

**TRABAJO REALIZADO POR: © ALEJANDRO GUERRA ABÁN, BRIAN BURGOS RECUERO Y JOSE ZAPATERO LÓPEZ**

## 1. Analizar accesos

Completa la siguiente tabla indicando si cada usuario puede Leer (L), Escribir (E) o Eliminar (X) archivos en cada carpeta.

Marca con ✓ si puede, ✗ si no puede.

CARPETA	JUAN	ANA	LUIS	MARTA
FINANZAS	L✓ E✓ X✓	L✓ E✗ X✗	L✓ E✗ X✗	L✓ E✗ X✗
VENTAS	L✓ E✗ X✗	L✓ E✓ X✓	L✓ E✗ X✗	L✓ E✗ X✗
IT	L✗ E✗ X✗	L✗ E✗ X✗	L✓ E✓ X✓	L✓ E✓ X✓
PÚBLICO	L✓ E✓ X✗	L✓ E✓ X✗	L✓ E✓ X✗	L✓ E✓ X✗

## 2. Detectar problemas de seguridad

- Responde a las siguientes preguntas:

1. ¿Algún usuario tiene más permisos de los que debería?

Sí, dado que “Todos” tiene permisos de Lectura en Finanzas y Ventas, lo cuál expone datos sensibles.

2. ¿Hay riesgo de que alguien lea archivos confidenciales?

Si, cualquier usuario puede leer: Finanzas (confidencial) y Ventas (Confidencial)

3. ¿Qué carpeta pública podría generar problemas si cualquiera puede modificar archivos?

La carpeta “Público” dado que todos pueden leer y escribir.

### 3. Proponer mejoras

- Indica cómo modificarías los permisos NTFS y de compartición para mejorar la seguridad, manteniendo el acceso correcto a cada usuario y grupo.

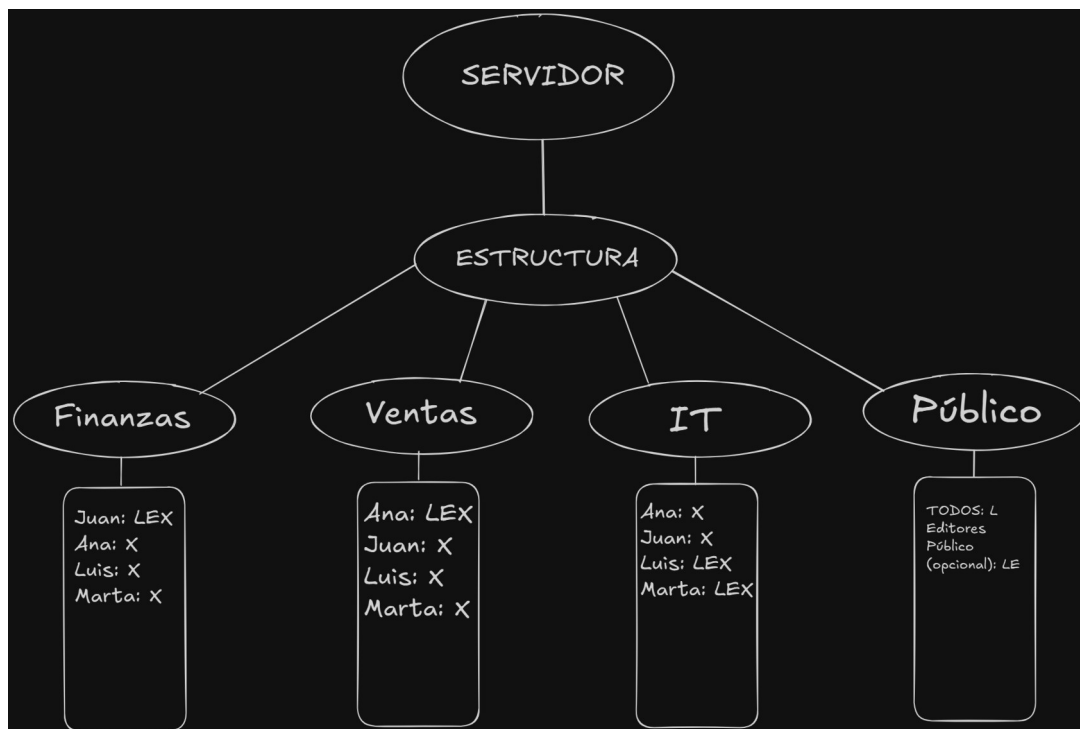
En finanzas se quitaría el permiso a “Todos” de lectura y le mantendría solo el grupo de administración.

Al grupo de ventas, le quitaría permisos a “Todos” de poder leer / ver el contenido

Al grupo de IT lo dejaría como esta

Al grupo público le cambiaría los permisos de Lectura y Escritura por Lectura o creacion de carpetas

- Haz un esquema visual con carpetas y usuarios.



- Explica brevemente por qué haces cada cambio.

### **1. Eliminar el permiso “Lectura” del grupo *Todos* en las carpetas Finanzas y Ventas**

Lo hago porque estas carpetas contienen información sensible de cada departamento, y permitir que todos los usuarios las lean supone un riesgo de filtración de datos. Cada carpeta debe ser accesible solo por su grupo correspondiente.

### **2. Mantener Control Total únicamente para los miembros del grupo de cada carpeta**

Se mantiene el Control Total (por ejemplo, Juan en Finanzas y Ana en Ventas) porque son los responsables de gestionar la información de su área. Restringir el acceso al resto evita modificaciones no autorizadas.

### **3. No dar permisos a usuarios externos al departamento en la carpeta IT**

IT maneja archivos técnicos y configuraciones que no deben ser alteradas por personal ajeno. Mantengo el acceso solo a Luis y Marta para garantizar la integridad de la información del sistema.

### **4. Cambiar la carpeta *Público* a solo Lectura**

Reduzco los permisos de Escritura porque cualquier usuario podría borrar o modificar archivos, creando conflictos, pérdidas de datos o riesgos de seguridad. Con Lectura, la información se comparte sin peligro de manipulación.

### **5. Ajuste de permisos de compartición y NTFS**

Establezco permisos de compartición amplios (Lectura) y uso NTFS para aplicar permisos reales, ya que NTFS ofrece control detallado y preciso sobre qué grupos o usuarios pueden leer, escribir o eliminar archivos.