MEDAC
Instituto Oficial de Formación Profesional

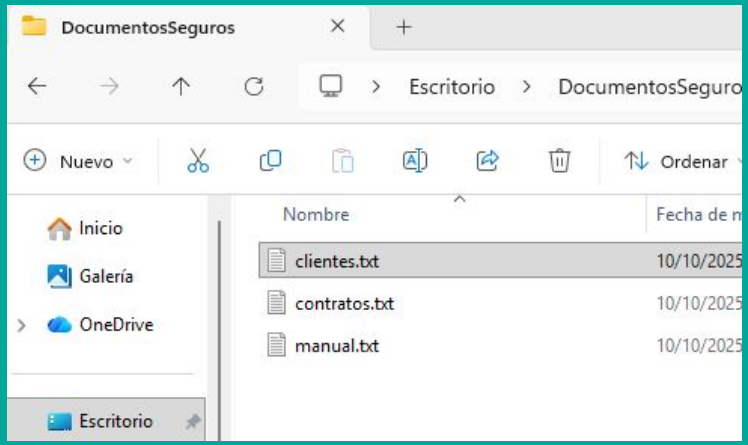
Tarea Evaluación Módulo 3

Alejandro Garcia-Mauriño Salas

Parte 1. Cifrado simétrico con AES Crypt

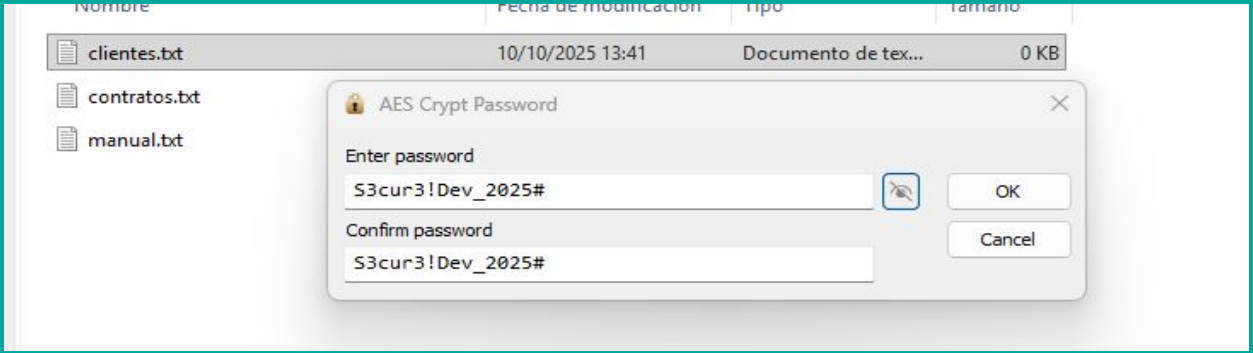
Descripción del proceso

1. Creé una carpeta llamada **DocumentosSeguros** en el escritorio.
2. Dentro, añadí tres archivos de prueba:
    - `clientes.txt`
    - `contratos.txt`
    - `manual.pdf`



Instalé el programa AES Crypt (versión para Windows).

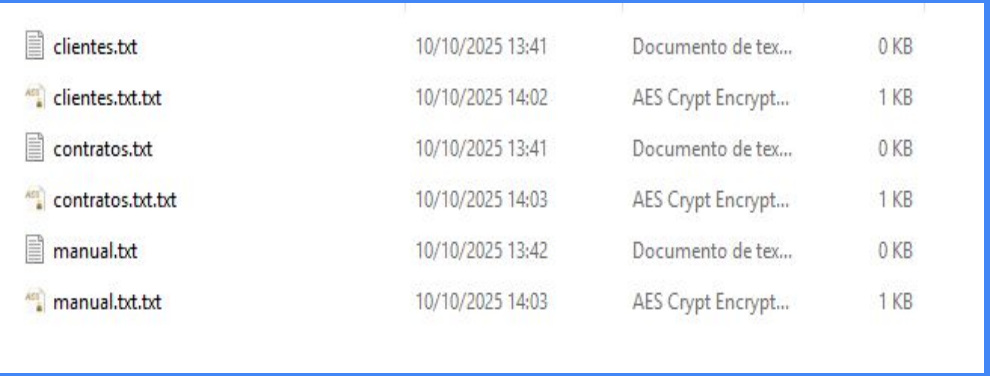
Hice clic derecho sobre cada archivo → **"AES Encrypt"** → escribí una contraseña segura:

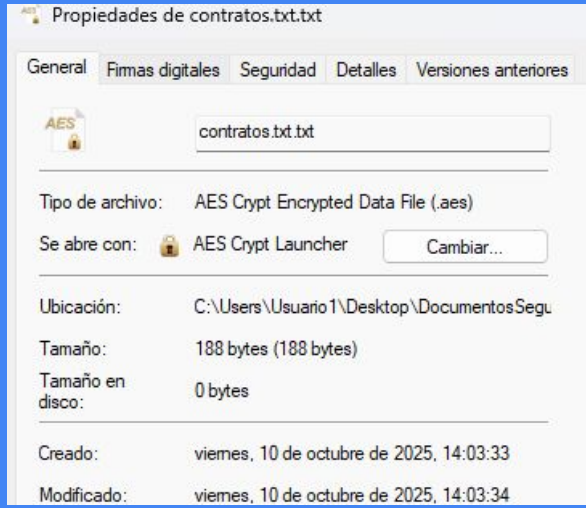


Parte 1. Cifrado simétrico con AES Crypt

El programa generó los archivos cifrados con extensión `.aes`, y los originales quedaron ilegibles si se abrían con el bloc de notas.

Luego probé a descifrar uno (clientes.txt.aes) con la misma contraseña y se recuperó perfectamente





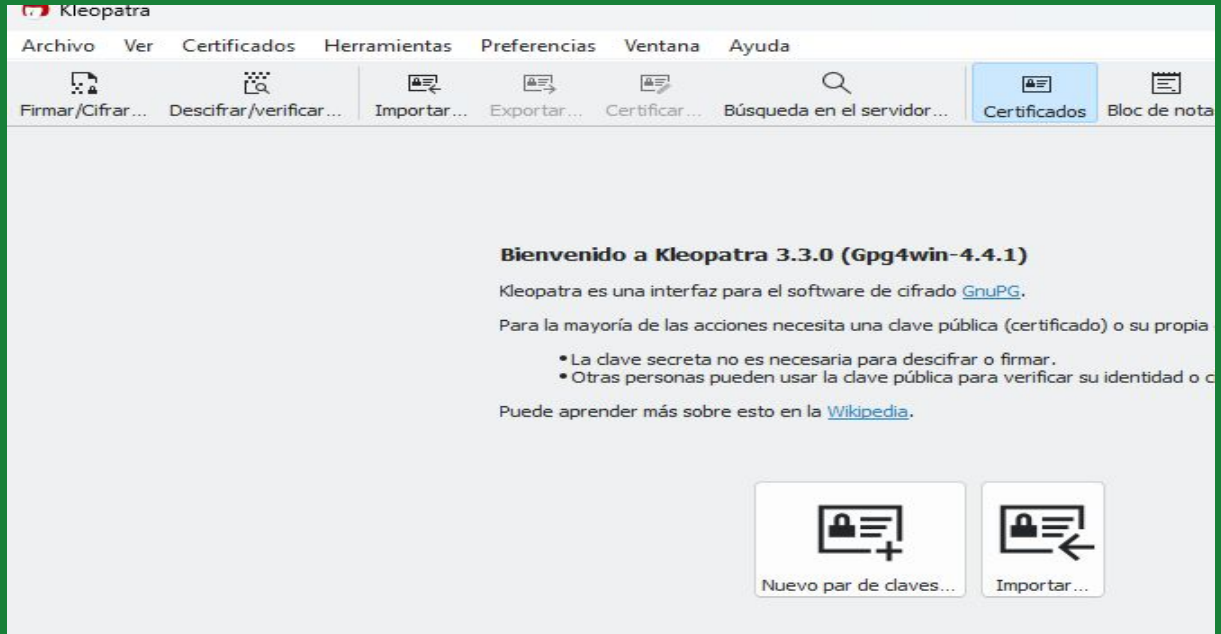
💭 Explicación breve

¿Qué ventajas y riesgos tiene usar una misma clave para todo?

Usar una sola clave es más cómodo porque no tienes que recordar varias contraseñas y puedes cifrar todo rápido.
El riesgo es que **si alguien consigue esa clave, podrá acceder a todos los archivos**, así que lo más recomendable sería usar diferentes contraseñas o guardarla en un gestor seguro.

Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

Instalé **Gpg4win** y abrí **Kleopatra**.



Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

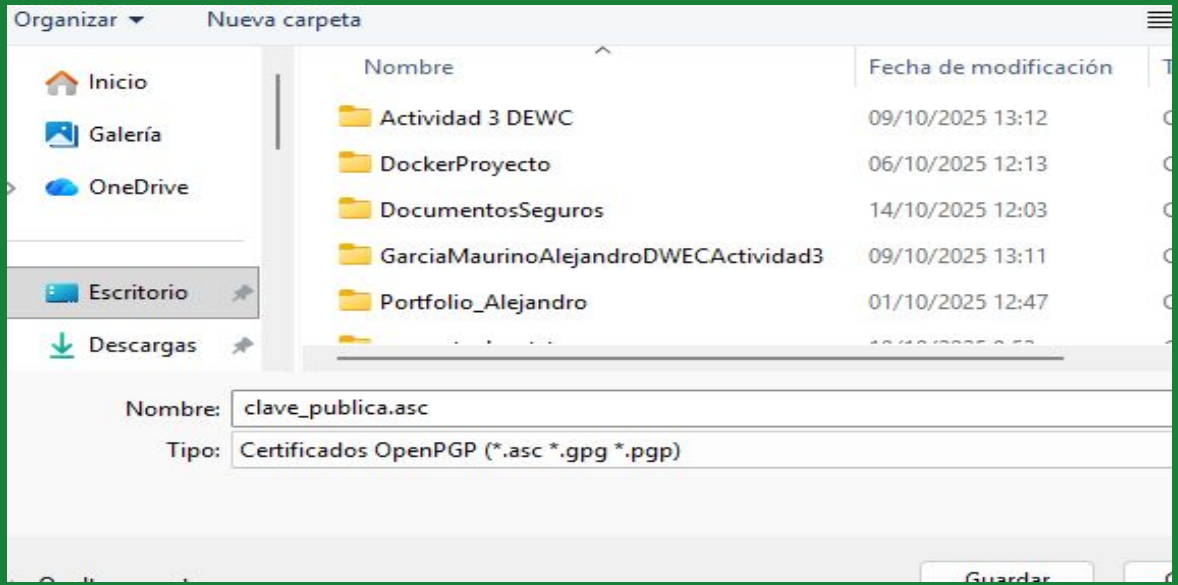
Creé un par de claves con mi nombre y correo ficticio:

Nombre: Alejandro Maurino

Correo: alejandro@securedevsolutions.com

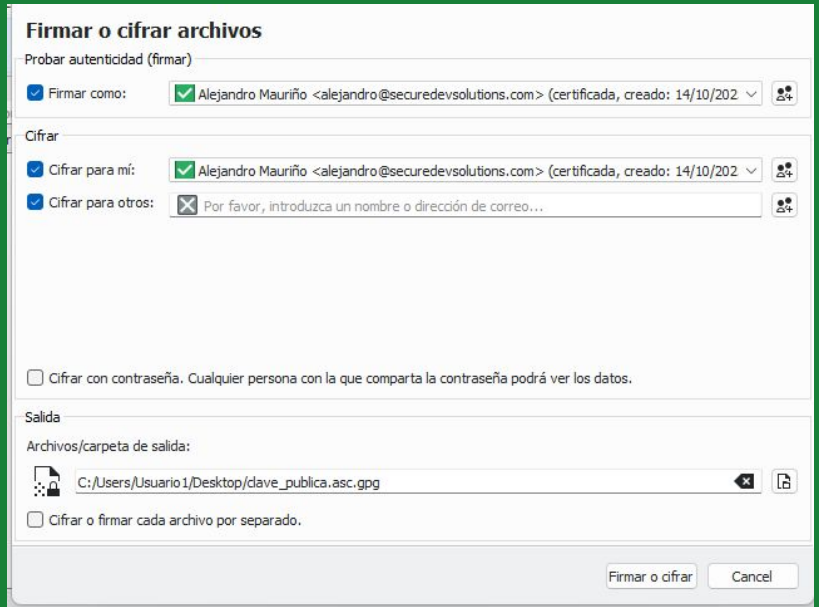
Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

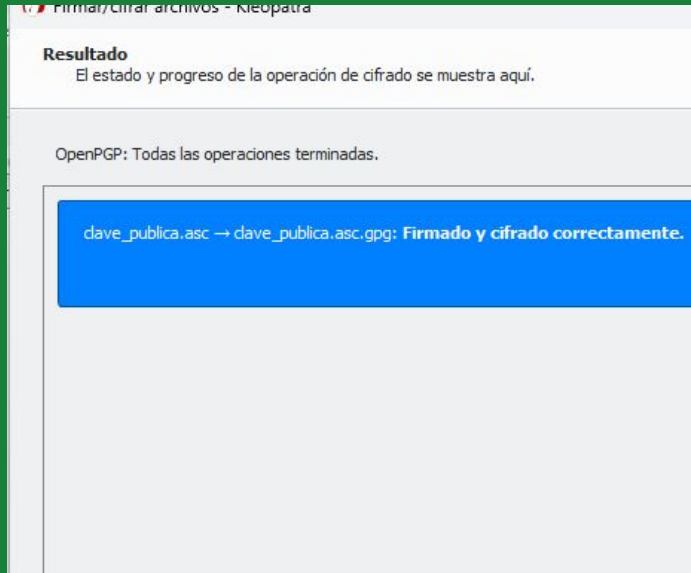
Después exporté mi **clave pública** con el nombre `clave_publica.asc`.



Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

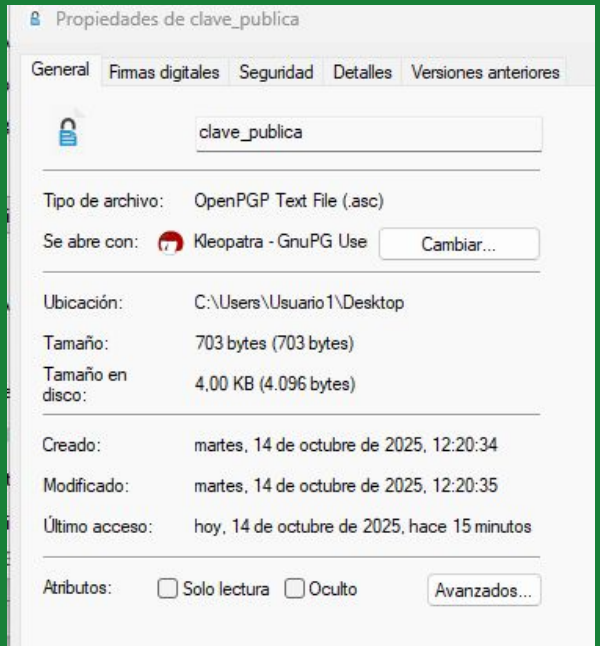
Luego, creé un archivo `mensaje.txt` con un texto corto y lo cifré con la clave pública usando Kleopatra.





Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

Esto generó el archivo `mensaje.txt.gpg`.



Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

💭 Explicación

¿Por qué solo puede descifrarlo el destinatario?

Porque el archivo se cifra con la **clave pública del destinatario**, y solo su **clave privada** puede descifrarlo.
Aunque otra persona intercepte el archivo, no podrá leerlo sin esa clave privada, lo que garantiza la confidencialidad.

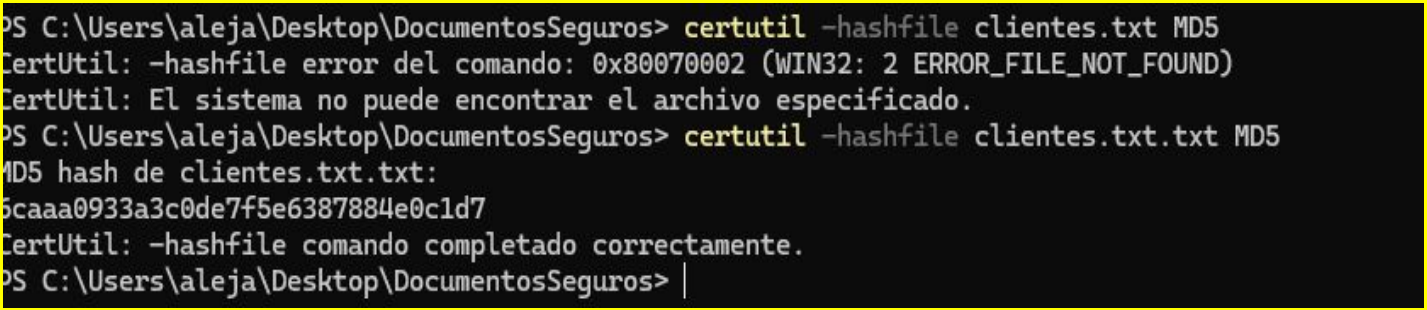
¿Qué pasaría si se filtrara mi clave privada?

Si alguien consigue mi clave privada, podría **hacerse pasar por mí o descifrar mensajes dirigidos a mí**, lo que sería muy peligroso.
Por eso hay que protegerla con contraseña fuerte y guardarla en un sitio seguro.

Parte 3. Verificación de integridad con MD5

Abrí el **Símbolo del sistema (CMD)** y ejecuté:

El hash obtenido lo guardé en `hash_original.txt`



Parte 3. Verificación de integridad con MD5

Guardé ese resultado como `hash_modificado.txt`.

Los dos valores eran completamente diferentes, aunque el cambio fue mínimo.

```
MD5 hash de clientes.txt.txt:
6caaa0933a3c0de7f5e6387884e0c1d7
CertUtil: -hashfile comando completado correctamente.
PS C:\Users\aleja\Desktop\DocumentosSeguros> certutil -hashfile clientes.txt.txt MD5
MD5 hash de clientes.txt.txt:
6e642e1b0946f7591267b58cc49b72eb
CertUtil: -hashfile comando completado correctamente.
PS C:\Users\aleja\Desktop\DocumentosSeguros>
```

Parte 3. Verificación de integridad con MD5

```
CertUtil: -hashfile comando completado correctamente.
PS C:\Users\aleja\Desktop\DocumentosSeguros> certutil -hashfile clientes.txt MD5 > hash_original.txt
PS C:\Users\aleja\Desktop\DocumentosSeguros>
```

Esto crea el archivo **hash_original.txt** con el hash del archivo original.

Puedes abrirlo con Bloc de notas y ver algo como:

Parte 3. Verificación de integridad con MD5

Ahora generamos el hash del archivo modificado:

```
PS C:\Users\aleja\Desktop\DocumentosSeguros> certutil -hashfile clientes.txt.txt MD5 > hash_original.txt.txt
PS C:\Users\aleja\Desktop\DocumentosSeguros> certutil -hashfile clientes.txt.txt MD5 > hash_modificado.txt.txt
PS C:\Users\aleja\Desktop\DocumentosSeguros>
```

- Esto crea **hash_modificado.txt** con el nuevo hash.

```
MD5 hash de clientes.txt.txt:
6e642e1b0946f7591267b58cc49b72eb
CertUtil: -hashfile comando completado correctamente.
```

Parte 3. Verificación de integridad con MD5

💭 Explicación

¿Por qué cambia completamente el hash aunque el cambio sea mínimo?

Porque el **algoritmo MD5** genera una huella digital única para cada contenido.
Si se modifica un solo carácter, el resultado cambia por completo, lo que sirve para detectar alteraciones o manipulaciones en los archivos.

Parte 4. Control de acceso con ACL en Windows

Creé tres usuarios locales desde **Administrar equipos → Usuarios y grupos locales**:

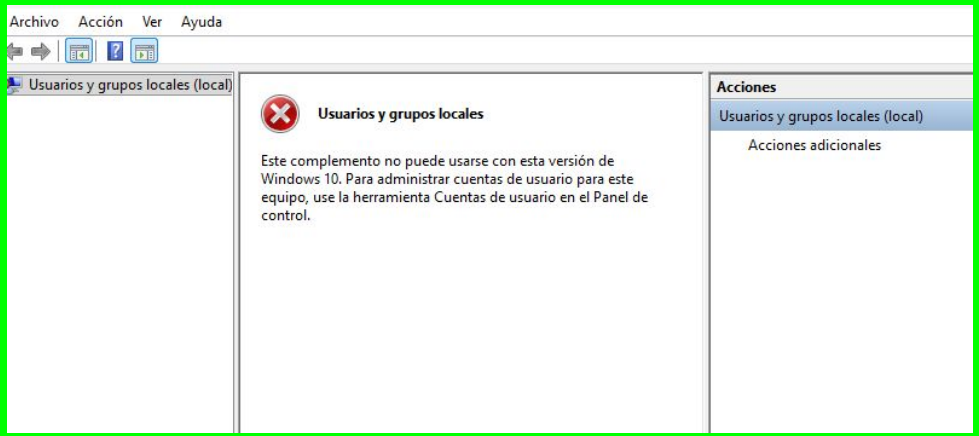
- `tecnico`
- `gerente`
- `externo`

En la carpeta **DocumentosSeguros**, configuré los permisos:

Parte 4. Control de acceso con ACL en Windows

Crear los usuarios locales

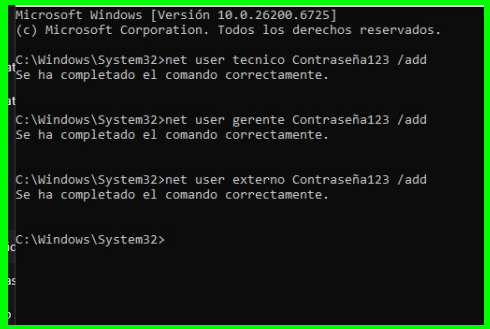
1. Presiona **Win + R**, escribe:



Parte 4. Control de acceso con ACL en Windows

2. En la carpeta **Usuarios**, haz clic derecho → **Nuevo usuario**.
   Crea tres usuarios:

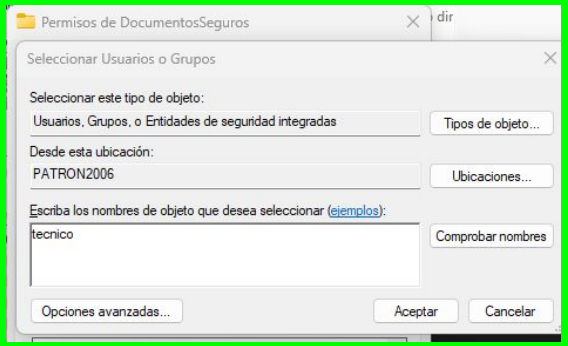
- **tecnico**
- **gerente**
- **externo**

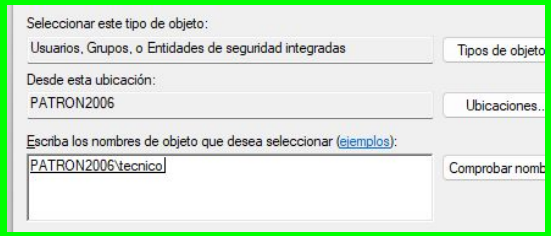


Parte 4. Control de acceso con ACL en Windows

Asignar permisos a la carpeta

1. Haz clic derecho sobre **DocumentosSeguros → Propiedades → Seguridad → Editar → Agregar**
2. Escribe el nombre del usuario (ejemplo: `tecnico`) → **Comprobar nombres → Aceptar**
3. Asigna permisos:

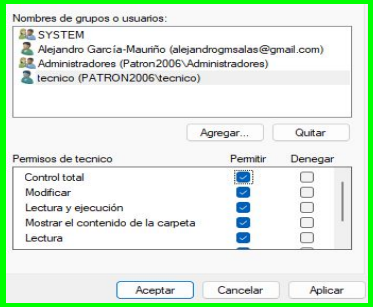


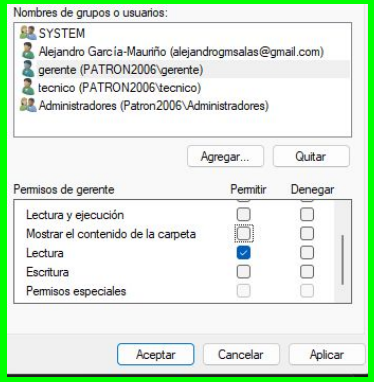


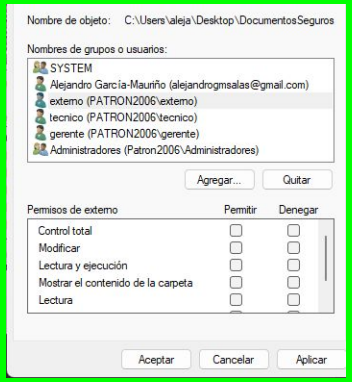
Parte 4. Control de acceso con ACL en Windows

Asigna permisos:

Usuario	Permiso
tecnico	Control total / Modificar
gerente	Solo lectura
externo	Ninguno







Parte 4. Control de acceso con ACL en Windows

Comprobación

Parte 4. Control de acceso con ACL en Windows

🧠 DIAPOSITIVA 6 – REFLEXIÓN FINAL

Importancia de la seguridad lógica:

- Protege la **información confidencial** de la empresa.
- Evita accesos no autorizados.
- Asegura la **integridad** y **confidencialidad** de los datos.
- Es fundamental en empresas que desarrollan software, ya que trabajan con datos de clientes y código sensible.