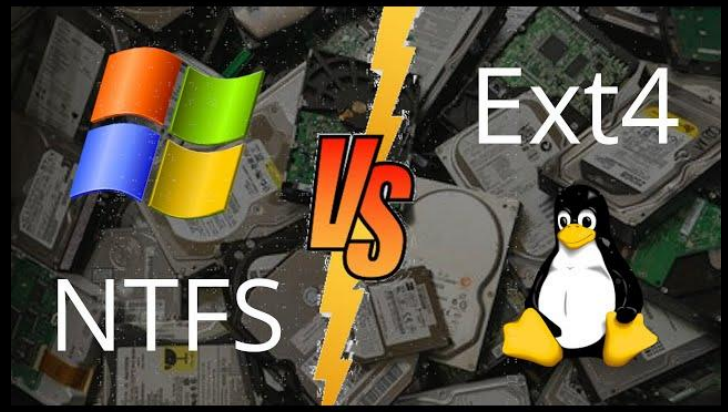
CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB

¿QUÉ ES UN SISTEMA DE ARCHIVOS?

Definición:

- Estructura lógica para organizar, almacenar y acceder a datos en discos duros, SSDs, etc.
  Funciones clave:
  - Gestionar espacio en disco.
  - Controlar permisos de acceso.
    Tipos comunes:
- Windows: NTFS (moderno), FAT32 (antiguo).
- Linux: ext4 (predeterminado en muchas distribuciones).



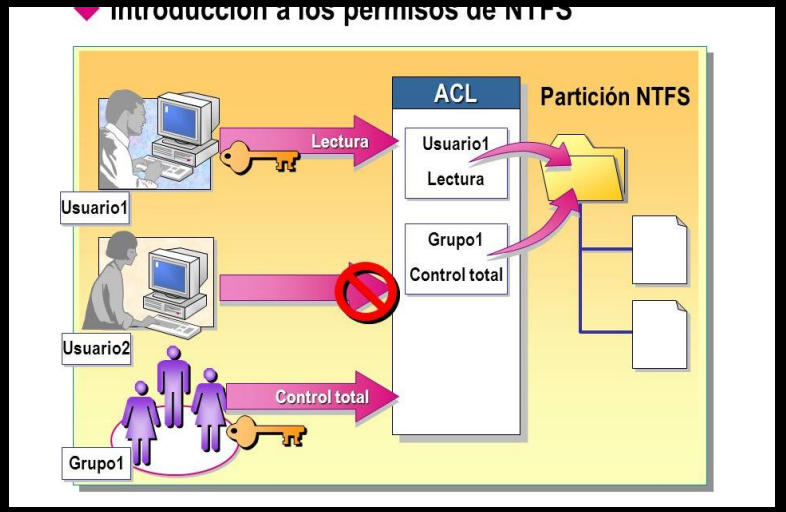
SEGURIDAD EN NTFS (WINDOWS)

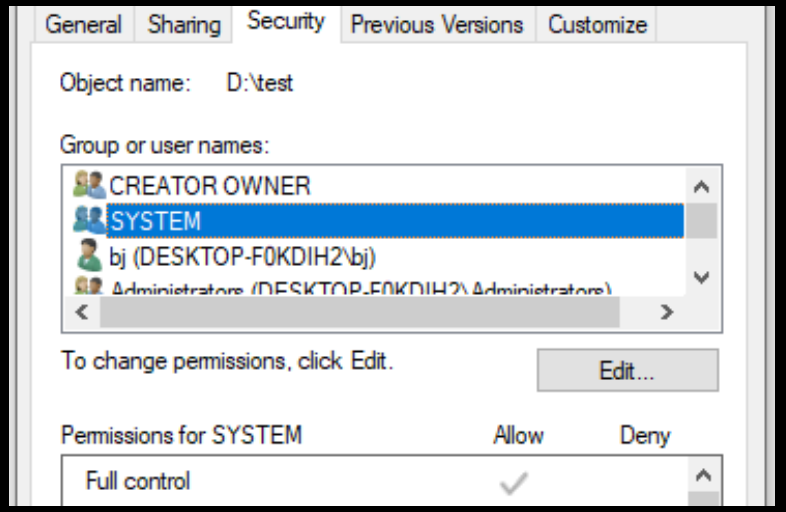
Permisos básicos:

- Lectura (Read), Escritura (Write), Ejecución (Execute). Permisos avanzados (DAC - Control de Acceso Discrecional):
- Permiten definir accesos específicos por usuario/grupo. Ejemplo práctico:

  icacls C:\web /grant usuario:(OI)(CI)RX

- Explicación: Otorga al usuario permiso de lectura (R) y ejecución (X) en la carpeta web, con herencia a subcarpetas (OI: Object Inherit, CI: Container Inherit).



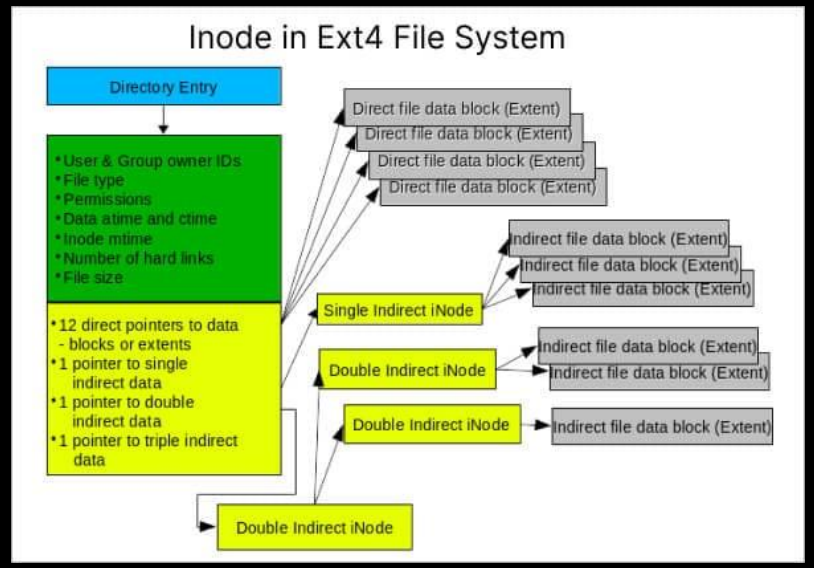


SEGURIDAD EN EXT4 (LINUX)

Permisos básicos:

- r (lectura), w (escritura), x (ejecución).
  Permisos avanzados:
- setuid (ejecutar como propietario), setgid (herederar grupo), sticky bit (evitar borrado de archivos por otros).
  Ejemplo práctico:

  chmod 755 /var/www/html
- Explicación:
  - Propietario: Lectura, escritura, ejecución (7 = 111 en binario).
  - Grupo y otros: Lectura y ejecución (5 = 101 en binario).



COMPARATIVA NTFS VS EXT4

Característica	NTFS (Windows)	ext4 (Linux)
Seguridad	Alta (DAC + ACLs)	Alta (Permisos Unix + ACLs)
Configuración	Interfaz gráfica + comandos	Principalmente comandos
Escenario típico	Entornos empresariales	Servidores web y desarrollo

GESTIÓN DE PERMISOS - BUENAS PRÁCTICAS

1. **Principio del menor privilegio:**
   - Otorgar solo los permisos necesarios (ej: no dar escritura si solo se necesita lectura).
2. **Auditoría periódica:**
   - Revisar permisos con herramientas como icacls (Windows) o ls -l (Linux).
3. **Evitar permisos 777 en Linux (acceso total a todos).**

CASO PRÁCTICO - PROTECCIÓN DE UNA CARPETA WEB

Escenario:

- **Carpeta /var/www/html (Linux) o C:\web (Windows) con archivos HTML, CSS y JS.**
  Pasos:

1. **Linux:**

   chmod 750 /var/www/html # Propietario: RWX, Grupo: RX, Otros: Ninguno

   chown www-data:www-data /var/www/html # Asignar propietario y grupo correctos

2. **Windows:**

   - **Usar icacls para restringir accesos no esenciales.**

RIESGOS DE UNA MALA CONFIGURACIÓN

Ejemplos reales:

- **Sitios web hackeados por permisos 777 en Linux.**
- **Exposición de bases de datos por permisos de escritura global en NTFS.**

Consecuencias:

- **Pérdida de datos.**
- **Daño a la reputación.**

RESUMEN Y CONCLUSIONES

Puntos clave:

- **Los sistemas de archivos (NTFS/ext4) son la base de la seguridad en servidores web.**
- **La gestión de permisos debe ser proactiva y rigurosa.**
  Acciones recomendadas:
- **Automatizar revisiones de permisos.**
- **Documentar políticas de acceso.**