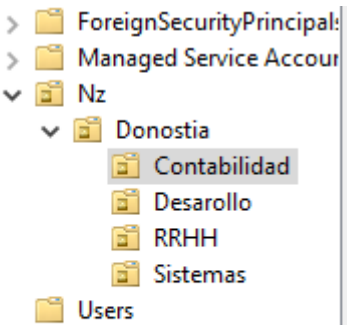


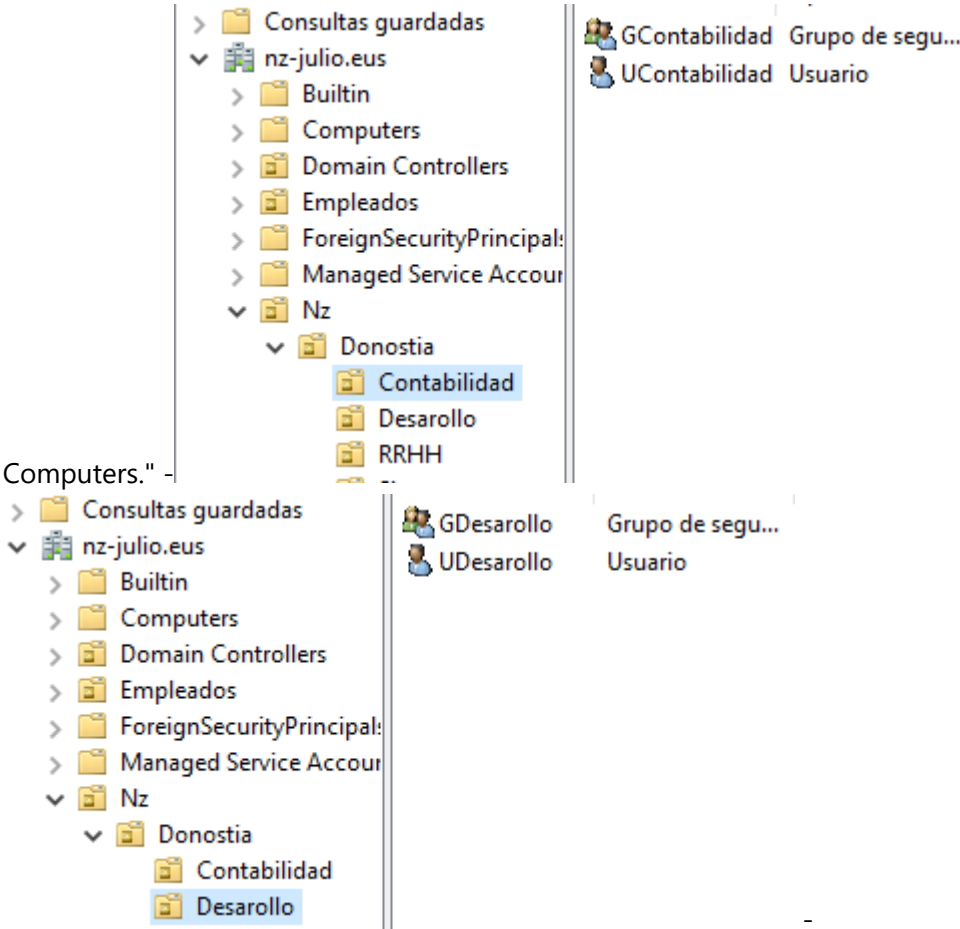
FILE SERVER

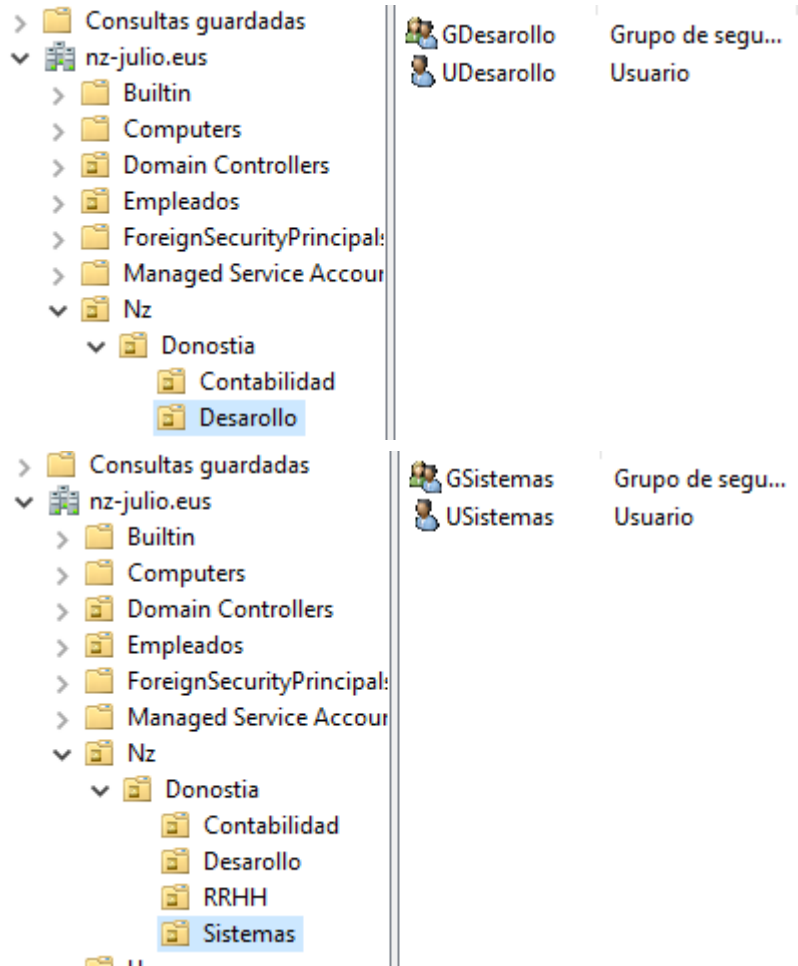


1. Crear la estructura de UO en tu servidor: -

2, 3, 4. Crear los grupos, Añadir usuarios a los grupos:

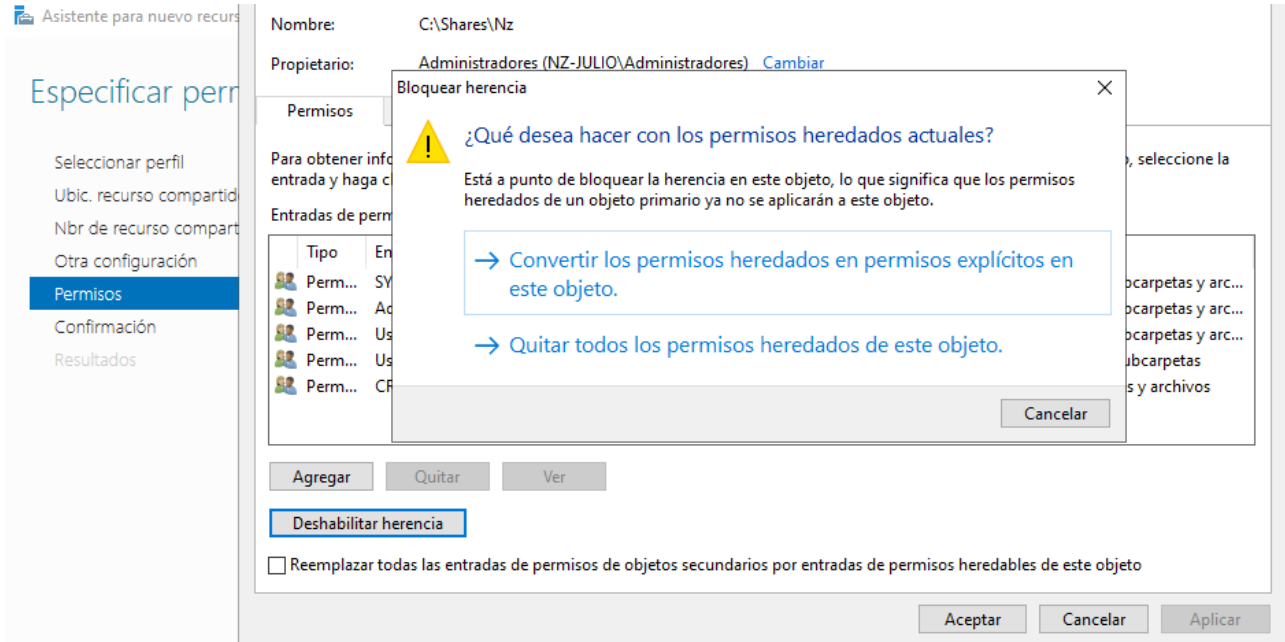
- Desde la misma herramienta "Active Directory Users and Computers," crear los grupos **GContabilidad**, GRRHH, GSistemas, GDesarrollo.
- Agrega usuarios a los grupos correspondientes utilizando la herramienta "Active Directory Users and





5. Deshabilitar herencia de permisos:

- En la configuración de recursos compartidos, especificando los permisos para el control de acceso, en permisos personalizados, deshabilitar la herencia. -



6. Habilitar enumeración basada en accesos:

- En los parametros de la configuracion de recursos compartidos habilitar las casilla -

Asistente para nuevo recurso compartido

Parámetros de configuración de recurso compartido

Seleccionar perfil

Ubic. recurso compartido

Nbr de recurso compart.

Otra configuración

Permisos

Confirmación

Resultados

☒ **Habilitar enumeración basada en el acceso**

La enumeración basada en acceso solamente muestra los archivos y carpetas para las que un usuario tiene permisos de acceso. Si un usuario no tiene permisos de lectura (o equivalente) para una carpeta, Windows oculta la carpeta desde la vista del usuario.

☒ **Permitir almacenamiento en caché del recurso compartido**

El almacenamiento en caché permite que los contenidos del recurso compartido estén disponibles para los usuarios sin conexión. Si el servicio de rol BranchCache para archivos de red está instalado, puede habilitar BranchCache en el recurso compartido.

☐ **Habilitar BranchCache en el recurso compartido de archivos**

BranchCache permite a los equipos en una sucursal guardar en caché archivos descargados desde este recurso compartido y, a continuación, permite que los archivos estén disponibles de forma segura en otros equipos de la sucursal.

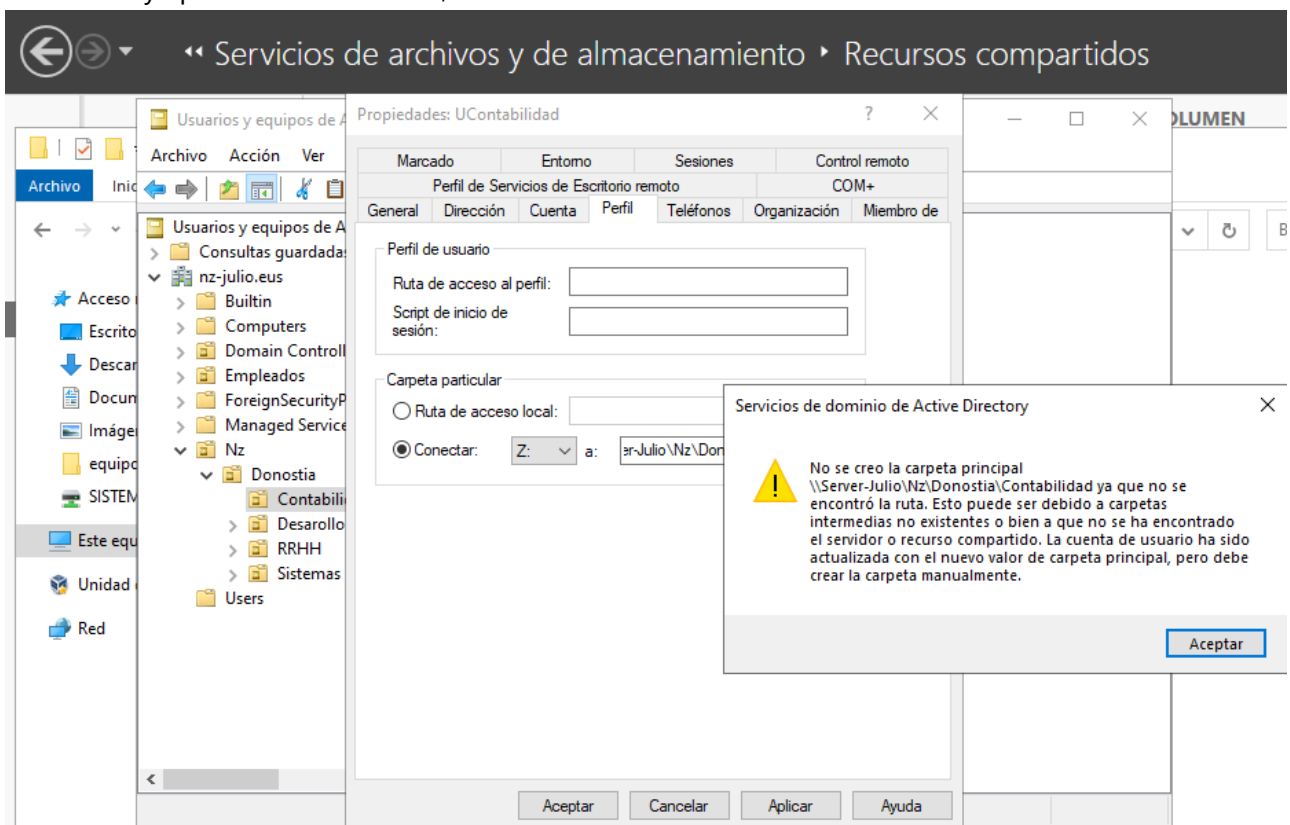
☐ **Cifrar acceso a datos**

Cuando esté habilitado, se cifrará el acceso a archivos remotos en este recurso compartido. Esto asegura los datos frente a un acceso no autorizado mientras se transfieren al recurso compartido o desde él. Si esta casilla está activada y atenuada, significa que el administrador activó el cifrado en todo el servidor.


< Anterior Siguiente > Crear Cancelar

7. Mapear unidades de red:

- Desde las propiedades del Miembro del Perfil seleccionamos la opción de conectar y la configuramos con la ruta y aplicamos los cambios, -



8. Mapear unidades de red desde el Active Directory: -Desde el Usuario en el explorador de archivos, nos conectamos a una unidad de red desde "Este equipo" y configuramos con el la ruta del recurso compartido compartido: -

←  Conectar a unidad de red

¿Qué carpeta de red desea asignar?

Especifique la letra de unidad para la conexión y la carpeta a la que desea conectarse:

Unidad:

Z:

Carpeta:

\\Server-Julio\Nz\Donostia\Contabilidad

Examinar...

Ejemplo: \\servidor\recurso_compartido

☒ Conectar de nuevo al iniciar sesión

☐ Conectar con otras credenciales

[Conectarse a un sitio web para usarlo como almacén de documentos e imágenes.](#)

Finalizar

Cancelar

9. Mapear unidades de red usando GPOs:

- En la herramientas de Servidor con la Adminictrasi3n de directaivas de Grupo Asignamos un controlador que creamos con la confugarici3n que aparece en pantalla. Para obtener los cambios Actualizaremos desde la terminal del servidor con el siguiente comando gpupdate /force -

Directiva Asignaci3n de Unidades Contabilidad [SERVER-JULIO.N

Configuraci3n del equipo

- Directivas
- Preferencias

Configuraci3n de usuario

- Directivas
- Preferencias
 - Configuraci3n de Windows
 - Aplicaciones
 - Asignaciones de unidades
 - Entorno
 - Archivos
 - Carpetas
 - Archivos .ini
 - Registro
 - Accesos directos
- Configuraci3n del Panel de control

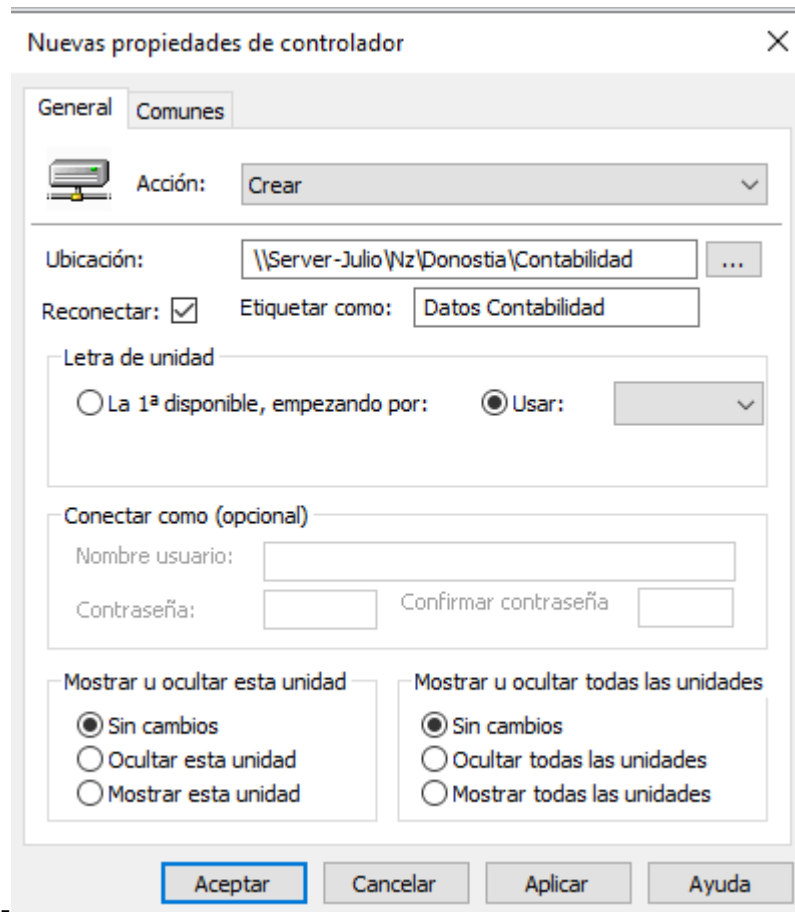
Asignaciones de unidades

Nombre	Orden	Acci3n	Ruta de acceso	Volver a conectar
No hay elementos disponibles en esta vista.				

Procesamiento

Descripci3n

No se seleccion3 ninguna directiva.



Administrador: Símbolo del sistema - gpupdate /force

```
Microsoft Windows [Versión 10.0.20348.587]
(c) Microsoft Corporation. Todos los derechos reservados.

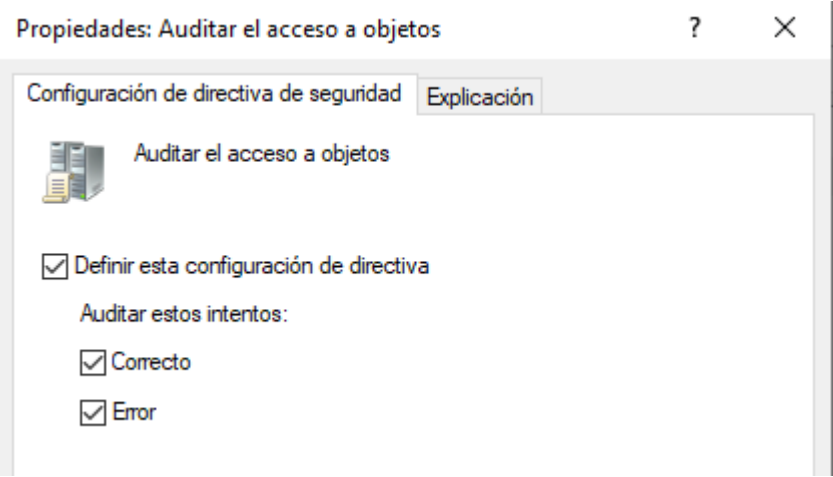
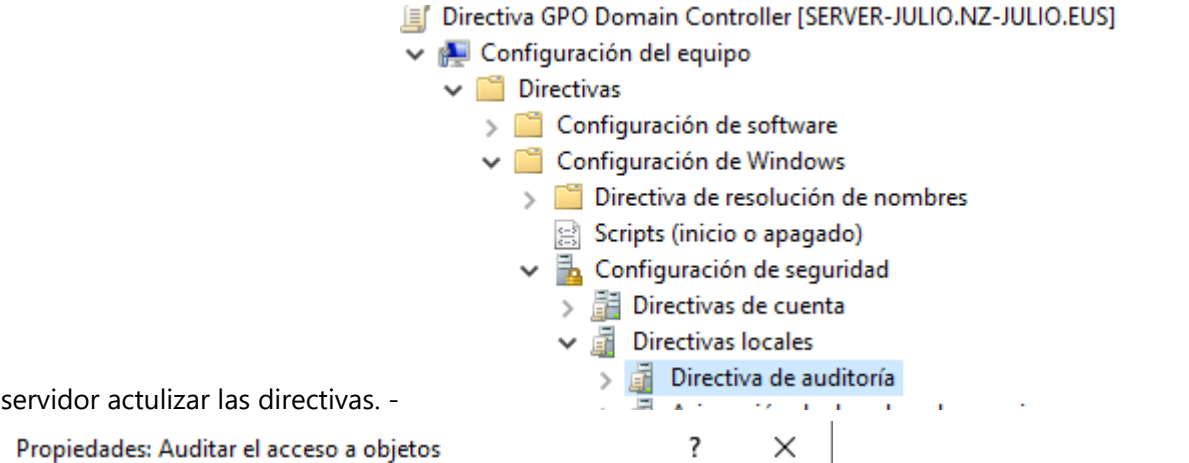
C:\Users\Administrador>gpupdate /force
Actualizando directiva...
```

Aclaración: Los

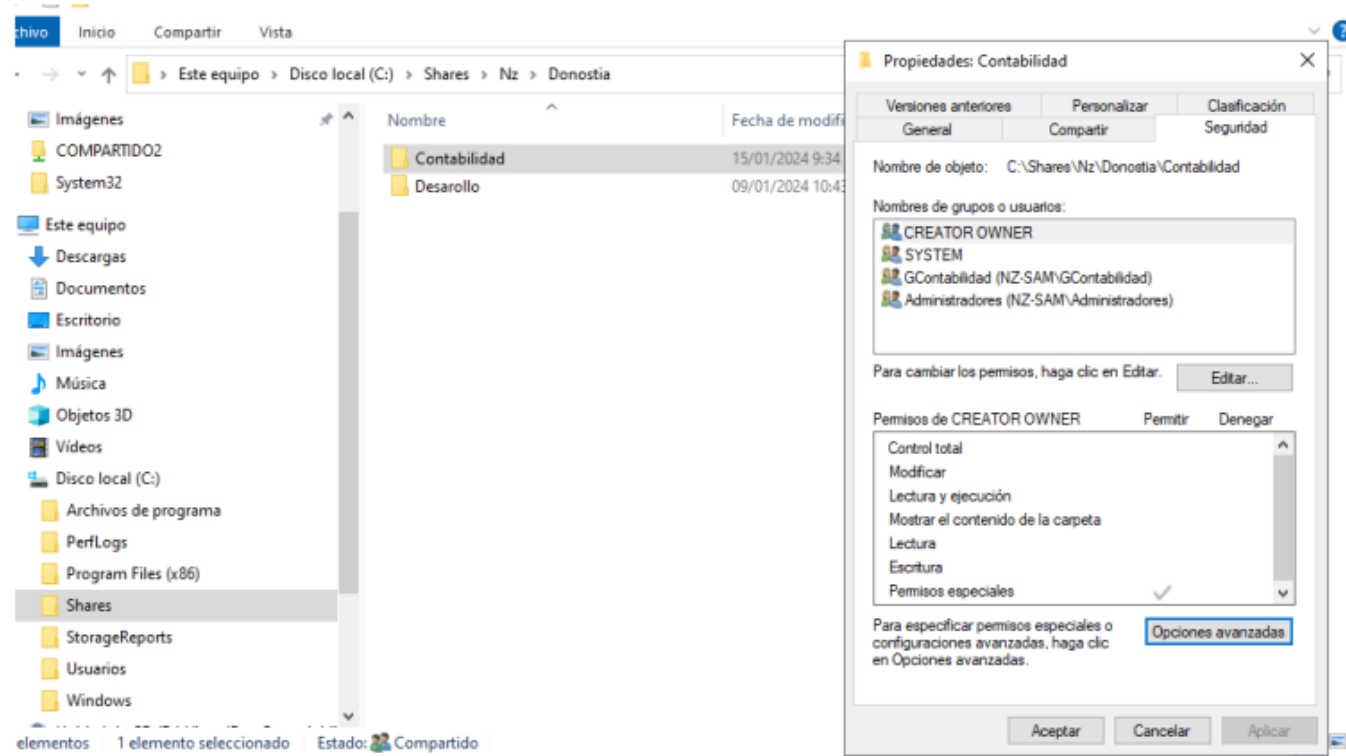
ejemplos del 7-9 solo se muestra con el caso de Contabilidad, el recurso compartido es /Nz/Donostia/...**

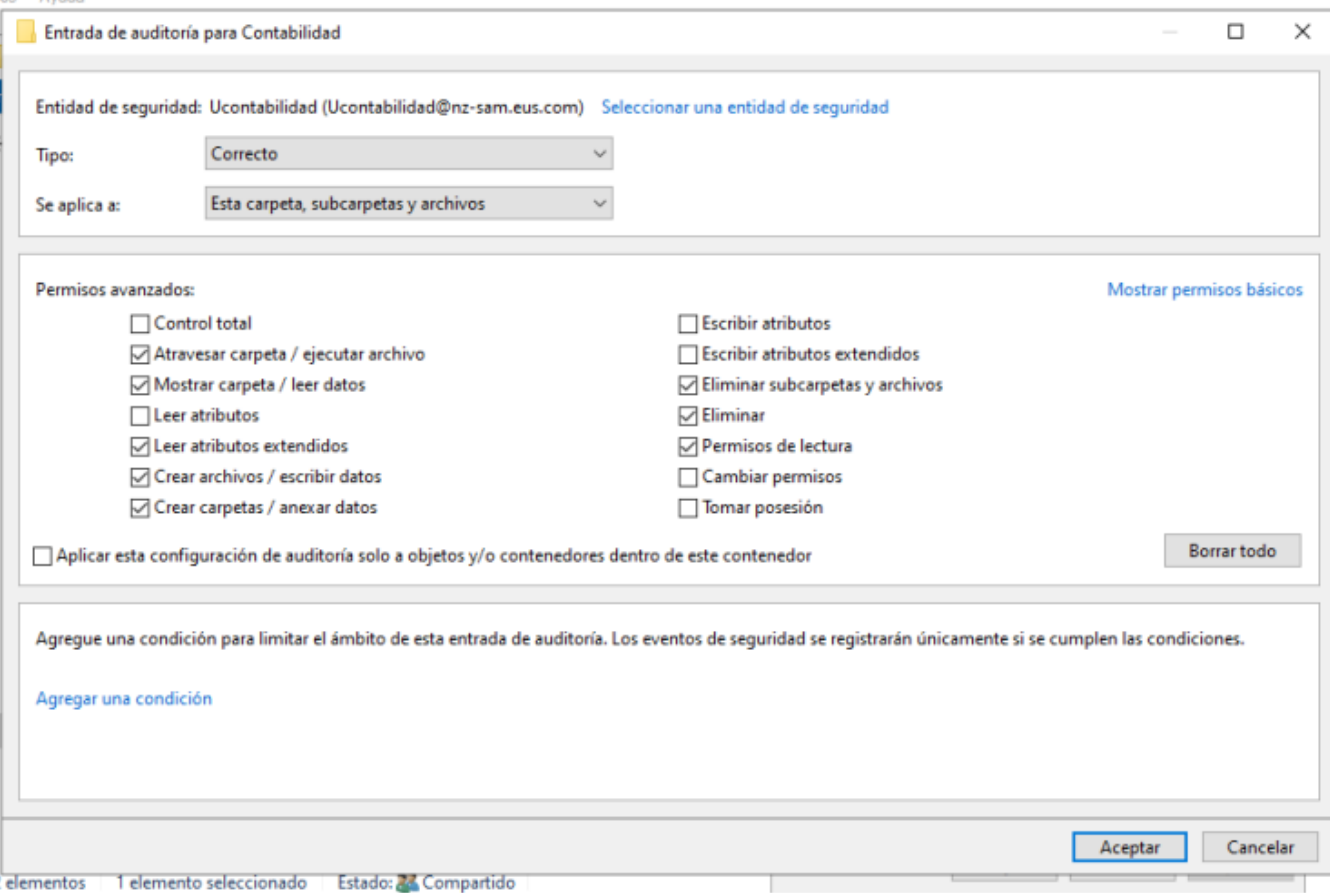
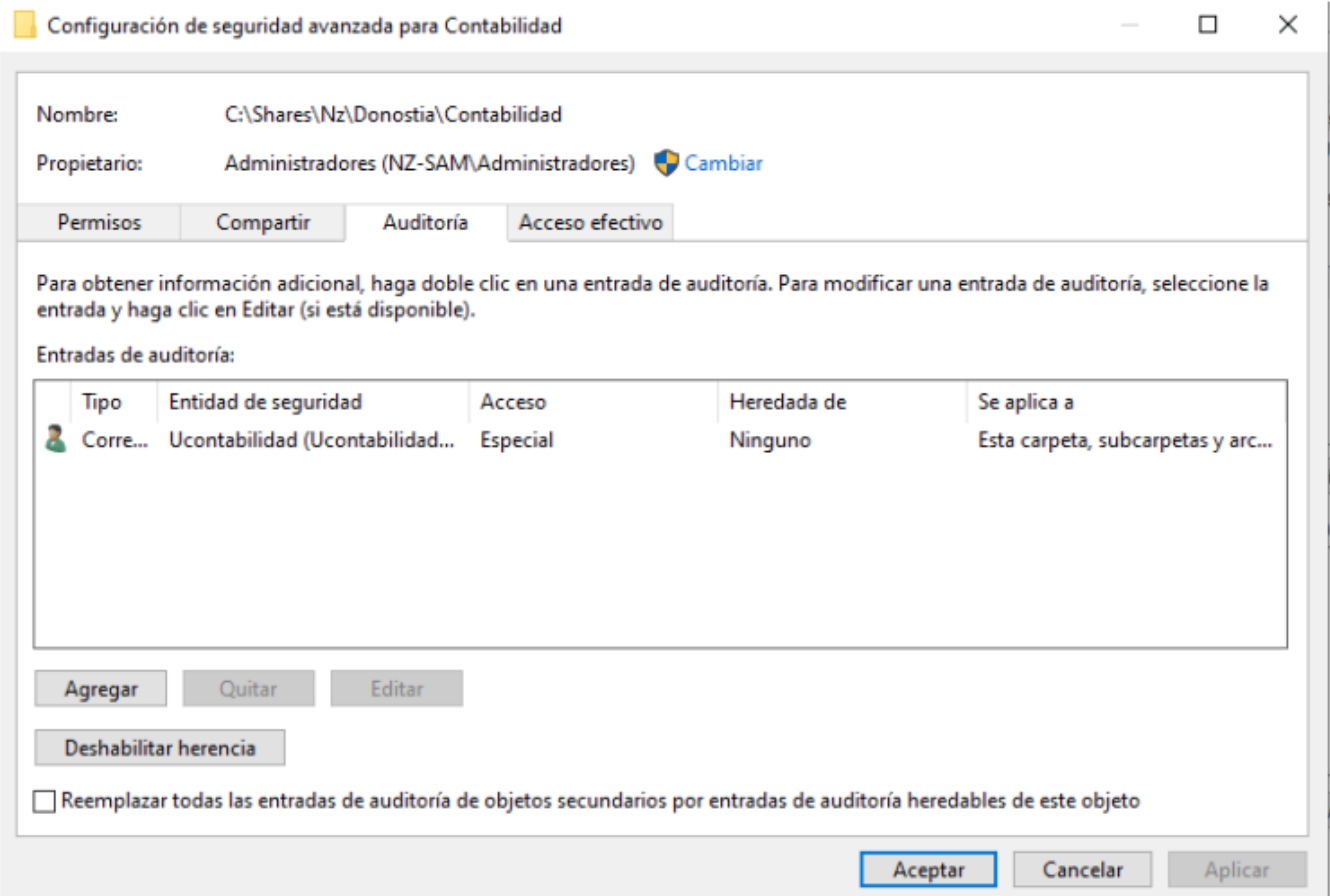
10. Habilitar la auditoría a nivel del controlador de dominio:

- Panel de servidor > Herramientas > Directivas a nivel de grupo. Ir donde se encuentra Directiva de Auditoría en Pantalla y configurar la primera directiva como aparece en pantalla. y Desde la terminal del

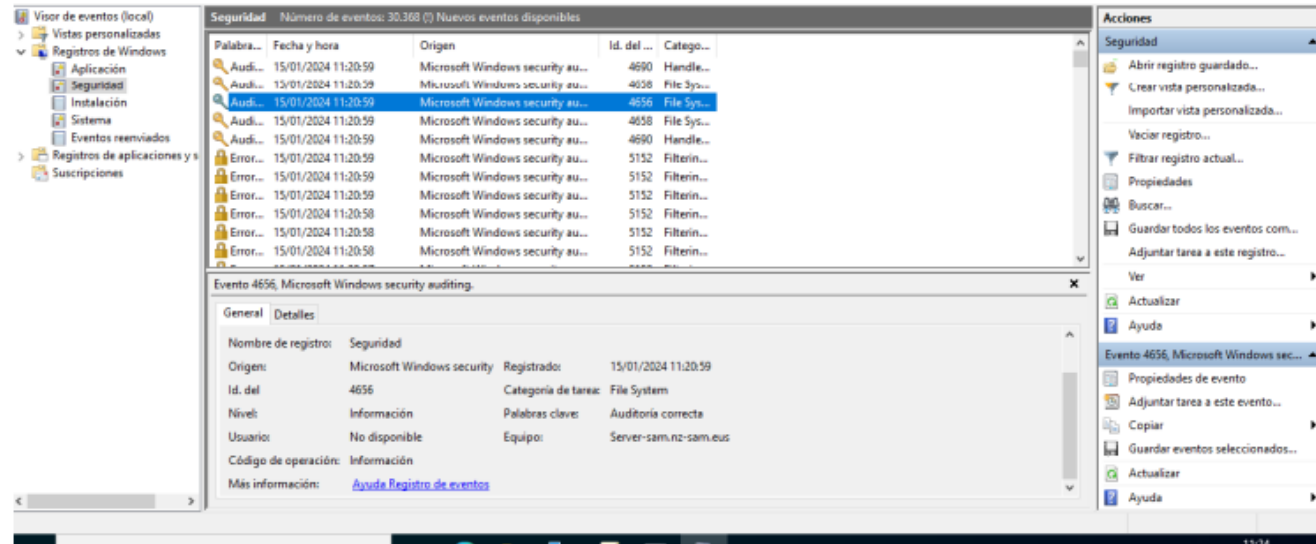
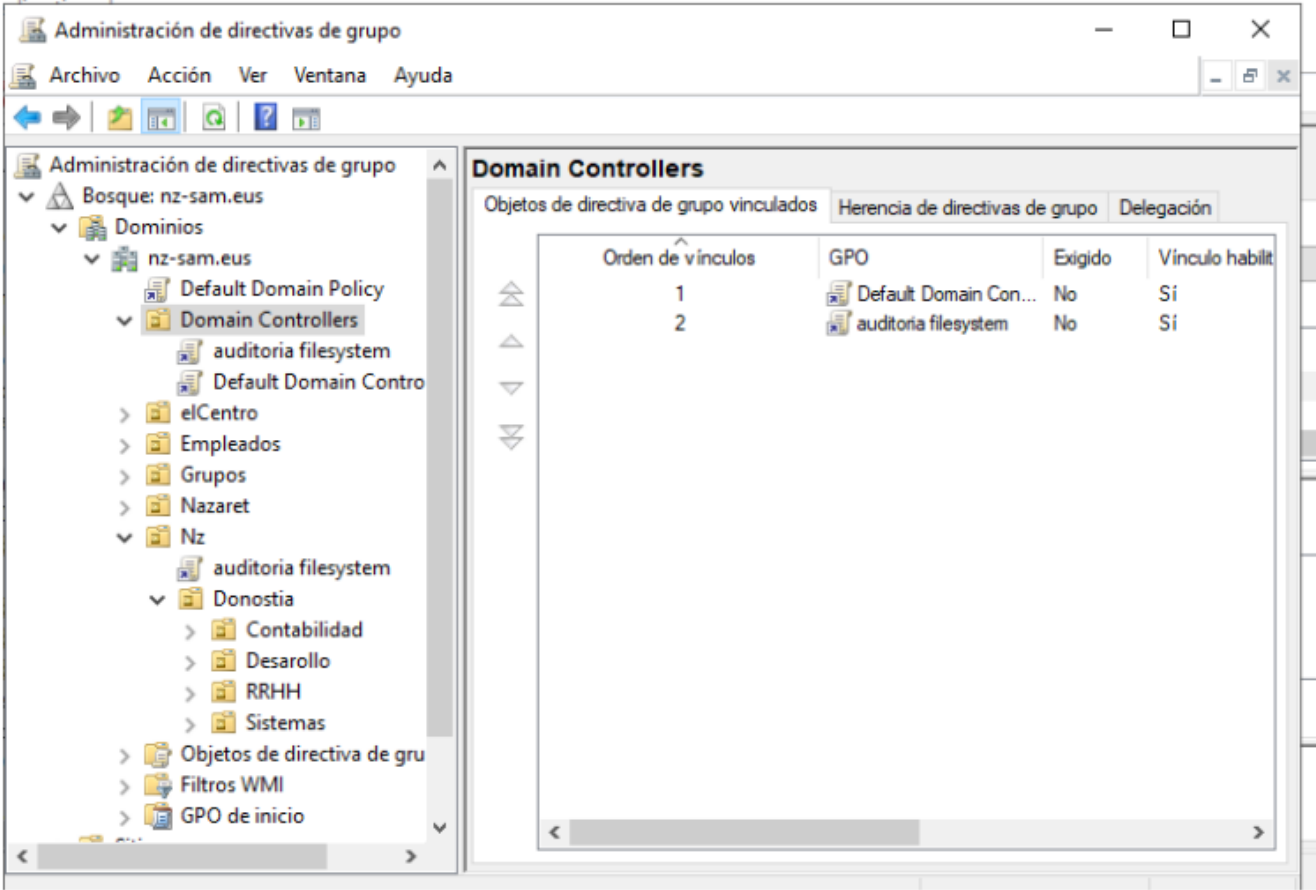


11,12. Habilitar la auditoría para un usuario específico en una carpeta, Probar eliminar archivos y crear carpetas: -





-Hay que crear una auditoria para Nz también, en Domain controllers -



-Aquí popdemos ver que el usuario UContabilidad solo puede acceder a la carpeta Contabilidad -

