

Practica Laboratorio Active Directory

Autora: Ingrid K.

Octubre 2025.

Índice

1. Configuración inicial y verificación del dominio.
2. Acceso a recursos compartidos y permisos basados en grupos.
3. Configuración del rol HelpDesk y delegación de permisos.
4. Reseteo de contraseñas como HelpDesk.
5. Verificación de políticas de seguridad y auditoría.
6. Conclusión y cierre. Herramientas utilizadas, comandos y scripts.

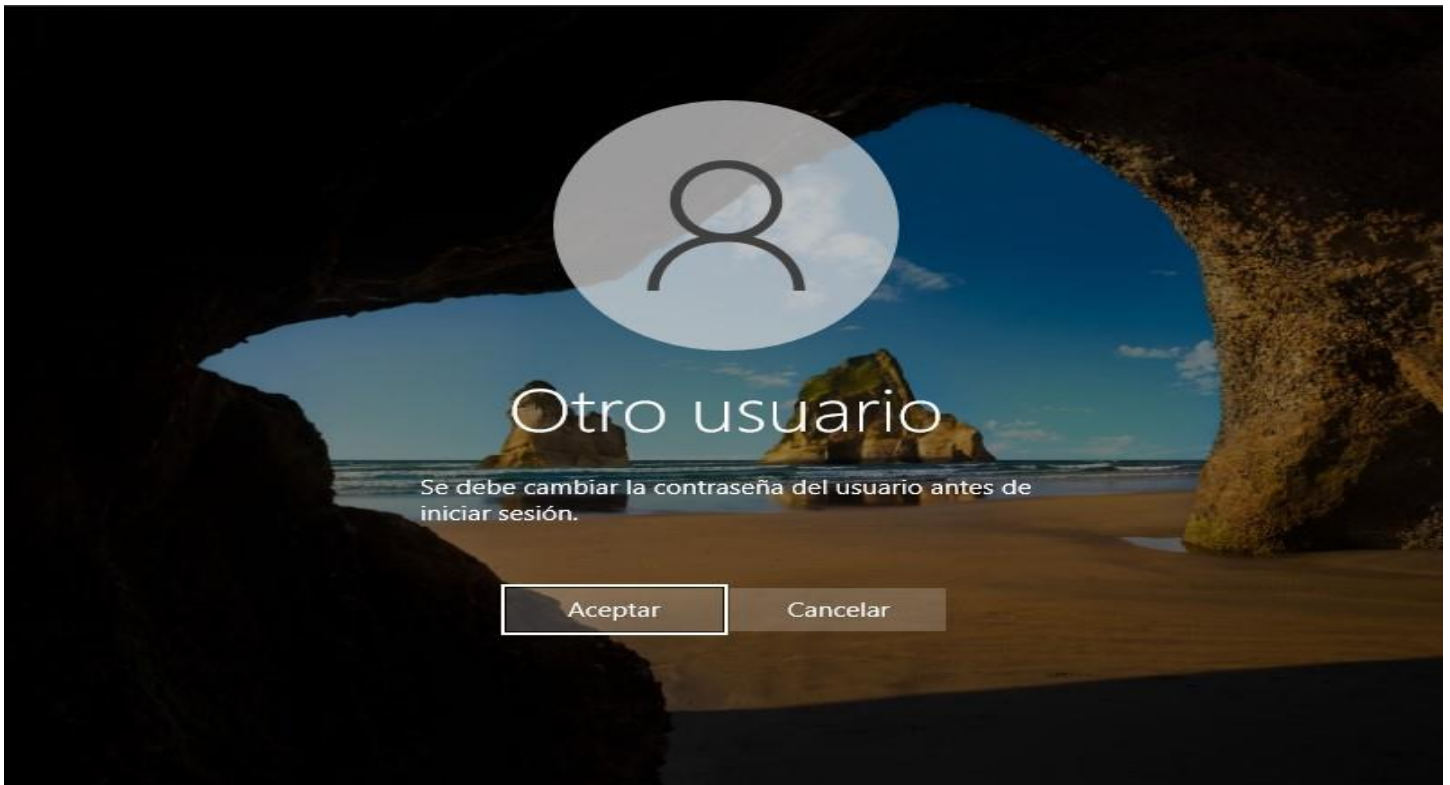
Configuración inicial y verificación del dominio

Verificar la correcta integración de la estación de trabajo al dominio y validar el proceso de autenticación de usuarios en el entorno de Active Directory.

Procedimiento Ejecutado

- Se unió la estación de trabajo al dominio "lab.local".
- Se verificó la resolución DNS y la conectividad de red con el controlador de dominio.
- Se realizó la autenticación exitosa utilizando credenciales del usuario de dominio "jgomez".

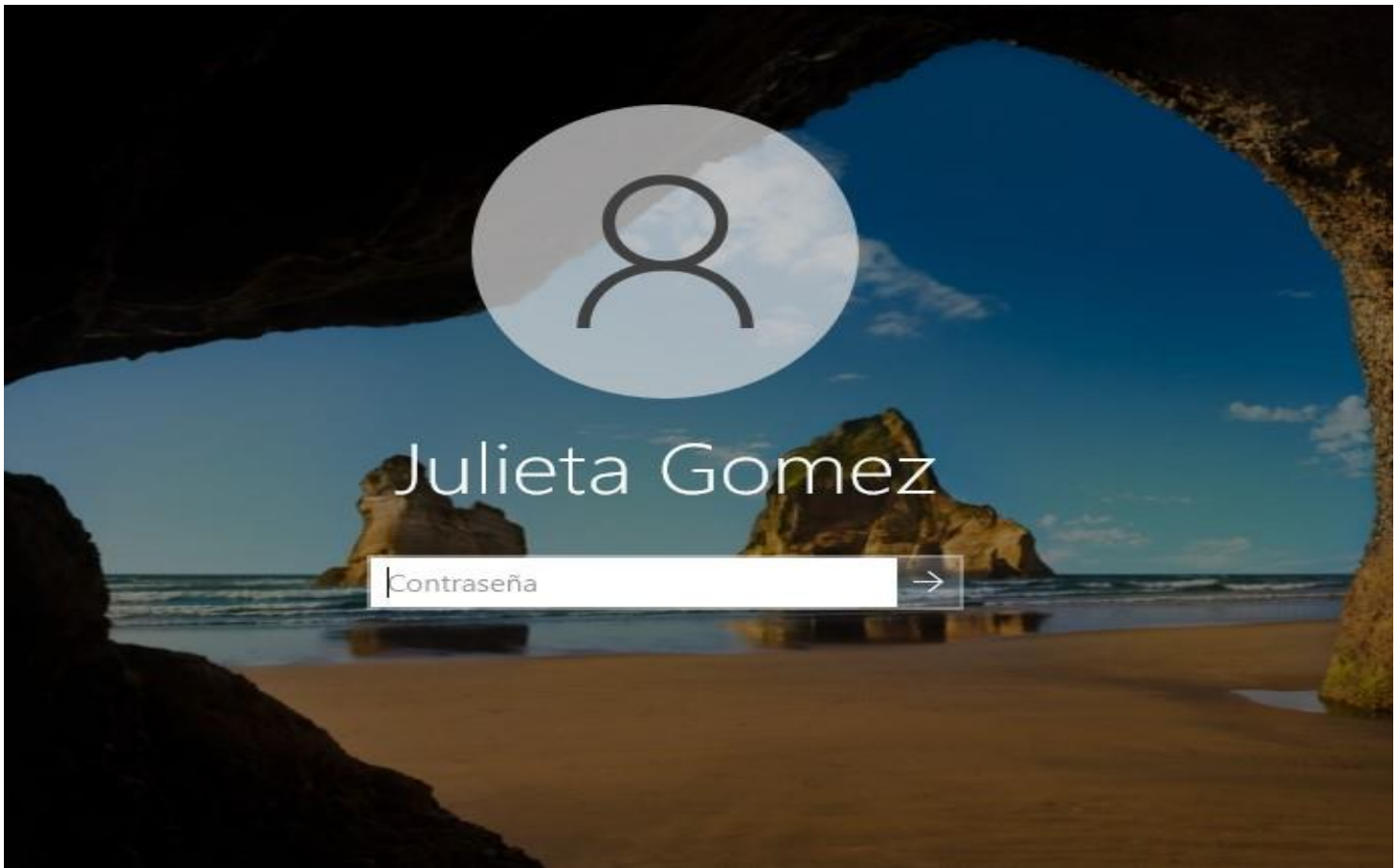
Evidencia 1: Cambio de contraseña en inicio de sesión. Política de seguridad aplicada.



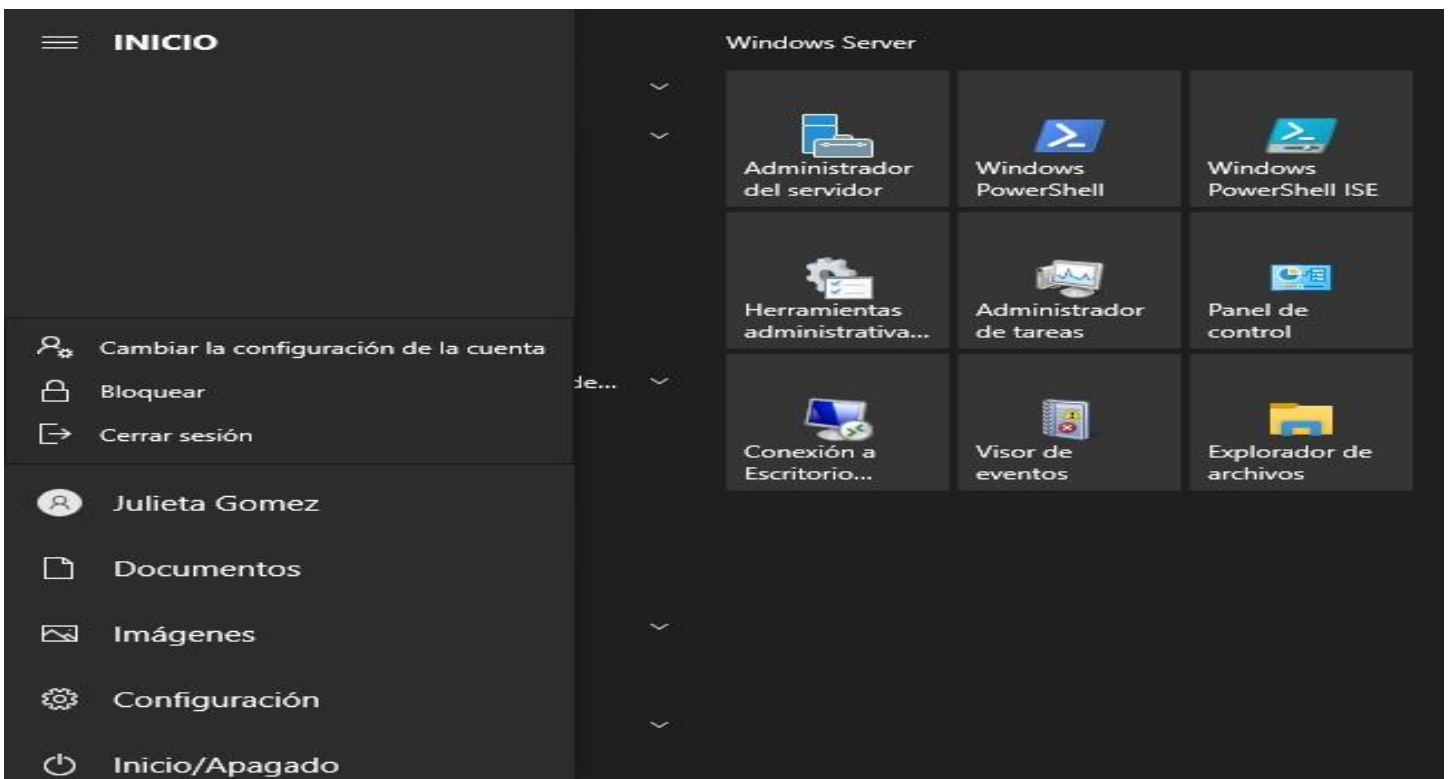
Evidencia 2: Confirmación de cambio de contraseña exitoso.



Evidencia 3: Autenticación de usuario (jgomez) en el dominio.



Evidencia 4: Sesión activa de usuario (jgomez) en estación de trabajo.



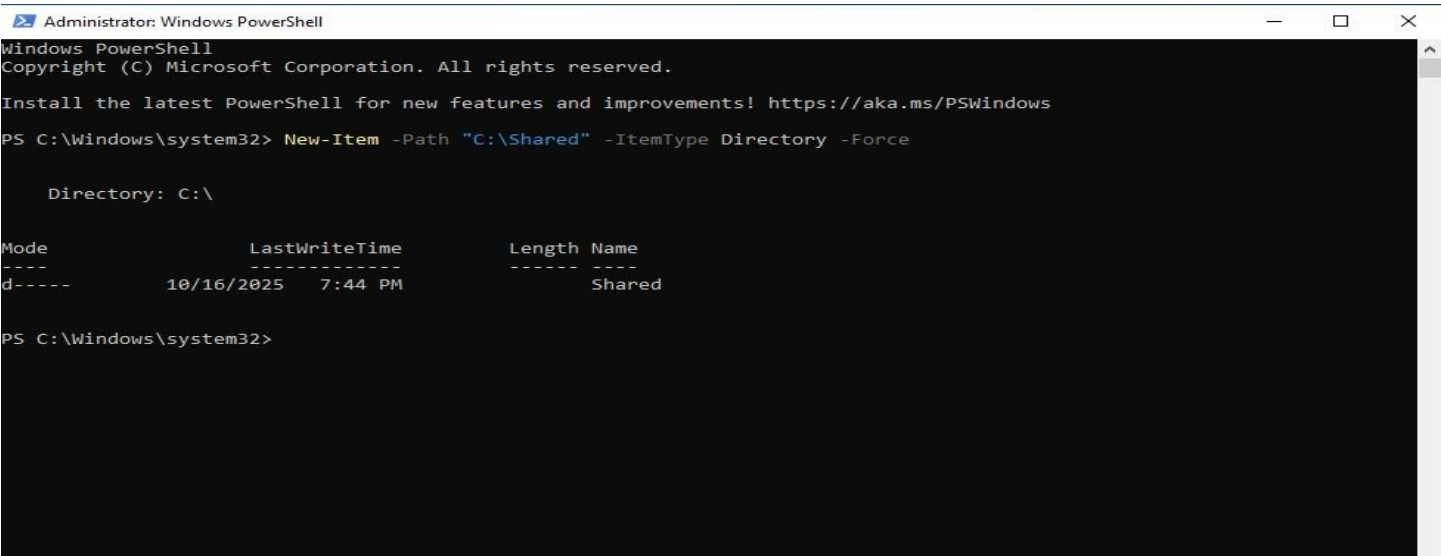
Acceso a recursos compartidos y permisos basados en grupos

Demostrar el correcto funcionamiento del sistema de permisos basados en grupos de seguridad para el acceso a recursos compartidos en la red.

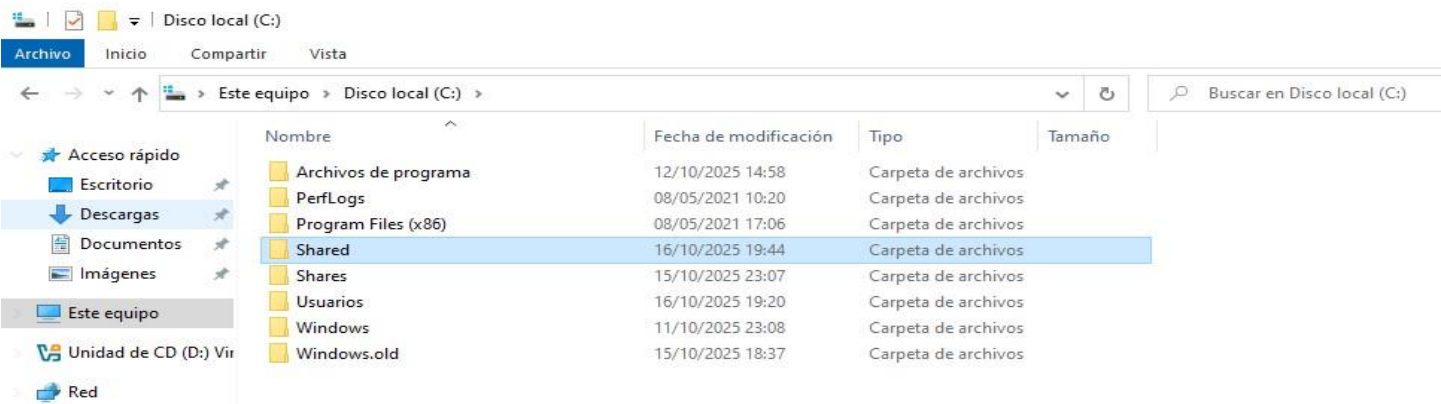
Procedimiento Ejecutado

- Se estableció conexión al recurso compartido \\servidor\Shared desde el equipo cliente.
- Se verificaron los permisos de lectura asignados en la carpeta compartida.
- Se validó el correcto funcionamiento de la estructura combinada de permisos NTFS y permisos de recurso compartido.

Evidencia 5: Creación de directorio compartido mediante PowerShell.



Evidencia 6: Directorio Shared creado en unidad C. Recurso disponible para configuración.



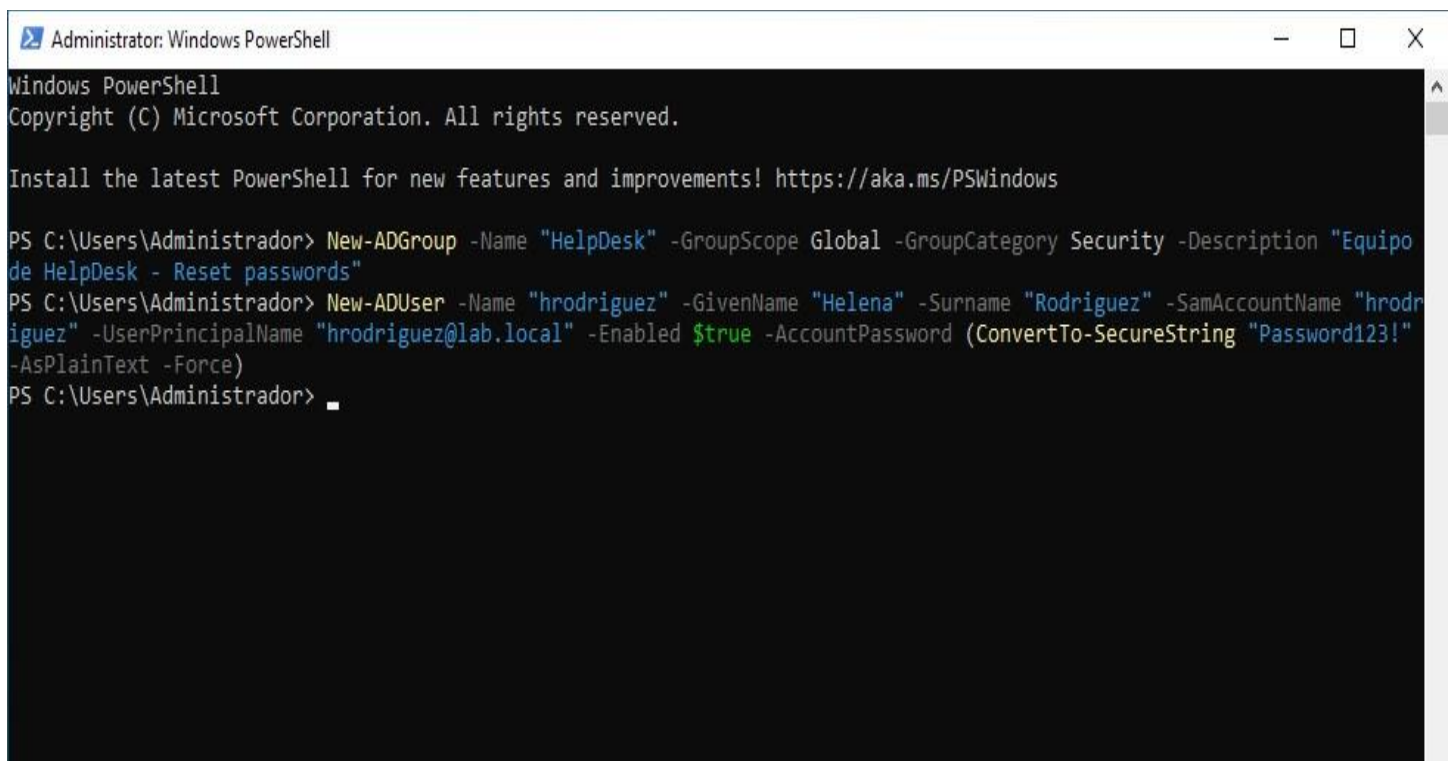
Configuración del rol HelpDesk y delegación de permisos

Establecer y configurar un rol especializado de Help Desk con permisos delegados específicos para la gestión de cuentas de usuario, manteniendo el principio de mínimo privilegio.

Procedimiento Ejecutado

- Se creó el grupo de seguridad "HelpDesk" en el Directorio Activo con ámbito global.
- Se asignó al usuario "hrodriguez" como miembro del grupo HelpDesk.
- Se delegaron permisos específicos al grupo HelpDesk para las siguientes operaciones:
 - Restablecimiento de contraseñas de usuario.
 - Lectura y escritura de restricciones de cuenta.
 - Gestión de tiempos de bloqueo de cuentas.

Evidencia 7: Creación de grupo HelpDesk y usuario hrodriguez.

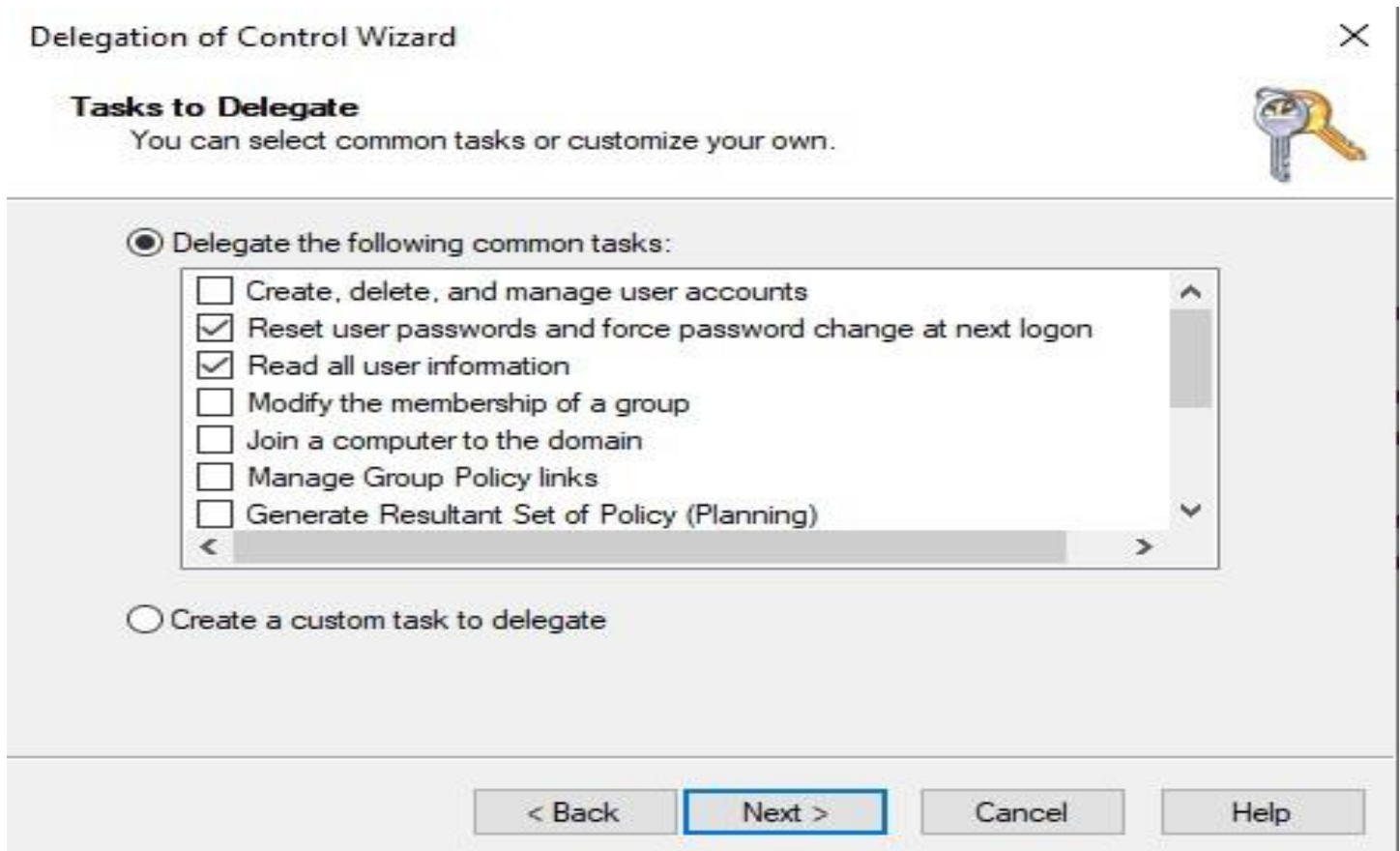


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\Administrador> New-ADGroup -Name "HelpDesk" -GroupScope Global -GroupCategory Security -Description "Equipo de HelpDesk - Reset passwords"
PS C:\Users\Administrador> New-ADUser -Name "hrodriguez" -GivenName "Helena" -Surname "Rodriguez" -SamAccountName "hrodriguez" -UserPrincipalName "hrodriguez@lab.local" -Enabled $true -AccountPassword (ConvertTo-SecureString "Password123!" -AsPlainText -Force)
PS C:\Users\Administrador> _
```

Evidencia 8: Delegación de permisos para reset de contraseñas.



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

☒ Delegate the following common tasks:

- ☐ Create, delete, and manage user accounts
- ☒ Reset user passwords and force password change at next logon
- ☒ Read all user information
- ☐ Modify the membership of a group
- ☐ Join a computer to the domain
- ☐ Manage Group Policy links
- ☐ Generate Resultant Set of Policy (Planning)

☐ Create a custom task to delegate

< Back Next > Cancel Help

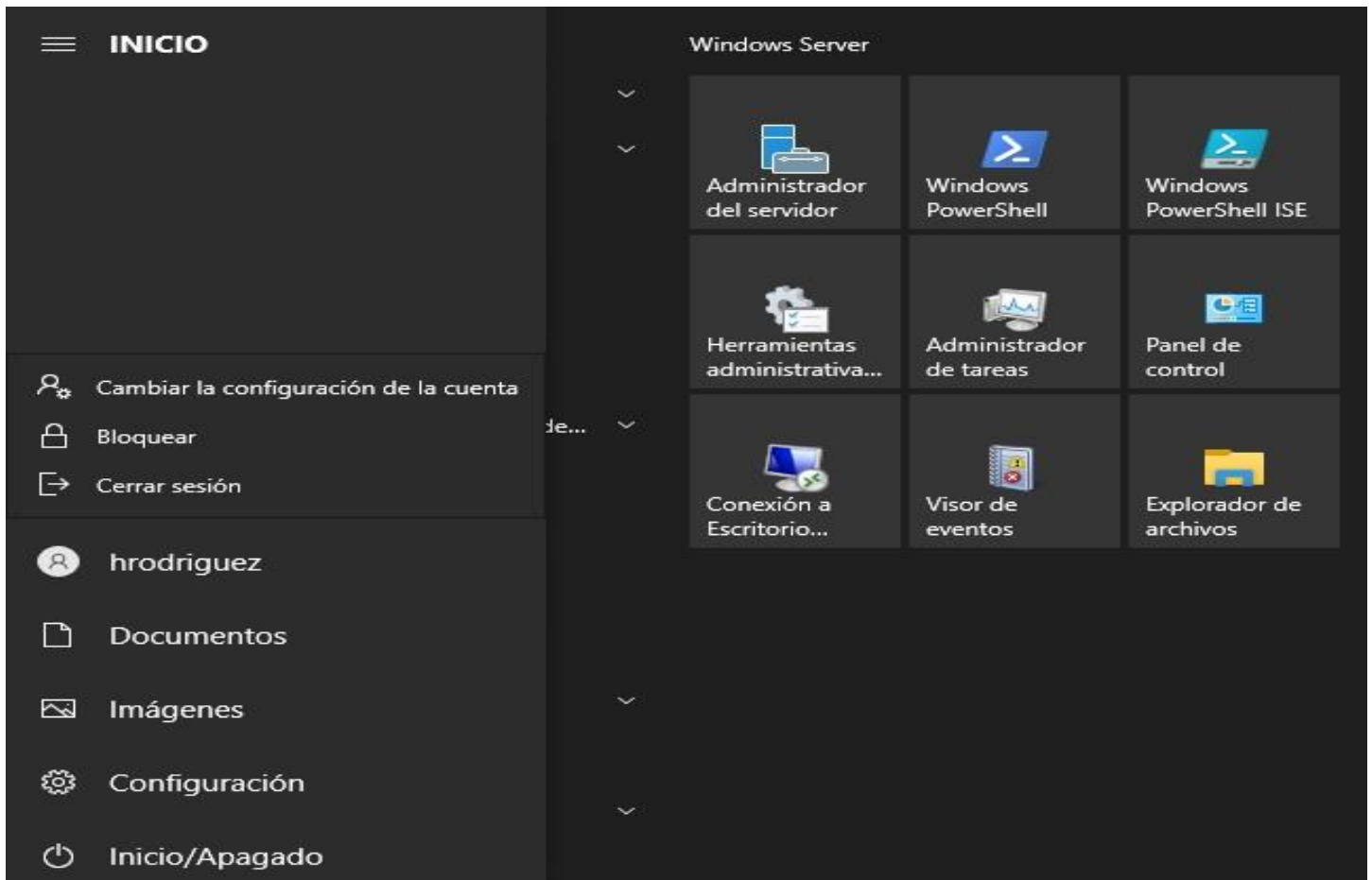
Reseteo de contraseñas como HelpDesk

Comprobar la funcionalidad operativa del reseteo de contraseñas por parte del personal autorizado de Help Desk y validar la correcta aplicación de los permisos delegados en el entorno de Active Directory.

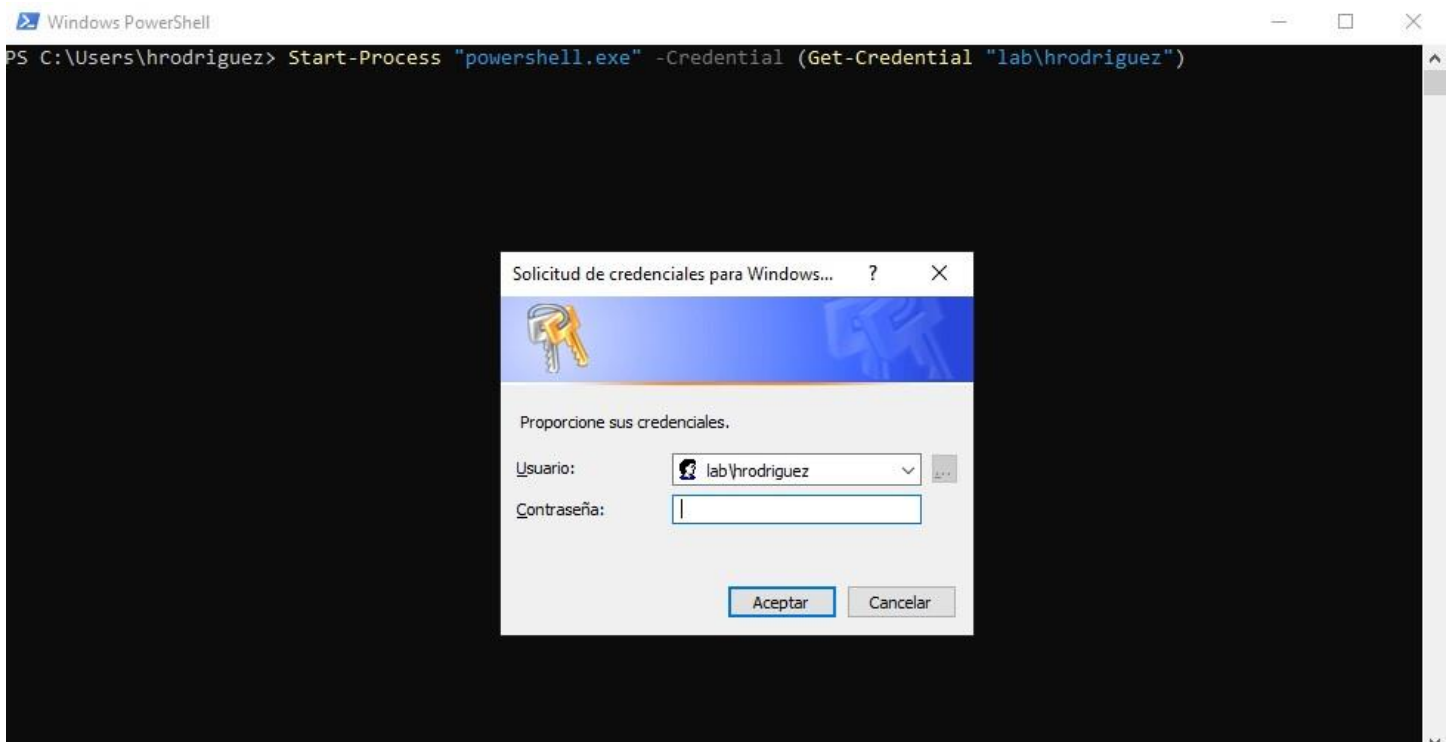
Procedimiento Ejecutado

- Inicio de sesión en el sistema utilizando credenciales de usuario perteneciente al grupo Help Desk.
- Ejecución de comandos específicos para el restablecimiento de contraseña de usuario de prueba.
- Configuración del parámetro de cambio obligatorio de contraseña en el próximo inicio de sesión.
- Verificación del comportamiento del sistema durante el siguiente acceso del usuario afectado.

Evidencia 9: Sesión activa de usuario. Autenticación exitosa con credenciales de HelpDesk.



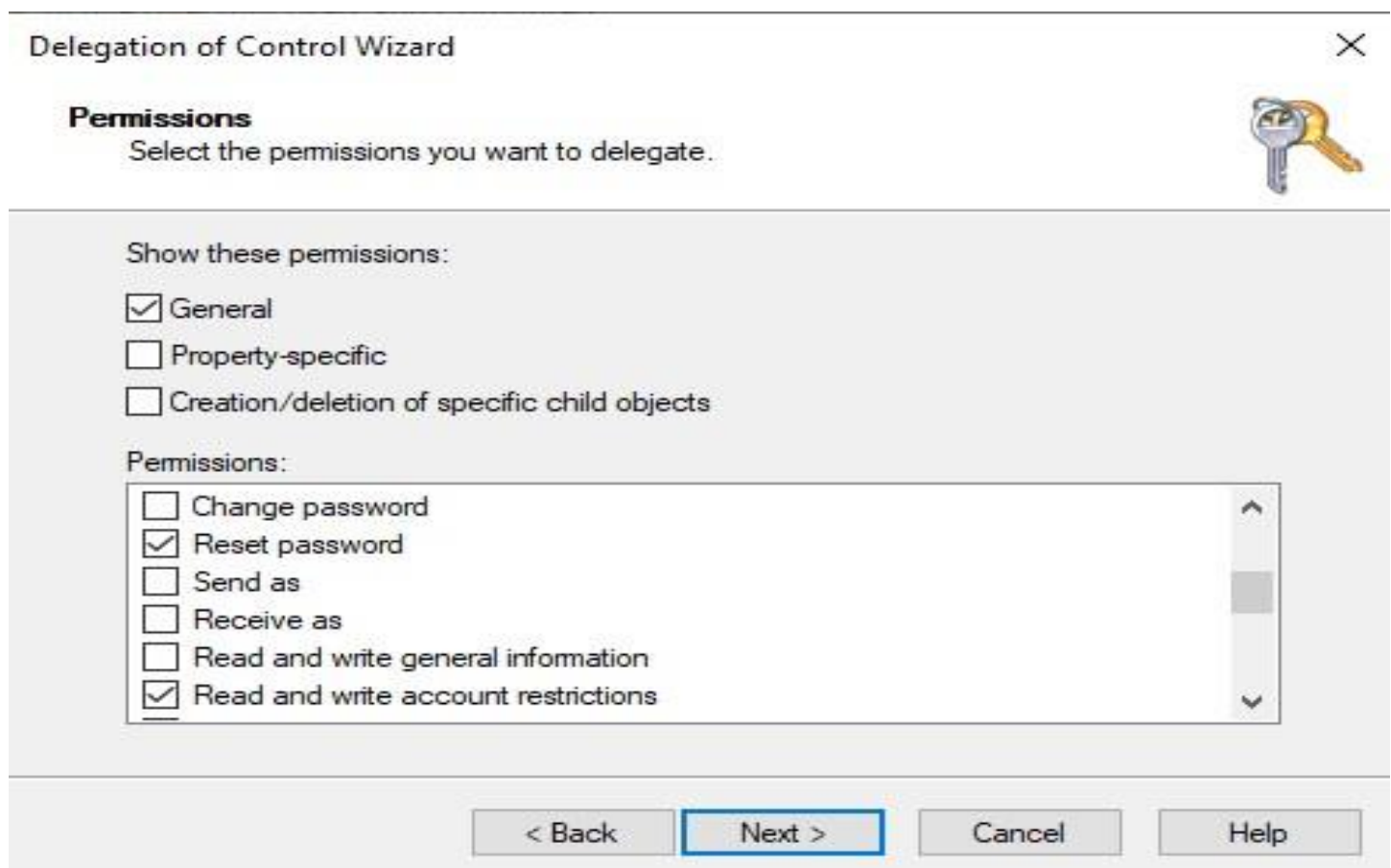
Evidencia 10: Autenticación para operaciones delegadas.



Evidencia 11: Consola PowerShell con privilegios HelpDesk.



Evidencia 12: Asignación de capacidades de gestión de contraseñas para HelpDesk.



Evidencia 13: Verificación de membresía en grupo HelpDesk.

```
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> Get-ADPrincipalGroupMembership -Identity "hrodriguez" | Select Name

Name
----
Usuarios del dominio
HelpDesk

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

Evidencia 14: Reset de contraseña ejecutado por HelpDesk.

```
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\hrodriguez> Set-ADAccountPassword -Identity "lsosa" -Reset -NewPassword (ConvertTo-SecureString "TempPass123" -AsPlainText -Force)
PS C:\Users\hrodriguez> Set-ADUser -Identity "lsosa" -ChangePasswordAtLogon $true
PS C:\Users\hrodriguez>
```

Evidencia 15: Gestión de estados de usuario con permisos delegados.

```
Windows PowerShell
PS C:\Users\hrodriguez> Disable-ADAccount -Identity "lsosa"
z> Get-ADUser -Filter {Enabled -eq $false} -Properties Name,Enabled

DistinguishedName : CN=Invitado,CN=Users,DC=lab,DC=local
Enabled           : False
GivenName        :
Name             : Invitado
ObjectClass      : user
ObjectGUID       : bdf6e48d-0005-4d87-b1cd-d7f128c19748
SamAccountName   : Invitado
SID              : S-1-5-21-3115137076-146667767-1695127003-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=lab,DC=local
Enabled           : False
GivenName        :
Name             : krbtgt
ObjectClass      : user
ObjectGUID       : 2035d51e-460f-4a30-9dac-3b04a451a216
SamAccountName   : krbtgt
SID              : S-1-5-21-3115137076-146667767-1695127003-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=Luciano Sosa,OU=Empleados,OU=Usuarios,DC=lab,DC=local
Enabled           : False
GivenName        : Luciano
Name             : Luciano Sosa
ObjectClass      : user
ObjectGUID       : d7f0a962-19ab-4d9e-9734-8fc5bb5fc69d
SamAccountName   : lsosa
SID              : S-1-5-21-3115137076-146667767-1695127003-1113
Surname          : Sosa
UserPrincipalName : lsosa@lab.local
```

Evidencia 16: Verificación de políticas de grupo aplicadas.

Windows PowerShell

```
PS C:\Users\hrodriguez> gpresult /r

Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
© Microsoft Corporation. Todos los derechos reservados.

Creado el 16/10/2025 a las 22:52:03

RSOP datos para LAB\hrodriguez en WIN-IN5MG5DHHU5 : modo de inicio de sesión
-----

Configuración del sistema operativo: Controlador de dominio principal
Versión del sistema operativo: 10.0.20348
Nombre de sitio: n/a
Perfil móvil: n/a
Perfil local: C:\Users\hrodriguez
¿Conectado a un vínculo de baja velocidad?: No

CONFIGURACIÓN DE USUARIO
-----
CN=hrodriguez,CN=Users,DC=lab,DC=local
Última vez que se aplicó la Directiva de grupo: 16/10/2025 a las 22:47:51
Directivas de grupo aplicadas desde WIN-IN5MG5DHHU5.lab.local
Umbral del vínculo de baja velocidad de las Directivas de grupo: 500 kbps
Nombre de dominio: LAB
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
n/a

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
```

Evidencia 17: Configuración de seguridad y políticas granulares aplicadas.

Administrator: Windows PowerShell

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

PS C:\Users\Administrador> Get-ADDefaultDomainPasswordPolicy

ComplexityEnabled           : True
DistinguishedName           : DC=lab,DC=local
LockoutDuration              : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold             : 0
MaxPasswordAge               : 42.00:00:00
MinPasswordAge               : 1.00:00:00
MinPasswordLength            : 7
objectClass                  : {domainDNS}
objectGuid                   : 9d5c9688-6ba5-4047-a5b4-a87207b93094
PasswordHistoryCount         : 24
ReversibleEncryptionEnabled : False

PS C:\Users\Administrador> Get-ADFineGrainedPasswordPolicy -Filter * | Format-Table Name,AppliesTo

Name                AppliesTo
-----
FGPP_Administradores {CN=G_Administradores,OU=Grupos,DC=lab,DC=local}
FGPP_Contadores     {CN=G_Contadores,OU=Grupos,DC=lab,DC=local}
FGPP_Empleados      {CN=G_Empleados,OU=Grupos,DC=lab,DC=local}

PS C:\Users\Administrador>
```

Verificación de políticas de seguridad y auditoría

Validar la correcta aplicación e implementación de políticas de grupo, políticas de contraseñas y sistemas de auditoría en el entorno de Active Directory, asegurando el cumplimiento de los estándares de seguridad establecidos y los requisitos normativos aplicables.

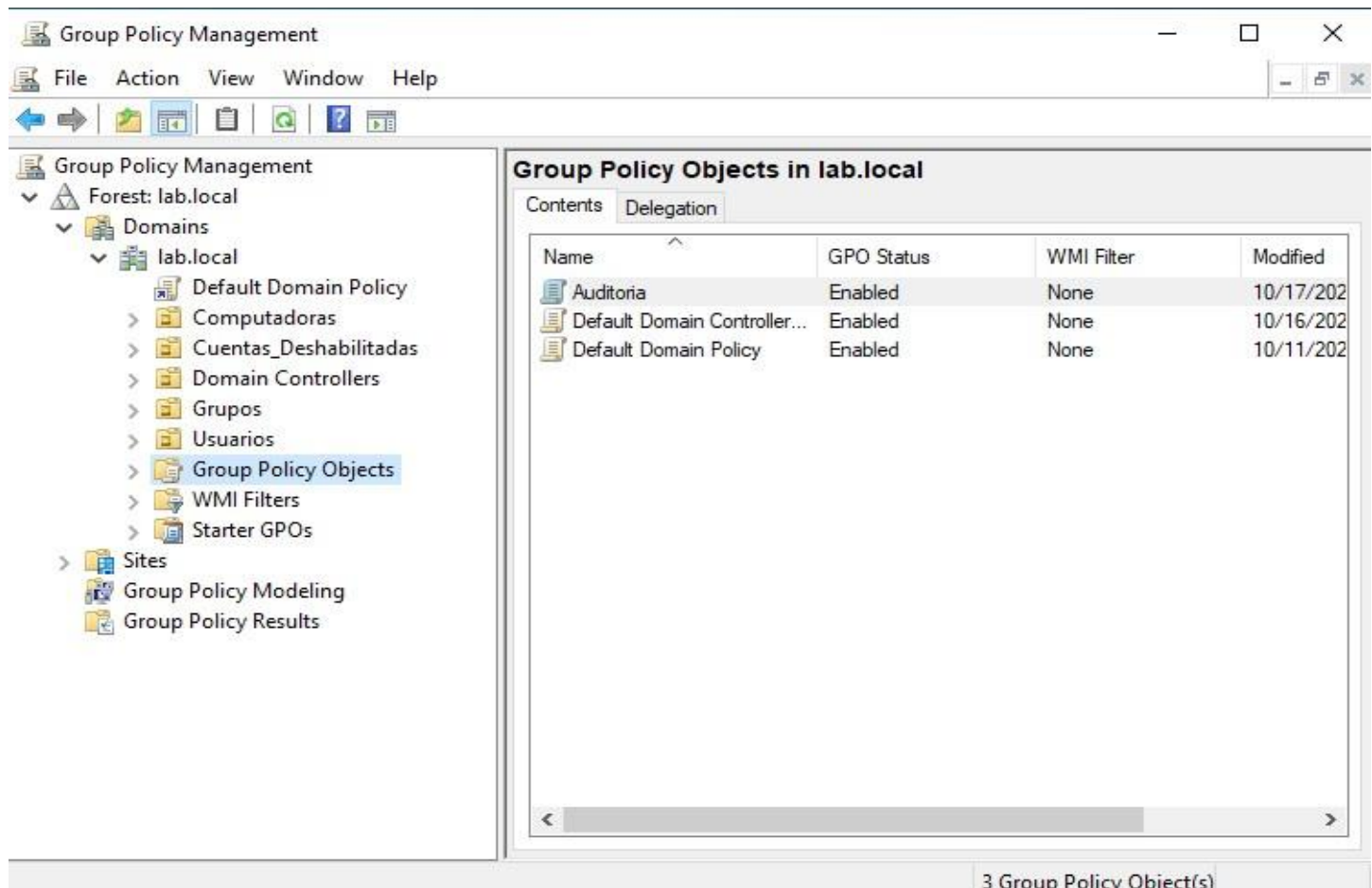
Procedimiento Ejecutado

- política de grupo habilitada para auditar logons (éxito/fracaso).
- actualización de políticas aplicada en clientes con gpupdate /force.
- verificación de eventos en security log mediante event viewer.

Eventos monitoreados

- 4624: logon exitoso.
- 4625: logon fallido.
- 4723: cambio de contraseña.

Evidencia 18: Configuración centralizada de políticas de seguridad.

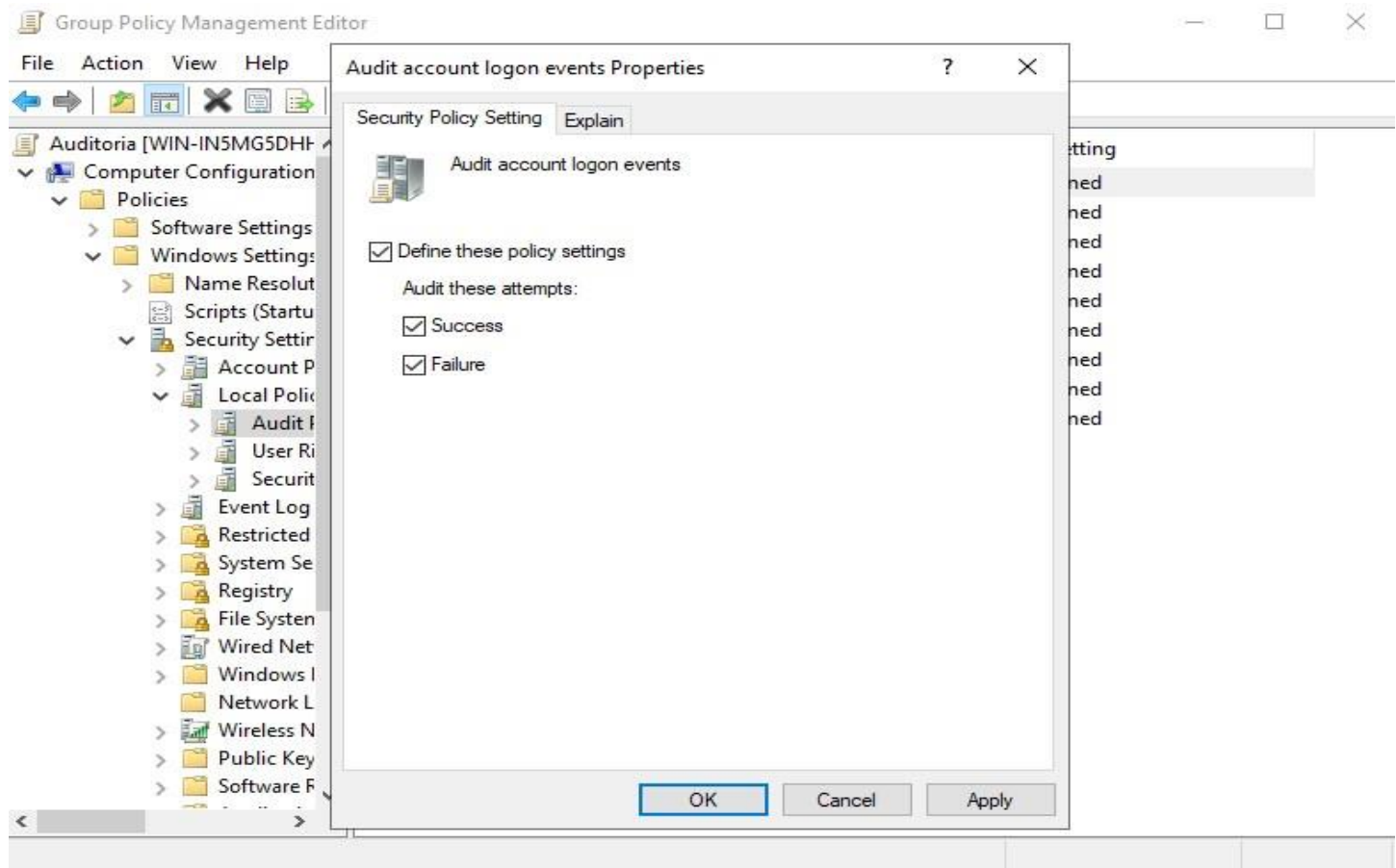


The screenshot displays the Group Policy Management console for the lab.local domain. The left pane shows the tree structure with 'Group Policy Objects' selected. The right pane shows a table of the configured GPOs.

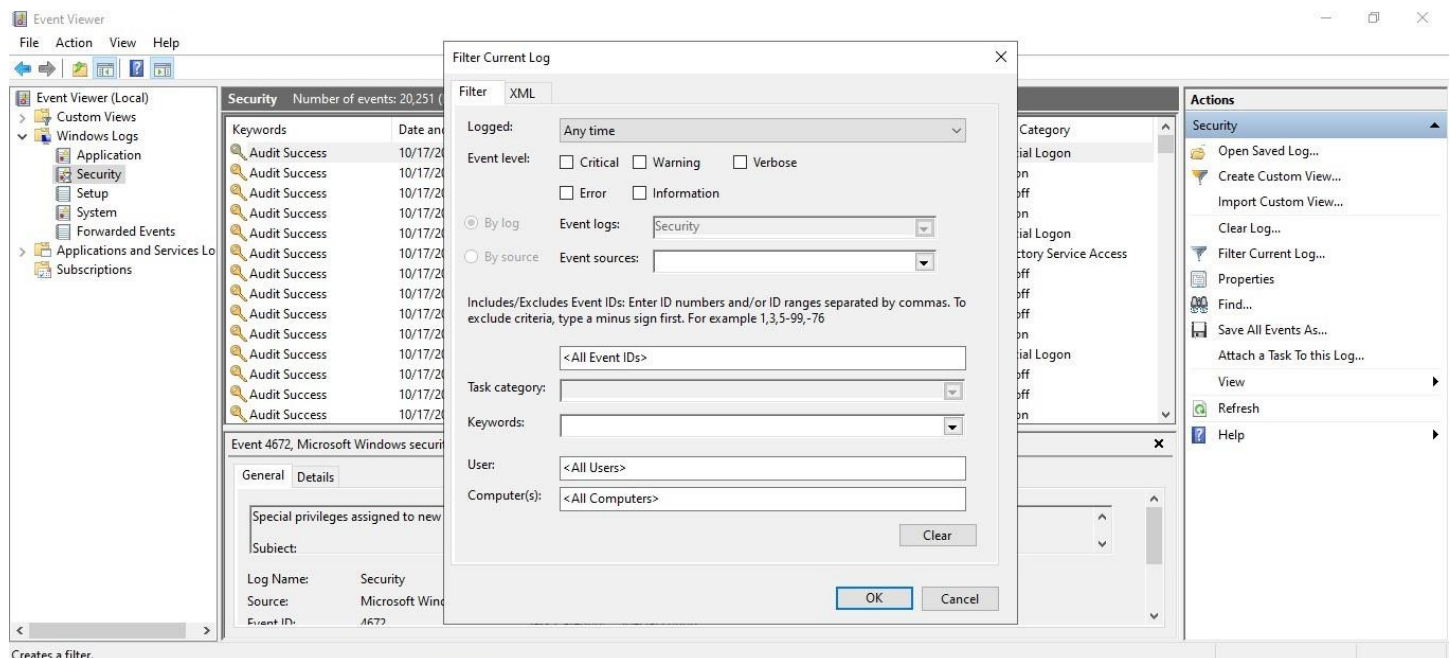
Name	GPO Status	WMI Filter	Modified
Auditoria	Enabled	None	10/17/2022
Default Domain Controller...	Enabled	None	10/16/2022
Default Domain Policy	Enabled	None	10/11/2022

3 Group Policy Object(s)

Evidencia 19: Configuración de políticas de auditoría para eventos de login.



Evidencia 20: Filtrado de eventos de seguridad por código. Análisis de logs del sistema.



Evidencia 21: Eventos 4624 filtrados - Registros de inicios de sesión exitosos en el sistema.

The screenshot displays the Windows Event Viewer interface. The top pane shows a list of filtered Security events (Log: Security; Source: ; Event ID: 4624). The bottom pane shows the details of a selected event (Event 4624, Microsoft Windows security auditing).

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/17/2025 3:08:42 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:07:42 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:54 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:42 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:20 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:20 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:20 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:20 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:10 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:06:10 AM	Microsoft Windows secur...	4624	Logon
Audit Success	10/17/2025 3:05:42 AM	Microsoft Windows secur...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Log Name: Security

Source: Microsoft Windows security Logged: 10/17/2025 3:08:42 AM

Event ID: 4624 Task Category: Logon

Conclusión

Este laboratorio permitió comprender el funcionamiento práctico de Active Directory Domain Services (AD DS) dentro de un entorno controlado, desde su instalación y configuración inicial hasta la administración de usuarios, grupos y políticas.

Se comprobó el acceso exitoso de usuarios al dominio desde un cliente Windows, la aplicación de políticas de contraseñas y la correcta asignación de permisos sobre recursos compartidos, consolidando conocimientos esenciales en administración de redes y sistemas Windows Server.

Herramientas

- Windows Server 2022
- Windows 10 Client
- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- Local Security Policy / gpresult / rsop.msc
- Shared Folder Manager
- Windows PowerShell
- VirtualBox
- DNS integrado en AD DS

Scripts y comandos

- **Crear Unidades Organizativas (OUs):**

New-ADOrganizationalUnit -Name "Users" -Path "DC=lab,DC=local"

- **Crear usuarios:**

New-ADUser -Name "Juan Pérez" -SamAccountName "jperez" -AccountPassword (ConvertTo-SecureString "P@ssw0rd1" -AsPlainText -Force) -Enabled \$true

- **Crear grupos de seguridad:**

New-ADGroup -Name "G_Students" -GroupScope Global GroupCategory Security -Path "OU=Groups,DC=lab,DC=local"

- **Agregar usuarios a grupos:**

Add-ADGroupMember -Identity "G_Students" -Members "jperez"

- **Modificar atributos de usuario:**

Set-ADUser -Identity "jperez" -Department "Informática"

- **Deshabilitar cuentas:**

Disable-ADAccount -Identity "mlopez"

- **Mover usuarios a otra OU:**

Move-ADObject -Identity (Get-ADUser "mlopez").DistinguishedName -TargetPath "OU=DisabledAccounts,DC=lab,DC=local"

- **Consultar política de contraseñas del dominio:**

Get-ADDefaultDomainPasswordPolicy

- **Ver políticas aplicadas a un usuario:**

gpresult /r o rsop.msc

- **Crear carpeta compartida:**

New-Item -Path "D:\Shares\Students" -ItemType Directory

- **Asignar permisos NTFS a un grupo:**

icacls "D:\Shares\Students" /grant "G_Students:(M)"