

# Laboratorio de Active Directory – Instalación, Configuración y Gestión Básica

## Introducción

El presente reporte documenta la implementación de un laboratorio práctico centrado en la creación y administración de un dominio de red. Para ello, se desplegó una instancia de Windows Server con el servicio de directorio Active Directory. El objetivo principal consistió en dominar las tareas fundamentales de administración de sistemas, entre las que se incluyen la creación y gestión de usuarios y grupos de seguridad, la aplicación y verificación de políticas de contraseñas, y la ejecución de operaciones cíclicas de administración como altas, bajas y asignación de permisos. La metodología de trabajo se sustentó en un procedimiento paso a paso, debidamente registrado y respaldado con capturas de pantalla que sirven como evidencia del correcto desarrollo de cada etapa del proceso.

## Preparación del entorno

El entorno de pruebas se implementó utilizando el software de virtualización Oracle VM VirtualBox. Para simular una red corporativa básica, se desplegaron dos máquinas virtuales con los siguientes roles:

1. Servidor (Windows Server 2022): Configurado para actuar como Controlador de Dominio (Domain Controller) de la red.
2. Estación de Trabajo (Windows 10): Utilizada como cliente de red para validar la integración al dominio, probar inicios de sesión de usuarios del directorio y verificar la aplicación de permisos y políticas.

Ambos sistemas se interconectaron mediante una red interna virtual dentro de VirtualBox. Se estableció un esquema de direccionamiento IP estático dentro del rango 192.168.100.x/24 para garantizar la comunicación y resolución de nombres. Como parte de la configuración de red, se asignó manualmente una dirección IP al servidor y se designó al mismo servidor como servidor DNS preferente para la resolución de nombres del dominio. Adicionalmente, se procedió a cambiar el nombre de host del servidor para alinearlos con su rol dentro del dominio.

## Evidencia 1: Interfaz de red configurada con dirección IPv4 estática 192.168.100.10/24.

```
Administrador: Windows PowerShell

PS C:\Users\Administrador> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.100.10 -PrefixLength 24

IPAddress      : 192.168.100.10
InterfaceIndex  : 5
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin     : Manual
AddressState    : Tentative
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : 192.168.100.10
InterfaceIndex  : 5
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin     : Manual
AddressState    : Invalid
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : PersistentStore
```

## Evidencia 2: Interfaz de red configurada con dirección IPv4 estática 192.168.100.20/24.

```
Administrador: Windows PowerShell

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

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.100.20 -PrefixLength 24

IPAddress      : 192.168.100.20
InterfaceIndex  : 6
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin     : Manual
AddressState    : Tentative
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : ActiveStore

IPAddress      : 192.168.100.20
InterfaceIndex  : 6
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin     : Manual
AddressState    : Invalid
ValidLifetime   : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource    : False
PolicyStore     : PersistentStore

PS C:\Windows\system32>
```

### Evidencia 3: Verificación de conectividad de red mediante comando ping.

```
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<1m TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1m 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<1m TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo<1m 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> _
```

### Evidencia 3: Prueba de conectividad exitosa entre servidor y estación de trabajo.

Administrador: 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<1m TTL=128
Respuesta desde 192.168.100.20: bytes=32 tiempo<1m 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<1m TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.10: bytes=32 tiempo<1m 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> _
```



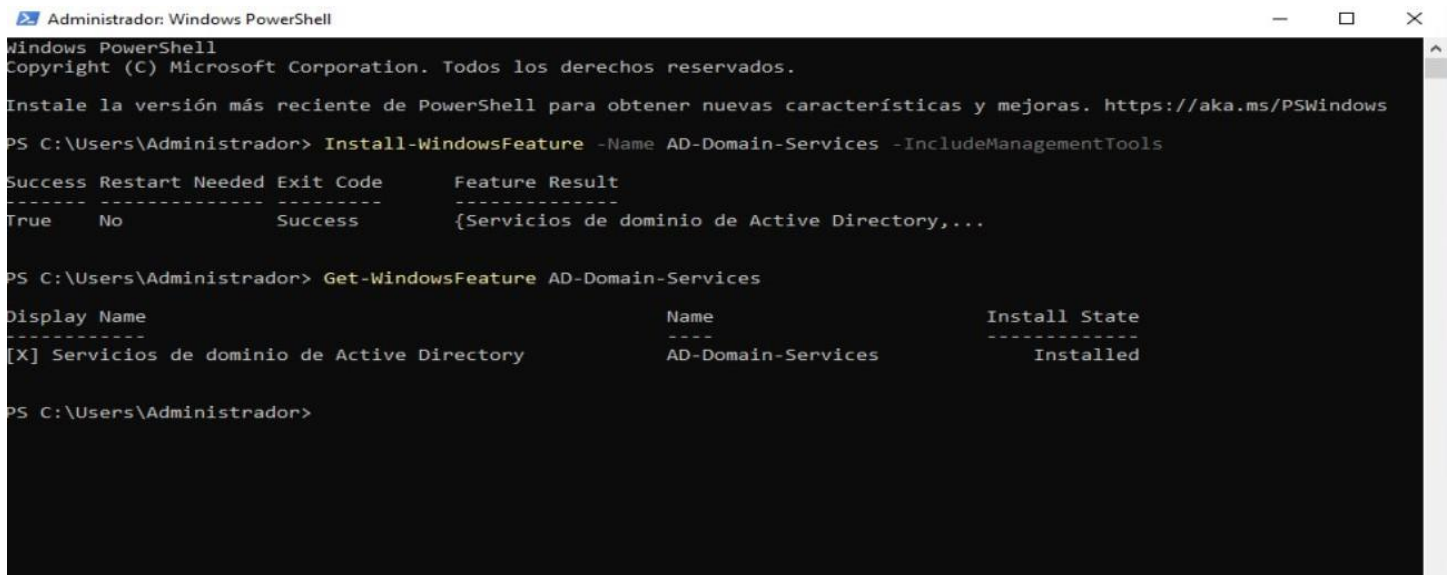
## Instalación del rol de Active Directory

En el servidor con Windows Server 2022, se procedió a instalar el rol de Active Directory Domain Services (AD DS) utilizando la herramienta administrativa Server Manager.

Una vez completada la instalación del rol, se inició el proceso de promoción del servidor a Controlador de Dominio. En este paso, se creó y se desplegó un nuevo bosque con el nombre de dominio lab.local.

Tras un reinicio requerido por el sistema, el servidor inició sus funciones como Domain Controller (DC) principal, con los servicios de Active Directory y DNS operativos y configurados para el dominio.

### Evidencia 4: Configuración del servidor: Agregar rol AD DS.



```
Administrador: 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

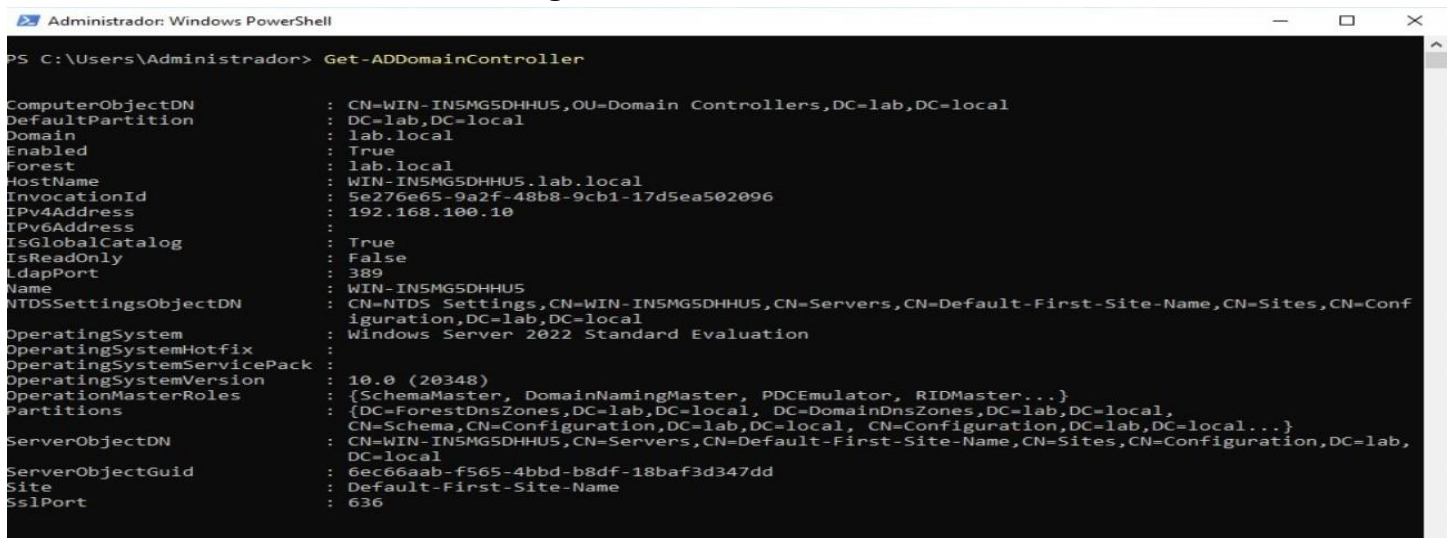
Success Restart Needed Exit Code      Feature Result
-----
True      No              Success      {Servicios de dominio de Active Directory,...

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>
```

### Evidencia 5: Verificación de la configuración del controlador de dominio.



```
Administrador: Windows PowerShell

PS C:\Users\Administrador> Get-ADDomainController

ComputerObjectDN      : CN=WIN-IN5MG5DHHU5,OU=Domain Controllers,DC=lab,DC=local
DefaultPartition      : DC=lab,DC=local
Domain                : lab.local
Enabled               : True
Forest                : lab.local
HostName              : WIN-IN5MG5DHHU5.lab.local
InvocationId          : 5e276e65-9a2f-48b8-9cb1-17d5ea502096
IPv4Address           : 192.168.100.10
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : WIN-IN5MG5DHHU5
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=WIN-IN5MG5DHHU5,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Conf
iguration,DC=lab,DC=local
OperatingSystem        : Windows Server 2022 Standard Evaluation
OperatingSystemHotfix :
OperatingSystemServicePack :
OperatingSystemVersion : 10.0 (20348)
OperationMasterRoles   : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions             : {DC=ForestDnsZones,DC=lab,DC=local, DC=DomainDnsZones,DC=lab,DC=local,
CN=Schema,CN=Configuration,DC=lab,DC=local, CN=Configuration,DC=lab,DC=local...}
ServerObjectDN         : CN=WIN-IN5MG5DHHU5,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,
DC=local
ServerObjectGuid       : 6ec66aab-f565-4bbd-b8df-18baf3d347dd
Site                   : Default-First-Site-Name
SslPort               : 636
```

## Evidencia 6: Verificación de las propiedades del dominio lab.local.

```
Administrador: Windows PowerShell

PS C:\Users\Administrador> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=lab,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=lab,DC=local
DistinguishedName       : DC=lab,DC=local
DNSRoot                 : lab.local
DomainControllersContainer : OU=Domain Controllers,DC=lab,DC=local
DomainMode              : Windows2016Domain
DomainSID                : S-1-5-21-3115137076-146667767-1695127003
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab,DC=local
Forest                  : lab.local
InfrastructureMaster     : WIN-IN5MG5DHHU5.lab.local
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab,DC=local}
LostAndFoundContainer    : CN=LostAndFound,DC=lab,DC=local
ManagedBy               :
Name                     : lab
NetBIOSName              : LAB
ObjectClass              : domainDNS
ObjectGUID               : 9d5c9688-6ba5-4047-a5b4-a87207b93094
ParentDomain              :
PDCEmulator              : WIN-IN5MG5DHHU5.lab.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer          : CN=NTDS Quotas,DC=lab,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers  : {WIN-IN5MG5DHHU5.lab.local}
RIDMaster                : WIN-IN5MG5DHHU5.lab.local
SubordinateReferences     : {DC=ForestDnsZones,DC=lab,DC=local, DC=DomainDnsZones,DC=lab,DC=local,
CN=Configuration,DC=lab,DC=local}
SystemsContainer         : CN=System,DC=lab,DC=local
UsersContainer           : CN=Users,DC=lab,DC=local
```

## Evidencia 7: Verificación del servicio DNS instalado y operativo.

```
PS C:\Users\Administrador> Get-Service DNS

Status      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>
```

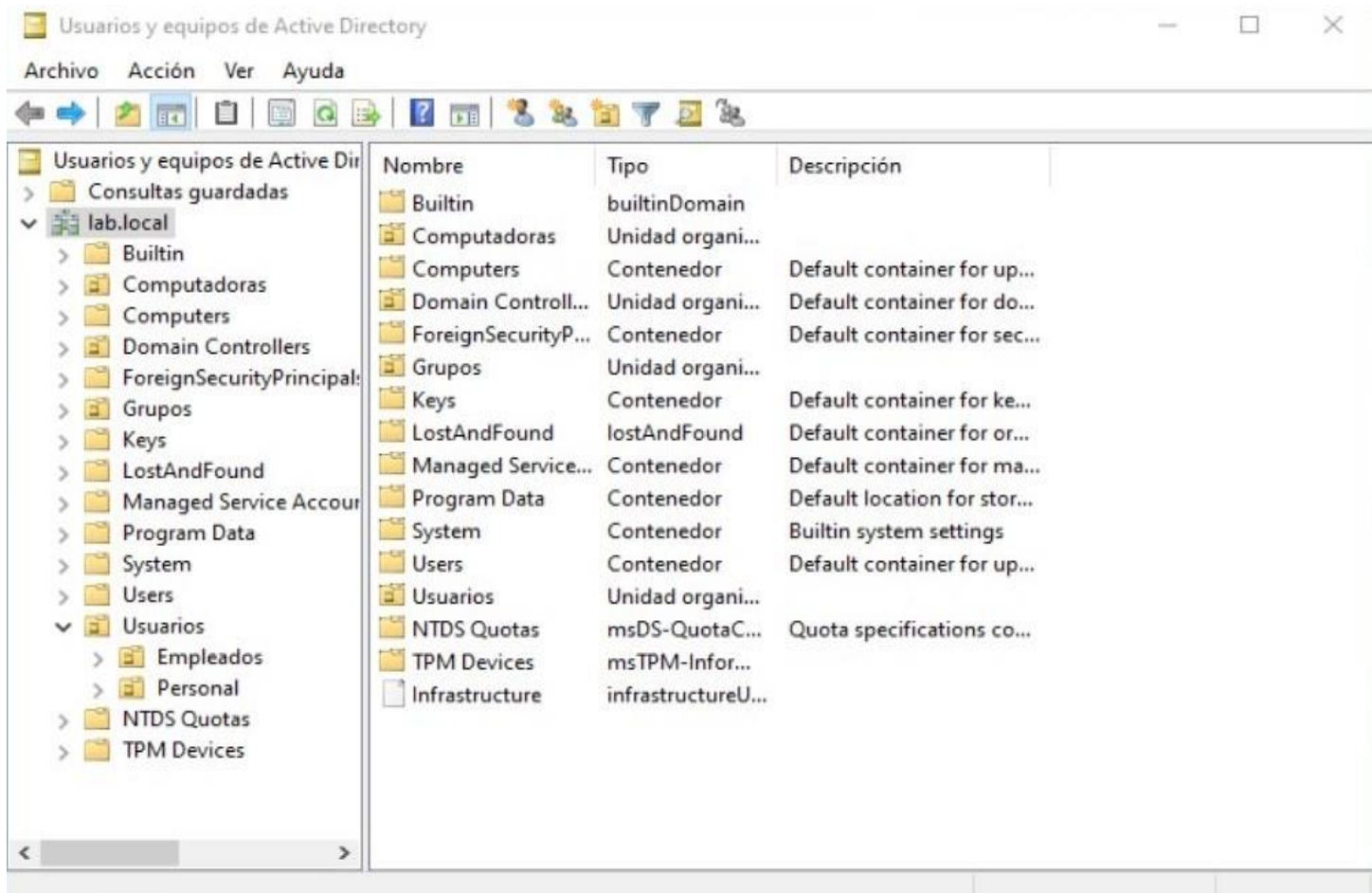
## Estructura del dominio

Para garantizar una administración ordenada y escalable de los objetos del directorio, se diseñó e implementó una estructura de Unidades Organizativas (OU) dentro del dominio lab.local. La jerarquía creada fue la siguiente:

- OU "Usuarios": Contenedor principal para todas las cuentas de usuario.
  - Sub-OU "Empleados": Destinada a los usuarios estándar de la organización.
  - Sub-OU "Personal": Designada para cuentas de personal administrativo o técnico.
- OU "Grupos": Contenedor centralizado para los grupos de seguridad y distribución.
- OU "Computadoras": Unidad organizativa para gestionar las estaciones de trabajo unidas al dominio.

Esta segmentación permite una administración delegada y aplicada de políticas, facilitando la aplicación futura de Políticas de Grupo (GPOs) específicas a cada categoría de objetos, así como una gestión más eficiente de permisos y configuraciones.

### Evidencia 8: Creación de la estructura de Unidades Organizativas (OU).



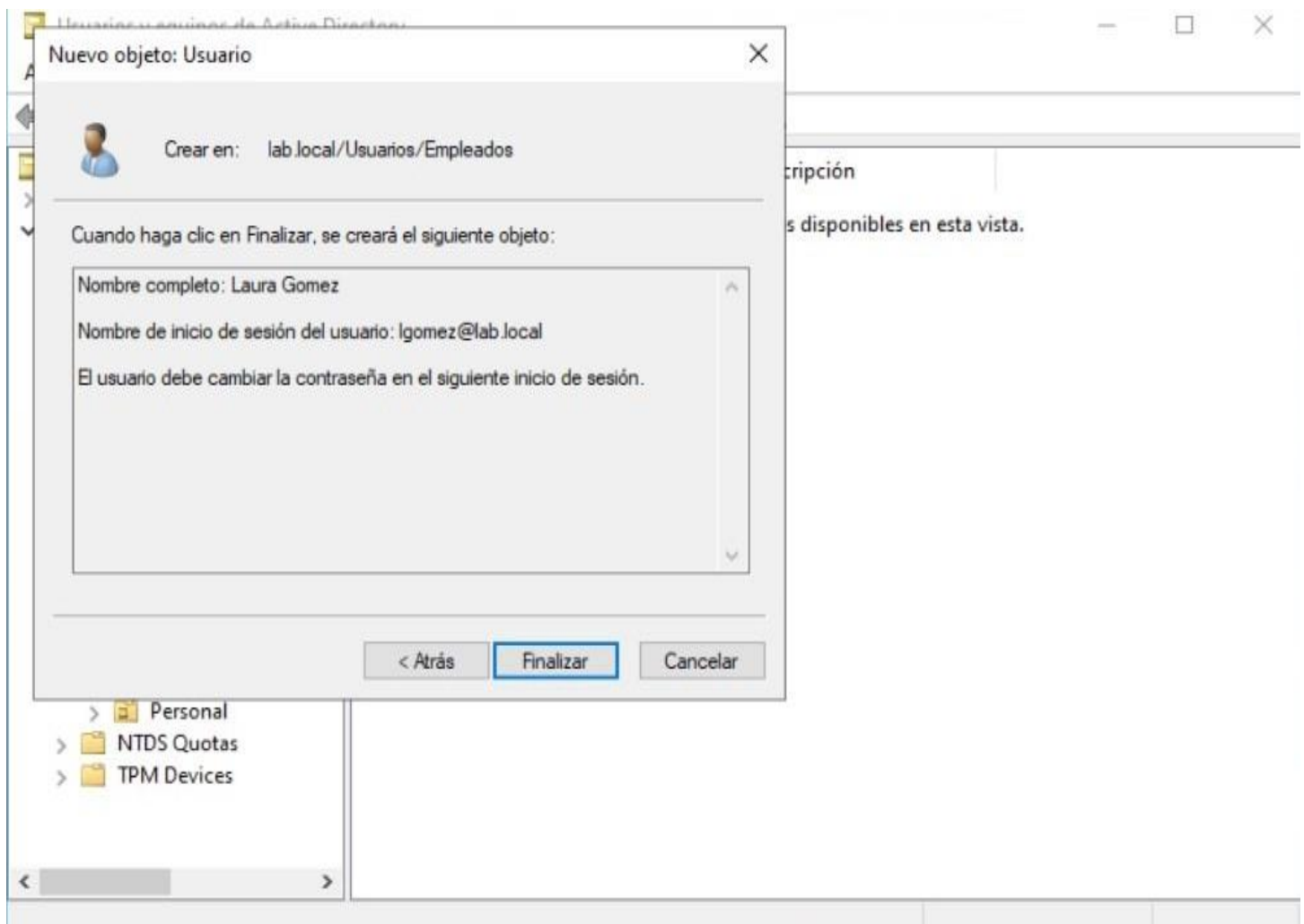
## Creación de usuarios y grupos

Posteriormente, se procedió con la creación de cuentas de usuario dentro de la Unidad Organizativa "Empleados". Como ejemplo, se generaron las cuentas para Luciano Sosa y Julieta Gomez.

Durante el proceso de creación, se configuraron contraseñas iniciales que cumplieran con la política de contraseñas del dominio. Adicionalmente, se habilitó la opción "El usuario debe cambiar la contraseña en el siguiente inicio de sesión", para garantizar la seguridad y la confidencialidad inicial de las credenciales.

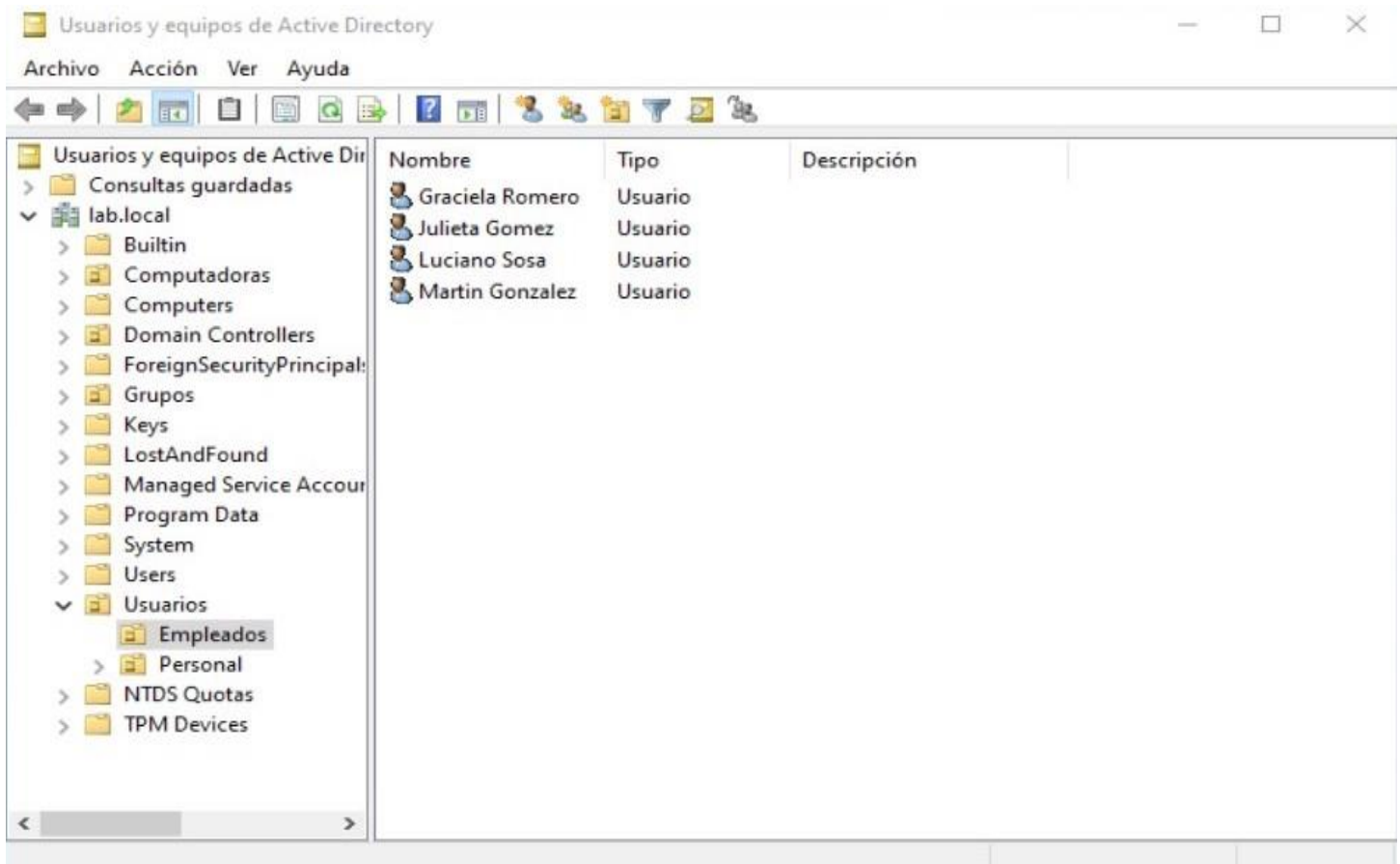
Paralelamente, se creó un grupo de seguridad denominado G\_Empleados dentro de la OU correspondiente. Tanto Luciano Sosa como Julieta Gomez fueron agregados como miembros de este grupo. Esta estrategia de agrupamiento permite una administración eficiente de permisos y accesos a recursos, los cuales podrán ser asignados al grupo en lugar de a usuarios individuales, facilitando la gestión posterior.

### Evidencia 9: Configuración de cuenta de usuario en la OU Empleados.

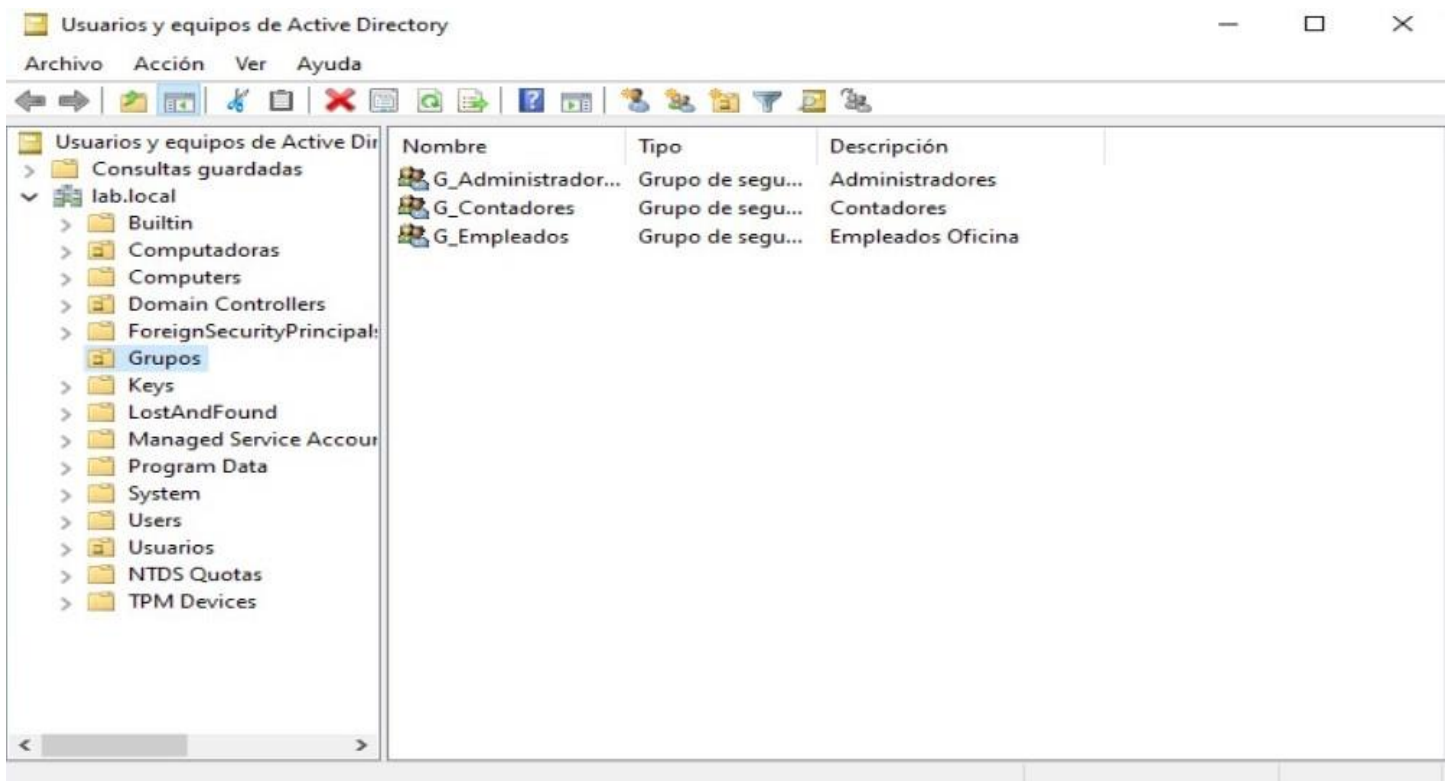




## Evidencia 10: Vista de usuarios registrados en la Unidad Organizativa Empleados.



## Evidencia 11: Creación de grupos de seguridad en Active Directory.





## Evidencia 12: Ejecución de comandos New-ADGroup para crear grupos globales.

```
PS C:\Users\Administrador> New-ADGroup -Name "G_Empleados" -SamAccountName "G_Empleados" -GroupScope Global -GroupCategory Security -Path "OU=Grupos,DC=lab,DC=local" -Description "Empleados Oficina"
PS C:\Users\Administrador> New-ADGroup -Name "G_Administradores" -SamAccountName "G_Administradores" -GroupScope Global -GroupCategory Security -Path "OU=Grupos,DC=lab,DC=local" -Description "Administradores"
PS C:\Users\Administrador> New-ADGroup -Name "G_Contadores" -SamAccountName "G_Contadores" -GroupScope Global -GroupCategory Security -Path "OU=Grupos,DC=lab,DC=local" -Description "Contadores"
PS C:\Users\Administrador>
```

## Políticas de contraseñas

Se procedió a configurar la política de contraseñas del dominio mediante la Group Policy Management Console (GPMC), modificando la Default Domain Policy. Los parámetros de seguridad establecidos fueron los siguientes:

- Longitud mínima de contraseña: 10 caracteres.
- Complejidad de contraseña: Habilitada (requiere mayúsculas, minúsculas, números y símbolos).
- Umbral de bloqueo de cuenta: 5 intentos fallidos de inicio de sesión.

Esta configuración implementa un esquema de seguridad robusto, simulando los estándares comúnmente utilizados en entornos corporativos para proteger las cuentas de usuario contra accesos no autorizados y ataques por fuerza bruta.

### Evidencia 13: Verificación de políticas de contraseñas granulares (FGPP) y su precedencia.

```
Administrador: Windows PowerShell

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
```

### Evidencia 14: Configuración específica de FGPP para cada grupo de seguridad.

```
Administrador: Windows PowerShell

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
```

## Evidencia 15: Asociación de políticas FGPP\_Empleados y FGPP\_Contadores con sus grupos.

```
Administrador: Windows PowerShell

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

DistinguishedName : CN=G_Empleados,OU=Grupos,DC=lab,DC=local
Name              : G_Empleados
ObjectClass       : group
ObjectGUID        : 0901fc5e-bb94-47bb-b789-3b8466c728ab
SamAccountName    : G_Empleados
SID               : S-1-5-21-3115137076-146667767-1695127003-1117

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

DistinguishedName : CN=G_Contadores,OU=Grupos,DC=lab,DC=local
Name              : G_Contadores
ObjectClass       : group
ObjectGUID        : 306b4124-eeed-4478-99ef-6947c65f21d7
SamAccountName    : G_Contadores
SID               : S-1-5-21-3115137076-146667767-1695127003-1119
```

## Evidencia 16: Asignación de FGPP\_Administradores al grupo correspondiente.

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

DistinguishedName : CN=G_Administradores,OU=Grupos,DC=lab,DC=local
Name              : G_Administradores
ObjectClass       : group
ObjectGUID        : 5a872277-4ff5-4571-a1e4-ef6206c26bbe
SamAccountName    : G_Administradores
SID               : S-1-5-21-3115137076-146667767-1695127003-1118
```

## Gestión de usuarios (altas, bajas, permisos)

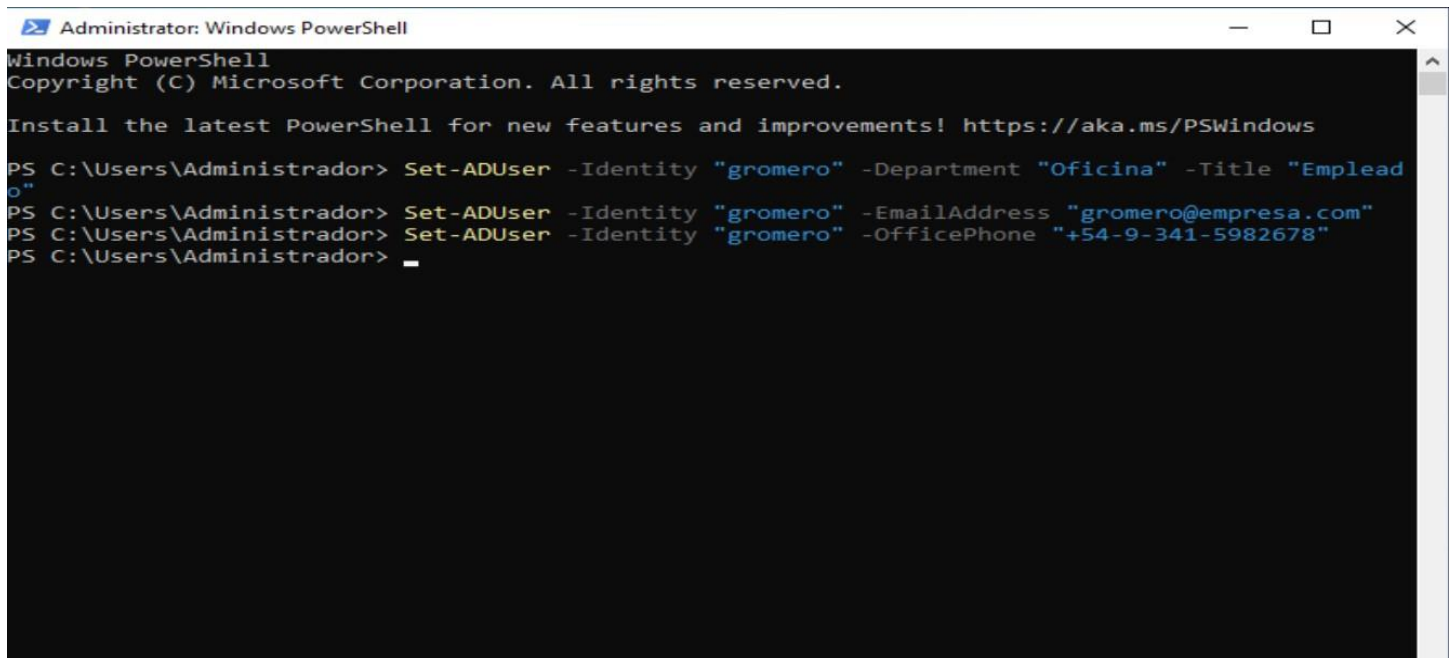
Se realizaron operaciones administrativas fundamentales para simular el ciclo de vida completo de una cuenta de usuario:

- Alta: Creación de nuevas cuentas de usuario mediante la consola de Active Directory Users and Computers.
- Modificación: Actualización de atributos de usuario, específicamente el cambio de departamento mediante las propiedades de la cuenta.

- Baja: Deshabilitación de cuentas y su posterior traslado a la Unidad Organizativa "Cuentas Deshabilitadas", manteniendo el historial de objetos mientras se revoca el acceso.

Este flujo de trabajo representa las prácticas estándar de administración de identidades en un entorno organizacional, garantizando el control adecuado del acceso a los recursos durante todas las fases del ciclo de vida del usuario.

### Evidencia 17: Modificación de atributos de usuario mediante PowerShell.

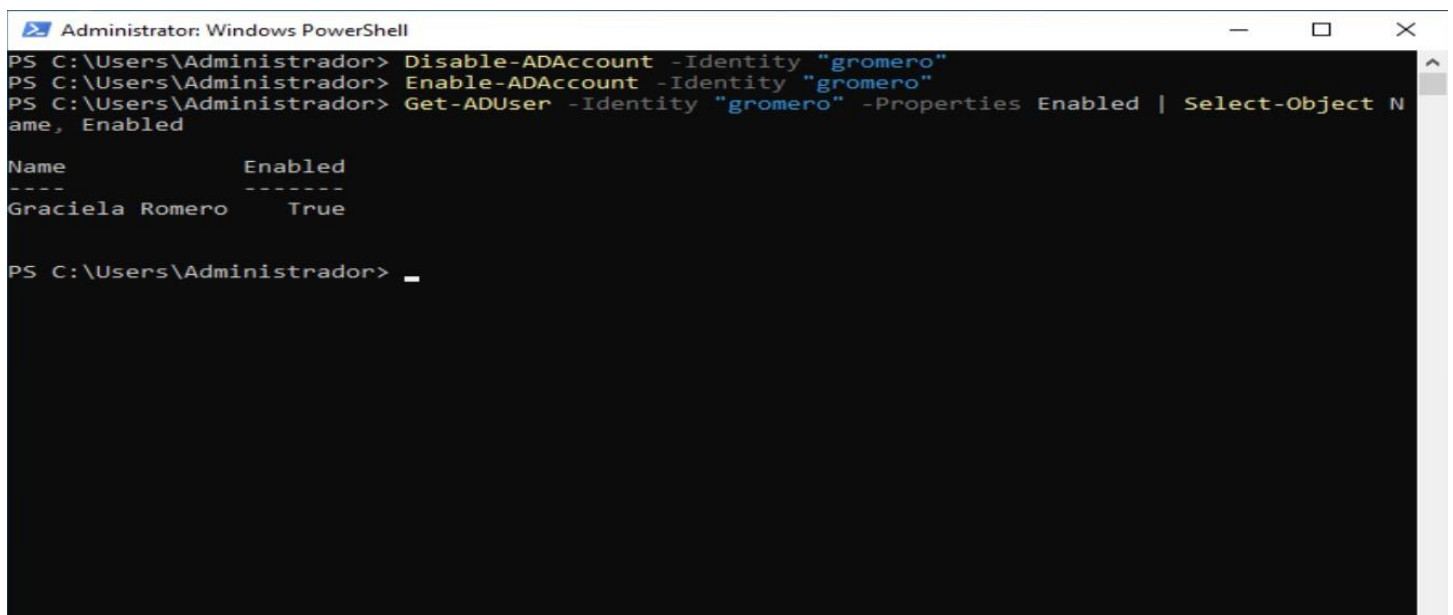


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\Administrador> Set-ADUser -Identity "gromero" -Department "Oficina" -Title "Emplead
o"
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> _
```

### Evidencia 18: Operación de deshabilitación, habilitación y verificación de estado del usuario.



```
Administrator: Windows PowerShell
PS C:\Users\Administrador> Disable-ADAccount -Identity "gromero"
PS C:\Users\Administrador> Enable-ADAccount -Identity "gromero"
PS C:\Users\Administrador> Get-ADUser -Identity "gromero" -Properties Enabled | Select-Object N
ame, Enabled

Name           Enabled
----
Graciela Romero True

PS C:\Users\Administrador> _
```



## Evidencia 19: Creación de OU para cuentas deshabilitadas y reubicación de usuario (baja).

```
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-ADAccount -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> _
```

## Evidencia 20: Eliminación permanente de cuenta de usuario del directorio activo.

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

## Evidencia 21: Consulta de propiedades completas de usuario mediante PowerShell.

```
Administrator: Windows PowerShell
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> Get-ADUser -Identity "gromero" -Properties *

AccountExpirationDate      :
accountExpires             : 9223372036854775807
AccountLockoutTime         :
AccountNotDelegated        : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy       : {}
AuthenticationPolicySilo   : {}
BadLogonCount              : 0
badPasswordTime            : 0
badPwdCount                : 0
CannotChangePassword       : False
CanonicalName              : lab.local/Cuentas_Deshabilitadas/Graciela Romero
Certificates               : {}
City                       :
CN                         : Graciela Romero
codePage                   : 0
Company                    :
CompoundIdentitySupported   : {}
Country                    :
countryCode                : 0
```

## Evidencia 22: Búsqueda y filtrado de usuarios por atributo de departamento.

```
Administrator: Windows PowerShell

uSNChanged      : 65574
uSNCreated      : 16460
whenChanged     : 10/15/2025 10:28:52 PM
whenCreated     : 10/12/2025 9:28:33 AM

PS C:\Users\Administrador> Get-ADUser -Filter "Department -eq 'Oficina'" | Select-Object Name, Title

Name          Title
----          -
Graciela Romero
```

## Permisos sobre recursos compartidos

Para demostrar la integración entre los servicios de directorio y el sistema de archivos, se procedió a crear una carpeta compartida denominada "Permisos\_Compartidos" en el servidor. Sobre este recurso, se implementó un esquema de permisos combinados que articula la gestión de identidades de Active Directory con los permisos NTFS del sistema operativo Windows.

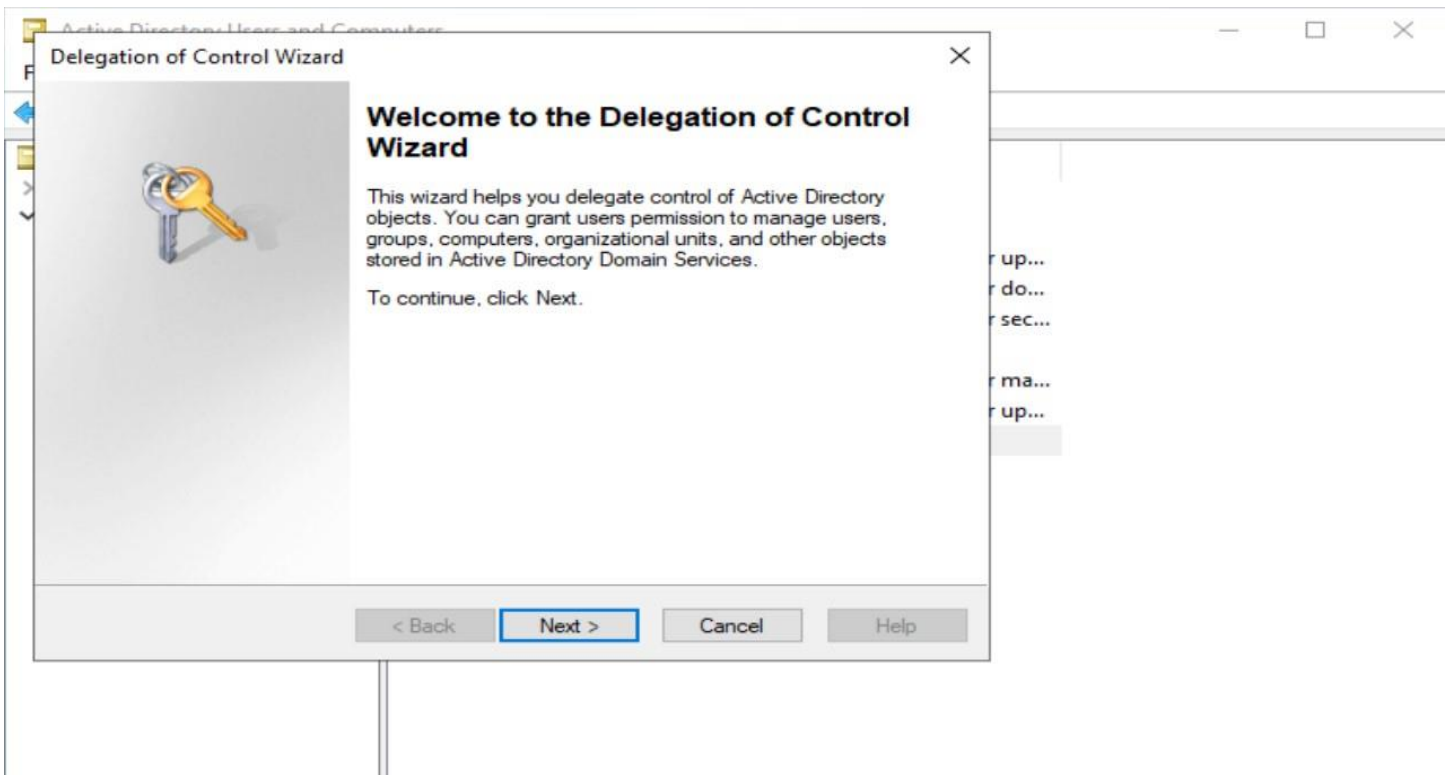
Específicamente, se configuraron los permisos NTFS de la carpeta para otorgar acceso de lectura y escritura exclusivamente al grupo de seguridad "G\_Empleados". De este modo, solo los usuarios miembros de dicho grupo pueden acceder al recurso, validándose sus credenciales contra el dominio. Esta práctica simula un escenario real donde el acceso a los recursos de red se gestiona de forma centralizada mediante grupos de seguridad, demostrando la aplicación efectiva de los principios de seguridad por grupos y mínimo privilegio.

## Evidencia 23: Creación del grupo de seguridad "G\_Helpdesk" y asignación de miembros.

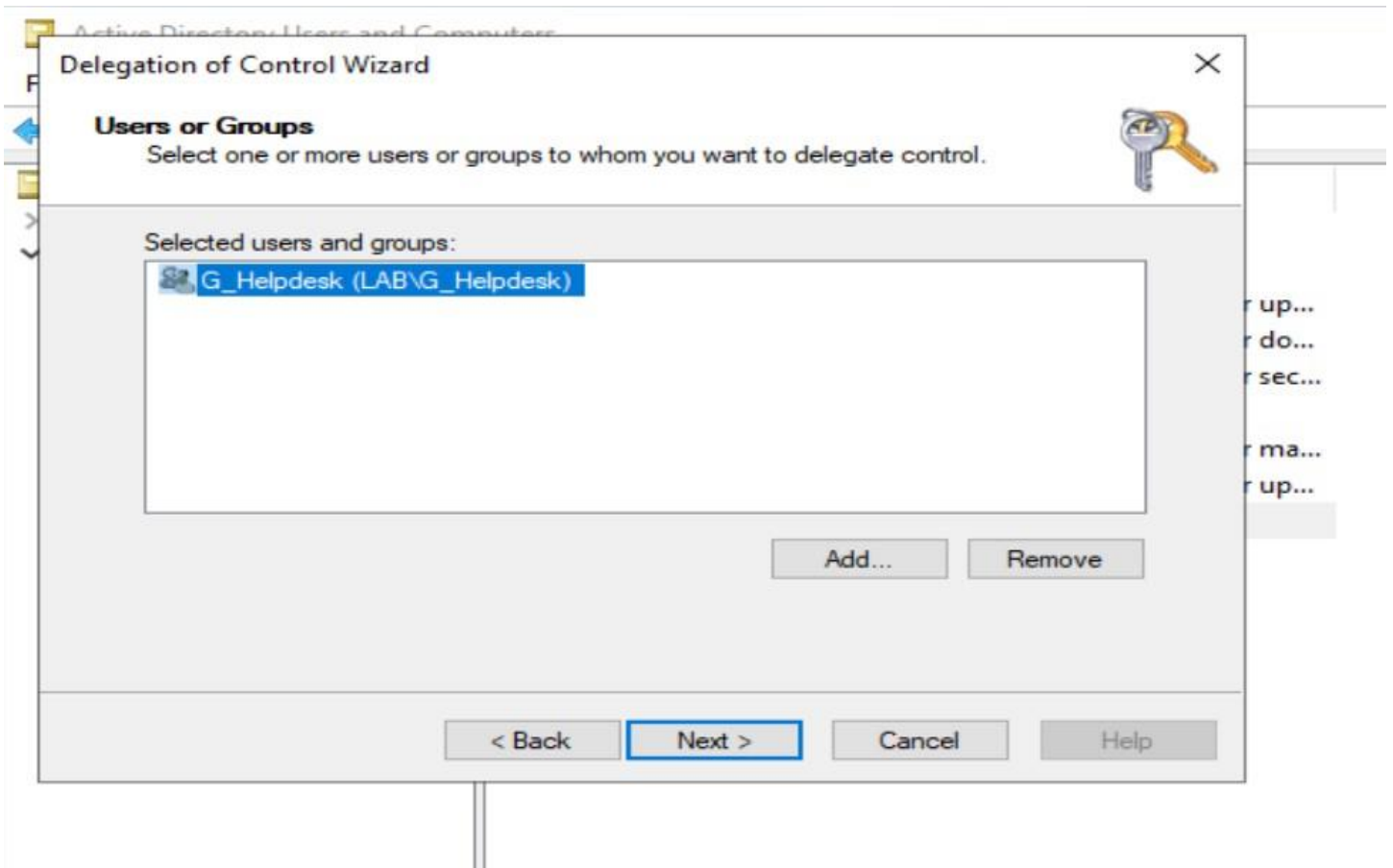
```
Administrator: Windows PowerShell

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>
```

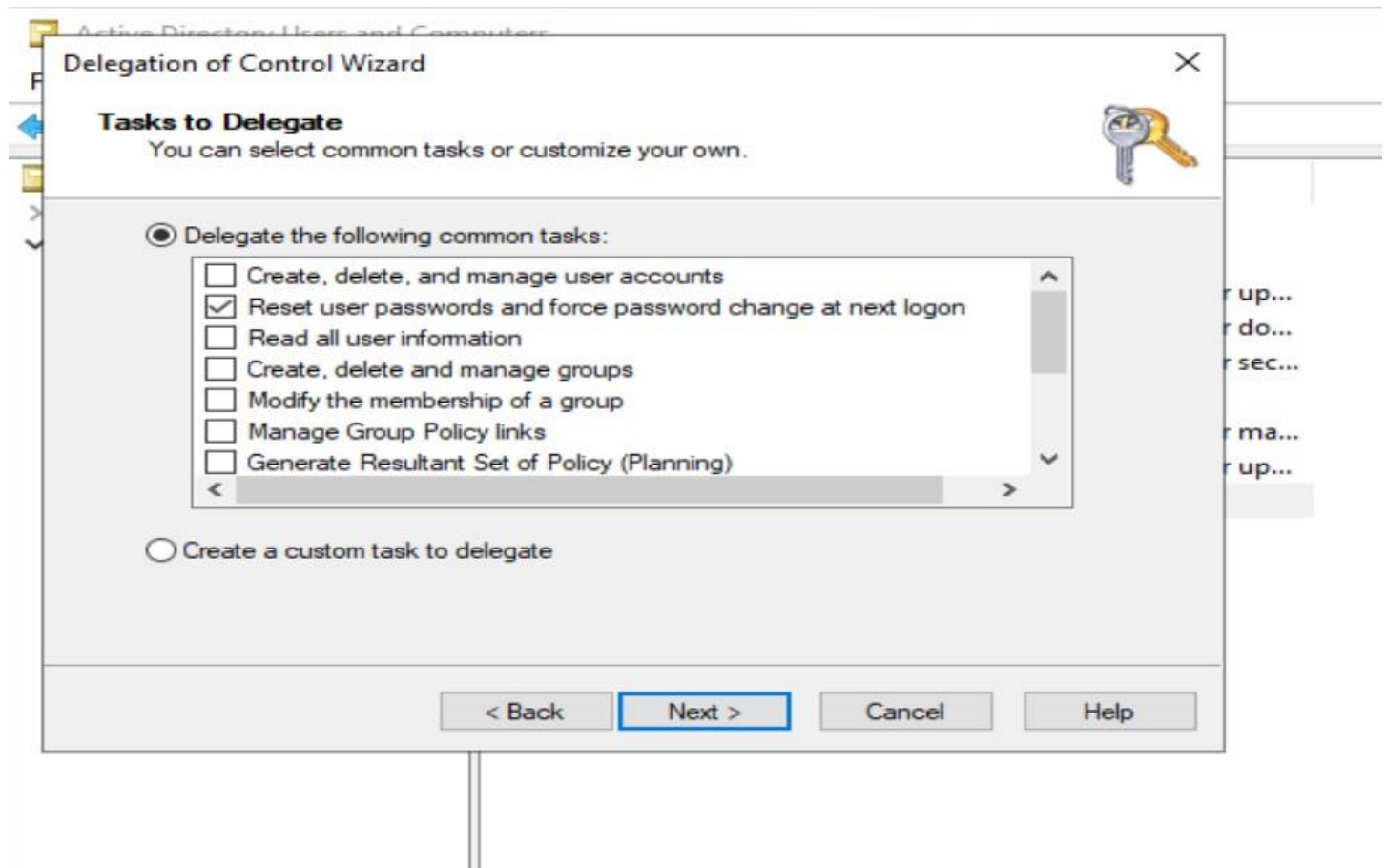
## Evidencia 24: Inicio del Asistente para Delegación de Control en Active Directory.



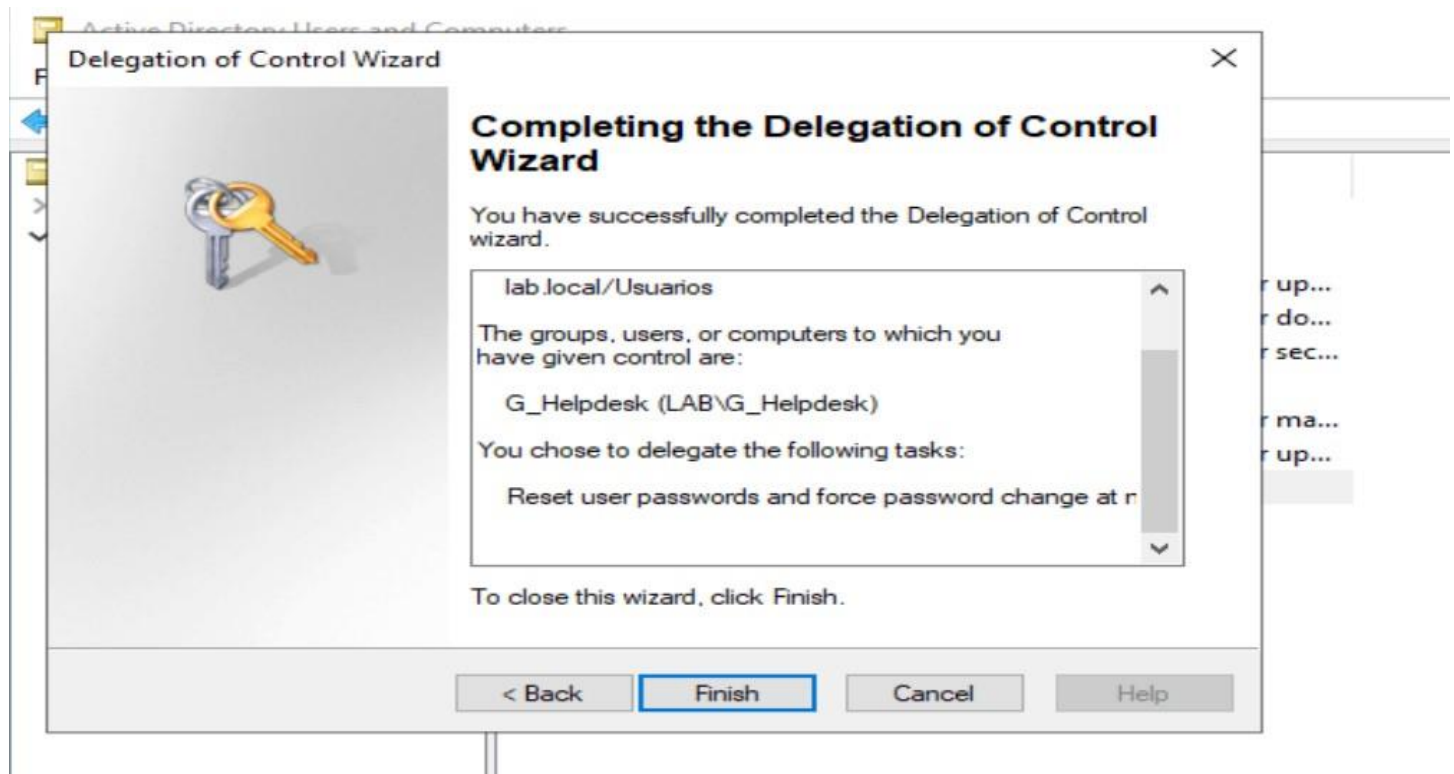
## Evidencia 25: Selección del grupo "G\_Helpdesk" como destinatario de los permisos.



## Evidencia 26: Configuración de tareas delegadas: restablecimiento de contraseñas.



## Evidencia 27: Finalización exitosa de la delegación de control sobre la OU Usuarios.





## Evidencia 28: Creación de la carpeta "Permisos\_Compartidos" mediante PowerShell.

```
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                Permisos_Compartidos

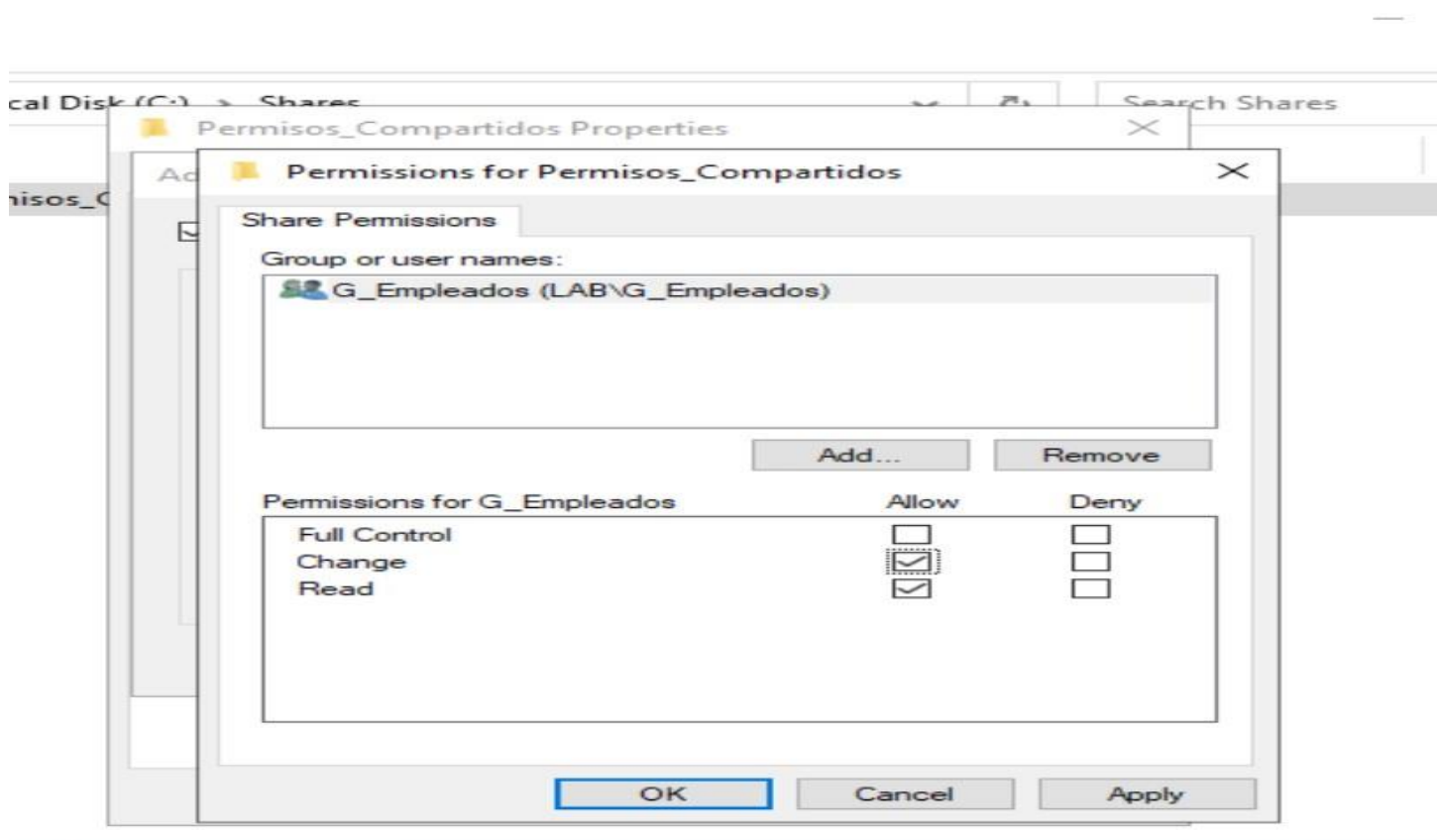
PS C:\Users\Administrador> Get-ChildItem "C:\Shares\"

Directory: C:\Shares

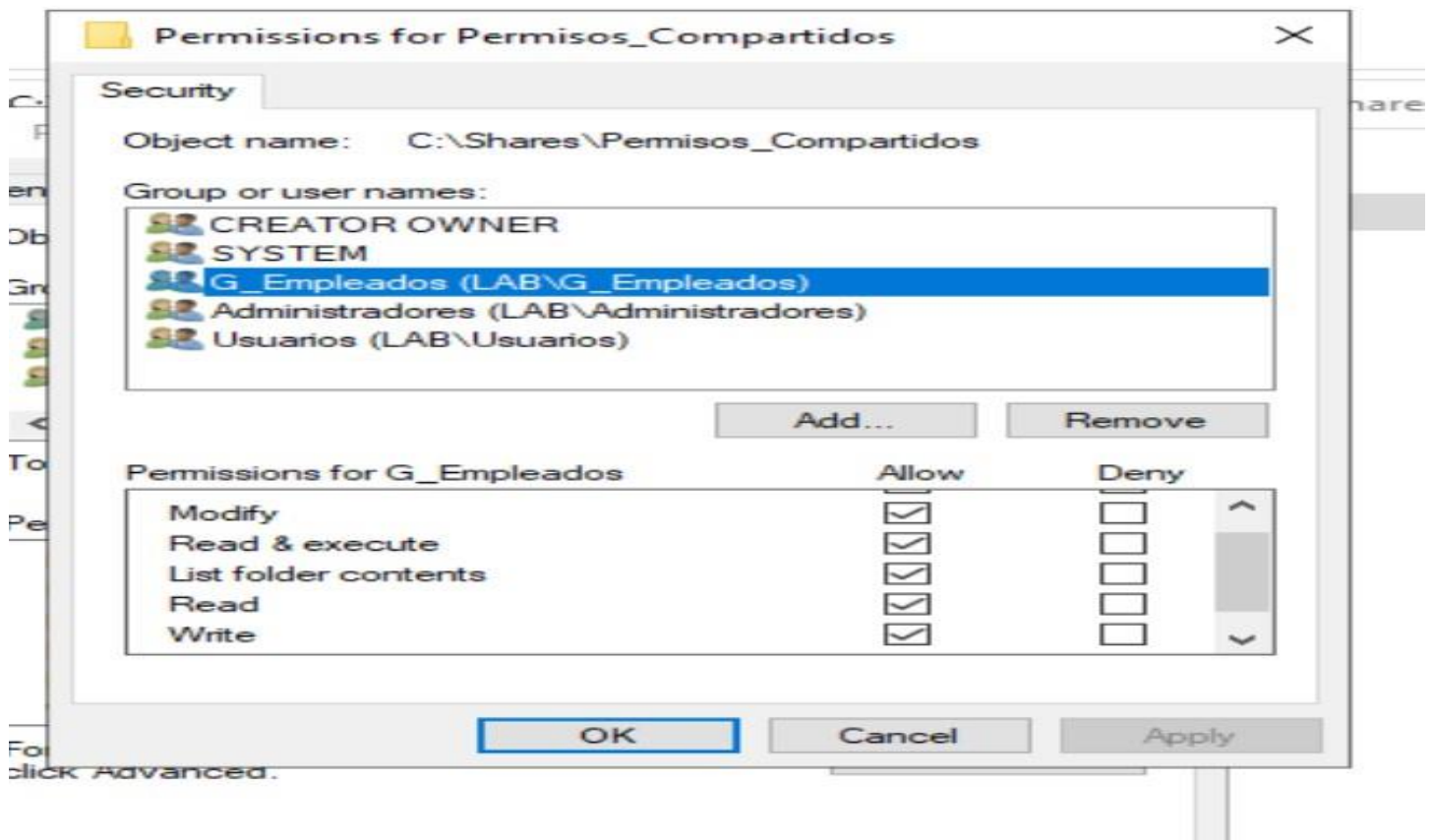
Mode                LastWriteTime         Length Name
----                -
d-----         10/15/2025  11:07 PM                Permisos_Compartidos

PS C:\Users\Administrador>
```

## Evidencia 29: Configuración de permisos de recurso compartido para el grupo G\_Empleados.



### Evidencia 30: Asignación de permisos NTFS a G\_Empleados en la carpeta compartida.



## Conclusiones

La implementación de este laboratorio permitió comprender de manera práctica la arquitectura y administración fundamental de un dominio de Active Directory. Se logró constatar la importancia de una estructura organizativa bien planificada mediante Unidades Organizativas (OUs) y el rol central de las Políticas de Grupo (GPOs) en la aplicación centralizada de configuraciones y restricciones de seguridad.

Si bien inicialmente representó un desafío conceptual comprender la interrelación entre las OUs, las GPOs y los permisos NTFS, la ejecución práctica de las tareas permitió consolidar estos conceptos y visualizar su funcionamiento integrado.

Adicionalmente, se adquirió experiencia básica en el uso de PowerShell para la administración de Active Directory, automatizando la creación de objetos y la configuración de políticas. Este enfoque demuestra un método eficiente y escalable para la gestión de entornos de directorio, de gran utilidad en un escenario productivo real.

En términos generales, la práctica constituyó una simulación integral que facilitó conectar los fundamentos teóricos con las competencias técnicas requeridas para la administración de un entorno Windows Server basado en dominios.

## Herramientas utilizadas

Para el desarrollo del presente laboratorio, se empleó el siguiente stack tecnológico y herramientas de administración:

- Sistemas Operativos:
  - Windows Server 2022 (Controlador de Dominio)
  - Windows 10 (Estación de trabajo cliente)
- Plataforma de Virtualización:
  - Oracle VM VirtualBox
- Herramientas de Administración de Active Directory:
  - Centro de Administración de Active Directory (Active Directory Users and Computers)
  - Consola de Administración de Políticas de Grupo (Group Policy Management Console - GPMC)
- Lenguaje de Automatización:
  - PowerShell (con módulo ActiveDirectory)

Esta selección de herramientas permitió emular de manera efectiva un entorno de dominio corporativo, facilitando la práctica integral de los conceptos de administración de directorios y políticas.

Autora: Ingrid K.

Octubre 2025.