

# M5 – P4: Ataque a GPOs mal configuradas en Active Directory

## Objetivos del laboratorio

- Entender qué permisos sobre una GPO permiten modificarla. (auditoría con `Get-GPPermission`). Simular abuso de una GPO mal delegada inyectando un **payload inocuo** (archivo marcador que se crea al aplicar la GPO).
- Detectar la manipulación mediante: (a) cambios en `SYSVOL`, (b) eventos de Directorio (Event ID 5136), (c) verificación en el equipo de destino.
- Proponer y aplicar mitigaciones: revisión de permisos, auditoría, AppLocker/Defender, controles de cambio.

## Entorno recomendado

- DC: Windows Server (ej. 2019/2022), dominio `corp.local`.
- OU con equipos de laboratorio (máquinas Windows clientes).
- Cuenta `soportel@corp.local` a la que se delega **permiso de edición** sobre la GPO de laboratorio.
- Máquina alumno: Windows 10/11 en la OU.

## Preparación (en controlador, con cuenta administrativa)

### 1) Preparativos previos (en DC)

Asegurarse de abrir PowerShell **como administrador** en el DC y de tener instalados/importados los módulos necesarios:

```
# Importar módulos (si no están cargados automáticamente)
Import-Module GroupPolicy
Import-Module ActiveDirectory
```

El módulo `GroupPolicy` contiene `New-GPO`, `Set-GPPermission`, `Get-GPPermission`; `ActiveDirectory` contiene `New-ADUser`.

### 2) Crear OU de laboratorio y contenedor de usuarios (opcional)

Si se quiere un entorno limpio para el laboratorio, cree una OU para equipos y una OU para usuarios:

```
# Crear OU para equipos de laboratorio
New-ADOrganizationalUnit -Name "LabComputers" -Path "DC=corp,DC=local"

# Crear OU para usuarios de laboratorio
New-ADOrganizationalUnit -Name "LabUsers" -Path "DC=corp,DC=local"
```

Usar OU separadas facilita enlazar la GPO solo a los equipos de laboratorio.

### 3) Crear la GPO de laboratorio: ControlUsuarios

Crear la GPO que se usará en la práctica:

```
# Crear GPO y guardar el objeto en una variable
$gpo = New-GPO -Name "ControlUsuarios" -Comment "GPO laboratorio: ControlUsuarios (práctica)"
$gpo.DisplayName; $gpo.Id.Guid
```

New-GPO crea la GPO. El objeto devuelto contiene el `Id` (GUID) necesario si más tarde se quiere manipular su carpeta en SYSVOL.

```
PS C:\Users> $gpo = New-GPO -Name "ControlUsuarios" -Comment "GPO laboratorio: ControlUsuarios (práctica)"
PS C:\Users> $gpo.DisplayName; $gpo.Id.Guid
ControlUsuarios
054619a9-6704-4ed2-ae8f-238929a12a76
PS C:\Users>
```

### 4) Enlazar la GPO a la OU de equipos, recomendado

Para que la GPO aplique a los equipos de laboratorio, crear un enlace a la OU:

```
# Ejemplo: enlazar la GPO a la OU "LabComputers"
New-GPLink -Name "ControlUsuarios" -Target "OU=LabComputers,DC=corp,DC=local" -
LinkEnabled Yes
```

New-GPLink enlaza la GPO al contenedor especificado. Si se omite este paso, la GPO no se aplicará a las máquinas hasta que esté enlazada al dominio/OU/ site correspondiente.

```
PS C:\Users> New-GPLink -Name "ControlUsuarios" -Target "OU=LabComputers,DC=corp,DC=local" -LinkEnabled Yes

GpoId       : 054619a9-6704-4ed2-ae8f-238929a12a76
DisplayName : ControlUsuarios
Enabled     : True
Enforced    : False
Target      : OU=LabComputers,DC=corp,DC=local
Order       : 1

PS C:\Users>
```

### 5) Crear el usuario de laboratorio soporte1

Crear una cuenta de usuario en la OU `LabUsers` o en `Users` si se prefiere:

```
# Contraseña segura de ejemplo para laboratorio (cambiarla en entornos reales)
$pass = ConvertTo-SecureString 'P@ssw0rd123' -AsPlainText -Force
```

```
# Crear el usuario en la OU LabUsers
New-ADUser -Name "Soporte 1" `
-SamAccountName "soporte1" `
-UserPrincipalName "soporte1@corp.local" `
-AccountPassword $pass `
-Enabled $true `
-Path "OU=LabUsers,DC=corp,DC=local" `
-Description "Cuenta de soporte para laboratorio (no usar en producción)"
```

Verificar la creación:

```
Get-ADUser -Identity "soporte1" -Properties * | Select-Object SamAccountName,
DistinguishedName, Enabled
```

New-ADUser crea la cuenta; la contraseña en el ejemplo es para laboratorio aislado únicamente.

```
PS C:\Users> Get-ADUser -Identity "soporte1" -Properties * | Select-Object SamAccountName, DistinguishedName, Enabled
```

| SamAccountName | DistinguishedName                    | Enabled |
|----------------|--------------------------------------|---------|
| soporte1       | CN=Soporte,CN=Users,DC=corp,DC=local | True    |

Activar Windows

## 6) Delegar permiso de edición sobre la GPO a soporte1

Ahora asignamos la delegación que simula el error: dar GpoEdit a un usuario no administrador.

Ejecutar desde el DC con una cuenta con permisos para modificar GPOs:

```
Set-GPPermission -Name "ControlUsuarios" -TargetName "soporte1" -TargetType User -
PermissionLevel GpoEdit
```

- o -Name identifica la GPO por su display name.
- o -TargetName es el nombre del trustee (usuario/grupo/computer). Se puede usar DOMINIO\soporte1 o sólo soporte1.
- o -PermissionLevel GpoEdit otorga permisos para editar la GPO, incluye la posibilidad de modificar scripts, plantillas, etc..
- o Por defecto, si el usuario ya tuviera un permiso mayor, la acción no reduce permisos existentes; usar -Replace si se quiere forzar reemplazo.

```
PS C:\Users> Set-GPPermission -Name "ControlUsuarios" -TargetName "soportel" -TargetType User -PermissionLevel GpoEdit

DisplayName      : ControlUsuarios
DomainName       : corp.local
Owner            : CORP\Admins. del dominio
Id               : 054619a9-6704-4ed2-ae8f-238929a12a76
GpoStatus        : AllSettingsEnabled
Description       : GPO laboratorio: ControlUsuarios (práctica)
CreationTime     : 26/09/2025 22:25:17
ModificationTime : 26/09/2025 22:25:16
UserVersion      : Versión de AD: 0; versión del volumen del sistema: 0
ComputerVersion  : Versión de AD: 0; versión del volumen del sistema: 0
WmiFilter        :

PS C:\Users>
```

## 7) Verificar permisos aplicados a la GPO

Comprobar que la delegación quedó aplicada:

```
# Mostrar todas las entradas de permisos de la GPO
Get-GPPermission -Name "ControlUsuarios" -All
```

Se debería obtener una entrada para `soportel` con `PermissionLevel = GpoEdit`.

```
PS C:\Users> Get-GPPermission -Name "ControlUsuarios" -All

Trustee      : Usuarios autenticados
TrusteeType   : WellKnownGroup
Permission    : GpoApply
Inherited     : False

Trustee      : Admins. del dominio
TrusteeType   : Group
Permission    : GpoEditDeleteModifySecurity
Inherited     : False

Trustee      : suportel
TrusteeType   : User
Permission    : GpoEdit
Inherited     : False

Trustee      : Administradores de empresas
TrusteeType   : Group
Permission    : GpoEditDeleteModifySecurity
Inherited     : False

Trustee      : ENTERPRISE DOMAIN CONTROLLERS
TrusteeType   : WellKnownGroup
Permission    : GpoRead
Inherited     : False

Trustee      : SYSTEM
TrusteeType   : WellKnownGroup
Permission    : GpoEditDeleteModifySecurity
Inherited     : False

PS C:\Users>
```

Si quieres filtrar por ese usuario:

```
Get-GPPermission -Name "ControlUsuarios" -TargetName "soportel" -TargetType User
```

Donde `Get-GPPermission` lista permisos sobre GPOs.

```
PS C:\Users> Get-GPPermission -Name "ControlUsuarios" -TargetName "soportel" -TargetType User

Trustee      : suportel
TrusteeType  : User
Permission   : GpoEdit
Inherited    : False
```

## 8) Eliminar o retirar permisos para revertir la delegación

Si después se quiere quitar el permiso delegado, se puede establecer `PermissionLevel` a `None` y usar `-Replace`:

```
# Quitar permisos de suportel
Set-GPPermission -Name "ControlUsuarios" -TargetName "soportel" -TargetType User -
PermissionLevel None -Replace
```

Verificar de nuevo con `Get-GPPermission`. Nota: `None` elimina la entrada para ese trustee en la GPO.

## Notas de seguridad y didácticas

- **Solo en laboratorio aislado:** ninguna cuenta creada o permiso modificado debe aplicarse en producción. Usar snapshots antes de la práctica para poder revertir rápidamente.
- **Payloads inofensivos:** para la demostración de ejecución posterior, usar scripts que sólo creen un fichero marcador, no crear cuentas ni añadir administradores.
- **Auditoría:** habilitar, temporalmente, la auditoría Directory Service Changes para que se puedan ver Event ID 5136 cuando una GPO es modificada.

## Referencias oficiales

- `Set-GPPermission` (doc Microsoft — sintaxis, `PermissionLevel` values, `Replace`). <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/set-gppermission?view=windowsserver2025-ps>
- `New-GPO` (crear GPOs con PowerShell). <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/new-gpo?view=windowsserver2025-ps>
- `Get-GPPermission` (listar permisos en una GPO). <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gppermission?view=windowsserver2025-ps>
- `New-ADUser` (crear usuarios en Active Directory con PowerShell). <https://learn.microsoft.com/en-us/powershell/module/activedirectory/new-aduser?view=windowsserver2025-ps>

- New-GPLink (enlazar GPO a OU/domain/site). <https://learn.microsoft.com/en-us/powershell/module/grouppolicy/new-gplink?view=windowsserver2025-ps>

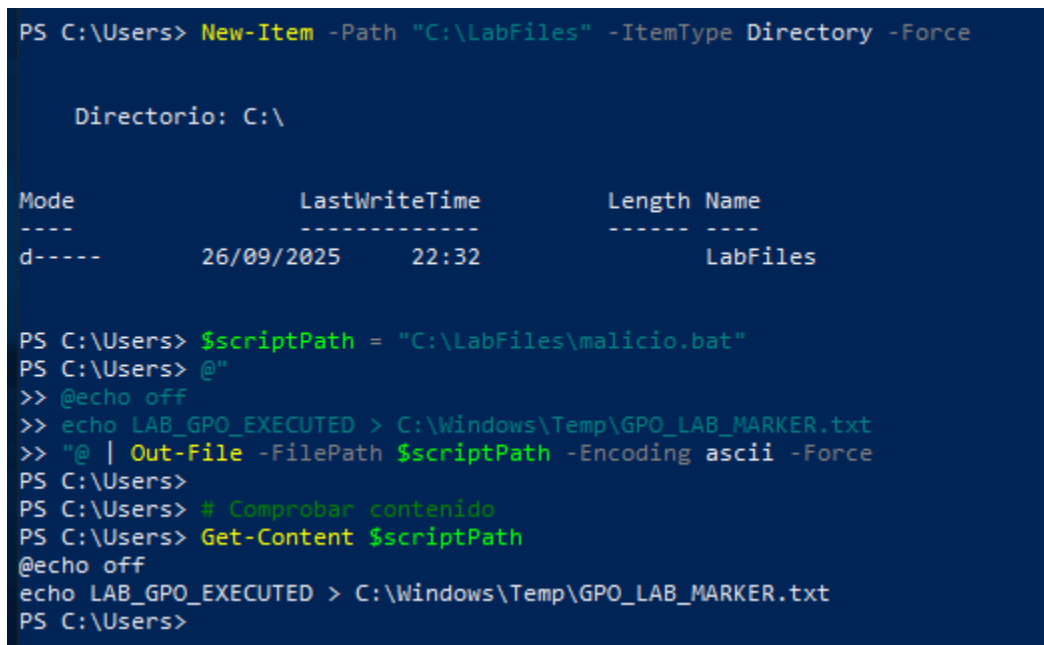
## A. Crear el script benigno en el DC

1. En el controlador de dominio, crea una carpeta temporal para archivos de laboratorio, si no existe:

```
New-Item -Path "C:\LabFiles" -ItemType Directory -Force
```

2. Crear el fichero malicio.bat con el contenido inocuo:

```
$scriptPath = "C:\LabFiles\malicio.bat"  
@"  
@echo off  
echo LAB_GPO_EXECUTED > C:\Windows\Temp\GPO_LAB_MARKER.txt  
"@ | Out-File -FilePath $scriptPath -Encoding ascii -Force  
  
# Comprobar contenido  
Get-Content $scriptPath
```



```
PS C:\Users> New-Item -Path "C:\LabFiles" -ItemType Directory -Force  
  
Directorio: C:\  
  
Mode                LastWriteTime         Length Name  
----                -  
d-----          26/09/2025   22:32             LabFiles  
  
PS C:\Users> $scriptPath = "C:\LabFiles\malicio.bat"  
PS C:\Users> @"  
>> @echo off  
>> echo LAB_GPO_EXECUTED > C:\Windows\Temp\GPO_LAB_MARKER.txt  
>> "@ | Out-File -FilePath $scriptPath -Encoding ascii -Force  
PS C:\Users>  
PS C:\Users> # Comprobar contenido  
PS C:\Users> Get-Content $scriptPath  
@echo off  
echo LAB_GPO_EXECUTED > C:\Windows\Temp\GPO_LAB_MARKER.txt  
PS C:\Users>
```

El .bat escribe un texto marcador en la ruta C:\Windows\Temp\GPO\_LAB\_MARKER.txt del equipo cliente cuando se ejecute en contexto SYSTEM al arranque. Ejecutar en DC sólo para preparar el archivo.

Referencia general sobre scripts GPO y tipos de scripts: Microsoft — *Using Startup, Shutdown, Logon, and Logoff Scripts*. <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196%28v%3Dws.11%29>

## B. Copiar el script al contenedor de la GPO en SYSVOL

Los componentes de una GPO quedan en AD y en la carpeta replicada SYSVOL. Los scripts de máquina (Startup/Shutdown) se colocan en ...\\Policies\\{GPO\_GUID}\\Machine\\Scripts\\Startup\\. Primero obtenemos el GUID de la GPO, luego copiamos el archivo.

1. Obtener GUID de la GPO, ejecutar en el DC con módulo GroupPolicy:

```
Import-Module GroupPolicy
$gpo = Get-GPO -Name "ControlUsuarios"
$gpo.Id.Guid
```

Get-GPO devuelve el objeto GPO y su Id.

```
PS C:\Users> Import-Module GroupPolicy
PS C:\Users> $gpo = Get-GPO -Name "ControlUsuarios"
PS C:\Users> $gpo.Id.Guid
054619a9-6704-4ed2-ae8f-238929a12a76
PS C:\Users> █
```

054619a9-6704-4ed2-ae8f-238929a12a76

2. Construir ruta SYSVOL y copiar el fichero:

```
$guid = $gpo.Id.Guid
$destDir = "\\corp.local\SYSVOL\corp.local\Policies\{$guid}\Machine\Scripts\Startup"
# Asegurar que exista la carpeta (si no existe, crearla)
if (-not (Test-Path $destDir)) { New-Item -Path $destDir -ItemType Directory -Force }
```

```
PS C:\Users> if (-not (Test-Path $destDir)) { New-Item -Path $destDir -ItemType Directory -Force }

Directorio: \\corp.local\SYSVOL\corp.local\Policies\{054619a9-6704-4ed2-ae8f-238929a12a76}\Machine\Scripts

Mode                LastWriteTime         Length Name
----                -
d-----         26/09/2025    22:38             Startup

PS C:\Users> █
```

Copiar el script

```
Copy-Item -Path "C:\LabFiles\malicio.bat" -Destination (Join-Path $destDir "malicio.bat") -Force
```

Verificar

```
Get-ChildItem -Path $destDir
```

```
PS C:\Users> Copy-Item -Path "C:\labFiles\malicio.bat" -Destination (Join-Path $destDir "malicio.bat") -Force
PS C:\Users> Get-ChildItem -Path $destDir

Directorio: \\corp.local\SYSVOL\corp.local\Policies\{054619a9-6704-4ed2-ae8f-238929a12a76}\Machine\Scripts\Startup

Mode                LastWriteTime         Length Name
----                -
-a----         26/09/2025   22:33             70 malicio.bat

PS C:\Users>
```

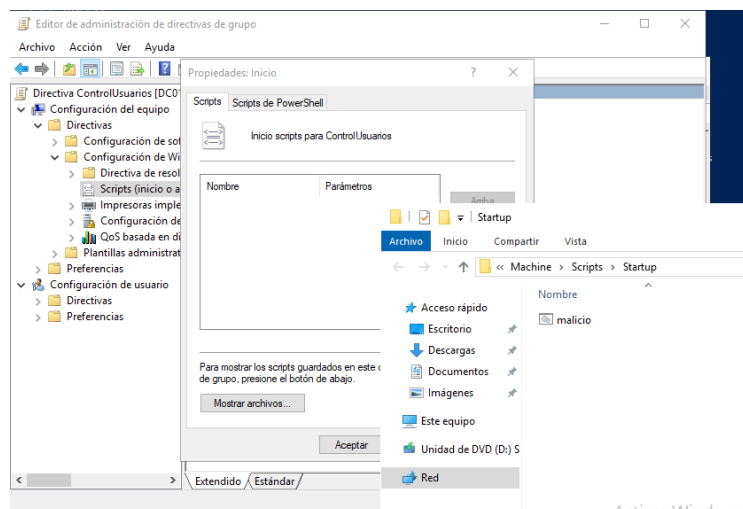
## Notas:

- La ruta UNC típica es  
\\<DOMINIO>\SYSVOL\<DOMINIO>\Policies\{GPO\_GUID}\Machine\Scripts\Startup\.
- SYSVOL es la carpeta replicada entre DCs.
- Si se refiere usar GPMC → *Edit* → *Scripts (Startup/Shutdown)* → *Show Files*, el botón *Show Files* abre esa carpeta y te permite copiar el script mediante GUI

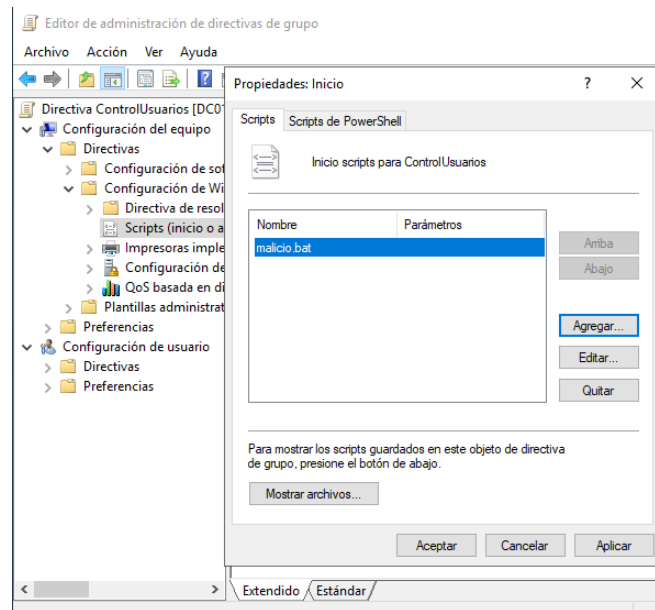
## C. Registrar el script en la GPO

La forma más clara y documentada para que el script quede registrado en la GPO es usar la consola **GPMC** (Group Policy Management Console), así se actualizan también los metadatos (*scripts.ini* / configuración interna).

- Abrir *gpmc.msc* en el DC o en una máquina con las RSAT instaladas.
- Navegar a: *Group Policy Objects* y hacer clic derecho en **ControlUsuarios** → **Edit**.
- En el editor de la GPO, ir a:  
*Computer Configuration* → *Policies* → *Windows Settings* → *Scripts (Startup/Shutdown)* → doble clic **Startup**.
- En la ventana *Startup Properties* → **Show Files**. Se abrirá la carpeta ...\\Machine\Scripts\Startup\ del GPO en el DC; confirmar que *malicio.bat* está presente. Si no estaba copiado, se puede arrastrar aquí.



5. En *Startup Properties* → **Add** → **Browse** → seleccionar `malicio.bat` → **OK** → **Apply** → **OK**.



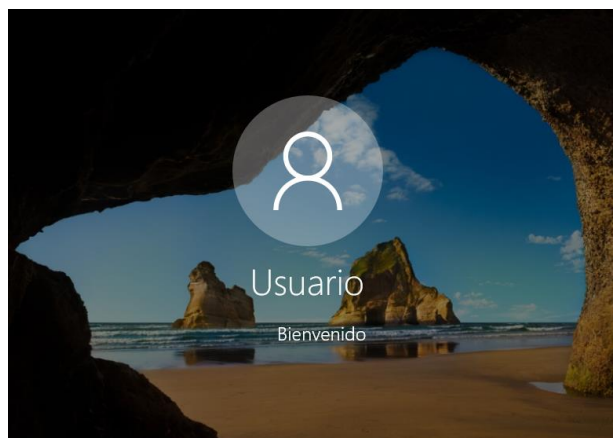
Al usar **Add** dentro del editor de GPO se asegura que la GPO registra el script en su `scripts.ini` y en los metadatos; copiar solo el archivo a `SYSDVOL` sin registrar puede no ser suficiente para que la GPO lo ejecute. La documentación de Microsoft describe el proceso de añadir scripts a la GPO via GPMC y el uso de *Show Files*.

## D. Forzar aplicación y verificación en la máquina cliente (alumno)

En la máquina cliente, unida al dominio y que pertenezca a la OU enlazada a la GPO:

1. Forzar actualización como administrador en la máquina cliente:

```
gpupdate /force
# o reiniciar el equipo para que se ejecute el Startup script (se ejecuta en contexto SYSTEM)
```



## 2. Verificar que el marcador fue creado:

```
Test-Path C:\Windows\Temp\GPO_LAB_MARKER.txt  
Get-Content C:\Windows\Temp\GPO_LAB_MARKER.txt
```

```
PS C:\Users\usuario1> Test-Path C:\Windows\Temp\GPO_LAB_MARKER.txt  
True  
PS C:\Users\usuario1> Get-Content C:\Windows\Temp\GPO_LAB_MARKER.txt  
LAB_GPO_EXECUTED  
PS C:\Users\usuario1>
```

Si el archivo existe y contiene LAB\_GPO\_EXECUTED, el script se ejecutó correctamente en contexto SYSTEM al aplicar la GPO. Recordar: *Startup* scripts se ejecutan en el arranque y con privilegios del sistema.

Si no existe comprobar en DC el OU

```
Get-ADComputer -Identity DESKTOP-CV3RQ72 | Select-Object Name, DistinguishedName
```

```
PS C:\Users> Get-ADComputer -Identity DESKTOP-CV3RQ72 | Select-Object Name, DistinguishedName  
  
Name           DistinguishedName  
----           -  
DESKTOP-CV3RQ72 CN=DESKTOP-CV3RQ72, OU=LabComputers, DC=corp, DC=local
```

Si no está ejecutar

```
Move-ADObject "CN=DESKTOP-CV3RQ72,CN=Computers,DC=corp,DC=local" `  
-TargetPath "OU=LabComputers,DC=corp,DC=local"
```

Y volver al paso 1

## E. Comprobaciones y resoluciones de problemas comunes

- Si el script no se ejecuta:
  - ¿La GPO está **enlazada** a la OU que contiene los equipos? Usa `Get-GPLink -Target "OU=LabComputers,DC=corp,DC=local"` para comprobar.
  - ¿Tiene el equipo permiso *Apply / Read* para la GPO (filtrado de seguridad)? Si se eliminó *Authenticated Users* del *Apply*, añadir la cuenta de equipo o *Security Group* correspondiente. (Si no se tiene permiso de *Apply* la GPO no se procesará).
  - ¿Se copió el script al folder correcto de *SYSDVOL* y se registró con *Add* en el editor de GPO? Copiar sin registrar puede dejar la GPO sin referencia a ese script.
- Para auditar/inspeccionar: se puede obtener un reporte de la GPO con `Get-GPOReport -Name "ControlUsuarios" -ReportType Html -Path C:\Temp\ControlUsuarios.html` y abrir el HTML para revisar la sección *Scripts/Startup*.

## Referencias principales

1. Microsoft — *Using Startup, Shutdown, Logon, and Logoff Scripts in Group Policy* (procedimiento en GPMC).  
<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196%28v%3Dws.11%29>
2. Microsoft — *Get-GPO (GroupPolicy) cmdlet* (obtener info y GUID de una GPO).  
<https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gpo?view=windowsserver2025-ps>
3. Microsoft — *Group Policy processing for Windows* (explica que partes de la GPO están en AD y en SYSVOL y cómo se replican).  
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-processing>
4. Semperis / análisis sobre scripts GPO y scripts.ini / SYSVOL (contexto operativo y seguridad).  
<https://www.semperis.com/blog/gpo-logon-script-security>
5. Varias guías prácticas que muestran cómo ejecutar PowerShell/batch como Startup script desde GPO.  
<https://woshub.com/running-powershell-startup-scripts-using-gpo/>

## Fase de validación, detección y registros.

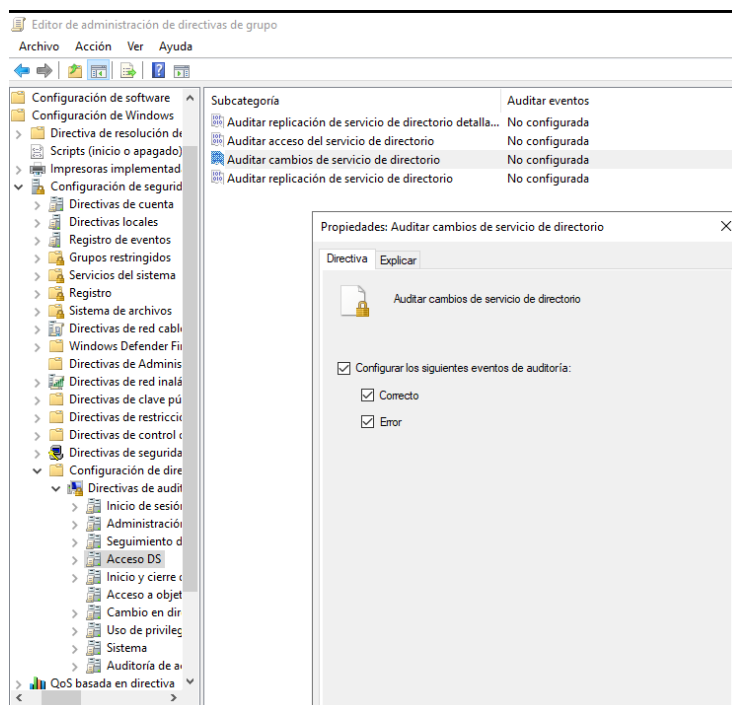
Esta parte es fundamental para comprobar:

1. Que el abuso **funcionó**, aunque el payload sea inocuo.
2. Qué **evidencias deja** en AD, en SYSVOL, en logs.
3. Cómo un administrador puede **detectar y corregir** la delegación indebida.

## Detección y registros

### 1. Cambios en Active Directory: Event ID 5136

- **Qué es:** cada vez que se modifica un objeto en AD, incluidas GPOs, se registra el **evento 5136** si se tiene habilitada la auditoría de **Directory Service Changes** en el DC.
- **Cómo habilitar** en el DC, GPO Default Domain Controllers Policy o una GPO específica sobre DCs:
  - Configuración de equipo → Políticas → Configuración de Windows → Configuración de seguridad → Configuración de directivas de auditoría avanzada → Directivas de Auditoría → Acceso DS → *Auditar cambios de servicio de directorio* → Activar éxito y fracaso.
- **Qué buscar en el visor de eventos en el menú Herramientas (Registro de Windows, Seguridad):**
  - Event ID: **5136**
  - SubjectUserName = el usuario que hizo el cambio (ej. soporte1).
  - ObjectDN = CN de la GPO modificada, p. ej.:
  - CN={GUID}, CN=Policies, CN=System, DC=corp, DC=local
- **Ejemplo práctico para alumnos:**  
Tras editar la GPO o registrar el script, que vayan al DC → *Visor de eventos* → *Security* y filtren por ID 5136.  
Allí deben identificarse que soporte1 fue quien modificó la GPO.



## 2. Monitorización de SYSVOL

- **Qué es:** SYSVOL almacena la parte “de archivos” de la GPO (scripts, plantillas ADM, etc.). Cualquier escritura en `\\<dominio>\SYSVOL\...` es un posible indicador de abuso.
- **En el laboratorio:**  
Revisar la fecha de modificación de la carpeta del script:

```
$gpo = Get-GPO -Name "ControlUsuarios"
$guid = $gpo.Id.Guid
Get-ChildItem
"\\corp.local\SYSVOL\corp.local\Policies\{$guid}\Machine\Scripts\Startup" |
Select-Object Name, LastWriteTime
```

```
PS C:\Users> $gpo = Get-GPO -Name "ControlUsuarios"
PS C:\Users> $gpo = Get-GPO -Name "ControlUsuarios"
PS C:\Users> Get-ChildItem "\\corp.local\SYSVOL\corp.local\Policies\{$guid}\Machine\Scripts\Startup" |
>> Select-Object Name, LastWriteTime

Name                LastWriteTime
----                -
malicio.bat         26/09/2025 22:33:11

PS C:\Users>
```

- **En entornos reales:**
  - Se recomienda configurar un **FIM (File Integrity Monitoring)** o reglas en un SIEM/EDR que alerten cuando se cree o modifique un archivo en `SYSVOL\Policies\...\Scripts`.
  - Por ejemplo: un `.bat` nuevo en `Startup` o `Logon` debería ser investigado.

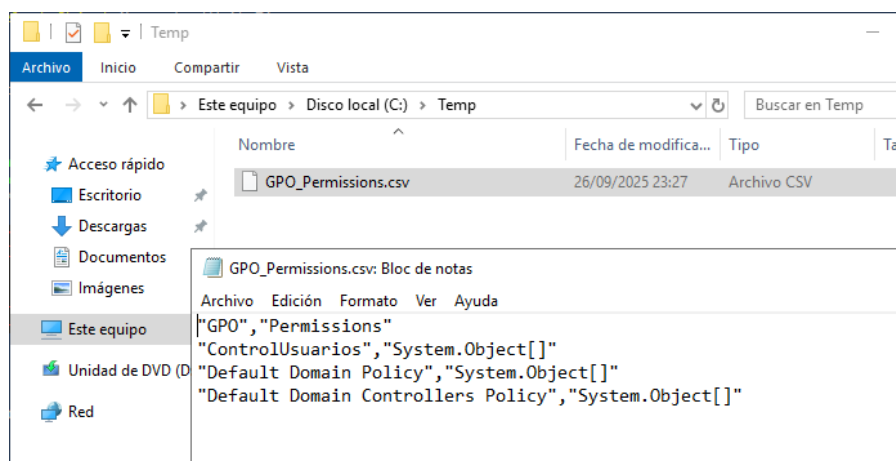
### 3. Revisión periódica de permisos de GPO

Un cambio de permisos mal controlado, como dar **GpoEdit** a un usuario no admin, es lo que permite este ataque.

#### Cómo detectarlo en PowerShell:

```
New-Item -Path "C:\Temp" -ItemType Directory -Force

Get-GPO -All | ForEach-Object {
    $name = $_.DisplayName
    $perms = Get-GPPermission -Name $name -All
    [PSCustomObject]@{ GPO=$name; Permissions=$perms }
} | Export-Csv C:\Temp\GPO_Permissions.csv -NoTypeInformation
```



En el laboratorio, se deben identificar que **soporte1** aparece con GpoEdit en ControlUsuarios.

### Resumen didáctico para tus alumnos

- **Validación:** Confirmar que el *payload* se ejecuta, archivo marcador.
- **Detección en AD:** Buscar eventos 5136 para cambios en objetos de GPO.
- **Detección en SYSVOL:** Revisar escrituras en carpetas de scripts de GPO.
- **Detección de delegación indebida:** Exportar permisos con Get-GPPermission.

### Material de apoyo y referencias

- SharpGPOAbuse: herramienta pública que muestra vector de abuso; revisar solo para contexto.  
<https://github.com/FSecureLABS/SharpGPOAbuse>
- Get-GPPermission / Set-GPPermission documentación Microsoft (PowerShell GroupPolicy).  
<https://learn.microsoft.com/en-us/powershell/module/grouppolicy/get-gppermision?view=windowsserver2025-ps>

- Event ID 5136: descripción y uso en auditoría de AD.  
<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5136>
- SYSVOL y ubicación de scripts GPO, Microsoft Q&A / docs explicando que scripts se almacenan en SYSVOL. <https://learn.microsoft.com/en-us/answers/questions/1516996/how-to-get-logon-scripts-distributed-by-gpo-in-loc>
- Buenas prácticas y hardening de Active Directory: revisión de privilegios, hosts administrativos seguros.  
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>