

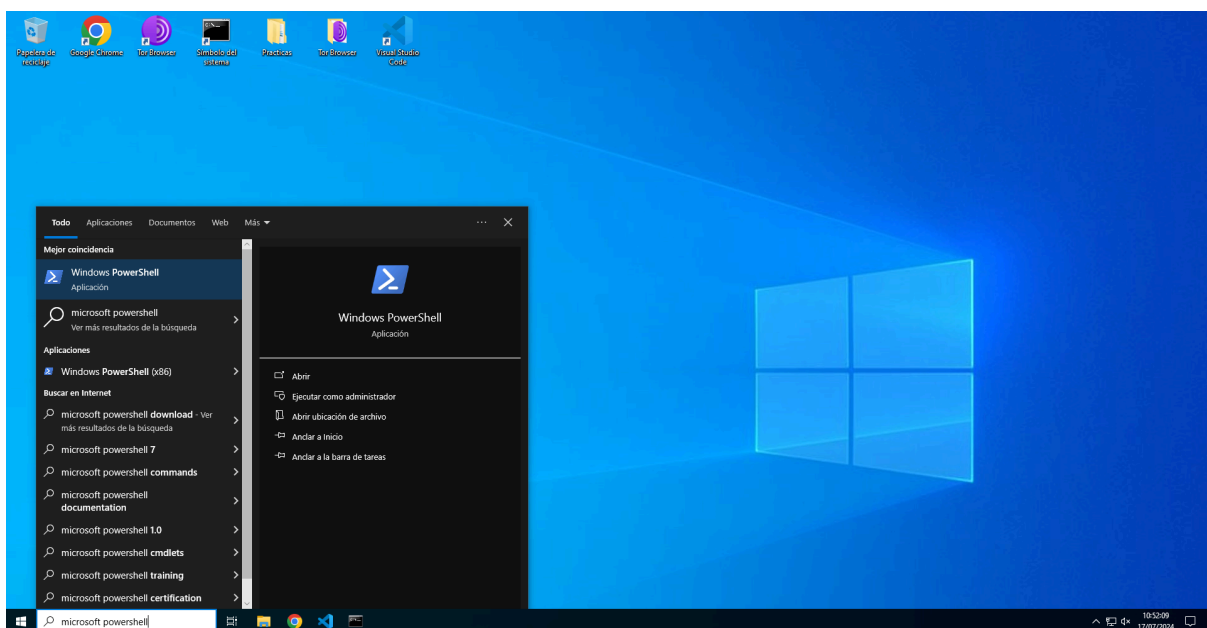
# **Actividad 04. Uso de Powershell**

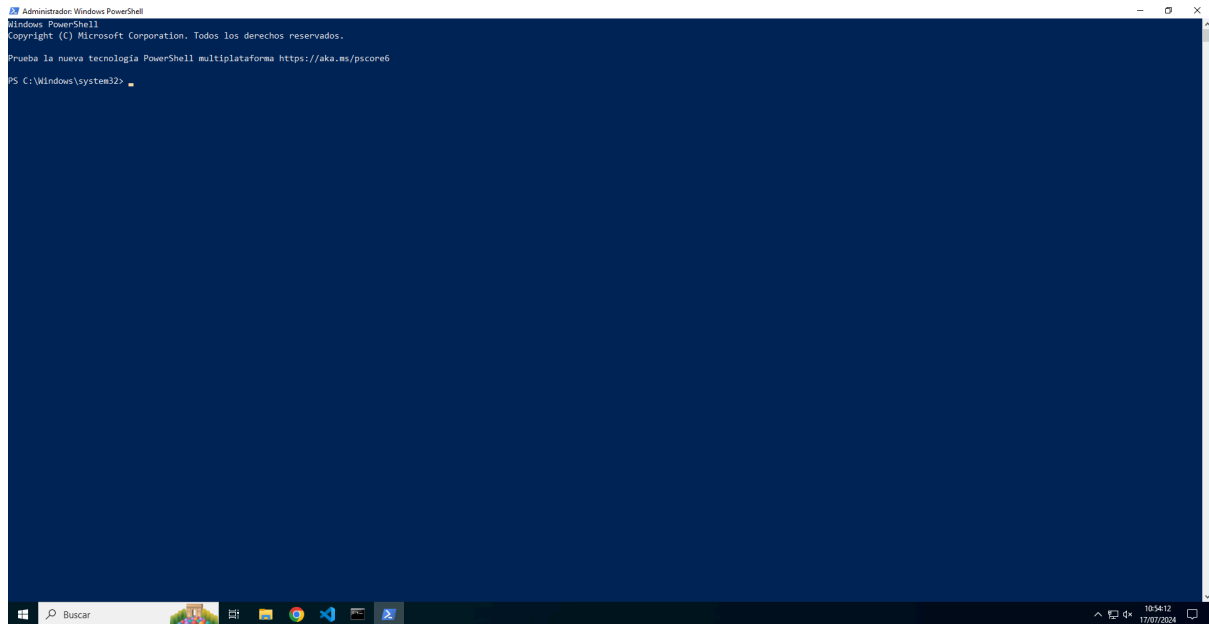
[1. Elaborar un documento mostrando el uso de los cmdlets de Powershell para gestionar usuarios y grupos](#)

[2. Prueba otros cmdlets](#)

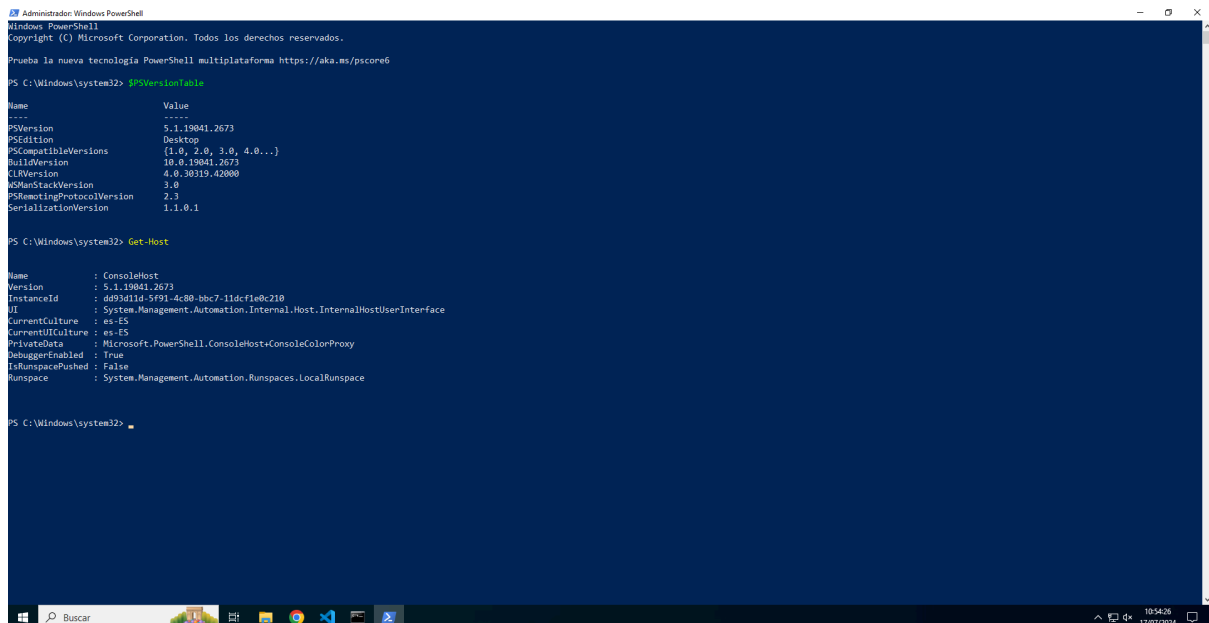
## **1. Elaborar un documento mostrando el uso de los cmdlets de Powershell para gestionar usuarios y grupos**

- En primer lugar, buscamos Powershell y lo iniciamos como Administrador para ejecutar la mayoría de cosas que queremos hacer:

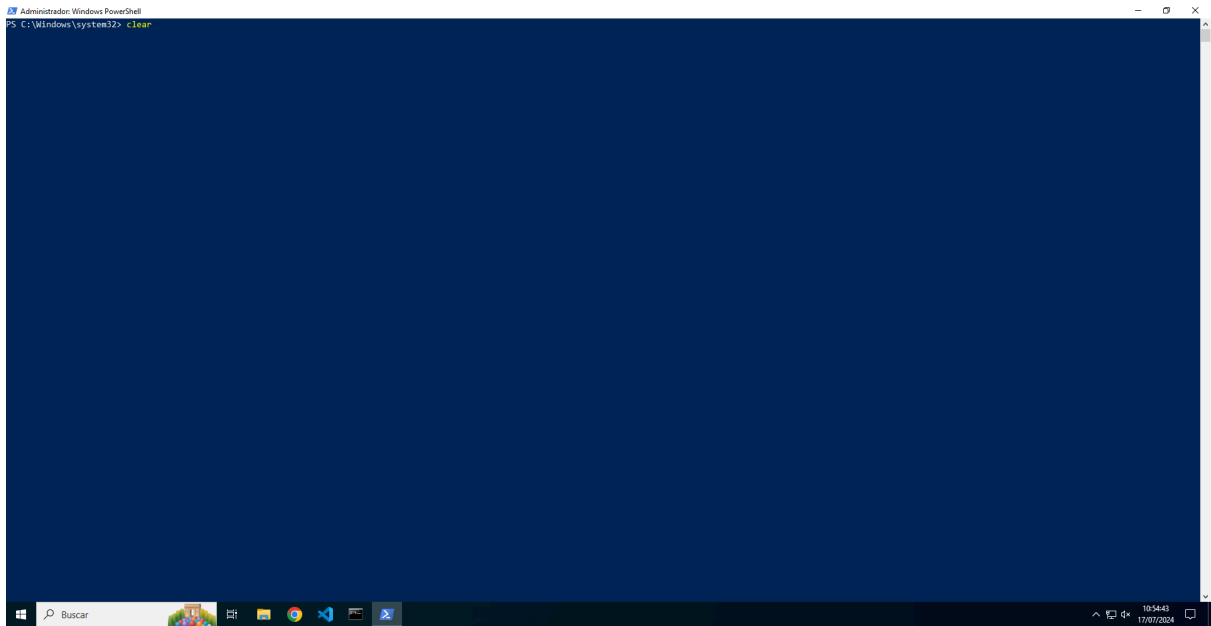




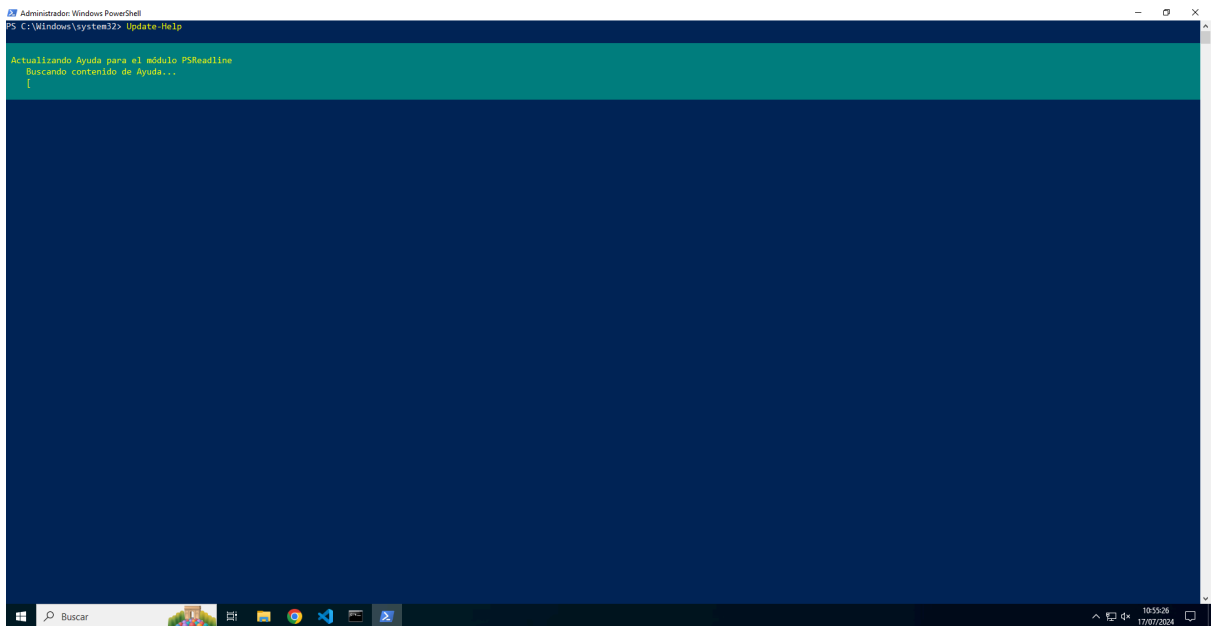
- Vemos la versión de Powershell con los comandos “*\$PSVersionTable*” o “*Get-Host*”:



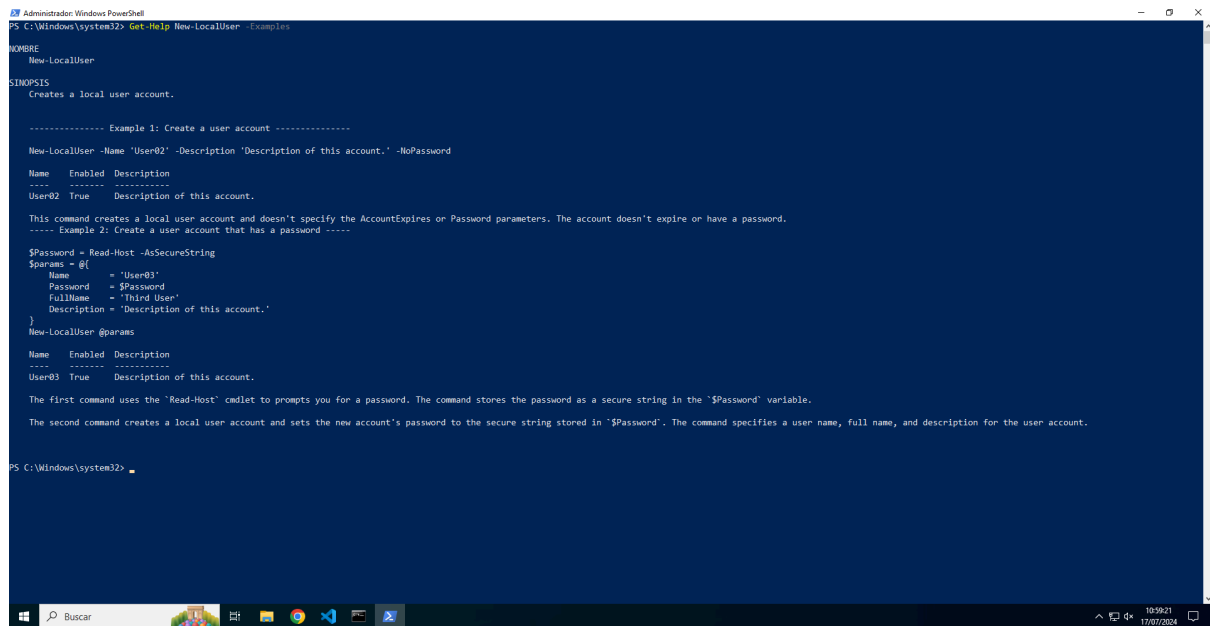
- Si queremos limpiar la terminal, ponemos el comando “*clear*”:



- Si queremos actualizar ayuda, utilizamos *"Update-Help"*:



- Un ejemplo de ayuda, con el comando *"Get-Help New-LocalUser -Examples"*:



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Help New-LocalUser -Examples

NAME
New-LocalUser

SYNOPSIS
Creates a local user account.

----- Example 1: Create a user account -----

New-LocalUser -Name 'User02' -Description 'Description of this account.' -NoPassword

Name      Enabled Description
-----
User02    True   Description of this account.

This command creates a local user account and doesn't specify the AccountExpires or Password parameters. The account doesn't expire or have a password.
----- Example 2: Create a user account that has a password -----

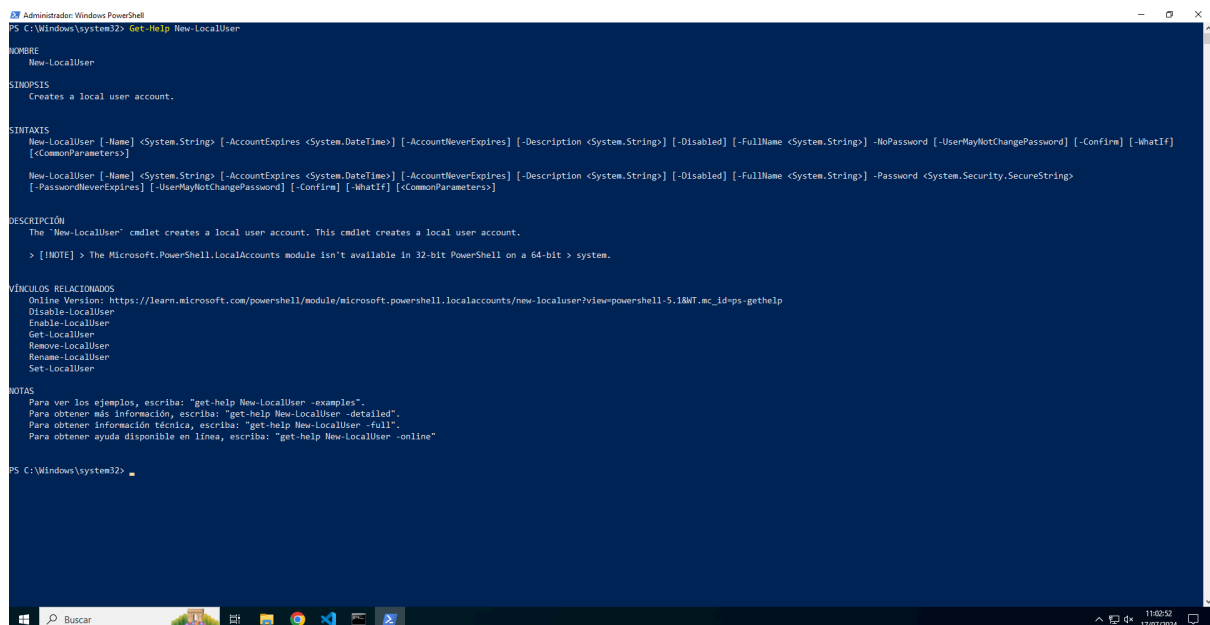
$Password = Read-Host -AsSecureString
$params = @{
    Name      = 'User03'
    Password  = $Password
    FullName  = 'Third User'
    Description = 'Description of this account.'
}
New-LocalUser @params

Name      Enabled Description
-----
User03    True   Description of this account.

The first command uses the 'Read-Host' cmdlet to prompt you for a password. The command stores the password as a secure string in the '$Password' variable.
The second command creates a local user account and sets the new account's password to the secure string stored in '$Password'. The command specifies a user name, full name, and description for the user account.

PS C:\Windows\system32>
```

- Ejemplo de ayuda del usuario con el comando “*Get-Help New-LocalUser*”:



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Help New-LocalUser

NAME
New-LocalUser

SYNOPSIS
Creates a local user account.

SYNTAX
New-LocalUser [-Name <System.String>] [-AccountExpires <System.DateTime>] [-AccountNeverExpires] [-Description <System.String>] [-Disabled] [-FullName <System.String>] [-NoPassword] [-UserMayNotChangePassword] [-Confirm] [-WhatIf]
[<<CommonParameters>]

New-LocalUser [-Name <System.String>] [-AccountExpires <System.DateTime>] [-AccountNeverExpires] [-Description <System.String>] [-Disabled] [-FullName <System.String>] -Password <System.Security.SecureString>
[-PasswordNeverExpires] [-UserMayNotChangePassword] [-Confirm] [-WhatIf] [<<CommonParameters>]

DESCRIPTION
The 'New-LocalUser' cmdlet creates a local user account. This cmdlet creates a local user account.

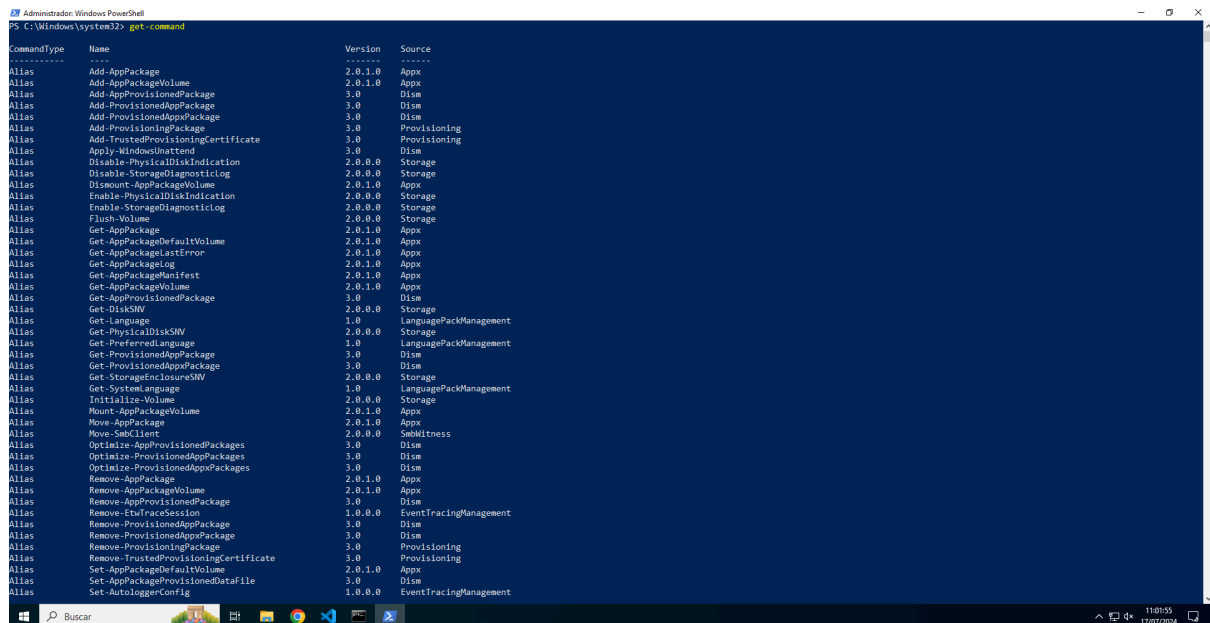
> [NOTE] > The Microsoft.PowerShell.LocalAccounts module isn't available in 32-bit PowerShell on a 64-bit system.

VÍNCULOS RELACIONADOS
Online Version: https://learn.microsoft.com/powershell/module/microsoft.powershell.localaccounts/new-localuser?view=powershell-5.1&wt.mc_id=ps-gethelp
Disable-LocalUser
Enable-LocalUser
Get-LocalUser
Remove-LocalUser
Rename-LocalUser
Set-LocalUser

NOTAS
Para ver los ejemplos, escriba: "get-help New-LocalUser -examples".
Para obtener más información, escriba: "get-help New-LocalUser -detailed".
Para obtener información técnica, escriba: "get-help New-LocalUser -full".
Para obtener ayuda disponible en línea, escriba: "get-help New-LocalUser -online"

PS C:\Windows\system32>
```

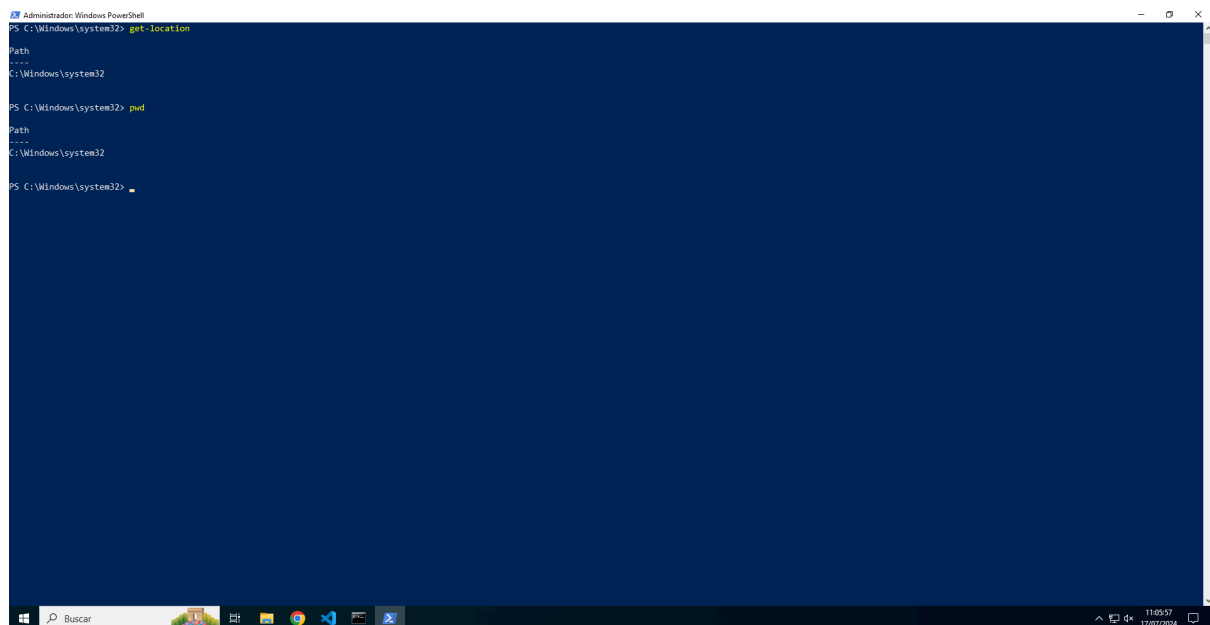
- Comandos de ayuda “*get-command*”:



```
PS C:\Windows\system32> get-command

CommandType      Name                                Version      Source
-----
Alias             Add-AppPackage                    2.0.1.0      Appx
Alias             Add-AppPackageVolume              2.0.1.0      Appx
Alias             Add-AppProvisionedPackage         3.0          DisM
Alias             Add-ProvisionedAppPackage         3.0          DisM
Alias             Add-ProvisionedAppxPackage        3.0          DisM
Alias             Add-ProvisioningPackage           3.0          Provisioning
Alias             Add-TrustedProvisioningCertificate 3.0          Provisioning
Alias             Apply-WindowsUnattend             3.0          DisM
Alias             Disable-PhysicalDiskIndication    2.0.0.0      Storage
Alias             Disable-StorageDiagnosticLog      2.0.0.0      Storage
Alias             Dismount-AppPackageVolume         2.0.1.0      Appx
Alias             Enable-PhysicalDiskIndication     2.0.0.0      Storage
Alias             Enable-StorageDiagnosticLog       2.0.0.0      Storage
Alias             Flush-Volume                      2.0.0.0      Storage
Alias             Get-AppPackage                    2.0.1.0      Appx
Alias             Get-AppPackageDefaultVolume       2.0.1.0      Appx
Alias             Get-AppPackageLastError           2.0.1.0      Appx
Alias             Get-AppPackageLog                 2.0.1.0      Appx
Alias             Get-AppPackageManifest            2.0.1.0      Appx
Alias             Get-AppPackageVolume              2.0.1.0      Appx
Alias             Get-AppProvisionedPackage         3.0          DisM
Alias             Get-DiskSW                        2.0.0.0      Storage
Alias             Get-Language                      1.0          LanguagePackManagement
Alias             Get-PhysicalDiskSW               2.0.0.0      Storage
Alias             Get-PreferredLanguage             1.0          LanguagePackManagement
Alias             Get-ProvisionedAppPackage         3.0          DisM
Alias             Get-ProvisionedAppxPackage        3.0          DisM
Alias             Get-StorageEnclosureSW           2.0.0.0      Storage
Alias             Get-SystemLanguage               1.0          LanguagePackManagement
Alias             Initialize-Volume                2.0.0.0      Storage
Alias             Mount-AppPackageVolume            2.0.1.0      Appx
Alias             Move-AppPackage                  2.0.1.0      Appx
Alias             Move-Sentinel                    2.0.0.0      Sentinel
Alias             Optimize-AppProvisionedPackages   3.0          DisM
Alias             Optimize-ProvisionedAppPackages   3.0          DisM
Alias             Optimize-ProvisionedAppxPackages 3.0          DisM
Alias             Remove-AppPackage                 2.0.1.0      Appx
Alias             Remove-AppPackageVolume           2.0.1.0      Appx
Alias             Remove-AppProvisionedPackage      3.0          DisM
Alias             Remove-EtdTraceSession            1.0.0.0      EventTracingManagement
Alias             Remove-ProvisionedAppPackage      3.0          DisM
Alias             Remove-ProvisionedAppxPackage     3.0          DisM
Alias             Remove-ProvisioningPackage        3.0          Provisioning
Alias             Remove-TrustedProvisioningCertificate 3.0          Provisioning
Alias             Set-AppPackageDefaultVolume       2.0.1.0      Appx
Alias             Set-AppPackageProvisionedDataFile 3.0          DisM
Alias             Set-AutologgerConfig              1.0.0.0      EventTracingManagement
```

- Saber en qué directorio estás con “*get-location*” y “*pwd*”:



```
PS C:\Windows\system32> get-location

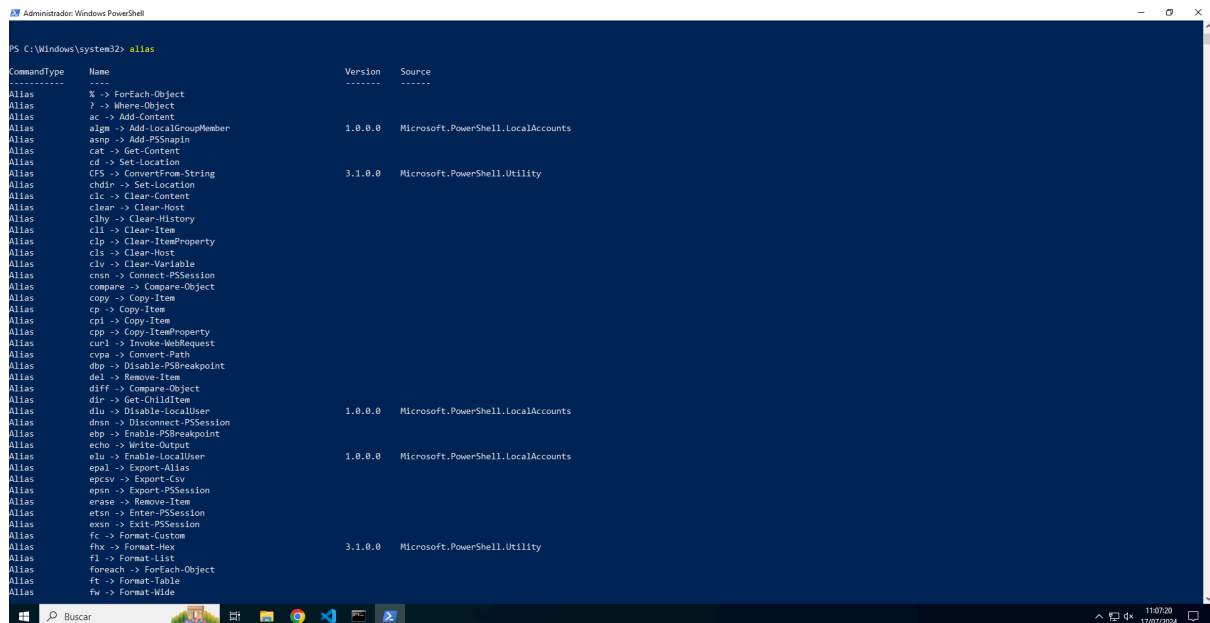
Path
---
C:\Windows\system32

PS C:\Windows\system32> pwd

Path
---
C:\Windows\system32

PS C:\Windows\system32>
```

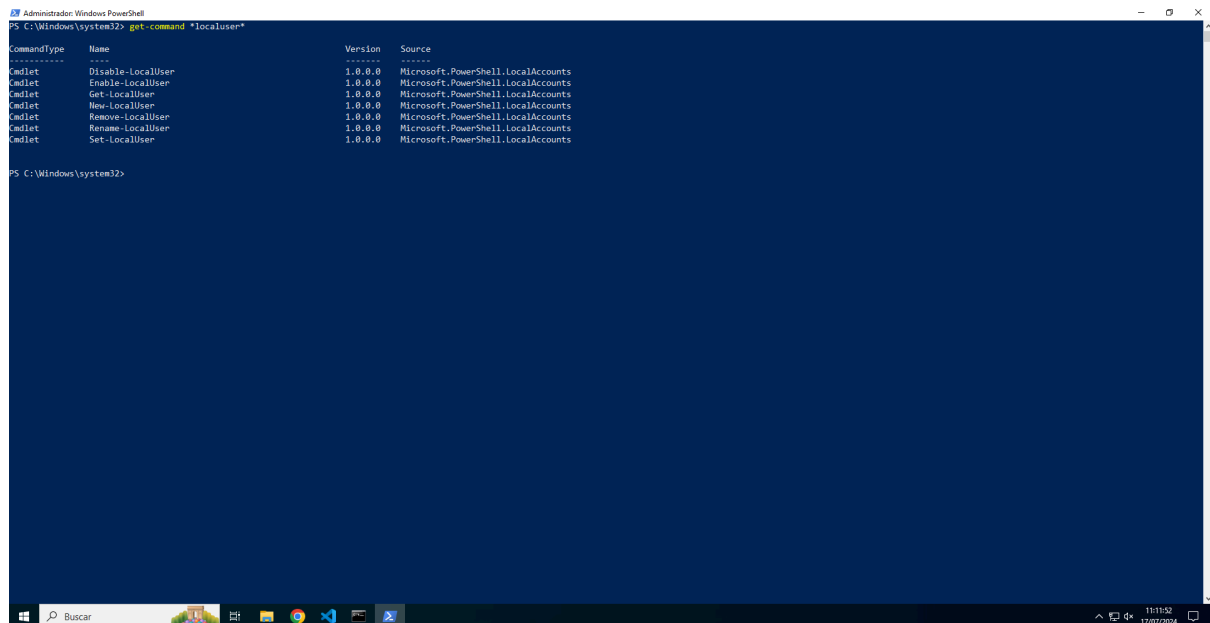
- Alias de los comandos de Windows y Linux “*alias*”:



```
PS C:\Windows\system32> alias

CommandType      Name                                Version      Source
-----
Alias             % -> ForEach-Object
Alias             ? -> Where-Object
Alias             ac -> Add-Content
Alias             algm -> Add-LocalGroupMember
Alias             asnp -> Add-PSnapin
Alias             cat -> Get-Content
Alias             cd -> Set-Location
Alias             CFS -> ConvertFrom-String
Alias             chdir -> Set-Location
Alias             clc -> Clear-Content
Alias             clear -> Clear-Host
Alias             clhy -> Clear-History
Alias             cli -> Clear-Item
Alias             clio -> Clear-ItemProperty
Alias             cls -> Clear-Host
Alias             clv -> Clear-Variable
Alias             cnan -> Connect-PSession
Alias             compare -> Compare-Object
Alias             copy -> Copy-Item
Alias             cp -> Copy-Item
Alias             cpi -> Copy-Item
Alias             cpp -> Copy-ItemProperty
Alias             curl -> Invoke-WebRequest
Alias             cpa -> Convert-Path
Alias             dbp -> Disable-PSBreakpoint
Alias             del -> Remove-Item
Alias             diff -> Compare-Object
Alias             dir -> Get-Childitem
Alias             diu -> Disable-LocalUser
Alias             dnan -> Disconnect-PSession
Alias             ebp -> Enable-PSBreakpoint
Alias             echo -> Write-Output
Alias             elu -> Enable-LocalUser
Alias             epal -> Export-Alias
Alias             epsv -> Export-Csv
Alias             epsn -> Export-PSession
Alias             erase -> Remove-Item
Alias             eten -> Enter-PSession
Alias             exsn -> Exit-PSession
Alias             fc -> Format-Custom
Alias             fhx -> Format-Hex
Alias             fl -> Format-List
Alias             foreach -> ForEach-Object
Alias             ft -> Format-Table
Alias             fw -> Format-Wide
```

- Usuarios locales con el comando “*get-command localuser*”:

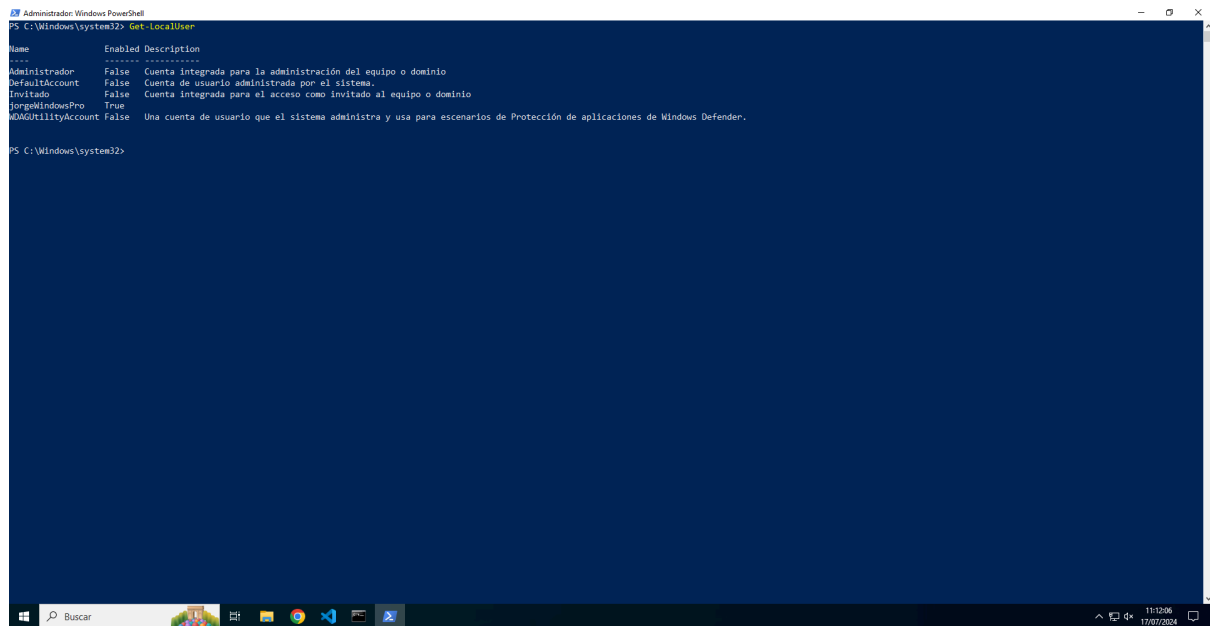


```
PS C:\Windows\system32> get-command localuser

CommandType      Name                                Version      Source
-----
Cmdlet            Disable-LocalUser                  1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            Enable-LocalUser                   1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            Get-LocalUser                      1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            New-LocalUser                     1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            Remove-LocalUser                   1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            Rename-LocalUser                   1.0.0.0      Microsoft.PowerShell.LocalAccounts
Cmdlet            Set-LocalUser                      1.0.0.0      Microsoft.PowerShell.LocalAccounts

PS C:\Windows\system32>
```

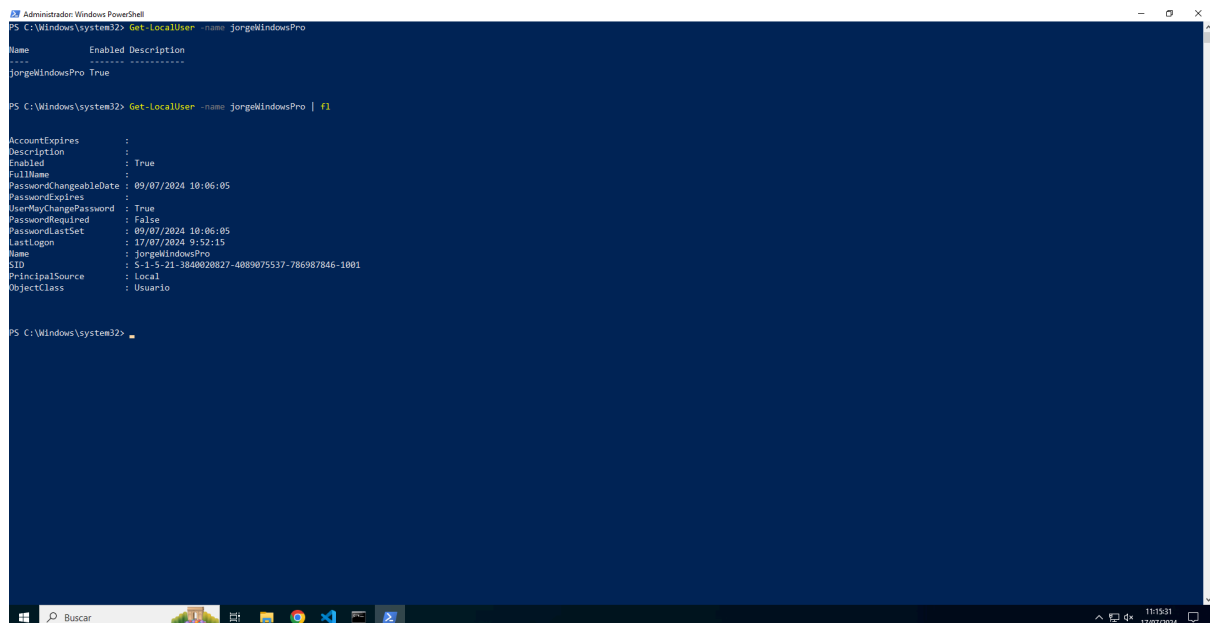
- Obtener información de los usuarios con “*Get-LocalUser*”:



```
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
jorgeWindowsPro True   Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.
WAGUtilityAccount False
```

- Para obtener la información de un usuario, con el comando *“Get-LocalUser -name nombre”* o *“Get-LocalUser -name nombre | FL”*:



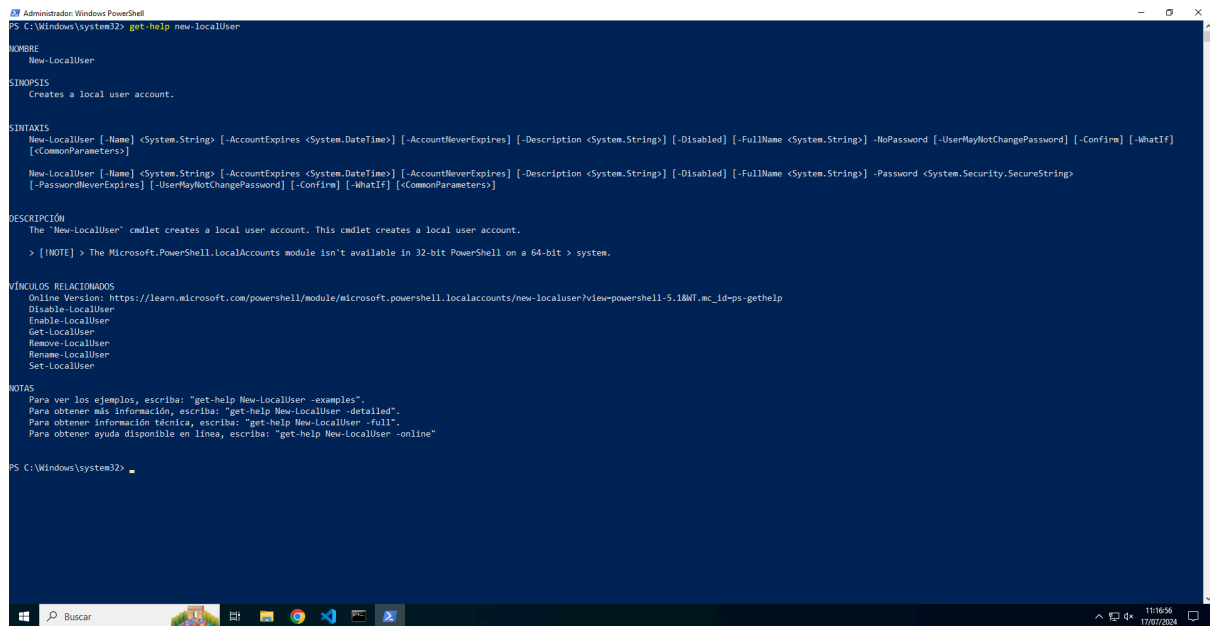
```
PS C:\Windows\system32> Get-LocalUser -name jorgeWindowsPro

Name           Enabled Description
-----
jorgeWindowsPro True

PS C:\Windows\system32> Get-LocalUser -name jorgeWindowsPro | FL

AccountExpires      :
Description          :
Enabled             : True
FullName            :
PasswordChangeableDate : 09/07/2024 10:06:05
PasswordExpires     :
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     : 09/07/2024 10:06:05
LastLogon           : 17/07/2024 9:52:15
Name                : jorgeWindowsPro
SID                 : S-1-5-21-3840020827-4089075537-786987846-1001
PrincipalSource      : local
ObjectClass          : Userio
```

- Ayuda para crear un nuevo usuario *“Get-Help New-LocalUser”*:



```
PS C:\Windows\system32> get-help new-localuser

NOMBRE
New-LocalUser

SINOPSIS
Creates a local user account.

SINTAXIS
New-LocalUser [-Name] <System.String> [-AccountExpires <System.DateTime>] [-AccountNeverExpires] [-Description <System.String>] [-Disabled] [-FullName <System.String>] [-NoPassword] [-UserMayNotChangePassword] [-Confirm] [-WhatIf]
[<CommonParameters>]

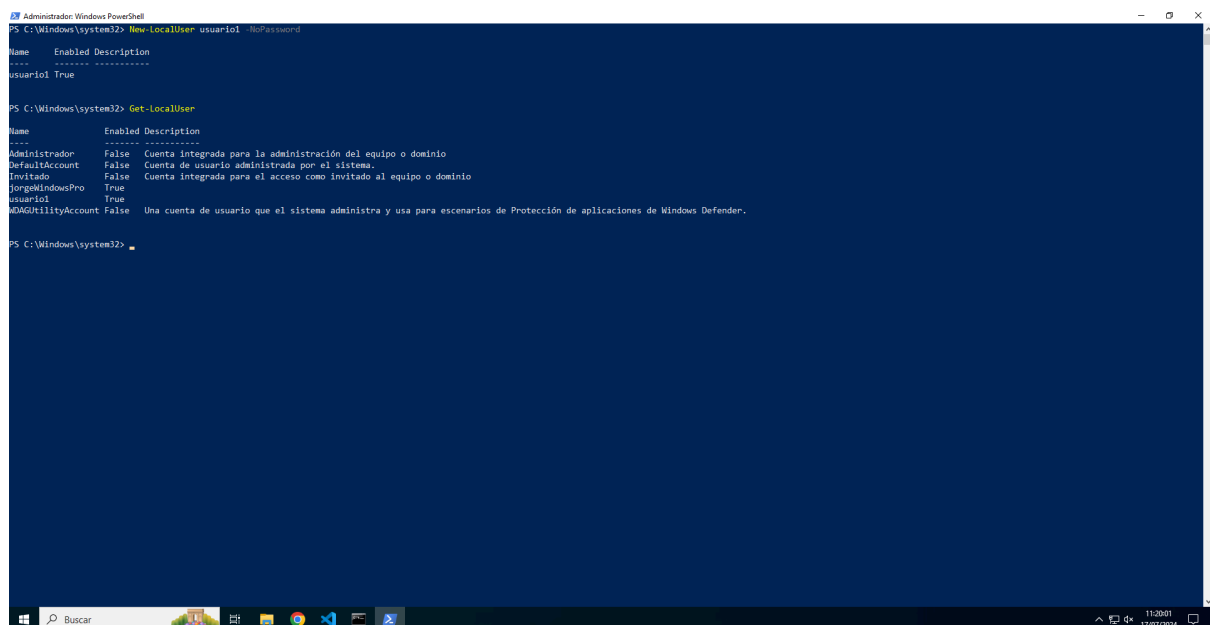
New-LocalUser [-Name] <System.String> [-AccountExpires <System.DateTime>] [-AccountNeverExpires] [-Description <System.String>] [-Disabled] [-FullName <System.String>] [-Password <System.Security.SecureString>]
[-PasswordNeverExpires] [-UserMayNotChangePassword] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPCIÓN
The 'New-LocalUser' cmdlet creates a local user account. This cmdlet creates a local user account.
> [NOTE] > The Microsoft.PowerShell.LocalAccounts module isn't available in 32-bit PowerShell on a 64-bit > system.

VÍNCULOS RELACIONADOS
Online Version: https://learn.microsoft.com/powershell/module/microsoft.powershell.localaccounts/new-localuser?view=powershell-5.1&WT.mc_id=ps-gethelp
Disable-LocalUser
Enable-LocalUser
Get-LocalUser
Remove-LocalUser
Rename-LocalUser
Set-LocalUser

NOTAS
Para ver los ejemplos, escriba: "get-help New-LocalUser -examples".
Para obtener más información, escriba: "get-help New-LocalUser -detailed".
Para obtener información técnica, escriba: "get-help New-LocalUser -full".
Para obtener ayuda disponible en línea, escriba: "get-help New-LocalUser -online"
```

- Creamos un usuario nuevo llamado **usuario1** con el comando “*New-LocalUser usuario1 -NoPassword*”:



```
PS C:\Windows\system32> New-LocalUser usuario1 -NoPassword

Name      Enabled Description
----      -
usuario1  True

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
jorgeWindowsPro True   Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.
usuario1   True
WGAUtilityAccount False  Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.
```

- Y si creamos una variable **contrasenia**, creamos un nuevo usuario llamado **usuario2** y la variable **contrasenia** se la añadimos al usuario [*\$contrasenia = ConvertTo-SecureString "clave001" -AsPlainText -Force*] [*New-LocalUser usuario2 -Password \$contrasenia*]:



```
PS C:\Windows\system32> New-LocalUser usuario1 -NoPassword

Name      Enabled Description
----      -
usuario1  True

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
jorgeWindowsPro True
usuario1 True
usuario2 False
WDAGUtilityAccount False Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

PS C:\Windows\system32> $contrasenia = ConvertTo-SecureString '12345678' -AsPlainText -Force
PS C:\Windows\system32> New-LocalUser usuario2 -Password $contrasenia

Name      Enabled Description
----      -
usuario2  True

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
jorgeWindowsPro True
usuario1 True
usuario2 True
WDAGUtilityAccount False Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

PS C:\Windows\system32>
```

- Enseñamos a los usuarios:

```
Invitado False Cuenta integrada para el acceso como invitado al equipo o dominio
jorgeWindowsPro True
usuario1 True
usuario2 True
WDAGUtilityAccount False Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

PS C:\Windows\system32> Get-LocalUser -name usuario1 | fl

AccountExpires      :
Description         :
Enabled             : True
FullName            :
PasswordChangeableDate :
PasswordExpires     :
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     :
LastLogon           :
Name                : usuario1
SID                 : S-1-5-21-3840020827-4089075537-786987846-1002
PrincipalSource     : Local
ObjectClass         : Usuario

PS C:\Windows\system32> Get-LocalUser -name usuario2 | fl

AccountExpires      :
Description         :
Enabled             : True
FullName            :
PasswordChangeableDate : 17/07/2024 11:22:06
PasswordExpires     : 28/08/2024 11:22:06
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     : 17/07/2024 11:22:06
LastLogon           :
Name                : usuario2
SID                 : S-1-5-21-3840020827-4089075537-786987846-1003
PrincipalSource     : Local
ObjectClass         : Usuario

PS C:\Windows\system32>
```

- Establecer una prioridad, añadimos Fullname y la contraseña nunca expira [Set-LocalUser usuario2 -FullName "Ana Perez Garcia"] [Set-LocalUser usuario2 -PasswordNeverExpires \$true] [Get-LocalUser usuario2 | FL \*]:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-LocalUser usuario2 -FullName "Ana Perez Garcia"
PS C:\Windows\system32> Set-LocalUser usuario2 -PasswordNeverExpires $true
PS C:\Windows\system32> Get-LocalUser -name usuario2 | fl

AccountExpires      :
Description         :
Enabled             : True
FullName            : Ana Perez Garcia
PasswordChangeableDate : 17/07/2024 11:22:06
PasswordExpires     :
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     : 17/07/2024 11:22:06
LastLogon           :
Name                : usuario2
SID                 : S-1-5-21-3840020827-4889075537-786987846-1003
PrincipalSource     : Local
ObjectClass         : Usuario

PS C:\Windows\system32>
```

- Modificamos al **usuario1** añadiéndole la prioridad y contraseña  
[Set-LocalUser -Name usuario1 -Password (ConvertTo-SecureString "clave02" -AsPlainText -Force)] [Get-LocalUser usuario1 | FL \*]:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-LocalUser -Name usuario1 -Password (ConvertTo-SecureString "clave02" -AsPlainText -Force)
PS C:\Windows\system32> Get-LocalUser -name usuario1 | fl

AccountExpires      :
Description         :
Enabled             : True
FullName            :
PasswordChangeableDate : 17/07/2024 11:32:35
PasswordExpires     : 28/08/2024 11:32:35
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     : 17/07/2024 11:32:35
LastLogon           :
Name                : usuario1
SID                 : S-1-5-21-3840020827-4889075537-786987846-1002
PrincipalSource     : Local
ObjectClass         : Usuario

PS C:\Windows\system32>
```

- Le cambiamos el nombre del **usuario1** al **usuario3**  
"Rename-LocalUser usuario1 -NewName usuario3" "Get-LocalUser -name usuario3 | FL":

```
Administrador: Windows PowerShell
PS C:\Windows\system32> Rename-LocalUser usuario1 -fullname usuario3
PS C:\Windows\system32> Get-LocalUser -name usuario3 | fl

AccountExpires      :
Description         :
Enabled             : True
FullName            :
PasswordChangeableDate : 17/07/2024 11:32:35
PasswordExpires     : 28/08/2024 11:32:35
UserMayChangePassword : True
PasswordRequired    : False
PasswordLastSet     : 17/07/2024 11:32:35
LastLogon           :
Name                : usuario3
SID                 : S-1-5-21-3840020227-4089075537-706907846-1002
PrincipalSource      : local
ObjectClass          : Usuario

PS C:\Windows\system32>
```

- Desactivar un usuario “*Disable-LocalUser usuario2, usuario3*”  
“*Get-LocalUser*”:

```
Administrador: Windows PowerShell
PS C:\Windows\system32> Disable-LocalUser usuario2, usuario3
PS C:\Windows\system32> Get-LocalUser
Get-LocalUser : El término 'GetLocalUser' 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)
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (GetLocalUser: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
JorgeWindowsPro     True
usuario2            False
usuario3            False
WdAGUtilityAccount  False Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

PS C:\Windows\system32>
```

- Activar un usuario “*Enable-LocalUser usuario2, usuario3*”  
“*Get-LocalUser*”:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Enable-LocalUser usuario2, usuario3
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
JorgeWindowsPro      True   Cuenta integrada para el acceso como invitado al equipo o dominio
usuario2             True   Cuenta integrada para el acceso como invitado al equipo o dominio
usuario3             True   Cuenta integrada para el acceso como invitado al equipo o dominio
WDAGUtilityAccount   False  Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

PS C:\Windows\system32>
```

- Eliminar un usuario “*Remove-LocalUser -Confirm usuario2, usuario3*”  
“*Get-LocalUser*”:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Remove-LocalUser -Confirm usuario2

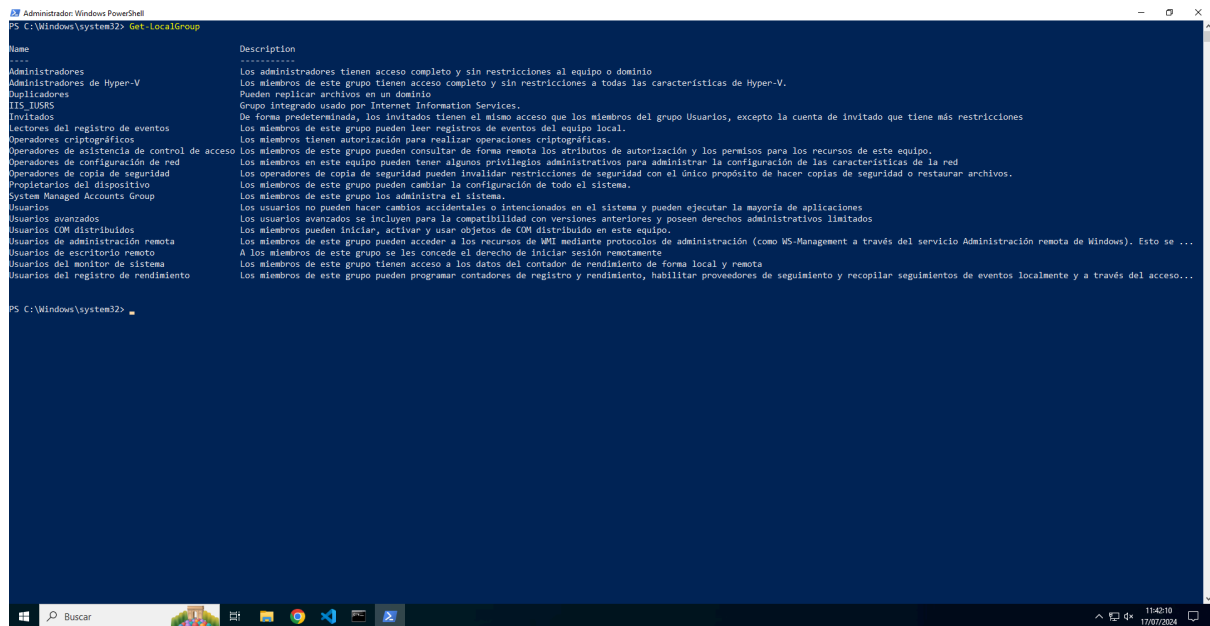
Confirm
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "Quitar usuario local" en el destino "usuario2".
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "S"): N
PS C:\Windows\system32> Remove-LocalUser -Confirm usuario3

Confirm
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "Quitar usuario local" en el destino "usuario3".
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "S"): S
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
JorgeWindowsPro      True   Cuenta integrada para el acceso como invitado al equipo o dominio
usuario2             True   Cuenta integrada para el acceso como invitado al equipo o dominio
usuario3             True   Cuenta integrada para el acceso como invitado al equipo o dominio
WDAGUtilityAccount   False  Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.

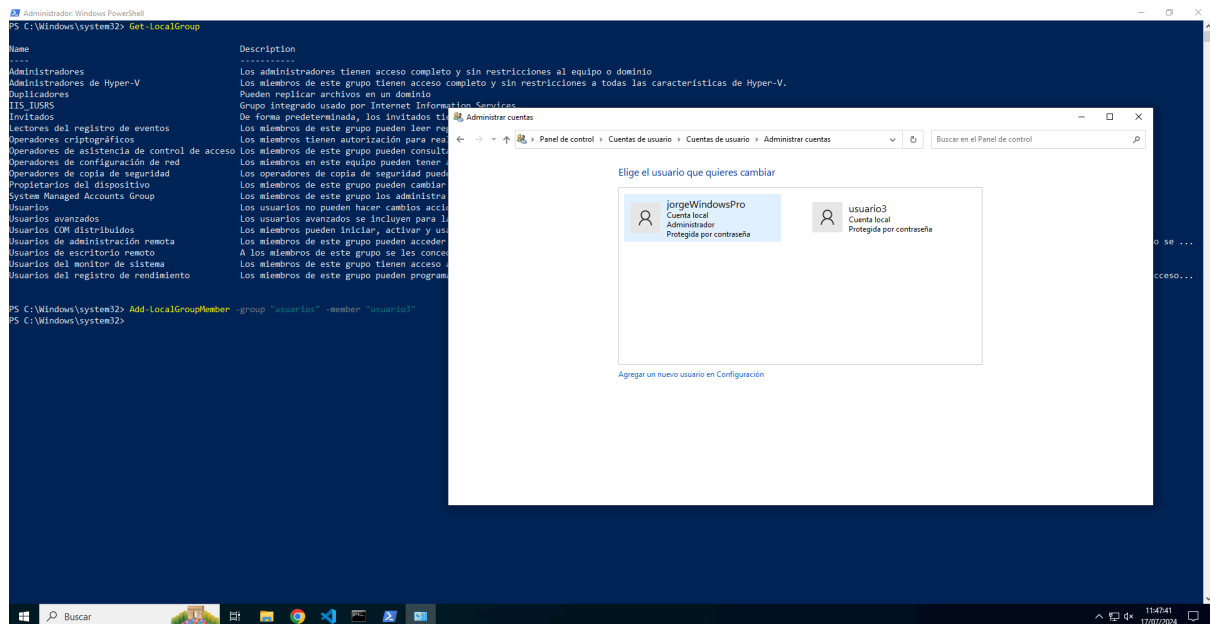
PS C:\Windows\system32>
```

- Mostramos los grupos locales y lo añadimos al grupo el **usuario3**  
[*Get-LocalGroup*] [*Add-LocalGroupMember -group “usuarios” -member “usuario3”*]:



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

Name                Description
-----
Administradores      Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Administradores de Hyper-V Los miembros de este grupo tienen acceso completo y sin restricciones a todas las características de Hyper-V.
Duplicadores         Pueden replicar archivos en un dominio
IIS_IUSRS            Grupo integrado usado por Internet Information Services.
Invitados            De forma predeterminada, los invitados tienen el mismo acceso que los miembros del grupo Usuarios, excepto la cuenta de invitado que tiene más restricciones
Lectores del registro de eventos Los miembros de este grupo pueden leer registros de eventos del equipo local.
Operadores de asistencia de control de acceso Los miembros tienen autorización para realizar operaciones criptográficas.
Operadores de configuración de red Los miembros de este grupo pueden consultar de forma remota los atributos de autorización y los permisos para los recursos de este equipo.
Operadores de copia de seguridad Los miembros en este equipo pueden tener algunos privilegios administrativos para administrar la configuración de las características de la red.
Propietarios del dispositivo Los operadores de copia de seguridad pueden invalidar restricciones de seguridad con el único propósito de hacer copias de seguridad o restaurar archivos.
System Managed Accounts Group Los miembros de este grupo pueden cambiar la configuración de todo el sistema.
Usuarios             Los miembros de este grupo pueden administrar el sistema.
Usuarios avanzados   Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar la mayoría de aplicaciones
Usuarios COM distribuidos Los usuarios avanzados se incluyen para la compatibilidad con versiones anteriores y poseen derechos administrativos limitados
Usuarios de administración remota Los miembros pueden iniciar, activar y usar objetos de COM distribuido en este equipo.
Usuarios de escritorio remoto Los miembros de este grupo pueden acceder a los recursos de WMI mediante protocolos de administración (como WS-Management a través del servicio Administración remota de Windows). Esto se ...
Usuarios del monitor de sistema A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente
Usuarios del registro de rendimiento Los miembros de este grupo tienen acceso a los datos del contador de rendimiento de forma local y remota
Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar proveedores de seguimiento y recopilar seguimientos de eventos localmente y a través del acceso...
```



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

Name                Description
-----
Administradores      Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Administradores de Hyper-V Los miembros de este grupo tienen acceso completo y sin restricciones a todas las características de Hyper-V.
Duplicadores         Pueden replicar archivos en un dominio
IIS_IUSRS            Grupo integrado usado por Internet Information Services.
Invitados            De forma predeterminada, los invitados tienen el mismo acceso que los miembros del grupo Usuarios, excepto la cuenta de invitado que tiene más restricciones
Lectores del registro de eventos Los miembros de este grupo pueden leer registros de eventos del equipo local.
Operadores de asistencia de control de acceso Los miembros tienen autorización para realizar operaciones criptográficas.
Operadores de configuración de red Los miembros de este grupo pueden consultar de forma remota los atributos de autorización y los permisos para los recursos de este equipo.
Operadores de copia de seguridad Los miembros en este equipo pueden tener algunos privilegios administrativos para administrar la configuración de las características de la red.
Propietarios del dispositivo Los operadores de copia de seguridad pueden invalidar restricciones de seguridad con el único propósito de hacer copias de seguridad o restaurar archivos.
System Managed Accounts Group Los miembros de este grupo pueden cambiar la configuración de todo el sistema.
Usuarios             Los miembros de este grupo pueden administrar el sistema.
Usuarios avanzados   Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar la mayoría de aplicaciones
Usuarios COM distribuidos Los usuarios avanzados se incluyen para la compatibilidad con versiones anteriores y poseen derechos administrativos limitados
Usuarios de administración remota Los miembros pueden iniciar, activar y usar objetos de COM distribuido en este equipo.
Usuarios de escritorio remoto Los miembros de este grupo pueden acceder a los recursos de WMI mediante protocolos de administración (como WS-Management a través del servicio Administración remota de Windows). Esto se ...
Usuarios del monitor de sistema A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente
Usuarios del registro de rendimiento Los miembros de este grupo tienen acceso a los datos del contador de rendimiento de forma local y remota
Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar proveedores de seguimiento y recopilar seguimientos de eventos localmente y a través del acceso...
```

```
PS C:\Windows\system32> Add-LocalGroupMember -group "usuarios" -member "usuario3"
PS C:\Windows\system32>
```

## 2. Prueba otros cmdlets

- Muestra información de los procesos "Get-Process":

```
Administrador: Windows PowerShell
PS C:\Windows\system32> Get-Process

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
341 20 7232 29344 0,53 4744 1 ApplicationFrameHost
268 14 6388 27608 25,49 4588 1 conhost
483 20 1880 6180 0,09 468 0 csrss
347 16 1816 5516 40,58 544 1 csrss
459 16 4376 21092 2,26 4188 1 ctfmon
304 16 3732 12944 0,56 404 1 dllhost
198 16 3192 11252 0,03 4572 0 dllhost
915 46 47136 83484 32,59 376 1 dm
2034 88 51072 152520 21,50 4236 1 explorer
36 5 1260 4052 0,03 888 0 fontdrvhost
36 7 2364 6328 0,30 816 1 fontdrvhost
0 0 60 8 0 0 Idle
1220 25 7140 20340 3,56 708 0 lsass
0 0 188 28760 3,56 2024 0 Memory Compression
488 16 8844 21632 0,80 1508 0 MpDefenderCoreService
870 190 250844 208044 56,95 1996 0 MpDefenderCoreService
199 37 3776 10764 0,14 1976 0 NisSrv
1256 107 47956 154428 2,45 6760 1 PhoneExperienceHost
1197 52 104936 139128 35,52 564 1 powershell
0 0 3880 67312 1,03 92 0 Registry
607 27 11924 40468 2,86 1728 1 RuntimeBroker
285 17 6068 25632 1,67 2932 1 RuntimeBroker
286 15 4912 18124 0,13 4580 1 RuntimeBroker
343 18 5636 24384 0,09 5750 1 RuntimeBroker
2843 161 218328 315060 35,56 4040 1 SearchApp
677 38 17740 27244 1,72 3948 0 SearchIndexer
386 15 4288 15484 0,77 4428 0 SecurityHealthService
160 9 1776 9312 0,08 772 1 SecurityHealthSystray
688 12 4800 9968 2,00 688 0 services
105 7 3712 6932 0,19 6452 0 SmbBroker
555 26 10696 39936 0,33 3616 1 ShellExperienceHost
538 18 5940 26588 1,69 1036 1 slhst
53 3 1060 1204 0,23 352 0 smss
48 4 568 1260 0,02 1572 0 spaceman
432 20 5180 15636 0,41 2624 0 spoolsv
598 29 18552 65328 2,58 2484 1 StartMenuExperienceHost
195 11 1844 8516 0,05 408 0 svchost
135 9 1512 11208 0,05 576 0 svchost
1358 21 9964 28956 3,58 880 0 svchost
218 12 2880 10152 0,06 850 0 svchost
1062 20 7052 15500 5,61 920 0 svchost
305 18 4824 17264 0,77 932 0 svchost
112 7 1236 5668 0,00 572 0 svchost
263 10 2312 8488 0,30 976 0 svchost
256 9 1908 11996 0,14 1864 0 svchost
306 14 3096 22108 0,44 1080 1 svchost
301 17 5948 15680 2,25 1152 0 svchost
```

- Iniciamos un proceso [*Start-Process “proceso”*]:

```
Administrador: Windows PowerShell
PS C:\Windows\system32> Start-Process "chrome"
PS C:\Windows\system32> Get-Process

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
341 20 7232 29344 0,53 4744 1 ApplicationFrameHost
293 19 14880 33816 0,17 1500 1 chrome
301 22 26488 62048 0,31 3816 1 chrome
209 14 12400 26004 0,06 3912 1 chrome
310 24 16360 45632 0,83 4144 1 chrome
245 20 17236 28856 0,06 4684 1 chrome
382 22 45068 82192 0,55 4952 1 chrome
193 10 6620 9248 0,03 5720 1 chrome
1292 50 39956 144920 1,98 5856 1 chrome
268 14 6588 27612 25,34 4580 1 conhost
404 20 1880 6180 0,09 468 0 csrss
373 18 1828 5548 41,22 544 1 csrss
463 16 4376 21092 2,41 4188 1 ctfmon
304 16 3732 12944 0,56 404 1 dllhost
198 16 3192 11252 0,03 4572 0 dllhost
920 47 47264 87012 33,38 376 1 dm
2083 81 53392 154204 21,58 4236 1 explorer
36 5 1260 4052 0,03 888 0 fontdrvhost
36 7 2364 6332 0,30 816 1 fontdrvhost
0 0 60 8 0 0 Idle
1246 25 7140 20340 3,56 708 0 lsass
0 0 188 28148 3,56 2024 0 Memory Compression
488 16 8844 21632 0,80 1508 0 MpDefenderCoreService
886 190 250844 214004 57,13 1996 0 MpDefenderCoreService
199 36 3776 10764 0,14 1976 0 NisSrv
1256 107 47956 154428 2,45 6760 1 PhoneExperienceHost
1227 52 108428 142596 35,92 564 1 powershell
0 0 3884 67312 1,03 92 0 Registry
607 27 11924 40468 2,86 1728 1 RuntimeBroker
285 17 6068 25632 1,67 2932 1 RuntimeBroker
286 15 4912 18124 0,13 4580 1 RuntimeBroker
343 18 5636 24384 0,09 5750 1 RuntimeBroker
2843 161 218328 315060 35,56 4040 1 SearchApp
677 38 17792 27244 1,72 3948 0 SearchIndexer
386 15 4288 15484 0,77 4428 0 SecurityHealthService
160 9 1776 9312 0,08 772 1 SecurityHealthSystray
627 12 4800 9968 2,00 688 0 services
105 7 3712 6932 0,19 6452 0 SmbBroker
555 26 10696 39936 0,33 3616 1 ShellExperienceHost
538 18 5940 26588 1,69 1036 1 slhst
53 3 1060 1204 0,23 352 0 smss
48 4 568 1260 0,02 1572 0 spaceman
432 20 5180 15636 0,41 2624 0 spoolsv
598 29 18552 65328 2,58 2484 1 StartMenuExperienceHost
```

- Paramos un proceso [*Stop-Process -name “proceso”*]:

```
Administrador: Windows PowerShell

PS C:\Windows\system32> Stop-Process -name "chrome"
PS C:\Windows\system32> Get-Process

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
341 20 7232 29344 0,53 4744 1 ApplicationFrameHost
215 12 2016 14976 0,02 796 1 backgroundTaskHost
266 14 6568 27680 25,72 4588 1 conhost
494 20 1880 6196 0,09 468 0 csrss
354 17 1852 5524 41,91 544 1 csrss
459 16 4352 21076 2,50 4188 1 ctfmon
384 16 3732 12944 0,56 484 1 dlhlohost
198 16 3192 11252 0,03 4572 0 dlhlohost
915 46 47140 33468 34,08 376 1 dm
2075 81 54144 154996 21,69 4236 1 explorer
36 5 1260 4052 0,03 888 0 fontdrvhost
36 7 2364 6332 0,30 816 1 fontdrvhost
0 0 0 0 0 0 0 Idle
1241 25 7140 20348 3,58 708 0 lsass
0 0 188 26984 3,56 2024 0 Memory Compression
488 16 8844 21628 0,80 1580 0 McDefenderCoreService
885 190 250844 211488 57,41 1996 0 McMpEng
199 36 3776 10764 0,14 1976 0 NisSrv
1268 107 47964 154800 2,55 6760 1 PhoneExperienceHost
1081 52 106040 140732 36,39 564 1 powershell
0 8 3896 67352 1,03 92 0 Registry
607 27 11924 40468 2,88 1728 1 RuntimeBroker
281 17 6080 25604 1,67 2932 1 RuntimeBroker
148 9 1924 9352 0,05 4476 1 RuntimeBroker
286 15 4912 18124 0,13 4580 1 RuntimeBroker
343 18 5636 24304 0,49 576 1 RuntimeBroker
2843 161 218328 315060 35,56 4040 1 SearchApp
679 38 17792 27264 1,72 3948 0 SearchIndexer
386 15 4288 15484 0,77 4428 0 SecurityHealthService
160 9 1776 9312 0,08 772 1 SecurityHealthSystray
627 12 4764 9972 2,00 688 0 services
105 7 3840 6812 0,20 6452 0 SgrmBroker
555 26 10696 39936 0,23 3616 1 ShellExperienceHost
544 18 5992 26636 1,69 1036 1 slhlohost
53 3 1068 1204 0,23 352 0 smss
48 4 568 1260 0,02 1572 0 specman
432 20 5180 15636 0,41 2624 0 spoolsv
597 29 18344 65320 2,59 2484 1 StartMenuExperienceHost
195 11 1844 8516 0,05 408 0 svchost
135 9 1512 11208 0,05 576 0 svchost
1387 22 10092 28648 3,61 800 0 svchost
218 12 2080 10152 0,06 856 0 svchost
1101 19 6096 15556 5,61 920 0 svchost
386 18 4928 17292 0,77 932 0 svchost
```

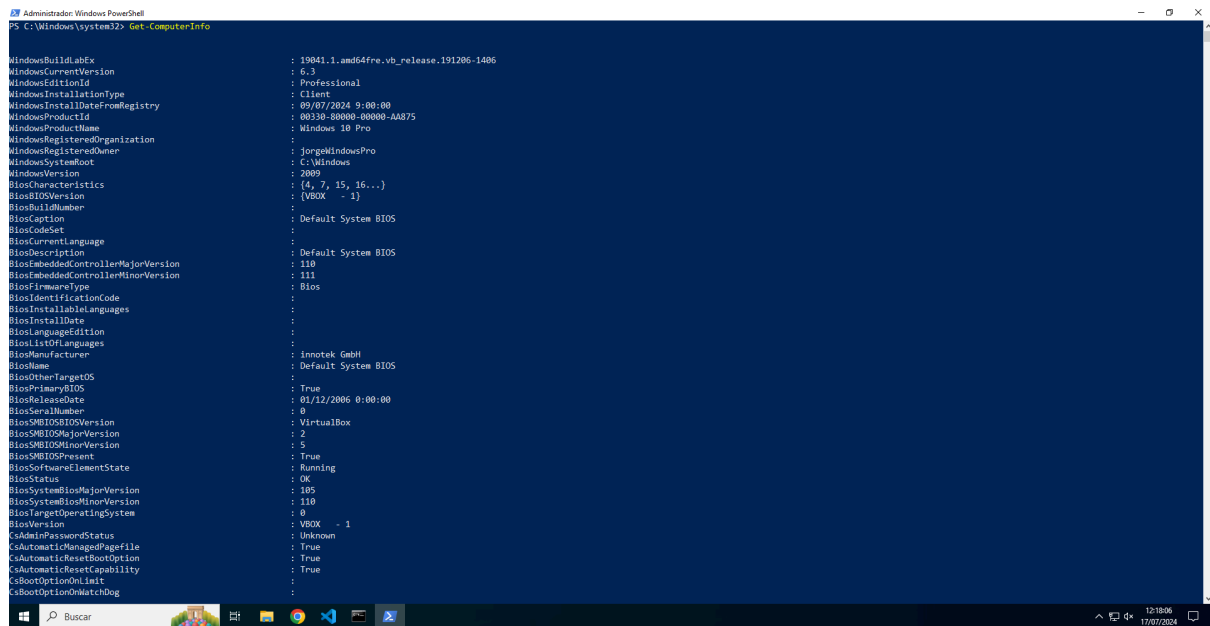
- Mostramos la información de los servicios “Get-Service”:

```
Administrador: Windows PowerShell

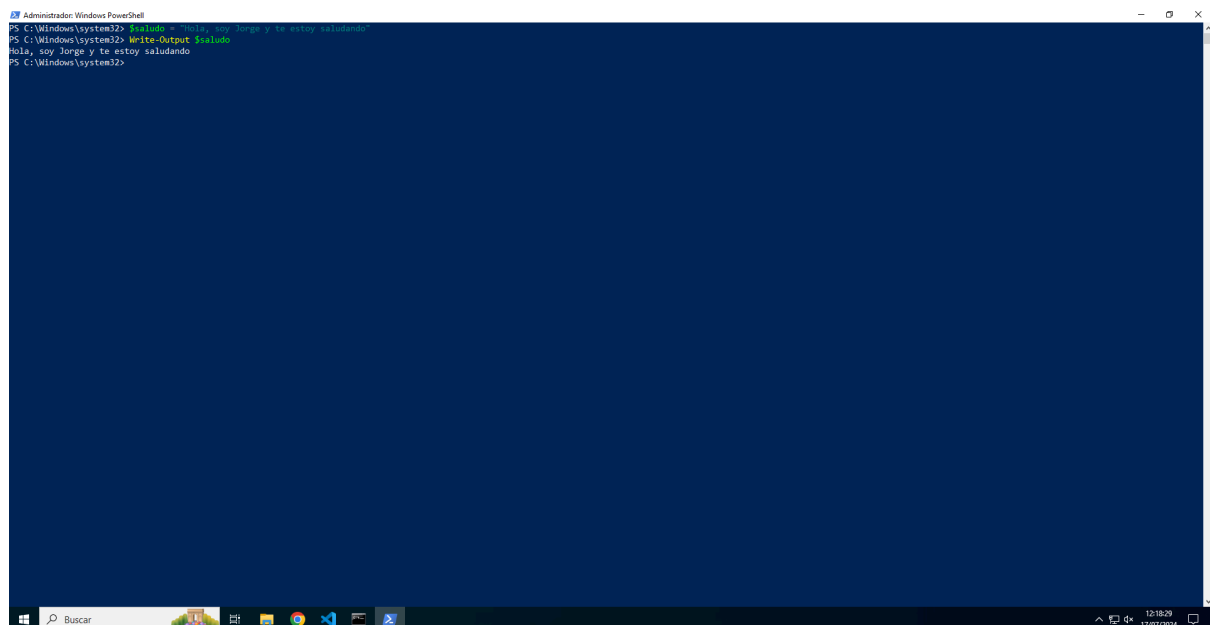
PS C:\Windows\system32> Get-Service

Status Name DisplayName
-----
Stopped AarSvc_31038 Agent Activation Runtime 31038
Stopped ALRouter 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 AppMgmt Administración de aplicaciones
Stopped AppReadiness Preparación de aplicaciones
Stopped AppVClient Microsoft App-V Client
Running AppXSvc Servicio de implementación de AppX ...
Stopped AssignedAccessManager Servicio AssignedAccessManager
Running AudioEndpointBuilder Compilador de extremo de audio de W...
Running AudioSvc Hora de la red de telefonía móvil
Stopped Autotimesvc Instalador de Activos (Autotimesvc)
Stopped BcastDVRUserService_31038 Servicio de usuario de difusión y G...
Stopped BDESVC Servicio Cifrado de unidad BitLocker
Running BFE Motor de filtrado de base
Stopped BITS Servicio de transferencia Inteligen...
Stopped BluetoothUserService_31038 Servicio de soporte técnico de usua...
Running BrokerInfrastructure Servicio de infraestructura de tane...
Stopped BTACService Servicio de puerta de enlace de aud...
Running BthAvctpSvc Servicio AVCTP
Stopped bthserv Servicio de compatibilidad con Blue...
Stopped camsvc Servicio Administrador de funcional...
Stopped CaptureService_31038 CaptureService_31038
Running cdbhsvc_31038 Servicio de usuario del portapapele...
Running CDPSvc Servicio de plataforma de dispositi...
Running CDPUserSvc_31038 Servicio de usuario de plataforma d...
Stopped CertPropSvc Propagación de certificados
Stopped ClipSvc Servicio de licencia de cliente (Cli...
Stopped CloudSvc Servicio de Identidad en la nube de...
Stopped COMSysApp Aplicación del sistema COM+
Running ConsentUserSvc_31038 ConsentUX_31038
Running CoreMessaging CoreMessaging
Stopped CredentialEnrollmentManagerUserSvc_31038 CredentialEnrollmentManagerUserSvc_...
Running CryptSvc Servicios de cifrado
Stopped CSCService Archivos sin conexión
Running DCOMLaunch Iniciador de procesos de servidor DCOM
Stopped dcsvc dcsvc
Stopped defragsvc Optimizar unidades
Stopped DeviceAssociationBroker_31038 DeviceAssociationBroker_31038
Stopped DeviceAssociationBroker_31038 Servicio de asociación de dispositivos
Stopped DeviceInstall Servicio de instalación de disposit...
Stopped DevicePickerSvc_31038 DevicePicker_31038
Stopped DevicesFlowUserSvc_31038 DevicesFlow_31038
Running DevQueryBroker Agente de detección en segundo plan...
Running Dhcp Cliente DHCP
```

- Información del sistema “Get-ComputerInfo”:

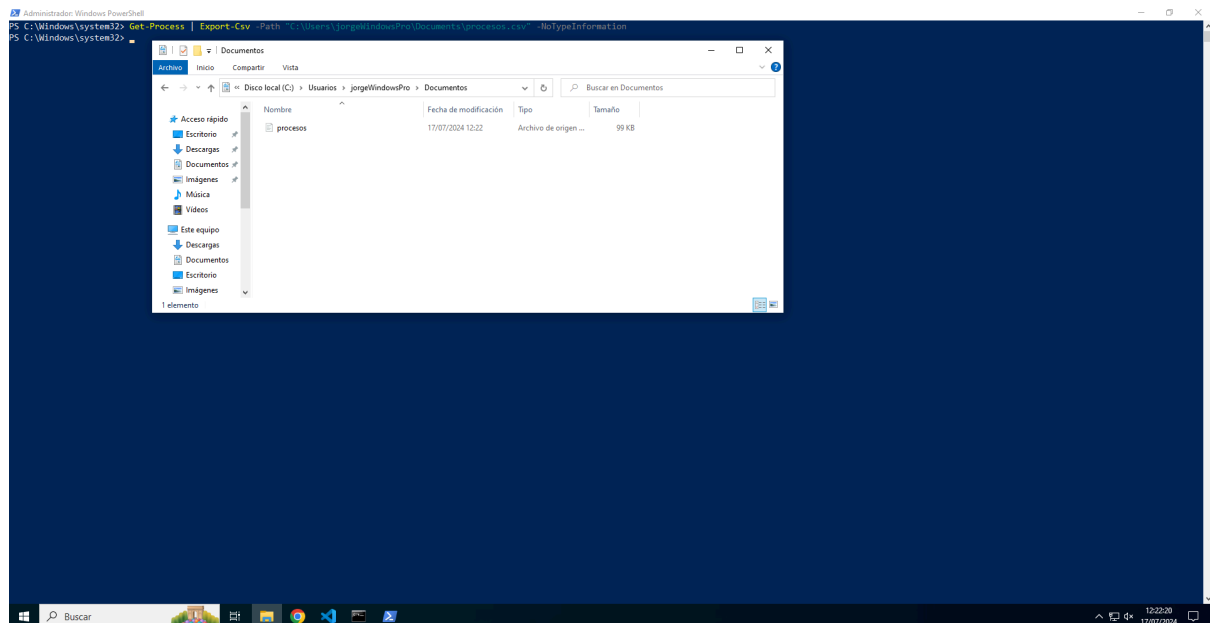


- Crear una variable y asignarle un valor [*\$greeting = "Hello, PowerShell!"*]  
[*Write-Output \$greeting*]:

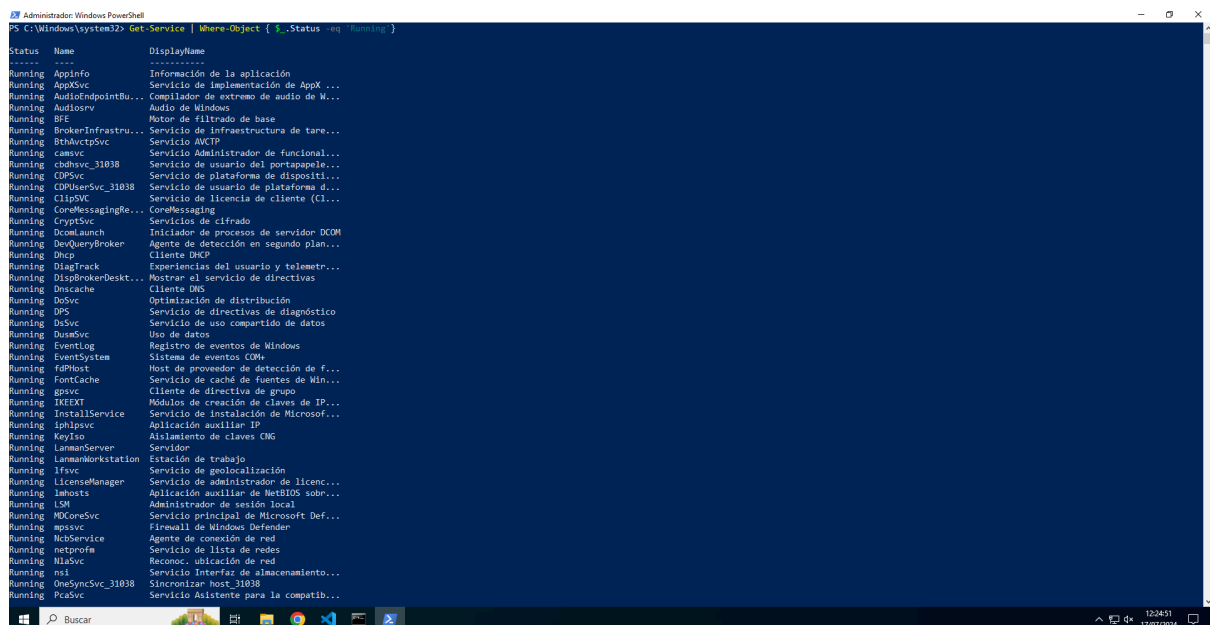


- Exportar lista de procesos a un CSV [*Get-Process* | *Export-Csv -Path "C:\processes.csv" -NoTypeInfo*]:

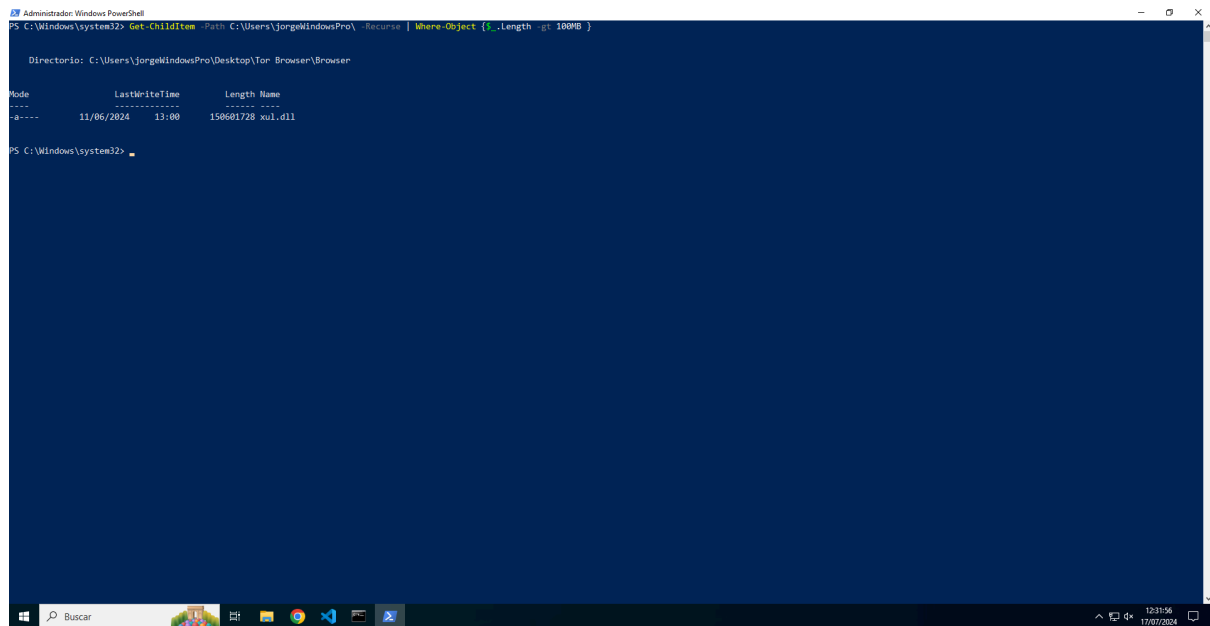




- Filtrar servicios por estado “*Get-Service | Where-Object { \$\_.Status -eq 'Running' }*”:



- Buscar archivos grandes en una carpeta “*Get-ChildItem -Path C:\Users\YourUsername\Documents -Recurse | Where-Object { \$\_.Length -gt 1GB }*”:



```
PS C:\Windows\system32> Get-Childitem -Path C:\Users\jorge\WindowsPro\Desktop\Tor Browser\Browser -Recurse | Where-Object { $_.Length -gt 100KB }

Directorio: C:\Users\jorge\WindowsPro\Desktop\Tor Browser\Browser

Mode                LastWriteTime         Length Name
----                -
-a-----         11/06/2024   13:00      156681728 xul.dll

PS C:\Windows\system32>
```

- Obtener el estado libre en todos los discos [*Get-PSDrive -PSProvider FileSystem | Select-Object Name, @{Name="Free(GB)";Expression="{0:N2}" -f (\$\_.Free/1GB) }}*]:

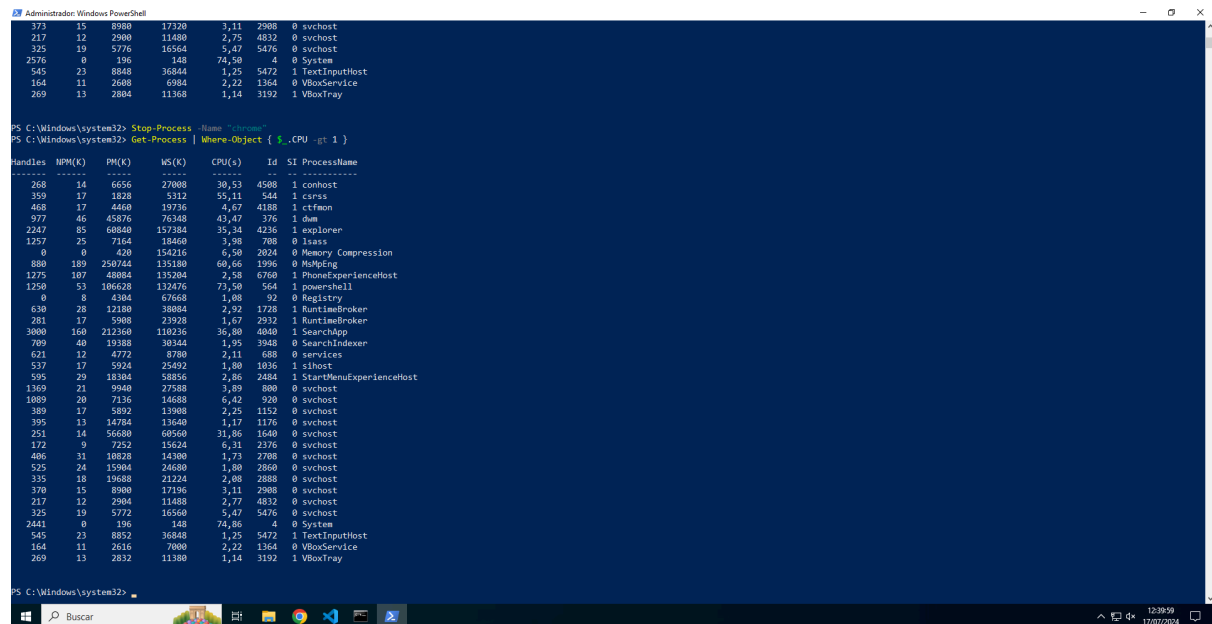
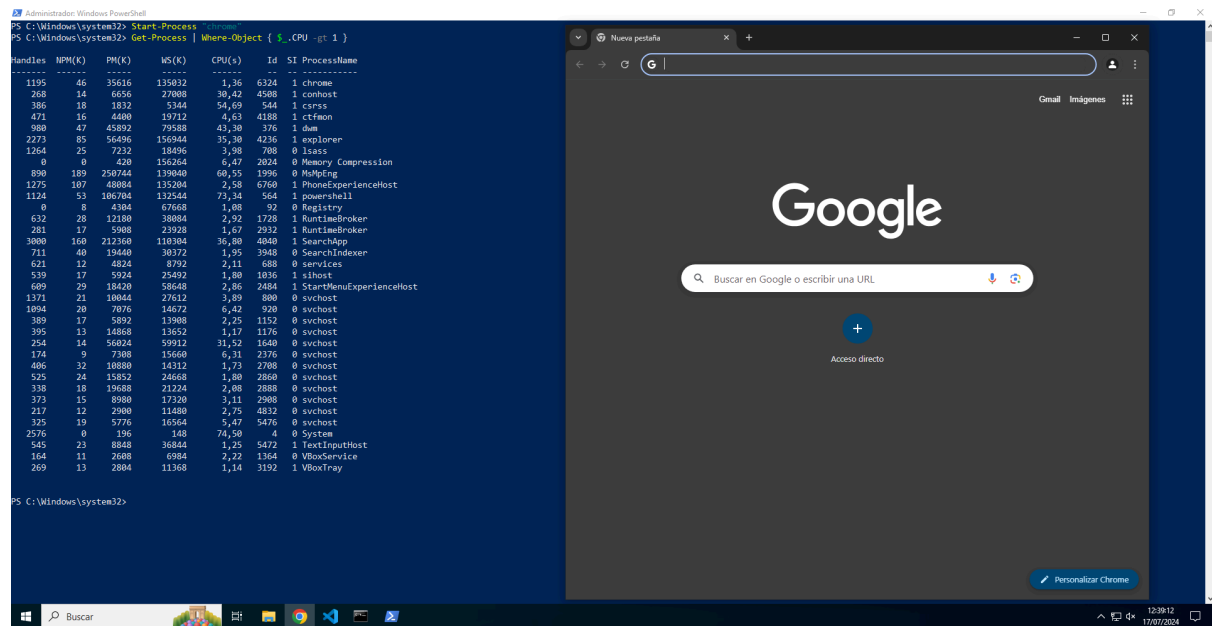


```
PS C:\Windows\system32> Get-PSDrive -PSProvider FileSystem | Select-Object Name, @{Name="Free(GB)";Expression="{0:N2}" -f ($_.Free/1GB) }}

Name Free(GB)
----
C      75,35
D       6,00
E      24,93
F      24,98
G       7,84
H     1.611,35

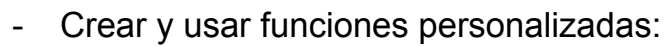
PS C:\Windows\system32>
```

- Administrar procesos (Listar los procesos por el % de CPU y parar el proceso) [*Get-Process | Where-Object { \$\_.CPU -gt 50 }*] [*Stop-Process -Name "notepad"*]:

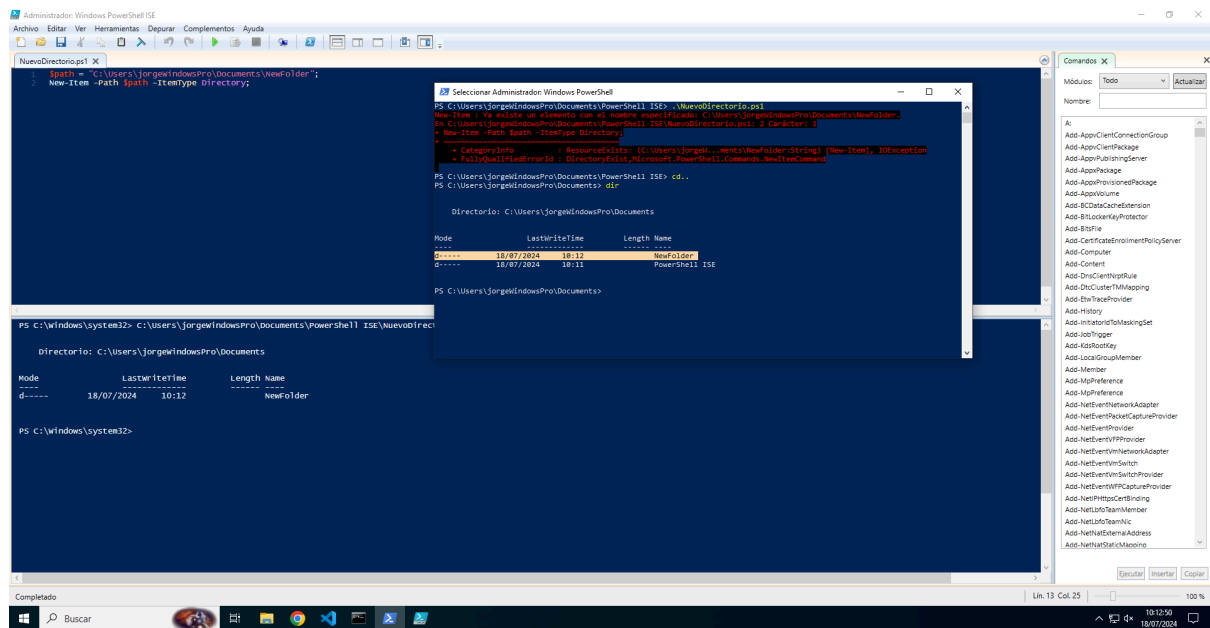


- Para modificar las medidas de seguridad, nos vamos a Powershell y ejecutamos “*Get-ExecutionPolicy*” “*Set-ExecutionPolicy Unrestricted*” “*Get-ExecutionPolicy*”:

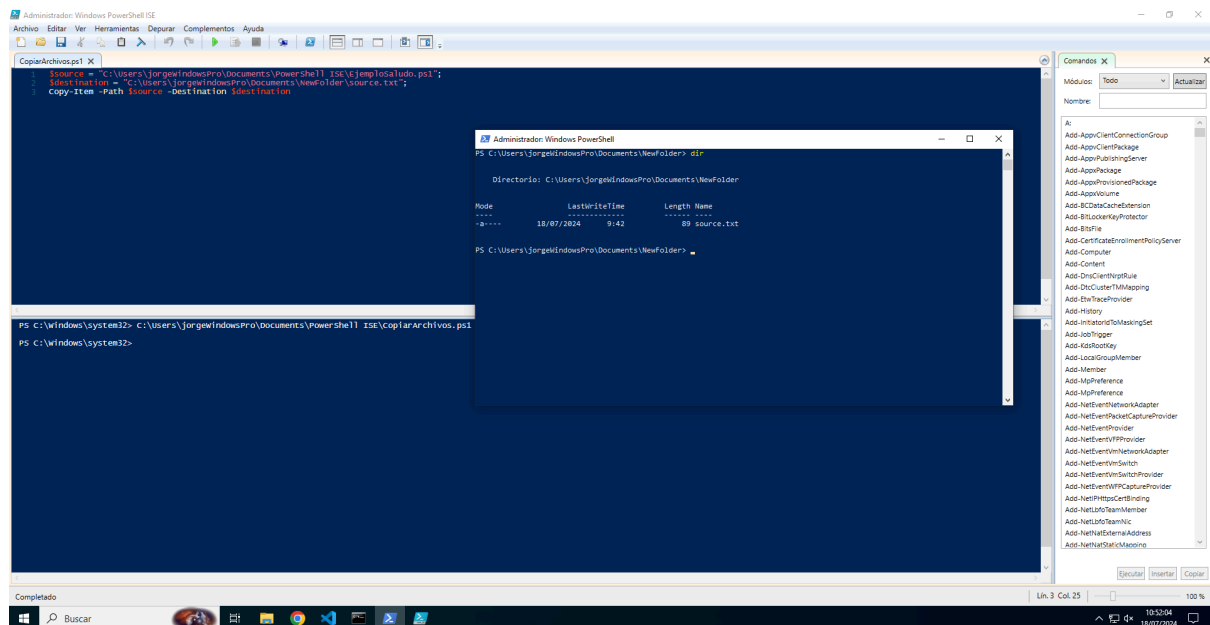








- Copiar Archivos:



- Obtener Información del Sistema:

