



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

LAB_4 - CIFRADO SIMÉTRICO

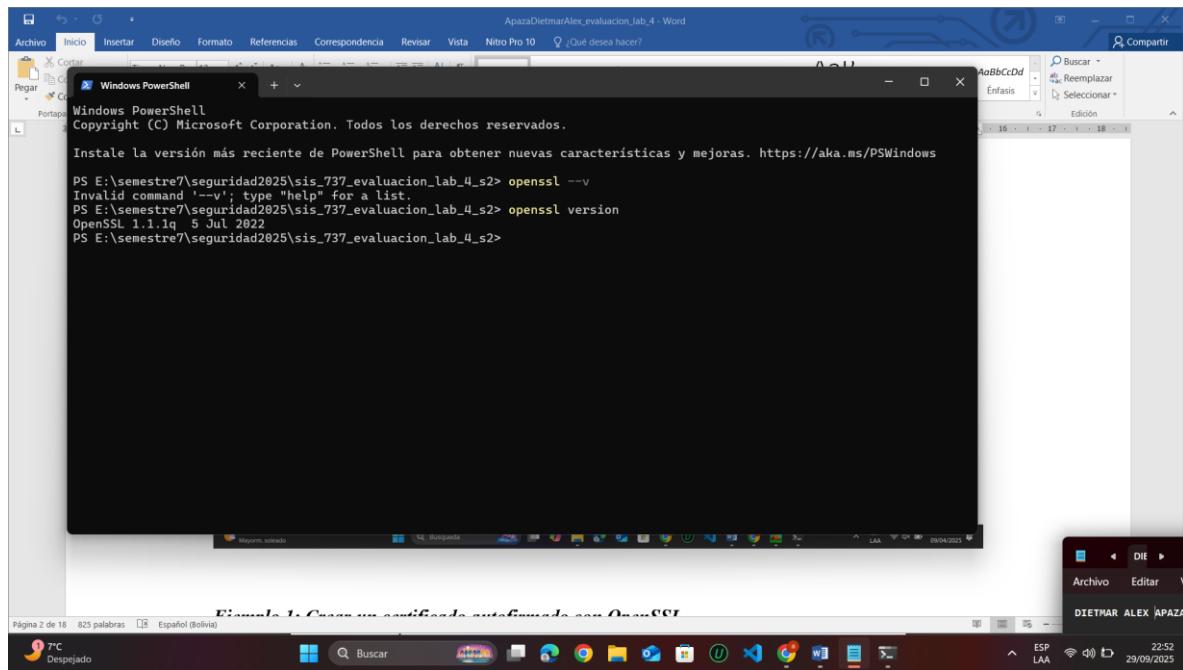
EVALUACIÓN

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

A screenshot of a Windows desktop environment. In the foreground, a PowerShell window is open with the following command history:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> openssl --v
Invalid command '-v'; type "help" for a list.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> openssl version
OpenSSL 1.1.1q 5 Jul 2022
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> mkdir Ejemplos_1_2_pregunta_3

Directorio: E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2

Mode           LastWriteTime      Length Name
----           -----          ----  --
d----
```

The PowerShell window shows a directory listing for the folder 'Ejemplos_1_2_pregunta_3' which was created earlier.

3. Verificamos que estamos dentro de la carpeta

A screenshot of a Windows desktop environment. In the foreground, a PowerShell window is open with the following command history:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> openssl --v
Invalid command '-v'; type "help" for a list.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> openssl version
OpenSSL 1.1.1q 5 Jul 2022
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2> mkdir Ejemplos_1_2_pregunta_3

Directorio: E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2

Mode           LastWriteTime      Length Name
----           -----          ----  --
d----
```

The command `cd .\Ejemplos_1_2_pregunta_3\` is highlighted in the PowerShell window, indicating the current working directory has been changed to the newly created folder.

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_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
req: Use -help for summary.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
req: Use -help for summary.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
req: Use -help for summary.
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.

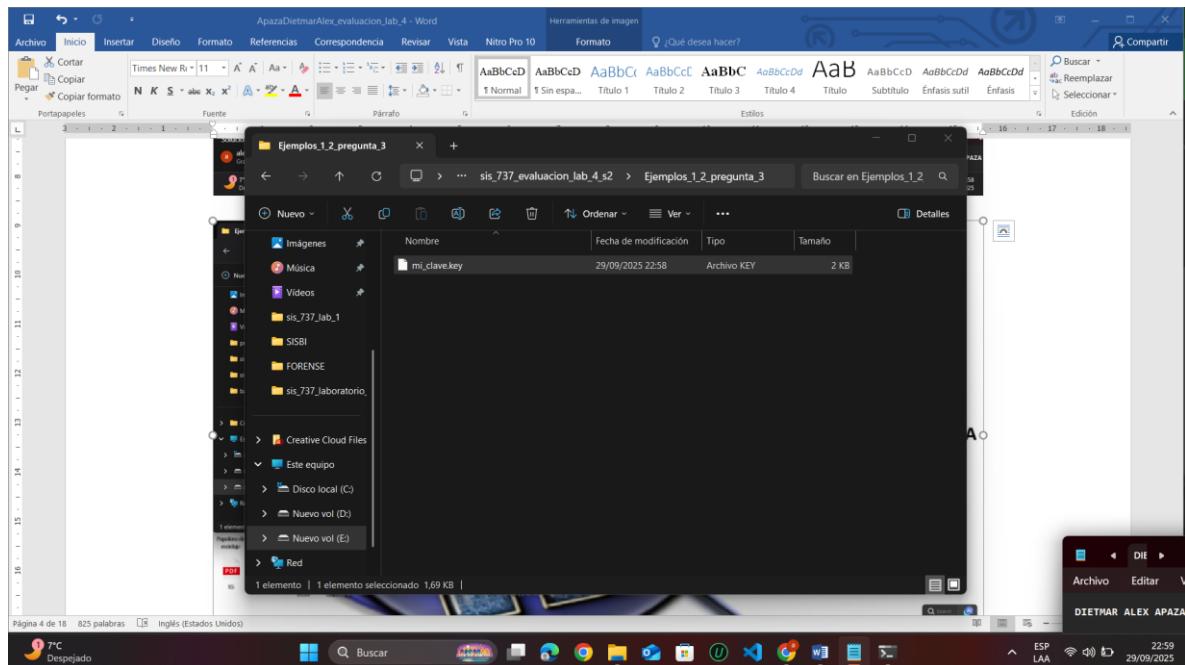
What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank.

For some fields there will be a default value.

Corregir If you enter '.', the field will be left blank.

Alternative Country Name (2 letter code) [AU]:



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. **Ingenieria de Sistemas**

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

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

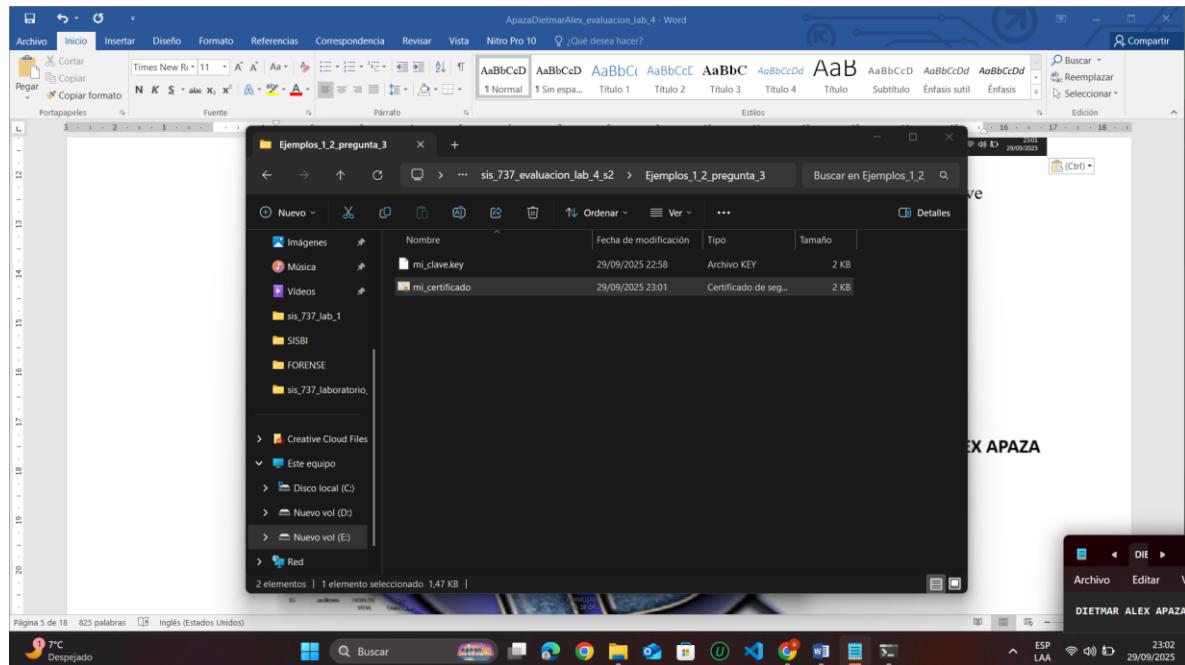
Email Address : alexapaza72361453@gmail.com

The screenshot shows a Windows desktop environment. In the center, there is a PowerShell window titled "Windows PowerShell" with the following command and output:

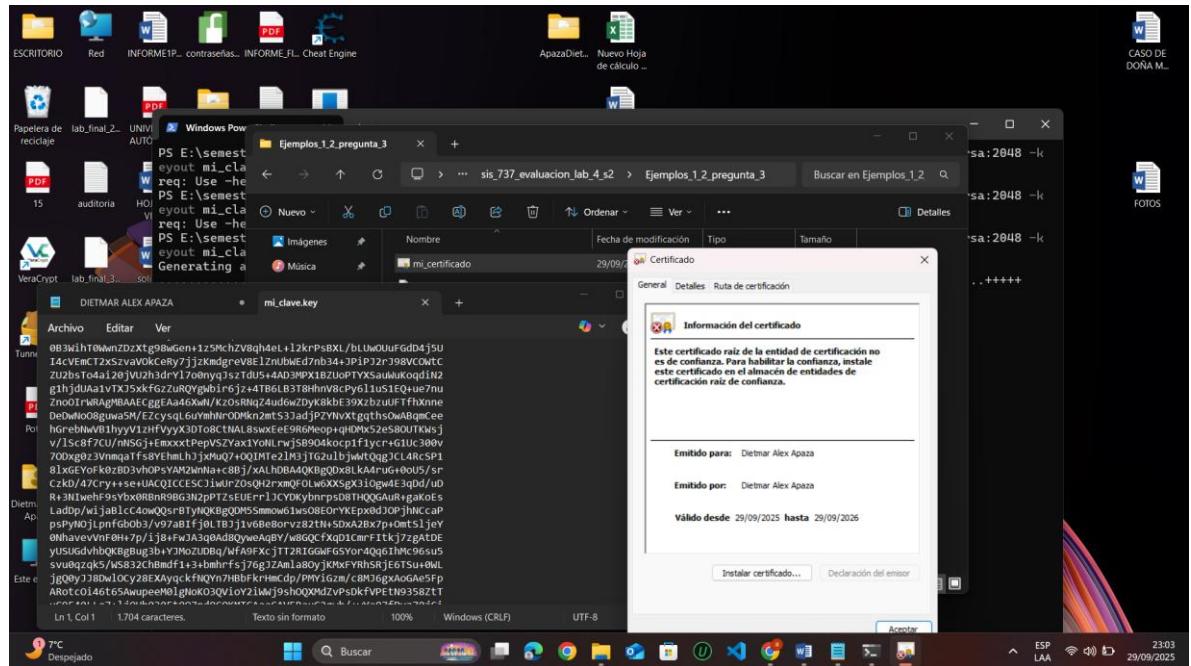
```
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
eyout mi_clave.key -out mi_certificado.crt -days 365 -nodes
req: Use -help for summary.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
eyout mi_clave.key -out mi_certificado.crt -days 365 -nodes
req: Use -help for summary.
PS E:\semestre7\seguridad2025\sis_737_evaluacion_lab_4_s2\Ejemplos_1_2_pregunta_3> openssl req -x509 -newkey rsa:2048 -k
eyout 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]:BO
State or Province Name (full name) [Some-State]:Tomas Frias
Locality Name (eg, city) []:Potosí
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ingierencia de Sistemas
Organizational Unit Name (eg, section) []
Common Name (e.g. server FQDN or YOUR name) []:Dietmar Alex Apaza
Email Address []:alexapaza72361453@gmail.com
```

Below the PowerShell window, a Microsoft Word document titled "ApazaDietmarAlex_evaluacion_lab_4 - Word" is open. The document contains the same text as the PowerShell output. The status bar at the bottom of the screen shows "Página 5 de 18 825 palabras".

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



- Como resultado tenemos la clave que esta cifrada y el certificado autofirmado



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

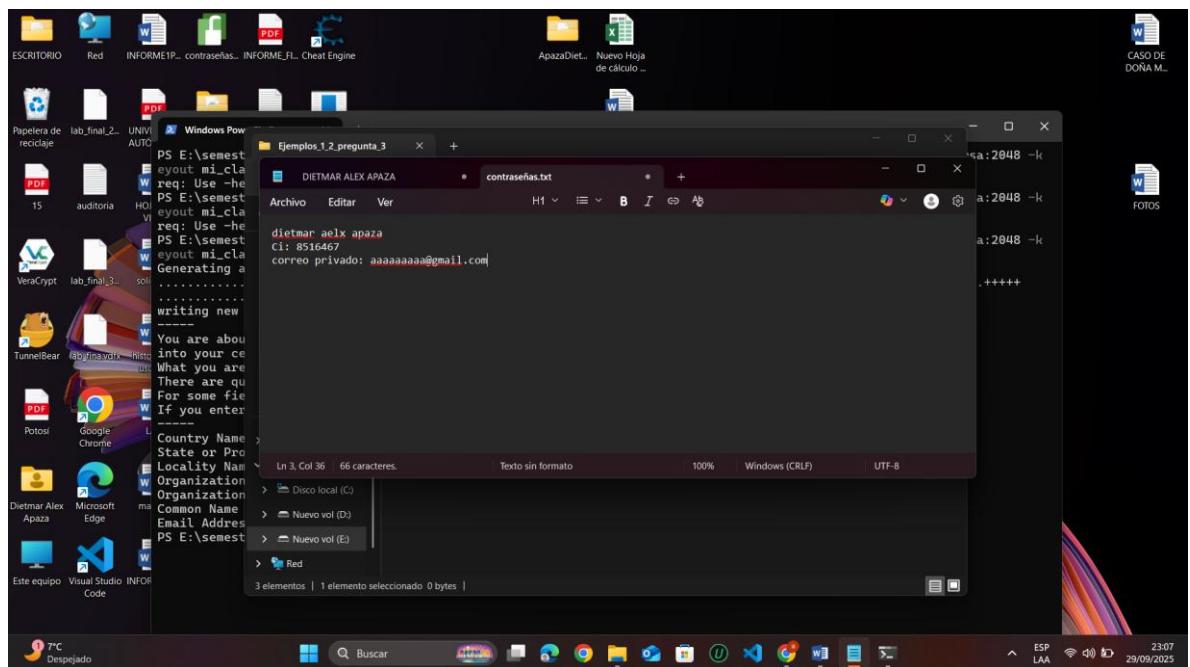
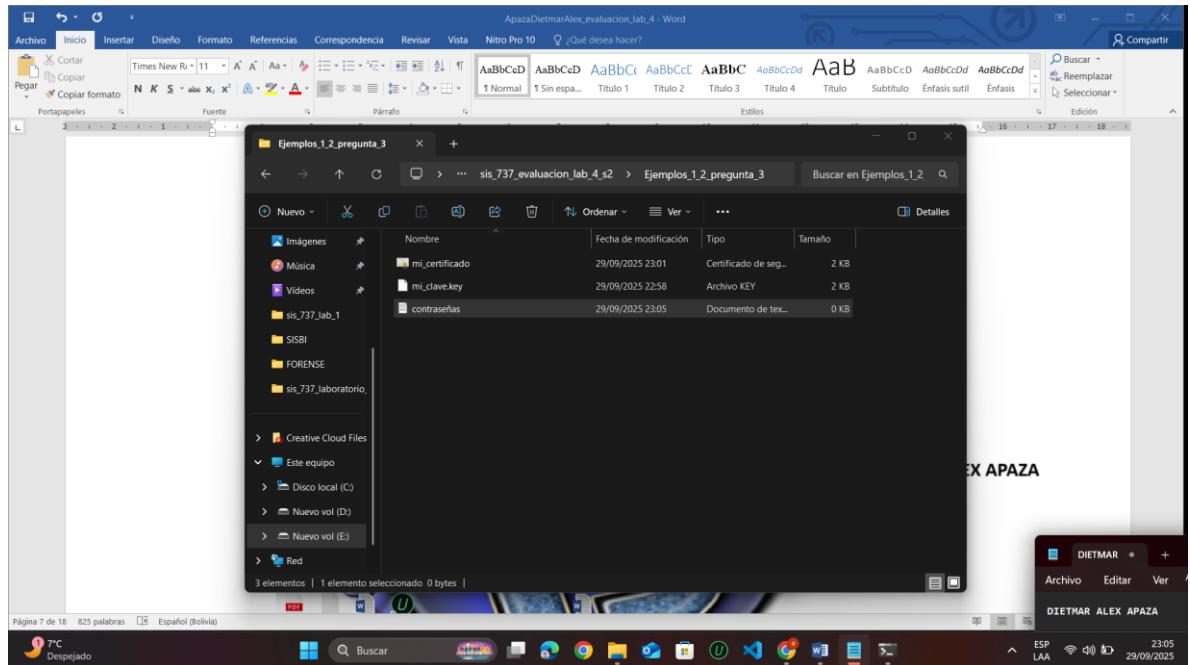
Ideal si quieres proteger archivos sensibles como contraseñas, información financiera, etc.

Objetivo:

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

Qué necesitas:

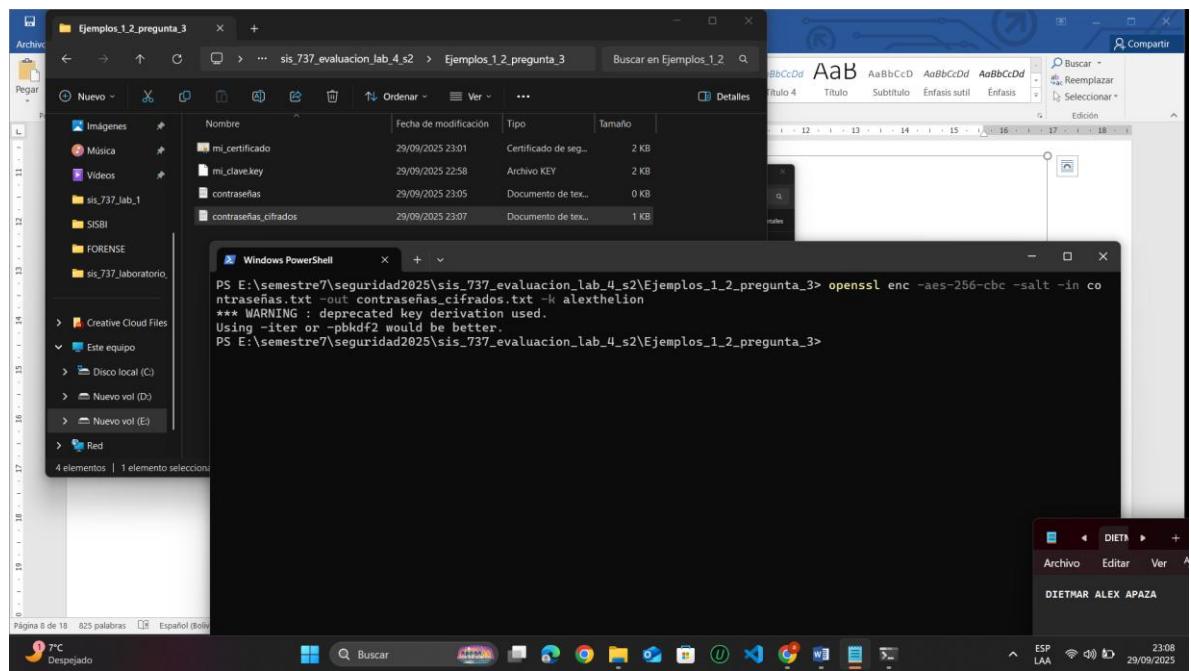
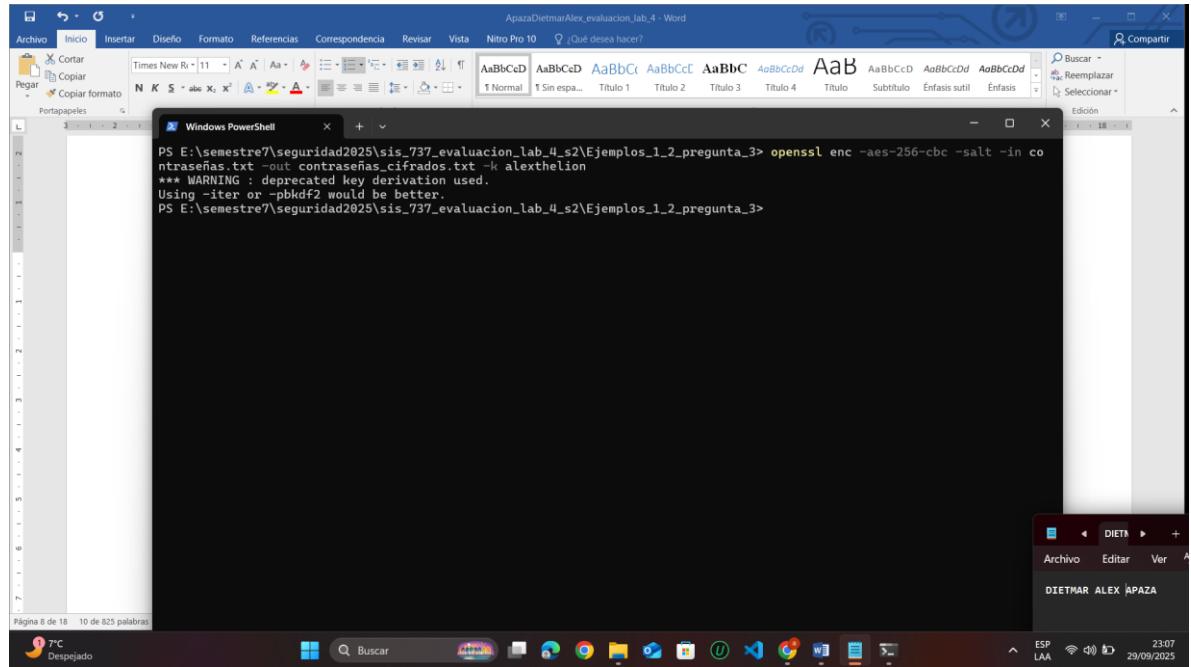
- Un archivo de texto (ej. `contraseñas.txt`) con información que quieras proteger.

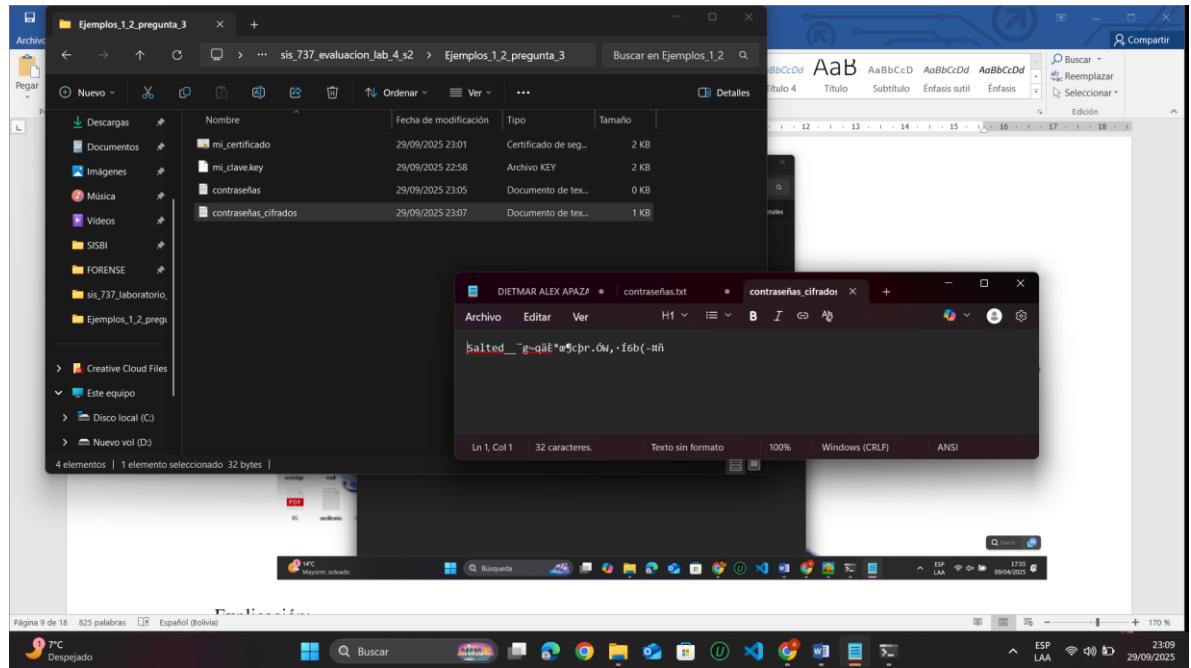


- La contraseña que utilizaremos para cifrar será: `alexthelion`

Cifrar el archivo

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



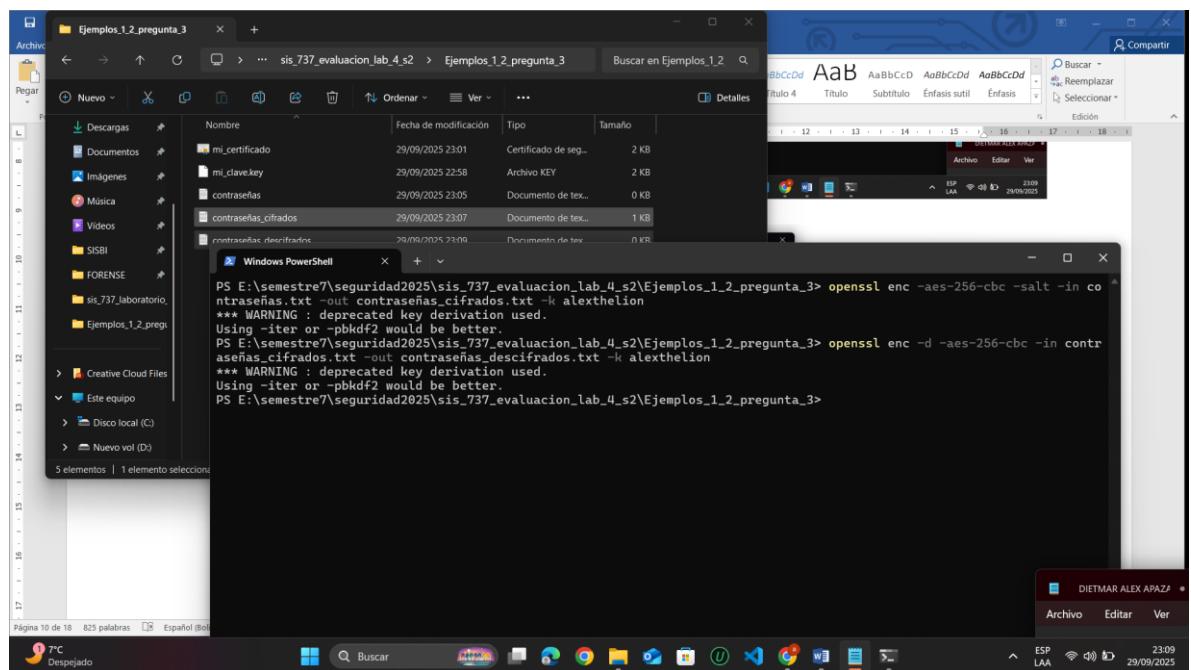
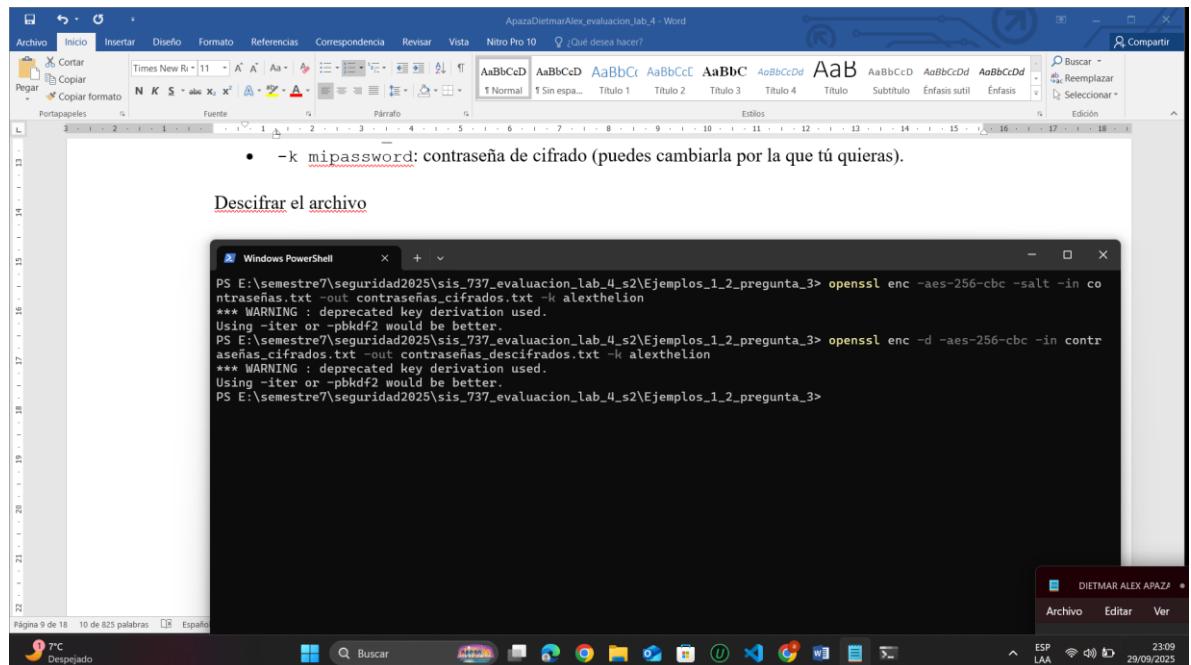


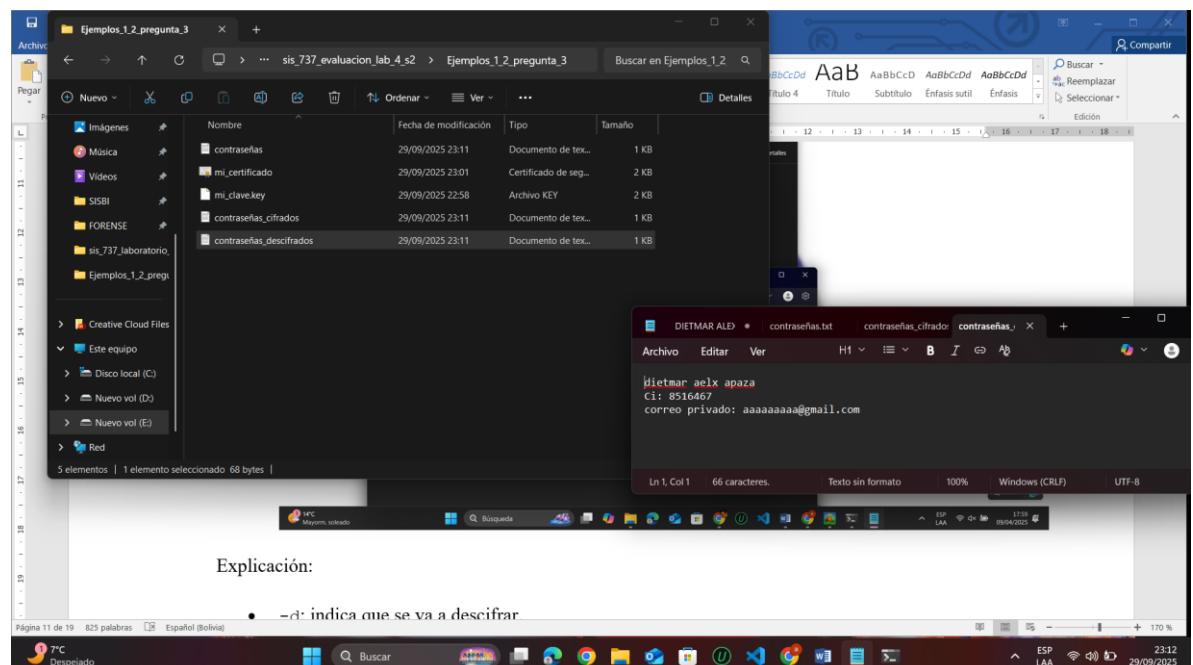
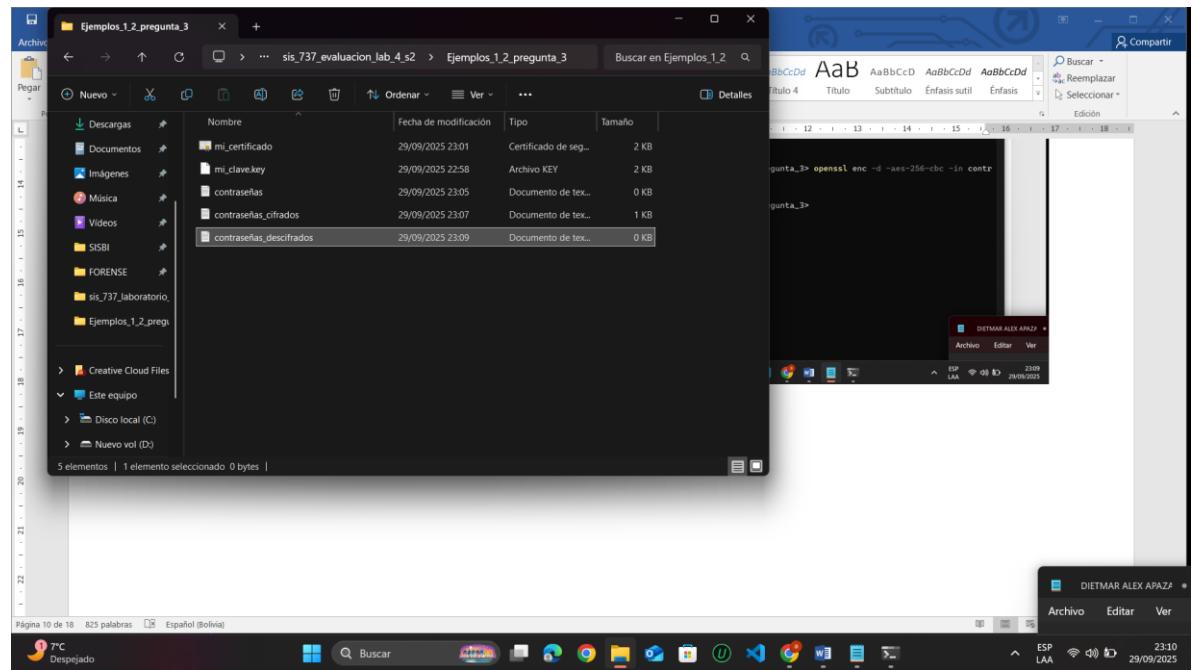
Explicación:

- **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`





Explicación:

- `-d`: indica que se va a descifrar.

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.

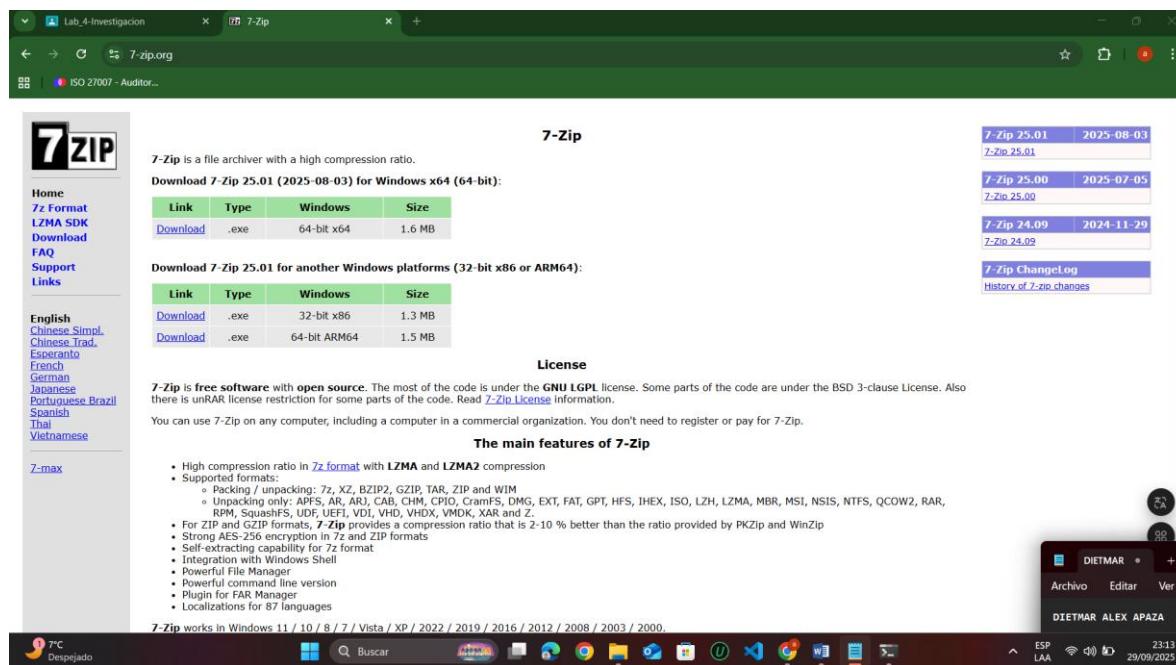
En esta actividad se procederá a **cifrar una carpeta que contiene archivos sensibles**, utilizando herramientas que permitan proteger su contenido mediante **algoritmos de cifrado seguros**.

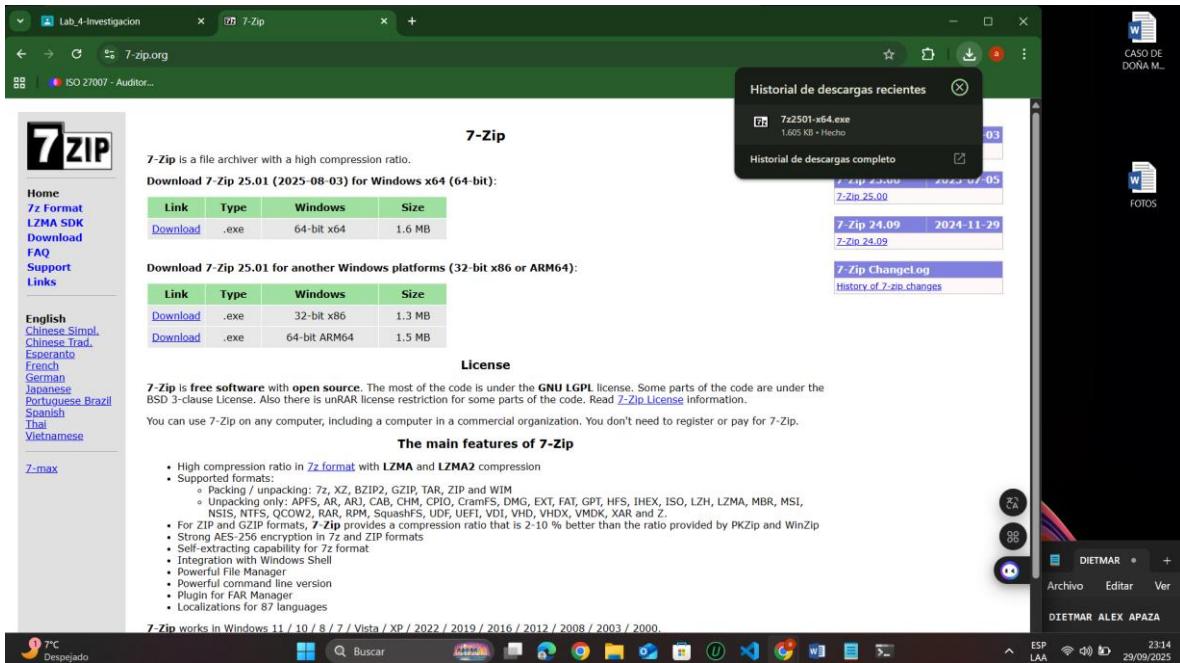
Para lograr esto, se utilizará la herramienta **7-Zip**, una aplicación de compresión que permite, además de reducir el tamaño de los archivos, aplicar una contraseña de acceso y cifrado AES-256 a los datos.

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

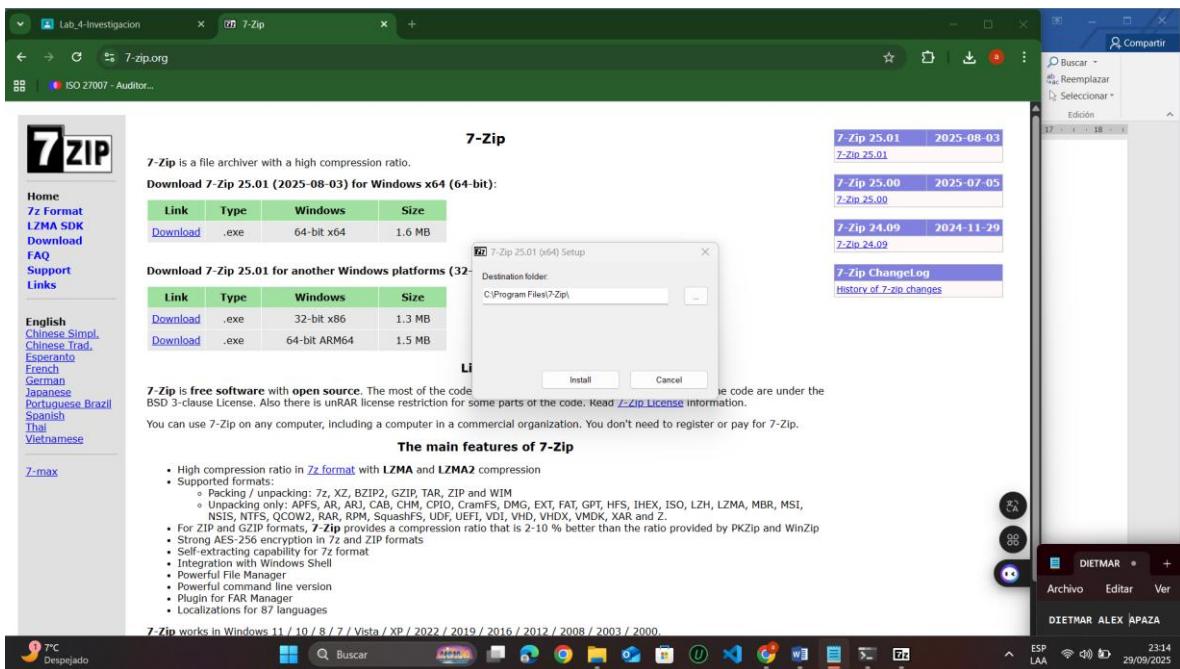
Paso 1: Instalar 7-Zip

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

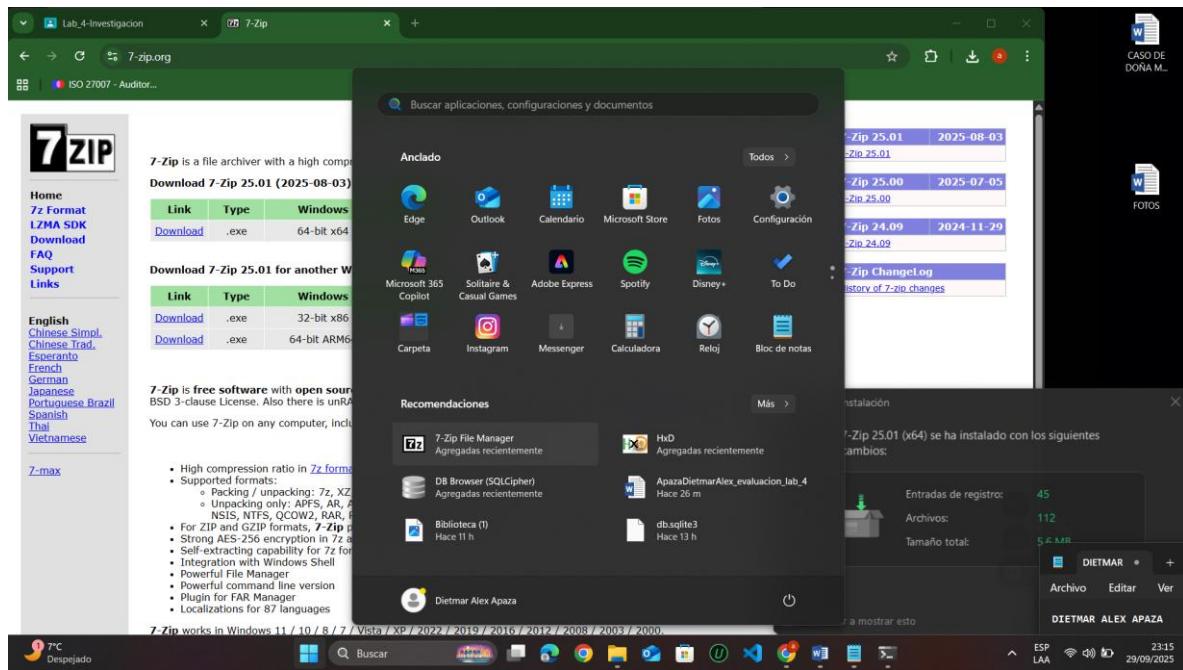




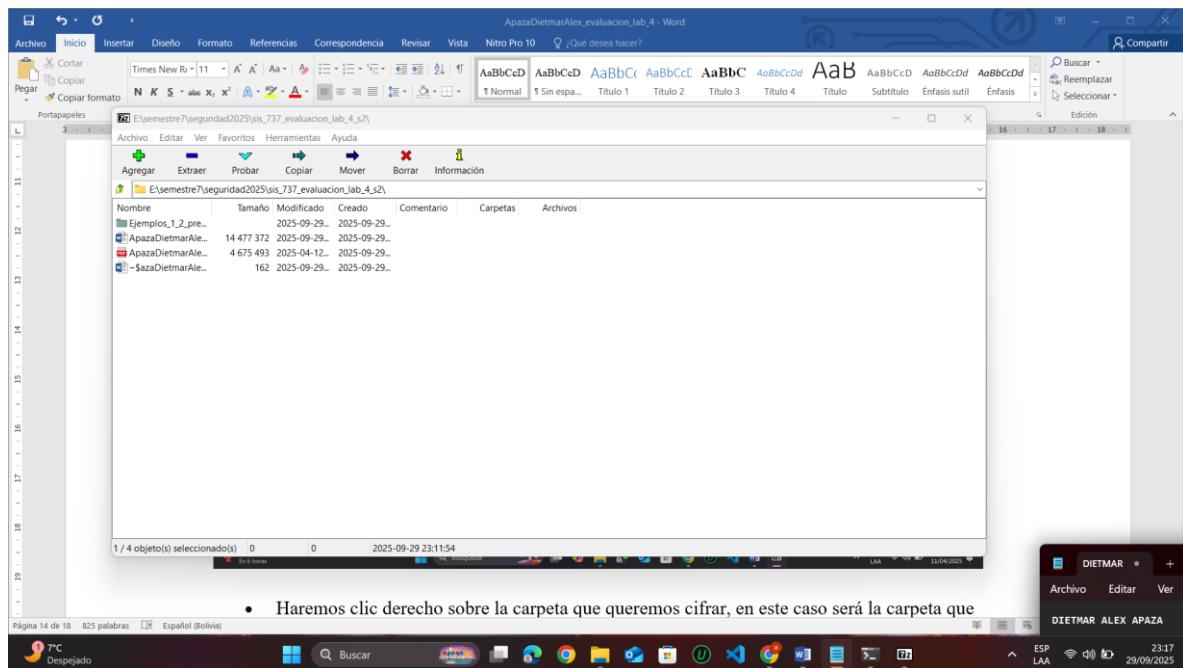
- Instálalo normalmente en tu PC.



Verificar que se instaló correctamente la aplicación 7-Zip

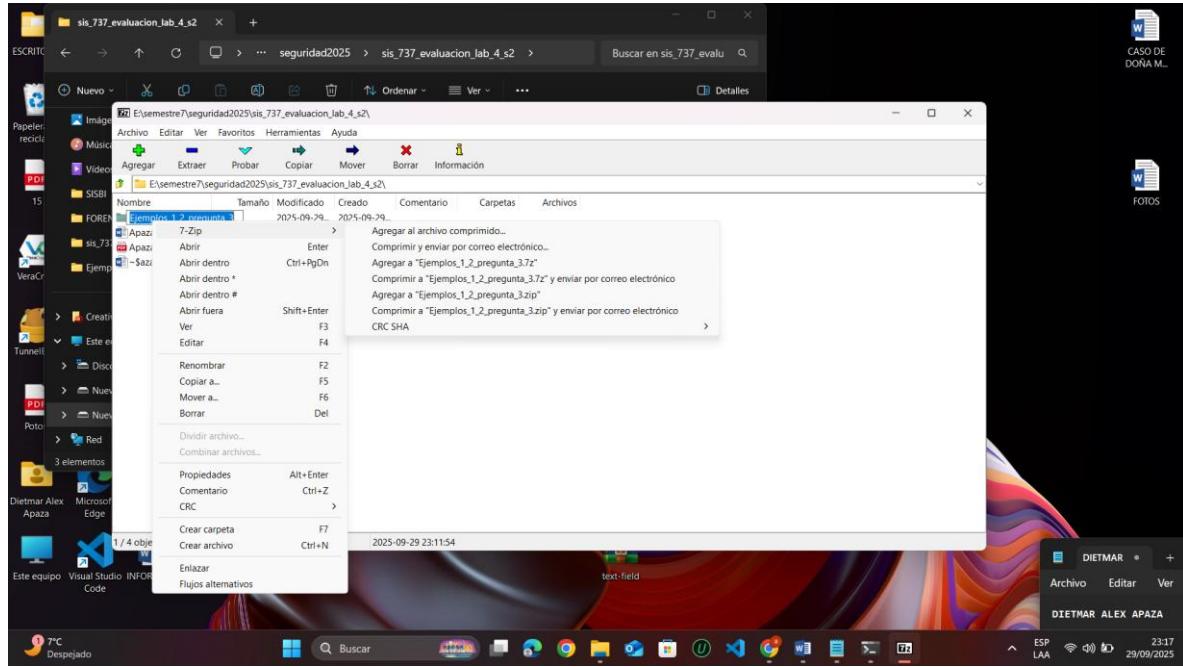


Paso 2: Comprimir y cifrar



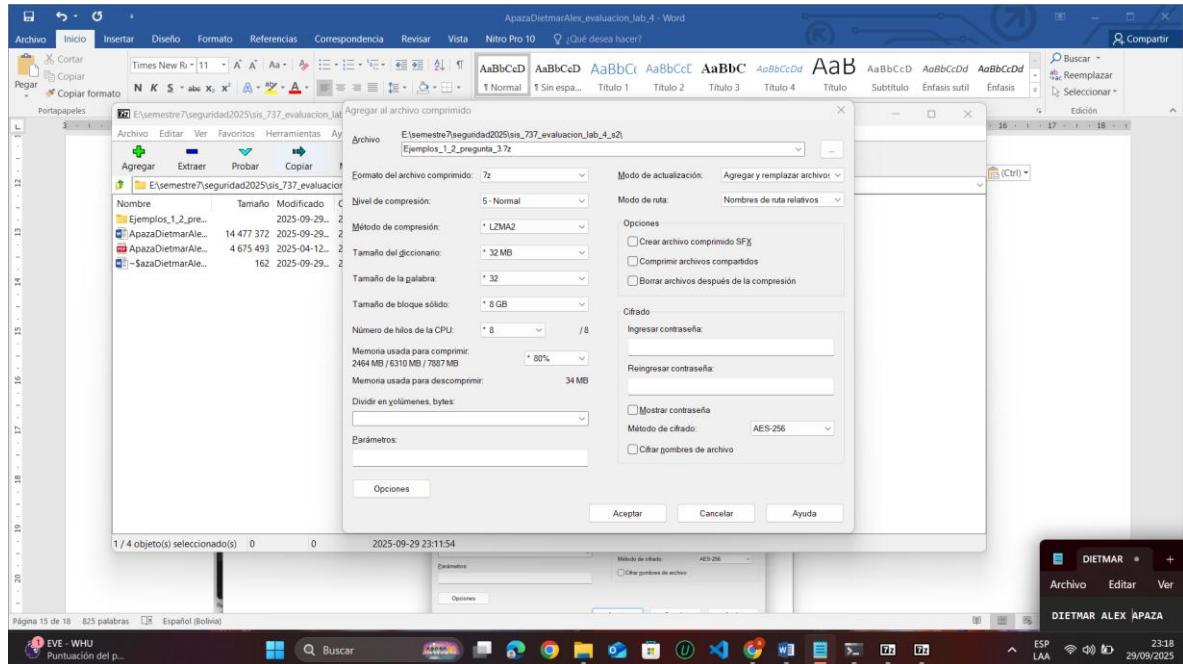
- Haremos clic derecho sobre la carpeta que queremos cifrar, en este caso será la carpeta que hicimos los dos ejemplos de la pregunta 3: **Ejemplos_1_2_pregunta_3**

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

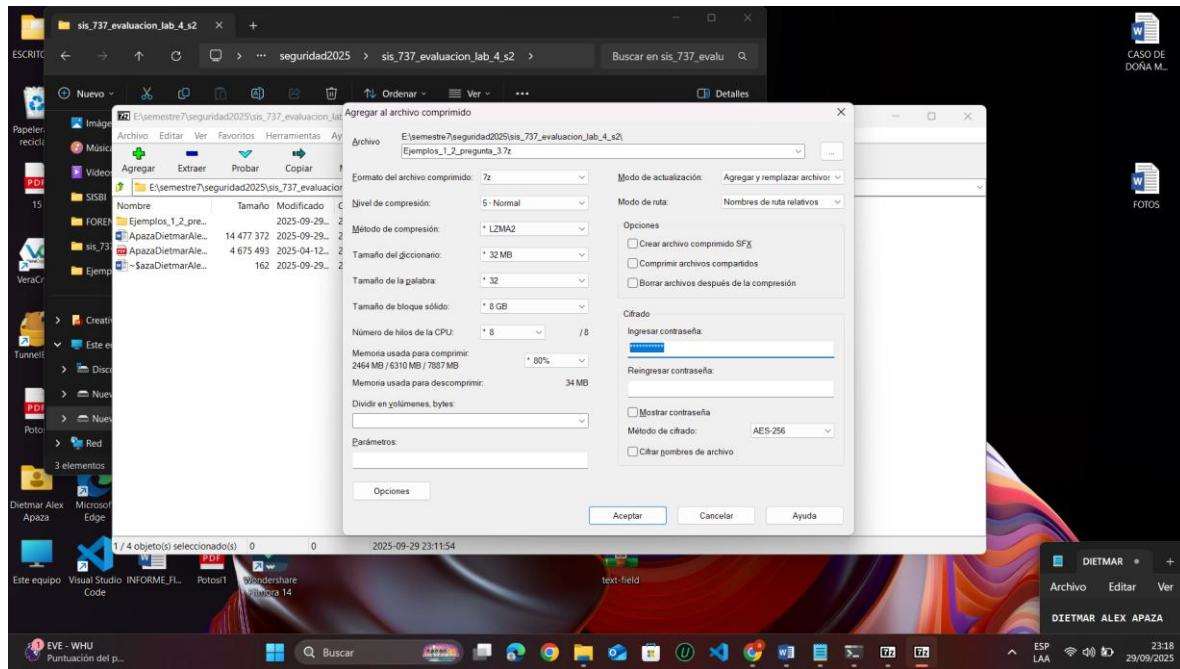


- En la ventana que aparece:

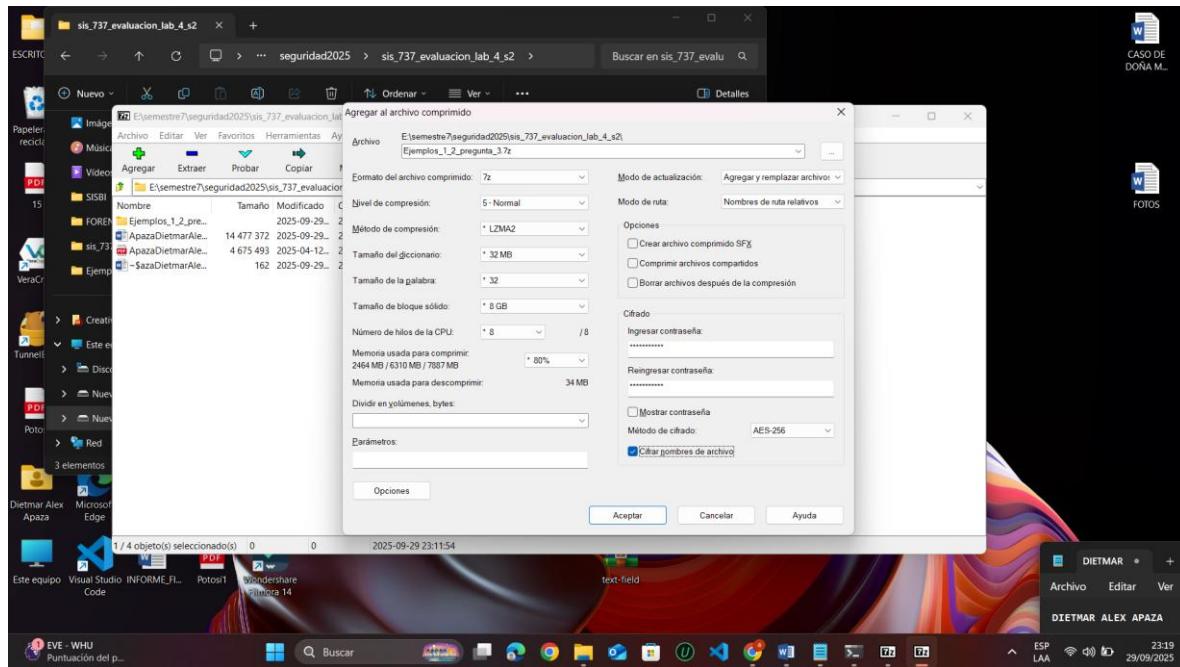
- **Formato de archivo:** zip o 7z



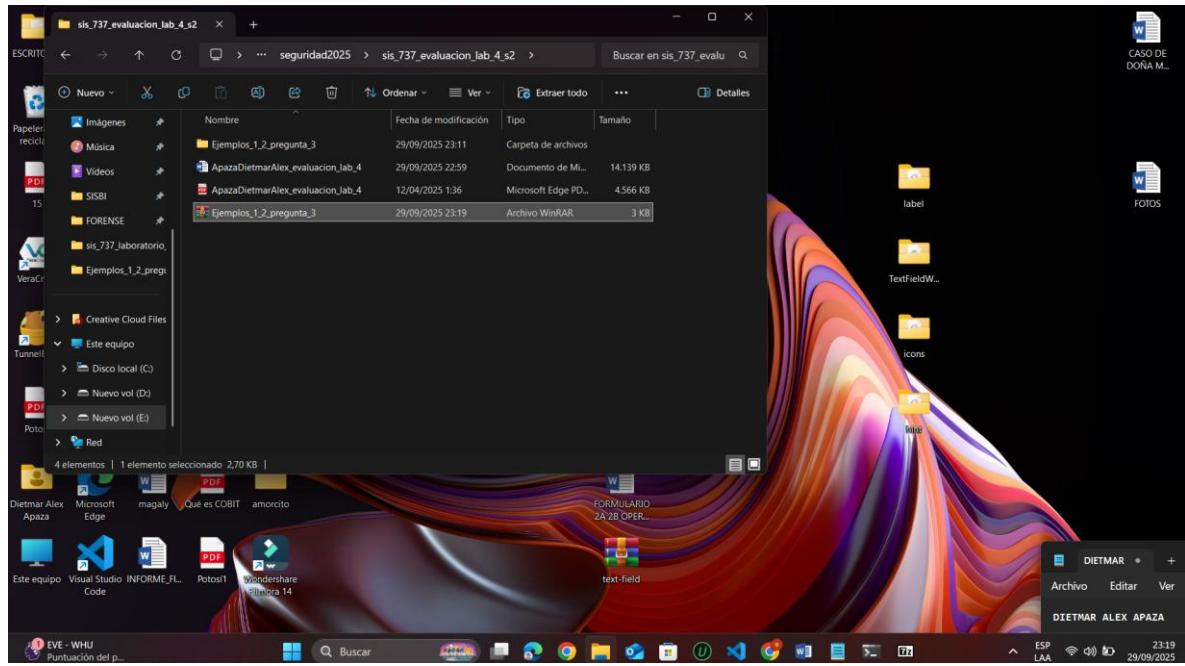
- Establece una contraseña en el campo de "Contraseña".



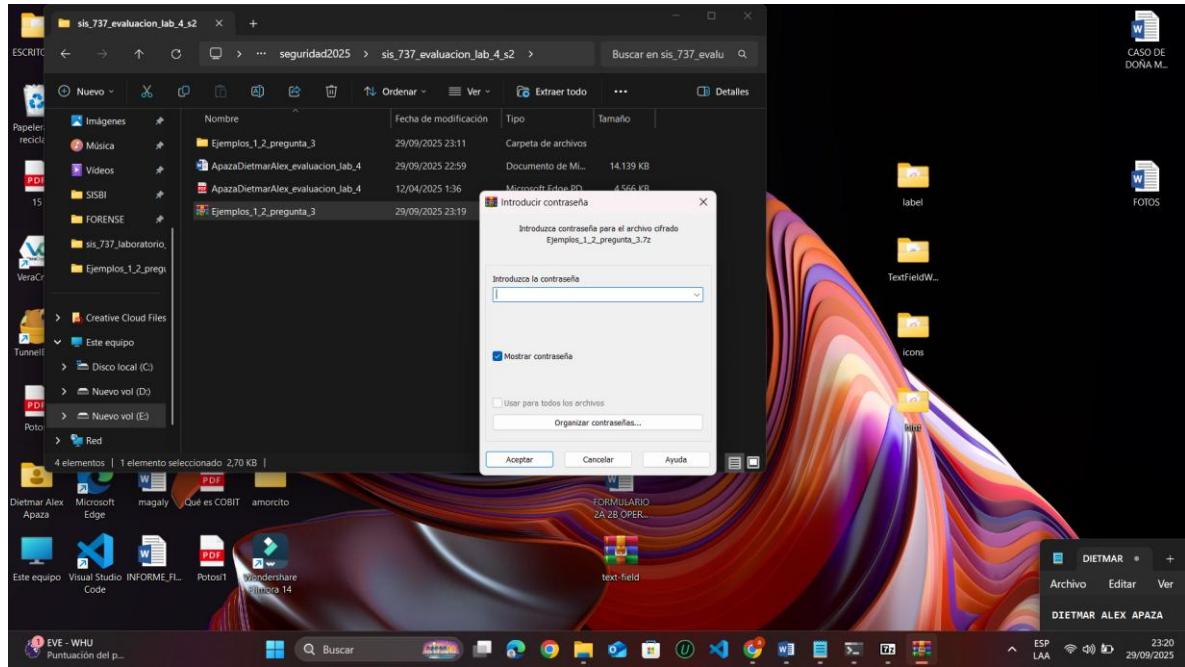
- Marca la opción "Cifrar nombres de archivos" si deseas mayor seguridad.



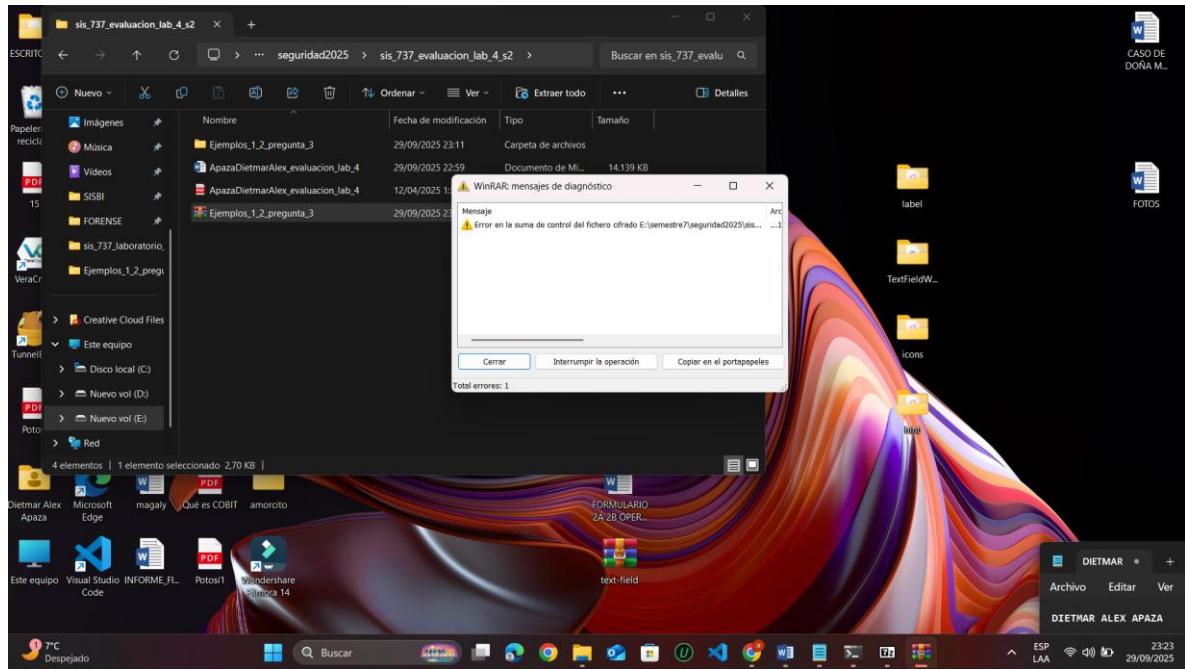
- Presiona Aceptar.



Una vez presionado aceptar se nos creara el archivo comprimido al abrir el archivo nos pedirá la contraseña con la que se cifro.



Si se ingresa la contraseña incorrecta el archivo nunca se abrirá y nos mostrara el siguiente mensaje



Si introducimos la contraseña correcta se nos abrirá todos los archivos y documentos que queríamos proteger

