



**UNIVERSIDAD AUTÓNOMA "TOMÁS FRÍAS"  
CARRERA DE INGENIERÍA DE SISTEMAS**

**MATERIA:** Seguridad de Sistemas (SIS - 737)

**NOMBRE:** Univ. Dietmar Alex Apaza

**EVALUACION  
LABORATORIO N°: 4**

**DOCENTE:** Ing. Alexander J. Duran Miranda

**AUXILIAR:** Univ. Aldrin Roger Perez Miranda

**GitHub**

**Nombre:** AlexTheLion99

**Enlace\_lab\_4:**[https://github.com/AlexTheLion99/sis\\_737\\_Laboratorio\\_4](https://github.com/AlexTheLion99/sis_737_Laboratorio_4)

**LAB\_4 - CIFRADO SIMÉTRICO**

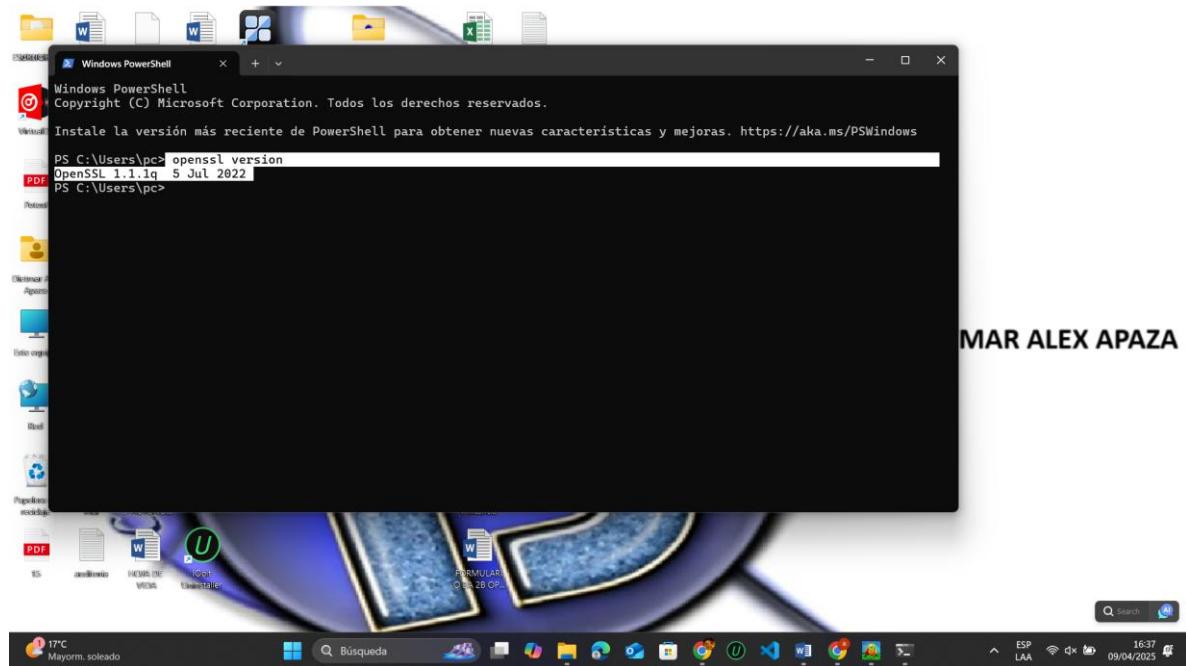
## **EVALUACIÓN**

### **3.- Investigue que es Openssl, además de indicar 2 ejemplos de su utilización**

**Openssl** es una biblioteca criptográfica que permite una implementación de código abierto de los protocolos de seguridad de la capa de transporte (TLS) y capa de sockets seguros (SSL). Proporciona funciones para generar claves privadas, administrar certificados y equipar aplicaciones cliente con cifrado y descifrado.

OpenSSL es ampliamente utilizado por desarrolladores de software y administradores de sistemas para implementar la comunicación segura y el cifrado en diversas aplicaciones, como servidores web (como NGINX), servidores de correo electrónico, VPN, etc. Está disponible como una biblioteca que puede integrarse en aplicaciones de software o utilizarse como herramientas independientes de línea de comandos para diversas operaciones criptográficas.

- **Verificamos si tenemos instalado Openssl en nuestro host**



### **Ejemplo 1: Crear un certificado autofirmado con OpenSSL**

Esto se usa, por ejemplo, para montar un servidor web con HTTPS en un entorno de pruebas o local.

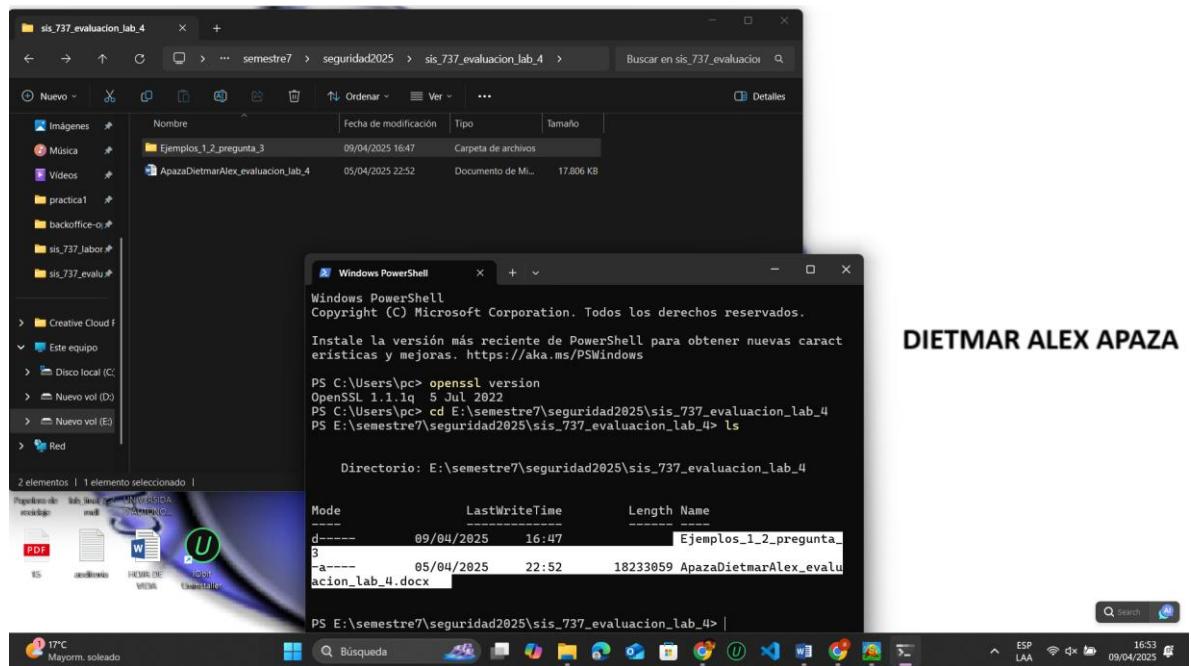
- Qué necesitas:

Tener OpenSSL instalado (ya viene por defecto en Linux/macOS, y se puede instalar en Windows).

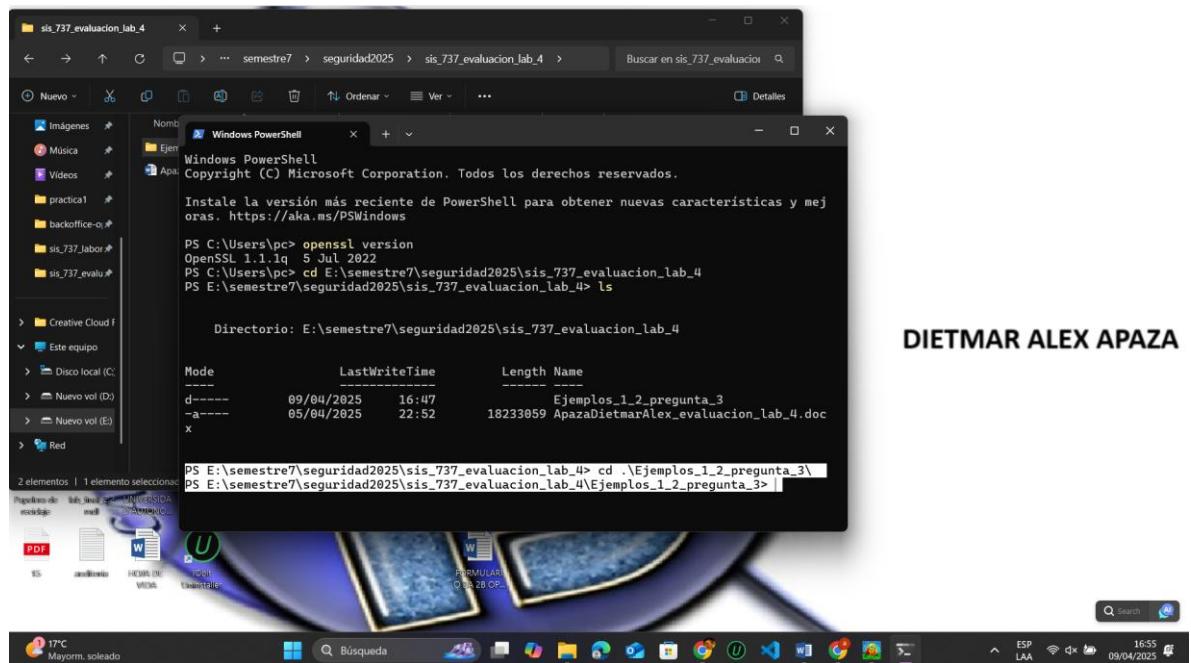
Acceso a una terminal (CMD, Bash, PowerShell).

Pasos:

1. Abrir la terminal.
2. Verificar que la carpeta esta creada para realizar la demostración del ejemplo 1 y 2



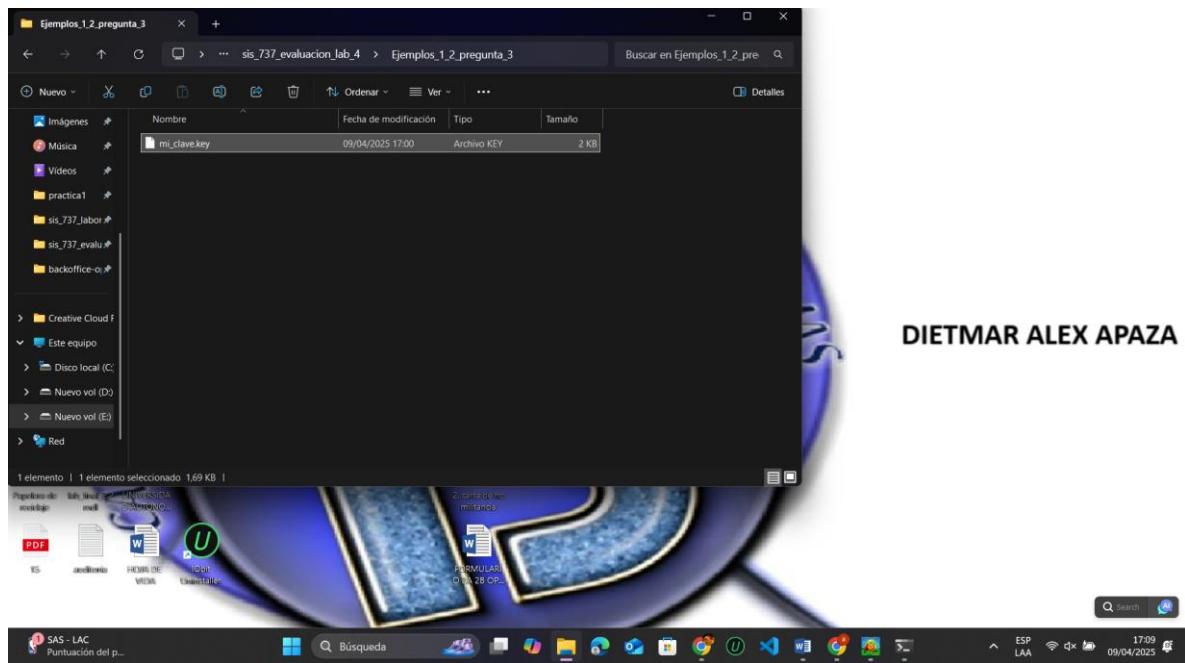
3. Verificamos que estamos dentro de la carpeta



4. Ejecutar este comando: openssl req -x509 -newkey rsa:2048 -keyout mi\_clave.key -out mi\_certificado.crt -days 365 –nodes

PS E:\semestre7\seguridad2025\sis\_737\_evaluacion\_lab\_4\Ejemplos\_1\_2\_pregunta\_3> openssl req -x509 -newkey rsa:2048 -keyout mi\_clave.key -out mi\_certificado.crt -days 365 -nodes  
Generating a RSA private key  
.....  
writing new private key to 'mi\_clave.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank.  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:

DIETMAR ALEX APAZA



5. Ahora te está pidiendo que llenes los campos para el **certificado autofirmado**. A continuación te explico **qué poner en cada campo**:

Pon el código de tu país. **BO**

El nombre de tu estado o provincia. **Tomas Frias**

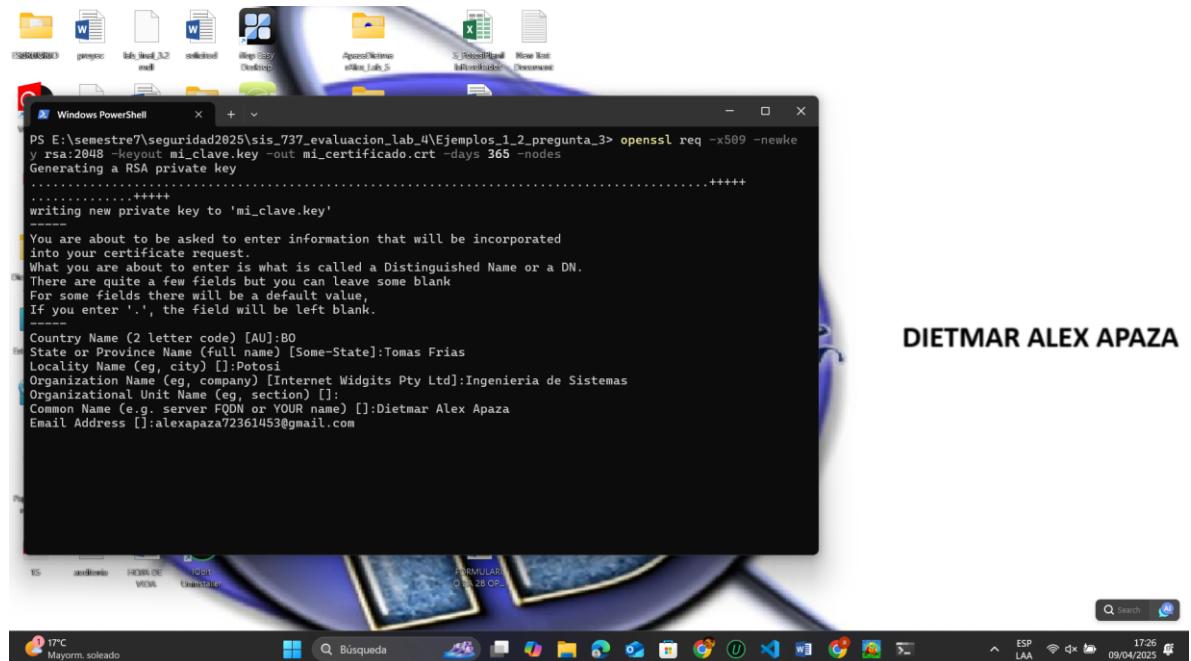
Tu ciudad o localidad. **Potosí**

Nombre de tu organización, universidad o empresa. **Ingeniería de Sistemas**

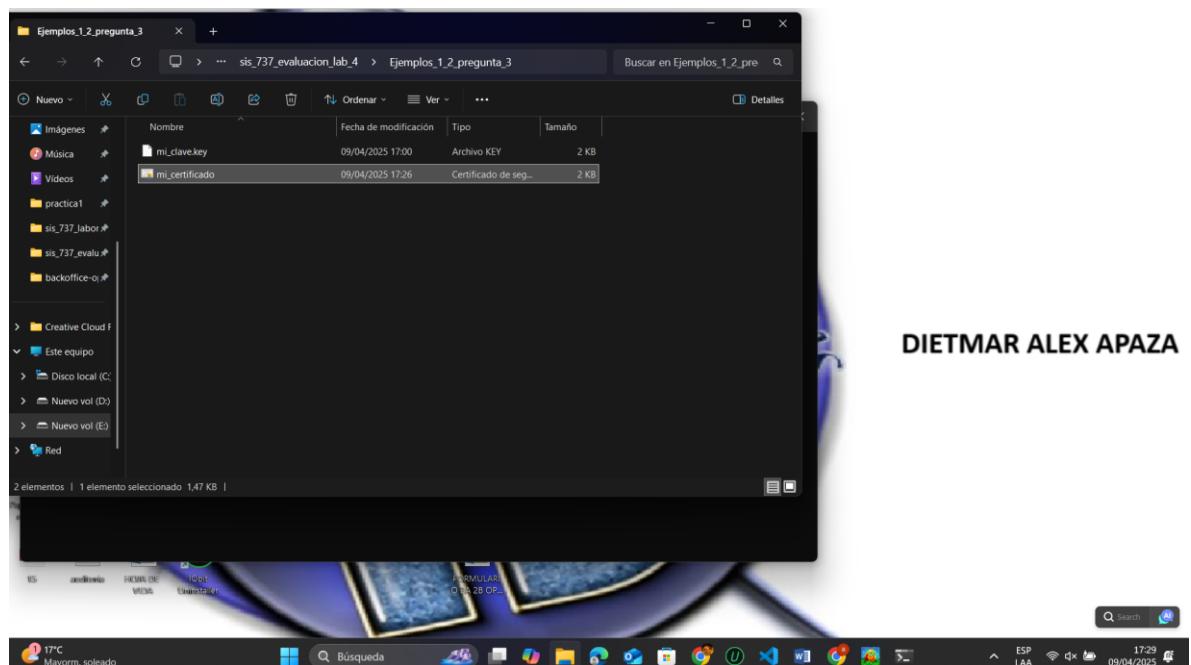
Puedes indicar un departamento, como: **Sistemas (opcional)**

Aquí va el **nombre común**, puede ser: Uso personal **Dietmar Alex Apaza**

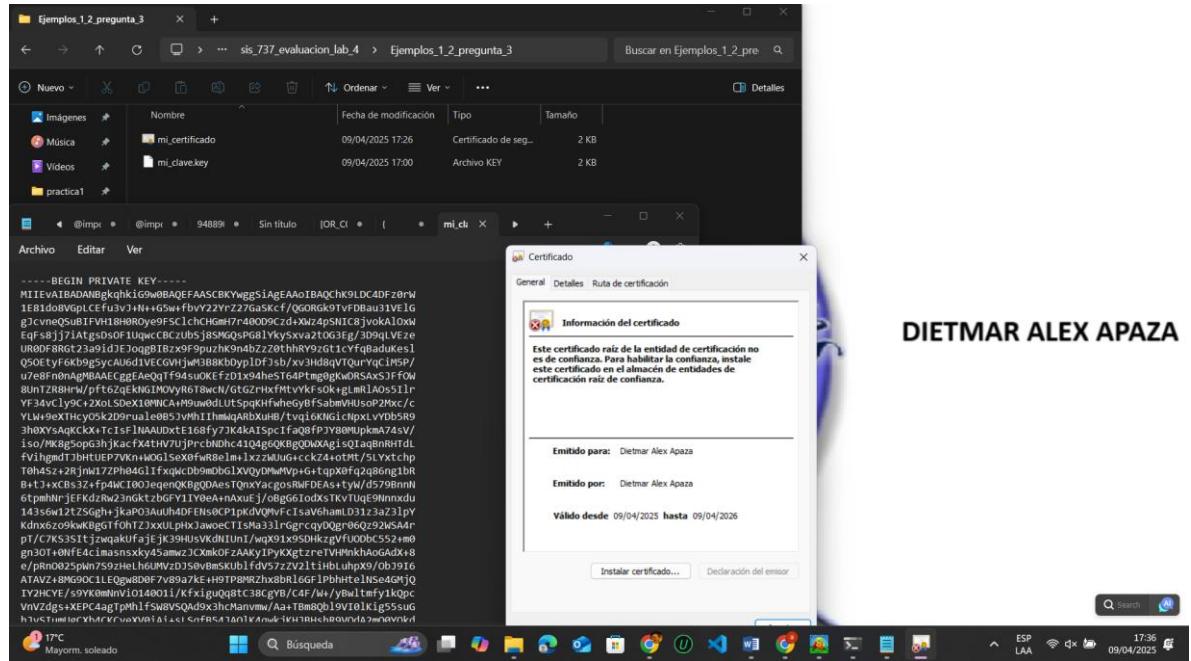
Email Address : [alexapaza72361453@gmail.com](mailto:alexapaza72361453@gmail.com)



- Una vez completados esos campos nos genera los archivos del certificado junto con la clave



## 7. Como resultado tenemos la clave que esta cifrada y el certificado autofirmado



DIETMAR ALEX APAZA

### Explicación:

- **req:** inicia la creación de una solicitud de certificado.
- **-x509:** crea un certificado X.509 (estándar para certificados SSL/TLS).
- **-newkey rsa:2048:** genera una nueva clave privada RSA de 2048 bits.
- **-keyout mi\_clave.key:** nombre del archivo que contendrá la clave privada.
- **-out mi\_certificado.crt:** nombre del archivo de salida para el certificado.
- **-days 365:** duración del certificado (1 año).
- **-nodes:** no cifra la clave privada (para evitar tener que escribir contraseña al usarla).

### Resultado:

Tendrás dos archivos:

- **mi\_clave.key** → la clave privada
- **mi\_certificado.crt** → el certificado autofirmado

### Ejemplo 2: Cifrar y descifrar un archivo con OpenSSL

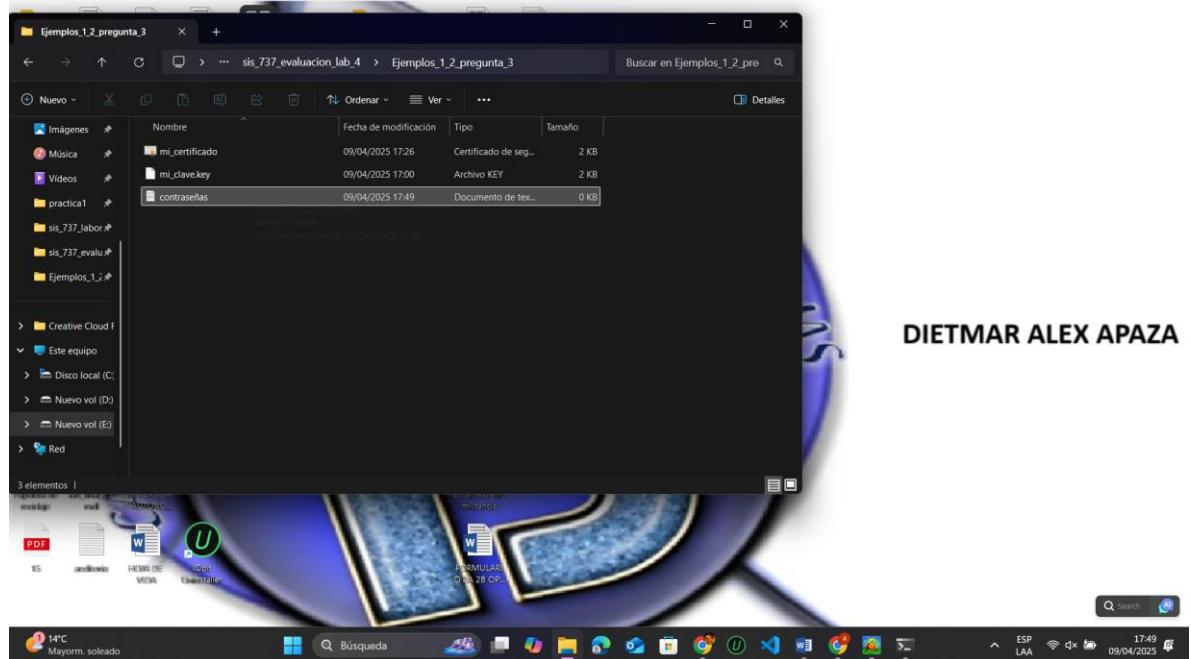
Ideal si quieras proteger archivos sensibles como contraseñas, información financiera, etc.

Objetivo:

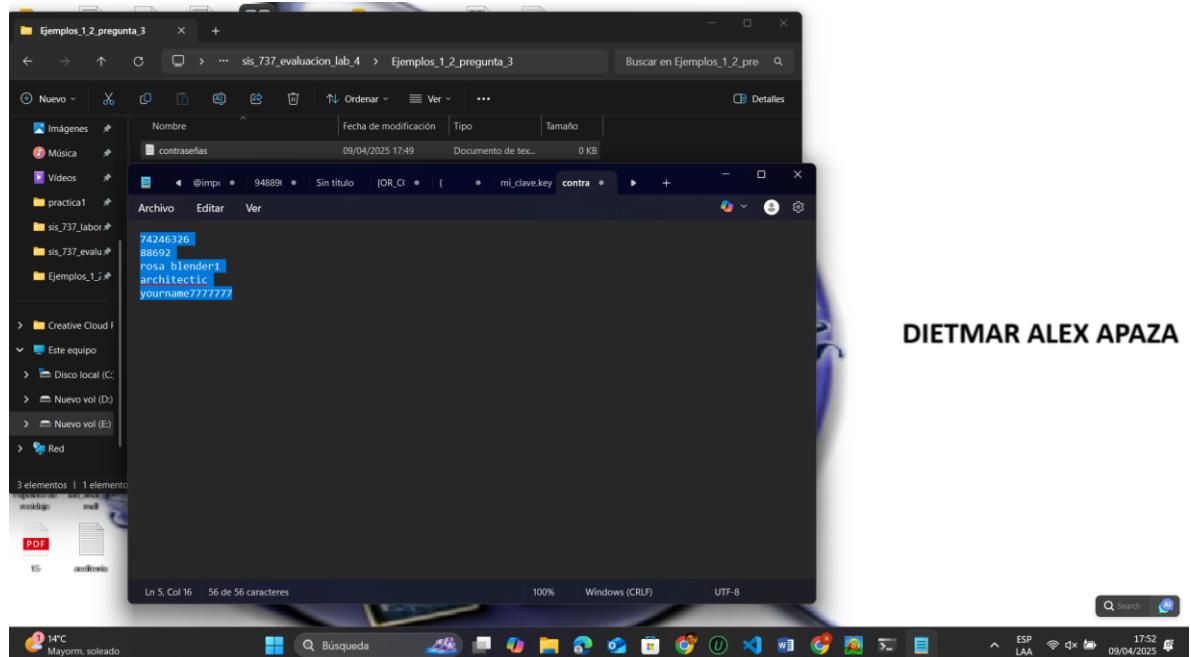
- Cifrar un archivo con una contraseña.
- Luego descifrarlo usando esa misma contraseña.

Qué necesitas:

- Un archivo de texto (ej. `contraseñas.txt`) con información que quieras proteger.



**DIETMAR ALEX APAZA**



**DIETMAR ALEX APAZA**

- La contraseña que utilizaremos para cifrar será: alexthelion

## Cifrar el archivo

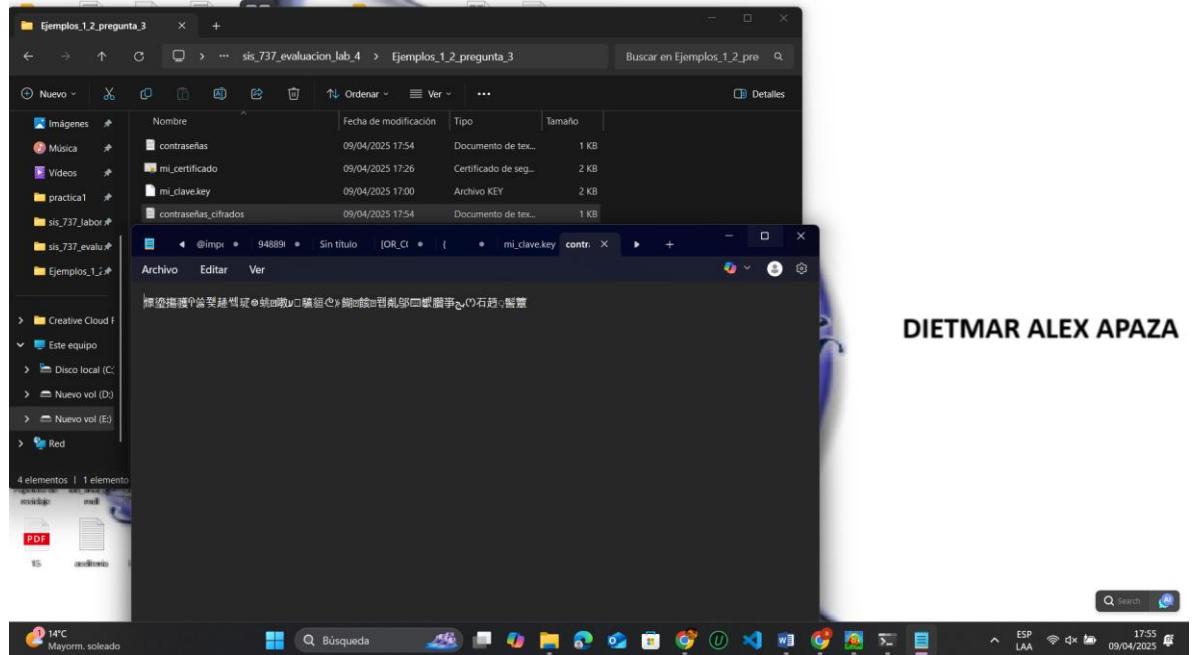
1. En la terminal, ejecuta: openssl enc -aes-256-cbc -salt -in contraseñas.txt -out contraseñas\_cifrados.txt -k alexthelion

The screenshot shows a Windows desktop environment. In the center, there is a Windows PowerShell window titled "Windows PowerShell" with the command: `openssl enc -aes-256-cbc -salt -in contraseñas.txt -out contraseñas_cifrados.txt -k alexthelion`. Below the PowerShell window is a file explorer window titled "Ejemplos\_1\_2\_pregunta\_3" showing a folder structure. The taskbar at the bottom displays various icons for applications like File Explorer, Edge, and File Explorer again.

DIETMAR ALEX APAZA

This screenshot is similar to the one above, showing a Windows desktop with a PowerShell window and a file explorer window. The PowerShell window contains the same command: `openssl enc -aes-256-cbc -salt -in contraseñas.txt -out contraseñas_cifrados.txt -k alexthelion`. The file explorer window shows the results of the encryption process, listing four files: "contraseñas" (1 KB), "mi\_certificado" (2 KB), "mi\_clave.key" (2 KB), and "contraseñas\_cifrados" (1 KB). The taskbar at the bottom is identical to the first screenshot.

DIETMAR ALEX APAZA



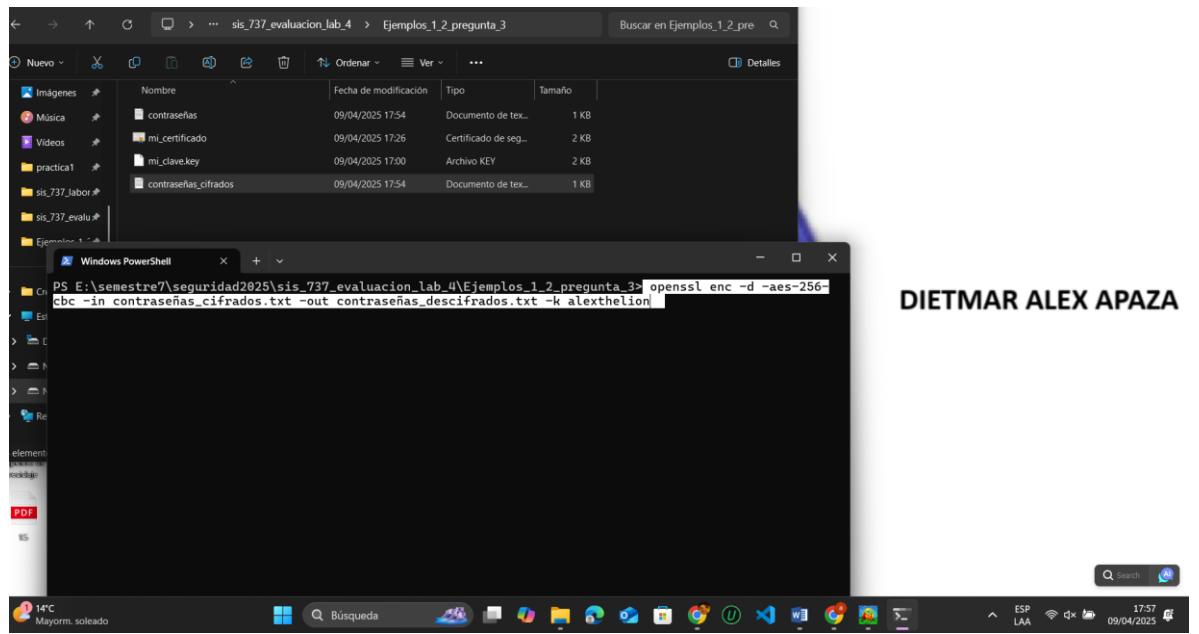
DIETMAR ALEX APAZA

### Explicación:

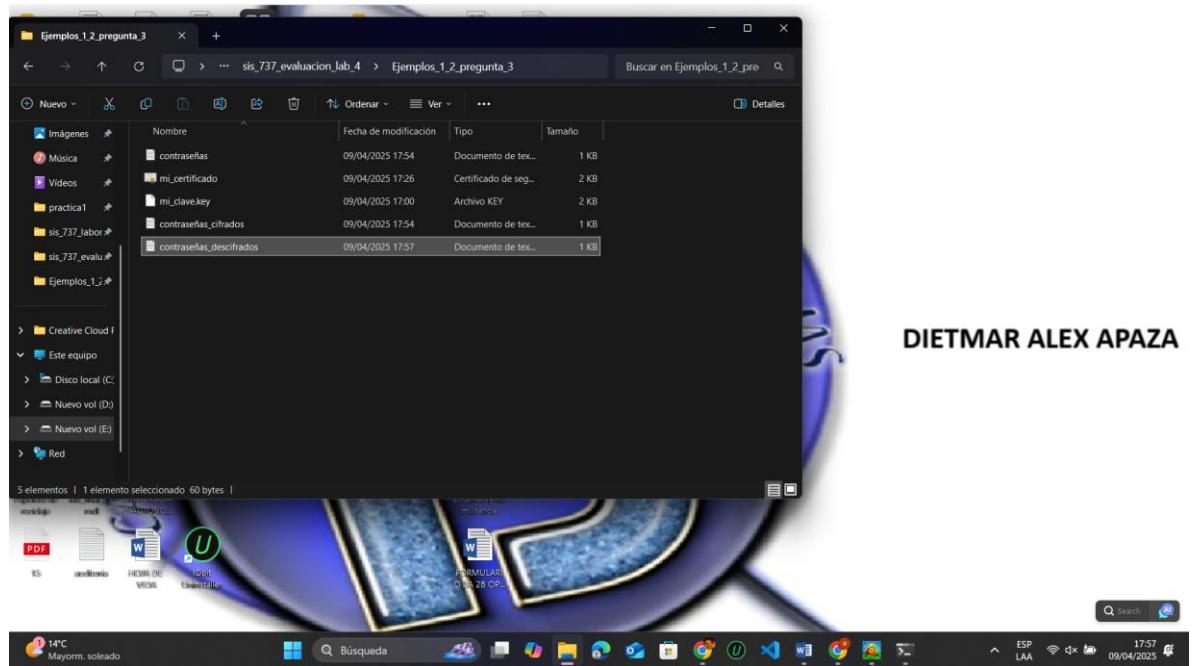
- **enc**: indica que se va a cifrar.
- **-aes-256-cbc**: algoritmo de cifrado (AES con clave de 256 bits en modo CBC).
- **-salt**: añade sal (salt) para mayor seguridad.
- **-in datos.txt**: archivo original.
- **-out datos\_cifrados.txt**: archivo cifrado.
- **-k mipassword**: contraseña de cifrado (puedes cambiarla por la que tú quieras).

### Descifrar el archivo

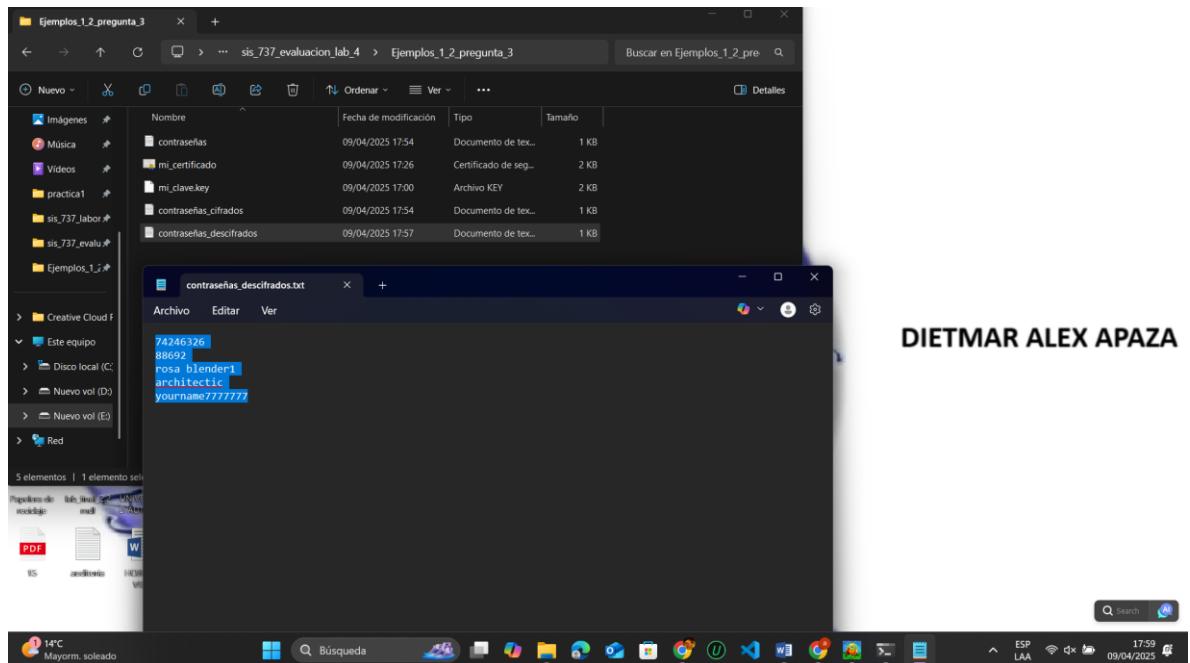
1. Ejecuta: `openssl enc -d -aes-256-cbc -in contraseñas_cifrados.txt -out contraseñas_descifrados.txt -k alexthelion`



DIETMAR ALEX APAZA



DIETMAR ALEX APAZA



DIETMAR ALEX APAZA

Explicación:

- `-d`: indica que se va a descifrar.
- El resto de parámetros deben coincidir con los usados al cifrar.

Resultado final:

- `datos_cifrados.txt` → contiene el archivo cifrado.
- `datos_descifrados.txt` → contiene el texto original recuperado.

#### 4.- Utilice alguna herramienta que le permita cifrar una carpeta con el contenido al anterior, adjunte capturas de pantalla.

En esta actividad se procederá a **cifrar una carpeta que contiene archivos sensibles**, utilizando herramientas que permitan proteger su contenido mediante **algoritmos de cifrado seguros**.

Para lograr esto, se utilizará la herramienta **7-Zip**, una aplicación de compresión que permite, además de reducir el tamaño de los archivos, aplicar una contraseña de acceso y cifrado AES-256 a los datos.

Este procedimiento es especialmente útil en entornos donde se necesita **proteger la confidencialidad de la información** antes de almacenarla o compartirla por medios inseguros, como correos electrónicos o dispositivos externos.

Paso 1: Instalar 7-Zip

- Descarga desde <https://www.7-zip.org/>

**7-Zip**

7-Zip is a file archiver with a high compression ratio.

**Download 7-Zip 24.09 (2024-11-29) for Windows x64 (64-bit):**

Link	Type	Windows	Size
<a href="#">Download .exe</a>	64-bit x64	1.6 MB	

**Download 7-Zip 24.09 for another Windows platforms (32-bit x86 or ARM64):**

Link	Type	Windows	Size
<a href="#">Download .exe</a>	32-bit x86	1.3 MB	
<a href="#">Download .exe</a>	64-bit ARM64	1.5 MB	

**License**

7-Zip is free software with open source. The most of the code is under the [GNU LGPL](#) license. Some parts of the code are under the BSD 3-clause License. Also there is unRAR license restriction for some parts of the code. Read [7-Zip License](#) information.

You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

**The main features of 7-Zip**

- High compression ratio in [7z format](#) with LZMA and LZMA2 compression
- Supported formats:
  - Packing / unpacking: 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM
  - Unpacking only: APFS, ARJ, CAB, CHM, CPIO, CrimF, DMG, EXT, FAT, GPT, HFS, JHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTF5, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VHDX, VMDK, XAR and Z.
- For ZIP and GZIP formats, 7-Zip provides a compression ratio that is 2-10 % better than the ratio provided by PKZip and WinZip
- Strong AES-256 encryption in 7z and ZIP formats
- Self-extracting capability for 7z format
- Integration with Windows Shell
- Powerful File Manager
- Powerful Command-line version

**DIETMAR ALEX APAZA**

**7-Zip**

7-Zip is a file archiver with a high compression ratio.

**Download 7-Zip 24.09 (2024-11-29) for Windows x64 (64-bit):**

Link	Type	Windows	Size
<a href="#">Download .exe</a>	64-bit x64	1.6 MB	

**Download 7-Zip 24.09 for another Windows platforms (32-bit x86 or ARM64):**

Link	Type	Windows	Size
<a href="#">Download .exe</a>	32-bit x86	1.3 MB	
<a href="#">Download .exe</a>	64-bit ARM64	1.5 MB	

**License**

7-Zip is free software with open source. The most of the code is under the [GNU LGPL](#) license. Some parts of the code are under the BSD 3-clause License. Also there is unRAR license restriction for some parts of the code. Read [7-Zip License](#) information.

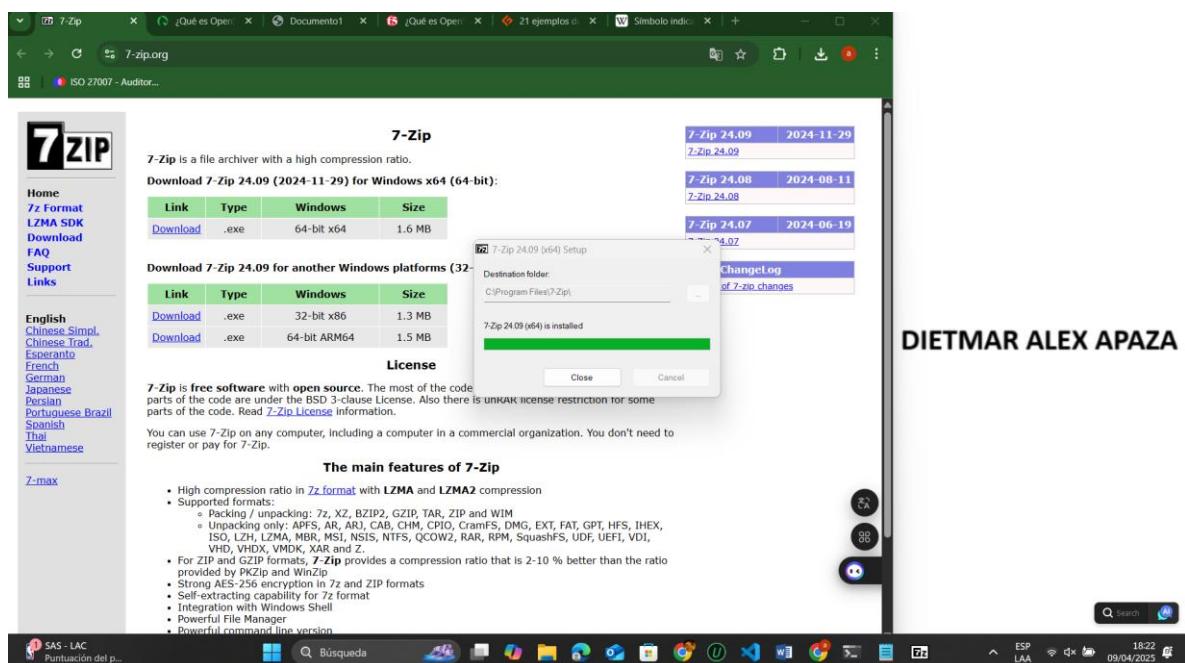
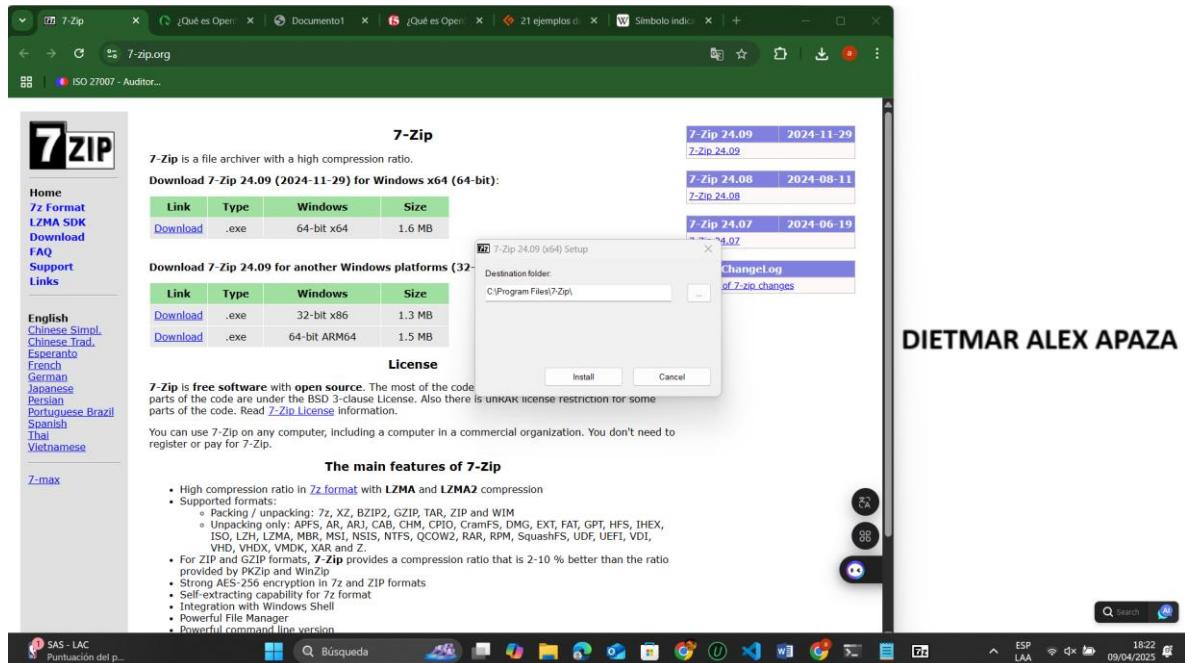
You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

**The main features of 7-Zip**

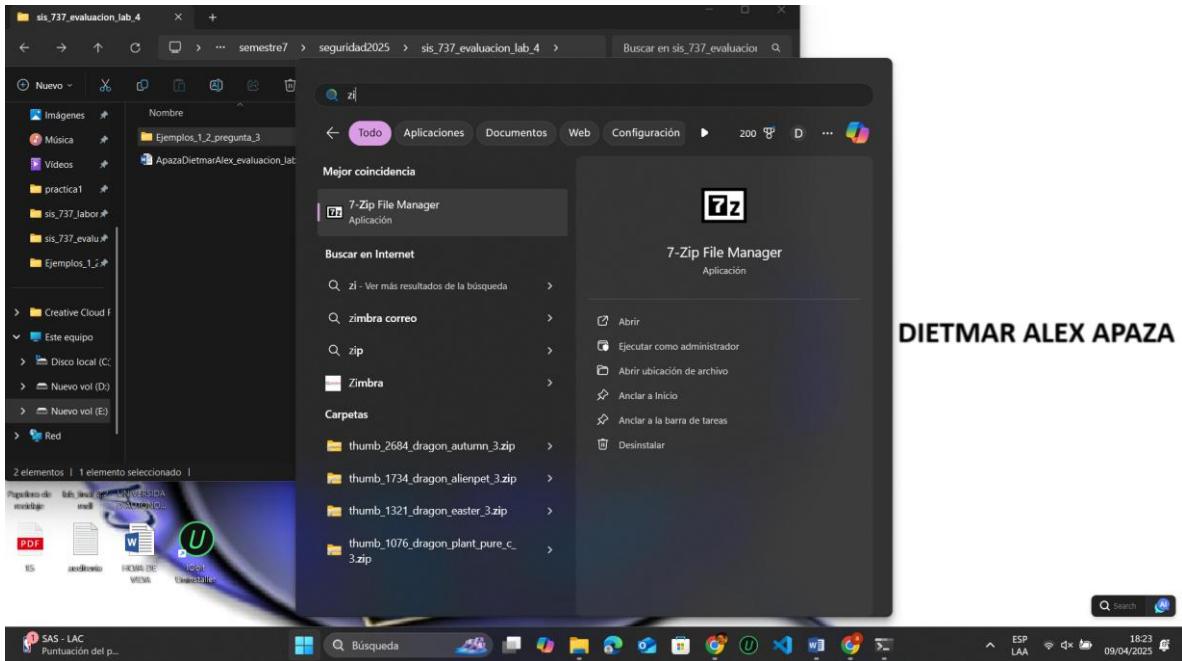
- High compression ratio in [7z format](#) with LZMA and LZMA2 compression
- Supported formats:
  - Packing / unpacking: 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM
  - Unpacking only: APFS, ARJ, CAB, CHM, CPIO, CrimF, DMG, EXT, FAT, GPT, HFS, JHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTF5, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VHDX, VMDK, XAR and Z.
- For ZIP and GZIP formats, 7-Zip provides a compression ratio that is 2-10 % better than the ratio provided by PKZip and WinZip
- Strong AES-256 encryption in 7z and ZIP formats
- Self-extracting capability for 7z format
- Integration with Windows Shell
- Powerful File Manager
- Powerful command-line version

**DIETMAR ALEX APAZA**

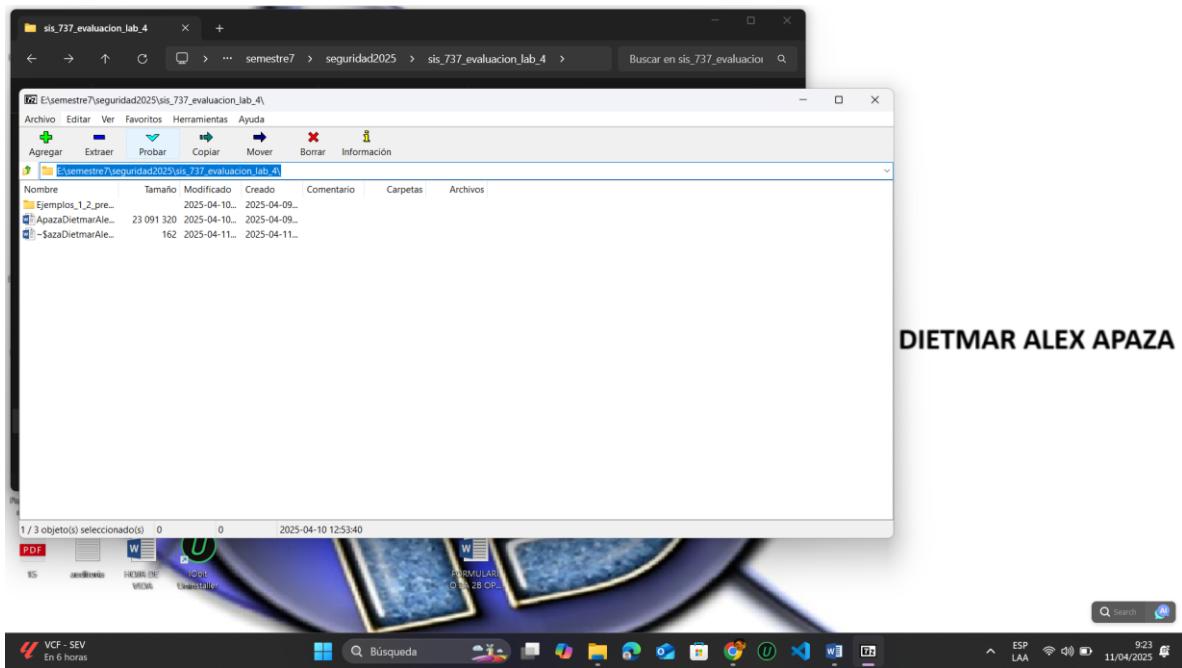
- Instálalo normalmente en tu PC.



Verificar que se instaló correctamente la aplicación 7-Zip

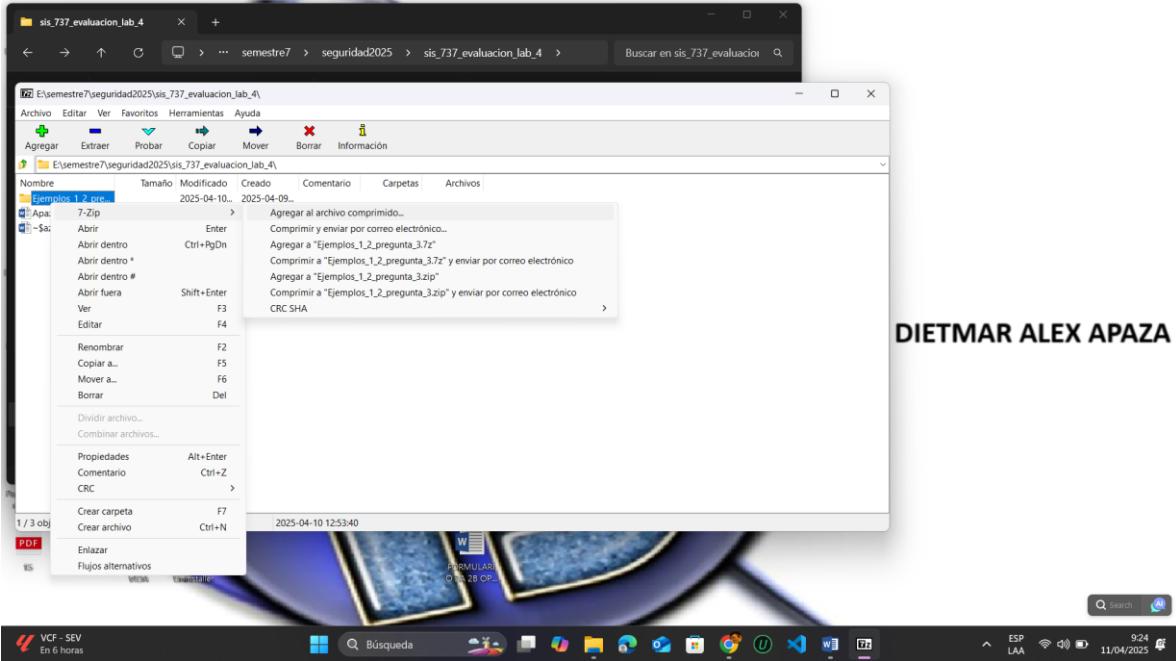


## Paso 2: Comprimir y cifrar



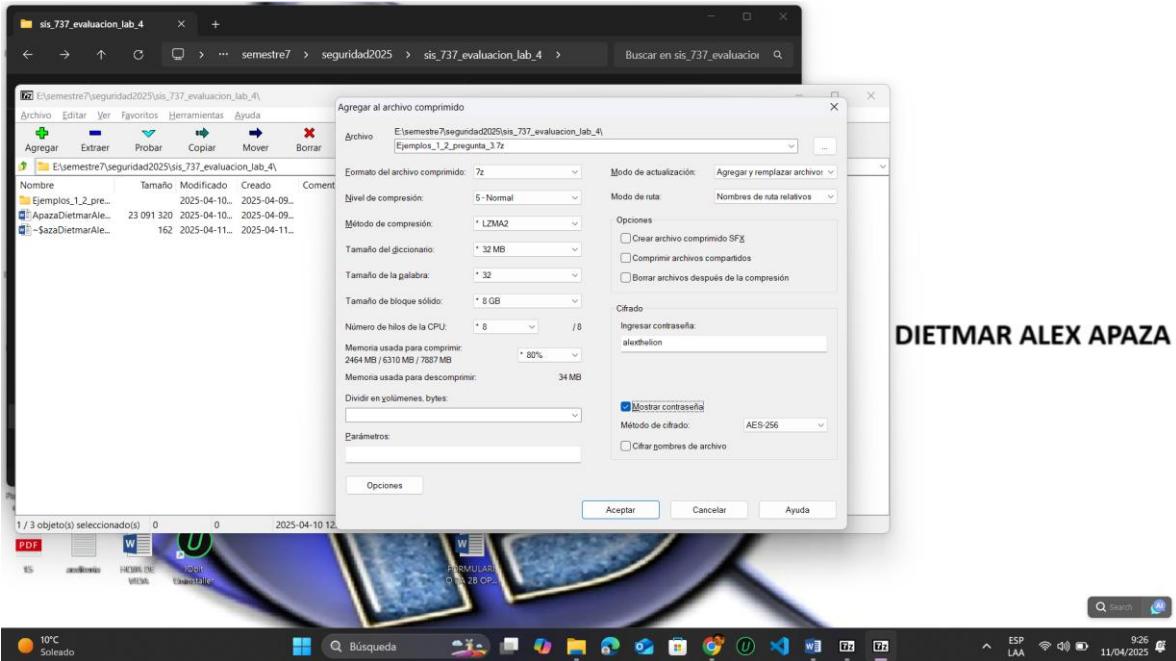
- Haremos clic derecho sobre la carpeta que queremos cifrar, en este caso será la carpeta que hicimos los dos ejemplos de la pregunta 3: **Ejemplos\_1\_2\_pregunta\_3**

- Selecciona 7-Zip > Añadir al archivo...

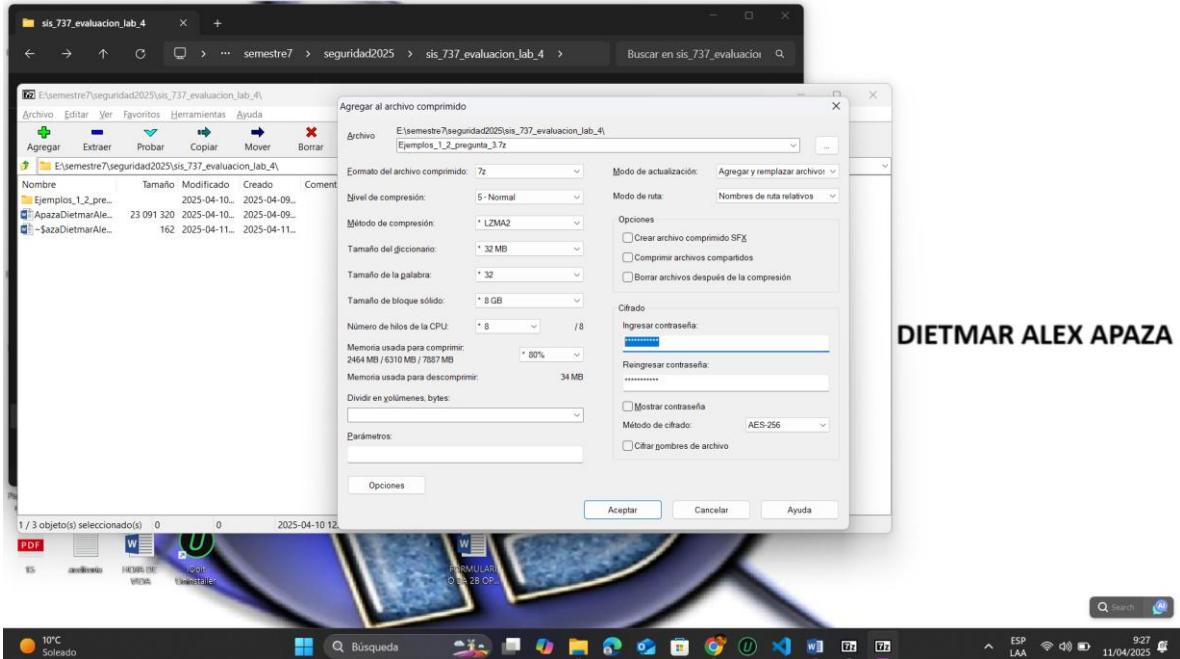


- En la ventana que aparece:

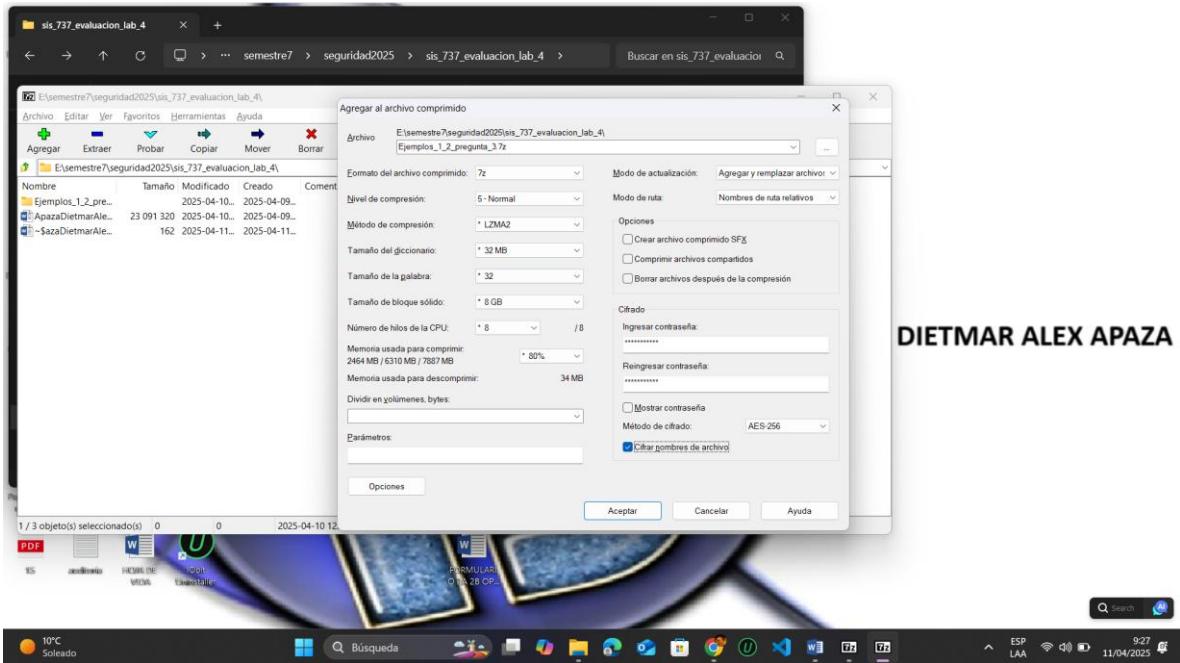
- **Formato de archivo:** zip o 7z



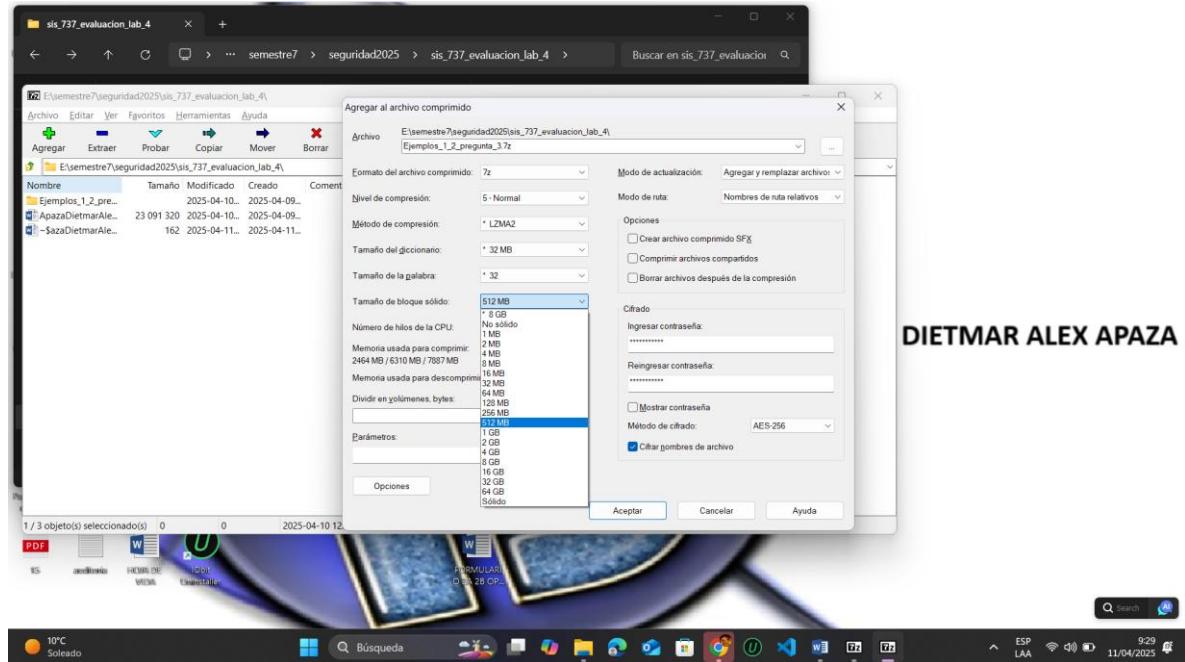
- Establece una contraseña en el campo de "Contraseña".



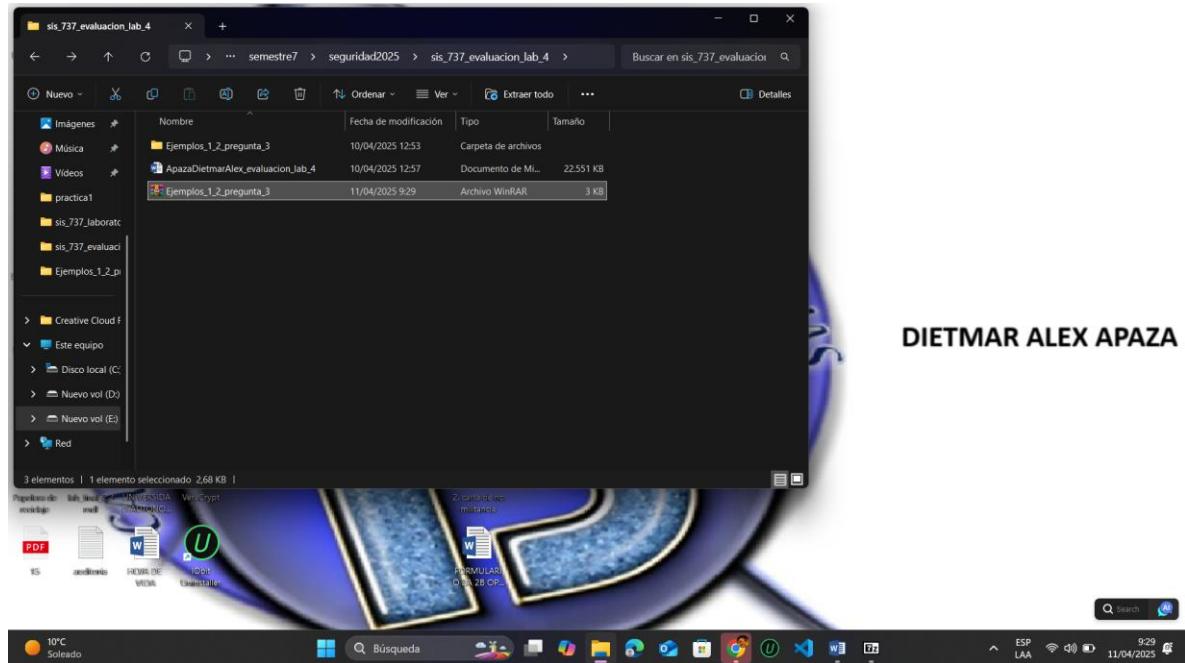
- Marca la opción "Cifrar nombres de archivos" si deseas mayor seguridad.



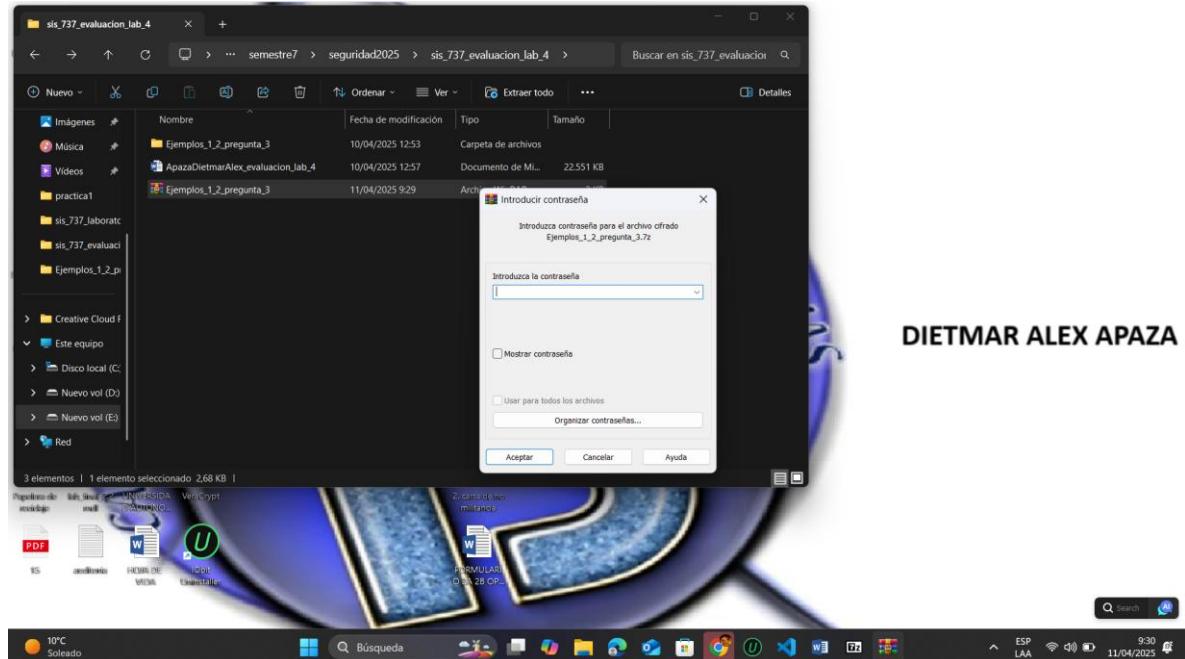
- Presiona Aceptar.



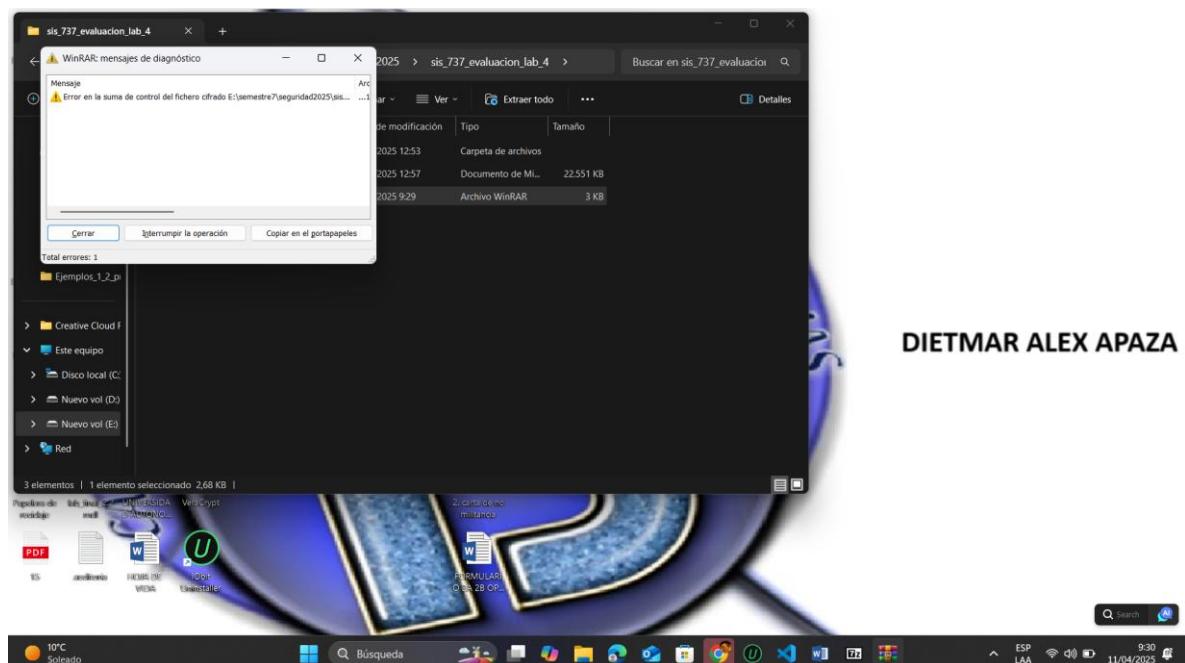
DIETMAR ALEX APAZA



DIETMAR ALEX APAZA



DIETMAR ALEX APAZA



DIETMAR ALEX APAZA