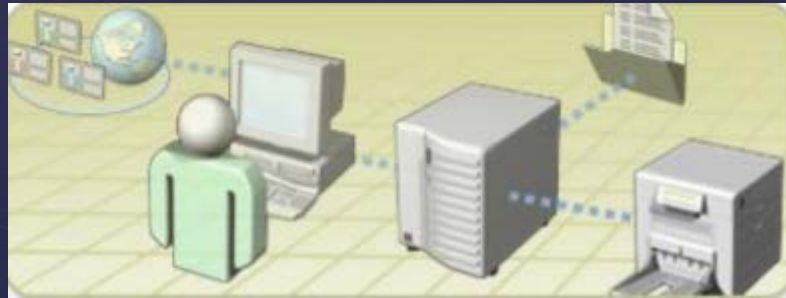


TEMA 7.

Administración de acceso a recursos



{ Implantación de Sistemas Operativos
1º ASIR
Profesora: Anabel Serradilla

CONTENIDOS

1. INTRODUCCIÓN
2. PERMISOS
3. GRUPOS DE TRABAJO
4. CARPETAS COMPARTIDAS
5. HERENCIA
6. RECOMENDACIONES
7. EJERCICIOS

1. INTRODUCCIÓN

- Uno de los objetivos de los sistemas informáticos es el de optimizar el uso de recursos → **COMPARTIR RECURSOS**
- Una de las tareas de los administradores de sistemas es gestionar la seguridad en el acceso a dichos recursos



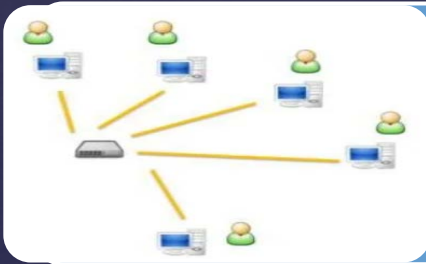
DERECHOS

PERMISOS

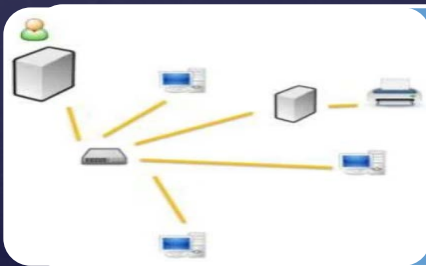
1. INTRODUCCIÓN

COMPARTIR RECURSOS

Tenemos varias formas de compartir recursos:



GRUPOS DE TRABAJO



DOMINIOS

1. INTRODUCCIÓN

USUARIOS

- Una cuenta de usuario es un objeto que posibilita el acceso a los recursos de dos modos:
 - Autenticando identidad. Solo inician sesión los usuarios con cuenta en el sistema
 - Autorizando o denegando el acceso a recursos del dominio
- Cada cuenta dispone de un SID (Security Identifier) único.

1. INTRODUCCIÓN

USUARIOS

- Cuentas predeterminadas: Administrador e Invitado
- Cuentas locales: para acceso a un servidor independiente.
- Cuentas de dominio o globales: permiten acceder a todos los recursos del dominio desde cualquier terminal asociado al servidor de dominio

1. INTRODUCCIÓN

GRUPOS

- Conjunto de objetos que pueden administrarse como un todo.
- Facilitan las tareas de administración y gestión.
- Hay grupos predefinidos: Administradores, Operadores de copia de seguridad, Operadores de impresión, ...

2. PERMISOS

DERECHOS

- Permiten autorizar las diferentes acciones o tareas que los usuarios o grupos de usuarios pueden desde el momento que entran en el sistema → Directivas de seguridad

Ejemplos:

- Inicio de sesión local
- Acceso al equipo desde la red
- Cambiar la hora del sistema
- Apagar el sistema

2. PERMISOS

PERMISOS

- Definen el tipo de acceso concedido a un usuario, grupo o equipo para un objeto.
- Se aplican a los objetos como archivos, carpetas, carpetas compartidas e impresoras.
- Se asignan a usuarios y grupos de Active Directory o de un equipo local

2. PERMISOS

PERMISOS

- Cada recurso dispondrá de un listado con los permisos que tiene cada usuario y grupos sobre él.

Ejemplos: lectura, escritura, ejecución, modificación, borrado, creación, ...

2. PERMISOS

PERMISOS

- Permisos estándar o predeterminados NTFS:
 - Control total: cambiar permisos, tomar la propiedad y todo lo que permiten los demás permisos
 - Modificar: modificar y borrar el archivo y lo que permite el permiso de Escritura y el de Lectura y ejecución

2. PERMISOS

PERMISOS

- Permisos estándar o predeterminados NTFS:
 - Lectura y ejecución: ejecución de aplicaciones y lo que permite Leer.
 - Escribir: sobrescribir el archivo, cambiar atributos, ver propietario del archivo, ...
 - Leer: leer el archivo y ver sus atributos, propietario y permisos

2. PERMISOS

PERMISOS

- Permisos estándar o predeterminados NTFS:
 - Lectura y escritura
 - Mostrar el contenido de la carpeta (solo carpetas): ver los nombres de los archivos y subcarpetas en la carpeta
- Permisos especiales: cambiar permisos, modificar atributos, tomar posesión, ...

2. PERMISOS

PERMISOS EFECTIVOS

- Cuando trabajamos localmente, nos afectan sólo los permisos de seguridad local. Pero cuando lo hacemos remotamente nos afectan también los permisos compartidos.
- El permiso efectivo es la combinación de todos los permisos “Permitido”, salvo los que tenga “Denegar”. Estos prevalecen siempre y ganan

2. PERMISOS

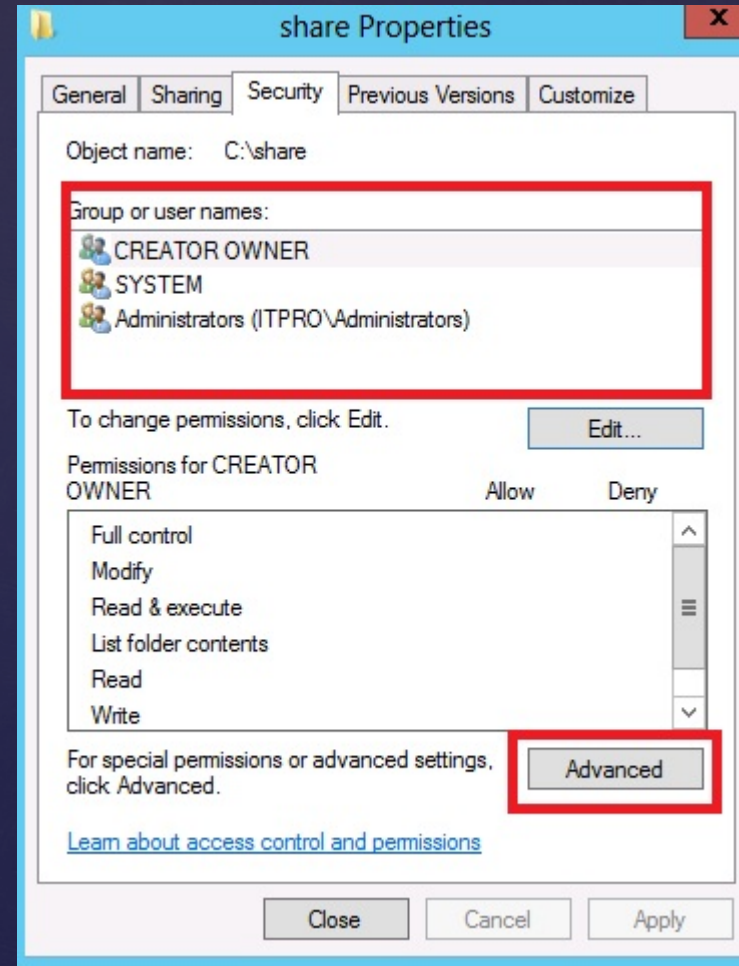
PERMISOS EFECTIVOS

- Por ejemplo, si de la pertenencia a un grupo tengo “Permitir Lectura” y de otro grupo “Permitir Escritura”, el permiso efectivo es “Lectura + Escritura”.
- Pero si por pertenencia a otro grupo obtengo algún “Denegar”, éste será el efectivo
- El permiso efectivo (final) será el más restrictivo entre todos los que apliquen.

2. PERMISOS

ACL (Access Control List)

Conjunto de reglas o permisos que especifican las condiciones necesarias para acceder a un objeto.



3. GRUPOS DE TRABAJO

- Es una de las posibles formas de organizar los equipos dentro de una red local
- Los equipos de un mismo grupo podrán verse entre ellos, compartir carpetas, impresoras, ...
- No se administran en común los permisos sino que cada equipo se administra de forma local

3. GRUPOS DE TRABAJO

- Relaciones entre equipos de igual a igual
- Número de equipos bajo
- Los equipos de un grupo de trabajo solo se verán si están en la misma red local
- El protocolo que gestiona los grupos de trabajo es SMB (Server Message Block)

4. CARPETAS COMPARTIDAS

- Permiten compartir carpetas para poder trabajar de forma colaborativa
- Se pueden establecer distintos permisos para distintos usuarios o grupos del sistema.
- Desde Propiedades del Explorador de Archivos o desde Herramientas administrativas / Administración de almacenamiento y recursos compartidos

4. CARPETAS COMPARTIDAS

Administración de almacenamiento y recursos compartidos

Administración de almacenamiento y recursos compartidos

Archivo Acción Ver Ventana Ayuda

Administración de almacenamiento y recursos compartidos (Local)

Recursos compartidos Volúmenes

5 entradas

Nombre ...	Protocolo	Ruta local	Cuota	Filtrad...	Instant...	Espaci...
Protocolo: SMB (5 elementos)						
ADMIN\$	SMB	C:\Windows	28,0 G			
ANABEL	SMB	c:\ANABEL	28,0 G			
C\$	SMB	C:\	28,0 G			
E\$	SMB	E:\	19,9 G			
IPC\$	SMB		-			

Acciones

Administración de almacenamiento y ...

- Conectarse a otro equipo...
- Aprovisionar almacenamiento...
- Aprovisionar recurso compartido...
- Administrar sesiones...
- Administrar archivos abiertos...
- Ver
- Nueva ventana desde aquí
- Actualizar
- Ayuda

IPC\$

- Detener uso compartido...
- Propiedades
- Ayuda

5. HERENCIA

- Facilitan la tarea de administrar permisos
- Permisos heredados son los que se propagan a un objeto desde otro objeto de nivel superior.

5. HERENCIA

- Copiar archivos: el archivo copiado hereda los permisos de la carpeta que lo contiene
- Mover archivos:
 - Si se mueven dentro del mismo disco cambian los permisos heredados, pero se mantienen los específicos del archivo
 - Si se mueven a otro disco solo hereda los nuevos permisos ya que mover = copiar + borrar el original

6. RECOMENDACIONES

- Conceder permisos a los grupos locales, en lugar de a los usuarios
- Agrupar los recursos para simplificar la administración
- Autorizar a los usuarios sólo el nivel de acceso que necesiten, no más

6. RECOMENDACIONES

- Conceder permiso de lectura y ejecución para las carpetas de aplicaciones
- Conceder permisos de lectura y ejecución, y de escritura para las carpetas de datos

7. EJERCICIOS

- Nombre servidor
- Conexión a grupo de trabajo
- Definir carpetas compartidas
- Definir permisos asociados
- Realizar pruebas de acceso