

Laboratorio Active Directory – Pruebas

Entorno

Windows Server 2022, Windows 10

VirtualBox

Active Directory Users and Computers

GPMC

PowerShell (módulo Active Directory)

Índice

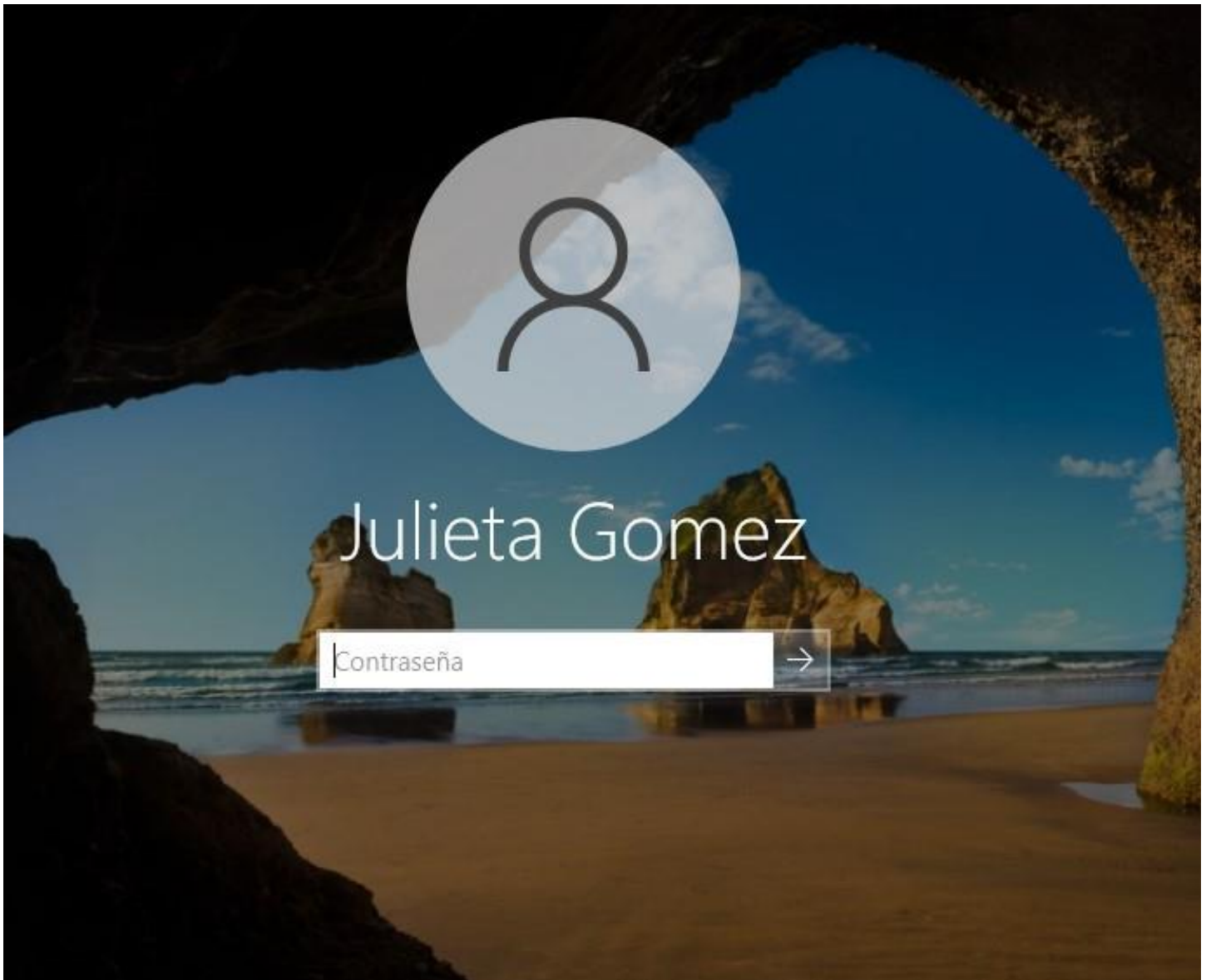
1. Verificación del Dominio y Acceso de Usuarios
2. Acceso a Recursos Compartidos y Permisos por Grupos
3. Rol HelpDesk y Delegación de Permisos
4. Reseteo de Contraseñas como HelpDesk
5. Políticas de Seguridad y Auditoría
6. Resumen final

1. Verificación del dominio y acceso de usuarios

Este apartado valida la correcta integración del cliente Windows al dominio lab.local, junto con la autenticación inicial de un usuario y la aplicación de políticas de contraseña

Acciones realizadas:

- Unión del equipo cliente al dominio
- Validación de DNS y conectividad
- Inicio de sesión exitoso del usuario jgomez y cambio obligatorio de contraseña

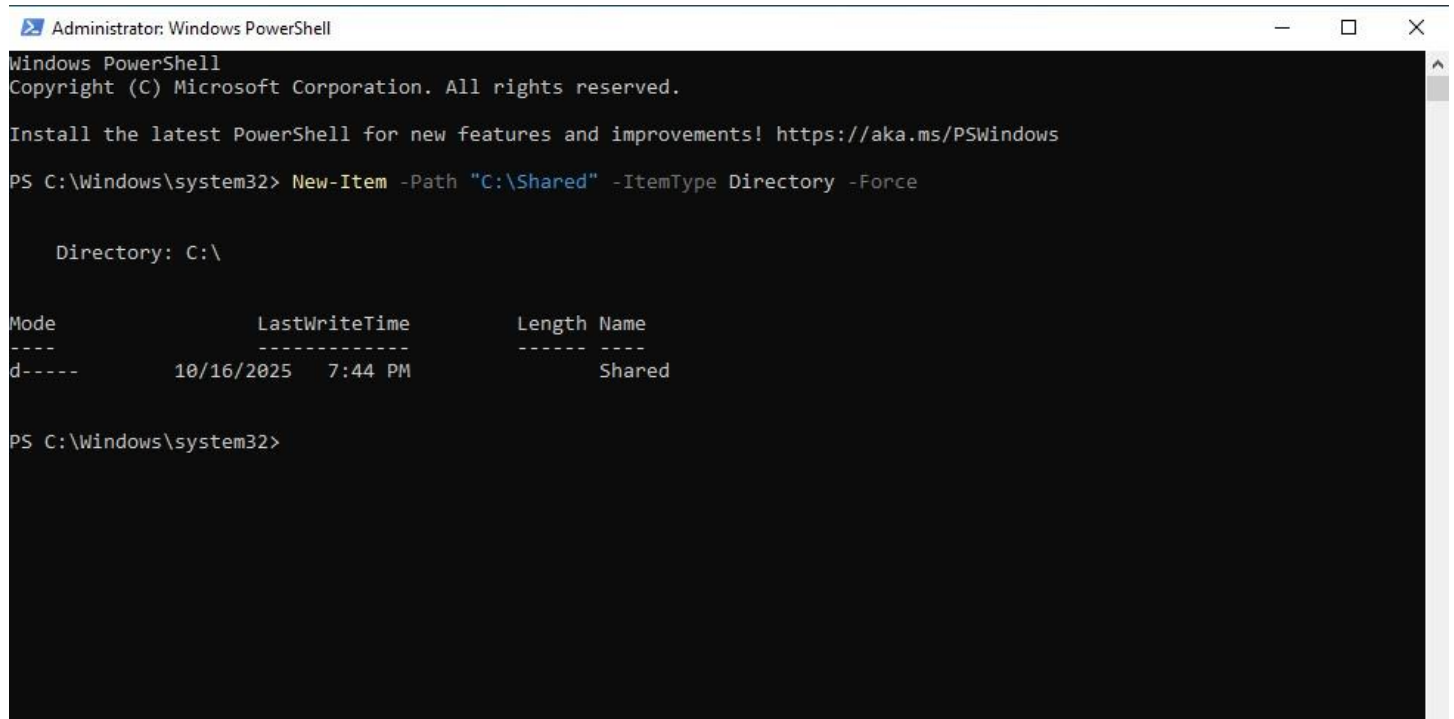


2. Acceso a recursos compartidos y permisos por grupos

Se comprobó el funcionamiento de los permisos NTFS + permisos de recurso, controlados por grupos de seguridad

Acciones realizadas:

- Acceso desde el cliente a Shared
- Verificación de permisos asignados a usuarios del grupo correspondiente
- Creación del directorio compartido desde 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:\Windows\system32> New-Item -Path "C:\Shared" -ItemType Directory -Force

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         10/16/2025   7:44 PM             Shared

PS C:\Windows\system32>
```

3. Rol HelpDesk y delegación de permisos

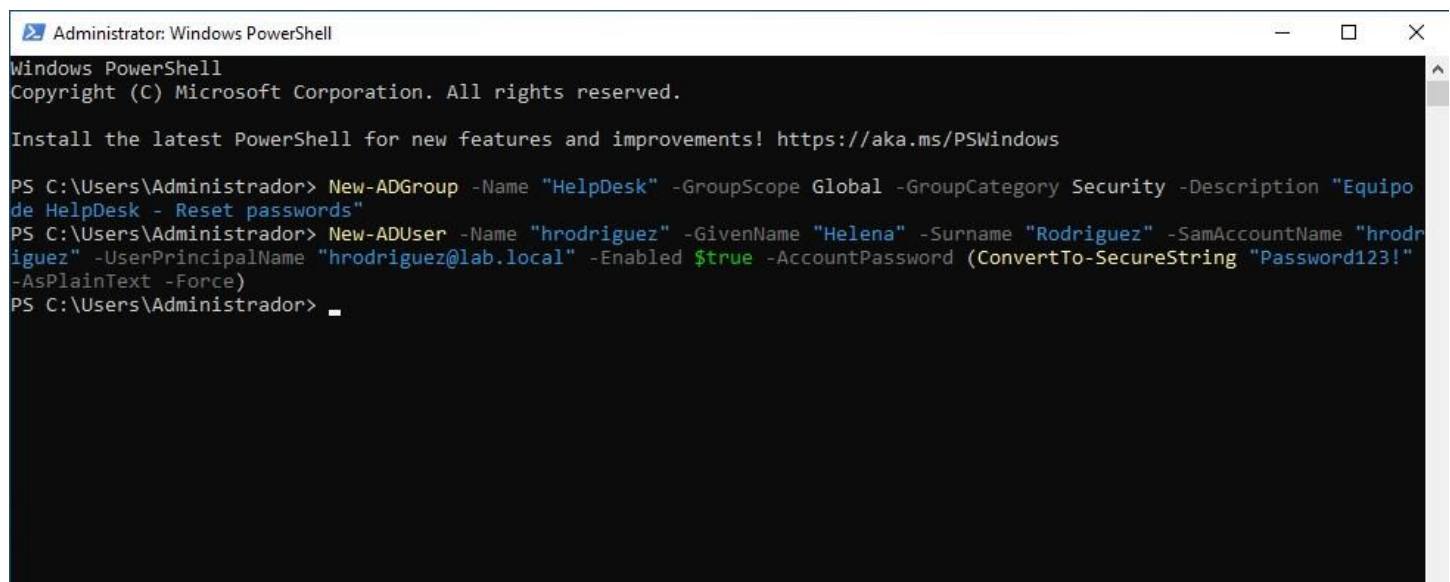
Se creó un rol especial HelpDesk, aplicando el principio de mínimo privilegio para tareas administrativas acotadas

Acciones realizadas:

- Creación del grupo HelpDesk
- Asignación del usuario hrodriguez

Delegación de permisos:

- Reset de contraseñas
- Modificación de restricciones de cuenta
- Lectura/escritura de atributos específicos



```
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

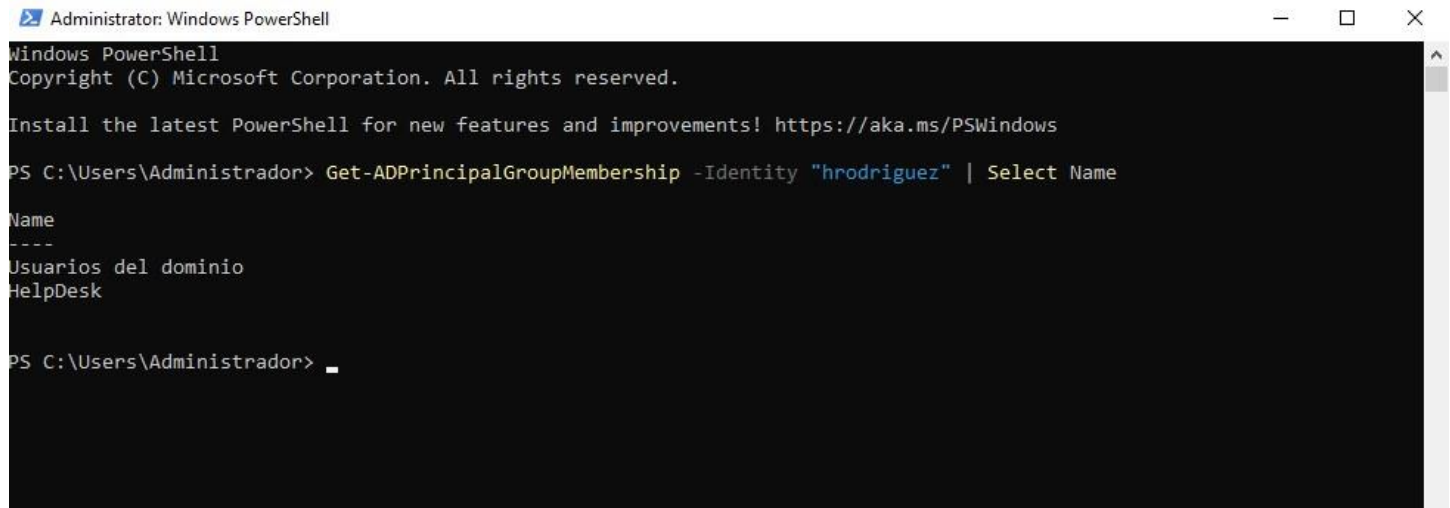
PS C:\Users\Administrador> New-ADGroup -Name "HelpDesk" -GroupScope Global -GroupCategory Security -Description "Equipo de HelpDesk - Reset passwords"
PS C:\Users\Administrador> New-ADUser -Name "hrodriguez" -GivenName "Helena" -Surname "Rodriguez" -SamAccountName "hrodriguez" -UserPrincipalName "hrodriguez@lab.local"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

4. Reseteo de contraseñas como HelpDesk

Se validó que el rol delegando pueda ejecutar sus tareas sin privilegios adicionales

Acciones realizadas:

- Inicio de sesión como hrodriguez.
- Ejecución del reset de contraseña desde herramienta delegada
- Verificación en PowerShell y en propiedades del usuario
- Confirmación del cambio en el siguiente inicio de sesión del usuario afectado



```
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

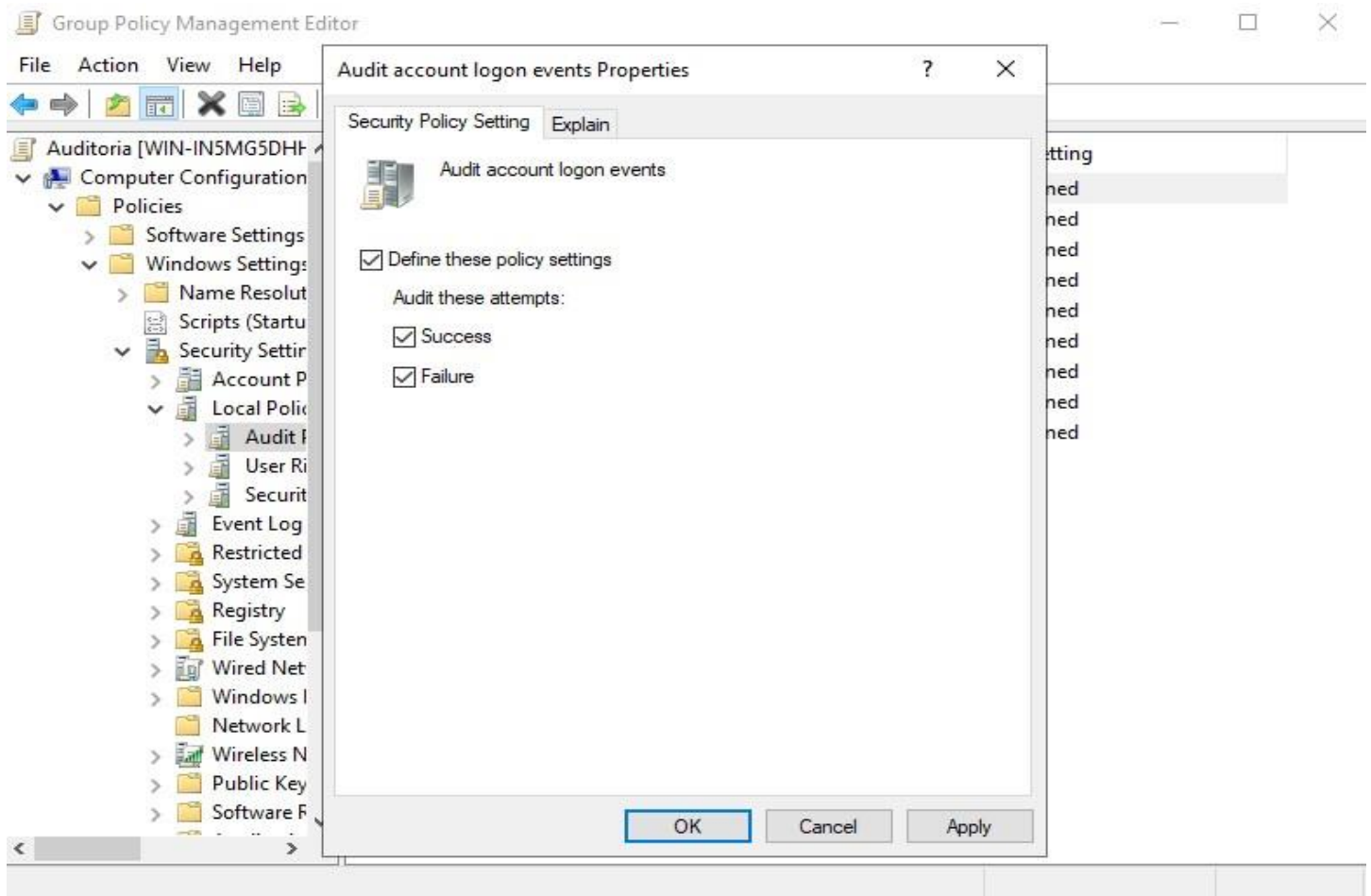
PS C:\Users\Administrador> _
```

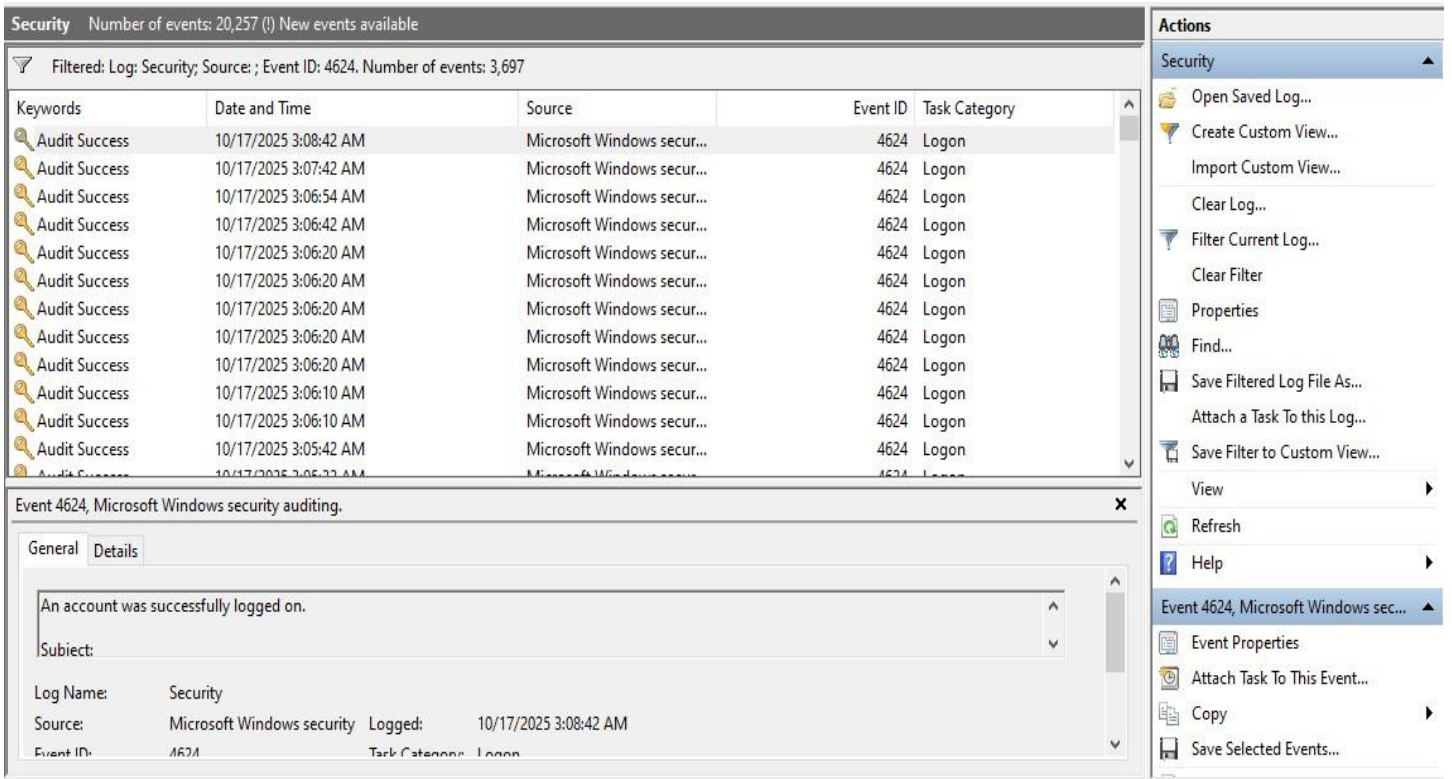
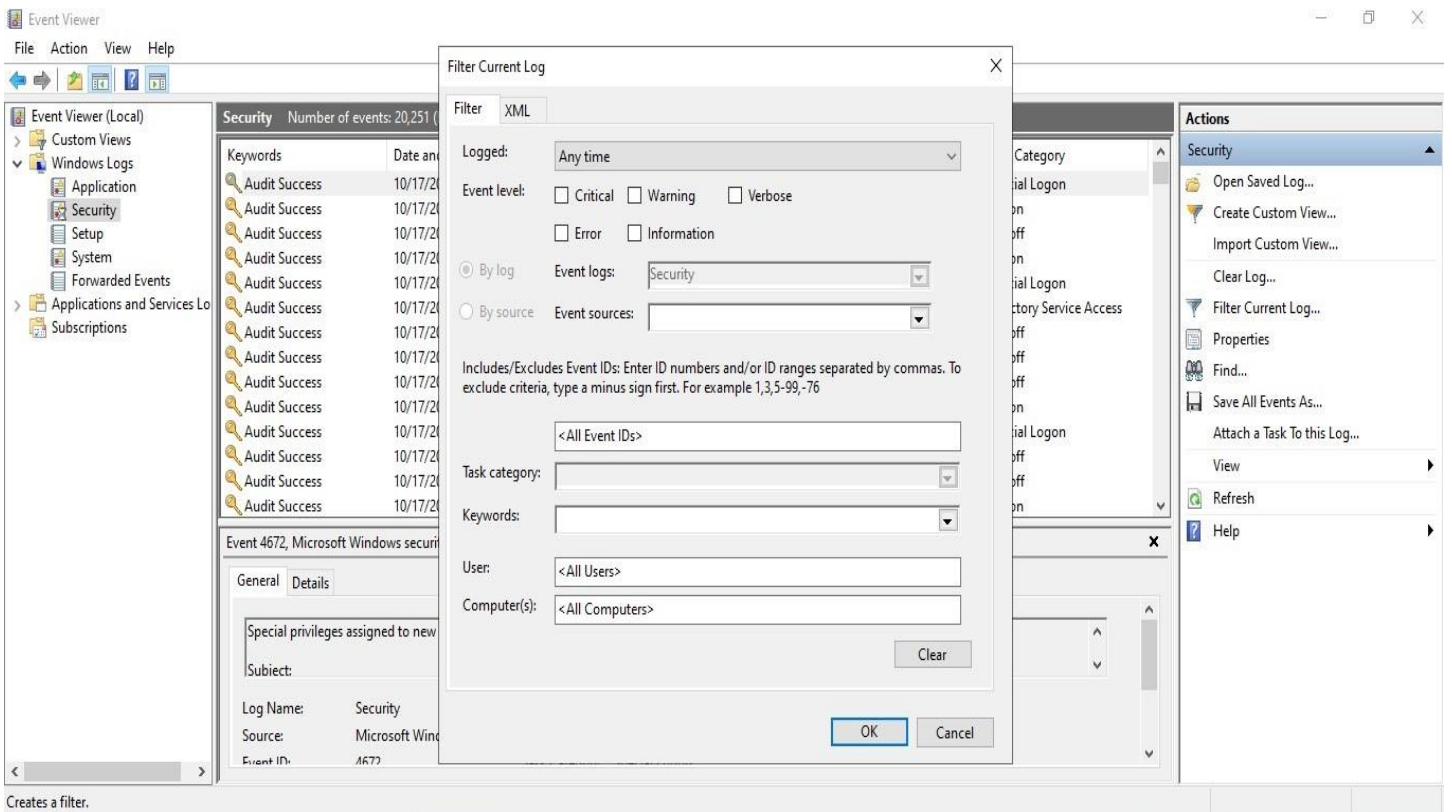
5. Políticas de seguridad y auditoría

Se revisó la aplicación de políticas de grupo, auditoría de eventos de inicio de sesión y logs relevantes

Acciones realizadas:

- Auditoría habilitada para login (4624/4625) y cambio de contraseña (4723)
- gpupdate /force desde clientes
- Análisis de eventos en Event Viewer → Security





6. Resumen final

Se trabajó con usuarios reales, grupos, recursos compartidos y auditoría para simular escenarios típicos de HelpDesk y soporte de primer nivel:

- Inicio de sesión, autenticación y políticas de contraseña
- Acceso a recursos compartidos y permisos NTFS
- Creación de roles operativos (HelpDesk) y delegación de tareas administrativas
- Gestión del ciclo de vida de usuarios (reset, desbloqueo, cambios)
- Auditoría de eventos críticos en el visor de sucesos