

## Actividad 04. Uso de Powershell

---

### ¿Qué es Powershell?

PowerShell es una herramienta utilizada principalmente por los administradores de sistemas Windows para:

- Automatizar tareas.
- Tener un mayor control.

Podemos realizar cualquier tarea desde la línea de comandos sin necesidad de un interfaz gráfico.

Además, si tenemos un entorno como muchos equipos, tendremos que automatizar los procesos, y eso lo haremos a través de scripts, no utilizaremos el interfaz gráfico.

## ¿Dónde podemos encontrar PowerShell?

Podemos encontrarla integrada en: Windows y Windows Server

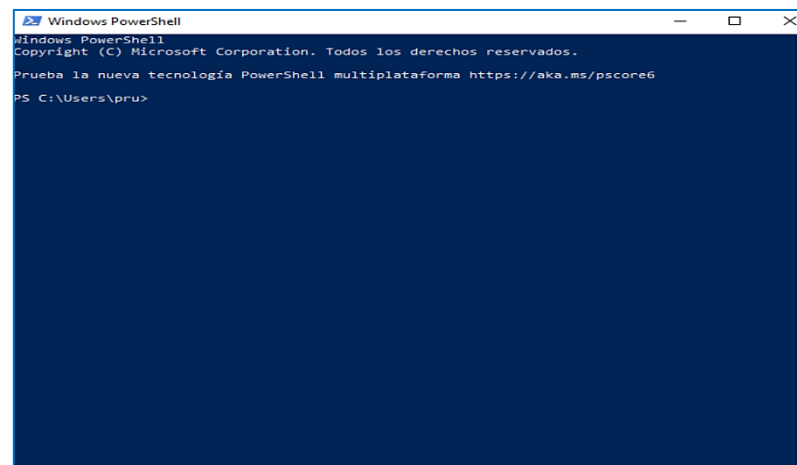
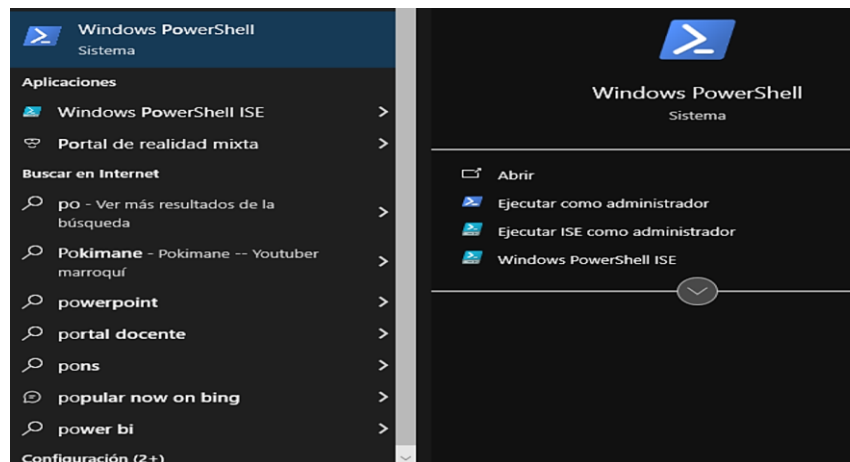
Podemos usarla en productos de Microsoft: Azure, SQL Server, Exchange, IIS (Internet Information Services), Office 365, etc.

Podemos administrar servicios y recursos como los de AWS (Amazon Web Services) y VMware vSphere con PowerShell.

PowerShell también es utilizada por los hackers para obtener información de un equipo y poder atacarlo.

También podemos instalar la PowerShell en macOS y Linux.

# Inicio de Powershell:



# Versión de Powershell:

\$PSVersionTable o Get-Host

```
PS C:\Users\pru> $PSVersionTable
```

Name	Value
PSVersion	5.1.19041.3996
PSEdition	Desktop
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
BuildVersion	10.0.19041.3996
CLRVersion	4.0.30319.42000
WSManStackVersion	3.0
PSRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1

```
PS C:\Users\pru> Get-Host
```

Name	: ConsoleHost
Version	: 5.1.19041.3996
InstanceId	: 69043a14-6d03-4fa6-a9d5-5dcf08b83a14
UI	: System.Management.Automation.Internal.Host.InternalHostUserInterface
CurrentCulture	: es-ES
CurrentUICulture	: es-ES
PrivateData	: Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
DebuggerEnabled	: True
IsRunspacePushed	: False
Runspace	: System.Management.Automation.Runspace.LocalRunspace

## Limpiar pantalla:

Clear

```
PS C:\Users\pru> Clear
```

## Actualizar ayuda:

Update-Help

```
PS C:\Users\pru> Update-Help
```

```
Actualizando Ayuda para el módulo PackageManagement
Buscando contenido de Ayuda...
[
```

# Ejemplo de ayuda:

## Get-Help New-LocalUser -Examples

```
PS C:\Users\pru> Get-Help New-LocalUser -Examples

NOMBRE
    New-LocalUser

SINOPSIS
    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 prompts 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.
```

## Concepto de cmdlet

Un cmdlet es Es una herramienta simple de línea de comandos de una sola función incluida en el shell, cuya finalidad es manipular objetos.

Es una combinación de **verbo** y **nombre** separados por un guión (-).por ejemplo, *Get-Help*. Los verbos expresan acciones específicas de Windows PowerShell, mientras que los nombres describen tipos específicos de objetos.

En Windows PowerShell, la mayoría de cmdlets son muy simples y están diseñados para utilizarlos en combinación con otros cmdlets. Por ejemplo, los cmdlets "get" sólo recuperan datos, los cmdlets "set" sólo establecen o cambian datos, los cmdlets "format" sólo formatean datos y los cmdlets "out" sólo dirigen la salida a un destino especificado.

Es posible que los cmdlets de PowerShell tengan parámetros obligatorios y opcionales. Si falta un parámetro obligatorio, el sistema le solicitará que lo introduzca. Si falta un parámetro opcional, PowerShell utilizará el valor predeterminado.

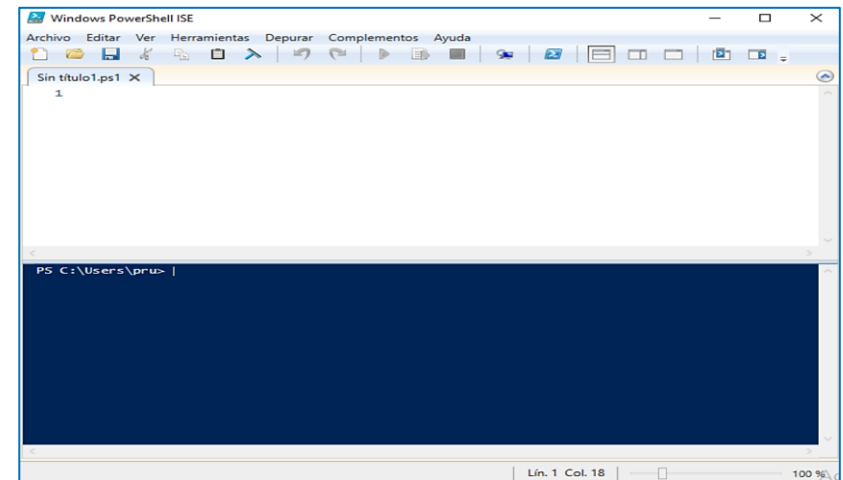
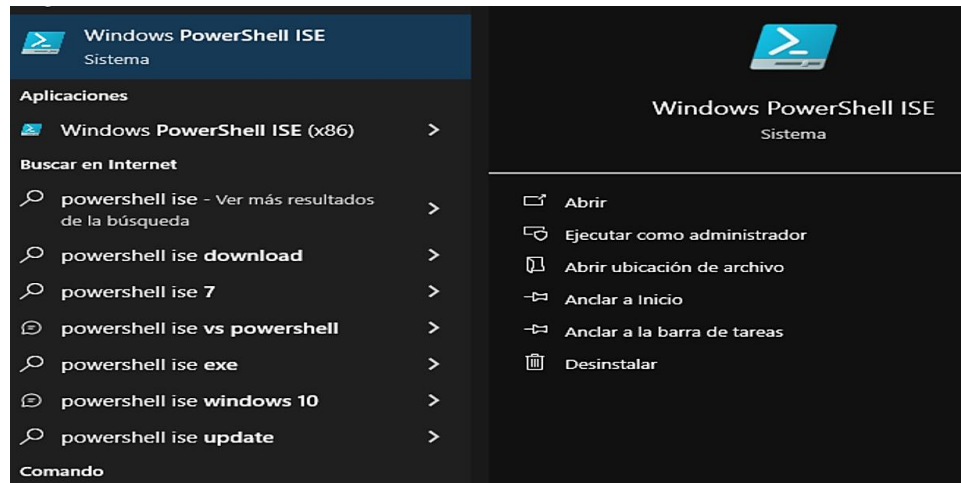
Los cmdlet se agrupan en conjuntos que se denominan módulos.



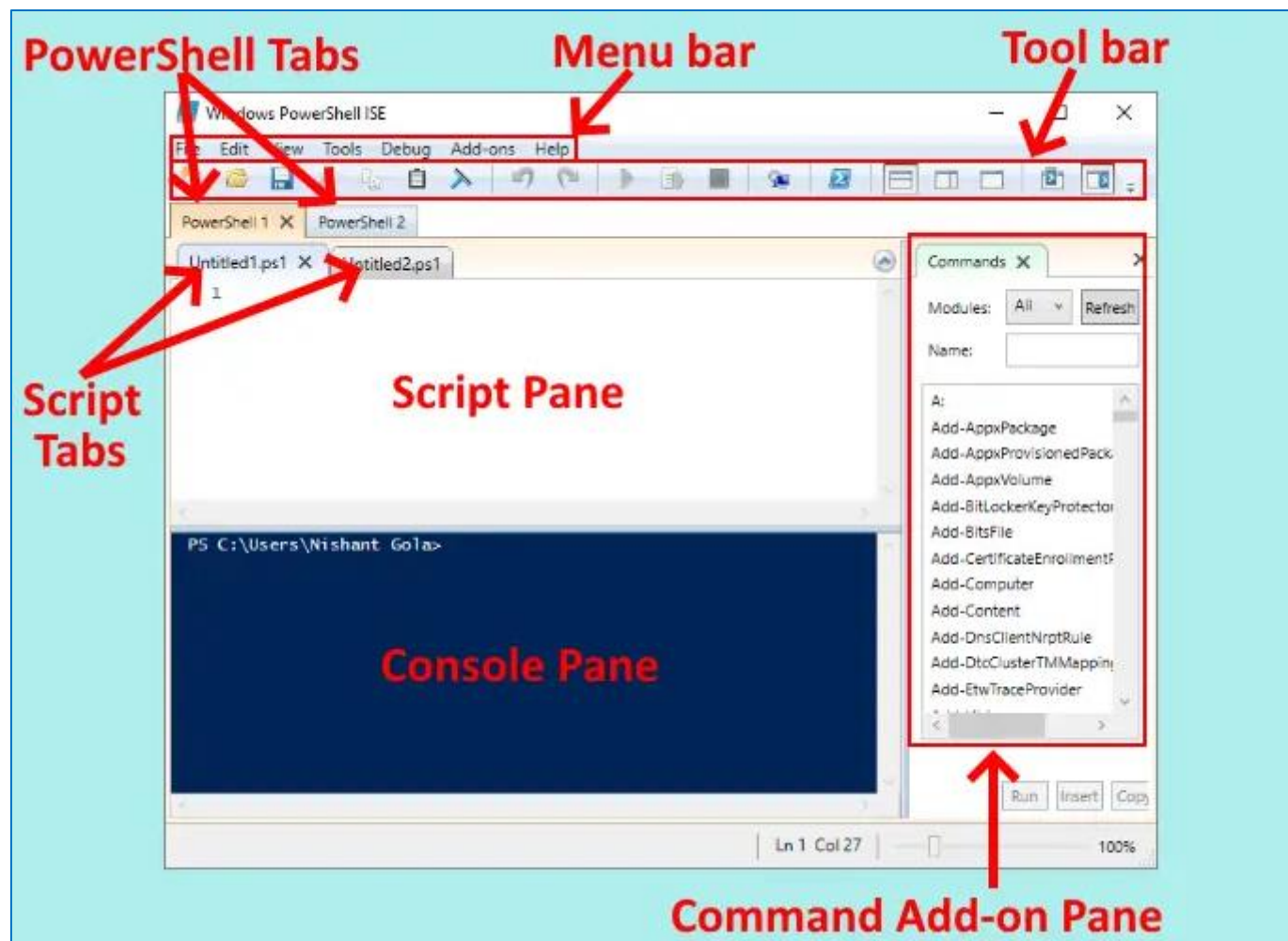
# ¿Qué es Powershell ISE?

Es un entorno que nos permite:

- Ejecutar comandos
- Escribir, probar y depurar scripts.



# Interfaz Powershell ISE



## Seguridad de los scripts:

PowerShell incorpora medidas de seguridad para evitar que se ejecuten, sin la autorización del usuario, scripts que puedan dañar al equipo. Podemos hablar de los siguientes niveles:

- **Restricted:** No se permite la ejecución de scripts. Esta la opción predeterminada.
- **AllSigned:** Todos los scripts deberán estar autenticados, para poder ejecutarlos. Es la opción más segura.
- **RemoteSigned:** En este caso, sólo deberán estar autenticados los scripts que procedan de una ubicación remota.
- **Unrestricted:** Se ejecutará cualquier script sin importar su origen. Se trata de la opción menos recomendada.

# Seguridad de los scripts:

Get-ExecutionPolicy

Set-ExecutionPolicy Unrestricted

Get-ExecutionPolicy

```
PS C:\Windows\system32> Get-ExecutionPolicy
Restricted
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted

Cambio de directiva de ejecución
La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías
exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en
https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución?
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspende [?] Ayuda (el valor predeterminado es "N"): s
PS C:\Windows\system32> Get-ExecutionPolicy
Unrestricted
PS C:\Windows\system32>
```

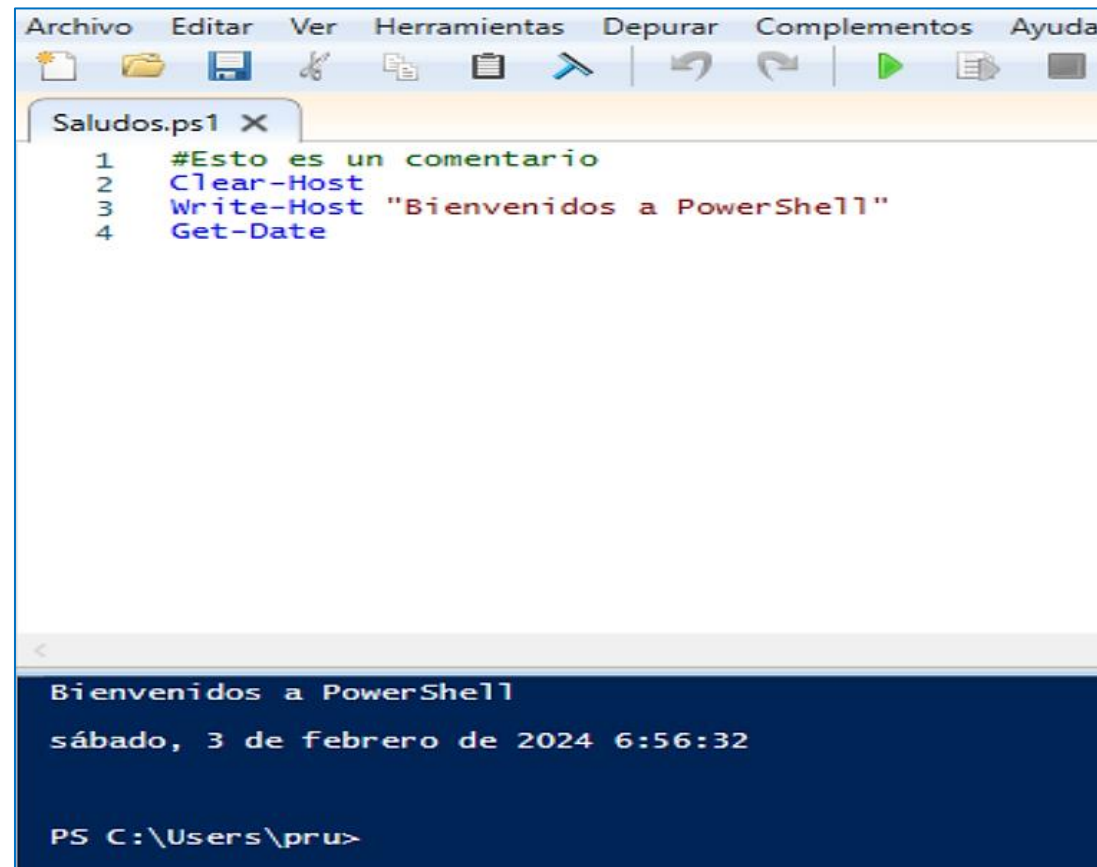
## Ejemplo de script:

#Esto es un comentario

Clear-Host

Write-Host "Bienvenidos a PowerShell"

Get-Date



The image shows a screenshot of a PowerShell script editor window titled 'Saludos.ps1'. The script contains four lines of code: a comment, clearing the host, writing a welcome message, and getting the date. Below the editor, the output of the script is displayed in a dark blue console window. The output shows the welcome message and the current date and time. The prompt 'PS C:\Users\pru>' is visible at the bottom of the console.

```
Archivo  Editar  Ver  Herramientas  Depurar  Complementos  Ayuda
Saludos.ps1 X
1  #Esto es un comentario
2  Clear-Host
3  Write-Host "Bienvenidos a PowerShell"
4  Get-Date

Bienvenidos a PowerShell
sábado, 3 de febrero de 2024 6:56:32

PS C:\Users\pru>
```

# Gestión de usuarios y grupos:

## Gestión usuarios:

### Cmdlets

**Get-LocalUser:** Muestra las cuentas de usuarios locales.

**New-LocalUser:** Crea una nueva cuenta de usuario local.

**Set-LocalUser:** Establece o modifica una propiedad de una cuenta de usuario local.

**Rename-LocalUser:** Renombra una cuenta de usuario local.

**Disable-LocalUser:** Desactiva una cuenta de usuario local.

**Enable-LocalUser:** Activa una cuenta de usuario local.

**Remove-LocalUser:** Elimina una cuenta de usuario local.

## Gestión de usuarios y grupos:

Vamos a trabajar con usuarios locales. Para ver los comandos que vamos a utilizar:

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

## Obtener información de los usuarios existentes:

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
pru	True	
WDAGUtilityAccount	False	Una cuenta de usuario que el sistema administra y usa para escenarios de Protección



# Gestión de usuarios y grupos:

## Obtener de un usuario:

Get-LocalUser -Name Pru | FL

```
PS C:\Windows\system32> Get-LocalUser -Name Pru | FL

AccountExpires           :
Description              :
Enabled                  : True
FullName                 :
PasswordChangeableDate  : 31/01/2024 16:54:41
PasswordExpires         :
UserMayChangePassword    : True
PasswordRequired        : False
PasswordLastSet         : 31/01/2024 16:54:41
LastLogon               : 02/02/2024 9:06:43
Name                    : pru
SID                     : S-1-5-21-3801936962-654424999-518916512-1001
PrincipalSource          : Local
ObjectClass              : Usuario
```



# Gestión de usuarios y grupos:

## Crear una cuenta de usuario:

New-LocalUser usuario1 -NoPassword

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

Name      Enabled Description
----      -
usuario1  True
```

Para crear una cuenta de usuario con contraseña, primero la encriptamos y luego creamos la cuenta:

\$contrasenia = ConvertTo-SecureString "clave001" -AsPlainText -Force

New-LocalUser usuario2 -Password \$contrasenia

```
PS C:\Windows\system32> $contrasenia = ConvertTo-SecureString "clave001" -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
pru               True
usuario1          True
usuario2          True
WDAGUtilityAccount False  Una cuenta de usuario que el sistema administra y usa para escenarios de Prote
```

# Gestión de usuarios y grupos:

## Modificar una cuenta de usuario:

**Establecer una propiedad.** Añadir fullName, La contraseña nunca expira

```
Set-LocalUser usuario2 -FullName "Ana Perez Garcia"
```

```
Set-LocalUser usuario2 -PasswordNeverExpires $true
```

```
Get-LocalUser usuario2 | FL *
```

```
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 usuario2 | FL *
```

AccountExpires	:	
Description	:	
Enabled	:	True
FullName	:	Ana Perez Garcia
PasswordChangeableDate	:	03/02/2024 8:38:07
PasswordExpires	:	
UserMayChangePassword	:	True
PasswordRequired	:	False
PasswordLastSet	:	03/02/2024 8:38:07
LastLogon	:	
Name	:	usuario2
SID	:	S-1-5-21-3801936962-654424999-518916512-1003
PrincipalSource	:	Local
ObjectClass	:	Usuario

# Gestión de usuarios y grupos:

## Modificar una cuenta de usuario:

### Establecer una propiedad. Añadir contraseña

```
Set-LocalUser -Name usuario1 -Password (ConvertTo-SecureString "clave02" -AsPlainText -Force)
```

```
Get-LocalUser usuario1 | FL *
```

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

AccountExpires	:	
Description	:	
Enabled	:	True
FullName	:	
PasswordChangeableDate	:	03/02/2024 8:51:23
PasswordExpires	:	16/03/2024 8:51:23
UserMayChangePassword	:	True
PasswordRequired	:	False
PasswordLastSet	:	03/02/2024 8:51:23
LastLogon	:	
Name	:	usuario1
SID	:	S-1-5-21-3801936962-654424999-518916512-1002
PrincipalSource	:	Local
ObjectClass	:	Usuario

# Gestión de usuarios y grupos:

## Renombrar una cuenta de usuario:

## Establecer una propiedad. Añadir contraseña

GetLocalUser

Rename-LocalUser usuario1 -NewName usuario3

GetLocalUser

```
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
pru                 True
usuario1            True
usuario2            True
WDAGUtilityAccount  False  Una cuenta de usuario que el sistema administra y usa para escenarios

PS C:\Windows\system32> Rename-LocalUser usuario1 -NewName 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
pru                 True
usuario2            True
usuario3            True
WDAGUtilityAccount  False  Una cuenta de usuario que el sistema administra y usa para escenarios
```



# Gestión de usuarios y grupos:

## Activar/Desactivar una cuenta de usuario:

Disable-LocalUser usuario2, usuario3

GetLocalUser

```
PS C:\Windows\system32> Disable-LocalUser usuario2, usuario3
PS C:\Windows\system32> Get-LocalUser

Name                Enabled Description
----                -
Administrador        False  Cuenta integrada para la administración del equipo.
DefaultAccount       False  Cuenta de usuario administrada por el sistema.
Invitado             False  Cuenta integrada para el acceso como invitado al sistema.
pru                  True   Cuenta de usuario administrada por el sistema.
usuario2             False
usuario3             False
WDAGUtilityAccount   False  Una cuenta de usuario que el sistema administra y
```

Enable-LocalUser usuario2, usuario3

GetLocalUser

```
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.
DefaultAccount       False  Cuenta de usuario administrada por el sistema.
Invitado             False  Cuenta integrada para el acceso como invitado al sistema.
pru                  True   Cuenta de usuario administrada por el sistema.
usuario2             True
usuario3             True
WDAGUtilityAccount   False  Una cuenta de usuario que el sistema administra y
```

# Gestión de usuarios y grupos:

## Eliminar una cuenta de usuario:

Remove-LocalUser -Confirm usuario2

Remove-LocalUser usuario3

GetLocalUser

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

Confirmar
¿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 p
PS C:\Windows\system32> Remove-LocalUser usuario3
PS C:\Windows\system32> Get-LocalUser

Name                Enabled Description
----                -
Administrador        False  Cuenta integrada para la administración del equipo o do
DefaultAccount       False  Cuenta de usuario administrada por el sistema.
Invitado             False  Cuenta integrada para el acceso como invitado al equipo
pru                  True
WDAGUtilityAccount   False  Una cuenta de usuario que el sistema administra y usa p
```

# Gestión de usuarios y grupos:

## Gestión de grupos de usuarios:

### Cmdlets

**Get-LocalGroup:** muestra los grupos locales.

**New-LocalGroup:** Crea un nuevo grupo local.

**Set-LocalGroup:** Establece o modifica una propiedad de un grupo local.

**Rename-LocalGroup:** Renombra un grupo local.

**Remove-LocalGroup:** Elimina un grupo local.

**Get-LocalGroupMember:** Muestra los miembros de un grupo.

**Add-LocalGroupMember:** Agrega un miembro a un grupo.

**Remove-LocalGroupMember:** Elimina un miembro de un grupo local.

# Gestión de usuarios y grupos:

## Gestión de grupos de usuarios:

### Información de grupos

Get-LocalGroup

Get-LocalGroup administradores | fl \*

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

Name
----
Administradores
Administradores de Hyper-V
Duplicadores
IIS_IUSRS
Invitados
Lectores del registro de eventos
Operadores criptográficos
Operadores de asistencia de control de acceso
Operadores de configuración de red
Operadores de copia de seguridad
Propietarios del dispositivo
System Managed Accounts Group
Usuarios
Usuarios avanzados
Usuarios COM distribuidos
Usuarios de administración remota
Usuarios de escritorio remoto
Usuarios del monitor de sistema
Usuarios del registro de rendimiento

Description
-----
Los administradores tienen acceso completo y sin restricción al equipo o dominio
Los miembros de este grupo tienen acceso completo y sin restricciones al equipo o dominio
Pueden replicar archivos en un dominio
Grupo integrado usado por Internet Information Services
De forma predeterminada, los invitados tienen el mismo nivel de acceso que los usuarios
Los miembros de este grupo pueden leer registros de eventos
Los miembros tienen autorización para realizar operaciones de administración
Los miembros de este grupo pueden consultar de forma remota el equipo
Los miembros en este equipo pueden tener algunos privilegios de administración
Los operadores de copia de seguridad pueden invalidar registros de eventos
Los miembros de este grupo pueden cambiar la configuración de seguridad
Los miembros de este grupo administran el sistema.
Los usuarios no pueden hacer cambios accidentales o intencionales en el sistema
Los usuarios avanzados se incluyen para la compatibilidad con versiones anteriores
Los miembros pueden iniciar, activar y usar objetos de seguridad
Los miembros de este grupo pueden acceder a los recursos de red
A los miembros de este grupo se les concede el derecho de control de acceso
Los miembros de este grupo tienen acceso a los datos de rendimiento
Los miembros de este grupo pueden programar contadores de rendimiento

PS C:\Windows\system32> Get-LocalGroup administradores | fl *

Description      : Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Name             : Administradores
SID              : S-1-5-32-544
PrincipalSource  : Local
ObjectClass      : Grupo
```



# Gestión de usuarios y grupos:

## Gestión de grupos de usuarios:

### Información de grupos

Get-LocalGroup

Get-LocalGroup administradores | fl \*

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

Name
----
Administradores
Administradores de Hyper-V
Duplicadores
IIS_IUSRS
Invitados
Lectores del registro de eventos
Operadores criptográficos
Operadores de asistencia de control de acceso
Operadores de configuración de red
Operadores de copia de seguridad
Propietarios del dispositivo
System Managed Accounts Group
Usuarios
Usuarios avanzados
Usuarios COM distribuidos
Usuarios de administración remota
Usuarios de escritorio remoto
Usuarios del monitor de sistema
Usuarios del registro de rendimiento

Description
-----
Los administradores tienen acceso completo y sin restricción al equipo o dominio
Los miembros de este grupo tienen acceso completo y sin restricciones al equipo o dominio
Pueden replicar archivos en un dominio
Grupo integrado usado por Internet Information Services
De forma predeterminada, los invitados tienen el mismo acceso que los usuarios invitados
Los miembros de este grupo pueden leer registros de eventos
Los miembros tienen autorización para realizar operaciones de administración de dispositivos
Los miembros de este grupo pueden consultar de forma remota el registro de eventos
Los miembros en este equipo pueden tener algunos privilegios de administración
Los operadores de copia de seguridad pueden invalidar registros de eventos
Los miembros de este grupo pueden cambiar la configuración de dispositivos
Los miembros de este grupo administran el sistema.
Los usuarios no pueden hacer cambios accidentales o intencionales en el sistema
Los usuarios avanzados se incluyen para la compatibilidad con aplicaciones de terceros
Los miembros pueden iniciar, activar y usar objetos de administración de dispositivos
Los miembros de este grupo pueden acceder a los recursos de administración de dispositivos
A los miembros de este grupo se les concede el derecho de control de acceso
Los miembros de este grupo tienen acceso a los datos de configuración de dispositivos
Los miembros de este grupo pueden programar contadores de rendimiento
```

```
PS C:\Windows\system32> Get-LocalGroup administradores | fl *
```

Description	: Los administradores tienen acceso completo y sin restricciones al equipo o dominio
Name	: Administradores
SID	: S-1-5-32-544
PrincipalSource	: Local
ObjectClass	: Grupo

# Gestión de usuarios y grupos:

## Scripts de ejemplo:

### Crear usuario:

```
##Creación de un usuario
```

```
Clear
```

```
$usuario=Read-Host "Introduce nombre de usuario"
```

```
$contra=Read-Host "Introduce contraseña" -AsSecureString
```

```
New-LocalUser $usuario -Password $contra
```

```
Add-LocalGroupMember usuarios -Member $usuario
```

# Gestión de carpetas compartidas:

## Cmdlets

**Get-SmbShare:** muestra las carpetas compartidas.

**New-SmbShare:** Crea una carpeta compartida. La carpeta debe existir.

**Set-SmbShare:** Establece o modifica una propiedad de la carpeta compartida.

**Remove-SmbShare:** Elimina una carpeta compartida

# Gestión de discos:

## Cmdlets

**Get-Disk:** muestra los discos detectados por el sistema.

**Get-Partition:** muestra las particiones visibles.

**New-VHD:** Crea un disco duro virtual.

**Mount-VHD:** Monta un disco virtual.

**Dismount-VHD:** desmonta un disco virtual.

**Initialize-Disk:** Inicializar un disco.

**New-Partition:** Crea una nueva partición.

**Format-volume:** Dar formato a una partición.

**Set-Disk:** Modificar las propiedades de un disco.

**Clear-Disk:** Limpiar de datos un disco duro y reinicializa el disco.

## Gestión de la red:

### Cmdlets

#### Información de los adaptadores de red:

**Get-NetAdapter:** muestra información de los adaptadores de red.

**Enable-NetAdapter:** Activa el adaptador de red.

**Disable-NetAdapter:** Desactiva el adaptador de red.

**Get-NetIPAddress:** IP de un adaptador.

#### Información de la configuración de la red

**Get-NetIPConfiguration:** muestra información de IP, DNS y puerta de enlace.

**Get-NetRoute:** nos muestra la tabla de enrutamiento.

### DNS

**Get-DnsClientCache:** Nos muestra la caché DNS.

**Get-DnsClientServerAddress:** Nos muestra los servidores DNS.

**Resolve-DnsName:** Para comprobar si resuelve el DNS.

**Clear-DNSClientCache:** Limpia la cache DNS

## **Puertos**

**Get-NetTCPConnection:** Muestra información de los puertos

## **Conectividad**

**Test-Connection:** Comprobar la conectividad de la red

## **Configuración estática:**

**Remove-NetIPAddress:** Borrarnos la IP.

**Remove-NetRoute:** Borrarnos la puerta de enlace.

**New-NetIPAddress:** Establecemos una nueva IP.

**Set-DnsClientServerAddress:** Establecemos los DNS.

## **Configuración dinámica:**

**Remove-NetIPAddress:** Borrarnos la IP.

**Remove-NetRoute:** Borrarnos la puerta de enlace.

**Set-NetInterface:** Habilitamos DHCP.

**Set-DnsClientServerAddress:** Establecemos los DNS.

# Gestión de procesos:

## Cmdlets

**Get-Process:** muestra información de los procesos.

**Stop-Process:** detiene un proceso.

**Start-Process:** Inicia un proceso.



# Gestión de servicios:

## Cmdlets

**Get-Service:** muestra información de los servicios.

**-RequiredServices:** Servicios necesarios para iniciar el servicio.

**-DependentServices:** Servicios que dependen.

**Stop-Service:** detiene el servicio. **Start-Service:** inicia el servicio.

**Set-Service:** Modifica los parámetros de un servicio.

# Gestión de tareas programadas:

## Cmdlets

**Get-ScheduledTask:** muestra información de las tareas programadas.

**New-ScheduledTaskAction:** Definimos la acción.

**New-ScheduledTaskTrigger:** Definimos el desencadenador.

**Register-ScheduledTask:** Registramos la tarea.

**Set-ScheduledTask:** Modifica una tarea programada.

**Export-ScheduledTask:** Exportar una tarea programada.

**Register-ScheduledTask –xml:** Importar una tarea programada.

**Enable-ScheduledTask:** Activa una tarea programada.

**Disable-ScheduledTask:** Desactiva una tarea programada.

**Unregister-ScheduledTask:** Eliminar una tarea programada

# Gestión de impresoras:

## Cmdlets

**Get-Printer:** muestra las impresoras instaladas en el equipo.

**Get-PrinterDriver:** muestra los controladores de impresión instalados.

**Add-Printerdrive:** Instalar un controlador de impresión.

**Add-PrinterPort:** Instala un puerto de impresión.

**Add-Printer:** Instala una impresora.

**Set-Printer:** Modifica/actualiza una propiedad de la impresora.

**Remove-Printer:** Elimina una impresora.

**Remove-PrinterDriver:** Elimina un controlador de impresora.

**Remove-PrinterPort:** Elimina un puerto de impresora.

# Gestión de eventos:

## Cmdlets

**Get-EventLog:** muestra los registros principales.

**Get-EventLog -LogName System :** muestra eventos relacionados con el sistema.

**Index:** número asociado al evento.

**Time:** Fecha y hora del evento.

**EntryType:** La importancia del evento: error, warning, etc  
**Source:** Origen del evento.

**InstanceID:** número asociado a un tipo de evento en concreto.

**Message:** El mensaje.

# Gestión de eventos:

## Cmdlets

**Get-WinEvent:** muestra los registros principales y los generados con la tecnología Windows Event Log.

**Get-WinEvent -LogName system:** muestra eventos relacionados con el sistema.

**TimeCreated:** La fecha de creación.

**ProviderName:** Fuente que escribió el evento.

**Id:** Número que indica el tipo de evento (equivalente a InstanceID)

**Message:** El mensaje.

**FilterHashtable:** nos permite hacer consultas más eficientes.

---

## Se pide:

1. Elaborar un documento mostrando el uso de los cmdlets de Powershell para gestionar usuarios y grupos
2. Prueba otros cmdlets