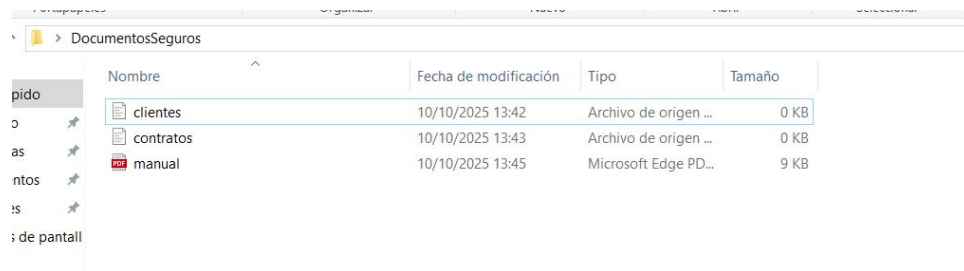

TAREA EVALUACIÓN MÓDULO 3

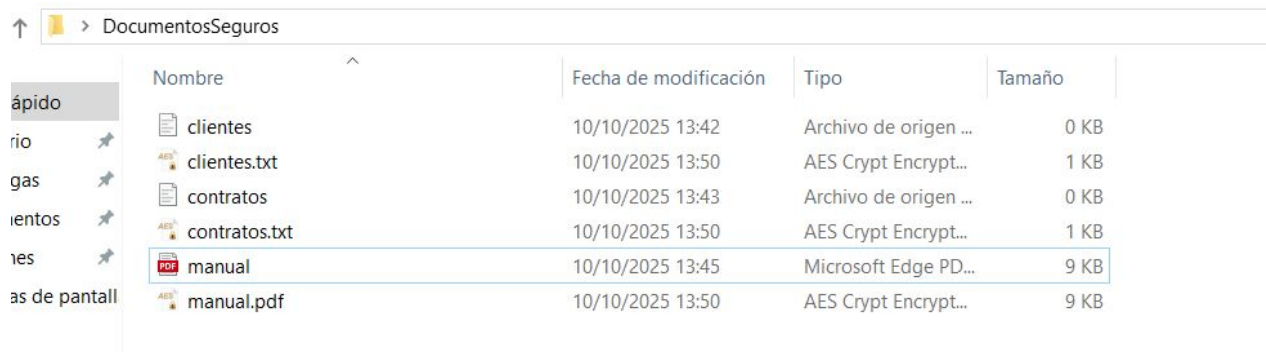
Javier Saravia Ogazón

Parte 1. Cifrado simétrico con AES Crypt

Creamos la carpeta DocumentosSeguros y creamos dos archivos .txt y un .pdf



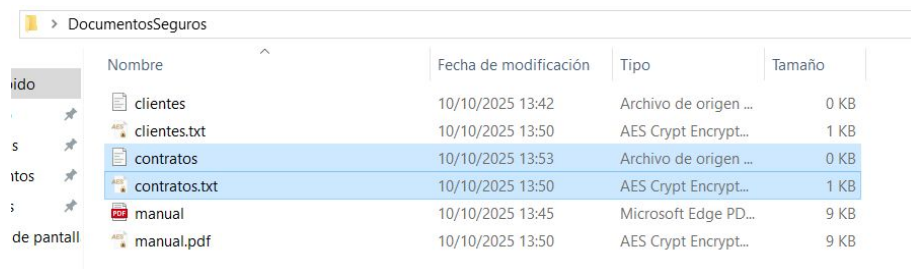
Ciframos los archivos con una contraseña segura para cada uno



↑ > DocumentosSeguros

	Nombre	Fecha de modificación	Tipo	Tamaño
ápido	clientes	10/10/2025 13:42	Archivo de origen ...	0 KB
rio	clientes.txt	10/10/2025 13:50	AES Crypt Encrypt...	1 KB
gas	contratos	10/10/2025 13:43	Archivo de origen ...	0 KB
ientos	contratos.txt	10/10/2025 13:50	AES Crypt Encrypt...	1 KB
ies	manual	10/10/2025 13:45	Microsoft Edge PD...	9 KB
as de pantall	manual.pdf	10/10/2025 13:50	AES Crypt Encrypt...	9 KB

Eliminamos el archivo original, introducimos la contraseña del cifrado y se nos abre el original



> DocumentosSeguros

	Nombre	Fecha de modificación	Tipo	Tamaño
ido	clientes	10/10/2025 13:42	Archivo de origen ...	0 KB
	clientes.txt	10/10/2025 13:50	AES Crypt Encrypt...	1 KB
s	contratos	10/10/2025 13:53	Archivo de origen ...	0 KB
itos	contratos.txt	10/10/2025 13:50	AES Crypt Encrypt...	1 KB
i	manual	10/10/2025 13:45	Microsoft Edge PD...	9 KB
de pantall	manual.pdf	10/10/2025 13:50	AES Crypt Encrypt...	9 KB

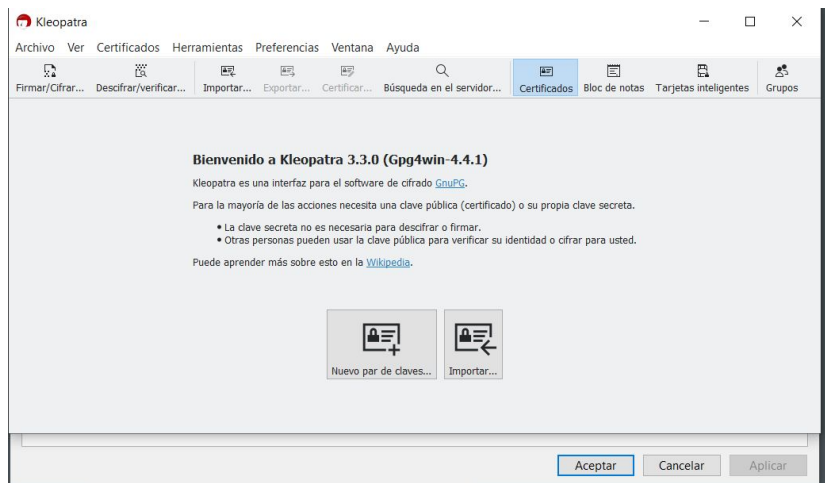
“¿Qué ventajas y riesgos tiene usar una misma clave para todo?”

Ventaja: Rápido y cómodo

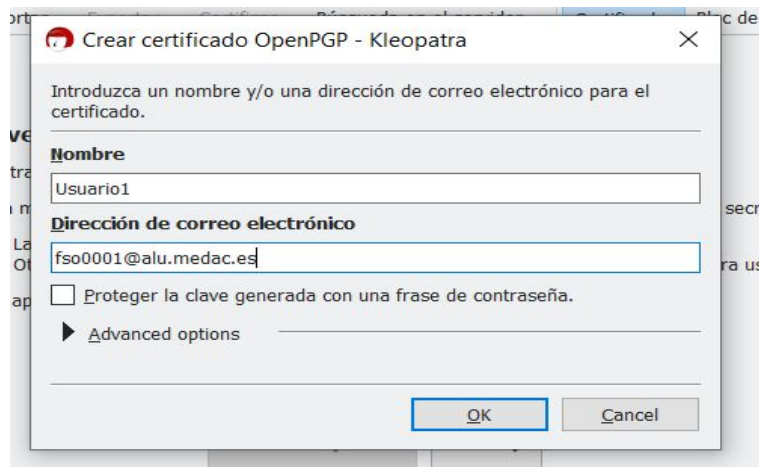
Desventaja: Muy peligroso

Parte 2. Cifrado asimétrico con Gpg4win / Kleopatra

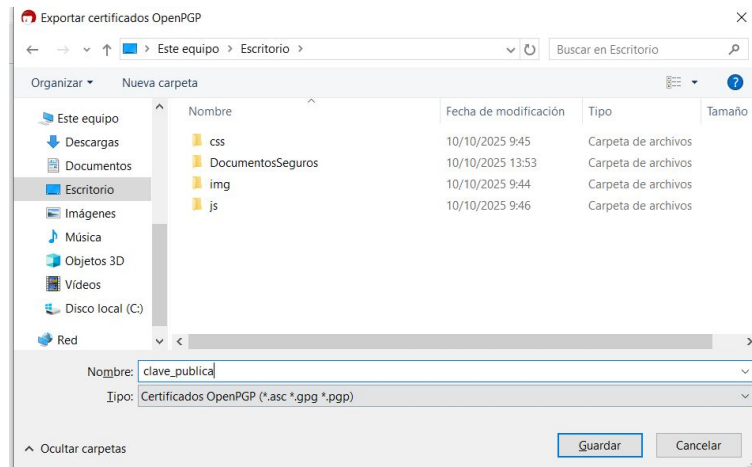
Creamos la clave pública y privada



Creamos la clave pública



La guardamos en clave_publica.asc



Ciframos el archivo para un compañero o profesor:

Firmar/cifrar archivos - Kleopatra

Firmar o cifrar archivos

Probar autenticidad (firmar)

☒ Firmar como: ✓ Usuario1 <fso0001@alu.medac.es> (certificada, creado: 10/10/2025)

Cifrar

☒ Cifrar para mí: ✓ Usuario1 <fso0001@alu.medac.es> (certificada, creado: 10/10/2025)


☒ Cifrar para gtros: ✓ Usuario1 <sjr0006@alu.medac.es> (certificada, OpenPGP, creado)

☐ Por favor, introduzca un nombre o dirección de correo...

☐ Cifrar con contraseña. Cualquier persona con la que comparta la contraseña podrá ver los datos.

Salida

Archivos/carpeta de salida:

 C:/Users/Usuario1/Desktop/DocumentosSeguros/mensaje.txt.gpg

☐ Cifrar o firmar cada archivo por separado.

Firmar o cifrar Cancel

Explica el proceso de descifrado y por qué solo puede hacerlo el destinatario.

El cifrado asimétrico se basa en el uso de dos claves relacionadas matemáticamente: una pública y una privada. La clave pública se puede compartir libremente y sirve para cifrar mensajes, mientras que la clave privada se mantiene secreta y se utiliza para descifrarlos.

En este proceso, solo el destinatario que posee la clave privada correspondiente puede descifrar el mensaje cifrado con su clave pública.

Aunque otra persona intercepte el archivo .gpg, no podrá leerlo porque no tiene la clave privada necesaria.

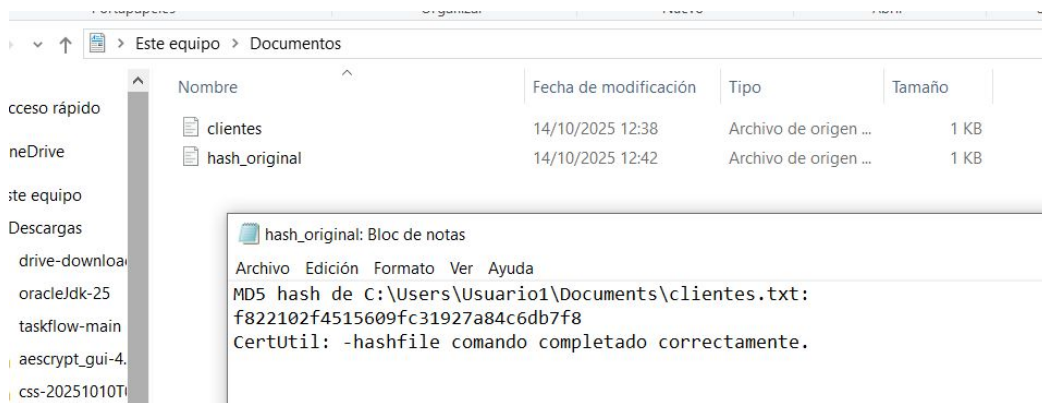
De esta forma, el cifrado asimétrico garantiza confidencialidad, autenticidad y seguridad en la comunicación digital.

Parte 3. Verificación de integridad con MD5

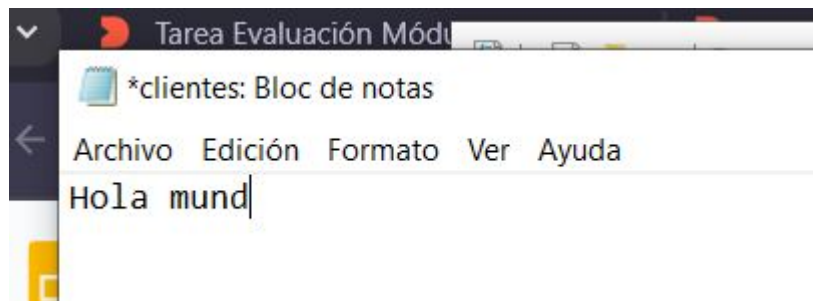
Utilizamos el comando certutil -hashfile

```
PS C:\Users\Usuario1> certutil -hashfile "C:\Users\Usuario1\Documents\clientes.txt" MD5
MD5 hash de C:\Users\Usuario1\Documents\clientes.txt:
f822102f4515609fc31927a84c6db7f8
CertUtil: -hashfile comando completado correctamente.
PS C:\Users\Usuario1>
```

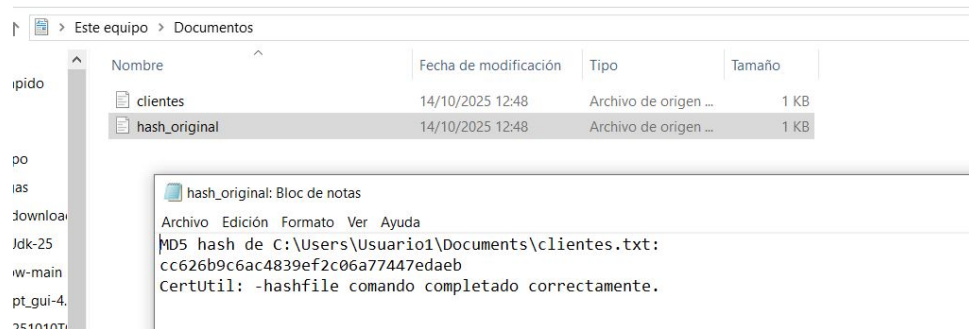
Guardamos el resultado en un
hash_original.txt



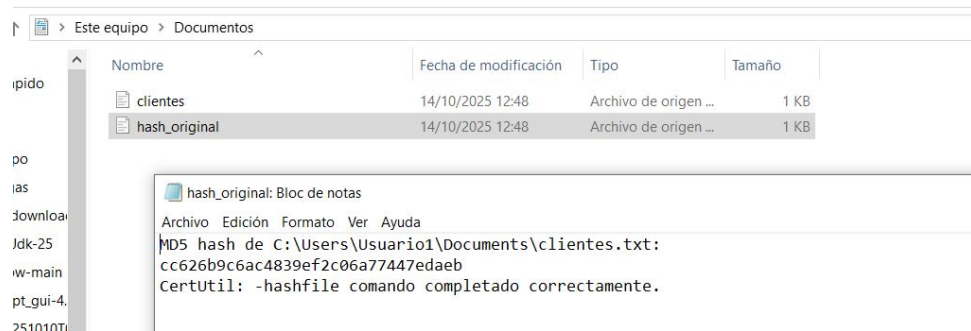
Cambiamos una letra del clientes.txt:



Recalculamos el hash



Podemos observar que al cambiar una letra,
el hash cambia completamente



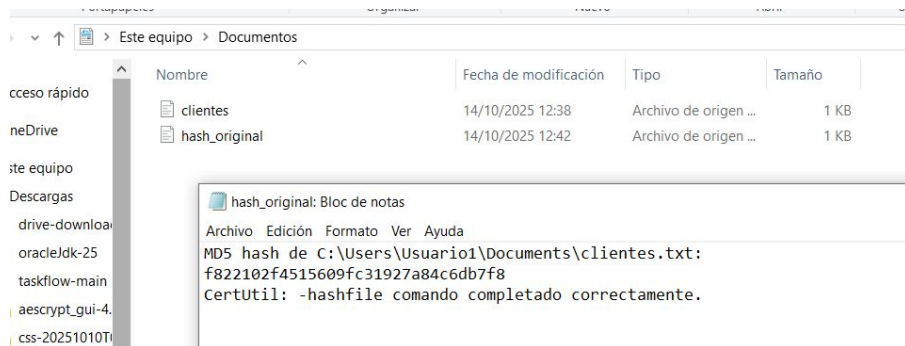
Nombre	Fecha de modificación	Tipo	Tamaño
clientes	14/10/2025 12:48	Archivo de origen ...	1 KB
hash_original	14/10/2025 12:48	Archivo de origen ...	1 KB

hash_original: Bloc de notas

Archivo Edición Formato Ver Ayuda

MD5 hash de C:\Users\Usuario1\Documents\clientes.txt:
cc626b9c6ac4839ef2c06a77447edaeb

CertUtil: -hashfile comando completado correctamente.



Nombre	Fecha de modificación	Tipo	Tamaño
clientes	14/10/2025 12:38	Archivo de origen ...	1 KB
hash_original	14/10/2025 12:42	Archivo de origen ...	1 KB

hash_original: Bloc de notas

Archivo Edición Formato Ver Ayuda

MD5 hash de C:\Users\Usuario1\Documents\clientes.txt:
f822102f4515609fc31927a84c6db7f8

CertUtil: -hashfile comando completado correctamente.

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

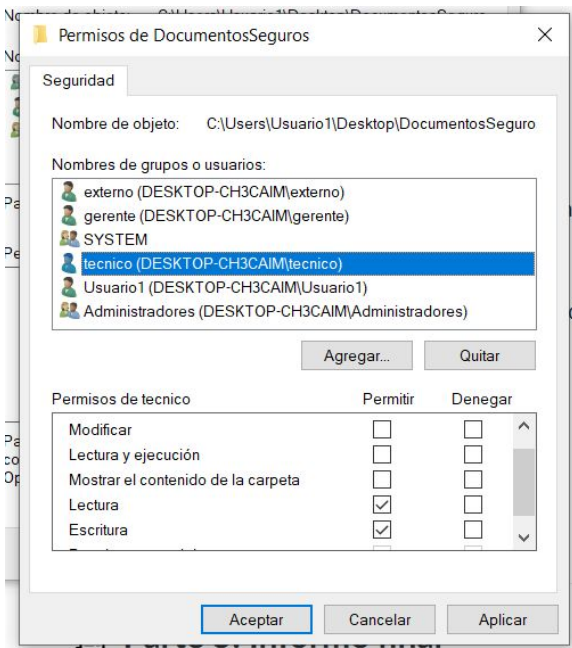
El hash cambió por completo porque las funciones hash como MD5 están diseñadas para que una mínima modificación en el contenido produzca un resultado completamente diferente.

A este comportamiento se le llama efecto avalancha.

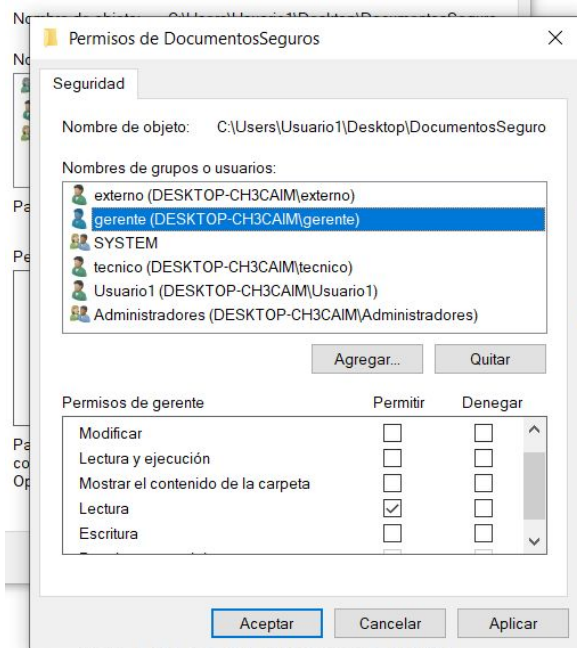
Sirve para comprobar la integridad de los archivos: si el hash cambia, significa que el archivo fue alterado, aunque sea ligeramente.

Parte 4. Control de acceso con ACL en Windows

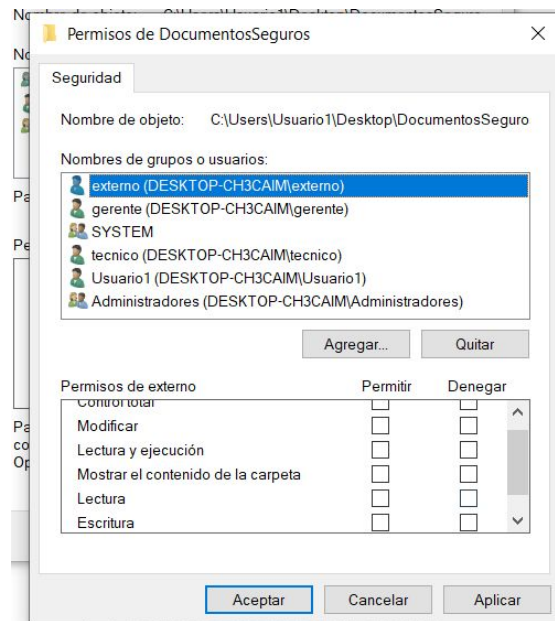
técnico: lectura y escritura



gerente: solo lectura



externo: sin acceso



Reflexión final

- Protege datos sensibles: El código fuente, los datos de la empresa y la información de los clientes.
- Genera confianza: Los clientes prefieren productos y servicios que saben que son seguros.
- Evita desastres: Previene hackeos, fugas de datos y ataques que pueden paralizar la empresa y costar mucho dinero.
- Mejora el producto: Integrar la seguridad desde el principio resulta en un software de mayor calidad y más robusto.



