

Guerra Jennifer

Get-CimInstance -ClassName Win32\_Desktop

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\jenni> Get-CimInstance -ClassName Win32_Desktop

SettingID Name ScreenSaverActive ScreenSaverSecure ScreenSaverTimeout
-----
NT AUTHORITY\SYSTEM False
MICHA\jenni False
.DEFAULT False
```

Get-CimInstance -ClassName Win32\_BIOS

```
PS C:\Users\jenni> Get-CimInstance -ClassName Win32_BIOS

SMBIOSBIOSVersion : FX507ZC4.310
Manufacturer      : American Megatrends International, LLC.
Name              : FX507ZC4.310
SerialNumber      : RANRCX05R54844E
Version           : _ASUS_ - 1072009
```

Get-CimInstance -ClassName Win32\_Processor

```
PS C:\Users\jenni> Get-CimInstance -ClassName Win32_Processor

DeviceID Name Caption MaxClockSpeed SocketDesignation Manufacturer
-----
CPU0 12th Gen Intel(R) Core(TM) i7-12700H Intel64 Family 6 Model 154 Stepping 3 2300 U3E1 Gen
```

GET-PROCESS.- Actividades que esta realizando la computadora

```
PS C:\Users\jenni> GET-PROCESS
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
186	11	1872	9692	0.00	1188	2	ACCIMonitor
147	10	2144	8944		6888	0	AggregatorHost
300	18	23152	37760	0.03	3980	2	ai
477	23	14536	38132	0.13	11032	2	ApplicationFrameHost
221	12	2912	10108		4908	0	ArmouryCrateControlInterface
394	30	132632	45928	0.02	4404	2	ArmouryCrateKeyControl
462	20	4580	20420		4936	0	AsusAppService
207	11	2168	7488		4140	0	AsusOptimization
126	10	1460	6640	0.02	10392	2	AsusOptimizationStartupTask
504	18	9356	19612		4988	0	AsusSoftwareManager
602	35	40804	44724	0.17	12628	2	AsusSoftwareManagerAgent
182	10	1796	6560		4996	0	AsusSwitch
263	14	4164	13456		5008	0	AsusSystemAnalysis
139	8	2416	8576	0.00	8952	2	AsusSystemAnalysis
191	11	2372	8772		4976	0	AsusSystemDiagnosis
738	25	70496	84452	1.13	14272	0	audiodg

GET-PROCESS -ID del proceso específico

```
PS C:\Users\jenni> GET-PROCESS -ID 1544
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
450	26	7312	13980		1544	0	WUDFHost

GET-SERVICE

```
PS C:\Users\jenni> GET-SERVICE
```

Status	Name	DisplayName
Stopped	AarSvc_1a9f8c	Agent Activation Runtime_1a9f8c
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
Stopped	AppReadiness	Preparación de aplicaciones
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Running	ArmouryCrateCon...	Armoury Crate Control Interface
Stopped	ArmouryCrateDow...	Armoury Crate Download Tool
Running	AsusAppService	ASUS App Service
Running	ASUSOptimization	ASUS Optimization
Running	ASUSSoftwareMan...	ASUS Software Manager
Running	ASUSSwitch	ASUS Switch
Running	ASUSSystemAnalysis	ASUS System Analysis
Running	ASUSSystemDiagn...	ASUS System Diagnosis
Running	AudioEndpointBu...	Compilador de extremo de audio de W...
Running	Audiosrv	Audio de Windows
Stopped	autotimesvc	Hora de la red de telefonía móvil
Stopped	AxInstSV	Instalador de ActiveX (AxInstSV)
Stopped	BcastDVRUserSer...	Servicio de usuario de difusión y G...
Stopped	BDESVC	Servicio Cifrado de unidad BitLocker

Activar servicio de windows update:

```
PS C:\Users\jenni> Start-Service -Name wuauserv
PS C:\Users\jenni> |
```

```

instalar la version mas reciente de powershell para obtener

PS C:\WINDOWS\system32> Stop-Service -Name wuauserv
PS C:\WINDOWS\system32>

```

Obtener info del Sistema operative

```

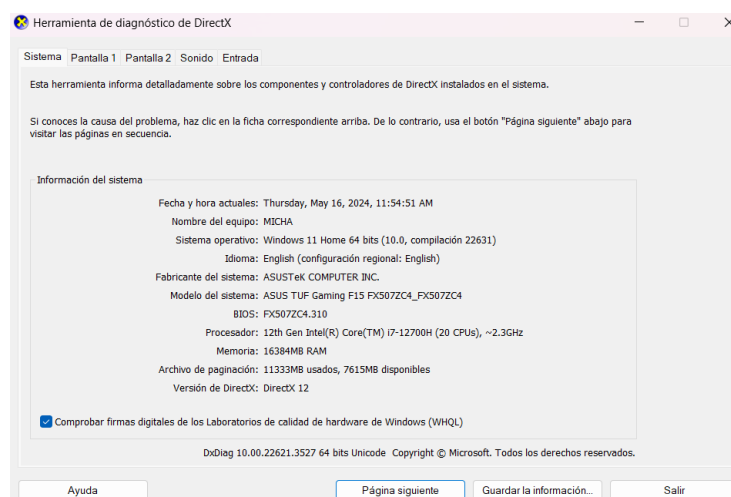
PS C:\Users\jenni> get-WmiObject -Class Win32_OperatingSystem

SystemDirectory : C:\WINDOWS\system32
Organization    :
BuildNumber     : 22631
RegisteredUser  : jenniguerra132@hotmail.com
SerialNumber    : 00325-96641-40107-AAOEM
Version         : 10.0.22631

PS C:\Users\jenni> |

```

Dxdiag: Información del dispositivo



Test de conexion a esa ip

Source	Destination	IPv4Address	IPv6Address	Bytes	Time(ms)
MICHA	8.8.8.8	8.8.4.4		32	82
MICHA	8.8.8.8	8.8.4.4		32	111
MICHA	8.8.8.8	8.8.4.4		32	89
MICHA	8.8.8.8	8.8.4.4		32	81

```
PS C:\Users\jenni> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 Local. . . : fe80::b890:dff3:b344:7a81%4
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :
```

Account	Enabled	Description
Administrador	False	Cuenta integrada para la administración del equipo o dominio
Guest	False	Cuenta de usuario administrada por el sistema.
Invitado	False	Cuenta integrada para el acceso como invitado al equipo o dominio
Local Administrator	True	
System	False	Cuenta de usuario administrada por el sistema.
SystemUtilityAccount	False	Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de ap...

```
PS C:\Windows\system32> New-LocalUser -Name "usuario_prueba"

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

Name           Enabled Description
-----
usuario_prueba True

PS C:\Windows\system32> -Fullname "Usuario de prueba"
Fullname : El término '-Fullname' no se reconoce como nombre de un cmdlet, función, archivo de script o programa
ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta
es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ ~Fullname "Usuario de prueba"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Fullname:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> 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
jenni          True
usuario_prueba  True
NDAGUtilityAccount False  Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de ap...
```

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

Id CommandLine
--
1 New-LocalUser -Name "usuario_prueba"
2 -Fullname "Usuario de prueba"
3 Get-LocalUser
4 Remove-LocalUser -Name "usuario_prueba"
```

```
PS C:\Users\jenni> Get-History

Id CommandLine
--
1 Get-CimInstance -ClassName Win32_Desktop
2 Get-CimInstance -ClassName Win32_BIOS
3 Get-CimInstance -ClassName Win32_Processor
4 GET-PROCESS
5 GET-PROCESS -ID 4572
6 GET-PROCESS -ID1544
7 GET-PROCESS -ID 1544
8 GET-SERVICE
9 Start-Service -Name wuauserv
10 Stop-Service -Name wuauserv
11 get-WmiObject
12 get-WmiObject - Class Win32_OperatingSystem
13 get-WmiObject -Class Win32_OperatingSystem
14 Test-Connection 8.8.8.8
15 ipconfig
16 Get-LocalUser
```

```
CommandLine
-----
Get-CimInstance -ClassName Win32_Desktop
Get-CimInstance -ClassName Win32_BIOS
Get-CimInstance -ClassName Win32_Processor
GET-PROCESS
GET-PROCESS -ID 4572
GET-PROCESS -ID1544
GET-PROCESS -ID 1544
GET-SERVICE
Start-Service -Name wuauserv
Stop-Service -Name wuauserv
get-WmiObject
get-WmiObject - Class Win32_OperatingSystem
get-WmiObject -Class Win32_OperatingSystem
Test-Connection 8.8.8.8
ipconfig
Get-LocalUser
Get-History
Test-Connection -ComputerName "google.com"
Test-Connection -ComputerName "youtube.com"
cd a
cd Escritorio
cd ESPE
cd C:\Users\jenni\OneDrive\Desktop\ESPE
TestGoogle
.\TestGoogle.ps1
ESPE...
cd..
```

## Eliminar Usuario

```
PS C:\Windows\system32> Remove-LocalUser -Name "usuario_prueba"
PS C:\Windows\system32> 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
jenni           True   Cuenta de usuario administrada por el sistema.
WDAGUtilityAccount False  Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de ap.
```

Para ver una página:

```
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri "http://www.google.com"

statusCode      : 200
statusDescription : OK
content         : <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="es-419"><html>
content         : content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta
content         : content="/images/branding/googlelogo/1x...
rawContent      : HTTP/1.1 200 OK
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src
'nonce-MtjED2BE10302R3V2y4G9A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-s
https: ...
forms           : {}
headers         : [{"Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src
'nonce-MtjED2BE10302R3V2y4G9A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-s
https://report-uri https://csp.withgoogle.com/csp/gws/other-hp), [X-XSS-Protection
[X-Frame-Options, SAMEORIGIN], [Cache-Control, private, max-age=0]...}]
images          : [{"@innerHTML=; innerText=; outerHTML= Test-Connection -ComputerName "youtube.com"

Source      Destination      IPV4Address      IPV6Address      Bytes      Time(ms)
-----
MICAHA      youtube.com      172.217.15.206   172.217.15.206   32         81
MICAHA      youtube.com      172.217.15.206   172.217.15.206   32         79
MICAHA      youtube.com      172.217.15.206   172.217.15.206   32         82
MICAHA      youtube.com      172.217.15.206   172.217.15.206   32         80
```

Ingresa a una carpeta, para ejecutar un archivo con extensión .ps1

```
Suggestion [3,General]: No se encontró el comando TestGoogle, pero existe en la ubicación actual. Windows PowerShell no
carga comandos de la ubicación actual de forma predeterminada. Si confía en este comando, escriba ".\TestGoogle". Vea "g
et-help about_Command_Precedence" para obtener información más detallada.
PS C:\Users\jenni\OneDrive\Desktop\ESPE> .\TestGoogle.ps1
PS C:\Users\jenni\OneDrive\Desktop\ESPE> ESPE...
```

