Práctica 1.1 Análisis del problema. Estudio de la implantación de AD y sus elementos.

Enunciado del problema

Perteneces al departamento de sistemas de la empresa XXXX a nivel nacional que se dedica a YYYYY.

Debido al gran auge experimentado por la empresa, y gracias al buen hacer de sus trabajadores (tú entre ellos), la empresa ha crecido y ya tiene 3 sedes : Córdoba (central), Málaga y Sevilla (secundarios).
A fecha de 1 de Noviembre de este año se plantea una migración del entorno corporativo a una versión de Windows Server actual. Nuestra labor como analistas y técnicos de sistemas es la de determinar los procedimientos necesarios para dicha migración y llevarlos a cabo para tal fecha.

Suponemos que tenemos que controlar en el nuevo entorno los mismos elementos que están actualmente en producción:

- Administración de usuarios y grupos.
- Administración de ficheros.
- Administración de discos.
- Copias de seguridad.
- Instalación de software controlada

pero ahora también hay que añadir los nuevos sites para las distintas sedes. Y además añadir otros servicios más que irán surgiendo durante el desarrollo.

El trabajo consiste en realizar un informe detallado de los pasos seguidos para la nueva implantación con el máximo nivel de detalle (incluyendo capturas de pantalla) de los pasos seguidos para la gestión de los servicios anteriormente citados y otros nuevos que añadiremos.

La información necesaria para esta labor en relación al entorno actual es la siguiente:

1. Será necesaria la instalación de un servicio de directorio para optimizar funcionamiento y mantenimiento. Las máquinas clientes deben formar parte del dominio y usarse como meros terminales para conectarse al servidor (no pueden utilizarse usuarios locales)

2. Se creará un esquema de directorio activo acorde a la organización de la empresa de modo que se representen todos los departamentos.

3. Se crearán usuarios por cada empleado. Su perfil .
    a. Existen dos usuarios especiales correspondientes al **gerente de la empresa** y al **director** de la sucursal de Córdoba.
    b. Existen al menos tres departamentos:
        i. CEOs, con gerentes y directores
        ii. RRHH (con 2 empleados, un jefe de RRHH y otro empleado)
        iii. INFORMÁTICA con dos equipos : Desarrollo y sistemas.
        Hay 5 empleados: un jefe de Informática, dos desarrolladores y dos sysadmin.
    c. Crearemos usuarios para los miembros de la empresa.

        Para cada uno de estos usuarios se creará un perfil dinámico (móvil) , que será oculto y privado para el resto de los usuarios (excepto para el administrador).

4. Recursos compartidos: carpetas y accesos a las carpetas.
   Las carpetas de los departamentos estarán en una partición o disco duro diferente a la del sistema operativo.
   Ayuda: si no lo hiciste ya, aquí tienes ayuda Cómo reducir disco y crear nuevo volumen.

Además:

a. El director y el gerente tienen sus propias carpetas. Cada uno tiene acceso a la suya.
b. Todos los directivos (directores y gerentes) tienen acceso al resto de la información relevante de la empresa en modo de lectura (ej. a las Nóminas)
c. El departamento de RRHH tendrá una carpeta compartida llamada EMPLEADOS. Podrán escribir los usuarios del dpto. Pero no tendrán control total.
d. El departamento de informática tendrá una carpeta general llamada "ManualesInformatica" y podrá controlar cualquier informático. El departamento de Desarrollo tiene una carpeta Desarrollo que solo pueden acceder los desarrolladores con control total.

5. Otros Recursos compartidos: impresoras

Hay una impresora HP en la planta 1 a la que accederán los empleados de Informática
Hay una impresora en la planta 2 a la que accederán el resto de departamentos.

Nota: como impresoras vamos a usar impresoras PDF. Descarga: https://tools.pdf24.org/es/creator#download

Practica 1.1 DISEÑO DE EMPRESA Y OBJETOS DE ACTIVE DIRECTORY.

DESARROLLO:

1 **ORGANIGRAMA DE LA EMPRESA** (empresalopez).

IDENTIFICAMOS los departamentos.

a) Diseñamos la empresa con los distintos niveles:

b) Para esta práctica creamos los distintos departamentos y la jerarquía entre ellos.

El organigrama va a tener menos 3 niveles:

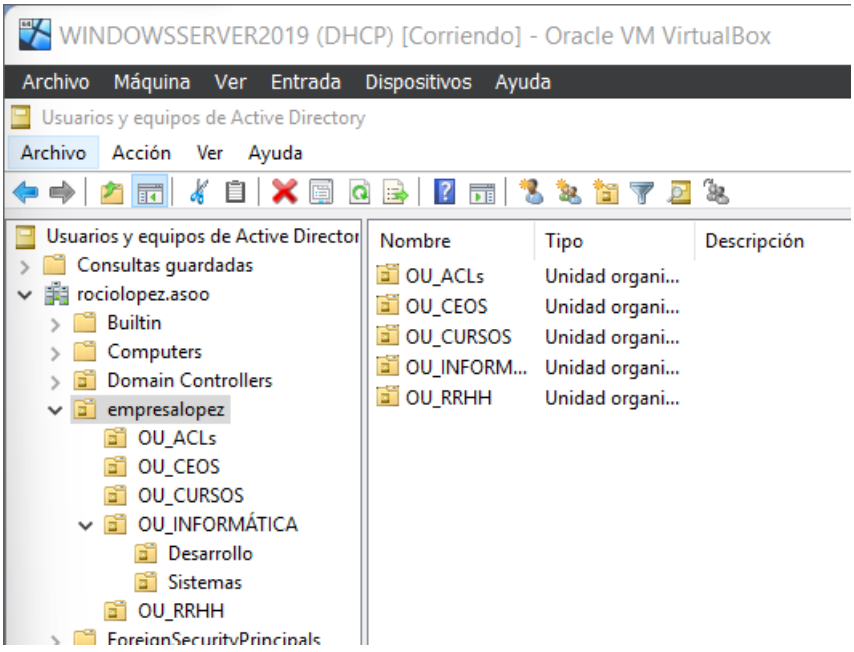
Empresa → Departamentos principales → Subdepartamentos.

c) Crear las OU's.

- Crear la jerarquía de OU's comenzando por una OU padre que sea el nombre de la empresa

- Por cada departamento , crea la unidad organizativa correspondiente en AD . Debes llamarlas OU_nombredpto

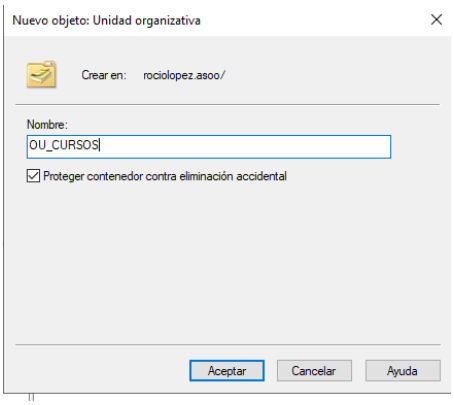
Nota: para crear la OU debes abrir Herramientas de AD-> Usuarios y Grupos de AD -> Nueva OU (Botón derecho sobre el nombre del dominio)



Ya está configurada (la de OU_CURSOS la creó en el punto siguiente)

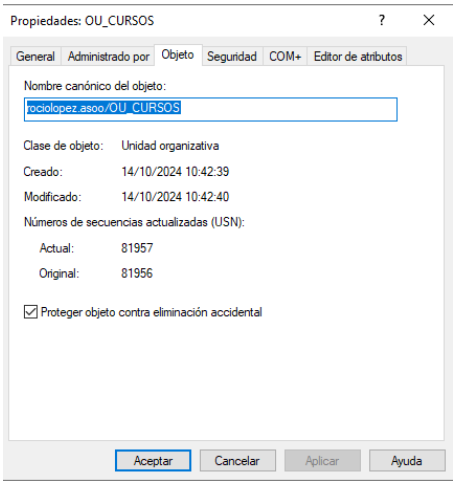
2 Gestionar las OU's

a) Crea una GPO con nombre OU_CURSOS protegida contra borrado accidental.

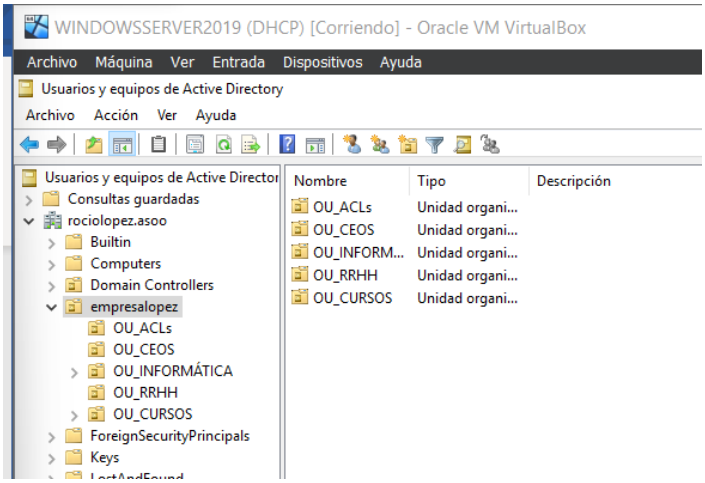


b) Mueve la OU_CURSOS bajo la empresa . Indica los pasos a seguir para conseguirlo

- Vamos a Ver > Características avanzadas.
- Luego vamos al objeto que queremos modificar, eliminar… y vamos a sus propiedades



- Desmarcamos la casilla y ya podríamos moverlo:



3 Carpetas personales de los nuevos usuarios del dominio (Perfiles$)

Antes de crear los usuarios se requiere preparar la carpeta donde se va a ubicar su perfil móvil.

Los usuarios que vamos a crear en AD ya no son locales al servidor, son del dominio. Por ello su espacio personal no se guarda en C:\Users\…

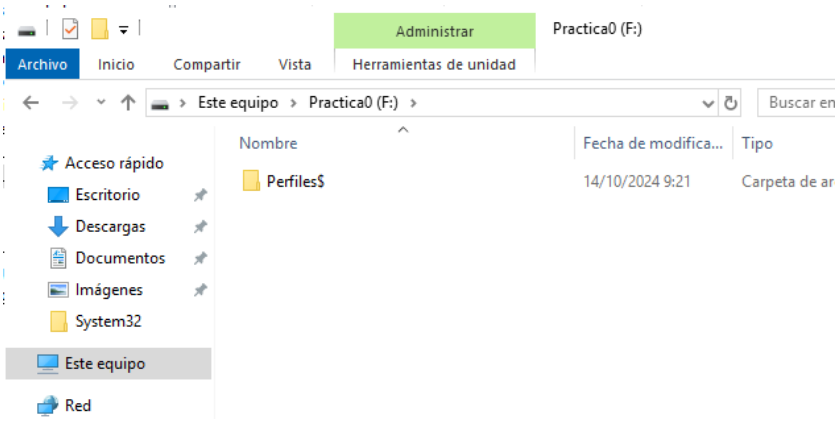
Debemos guardar sus perfiles en una carpeta compartida específica para ello .

3.1 Justifica por qué tiene que ser compartida

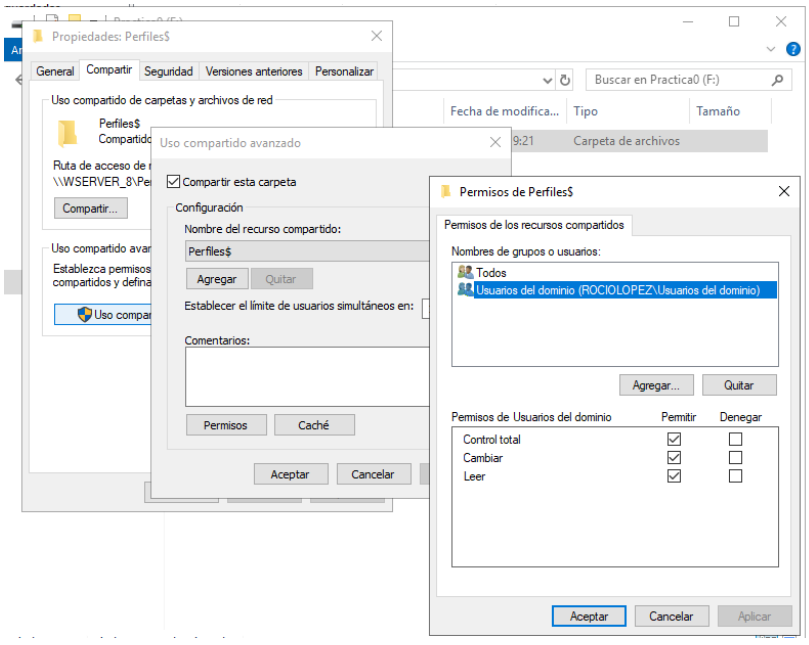
- La carpeta debe ser compartida para que los usuarios del dominio puedan acceder a su perfil móvil desde cualquier equipo en la red. Esto centraliza la gestión de sus datos, permite la sincronización, facilita las copias de seguridad y garantiza una experiencia de usuario consistente en todo el dominio. Además, es un requisito de Active Directory para que los perfiles funcionen correctamente.

3.2 Creamos dicha carpeta que llamaremos "**Perfiles$**" (acaba en $ para que sea oculta en el sistema)

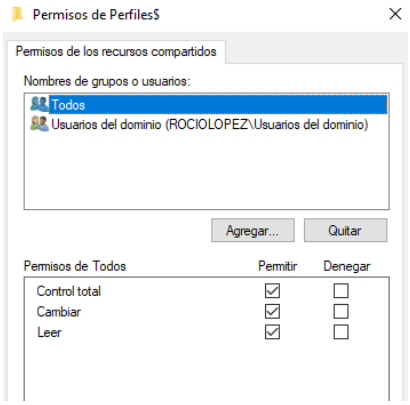
- Creamos la carpeta en la partición nueva del disco*:*



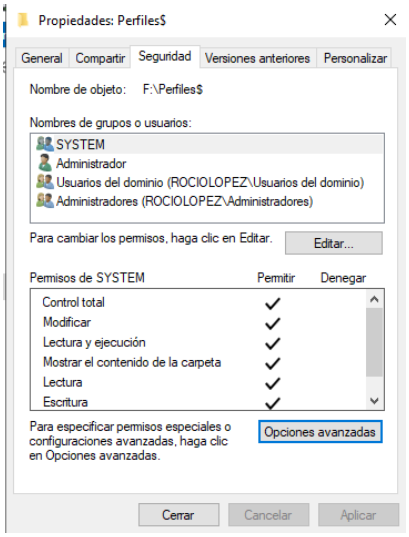
- *En "Compartir" > Uso compartido avanzado > Marcamos la casilla, y pulsamos permisos, y en permisos ponemos control total a los usuarios de dominios*



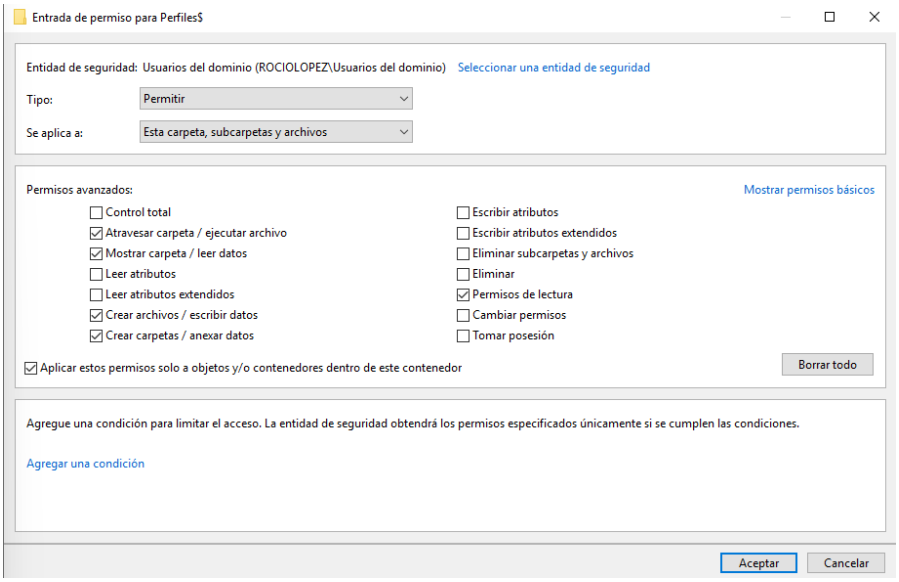
- *Y en Todos, ponemos también "Control total":*



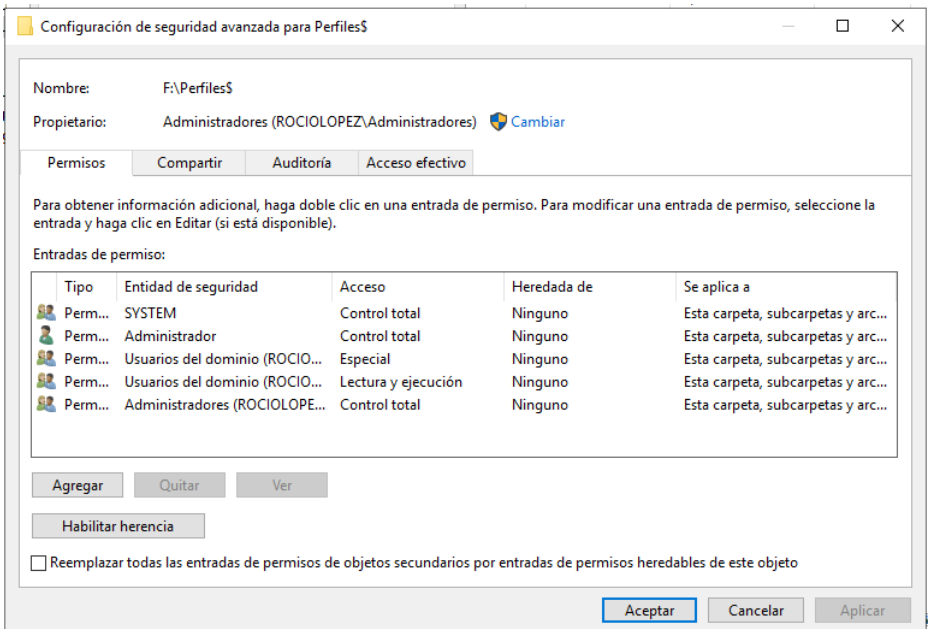
- *Luego en seguridad ponemos lo siguiente con control total:*



- *Menos los usuarios de dominio, que pondremos lo siguiente:*



- *Así quedaría:*



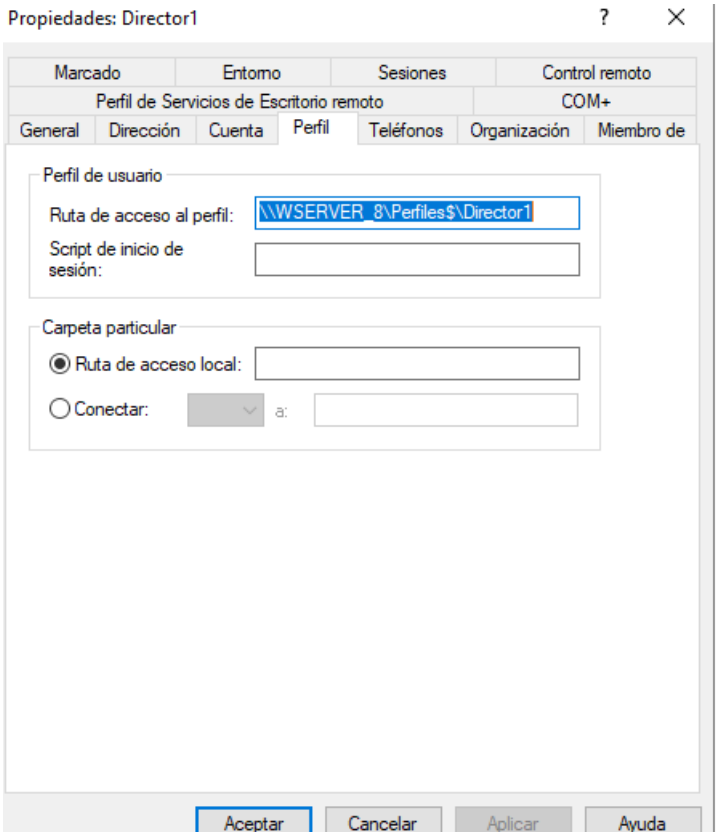
4 Usuarios y Grupos Globales

Vamos a seguir la estrategia **IGDLP** (Identidad, grupo Global, grupo Local, Listas de Acceso y Permisos)

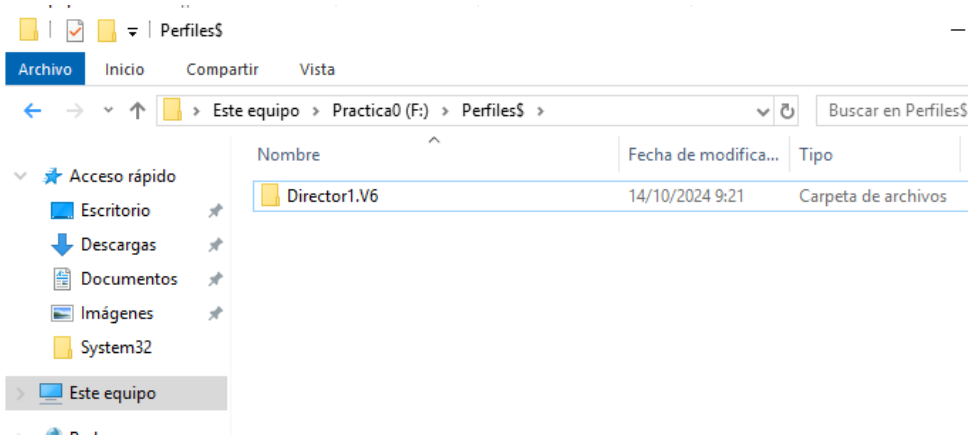
4.1 Mete a los user creados (en el punto 3 de la introducción) de cada departamento para que tengan perfil móvil:

- *Los usuarios que creemos en AD ponemos en su perfil la ruta de la carpeta para que se cree ahí sus perfiles al iniciar sesión:*

\\WSERVER_8\Perfiles$\%USERNAME%



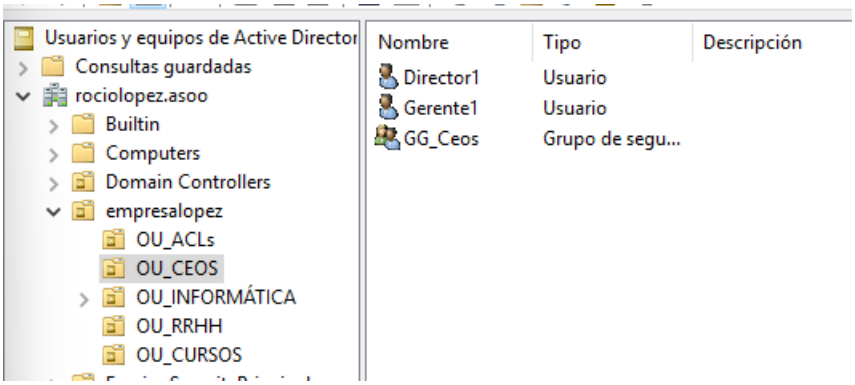
- *Como vemos cuando iniciamos sesión se creará la carpeta:*



4.2Crea los Grupos Globales necesarios. Llámalos GG_nombre.

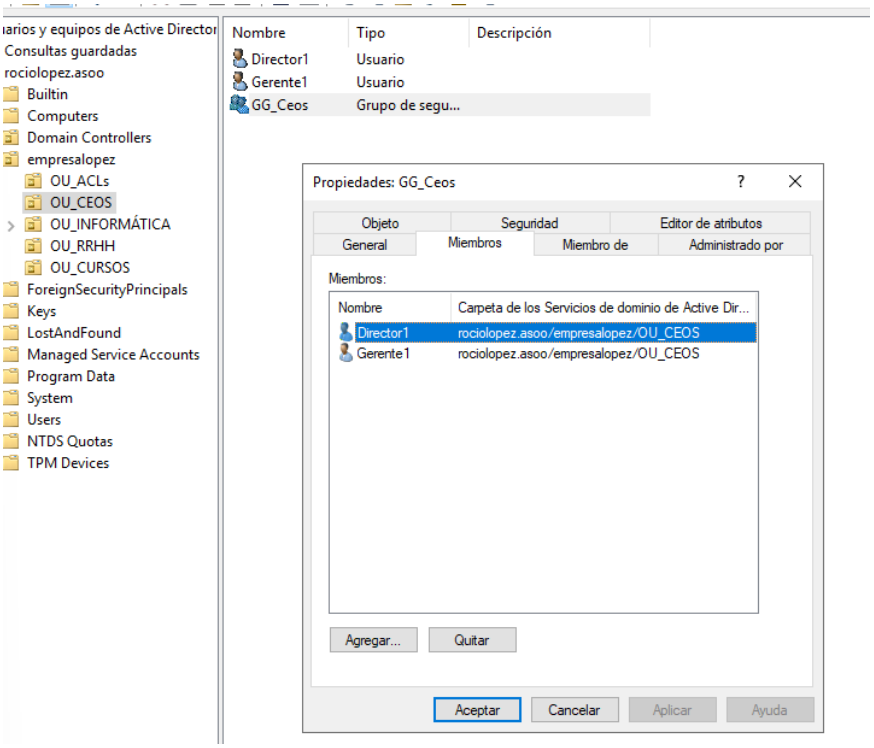
Ahora hay que c**rearlos bajo la OU correspondiente**: *Herramientas de AD-> Usuarios y Grupos de AD -> Seleccionar la OU (departamento) -> botón derecho Nuevo Grupo*

Así en todos:



4.3Mete cada usuario en su GG correspondiente.

Así en todos:



5 **Diseño de RECURSOS y Grupos LOCALES de Dominio para permisos a los recursos (ACL)**

Crearemos una carpeta padre (Empresa)

- Los gerentes y directores controlan una carpeta sobre CLIENTES.
- Una carpeta de Imágenes (.iso) para todo Informática. Podrán leer escribir todos los informáticos, pero el control de la carpeta lo tiene el jefe de informática.
- Una carpeta para cada subdepartamento de informática. Solo podrán acceder los empleados de cada subdepartamento y el jefe de informática.

    a. El director y el gerente tienen sus propias carpetas. Cada uno tiene acceso a la suya.
    b. Todos los directivos (directores y gerentes) tienen acceso al resto de la información relevante de la empresa en modo de lectura (ej. a las Nóminas)
    c. El departamento de RRHH tendrá una carpeta compartida llamada EMPLEADOS. Podrán escribir los usuarios del dpto. Pero no tendrán control total.
    d. El departamento de informática tendrá una carpeta general llamada "ManualesInformatica" y podrá controlar cualquier informático.

- Con todo lo anterior, completa la tabla de abajo.

Los grupos Locales van a ir asociados a recursos compartidos y los permisos sobre éstos (Carpetas, impresoras, etc). Por ello primero tenemos que saber qué recursos se van a compartir en el dominio.

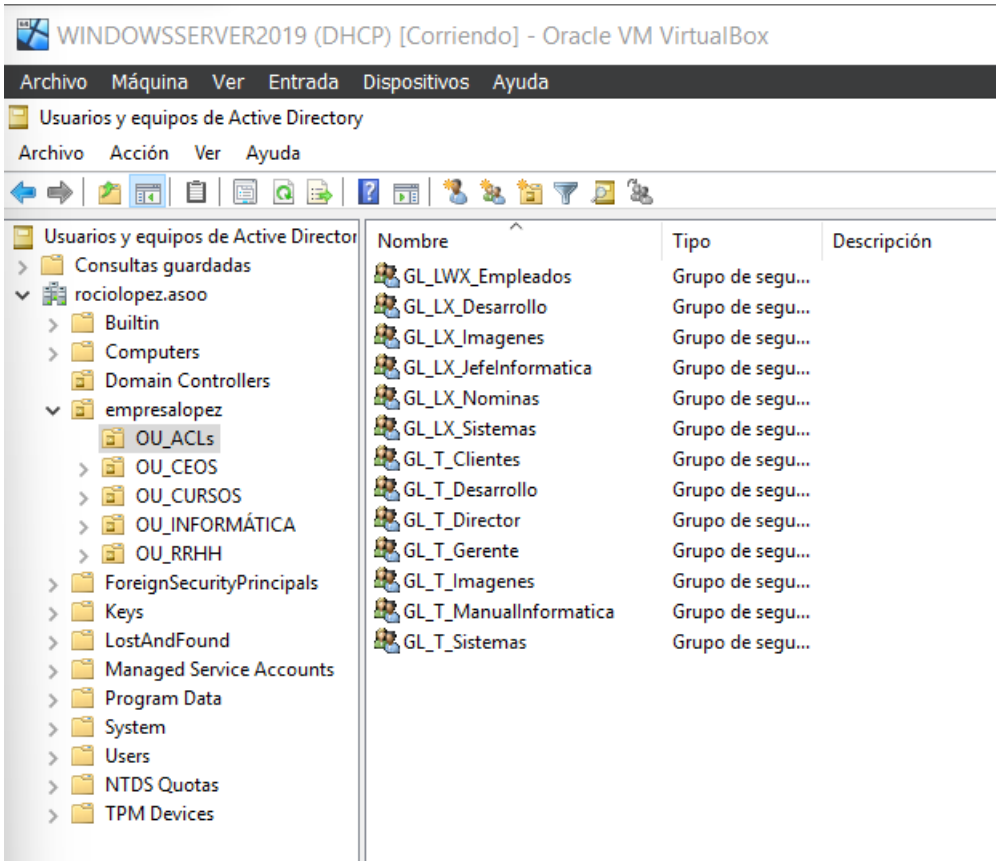
5.1- Diseña los grupos Locales de dominio para representar todo esto.

5.2 Rellena la siguiente tabla con todo el diseño pensado anterior. (EMPRESA)

Recurso	Usuarios con acceso y Tipo Acceso (permisos)	Grupo Local de dominio (ACL) a crear	GG miembros del grupo Local de dominio
Carpeta Nominas	Solo pueden acceder los CEOS (lectura)	GL_LX_Nominas	GG_Directores GG_Gerentes
Carpeta Imagenes	Jefe de informatica (Control Total)	GL_T_Imagenes	GG_ Informática
	Resto de informáticos (Leer)	GL_LX_Imagenes	GG_Sistemas GG_Desarrollo
Carpeta Desarrollo	Jefe de informática (Control total)	GL_T_Desarrollo	GG_ Informática
	Informáticos Desarrollo (lectura)	GL_LX_Desarollo	GG_Desarrollo
Carpeta Sistemas	Jefe de informática (Control total)	GL_T_Sistemas	GG_ Informática
	Informáticos Sistemas (lectura)	GL_LX_Sistemas	GG_Sistemas
Carpeta Director	Director (Control total)	GL_T_Director	GG_Directores
Carpeta Gerente	Gerente (Control total)	GL_T_Gerente	GG_Gerentes
Carpeta Empleados	Usuarios (Lectura, ejecución y escritura)	GL_LWX_Empleados	GG_RRHH
Carpeta ManualesInformatica	Usuarios Informática (control total)	GL_T_ManualInformatica	GG_Desarrollo GG_Informática GG_Sistemas
Carpeta Clientes	Gerente (Control total) Director (Control total)	GL_T_Clientes	GG_Gerentes GG_Directores

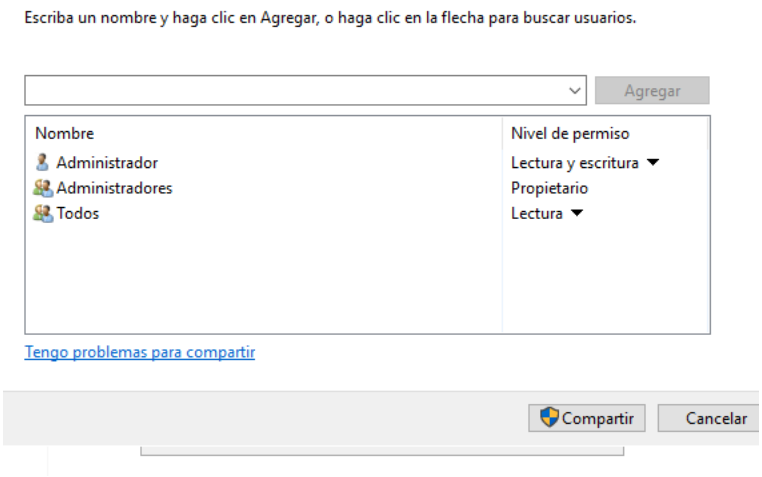
6 Crear los grupos locales y recursos.

Herramientas de AD-> Usuarios y Grupos de AD -> Seleccionar la OU -> botón derecho Nuevo Grupo tipo Dominio Local.

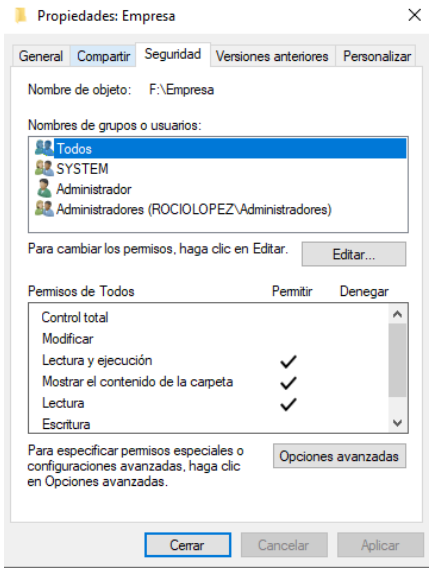


6.1 Crea los recursos carpetas

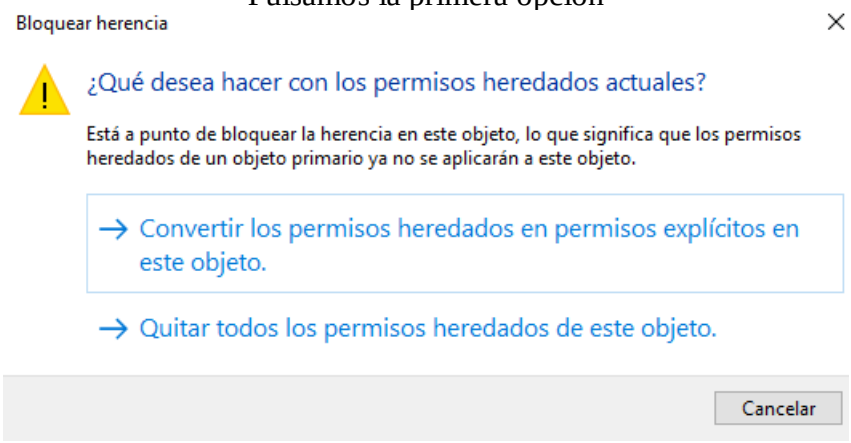
- Crea una carpeta padre con el nombre de la empresa. Compártela en la red
- Primero crearemos la carpeta “Empresa”, y la compartimos, en propiedades > Compartir y ponemos que “Todos” tengan permisos de Lectura.



- Luego en Seguridad, “Todos”, le pondremos solo permisos de “Lectura y ejecución”, si está protegido porque lo ha heredado, tendremos que deshabilitar la herencia en “Opciones avanzadas”.



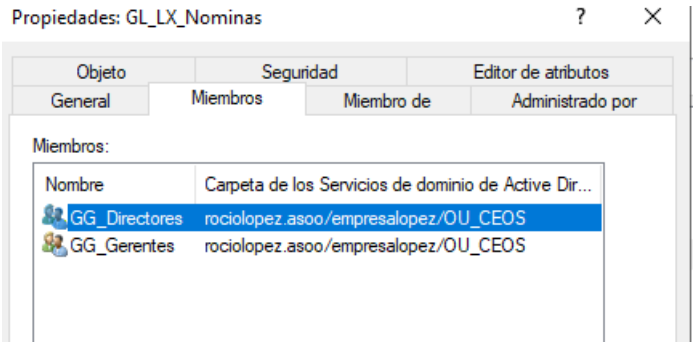
Pulsamos la primera opción



- Debajo de ella crea todos los recursos compartidos tipo carpetas según la tabla anterior.

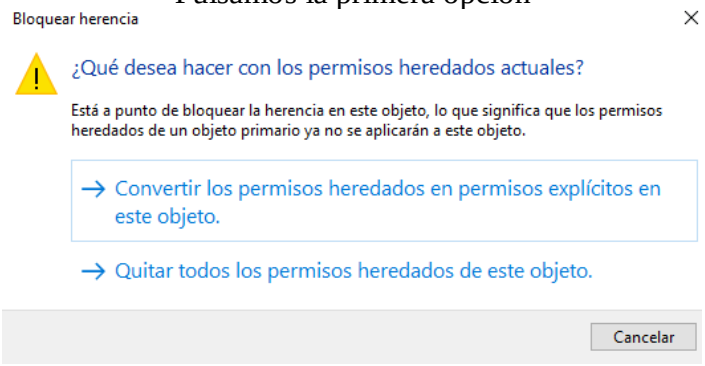
  - Todos los directivos (directores y gerentes) tienen acceso al resto de la información relevante de la empresa en modo de lectura

- Creamos ACLs

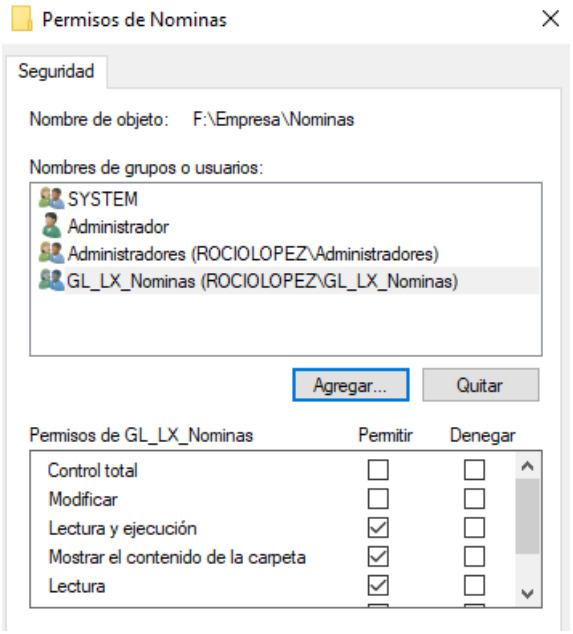


- Luego en Seguridad, “Todos”, lo quitaremos, si está protegido porque lo ha heredado, tendremos que deshabilitar la herencia en “Opciones avanzadas”.

Pulsamos la primera opción

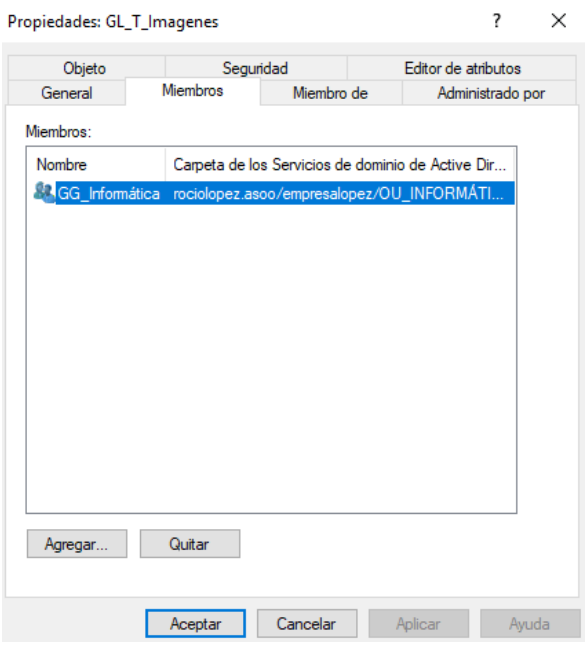


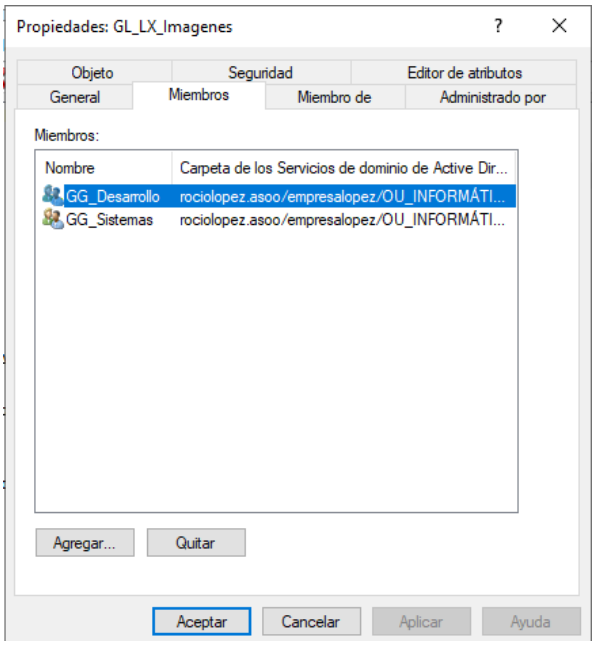
- Luego añadiremos el grupo local de nóminas, el cual contiene el grupo global de directores y el grupo global de gerentes, dándole permisos de “Lectura y ejecución”



- Una carpeta de Imágenes (.iso) para todo Informática. Podrán leer escribir todos los informáticos, pero el control de la carpeta lo tiene el jefe de informática.

- Creamos dos ACL para el grupo de informática y metemos el grupo global de usuarios de informática, y otra para el grupo global del jefe

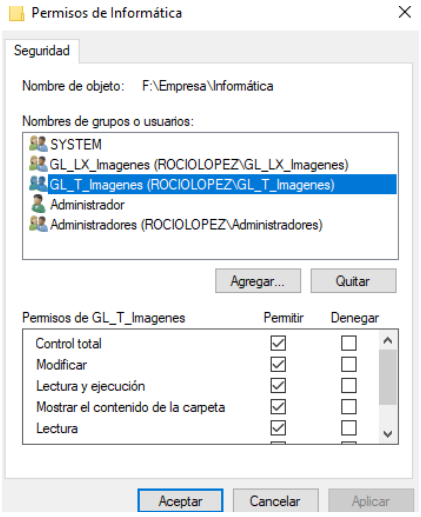


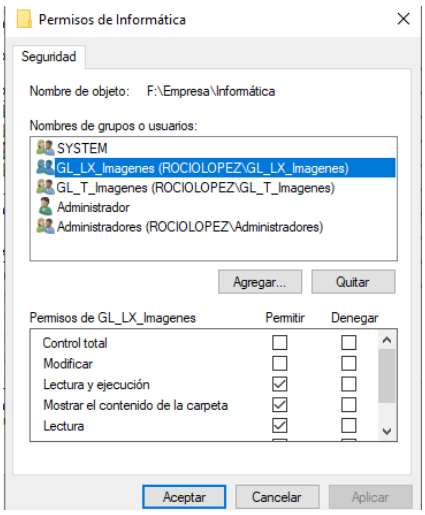


- Luego crearemos dentro de "Empresas" la carpeta "Imagenes" y deberá haber heredado el compartirse

- Luego en Seguridad, "Todos", lo quitaremos (Como en el punto anterior)

- Luego al grupo de informáticos le damos "Lectura y ejecución" y "Escritura, y al jefe de informática le pondremos el "Control total":

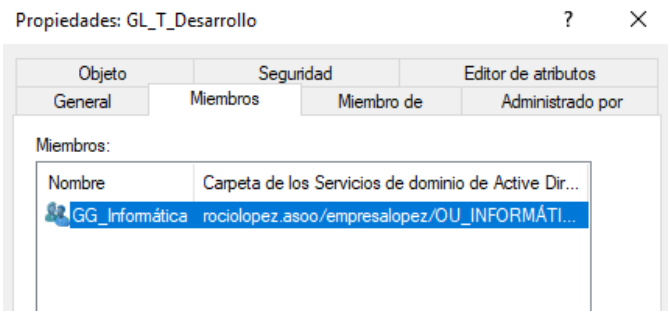


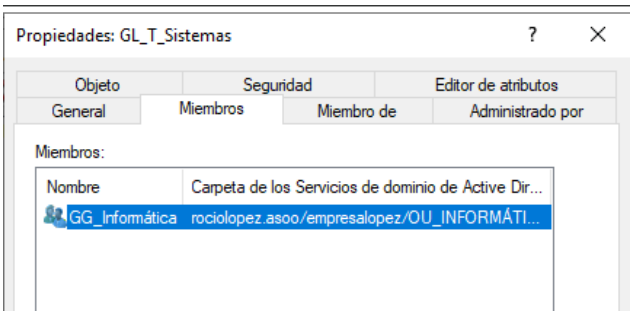


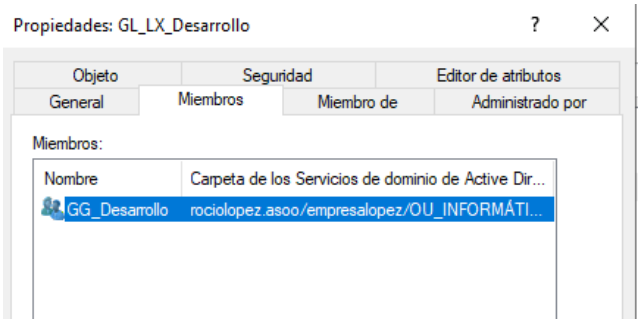
- Una carpeta para cada subdepartamento de informática. Solo podrán acceder los empleados de cada subdepartamento y el jefe de informática.

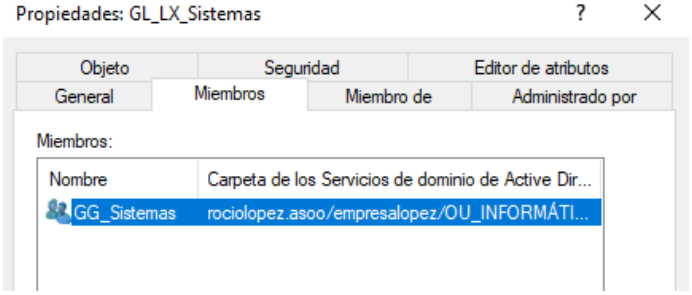
SEGUIMOS LOS PASOS DE LOS PUNTOS DE ANTES

- Creamos las ACLs:



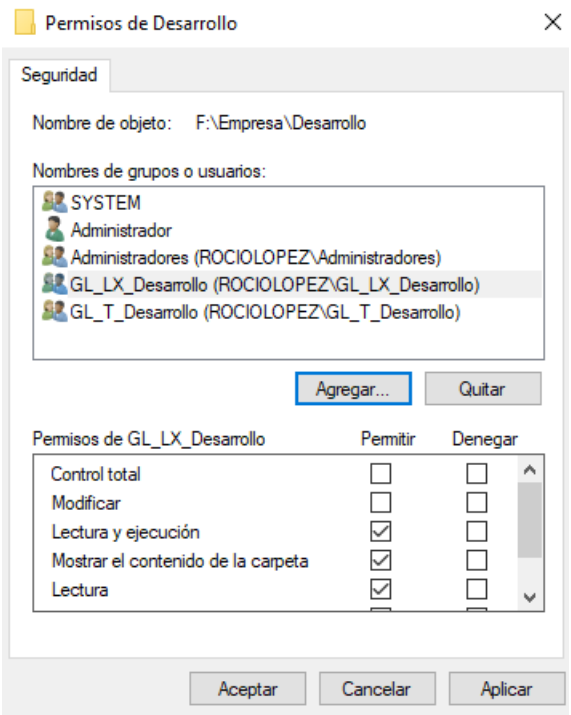


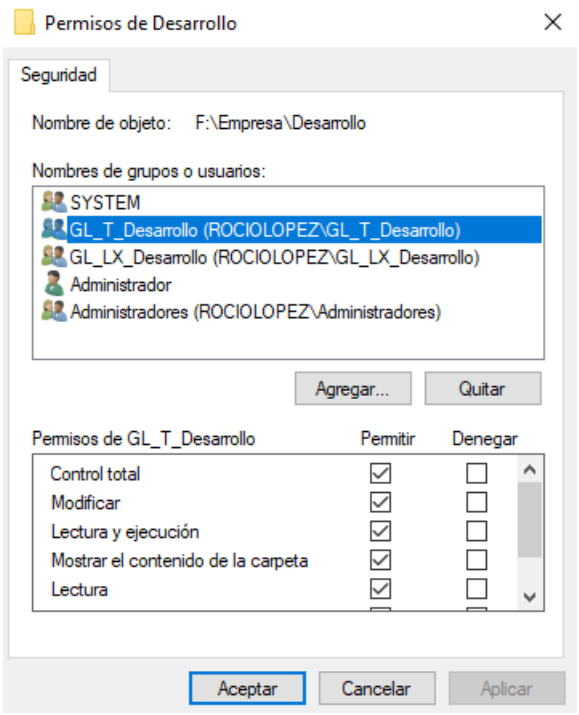




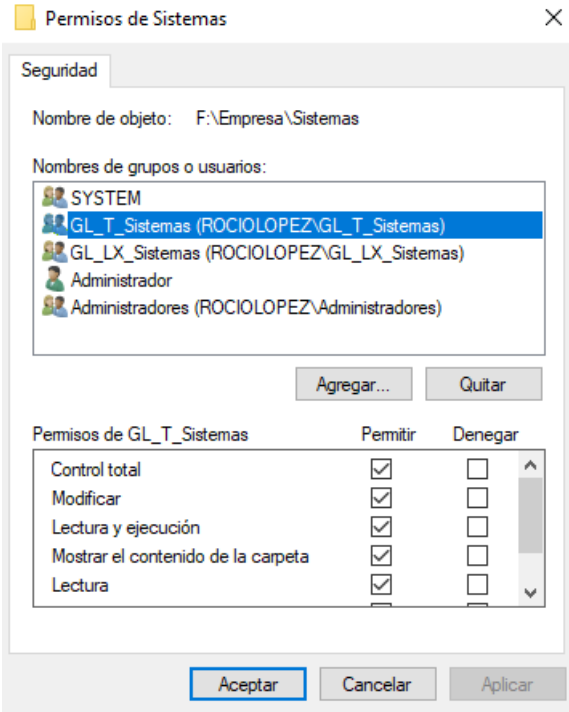
- Permisos de carpetas:

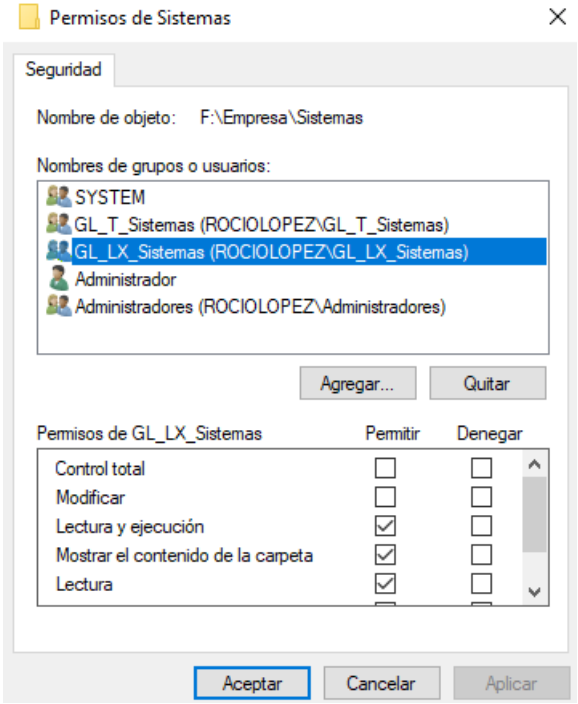
DESARROLLO:





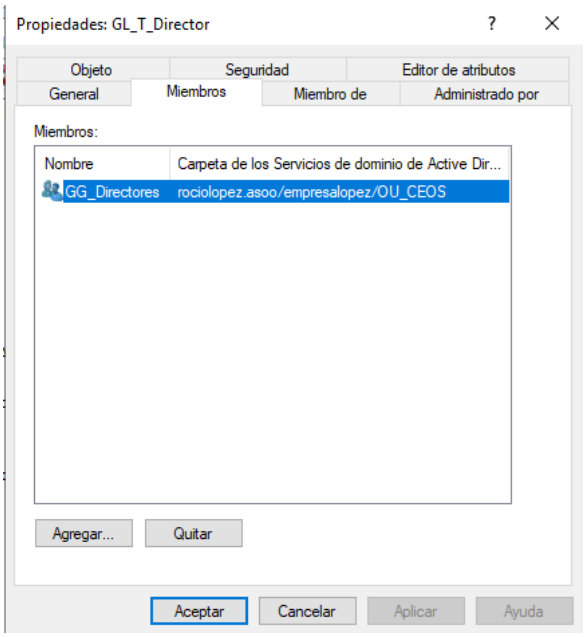
SISTEMAS:

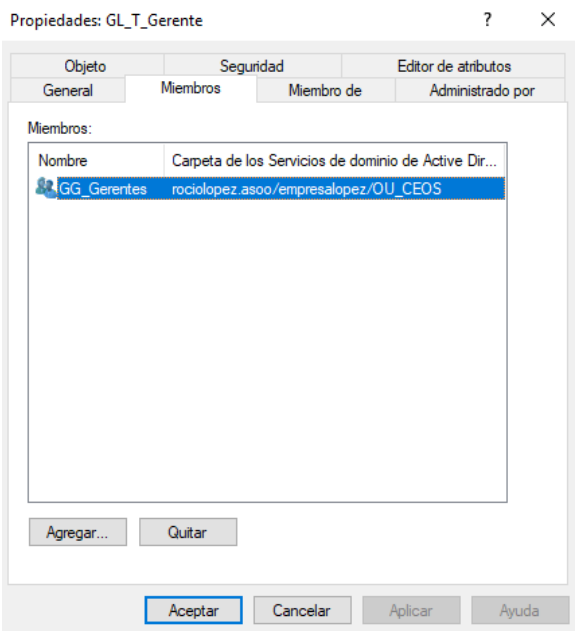




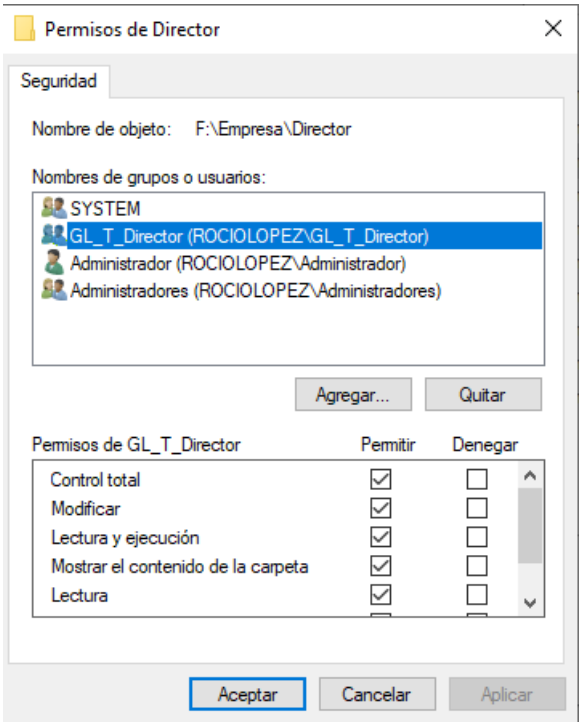
- El director y el gerente tienen sus propias carpetas. Cada uno tiene acceso a la suya.

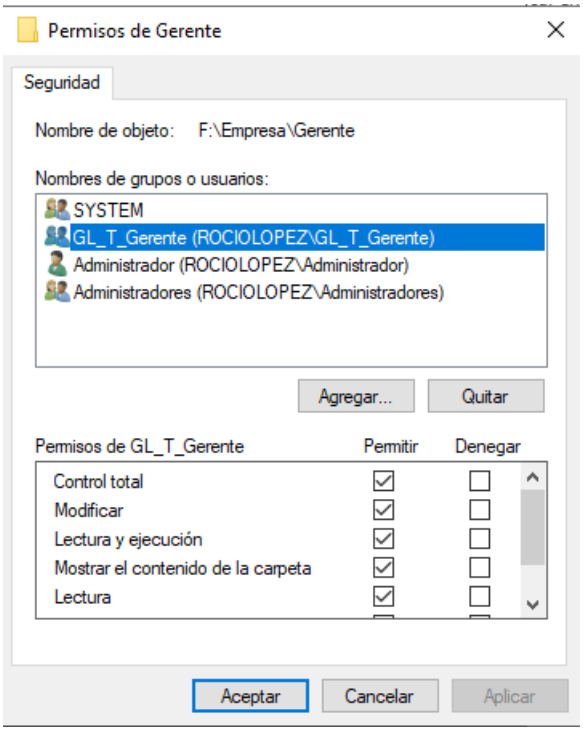
- Crear ACLs





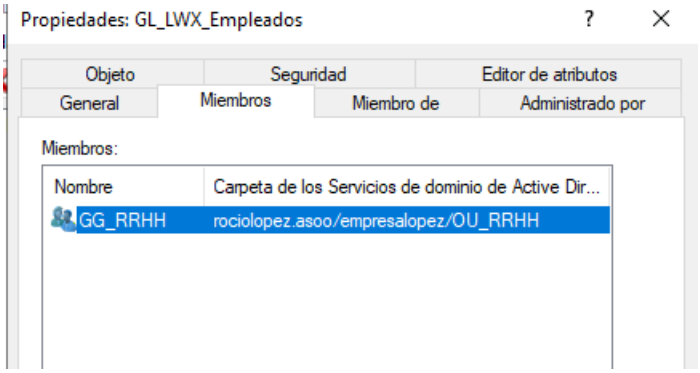
- Permisos



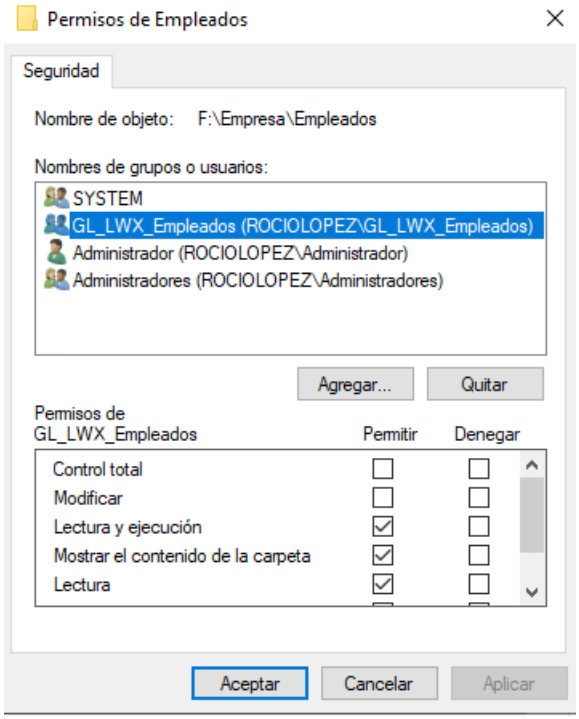


- El departamento de RRHH tendrá una carpeta compartida llamada EMPLEADOS. Podrán escribir los usuarios del dpto. Pero no tendrán control total.

- Crear ACLs

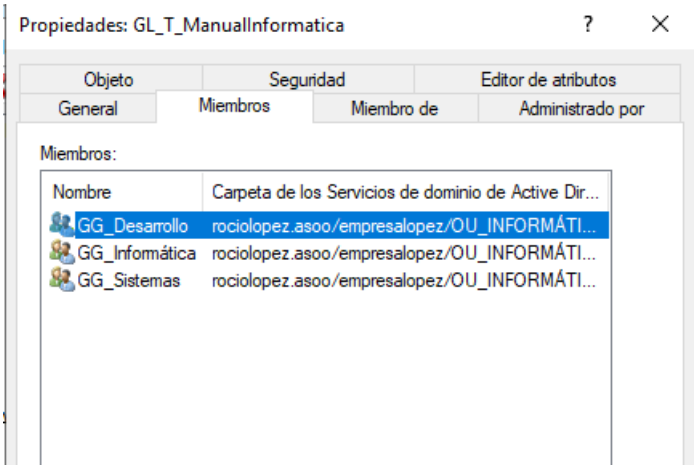


- Permisos

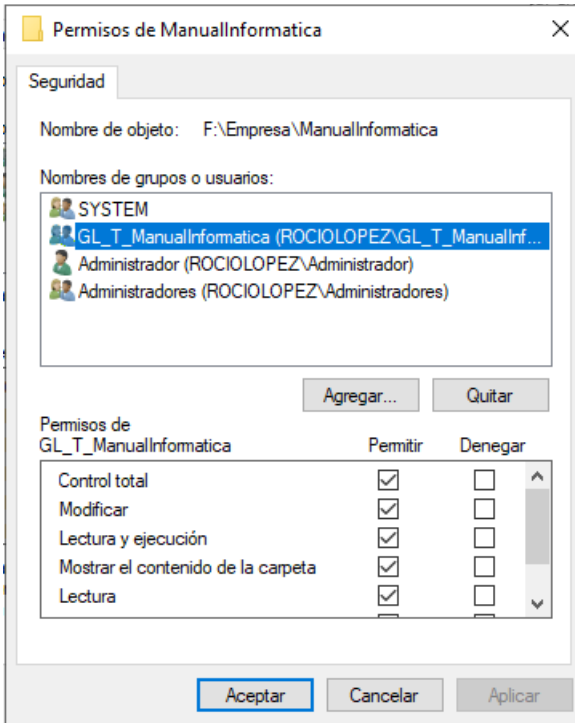


- El departamento de informática tendrá una carpeta general llamada “ManualesInformatica” y podrá controlar cualquier informático.

- Crear ACLs

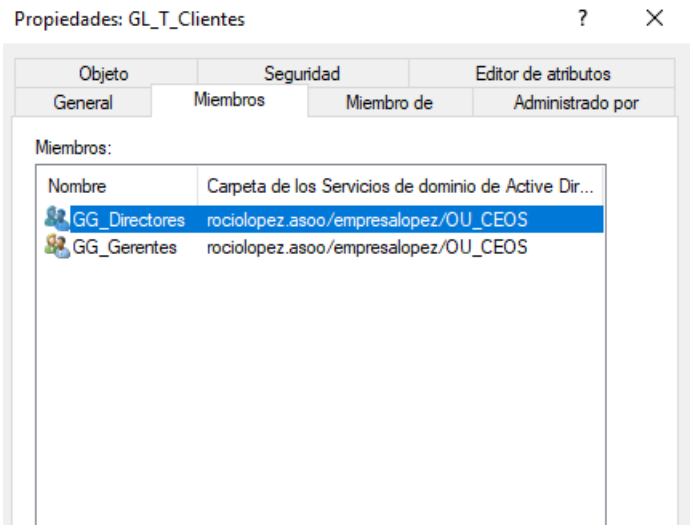


- Permisos

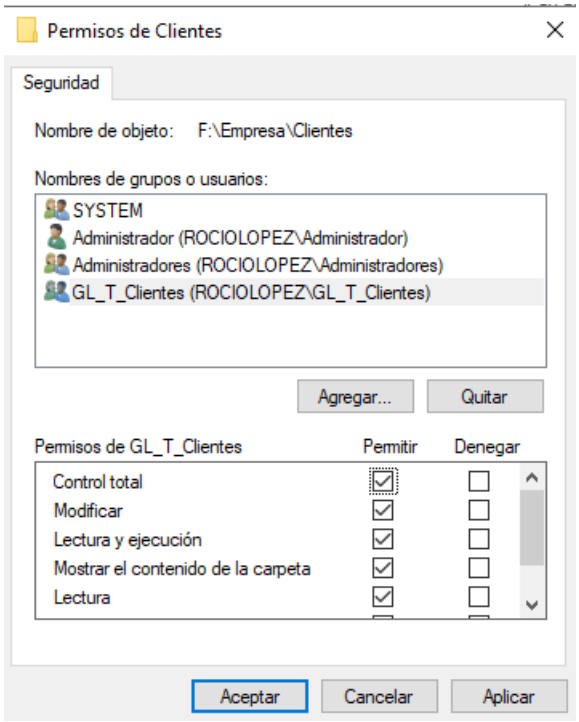


- Los gerentes y directores controlan una carpeta sobre CLIENTES.

- Crear ACLs

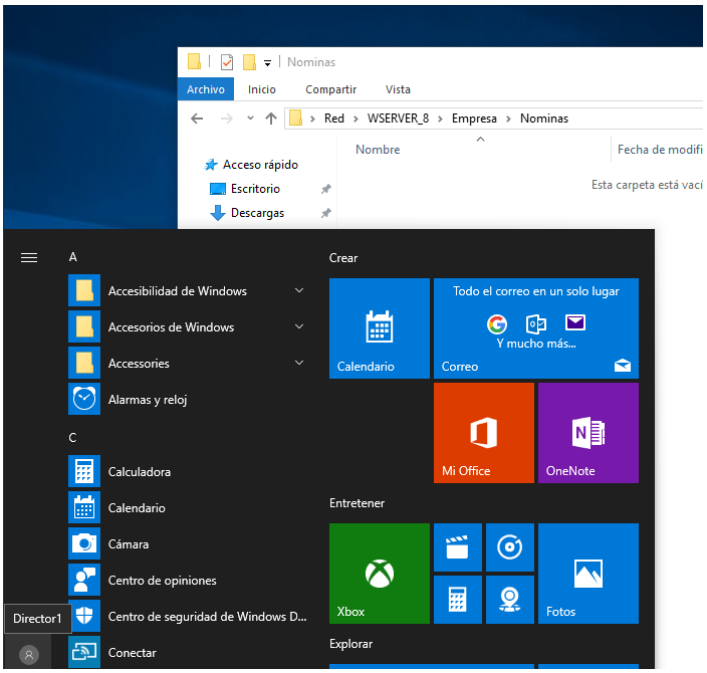


- Permisos

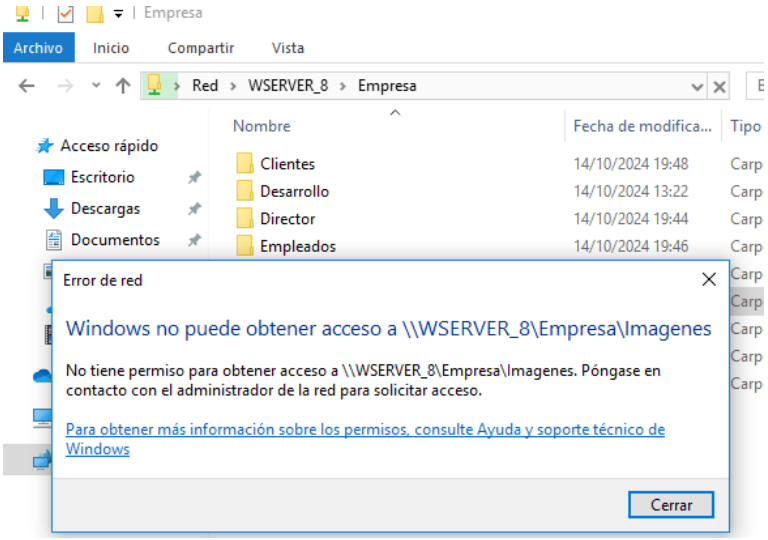


6.2 **Mostrar los recursos compartidos** Desde el Administrador de Equipos de Windows, mostrar las carpetas compartidas.

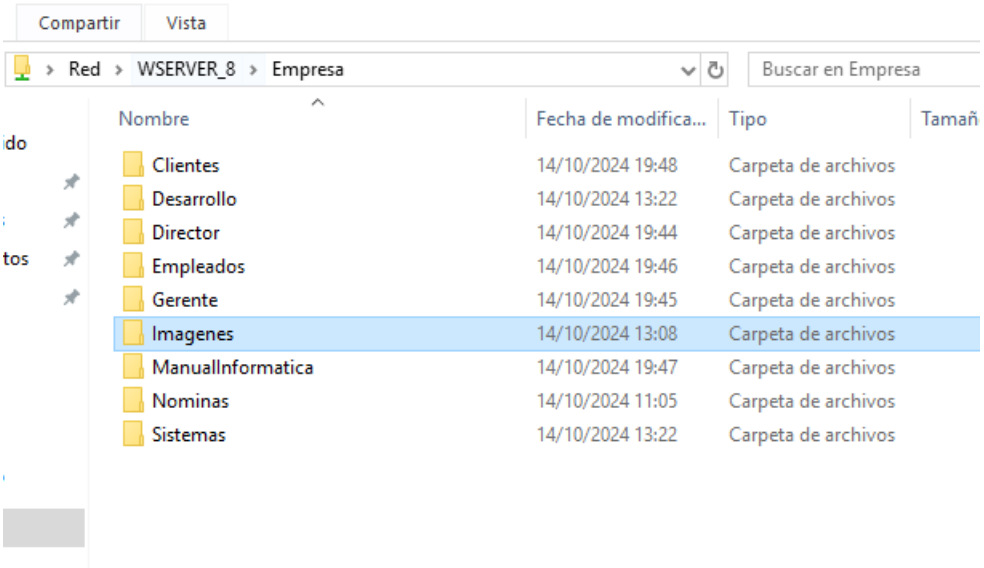
- Todos los directivos (directores y gerentes) tienen acceso al resto de la información relevante de la empresa en modo de lectura (ej. a las Nóminas)



Como vemos si intentamos acceder a otro recurso que no tenga permisos nos saldrá lo siguiente:



- Según en que cliente entremos nos dejará acceder a una carpeta u otra, y como ya hemos configurado antes estás son las copiones (cada usuario podrá entrar o no en cierta carpeta y realizar acciones dentro según su nivel de permisos asignado antes)



ANEXOS

ANEXO 1: Ayuda a crear los usuarios

Crea los usuarios.

Hay dos formas:
- Ir a cada OU y crear los usuarios y grupos dentro de ellas
Abrir Herramientas de AD-> Usuarios y Grupos de AD -> Seleccionar la OU (departamento) -> botón derecho Nuevo Usuario

- o crearlos fuera y luego moverlos (*ir al usuario o grupo o equipo y con botón derecho "Mover" a la OU).*
Nota: se da la circunstancia que el usuario desaparece del listado. Entonces, ¿es que un usuario no puede pertenecer a más de una OU? Claro que sí, pero para ello es mejor hacerlo de otra forma: si quieres copiarla de forma que permanezca en la OU original y al mismo tiempo sea parte de una OU nueva, la forma mas apropiada de hacerlo es creando grupo dentro de cada OU y agregando a ese usuario al grupo que has creado en cada OU nueva.

Recomendación: *deshabilitar la complejidad en las contraseñas:*

Inicio-Ejecutar-gpmc.msc
Doble Clik en el Dominio en cuestión → Botón Derecho en "Default Domain Policy" - Editar Configuración del Equipo -> Directivas ->Configuración de Windows-> Configuración de Seguridad -> Directivas de cuenta-> Directiva de Contraseñas.

ANEXO 2: Crear las carpetas y compartirlas.

Carpeta Perfiles$

Crea el directorio donde se almacenarán las carpetas personales de los usuarios (Escritorio, descargas, etc) . Se llamará Perfiles$ en lugar de que se cree por defecto en C: (como hace por defecto Windows) vamos a hacer que se almacene en la partición de datos.
Nota : El símbolo de $ al final, haciéndolo oculto en la red así los usuarios no podrán ver este recurso a no ser que conozcan su existencia.

- Compartir en la red la carpeta Perfiles$
  Compartir la carpeta desde las Propiedades de la carpeta
  o, desde el *Administrador del Servidor-> Servicios de archivos y almacenamiento → Recursos compartidos*
  Permisos de compartición:

  Control total "Usuarios del dominio"
  Control total: administrador

- Permisos de seguridad:
  - Permisos avanzados
  - ***Bloquear la herencia de permisos*** *para controlar que sólo un usuario acceda a su carpeta personal. Sólo debe tener acceso a todas las subcarpetas el administrador , el SYSTEM y poco más.*
  - Asegurarse que puede crear carpetas

- Creación de perfiles móviles :
  Y finalmente hacemos uso del recurso Perfiles$
  Asignar perfil: marcar todos los usuarios y asignarles \\servidor\Perfiles$\%username%
  El uso de la variable %username% hace que podamos asignar los perfiles móviles a los usuarios de forma "masiva", no individualmente.

  Nota: observar que, como ya se ha comentado, la carpeta es un recurso compartido y la forma de nombrarlo es con su nombre en red (nunca con la ruta local)