	DEPARTAMENTO INFORMÁTICA	
	2º ASIR - ASO	
	TALLER GRUPOS - PERMISOS	

0. OBJETIVOS

- Repasar las características de los **GRUPOS DE SEGURIDAD** – Ambitos y permisos básicos.
- Repaso con atención de la documentación sobre **PERMISOS** adjunta.

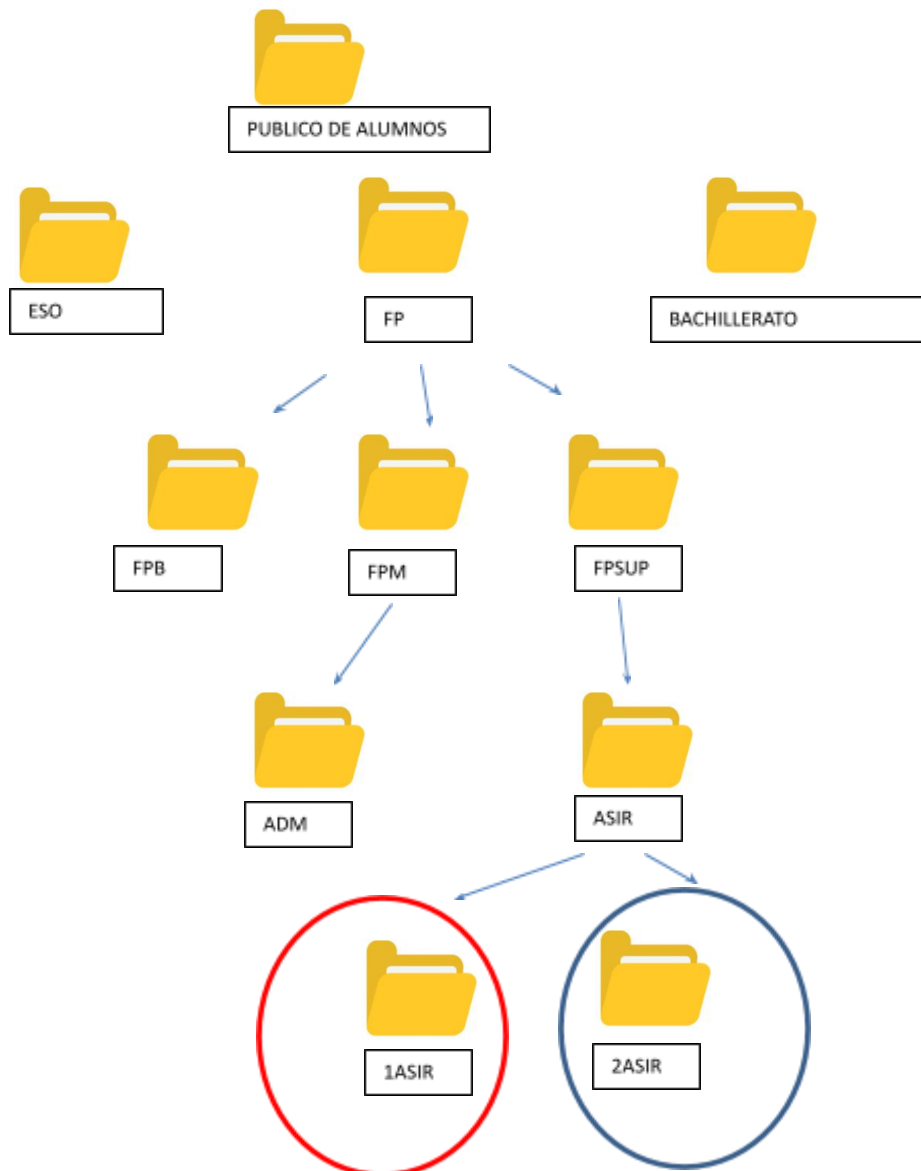
1. EJERCICIOS DE GRUPOS Y PERMISOS

A TENER EN CUENTA:

- Los grupos de seguridad son una ayuda elemental para adjudicar permisos en masa
- Todos los ejercicios se deben de realizar bajo la Carpeta de RECURSOS, en W, que tendrá los **mínimos permisos posibles para evitar la transmisión por herencia** de permisos que sean contraproducentes para los procedimientos.
- **Habrà que crear al menos dos grupos de seguridad de ámbito global con al menos un usuario creado a partir de plantilla.**
- Hay que tener cuidado cuando el usuario pertenece a dos grupos, ya que la suma de permisos de ambas ACE's será la resultante de sus permisos finales.
- Hay que tener en cuenta la herencia por defecto ya que la resultante de permisos hacia un grupo parte de la suma de los permisos implícitos mas explícitos.

1.1 EJERCICIOS DE CLASICO

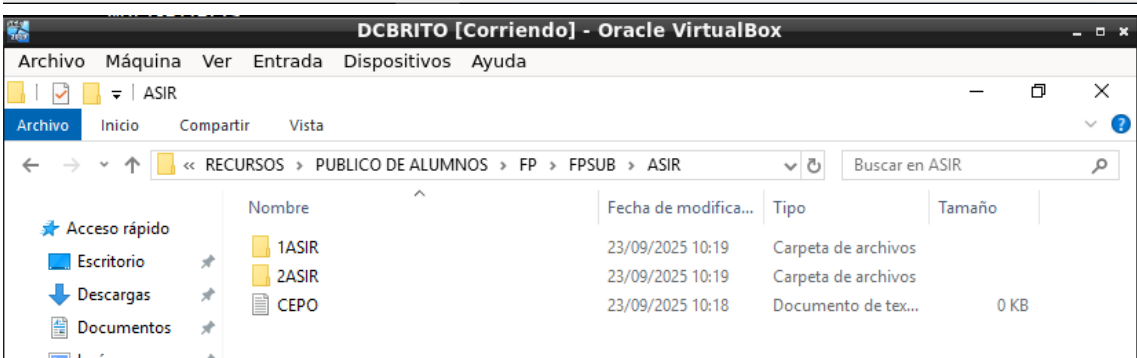
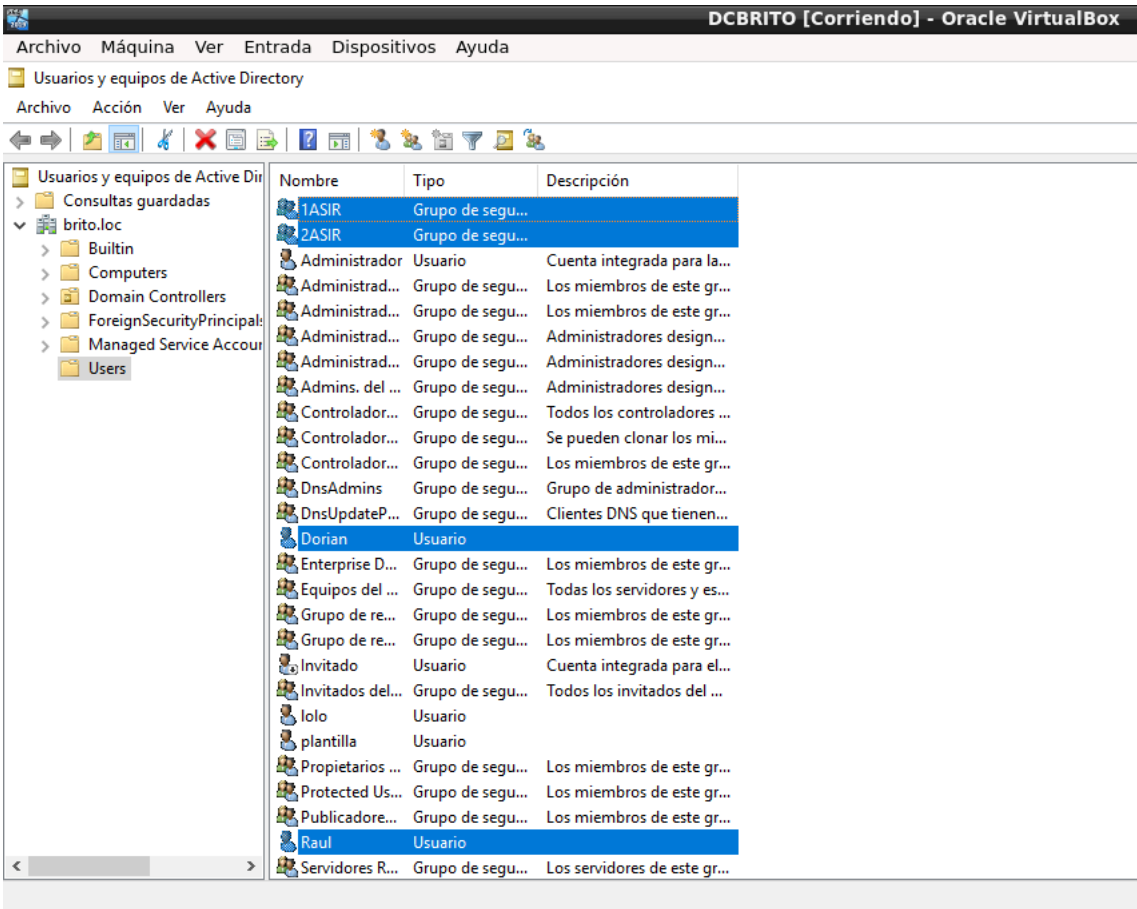
Crear una estructura parecida al público de alumnos del colegio donde dos grupos (1ASIR y 2ASIR) puedan ir recorriendo todo el árbol sin poder leer ni modificar nada hasta que no estén en su respectiva carpeta compartida de curso. Podéis insertar archivos aleatoriamente en diversas carpetas, “CEPO”, para que los usuarios de estos dos grupos no las vean.

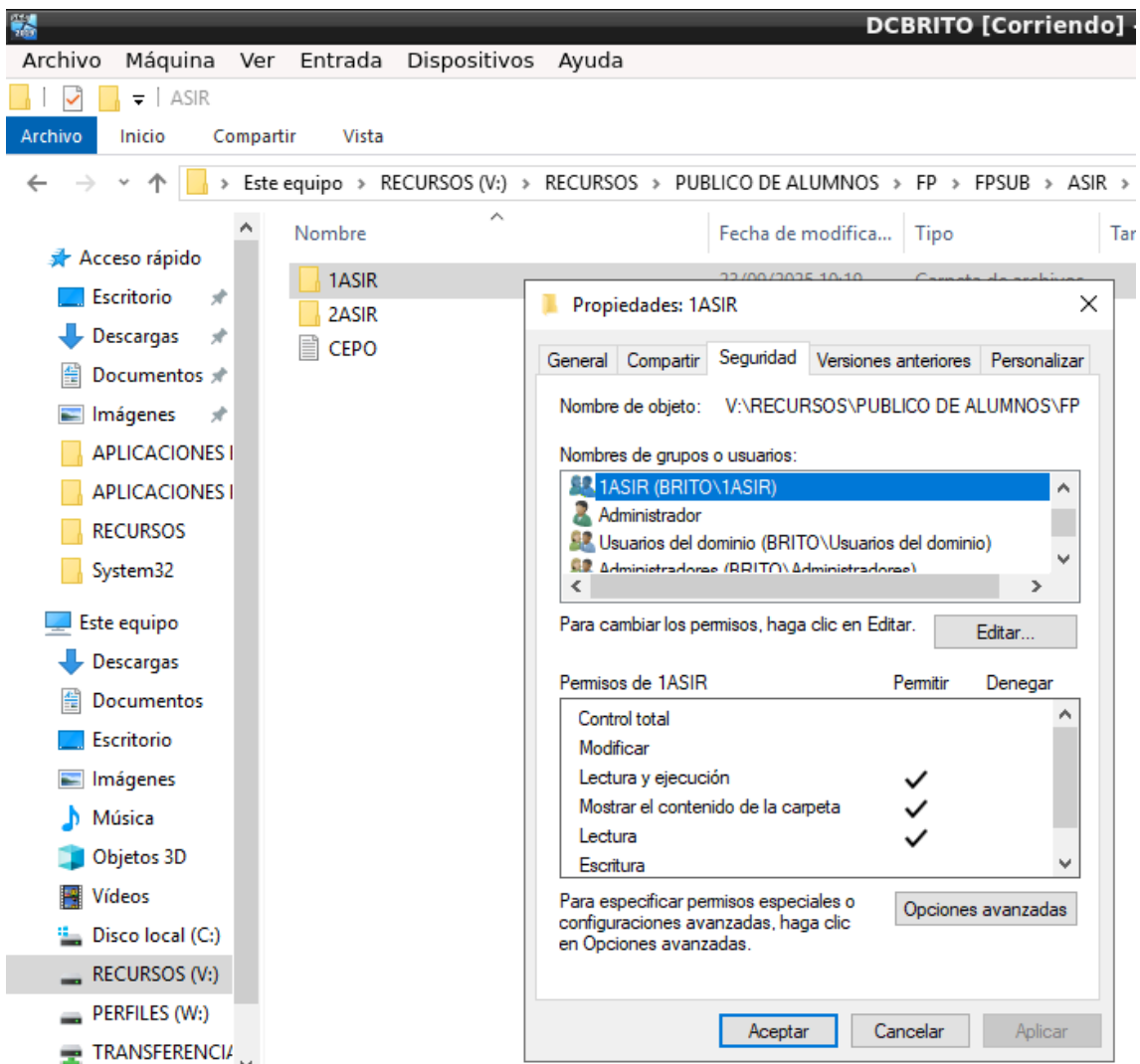


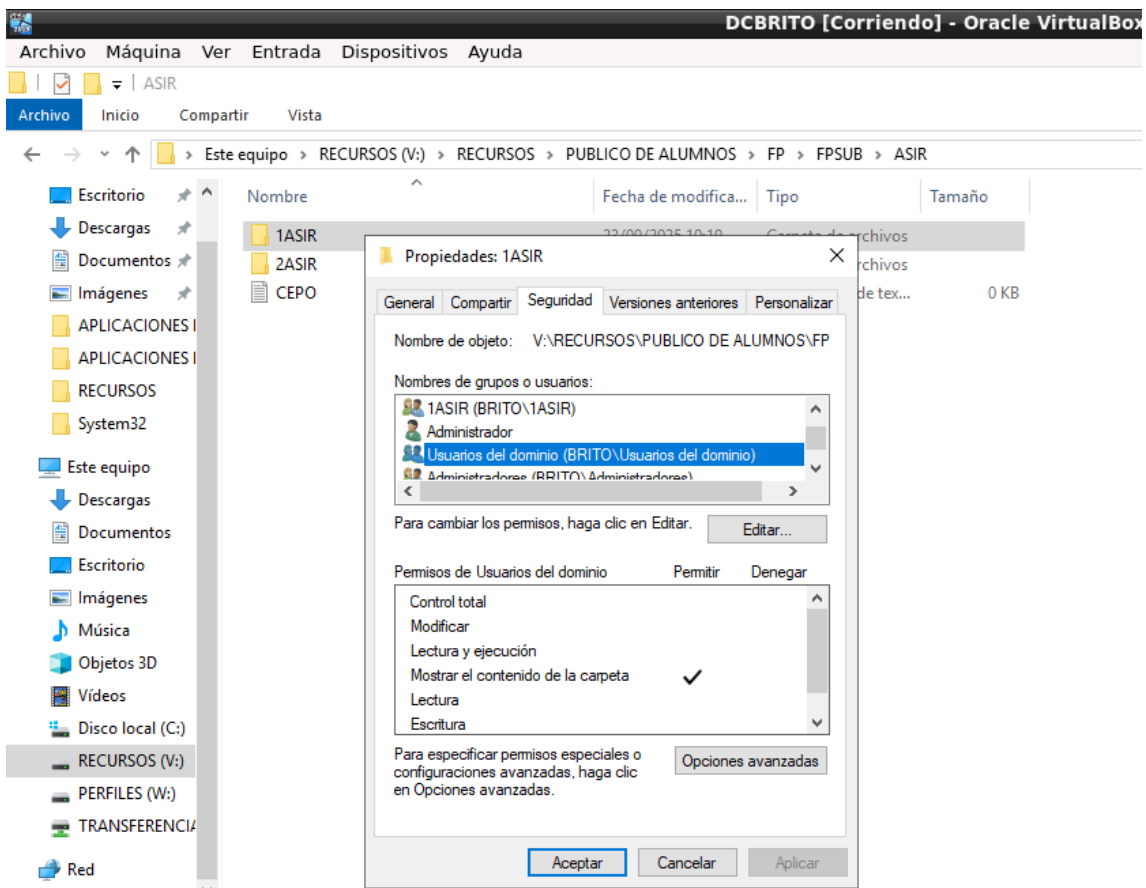
EVIDENCIA

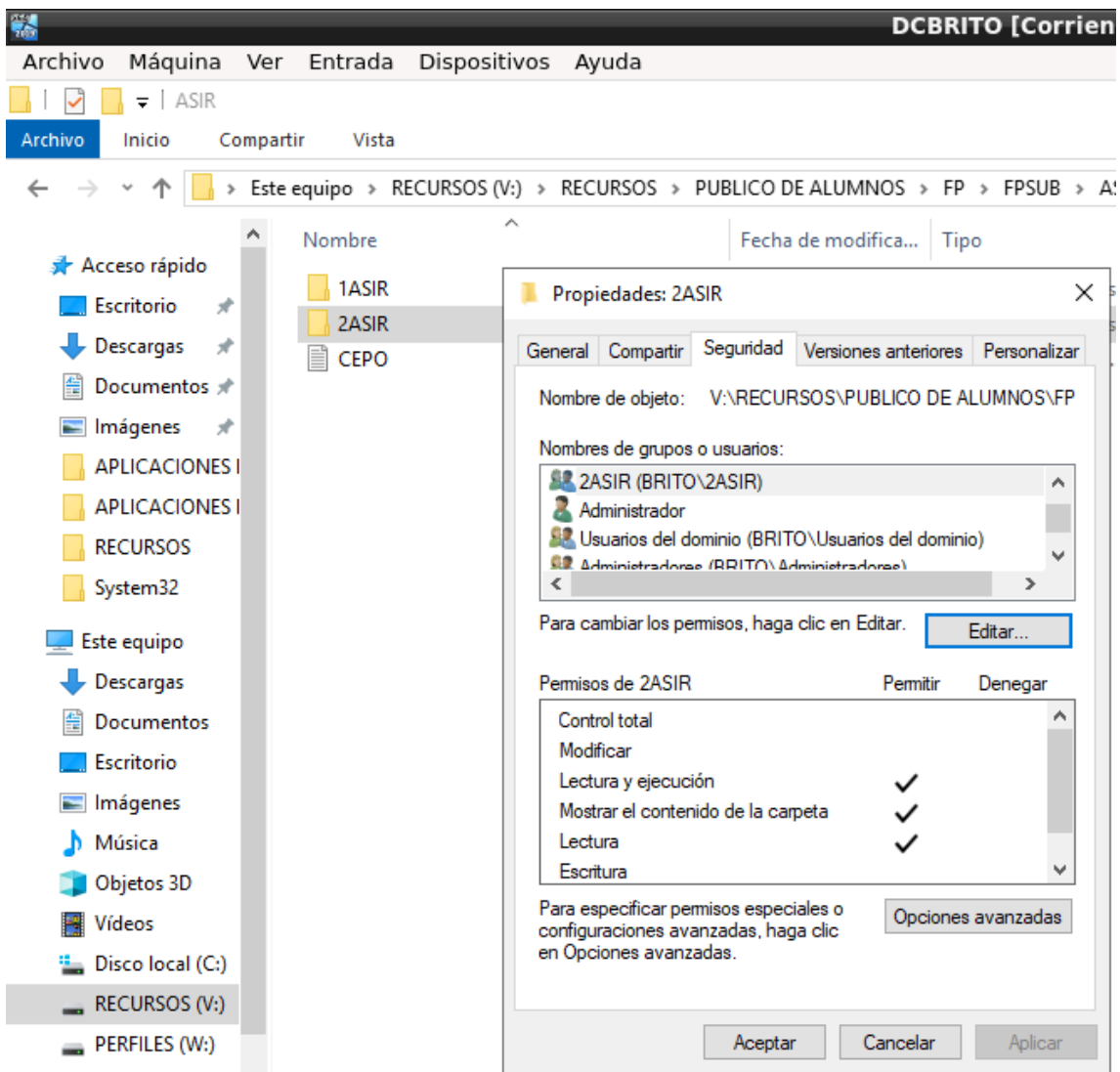
Raul pertenece al grupo 1ASIR

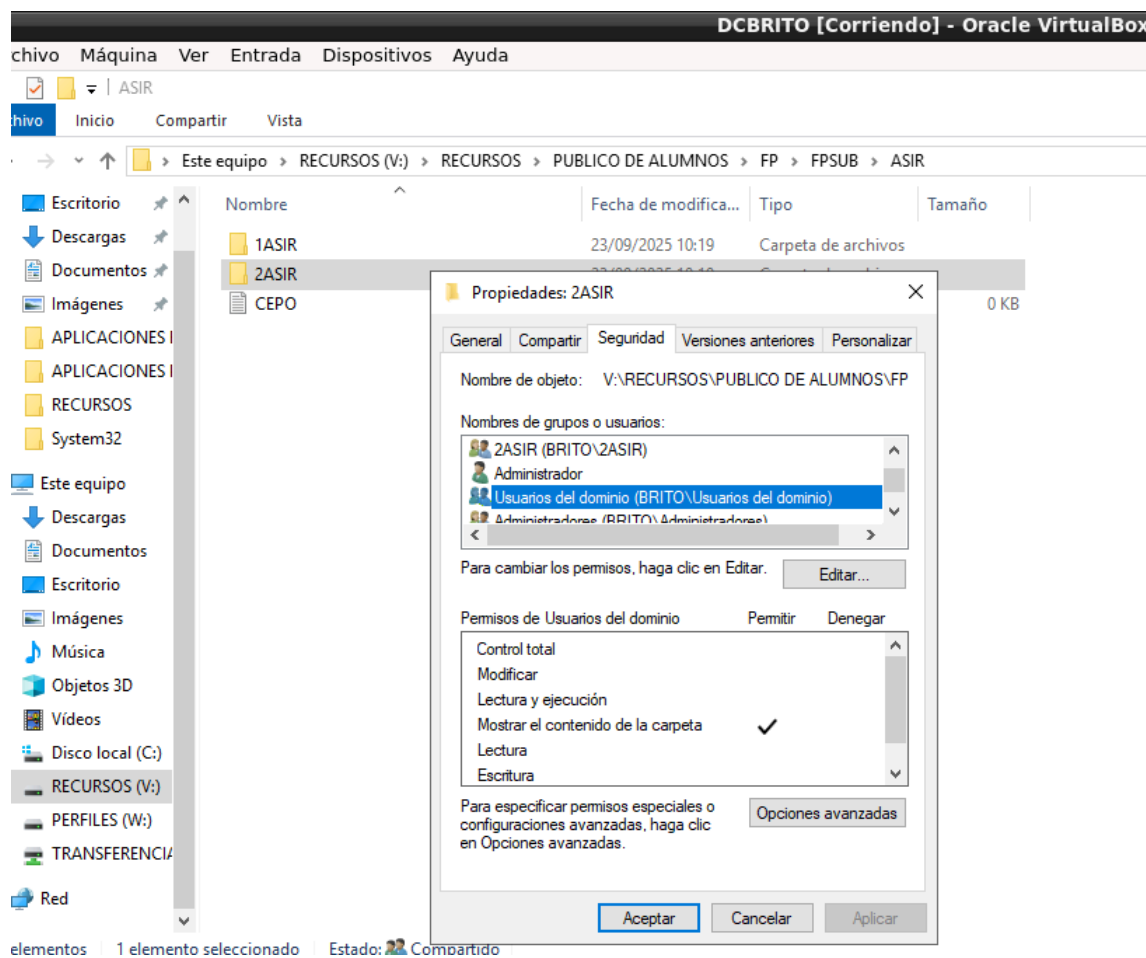
Dorian pertenece al grupo 2ASIR



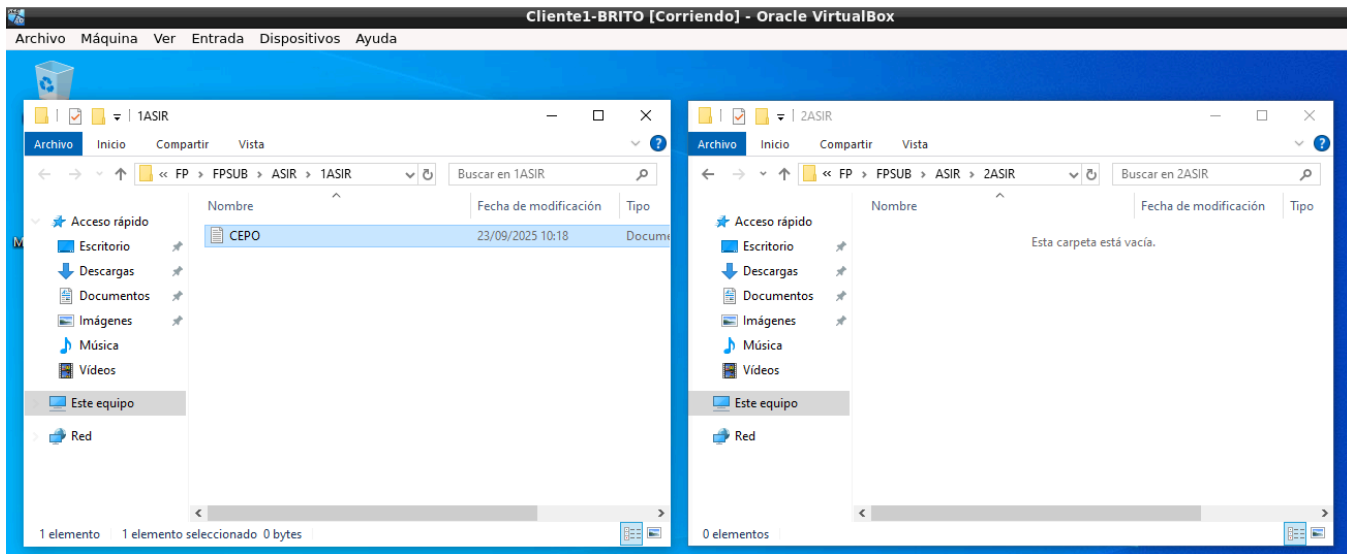




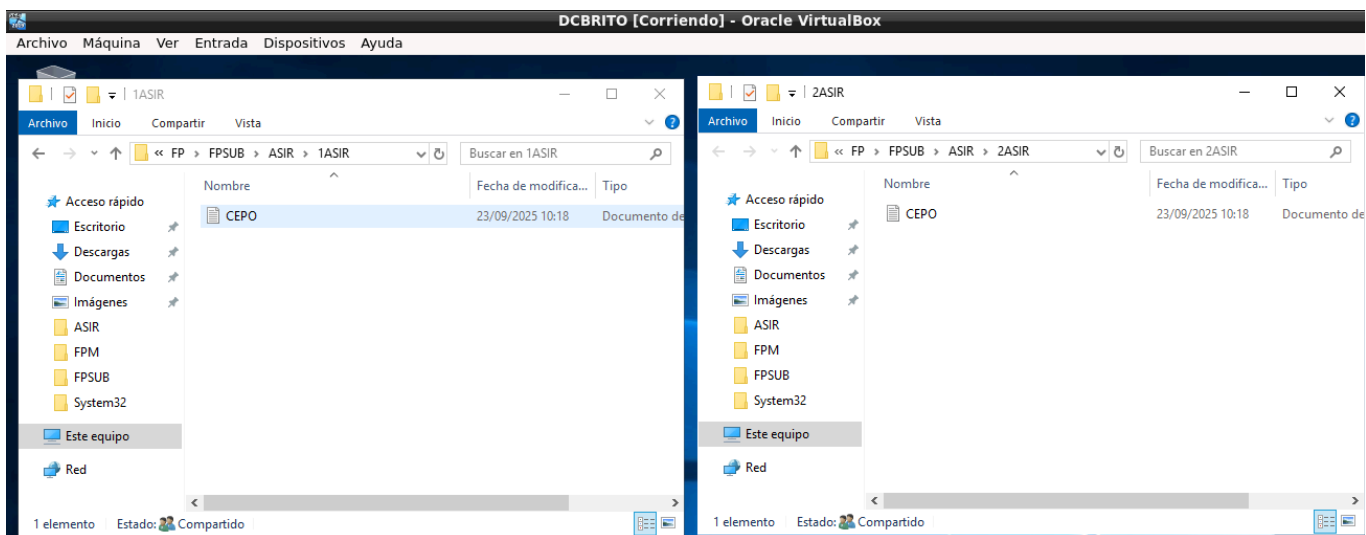




- USUARIO DEL GRUPO 1ASIR PUEDE VER EL CONTENIDO DE SU CARPETA Y LA DE 2ASIR NO (Y VICEVERSA)



- COMPROBACIÓN QUE LOS ARCHIVOS SI SE ESTAN EN AMBAS CARPETAS



1.2 REPOSITORIO DE EJECUTABLES

Es otro recurso muy utilizado, **solamente es posible realizar con ejecutables portables**. Cuando el usuario accede, se ejecuta una instancia de la aplicación localmente en el cliente sin apenas suponer carga sobre el servidor.

Para evitar la manipulación por parte del usuario crearemos una carpeta con accesos directos al ejecutable-

Tenéis que buscar programas aplicaciones portables, unas 3 para posteriormente ubicarlas como recurso.

Crear en RECURSOS una carpeta denominada APLICACIONES EN RED, dentro de la carpeta habrá otra carpeta para las aplicaciones portables, los usuarios del dominio no pueden ver esta carpeta, lo que verán son accesos directos a los ejecutables portables y tendrán el permiso de ejecución.

\\RECURSOS\APLICACIONES EN RED

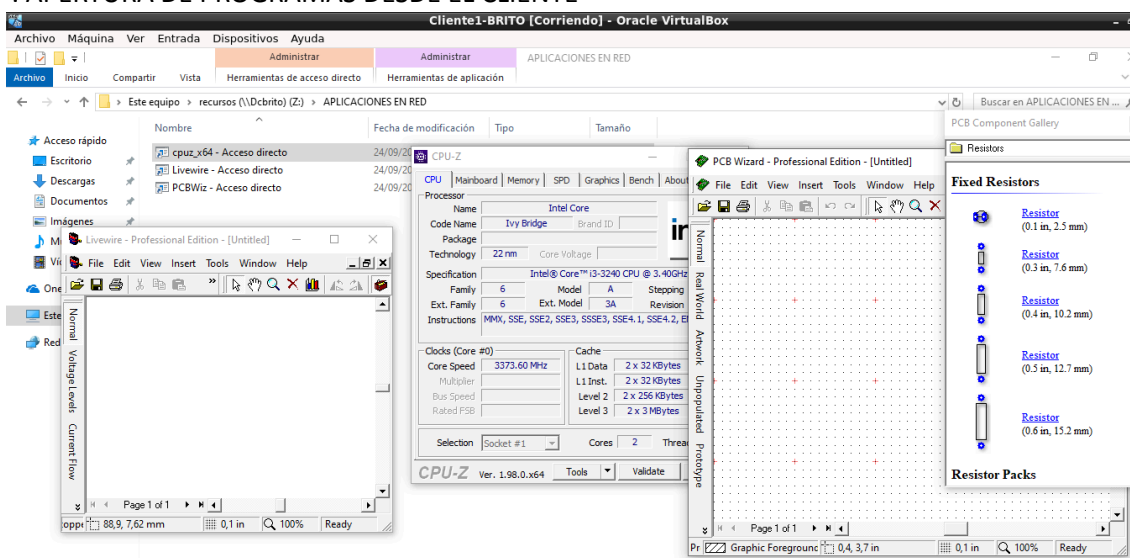
- Acceso directo a la aplicación 1 ---- visible y ejecutable
- Acceso directo a la aplicación 2---- visible y ejecutable
- Acceso directo a la aplicación 2---- visible y ejecutable

\\APLICACIONES PORTABLES -----INVISIBLE CON LAS APLICACIONES

- Aplicación 1
- Aplicación 2
- Aplicación 3

EVIDENCIA

- APERTURA DE PROGRAMAS DESDE EL CLIENTE



- PERMISOS DE LAS CARPETAS

DCBRITO [Corriendo] - Oracle VirtualBox

ArchivoMáquinaVerEntradaDispositivosAyuda

APLICACIONES EN RED

ArchivoInicioCompartirVista

Este equipo > RECURSOS (V:) > RECURSOS > APLICACIONES EN RED

Acceso rápido

Escritorio

Descargas

Documentos

Imágenes

APLICACIONES I

APLICACIONES I

FRONTERA

System32

Este equipo

Descargas

Documentos

Escritorio

Imágenes

Música

Objetos 3D

Videos

Disco local (C:)

RECURSOS (V:)

PERFILES (W:)

Nombre	Fecha de modifica...	Tipo	Tamaño
APLICACIONES PORTABLES	24/09/2025 12:01	Carpeta de archivos	
cpuz_x64 - Acceso directo	24/09/2025 12:09	Acceso directo	2 KB
Livewire - Acceso directo	24/09/2025 12:09	Acceso directo	2 KB
PCBWiz - Acceso directo	24/09/2025 12:09	Acceso directo	2 KB

Propiedades: APLICACIONES PORTABLES

GeneralCompartirSeguridadVersiones anterioresPersonalizar

Nombre de objeto: V:\RECURSOS\APLICACIONES EN RED\AF

Names de grupos o usuarios:

SYSTEMAdministradorAdministradores (BRITO\Administradores)

Para cambiar los permisos, haga clic en Editar: Editar...

Permisos de SYSTEM	Permitir	Denegar
Control total	✓	
Modificar	✓	
Lectura y ejecución	✓	
Mostrar el contenido de la carpeta	✓	
Lectura	✓	
Escritura	✓	

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Opciones avanzadas

AceptarCancelarAplicar

DCBRITO [Corriendo] - Oracle VirtualBox

ArchivoMáquinaVerEntradaDispositivosAyuda

FRONTERA

ArchivoInicioCompartirVista

Este equipo > RECURSOS (V:) > RECURSOS > APLICACIONES EN RED > APLICACIONES PORTABLES > FRONTERA

Acceso rápido

Escritorio

Descargas

Documentos

Imágenes

APLICACIONES I

APLICACIONES I

FRONTERA

System32

Este equipo

Descargas

Documentos

Escritorio

Imágenes

Música

Objetos 3D

Videos

Disco local (C:)

RECURSOS (V:)

PERFILES (W:)

TRANSFERENCIA

Nombre	Fecha de modifica...	Tipo	Tamaño
LiveWire	24/09/2025 12:09	Carpeta de archivos	
PCB Wizard	24/09/2025 12:09	Carpeta de archivos	
cpuz_x64	25/10/2021 10:14	Aplicación	4,315 KB

Propiedades: FRONTERA

GeneralCompartirSeguridadVersiones anterioresPersonalizar

Nombre de objeto: V:\RECURSOS\APLICACIONES EN RED\AF

Names de grupos o usuarios:

SYSTEMAdministradorUsuarios del dominio (BRITO\Usuarios del dominio)Administradores (BRITO\Administradores)

Para cambiar los permisos, haga clic en Editar: Editar...

Permisos de Usuarios del dominio	Permitir	Denegar
Control total		
Modificar		
Lectura y ejecución	✓	
Mostrar el contenido de la carpeta	✓	
Lectura	✓	
Escritura		

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Opciones avanzadas

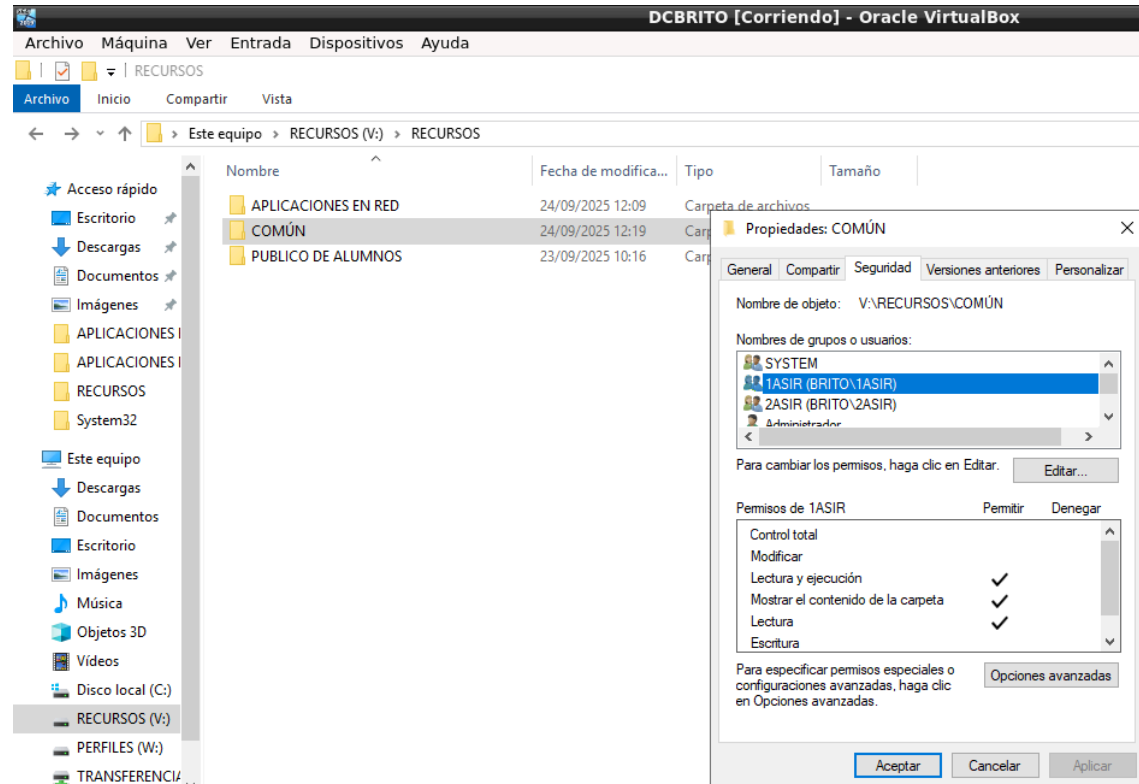
AceptarCancelarAplicar

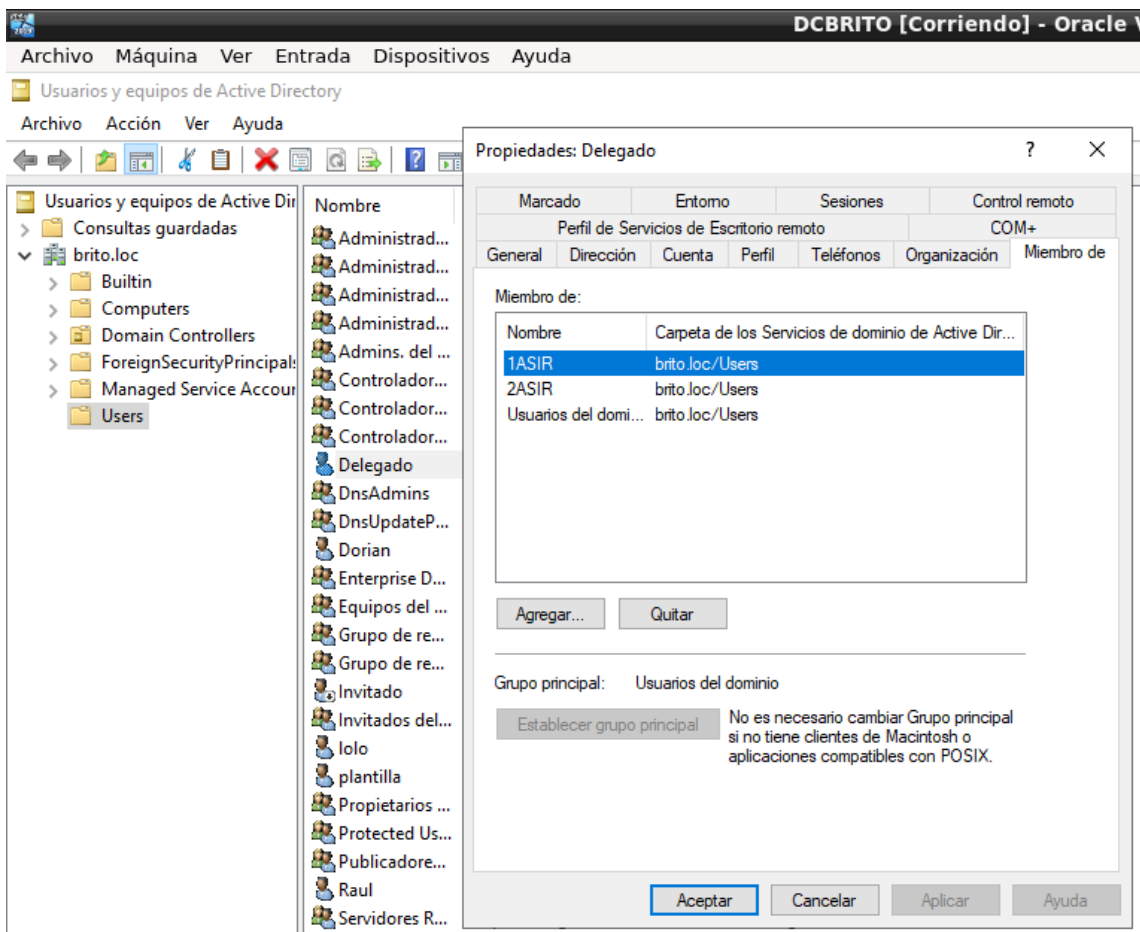
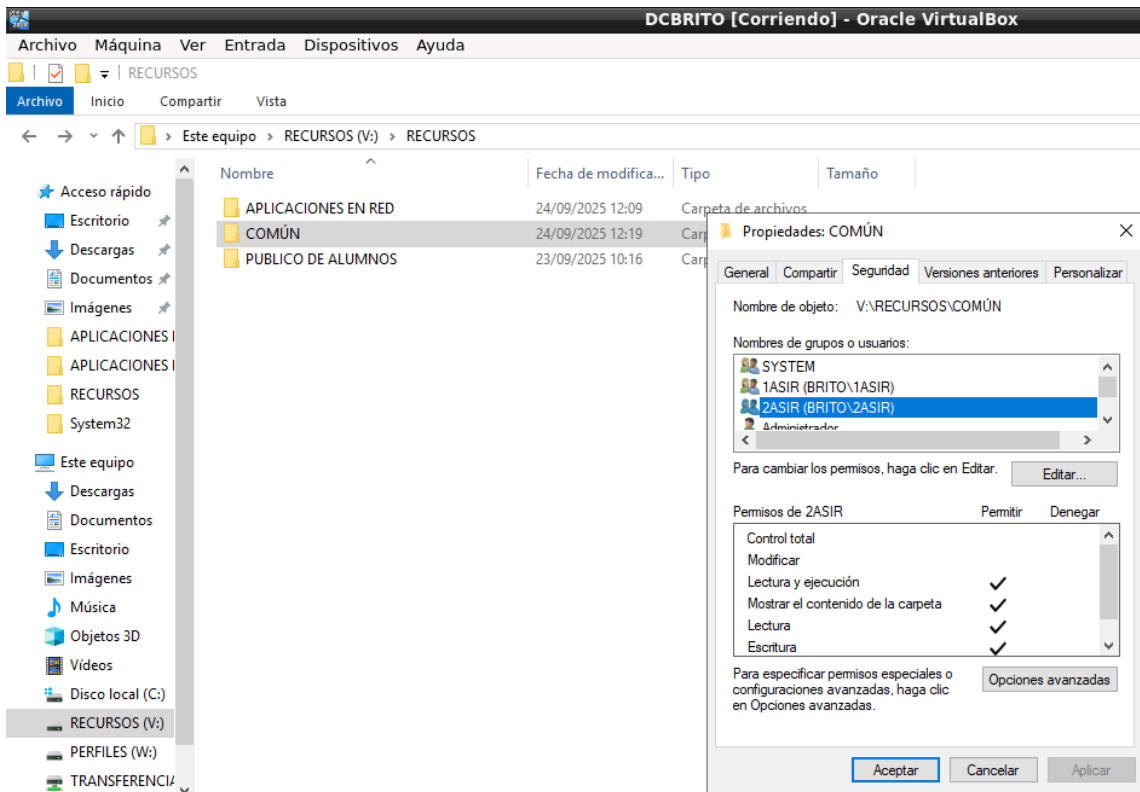
1.3 SUMA DE PERMISOS

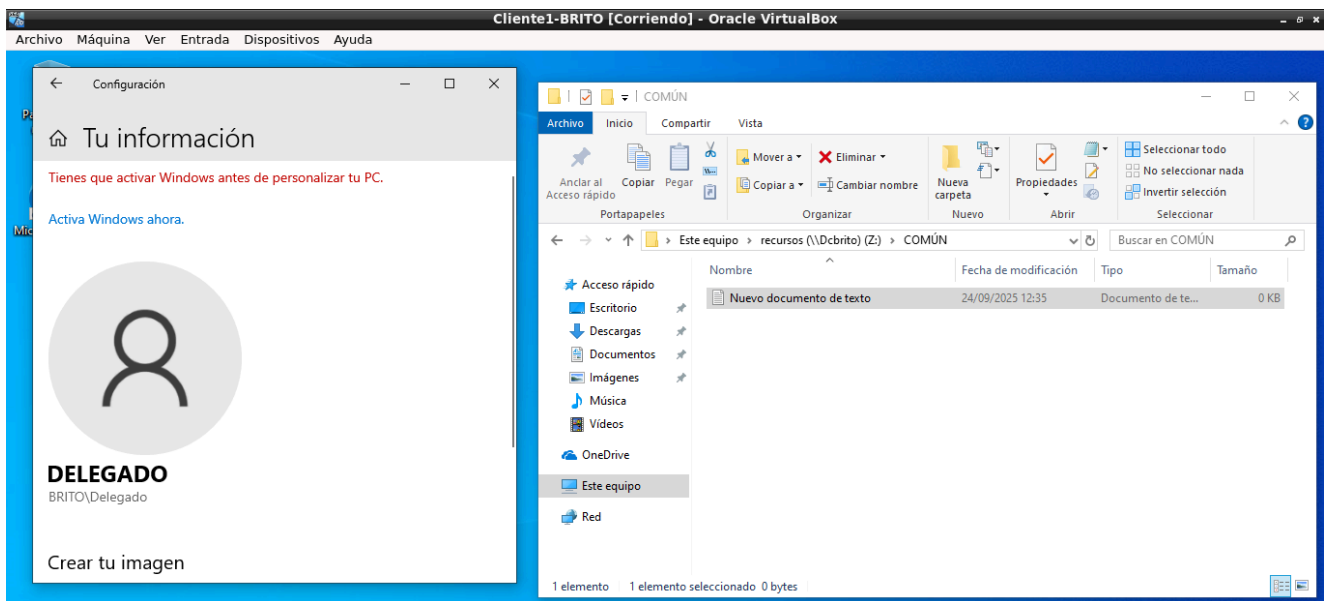
Crear un recurso denominado COMÚN con permisos de lectura para un grupo y con permisos de lectura- escritura para otro grupo. Integrar archivos en su interior.

Crear un usuario “delegado” que pertenezca a ambos grupos y comprobar su acceso.

EVIDENCIA



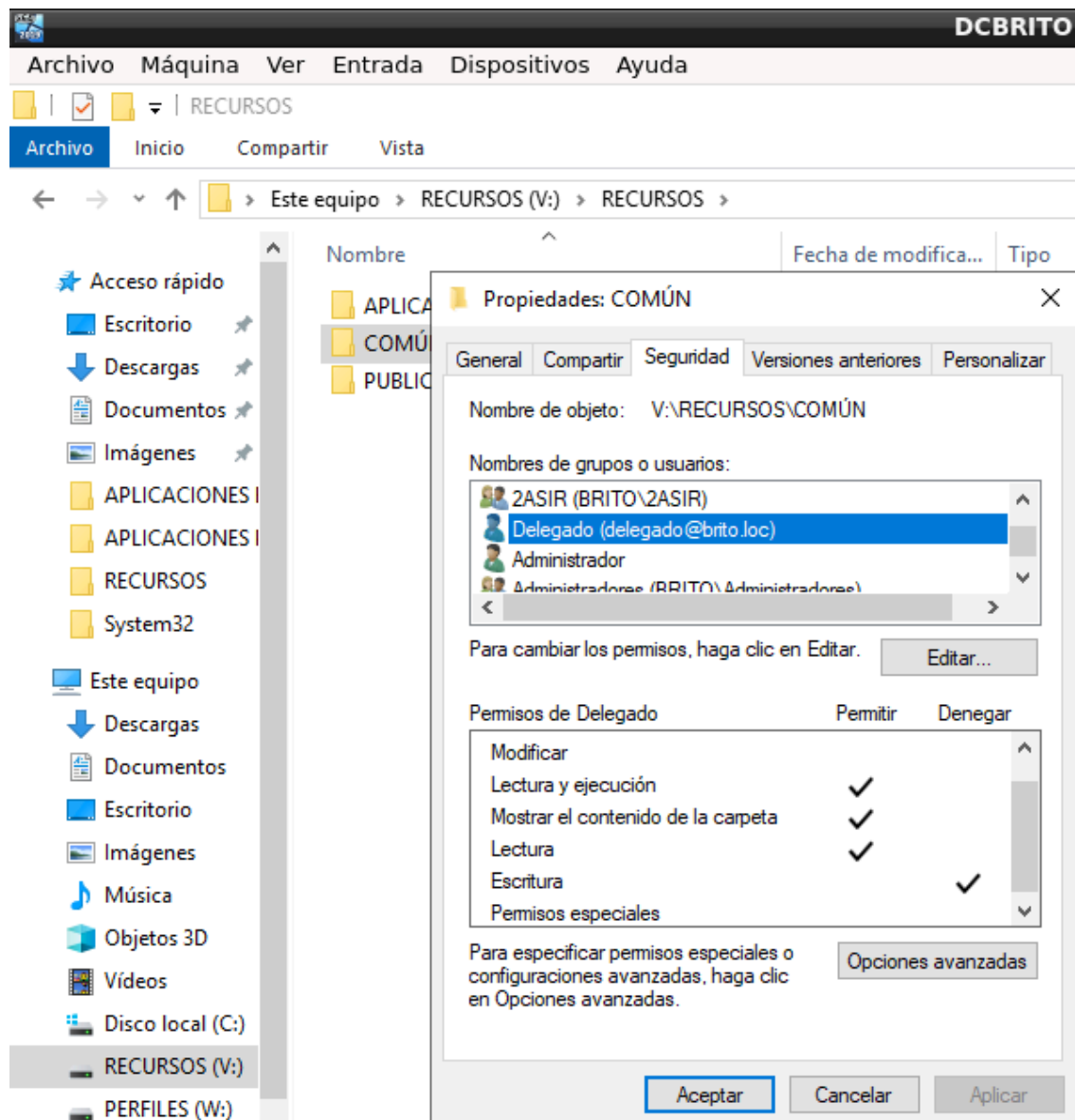


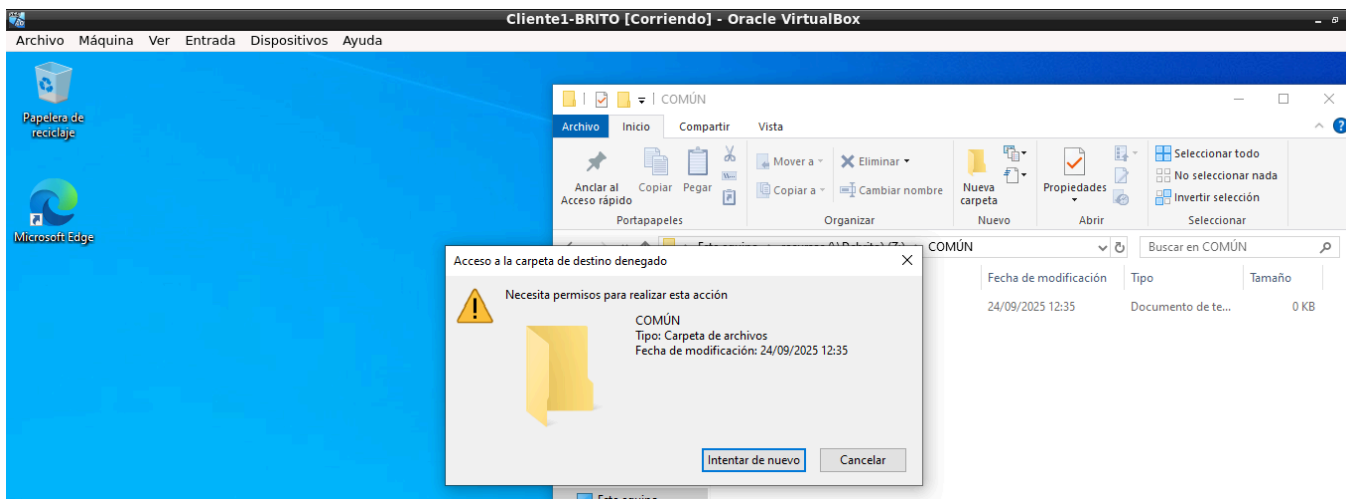


1.4 DENEGACIÓN

Partiendo de la estructura anterior probar a denegar al “delegado” en este caso una operación, escritura por ejemplo.

EVIDENCIA





LA DENEGACIÓN HAY QUE INTENTAR EVITARLA SIEMPRE. Ya que produce una sobrecarga, nueva lista ACE, para aplicarla a todo un grupo es equivalente a quitar el grupo de la lista PERMITIR, y así no es necesario DENEGAR.

¿EN QUÉ CASOS SE DEBE DENEGAR?

Tan solamente cuando a un grupo le está permitido el acceso y operaciones, pero queremos a un usuario en concreto perteneciente a ese grupo, denegarle el permiso,

2. SEGUIMIENTO INSTANTÁNEO DEL ACCESO A UN RECURSO.

Para realizar una administración centralizada de los recursos compartidos locales accedemos a la herramienta administrativa “Administración de equipos” y pulsamos en RECURSOS COMPARTIDOS, comprobar las SESIONES activas en ese momento, y el acceso a un recurso por parte de un usuario.

EVIDENCIA

