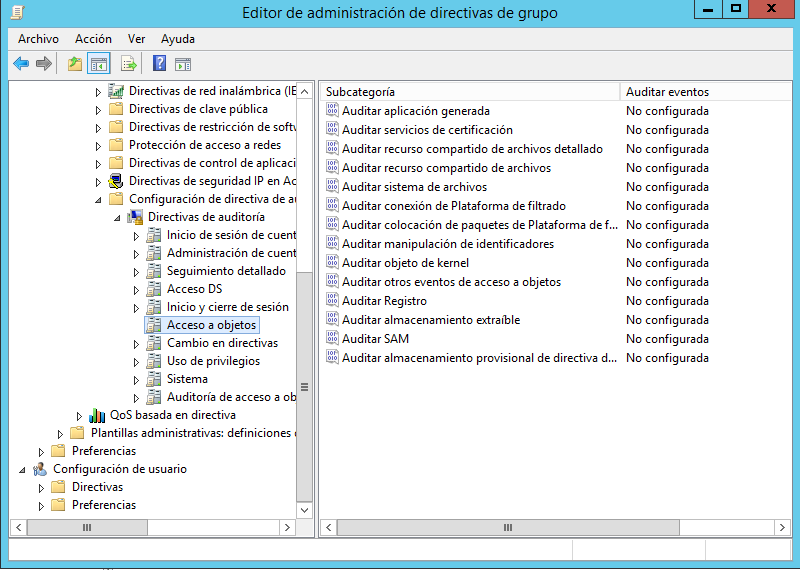
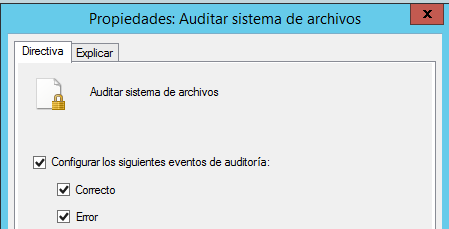
**Práctica 3: Auditar el acceso a objetos del dominio**

Configurar una GPO en tu dominio para auditar el acceso a objetos. Configura las auditorías en el AD para detectar:

**Configurar auditoria acceso a objetos mediante la direct. Auditoría avanzada**

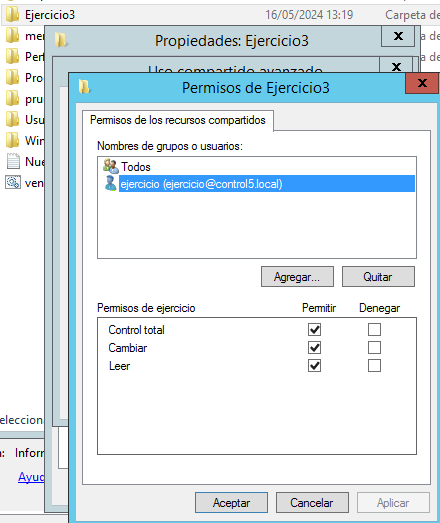
**Equipo → Directivas → Windows → Seguridad → Directiva Avanzada → Acceso a objetos → Sistema de archivos**



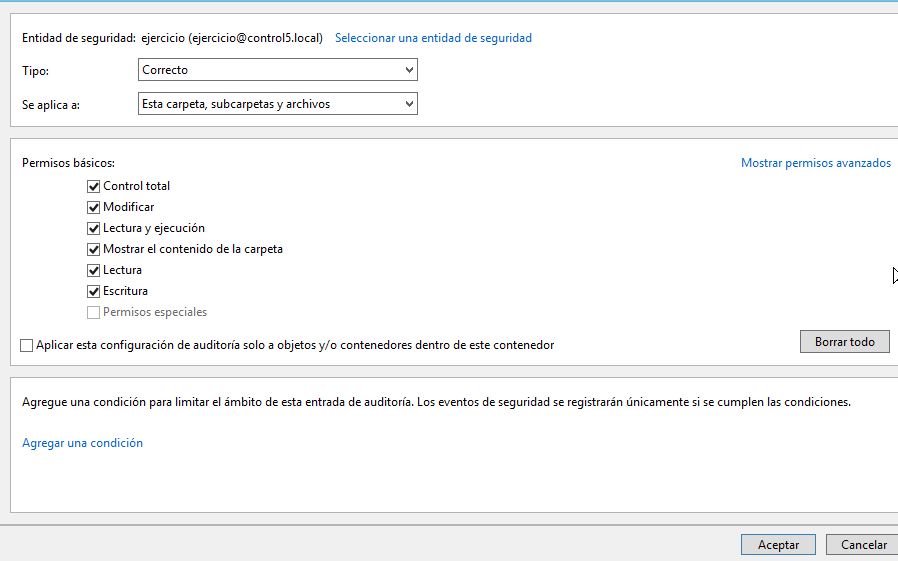


1. **Un acceso permitido a una carpeta mediante acceso local.**

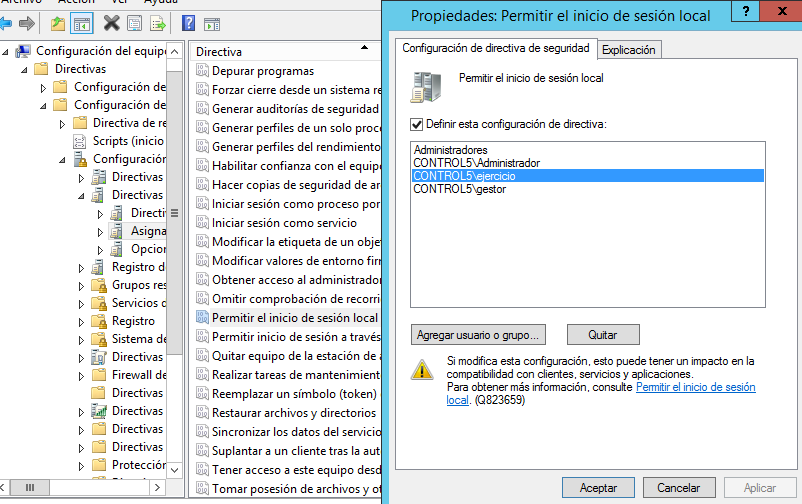
Crearemos una carpeta para esta actividad llamada Ejercicio3 y un usuario llamado ejercicio. Una vez creada añadimos al usuario creado en la configuración de compartir con todos los permisos.



Una vez agregado, entramos en las Opciones avanzadas de la carpeta y en Auditoría en la parte superior agregamos al usuario ejercicio con los siguientes permisos:



Si ya hemos agregado al usuario en la auditoría, iremos a la configuración de Default Domain Controller Policy → Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos → Permitir inicio de sesión local. Aquí agregaremos al usuario creado



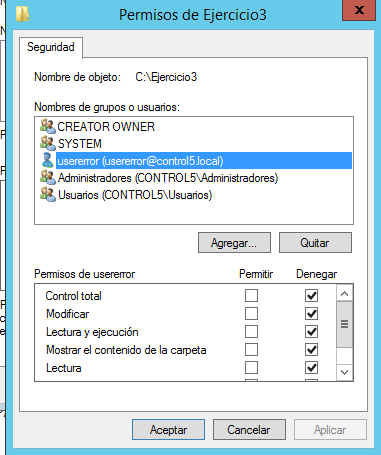
Ahora cerraremos sesión con el servidor e iniciaremos sesión con el usuario ejercicio. Volveremos a cerrar sesión y al iniciar sesion como Administrador encontraremos en el

Visor de eventos un nuevo registro con id 4663, que nos muestra la siguiente información.

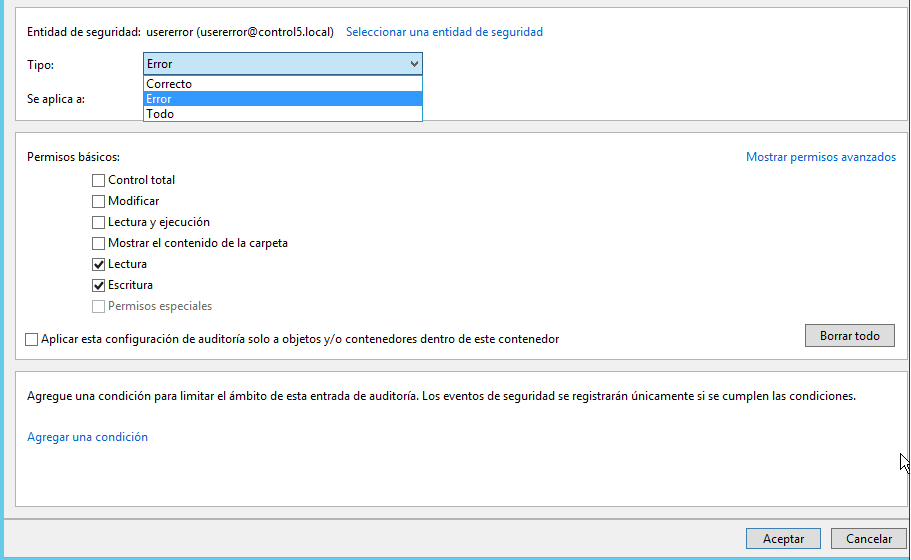


1. **Un acceso no permitido a una carpeta mediante acceso local.**

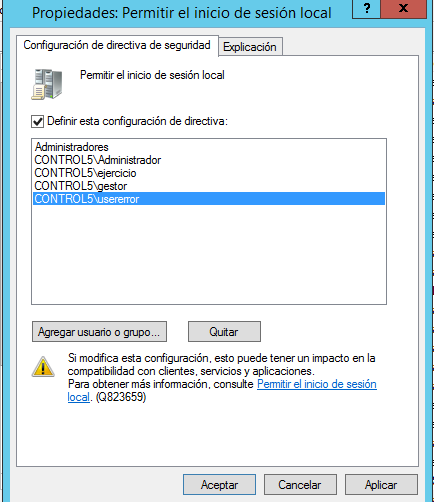
Ahora crearemos un nuevo usuario llamado usererror. Y lo agregaremos a la carpeta Ejercicio3 con todos los permisos denegados



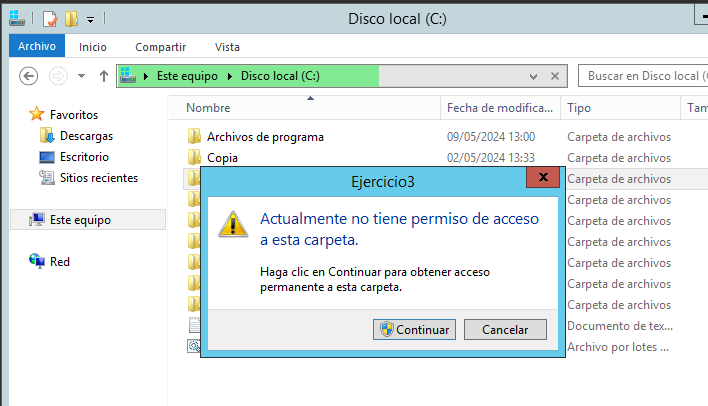
Despues lo añadiremos a una nueva auditoría de error



Y al igual que el usuario anterior, lo agregaremos a el permiso de Iniciar Sesión siguiendo la ruta anteriormente descrita



Entramos con este usuario al servidor y comprobamos que no tenemos permiso a esta carpeta

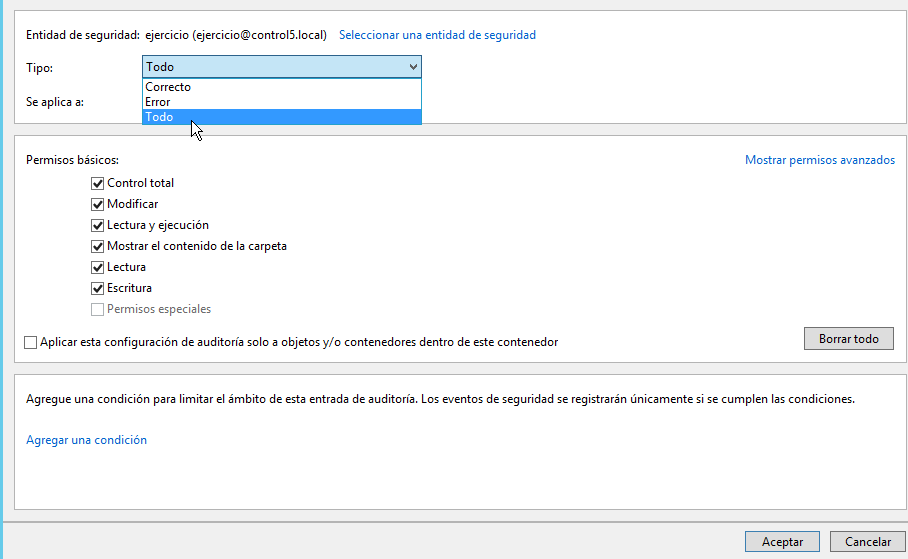


Entramos al visor de eventos y comprobamos que el usuario de error ha solicitado un identificador para un objeto. Podemos ver que su id es 4656



1. **La eliminación de un determinado fichero. Debes mostrar cómo puede el administrador del sistema averiguar qué usuario del dominio eliminó el fichero.**

Con el mismo usuario de ejercicio crearemos una nueva auditoría con el Tipo Todo.



Entrando con el usuario ejercicio al sistema, eliminamos una carpeta. Al entrar de nuevo al Administrador podremos ver como en el Visor de eventos tenemos un nuevo identificador el cual corresponde con una eliminación de objeto

