FUNDAMENTACIÓN CONCEPTUAL: PERMISOS NTFS Y CONTROL DE ACCESO 🔒

1. El Concepto de Control de Acceso y las Dos Capas

El **Control de Acceso** es el proceso por el cual el sistema operativo decide si una identidad (usuario o grupo) puede realizar una acción específica (leer, modificar) sobre un recurso. En Windows, este proceso se gestiona mediante dos capas de permisos.

1.1 Permisos de Compartición (Share Permissions)

Los Permisos de Compartición son la **primera capa de defensa**. Se aplican a la **carpeta compartida** (`\\servidor\carpeta`) y determinan si un usuario puede **establecer una conexión** con el recurso a través de la red (vía protocolo SMB/CIFS).

- **Alcance:** Solo se aplican cuando el acceso es **remoto** (a través de la red). Si accedes al archivo directamente en el servidor (localmente), se ignoran.
- **Permisos Clave:** Son simples: **Leer**, **Cambiar** y **Control Total**.
- **Regla Práctica Organizacional:** Se recomienda dar el permiso de **Control Total** al grupo de **Dominio Local (DLG)** que contiene a los usuarios. Esto se hace para que el control granular de la seguridad recaiga por completo en la capa NTFS (la segunda capa), simplificando la administración de la compartición.

1.2 Permisos NTFS (New Technology File System)

Los Permisos NTFS son la **segunda capa de defensa y el control de seguridad definitivo**. Se aplican a **archivos y carpetas** y definen exactamente qué acciones puede realizar el usuario una vez que ha accedido al recurso.

- **Alcance:** Se aplican tanto al acceso **remoto** como al acceso **local** (directamente en el servidor).
- **Permisos Clave:** Son granulares: **Leer**, **Escribir**, **Modificar**, **Control Total**, **Recorrer carpeta**, etc.
- **Regla de Oro:** El acceso final de un usuario es el **permiso más restrictivo** entre la capa de Compartición y la capa NTFS.

Ejemplo: Si el permiso de Compartición es **Control Total**, pero el permiso NTFS es solo **Leer**, el usuario solo podrá **Leer**.

---

2. Principios de Seguridad en la Asignación de Permisos

La correcta asignación de permisos es más un arte de seguridad que una simple configuración técnica.

2.1 El Principio del Mínimo Privilegio (PoLP)

El **Principio del Mínimo Privilegio (PoLP)** es la piedra angular de la seguridad. Dicta que un usuario o servicio solo debe tener los derechos y permisos **estrictamente necesarios** para realizar su trabajo.

- **Justificación:** Si un usuario solo necesita ver documentos, no se le debe dar la capacidad de modificarlos o eliminarlos. Esto previene la **eliminación accidental**, limita el daño potencial de *ransomware* (que solo puede cifrar archivos a los que el usuario tiene permiso de **Modificación**) y reduce el riesgo de ataques internos.
- **Aplicación Práctica:** No usar jamás el permiso de **Control Total** para usuarios estándar, sino solo el permiso de **Modificar** o **Lectura**.

2.2 La Herencia y Denegación Explícita

- **Herencia:** Los permisos se heredan por defecto de la carpeta principal a las subcarpetas y archivos. Si la carpeta raíz tiene permiso de Lectura para el grupo `GG-Ventas`, todas las subcarpetas lo heredarán. Esto simplifica la gestión.
- **Desactivación de Herencia:** Para crear carpetas con seguridad especial (ej., una carpeta de "Gerencia" dentro de la carpeta "Datos"), se debe **desactivar la herencia** en esa subcarpeta para romper la cadena y aplicar un conjunto de permisos únicos.
- **Denegación Explícita:** El permiso de **Denegación** anula a cualquier otro permiso, incluyendo el de Control Total. Su uso está **desaconsejado** a menos que sea absolutamente necesario, ya que complica la auditoría y la solución de problemas.

2.3 El Modelo AGDLP en la Práctica de Permisos

El modelo **AGDLP** consolida la seguridad y la auditoría. Los permisos NTFS **nunca** deben asignarse a usuarios individuales ni a Grupos Globales (GG).

Elemento	Función en la Asignación de Permisos	Riesgo de No Usarlo
GG (Grupo Global)	**No recibe Permisos NTFS.** Solo contiene usuarios con el mismo rol funcional.	Si se asigna permiso a GG, es difícil mover usuarios de una unidad organizativa a otra sin afectar los permisos.
DLG (Grupo de Dominio Local)	**Recibe el Permiso NTFS (Modificar/Leer) directamente.** Su nombre debe indicar el recurso y el acceso (Ej., `DL-RW_DatosVentas`).	Si se asigna permiso directamente a los usuarios, la administración es imposible de

	escalar (N usuarios = N asignaciones).

Exportar a Hojas de cálculo

---

3. Trabajo Práctico: Implementación Detallada de Permisos (Clase 4)

3.1 Escenario de Permisos

- **Servidor:** `SRV-ARCHIVOS`
- **Recurso:** Carpeta `D:\Datos_Compartidos`
- **Requerimiento:** El grupo `GG-Ventas` debe tener la capacidad de crear, leer y modificar archivos en `D:\Datos_Compartidos\Ventas`.

3.2 Pasos de Implementación

Paso	Acción Técnica	Objetivo de Seguridad
1. Creación del DLG	Crear el grupo **`DL-RW_DatosVentas`** (Dominio Local) en la OU de Grupos.	Seguir el modelo **AGDLP**. Este es el objeto que recibirá los permisos.
2. Anidamiento	Añadir el grupo **`GG-Ventas`** como miembro del grupo **`DL-RW_DatosVentas`**.	Conectar la identidad del usuario (GG) con el permiso del recurso (DLG).
3. Permisos de Compartición	En la pestaña **Compartir** de `D:\Datos_Compartidos`: Asignar **Control Total** al grupo **`DL-RW_DatosVentas`**.	Permitir la conexión de red (el Control Total aquí no es peligroso, ya que NTFS actuará como filtro).
4. Permisos NTFS (Filtro Final)	En la pestaña **Seguridad** (NTFS) de `D:\Datos_Compartidos`: - Deshabilitar la herencia. - Asignar el permiso **Modificar** al grupo **`DL-RW_DatosVentas`**. - Asignar el permiso **Control Total** al grupo de **`GG-Admin_Infraestructura`**.	Aplicar el **Mínimo Privilegio**. El permiso **Modificar** es el correcto para la creación/escritura de datos sin dar acceso para cambiar permisos. El **Control Total** es solo para IT.

Exportar a Hojas de cálculo

3.3 Verificación y Solución de Problemas

Tras la asignación, es vital verificar la efectividad:

Herramienta	Uso
Ventana de Permisos Avanzados (NTFS)	Usar la pestaña **"Acceso Efectivo"** para verificar qué permisos finales obtiene un usuario específico (ej., `alopez`) sobre un archivo. Esta es la herramienta de diagnóstico principal para el administrador.
Cliente de Red	Acceder al recurso (`\\srv-archivos\datos_compartidos`) como el usuario `alopez` y comprobar que puede crear y modificar archivos (Permiso Modificar), pero no puede cambiar la pestaña de **Seguridad** (no tiene Control Total).