

# Laboratorio de Active Directory

## Entorno

Windows Server 2022, Windows 10

VirtualBox

Active Directory Users and Computers

GPMC

PowerShell (módulo Active Directory)

## Índice

1. Introducción
2. Preparación del entorno
3. Instalación del rol de Active Directory
4. Estructura del dominio
5. Creación de usuarios y grupos
6. Políticas de contraseñas
7. Gestión del ciclo de vida de usuarios
8. Permisos sobre recursos compartidos
9. Resumen final

## 1. Introducción

Este laboratorio documenta la instalación, configuración y administración básica de un dominio Active Directory en un entorno aislado. El objetivo fue practicar tareas fundamentales de administración: creación de usuarios y grupos, estructura del dominio, políticas de contraseñas, gestión del ciclo de vida de usuarios y permisos sobre recursos compartidos.

## 2. Preparación del entorno

Se utilizó VirtualBox para desplegar dos máquinas:

- Windows Server 2022 – Controlador de Dominio
- Windows 10 – Cliente para pruebas

Ambas máquinas se configuraron con IP estática (192.168.100.x/24) y el servidor se estableció como DNS principal

```
PS C:\Windows\system32> ping 192.168.100.10

Haciendo ping a 192.168.100.10 con 32 bytes de datos:
Respuesta desde 192.168.100.10: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.100.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
PS C:\Windows\system32> ping 192.168.100.20

Haciendo ping a 192.168.100.20 con 32 bytes de datos:
Respuesta desde 192.168.100.20: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.100.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Windows\system32> ■
```

Se comprobó conectividad entre ambos hosts mediante ping

```
Administrator: Windows PowerShell
Aceptar
PS C:\Users\Administrador> ping 192.168.100.20

Haciendo ping a 192.168.100.20 con 32 bytes de datos:
Respuesta desde 192.168.100.20: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.100.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
PS C:\Users\Administrador> ping 192.168.100.10

Haciendo ping a 192.168.100.10 con 32 bytes de datos:
Respuesta desde 192.168.100.10: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.100.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\Administrador> -
```

### 3. Instalación del rol de Active Directory

Se instaló AD DS desde Server Manager y se promovió el servidor creando un nuevo bosque con dominio lab.local

```
Administrator: Windows PowerShell
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\Administrador> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True   No           Success       {Servicios de dominio de Active Directory,...}

PS C:\Users\Administrador> Get-WindowsFeature AD-Domain-Services

Display Name                               Name                               Install State
-----                                     -----
[X] Servicios de dominio de Active Directory          AD-Domain-Services           Installed

PS C:\Users\Administrador>
```

Tras el reinicio, el servidor comenzó a funcionar como Domain Controller, con AD DS y DNS

```
PS C:\Users\Administrador> Get-Service DNS
Status     Name               DisplayName
-----     --name--           --displayname--
Running    DNS               Servidor DNS

PS C:\Users\Administrador> nslookup lab.local
DNS request timed out.
      timeout was 2 seconds.
Servidor:  Unknown
Address:   ::1

Nombre:  lab.local
Address:  192.168.100.10
PS C:\Users\Administrador>
```

## 4. Estructura del dominio

Se creó una estructura básica de Unidades Organizativas para administrar los objetos del dominio:

- o OU Usuarios
- o Empleados
- o Personal
- o OU Grupos
- o OU Computadoras
- o OU destinada a cuentas deshabilitadas

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the domain structure under 'lab.local'. On the right, a detailed list view shows various objects within the domain, including 'Computadoras' (Computers), 'Grupos' (Groups), and 'Usuarios' (Users). A specific entry for 'Usuarios' is selected, showing its properties in the details pane.

Nombre	Tipo	Descripción
Builtin	builtinDomain	
Computadoras	Unidad organi...	
Computers	Contenedor	Default container for up...
Domain Controll...	Unidad organi...	Default container for do...
ForeignSecurityP...	Contenedor	Default container for sec...
Grupos	Unidad organi...	
Keys	Contenedor	Default container for ke...
LostAndFound	lostAndFound	Default container for or...
Managed Service...	Contenedor	Default container for ma...
Program Data	Contenedor	Default location for stor...
System	Contenedor	Builtin system settings
Users	Contenedor	Default container for up...
Usuarios	Unidad organi...	
NTDS Quotas	msDS-QuotaC...	Quota specifications co...
TPM Devices	msTPM-Infor...	
Infrastructure	infrastructureU...	

## 5. Creación de usuarios y grupos

Se crearon usuarios dentro de la OU Empleados (ej. Luciano Sosa, Julieta Gomez), con contraseñas iniciales y obligación de cambiarla en el primer inicio

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the structure of the Active Directory, including the root 'Usuarios y equipos de Active Directory' and the 'lab.local' domain. Under 'lab.local', several containers like 'Builtin', 'Computadoras', 'Computers', 'Domain Controllers', etc., are listed. A folder named 'Empleados' is highlighted under the 'Users' container. On the right, a table lists four users: Graciela Romero, Julieta Gomez, Luciano Sosa, and Martin Gonzalez, all categorized as 'Usuario'. The table has columns for 'Nombre', 'Tipo', and 'Descripción'.

Nombre	Tipo	Descripción
Graciela Romero	Usuario	
Julieta Gomez	Usuario	
Luciano Sosa	Usuario	
Martin Gonzalez	Usuario	

Se creó el grupo G\_Employees and the users were added to it. It was worked both from GUI as from PowerShell

The screenshot shows the same ADUC interface. The 'Groups' folder under 'lab.local' is now highlighted. On the right, a table lists three groups: 'G\_Administrador...', 'G\_Contadores', and 'G\_Employees'. All three groups are categorized as 'Grupo de segu...' (Group of Security). The table has columns for 'Nombre', 'Tipo', and 'Descripción'.

Nombre	Tipo	Descripción
G_Administrador...	Grupo de segu...	Administradores
G_Contadores	Grupo de segu...	Contadores
G_Employees	Grupo de segu...	Empleados Oficina

## 6. Políticas de contraseñas

Se configuró la política del dominio mediante GPMC, definiendo:

- Longitud mínima según el grupo
- Complejidad activa
- Bloqueo tras 5 intentos fallidos
- Se implementaron FGPP para grupos específicos (Contadores, empleados, administradores)

```
PS C:\Users\Administrador> Get-ADFinegrainedPasswordPolicy -Identity "FGPP_Contadores"

AppliesTo          : {CN=G_Contadores,OU=Grupos,DC=lab,DC=local}
ComplexityEnabled  : True
DistinguishedName : CN=FGPP_Contadores,CN=Password Settings Container,CN=System,DC=lab,DC=local
LockoutDuration    : 00:15:00
LockoutObservationWindow : 00:15:00
LockoutThreshold   : 5
MaxPasswordAge     : 90.00:00:00
MinPasswordAge     : 1.00:00:00
MinPasswordLength  : 12
Name               : FGPP_Contadores
ObjectClass        : msDS-PasswordSettings
ObjectGUID         : 15919a8d-594b-4f38-977f-bbe4da1f958f
PasswordHistoryCount : 12
Precedence         : 20
ReversibleEncryptionEnabled : False

PS C:\Users\Administrador> Get-ADFinegrainedPasswordPolicy -Identity "FGPP_Empleados"

AppliesTo          : {}
ComplexityEnabled  : True
DistinguishedName : CN=FGPP_Empleados,CN=Password Settings Container,CN=System,DC=lab,DC=local
LockoutDuration    : 00:10:00
LockoutObservationWindow : 00:10:00
LockoutThreshold   : 8
MaxPasswordAge     : 180.00:00:00
MinPasswordAge     : 00:00:00
MinPasswordLength  : 8
Name               : FGPP_Empleados
ObjectClass        : msDS-PasswordSettings
ObjectGUID         : c6f47fa2-4b78-465a-8473-de7e82744b22
PasswordHistoryCount : 8
Precedence         : 30
ReversibleEncryptionEnabled : False
```

```
PS C:\Users\Administrador> Get-ADFinegrainedPasswordPolicy -Filter * | Select Name, Precedence, AppliesTo

Name           Precedence AppliesTo
----          -----
FGPP_Administradores 10 {CN=G_Administradores,OU=Grupos,DC=lab,DC=local}
FGPP_Contadores      20 {CN=G_Contadores,OU=Grupos,DC=lab,DC=local}
FGPP_Empleados        30 {}

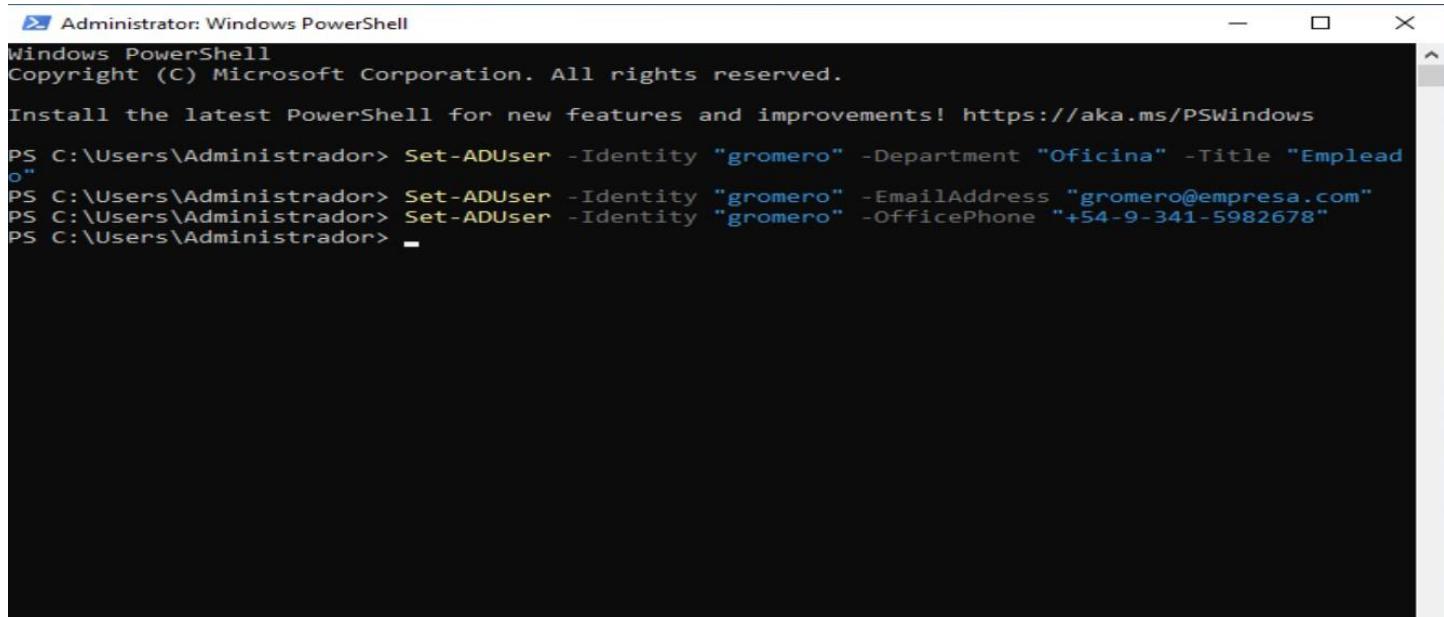
PS C:\Users\Administrador> Get-ADFinegrainedPasswordPolicy -Identity "FGPP_Administradores"

AppliesTo          : {CN=G_Administradores,OU=Grupos,DC=lab,DC=local}
ComplexityEnabled  : True
DistinguishedName : CN=FGPP_Administradores,CN=Password Settings Container,CN=System,DC=lab,DC=local
LockoutDuration    : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold   : 3
MaxPasswordAge     : 60.00:00:00
MinPasswordAge     : 1.00:00:00
MinPasswordLength  : 14
Name               : FGPP_Administradores
ObjectClass        : msDS-PasswordSettings
ObjectGUID         : 2f125afc-c4f0-4a82-805d-6d6b2c7974aa
PasswordHistoryCount : 24
Precedence         : 10
ReversibleEncryptionEnabled : False
```

## 7. Gestión del ciclo de vida de usuarios

Se realizaron tareas clave de administración:

Altas y modificaciones, creación de nuevas cuentas y edición de atributos

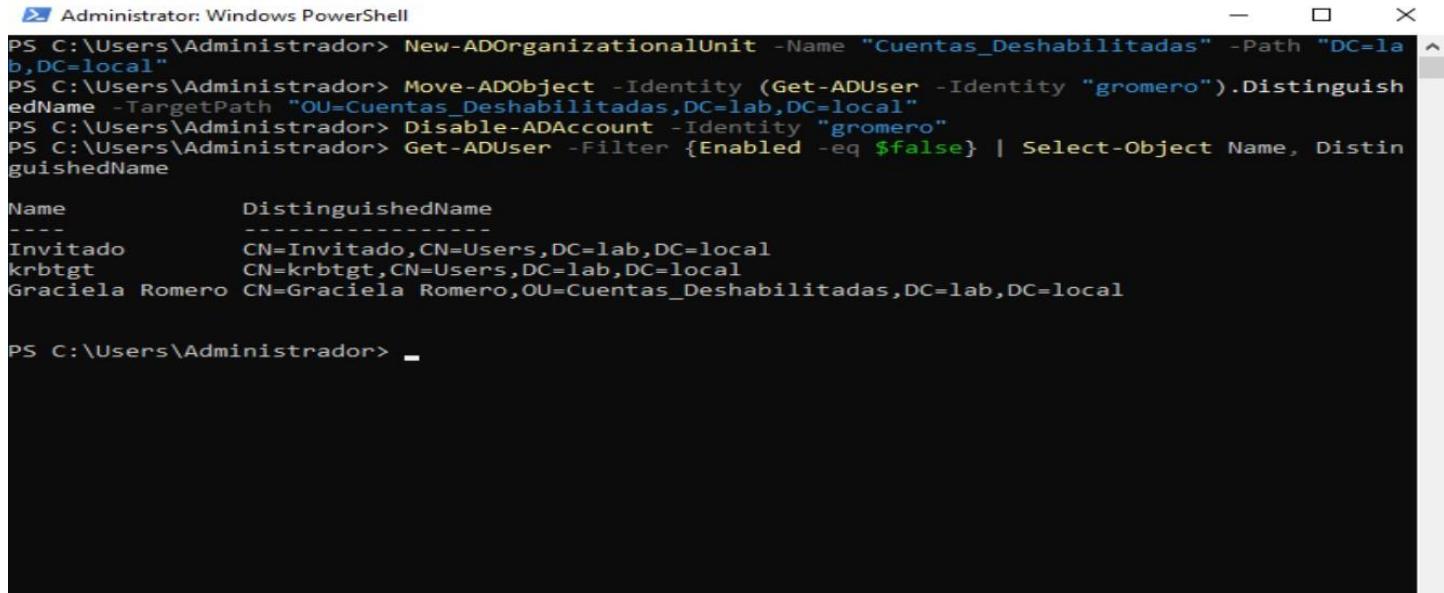


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrador> Set-ADUser -Identity "gromero" -Department "Oficina" -Title "Empleado"
PS C:\Users\Administrador> Set-ADUser -Identity "gromero" -EmailAddress "gromero@empresa.com"
PS C:\Users\Administrador> Set-ADUser -Identity "gromero" -OfficePhone "+54-9-341-5982678"
PS C:\Users\Administrador>
```

Bajas, deshabilitación y traslado a OU Cuentas Deshabilitadas

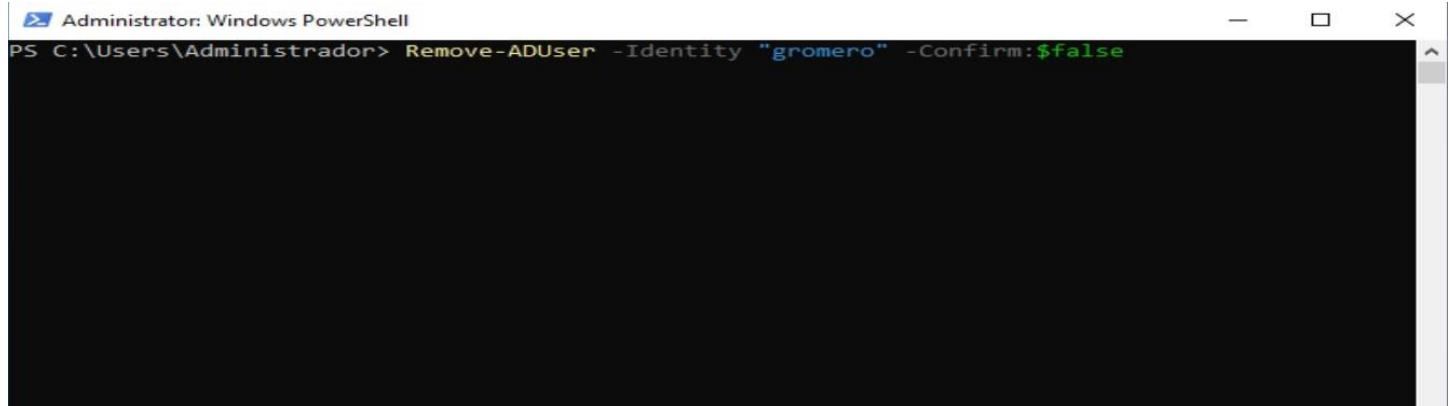


```
Administrator: Windows PowerShell
PS C:\Users\Administrador> New-ADOrganizationalUnit -Name "Cuentas_Deshabilitadas" -Path "DC=lab,DC=local"
PS C:\Users\Administrador> Move-ADObject -Identity (Get-ADUser -Identity "gromero").DistinguishedName -TargetPath "OU=Cuentas_Deshabilitadas,DC=lab,DC=local"
PS C:\Users\Administrador> Disable-ADAAccount -Identity "gromero"
PS C:\Users\Administrador> Get-ADUser -Filter {Enabled -eq $false} | Select-Object Name, DistinguishedName

Name          DistinguishedName
----          -----
Invitado      CN=Invitado,CN=Users,DC=lab,DC=local
krbtgt        CN=krbtgt,CN=Users,DC=lab,DC=local
Graciela Romero CN=Graciela Romero,OU=Cuentas_Deshabilitadas,DC=lab,DC=local

PS C:\Users\Administrador>
```

## Eliminación, remoción definitiva del objeto

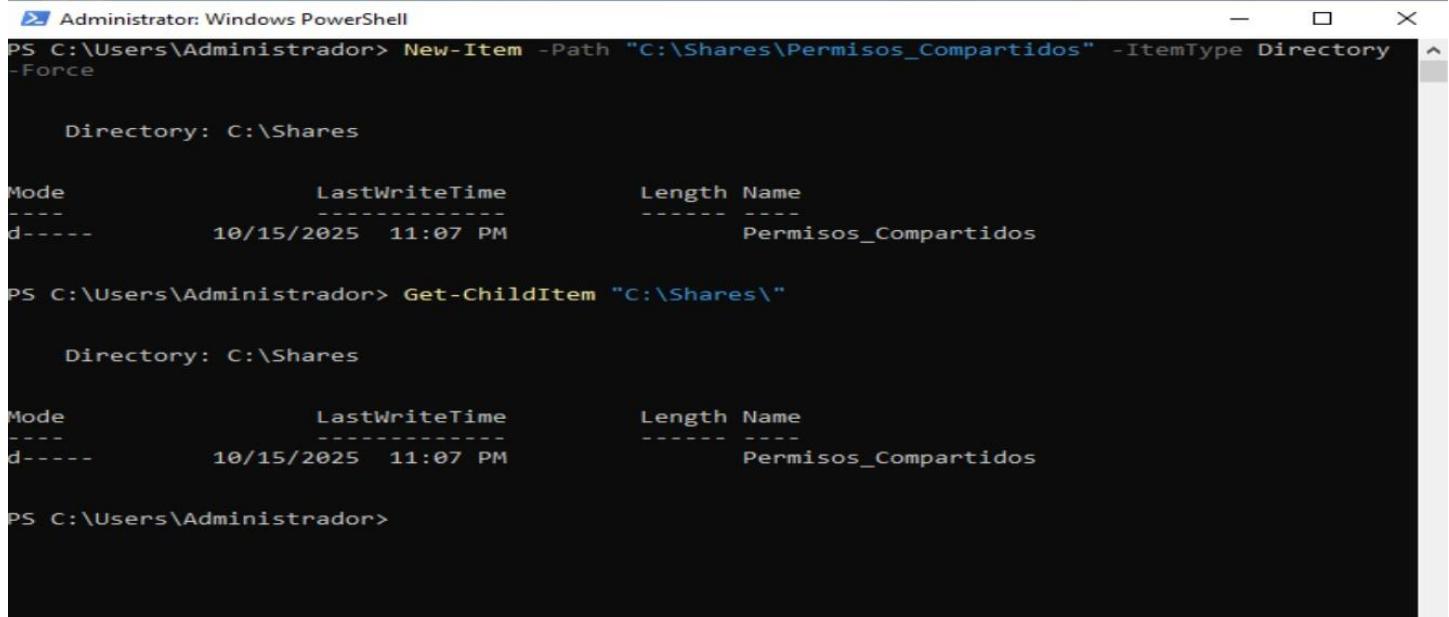


```
Administrator: Windows PowerShell
PS C:\Users\Administrador> Remove-ADUser -Identity "gromero" -Confirm:$false
```

## 8. Permisos sobre recursos compartidos

Se creó la carpeta **Permisos\_Compartidos** y se aplicaron permisos combinados:

- o NTFS: acceso solo para **G\_Employees**
- o Permisos de recurso compartido: alineados con la misma política



```
Administrator: Windows PowerShell
PS C:\Users\Administrador> New-Item -Path "C:\Shares\Permisos_Compartidos" -ItemType Directory -Force

Directory: C:\Shares

Mode                LastWriteTime         Length Name
----                -----          ----  -
d-----        10/15/2025  11:07 PM           0  Permisos_Compartidos

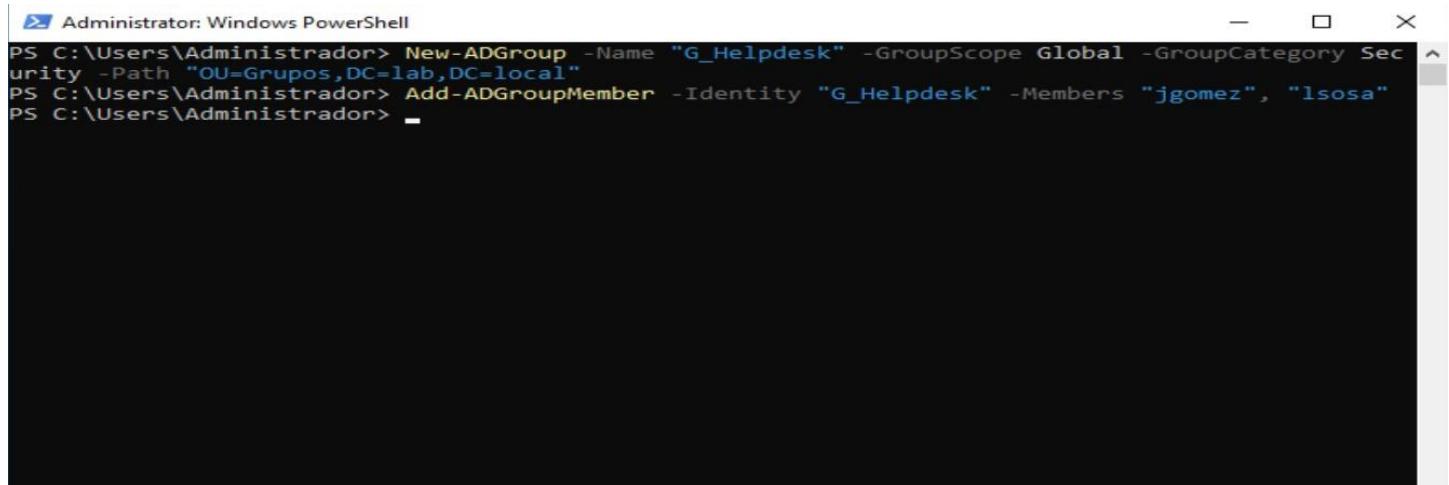
PS C:\Users\Administrador> Get-ChildItem "C:\Shares\"

Directory: C:\Shares

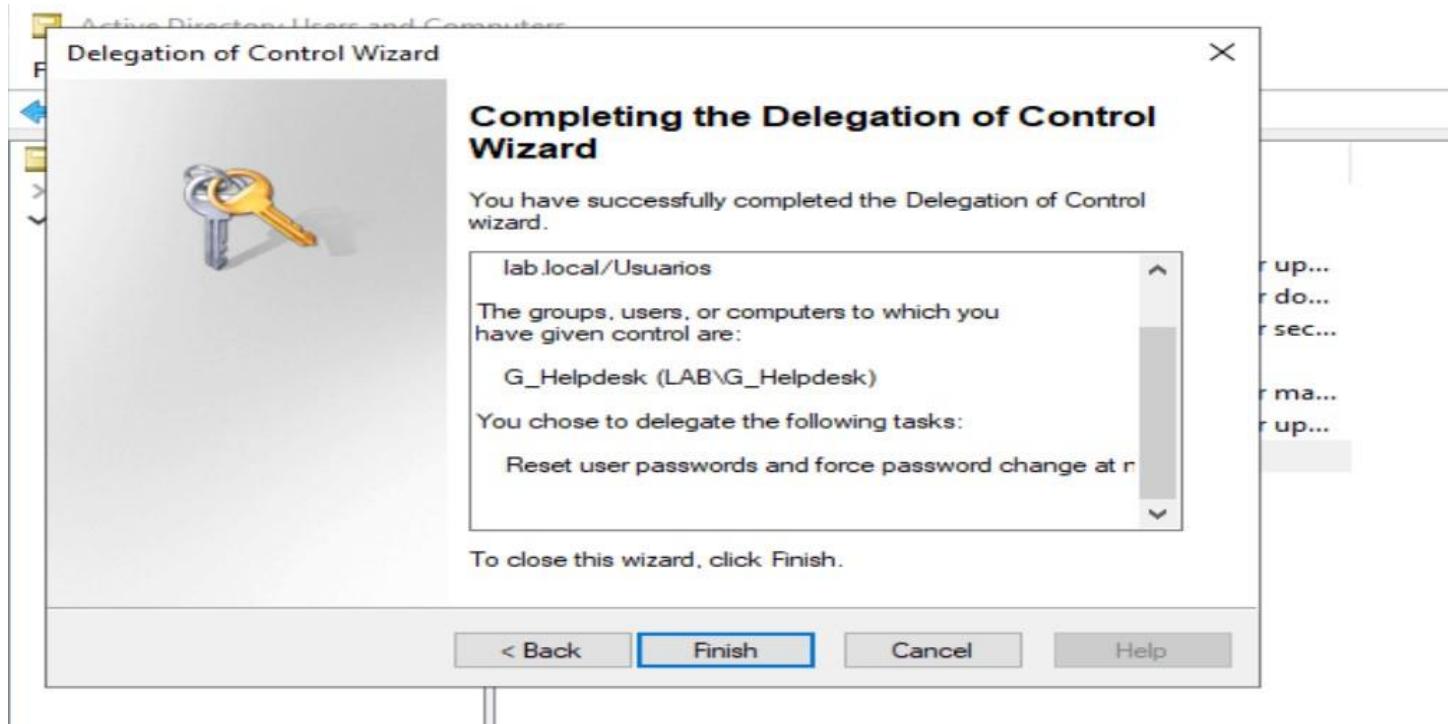
Mode                LastWriteTime         Length Name
----                -----          ----  -
d-----        10/15/2025  11:07 PM           0  Permisos_Compartidos

PS C:\Users\Administrador>
```

Además, se ejecutó delegación de control para el grupo G\_Helpdesk, específicamente la tarea de restablecer contraseñas



```
Administrator: Windows PowerShell
PS C:\Users\Administrador> New-ADGroup -Name "G_Helpdesk" -GroupScope Global -GroupCategory Security -Path "OU=Grupos,DC=lab,DC=local"
PS C:\Users\Administrador> Add-ADGroupMember -Identity "G_Helpdesk" -Members "jgomez", "lsosa"
PS C:\Users\Administrador>
```



## 9. Resumen final

El laboratorio permitió comprender de forma práctica la arquitectura base de Active Directory y la relación entre:

- Estructura de OUs
- Políticas GPO/FGPP
- Permisos NTFS y delegación
- Administración de identidades con GUI y PowerShell