannow

Iniciando examen en el sistema. Este proceso tardará algún tiempo.

Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 12%.
```

20. Verificar el estado de los discos duros: El comando "chkdsk" revisa los discos duros en busca de errores y los repara si es necesario.

```
C:\Windows\System32>
C:\Windows\System32>chkdsk
El tipo del sistema de archivos es NTFS.
La etiqueta de volumen es Windows.

ADVERTENCIA: parámetro /F no especificado.
Ejecutando CHKDSK en modo de solo lectura.
```

21. Bloquear una IP específica: El comando "netsh advfirewall firewall add rule name="Bloquear IP" dir=in action=block remoteip=X.X.X.X" bloquea una dirección IP específica.

```
C:\Windows\System32>
C:\Windows\System32>netsh advfirewall firewall add rule name="Bloqueo IP Simulada" dir=in action=block remoteip=203.0.113.77 enable=yes
Aceptar

C:\Windows\System32>
```

22. Restaurar configuración de seguridad predeterminada: El comando "netsh advfirewall reset" restablece la configuración predeterminada del firewall de Windows.

```
C:\Users\aniba>netsh advfirewall reset
Restableciendo la configuración del firewall...
Aceptar

C:\Users\aniba>
```

23. Cambiar la contraseña de un usuario: El comando "net user usuario *" permite cambiar la contraseña de un usuario.

```
C:\Windows\System32>net user aniba *
Escriba una contraseña para el usuario:
```

24. Verificar la configuración del firewall: El comando "netsh advfirewall show allprofiles" muestra la configuración del firewall.

```
C:\Windows\System32>netsh advfirewall show allprofiles

Configuración de Perfil de dominio:
-----
```

25. Eliminar virus y malware: El comando "malwarebytes /runupdate /scan" permite ejecutar un análisis en busca de virus y malware.

```
C:\Windows\System32>malwarebytes /runupdate /scan
"malwarebytes" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\System32>
```

no funciona directamente en CMD salvo que tengas **Malwarebytes instalado** y su ruta esté correctamente añadida al PATH del sistema.

26. Verificar los puertos abiertos: El comando "netstat -an" muestra los puertos abiertos en el sistema.

```
C:\Windows\System32>netstat -an

Conexiones activas

Proto  Dirección local          Dirección remota          Estado
```

27. Verificar los procesos en ejecución: El comando "tasklist" muestra los

procesos que se están ejecutando en el sistema.

```
C:\Windows\System32>tasklist

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor
=====
System Idle Process             0 Services              0           8 KB
```

28. Eliminar programas no deseados: El comando "wmic product get name" muestra una lista de los programas instalados en el sistema. Luego, se puede usar "wmic product where name="Nombre del programa" call uninstall" para desinstalar programas específicos.

```
C:\Windows\System32>wmic product get name
Name
Microsoft Teams Meeting Add-in for Microsoft Office
Python 3.12.2 Standard Library (64-bit)
Python 3.12.2 Executables (64-bit)
```

29.Desactivar el protocolo SMBv1: El comando "sc.exe config lanmanworkstation depend= bowser/mrxsmb20/lsi" desactiva el protocolo SMBv1, que es vulnerable a ataques de ransomware.

```
C:\Windows\System32>sc.exe config lanmanworkstation depend= bowser/mrxsmb20/lsi
[SC] ChangeServiceConfig CORRECTO

C:\Windows\System32>
```

30.Bloquear un puerto específico: El comando "netsh advfirewall firewall add rule name="Bloquear Puerto" dir=in action=block protocol=TCP localport=XX" bloquea un puerto específico.

```
C:\Windows\System32>netsh advfirewall firewall add rule name="Bloquear Puerto 445" dir=in action=block protocol=TCP localport=445 enable=yes
Aceptar

C:\Windows\System32>
```

31.Verificar la información de la cuenta de usuario: El comando "net user usuario" muestra la información de la cuenta de usuario, incluyendo la última vez que se cambió la contraseña.

```
C:\Windows\System32>net user aniba
Nombre de usuario
Nombre completo
Comentario
Comentario del usuario
Código de país o región
Cuenta activa
La cuenta expira

Ultimo cambio de contraseña
La contraseña expira
Cambio de contraseña
Contraseña requerida
El usuario puede cambiar la contraseña

Estaciones de trabajo autorizadas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada

Horas de inicio de sesión autorizadas

Miembros del grupo local
```

32. Mostrar información de red: El comando "ipconfig /all" muestra la información de la red, incluyendo la dirección IP, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS.


```

C:\Windows\System32>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . .
Sufijo DNS principal . . . . .
Tipo de nodo. . . . .
Enrutamiento IP habilitado. . .
Proxy WINS habilitado . . . . .

Adaptador desconocido Conexión de a

Estado de los medios. . . . .
Sufijo DNS específico para la co
Descripción . . . . .
Dirección física. . . . .
DHCP habilitado . . . . .
Configuración automática habilit

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la co
Descripción . . . . .
Dirección física. . . . .
DHCP habilitado . . . . .
Configuración automática habilit
Vínculo: dirección IPv6 local. .
Dirección IPv4. . . . .
Método de autenti

```

33. Restaurar la configuración de fábrica del firewall: El comando "netsh advfirewall reset to defaults" restaura la configuración de fábrica del firewall de Windows.

```

C:\Users\aniba>netsh advfirewall reset
Restableciendo la configuración del firewall...
Aceptar

C:\Users\aniba>

```

34. Habilitar la autenticación de dos factores: El comando "netsh advfirewall set allprofiles settings WindowsAuthentication set AuthPersistNonNTLM n" habilita la autenticación de dos factores.

Este comando está **mal formado y no existe** en esa estructura. De hecho, netsh advfirewall no tiene una opción directa para configurar autenticación multifactor.

La **autenticación de dos factores (2FA)** en Windows se gestiona a través de:

- **Políticas de grupo (GPO)**
- **Azure AD / Microsoft 365**
- **Autenticadores de terceros** (como Duo, Authy)

35. Escanear el sistema en busca de malware: El comando "sfc /scanfile=nombre_archivo" escanea un archivo específico en busca de malware.

```
C:\Windows\System32>sfc /scanfile=C:\Windows\System32\kernel32.dll

Protección de recursos de Windows no encontró ninguna infracción
de integridad.

C:\Windows\System32>
```

36. Limpiar el registro del sistema: El comando "regedit" permite acceder al registro del sistema para limpiar claves innecesarias o sospechosas.

