

CIPFP Mislata

Luis García Bonifaz - l.garciabonifaz@edu.gva.es

SOM T06 - Administración Windows

Actividad 2

Actividad 2: Estructura de empresa y permisos NTFS por departamentos

Contexto

Una empresa pequeña quiere organizar su información por departamentos y proyectos. Hay conflictos porque:

- Algunos usuarios ven carpetas que no deberían.
- Otros pueden borrar documentos sin querer.
- Los responsables necesitan acceso total.
- El equipo de soporte debe poder recuperar y auditar, pero sin trabajar como “dueño” de los archivos.

Tu misión es **diseñar y aplicar una estructura de permisos** basada en **grupos**, no en usuarios individuales, y **demostrar con pruebas** que funciona.

1) Objetivos

Al finalizar, el alumnado será capaz de:

- Diseñar un modelo de permisos por **roles** (grupos).
- Aplicar permisos NTFS correctos usando **herencia** y **excepciones**.
- Entender la diferencia entre **Listar carpeta**, **Leer**, **Modificar**, **Control total** y permisos avanzados (eliminar, crear, escribir).
- Aplicar y justificar una **ruptura de herencia** en subcarpetas.
- Verificar con **Permisos efectivos / Acceso efectivo** y con pruebas reales (logins).
- Documentar el diseño y las evidencias.

2) Preparación (usuarios y grupos)

Si ya tienes cuentas del ejercicio anterior, reutilízalas. Si no, créalas.

Usuarios

- `ana_admin` (Administración)
- `dani_com` (Comercial)
- `carmen_it` (IT)
- `sergio_dir` (Dirección)
- `soporte` (cuenta técnica / administradora, para recuperación)

!!! Warning "Cuidado"

Si creas las cuentas de usuario con PowerShell debes añadirlos de forma manual al grupo Usuarios, sino no aparecerán en la pantalla de inicio para seleccionarlos

Grupos (roles)

- `GG_Direccion`
- `GG_Administracion`
- `GG_Comercial`
- `GG_IT`
- `GG_Todos` (incluye a los empleados, excluye soporte si así lo decides)

3) Estructura de carpetas (a crear)

Crea un script de PowerShell que cree esta estructura en `C:\USERS\tu_usuario\EMPRESA`.

```
EMPRESA
|
|— 00_PUBLICO
|   |— Plantillas
|   |— Comunicados
|
|— 10_ADMIN
|   |— Facturas
|   |— Nominas
|   |— Proveedores
|
|— 20_COMERCIAL
|   |— Clientes
|   |— Ofertas
|   |— Contratos
|
|— 30_IT
|   |— Documentacion
|   |— Scripts
|   |— Backups
|
|— 99_DIRECCION
|   |— Estrategia
|   |— Confidencial
```

4) Reglas de negocio (lo que debe cumplirse) — MUY IMPORTANTE

Estas reglas definen el reto. Tu configuración debe cumplirlas **exactamente**:

Regla A — Público (00_PUBLICO)

1. Todos los empleados (GG_Todos) pueden:
 - **Leer** 00_PUBLICO completo.
2. Solo GG_IT puede:
 - **Modificar** 00_PUBLICO\Plantillas.
3. En 00_PUBLICO\Comunicados:
 - GG_Direccion puede **Modificar**.
 - GG_Todos solo **Leer**.

Regla B — Administración (10_ADMIN)

1. Solo GG_Administracion y GG_Direccion pueden acceder a 10_ADMIN.
2. GG_Administracion tiene:
 - **Modificar** en 10_ADMIN y subcarpetas.
3. GG_Direccion tiene:
 - **Lectura** en 10_ADMIN, salvo Nominas donde tiene **Control total**.
4. Nadie más (ni Comercial ni IT) debe **ver** el contenido de 10_ADMIN.

Regla C — Comercial (20_COMERCIAL)

1. GG_Comercial puede **Modificar** todo 20_COMERCIAL.
2. GG_Direccion puede **Lectura** en todo 20_COMERCIAL.
3. Subcarpeta 20_COMERCIAL\Contratos:
 - Solo GG_Comercial y GG_Direccion pueden acceder.
 - IT **no** debe ver esta carpeta.

Regla D — IT (30_IT)

1. GG_IT tiene **Modificar** en 30_IT\Documentacion.
2. 30_IT\Scripts:
 - Solo GG_IT puede acceder.
 - Y dentro, cada usuario de IT debe poder modificar **solo sus scripts**:
 - Crea subcarpetas: Scripts\carmen_it, Scripts\carlos_it (si no existe, inventa otro usuario IT).
 - Cada usuario solo puede modificar su carpeta.
 - GG_IT puede leer todo Scripts, pero no modificar carpetas ajenas.
 - soporte (admin) puede Control total en todo 30_IT.
3. 30_IT\Backups:






- Solo `soporte` puede Control total.
- `GG_IT` solo Lectura.

Regla E — Dirección (99_DIRECCION)

1. Solo `GG_Direccion` puede acceder a `99_DIRECCION`.
2. `99_DIRECCION\Confidencial`:
 - Solo `sergio_dir` (usuario) debe tener acceso total.
 - Ni siquiera otros de Dirección (si los hay) deben entrar.
3. Todo lo anterior debe seguir permitiendo que `soporte` (admin) pueda recuperar información (por ser admin), pero el informe debe explicar la diferencia entre:
 - acceso por permisos NTFS
 - acceso por privilegios de administrador / tomar posesión

5) Pruebas prácticas (opcionales)

Para cada usuario (ana_admin, dani_com, carmen_it, sergio_dir):

1. Inicia sesión o usa "Ejecutar como usuario" y prueba:
 - Entrar en carpetas permitidas.
 - Confirmar que carpetas prohibidas **no se ven** o dan acceso denegado (según diseño).
2. En carpetas con Modificar:
 - Crear archivo
 - Modificar
 - Renombrar
3. En `Clientes` (Comercial) prueba específicamente:
 - Crear archivo 
 - Modificar archivo 
 - Intentar borrar archivo  (debe fallar)
4. En `Scripts` (IT) prueba:
 - Carmen puede modificar `Scripts\carmen_it`
 - Carmen no puede modificar `Scripts\carlos_it`
 - IT (grupo) puede leer ambos
5. En `99_DIRECCION\Confidencial`:
 - `sergio_dir` entra 
 - otro usuario de Dirección (si creas uno) no entra 

6) Entregables

1. Permisos

- Captura de pantalla de la configuración avanzada de cada carpeta y subcarpeta en la que se vean todos los permisos con:

2. Informe con:

- Justificación del diseño (por qué así)
- Capturas clave
- Explicación de herencia y rupturas

3. Script

- Script de creación de carpetas.

Todo en un zip con:

- Informe en formato PDF
- Script de PowerShell