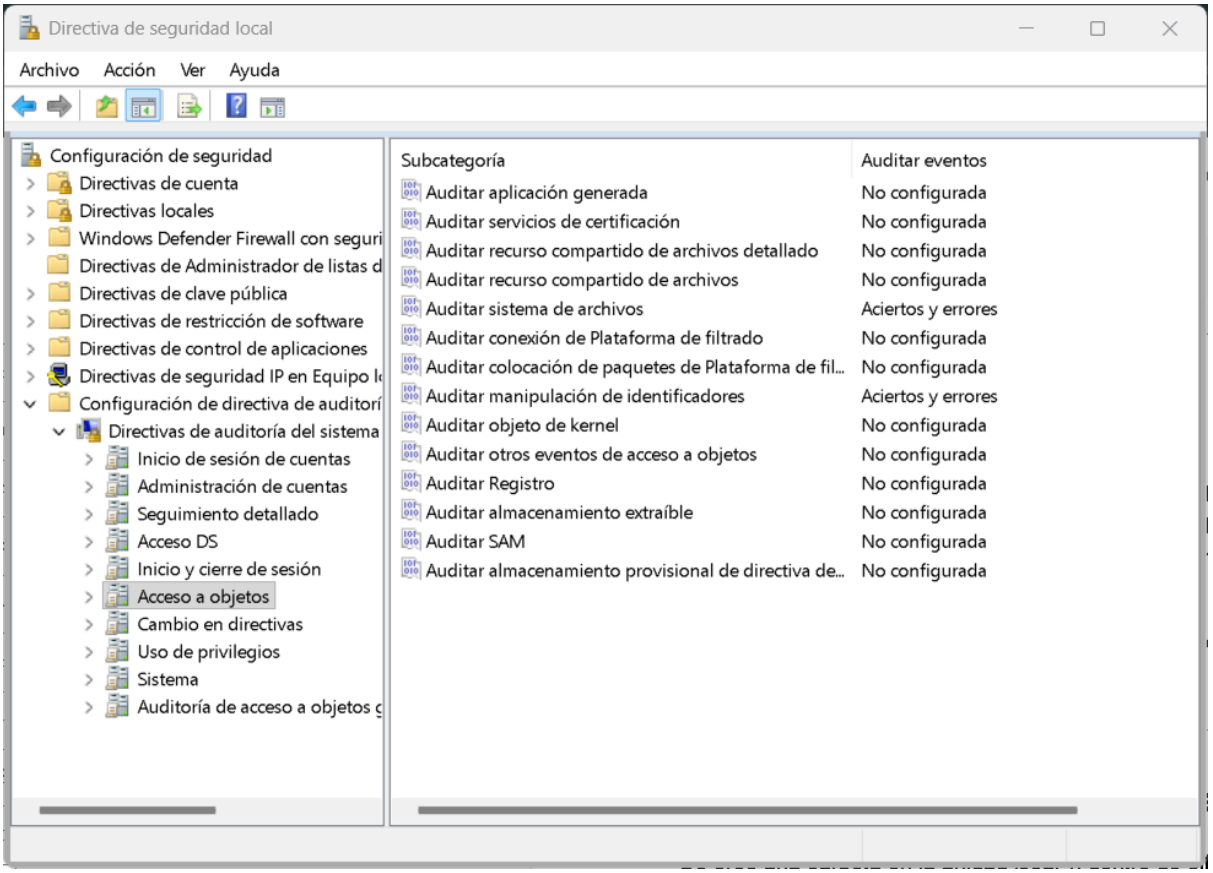
Práctica: Auditoría de Acceso a Objetos en Windows

1. Activación de la Directiva de Seguridad

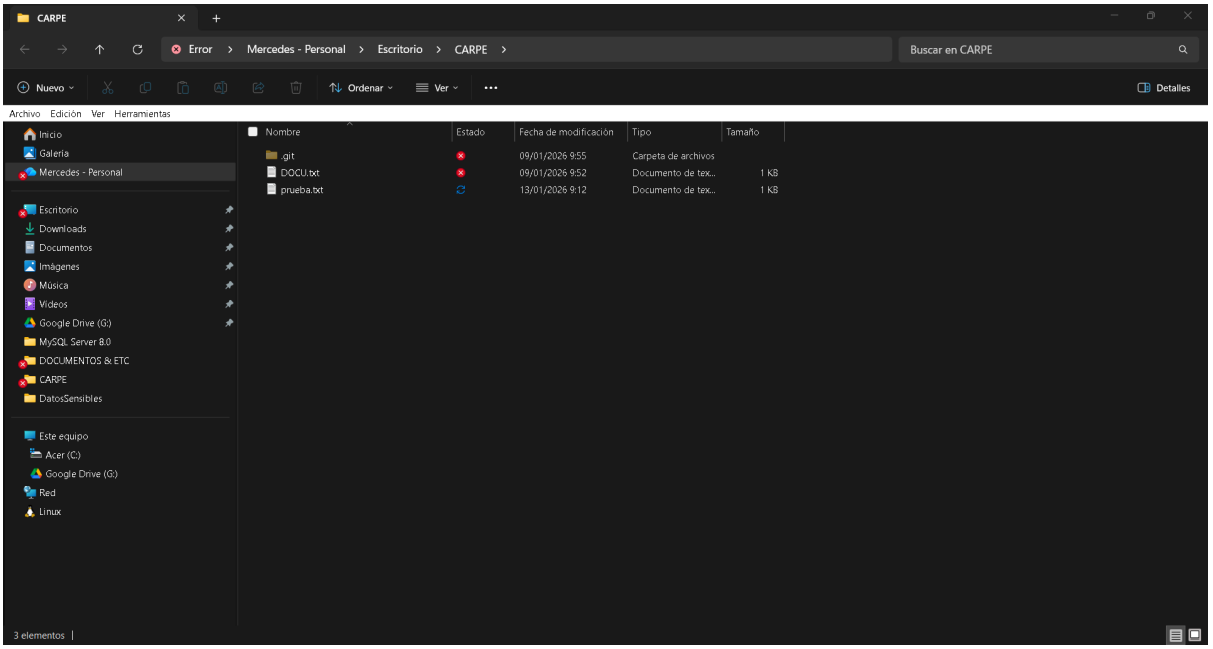
Para permitir el registro de eventos, se accedió a la "Directiva de seguridad local" *(secpol.msc*) y se activó la auditoría de acceso a objetos (o del sistema de archivos en la configuración avanzada). Se configuró para registrar tanto los eventos **Correctos** como los de **Error**.



2. Creación del Entorno de Prueba

Se creó una carpeta en la unidad local y, dentro de ella, un archivo de texto para realizar las pruebas de acceso.

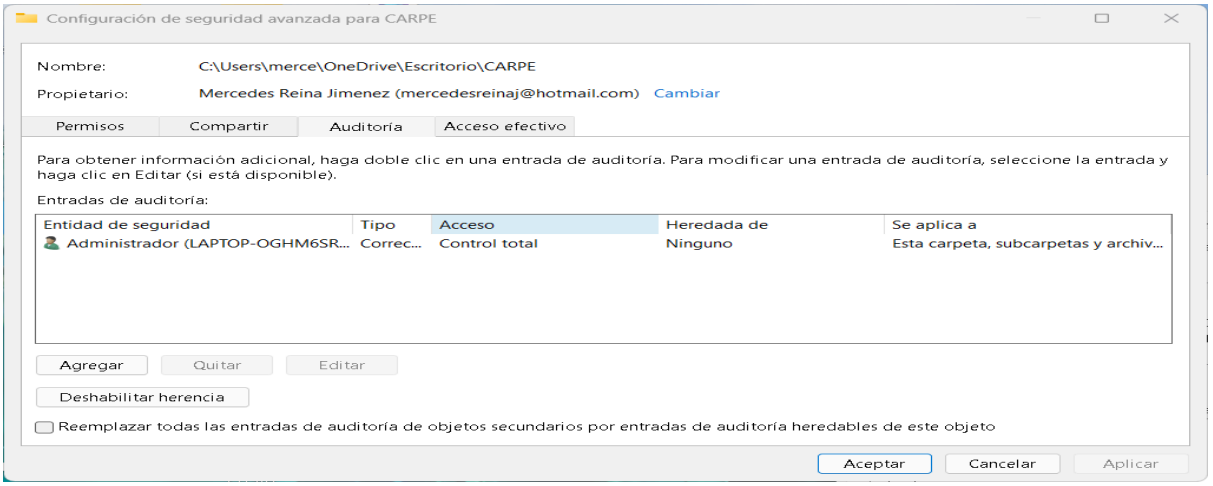
- **Ruta de la carpeta:** C:\Datos (o el nombre que hayas puesto)
- **Archivo:** Secreto.txt



---

3. Configuración de la Auditoría en la Carpeta (SACL)

Se configuraron las opciones avanzadas de seguridad de la carpeta para auditar las acciones del usuario. En la pestaña "Auditoría", se agregó una entrada para el usuario actual (abelreiinaa) monitorizando los permisos de escritura, lectura y eliminación.



4. Verificación de Eventos en el Registro de Seguridad

Tras realizar acciones sobre el archivo (abrir, modificar, guardar), se consultó el **Visor de Eventos** de Windows. Se filtró el registro de seguridad para localizar las acciones realizadas sobre el archivo creado.

A continuación se muestra la evidencia del acceso:

- **Evento ID:** 4656 / 4663
- **Usuario:** abelreiinaa
- **Objeto accedido:** [Ruta de tu archivo de texto]
- **Proceso:** notepad.exe (Bloc de notas)