



UNIVERSIDAD AUTÓNOMA "TOMÁS FRÍAS"  
CARRERA DE INGENIERÍA DE SISTEMAS

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

**NOMBRE:** Univ. Dietmar Alex Apaza

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

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

GitHub

Nombre: AlexTheLion99

Enlace\_lab\_6:[https://github.com/AlexTheLion99/sis\\_737\\_Laboratorio\\_6](https://github.com/AlexTheLion99/sis_737_Laboratorio_6)

**LABORATORIO N°: 6**

## LABORATORIO 6 – ESTEGANOGRAFÍA CON STEGHIDE

**Propósito:** Steghide es un programa de esteganografía de código abierto que oculta los datos de distintos tipos de archivos como archivos de audio y de imagen. De esta manera se puede ocultar información, que muchas veces pasa desapercibida a diferencia de un archivo cifrado.

**Competencia:** El estudiante comprende la importancia de la ocultación de la información empleando imágenes o archivos de audio para que esta sea imperceptible.

### PARTE 1

#### DESCRIPCIÓN

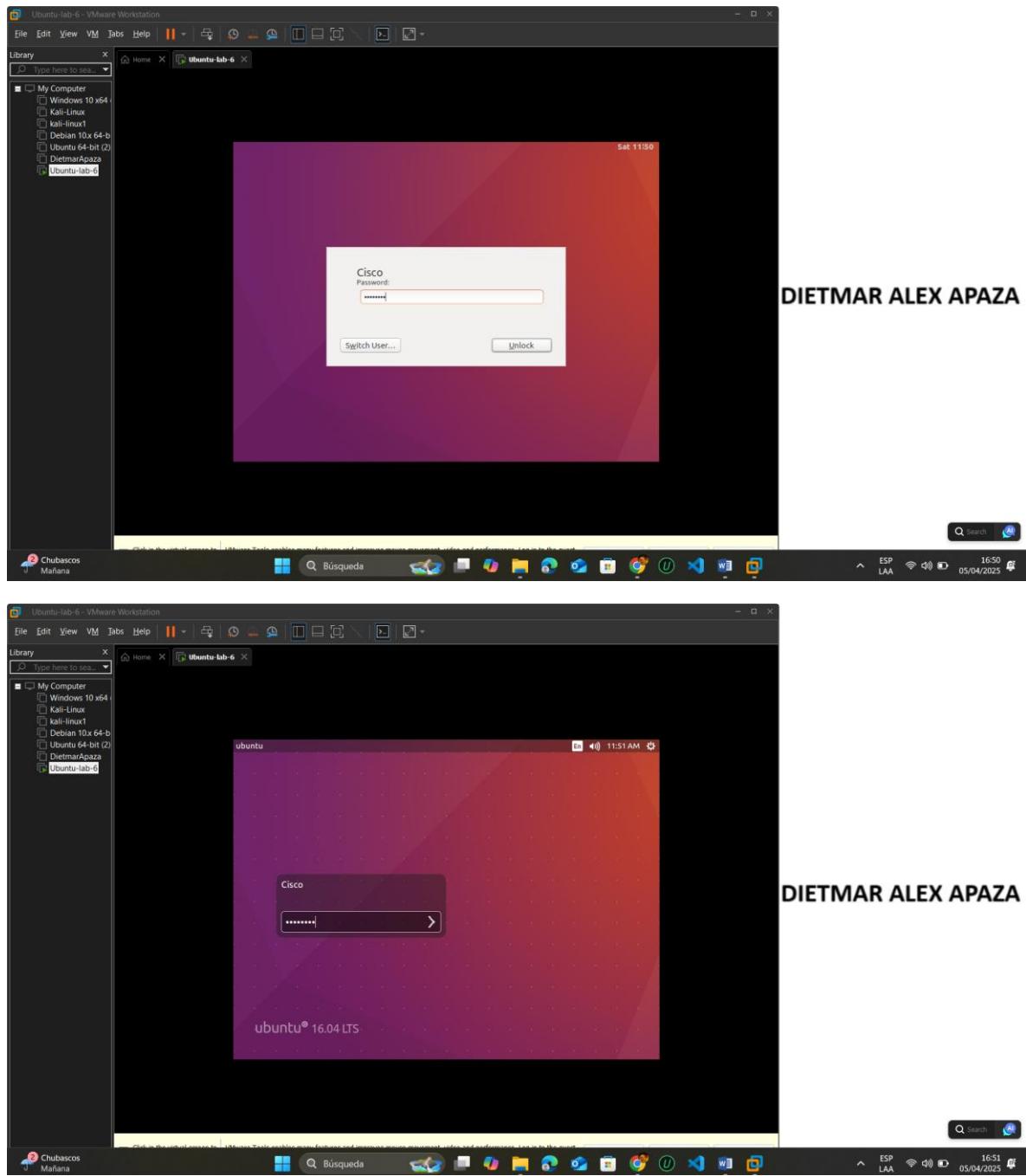
**Recursos:** Computadora de escritorio con Ubuntu CISCO 16.04.4 LTS instalado en una máquina virtual de VirtualBox o VMware.

**Paso 1:** Abra una ventana del terminal en Ubuntu.

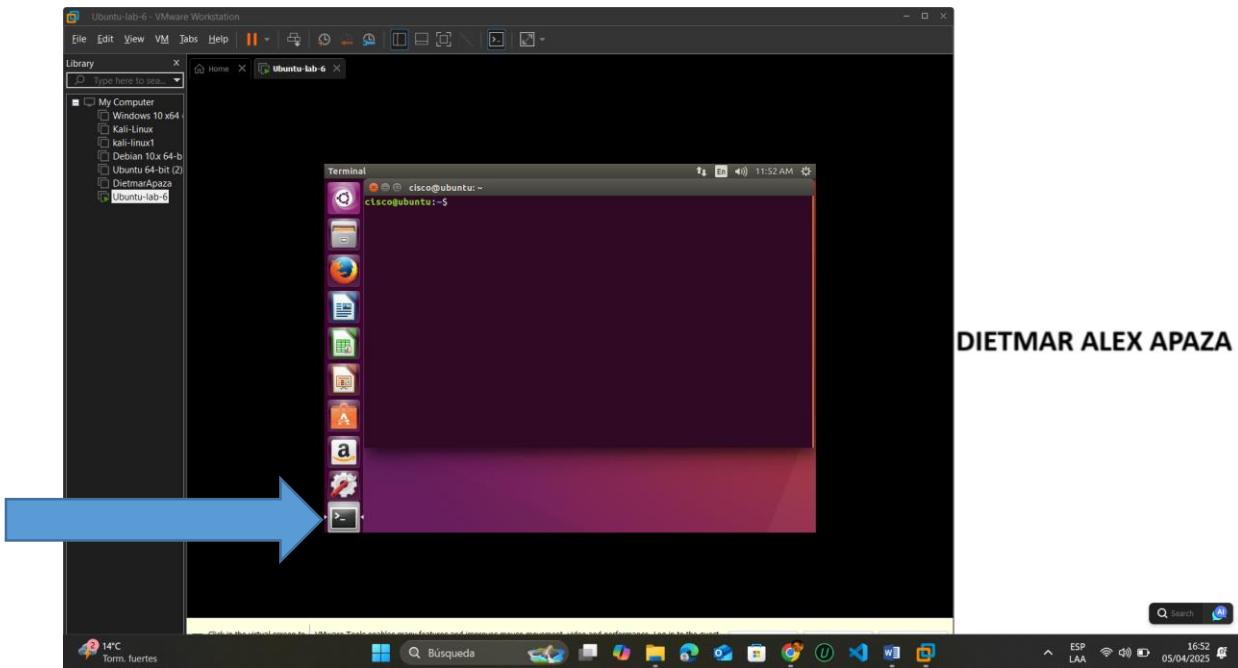
a. Inicie sesión en Ubuntu con las siguientes credenciales:

**Usuario:** cisco

**Contraseña:** password



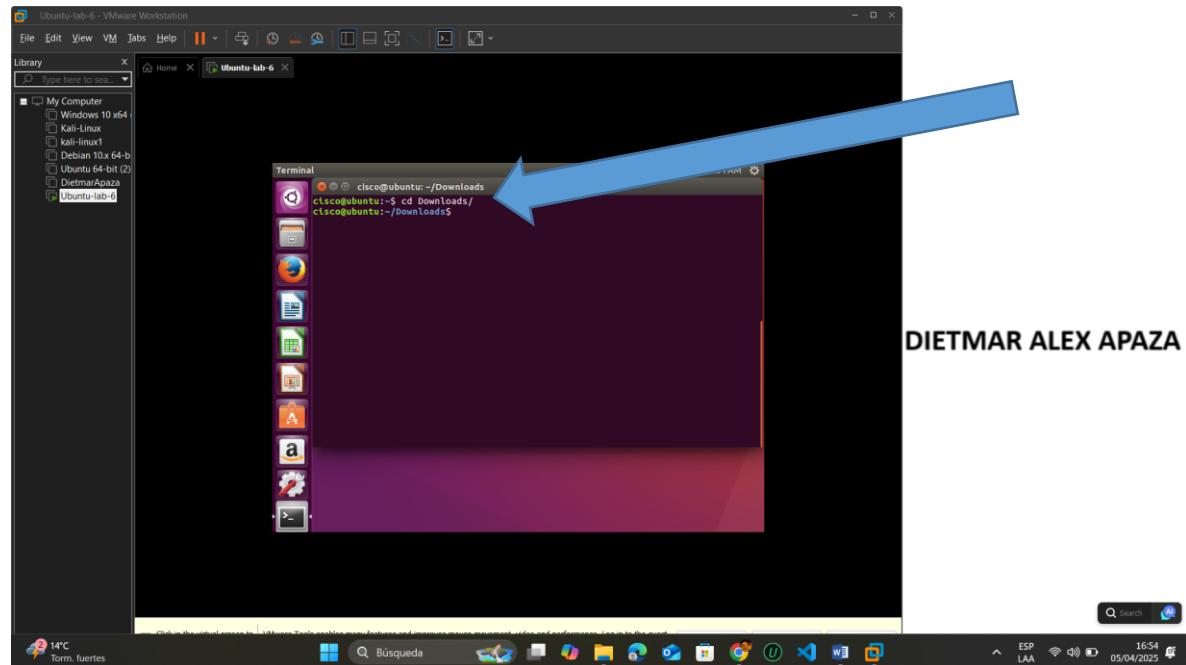
b. Haga clic en el icono de terminal para abrir un terminal.



## Paso 2: Ejecute Steghide.

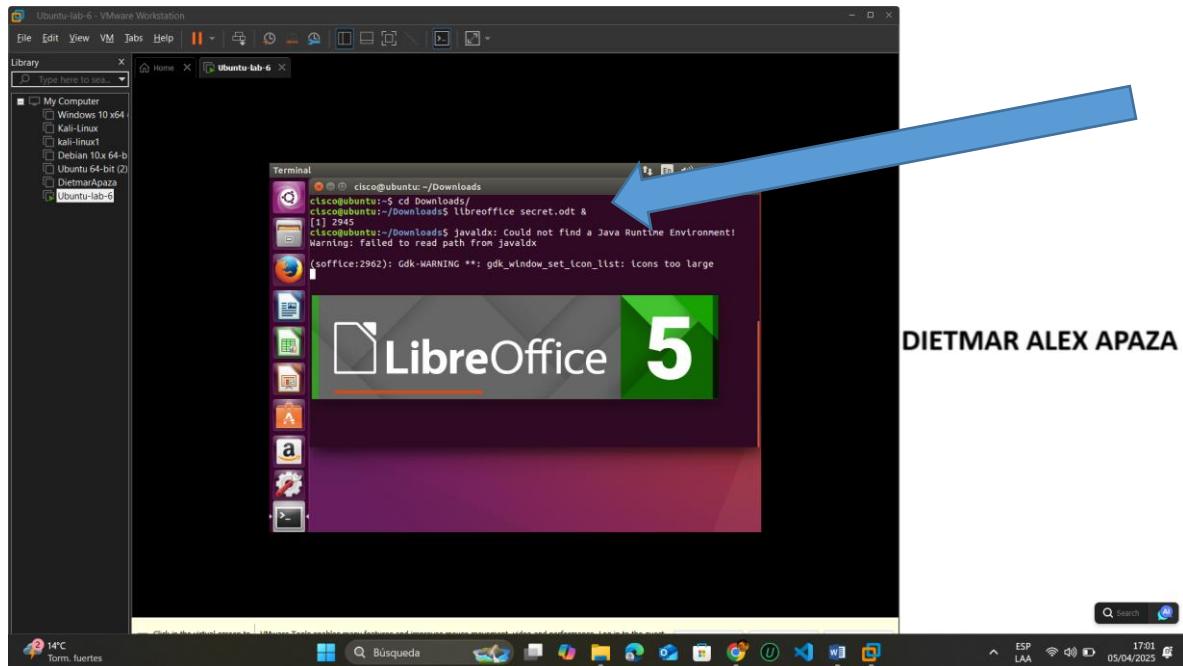
- En la petición de ingreso de comando, ingrese el siguiente comando para cambiar el directorio de descargas:

```
cisco@ubuntu:~$ cd Downloads/
```



- Introduzca **libreoffice secret.odt &** en la petición de ingreso.

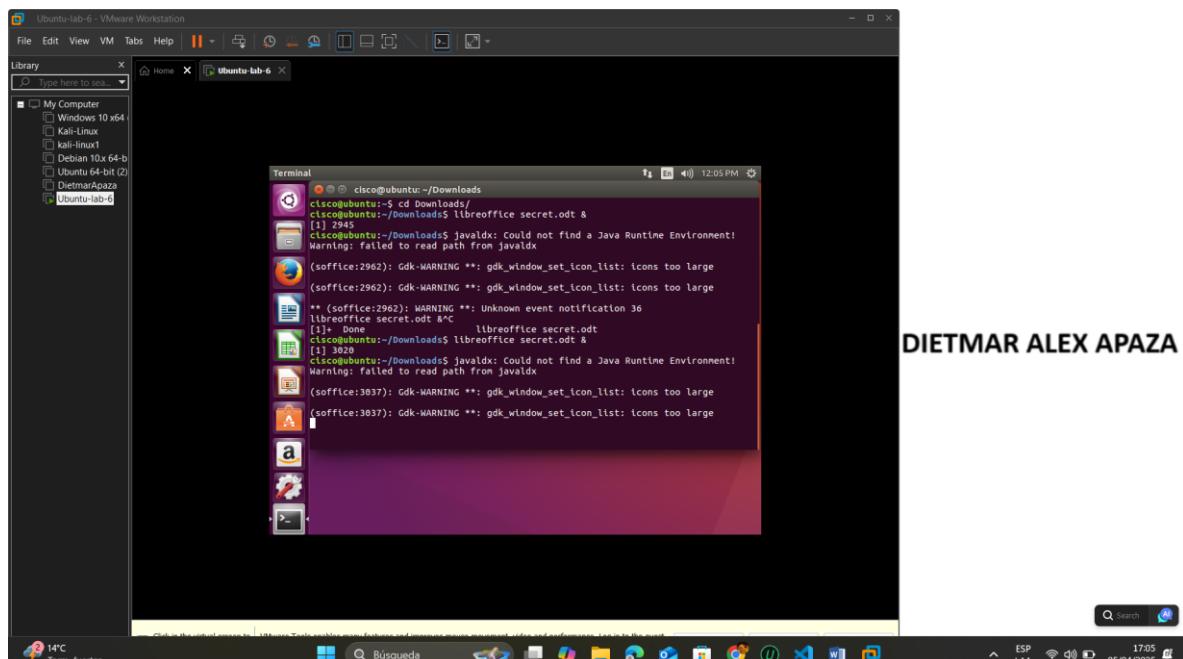
cisco@ubuntu:~/Downloads\$ libreoffice secret.odt &



¿Cuál es el mensaje en el archivo secret.odt?

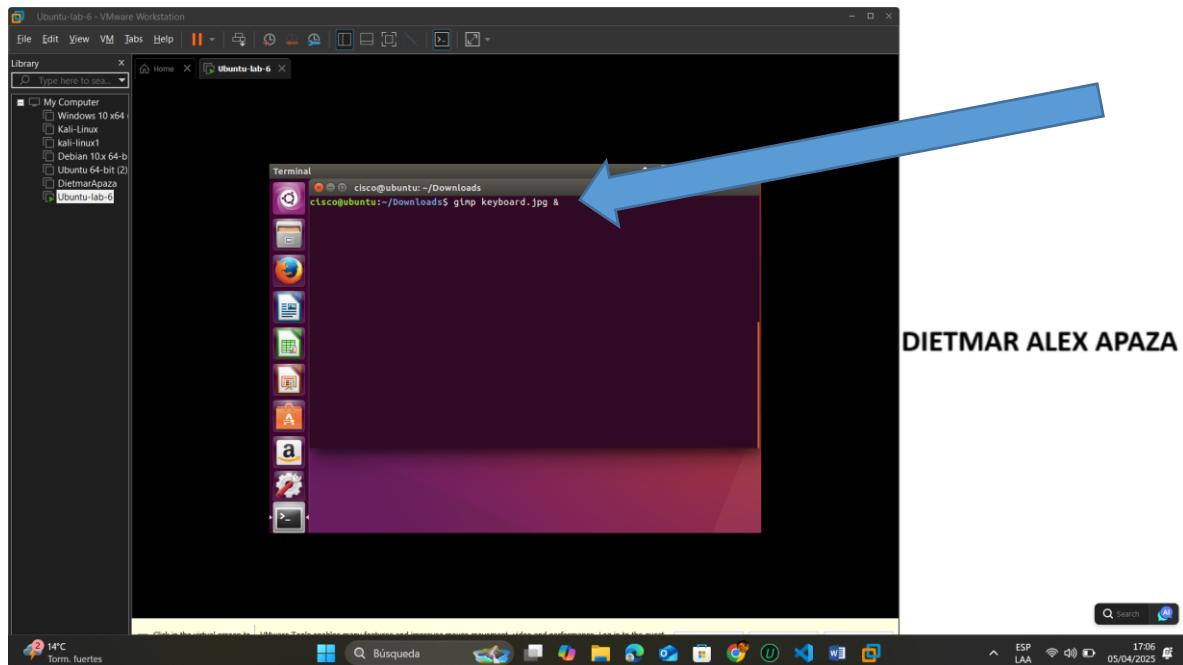
R.- The secret document

c. Cierre el archivo secret.odt cuando haya terminado.

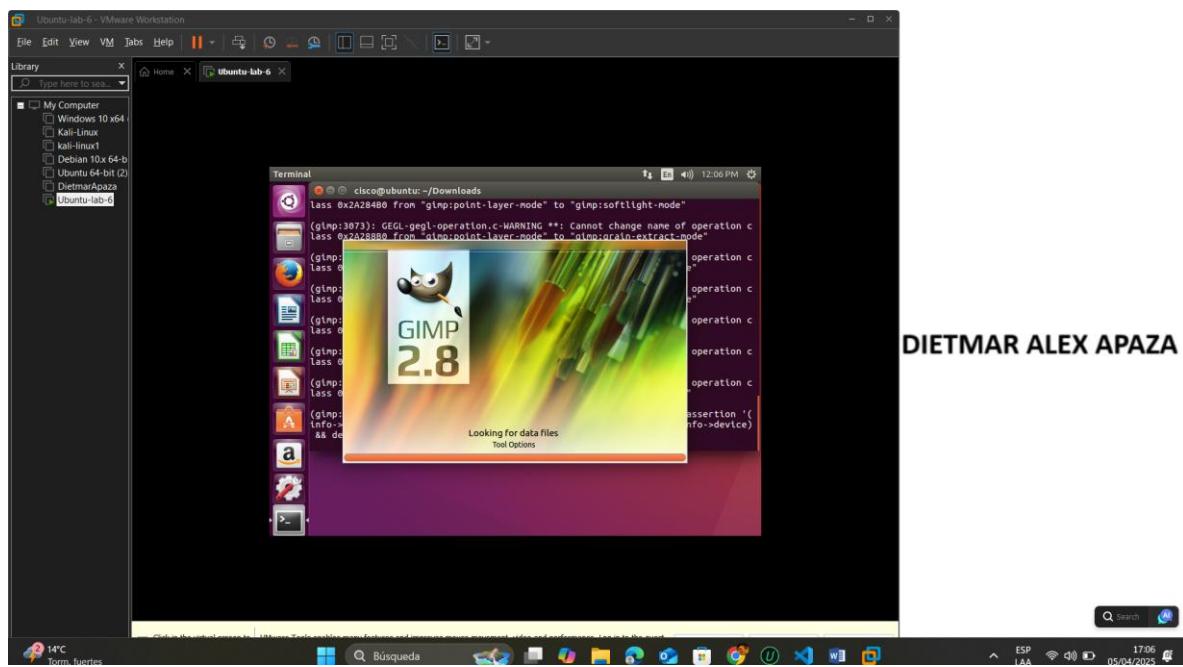


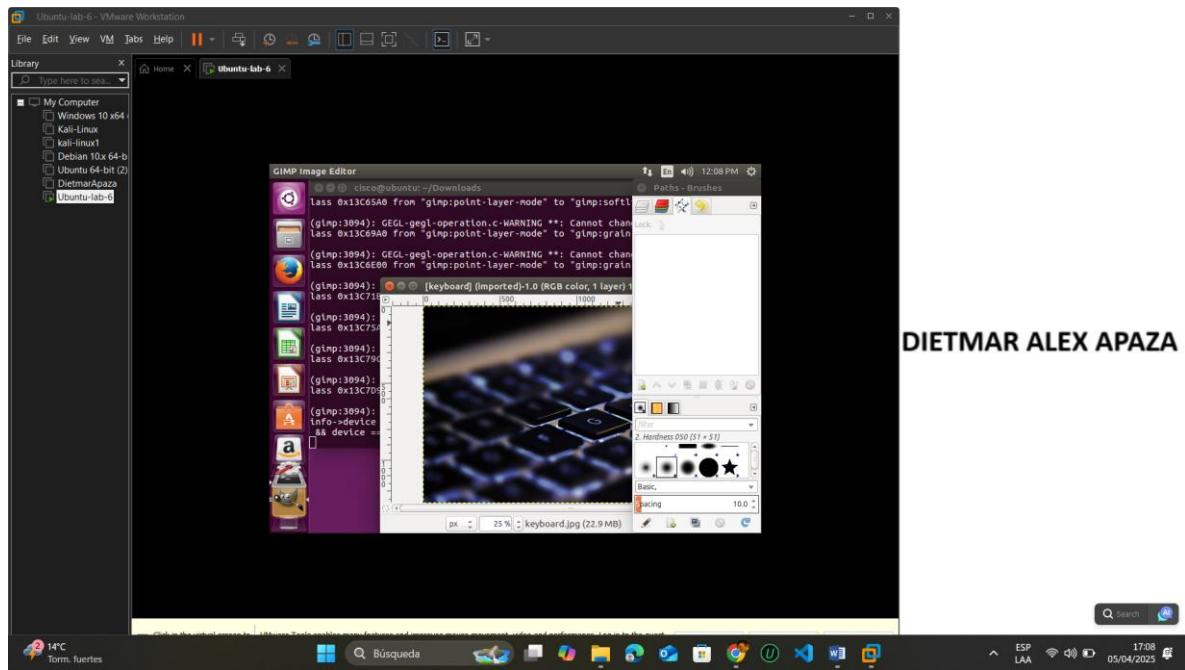
d. Introduzca gimp keyboard.jpg & en la petición de ingreso para ver el archivo de imagen

cisco@ubuntu:~/Downloads\$ gimp keyboard.jpg &

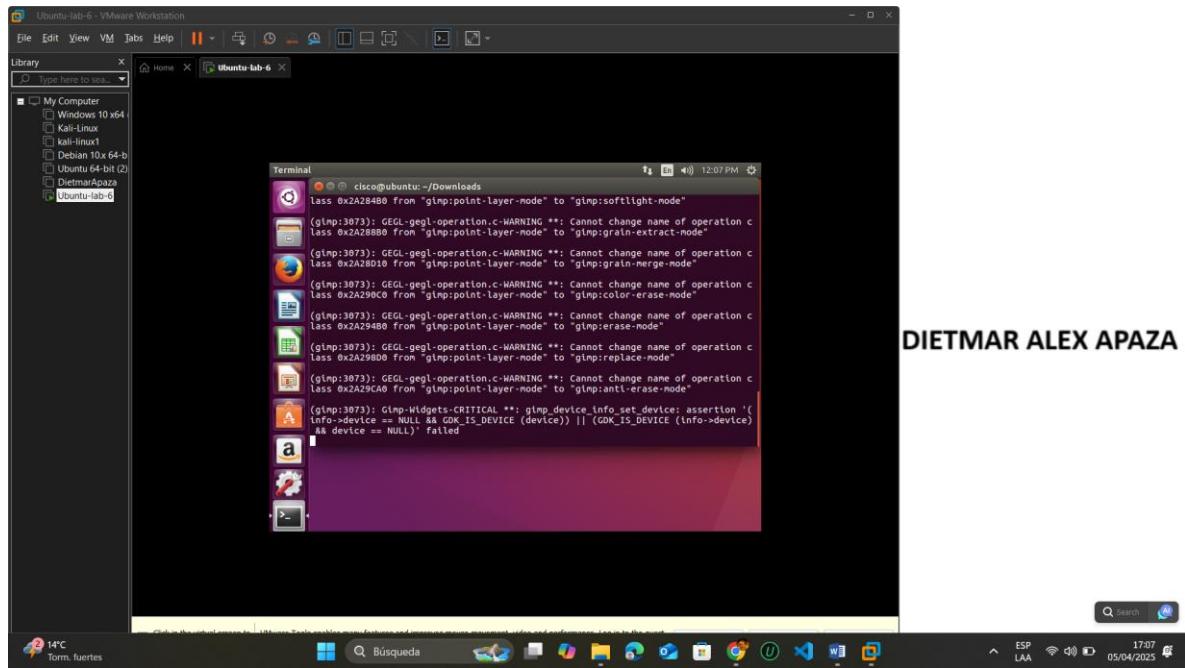


El comando abrirá la imagen que está en Download

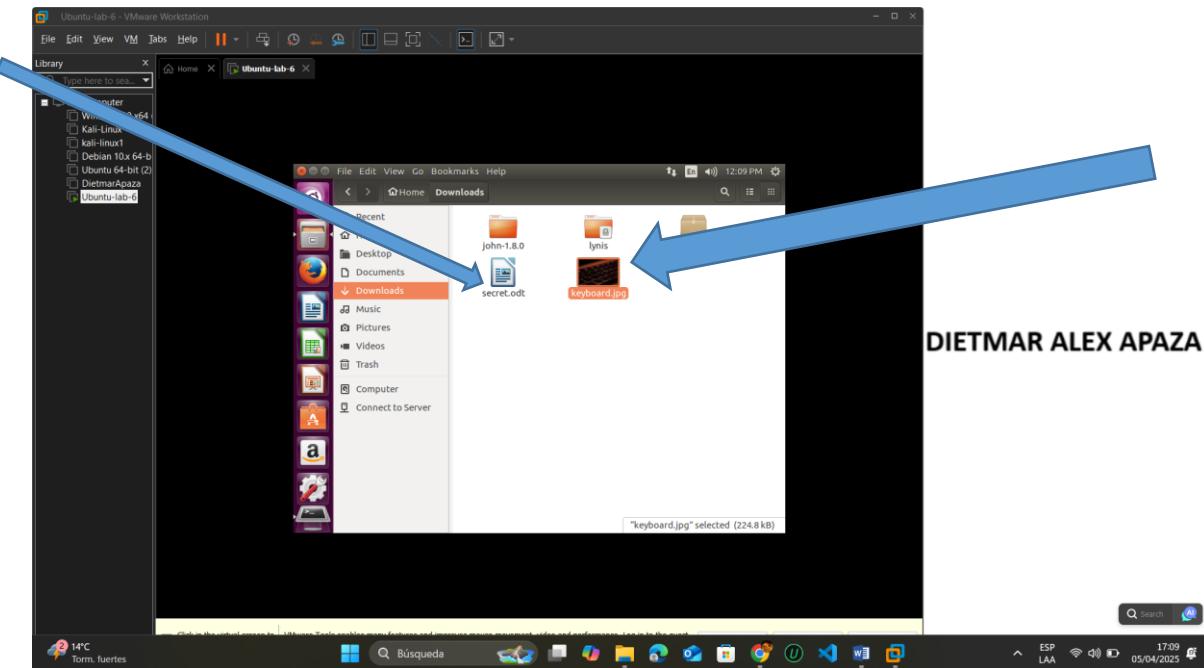




e. Cierre el archivo keyboard.jpg cuando haya terminado.

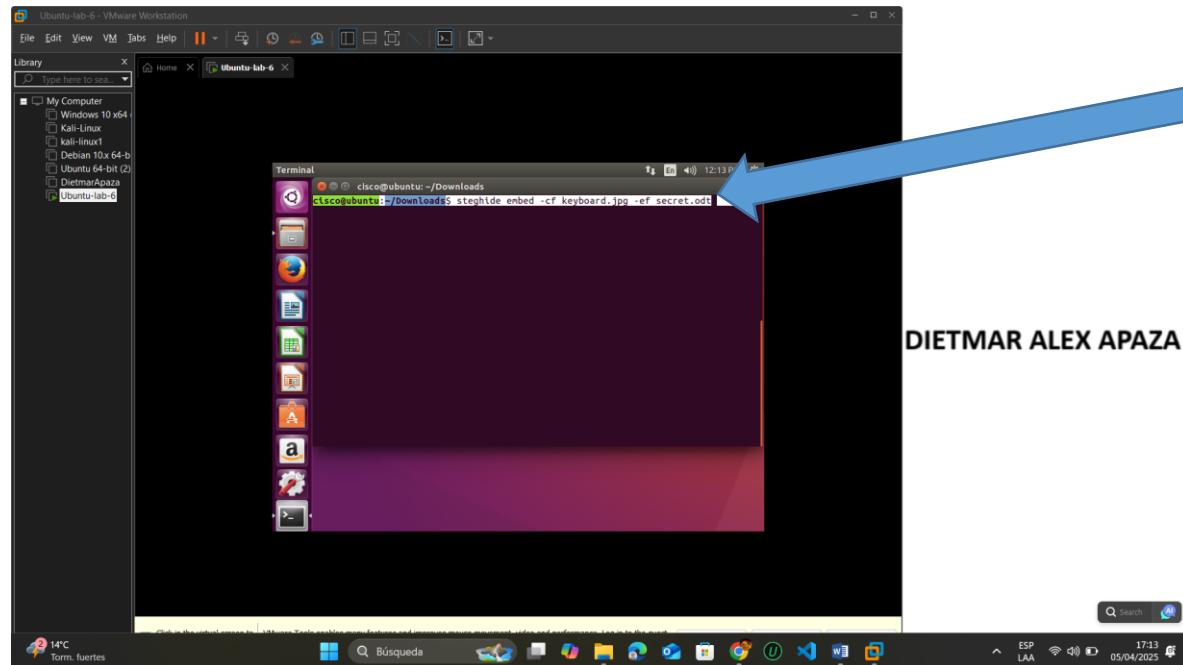


Puede visualizar estos archivos si ingresa a la carpeta Donwloads



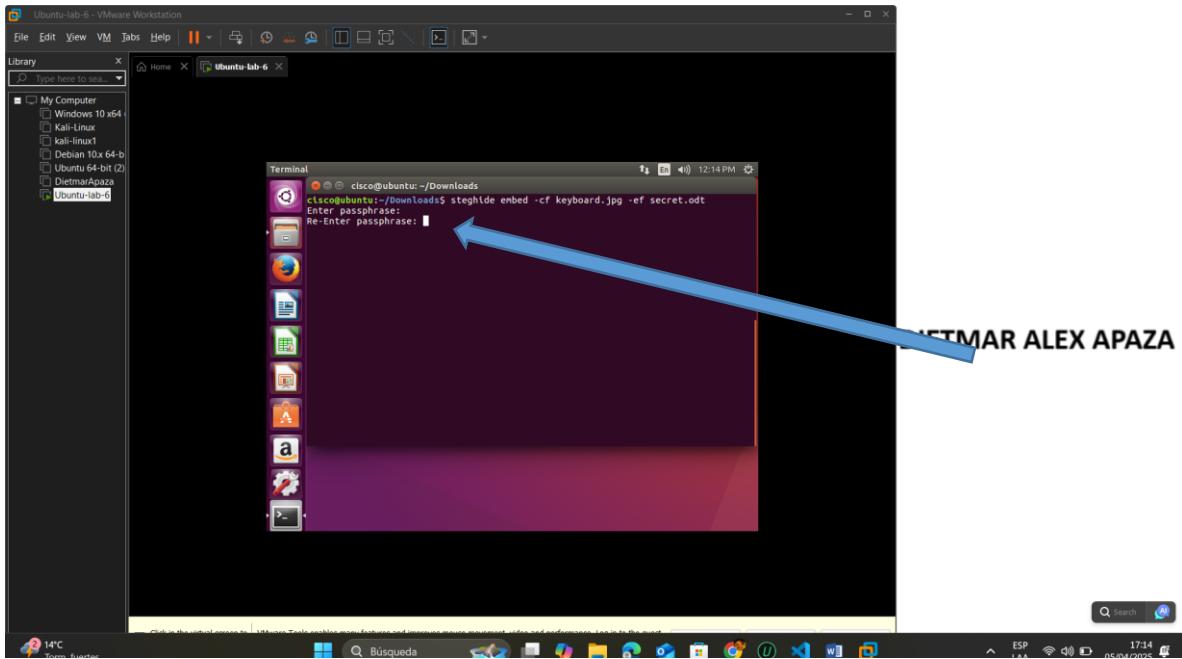
f. En la petición de ingreso de comando, introduzca el siguiente comando:

```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
```

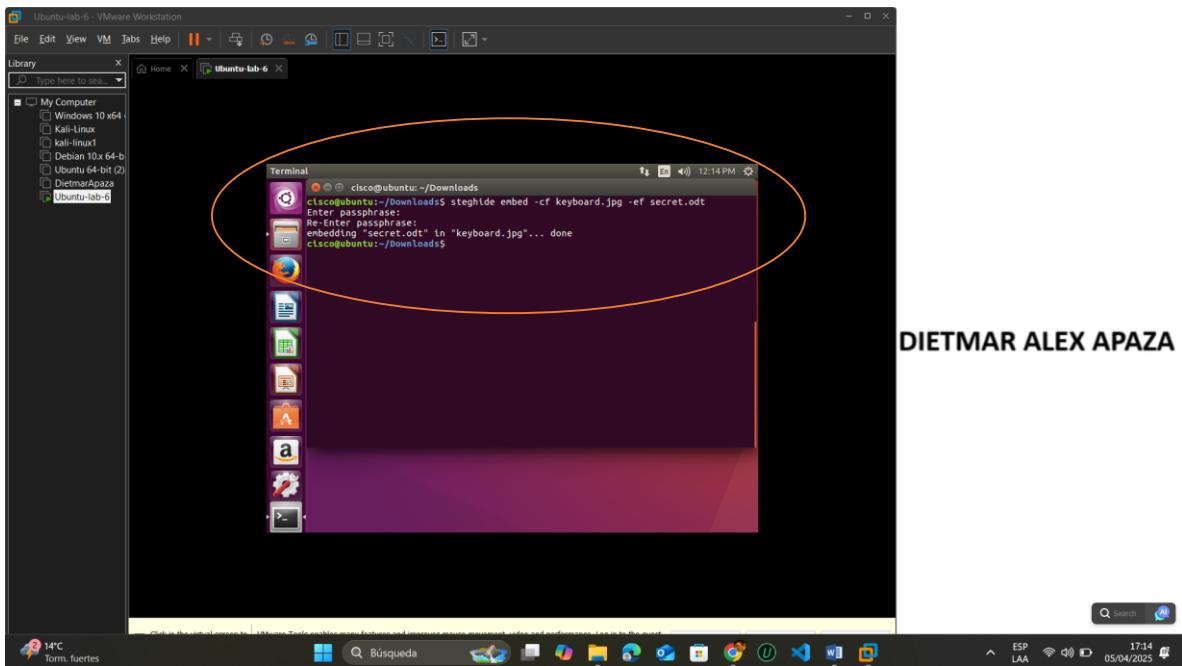


Este comando acepta el archivo JPEG llamado «keyboard.jpg» y lo utiliza como transportista para incorporar el documento, secret.odt en él.

g. Cuando se le solicite una contraseña, utilice **Cisco**. Reintroduzca la contraseña cuando se le solicite.



h. Ha incorporado el documento secret.odt, en el archivo de imagen, keyboard.jpg.



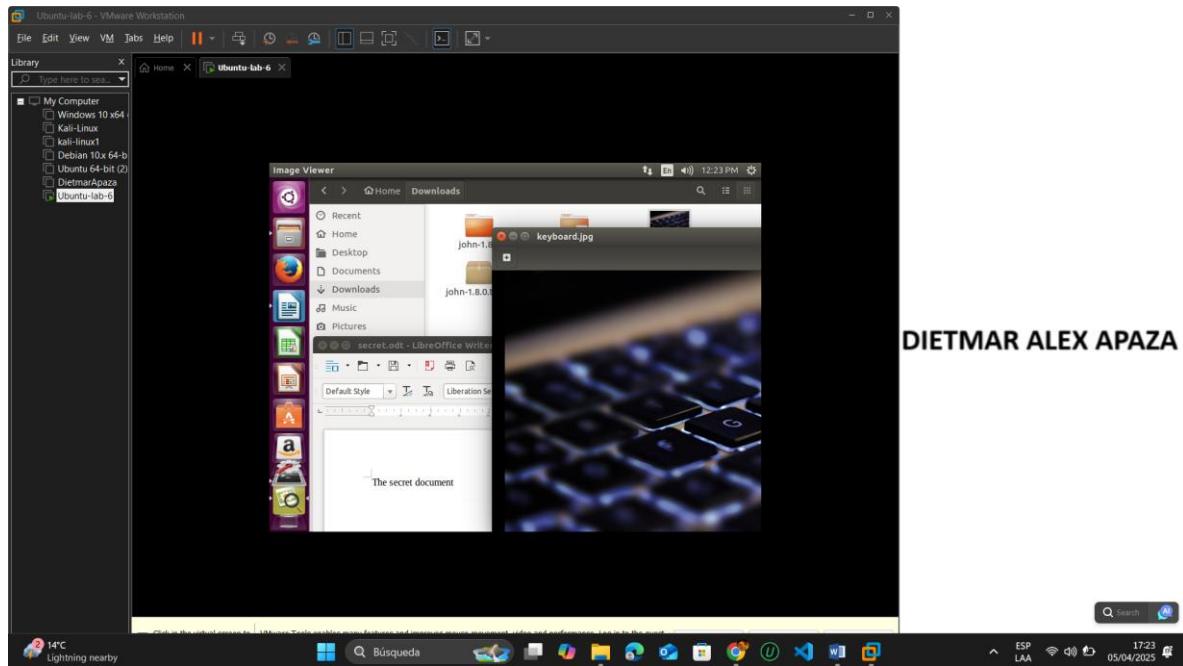
i. Abra los archivos secret.odt y keyboard.jpg. ¿Se modificaron estos archivos?

R.-

**secret.odt:** No se modificó visual ni estructuralmente.

**keyboard.jpg:** Sí fue modificado, pero el cambio es imperceptible visualmente.

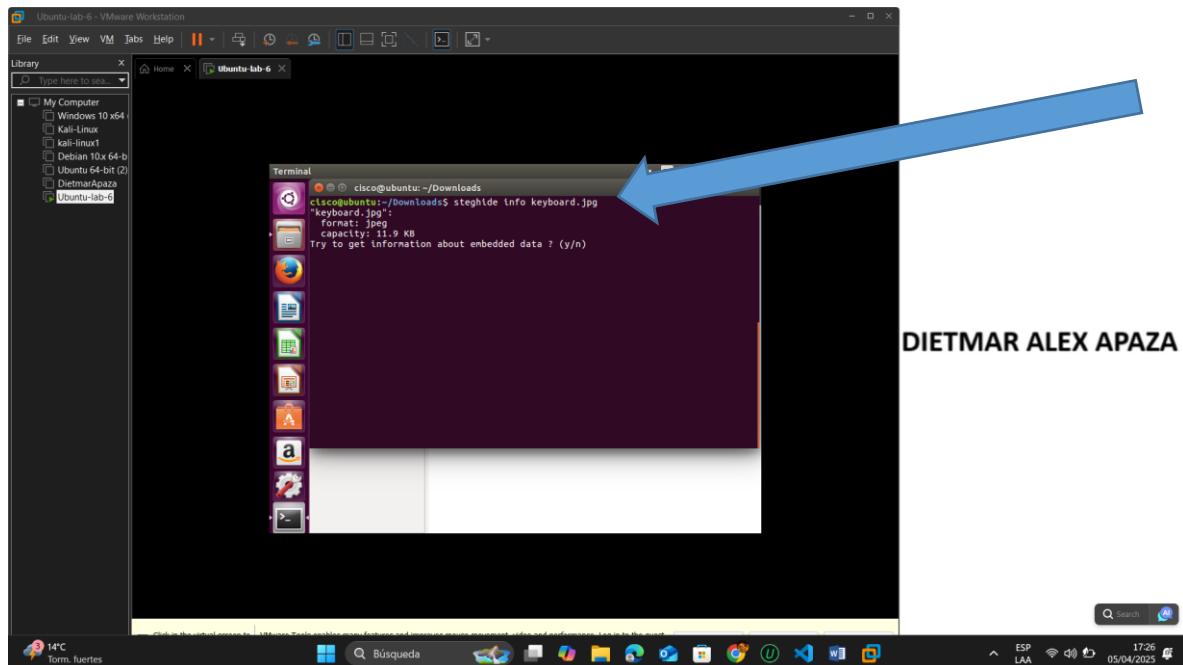
Puede abrirlos mediante comandos o también desde la carpeta Downloads



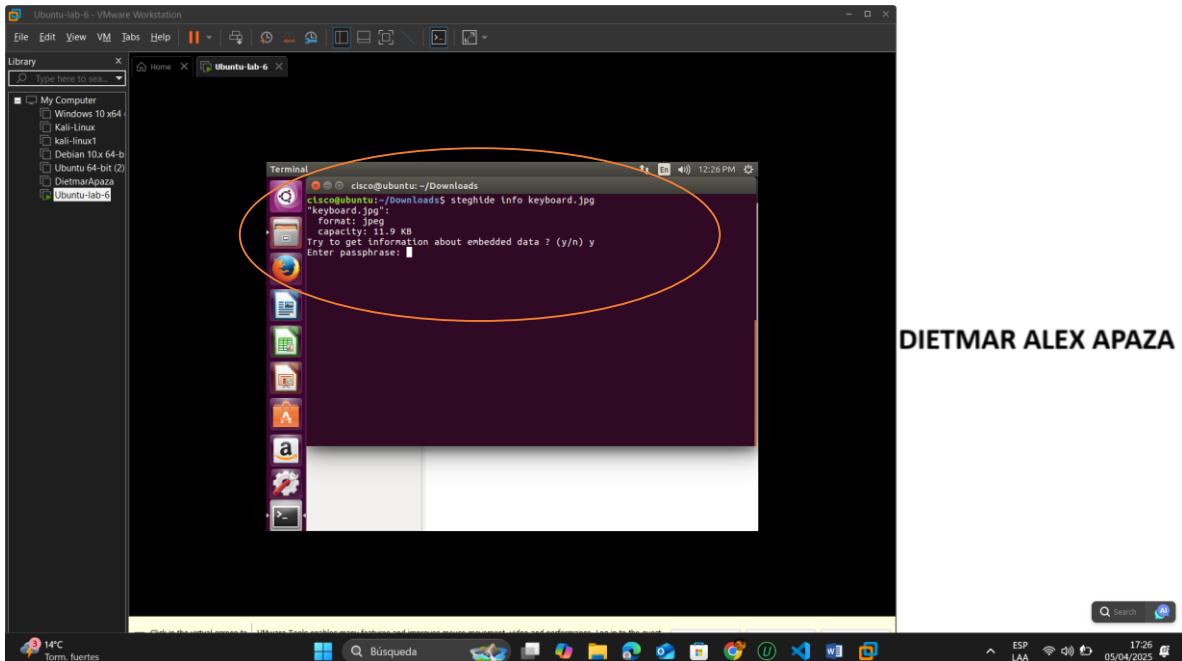
**Paso 3:** Verifique el archivo oculto.

- a. Escriba el siguiente comando en el terminal.

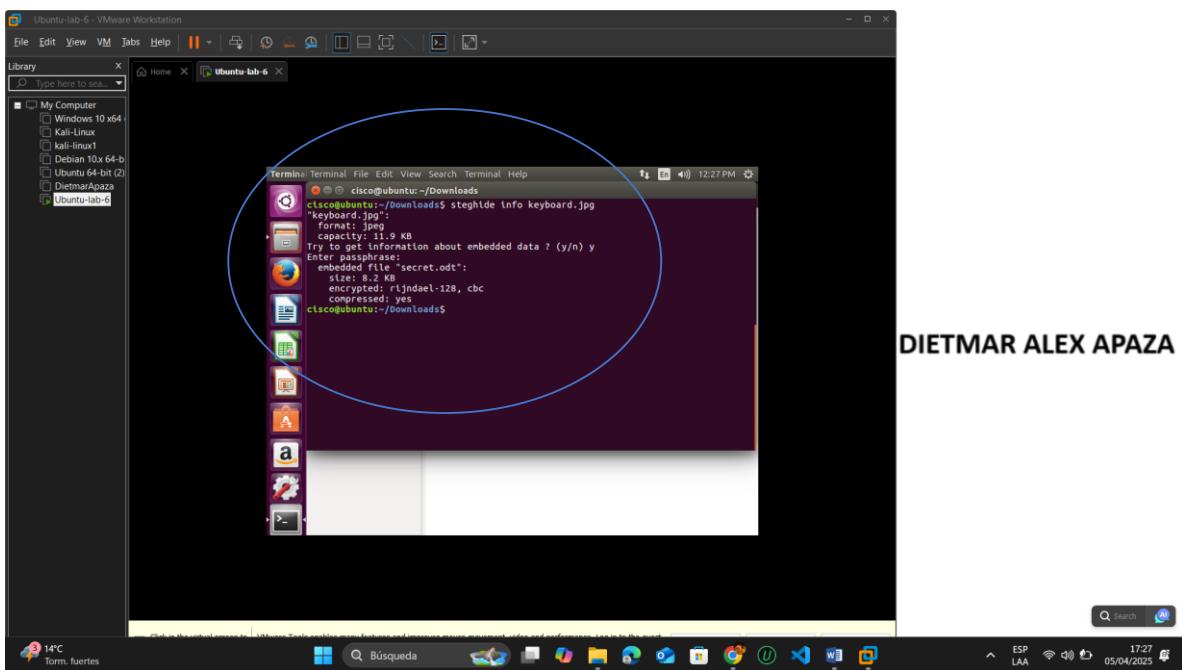
cisco@ubuntu:~/Downloads\$ **steghide info keyboard.jpg**



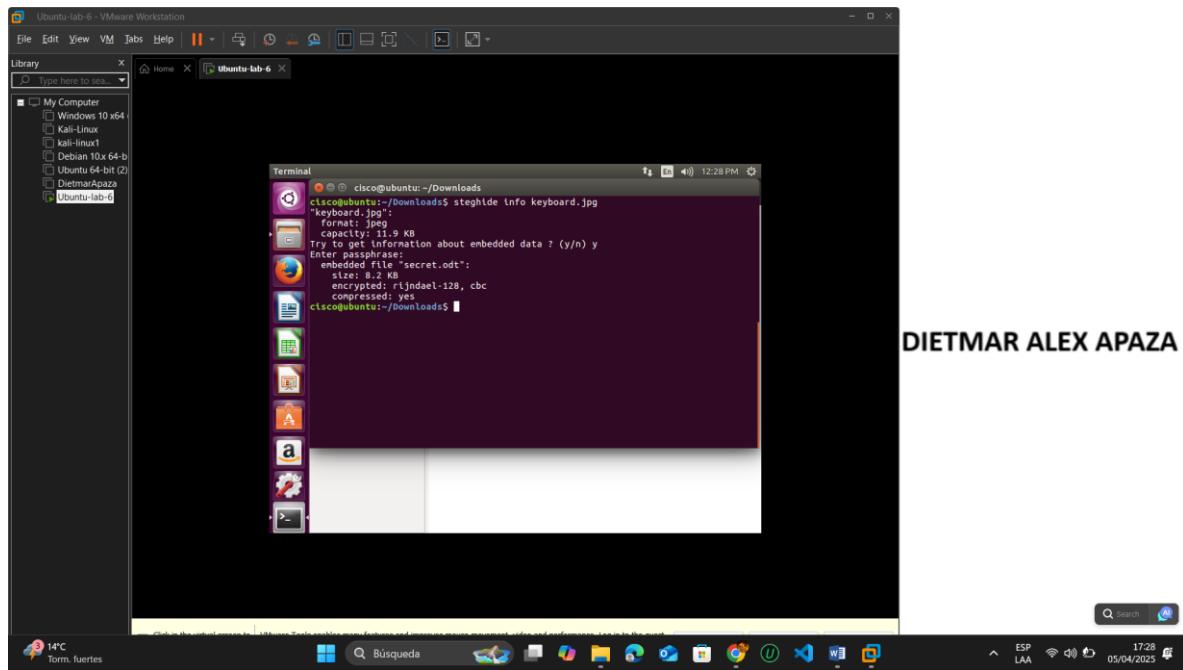
- b. Escriba y en la petición de ingreso. (No presione Intro).



c. Introduzca la contraseña Cisco y presione Intro.

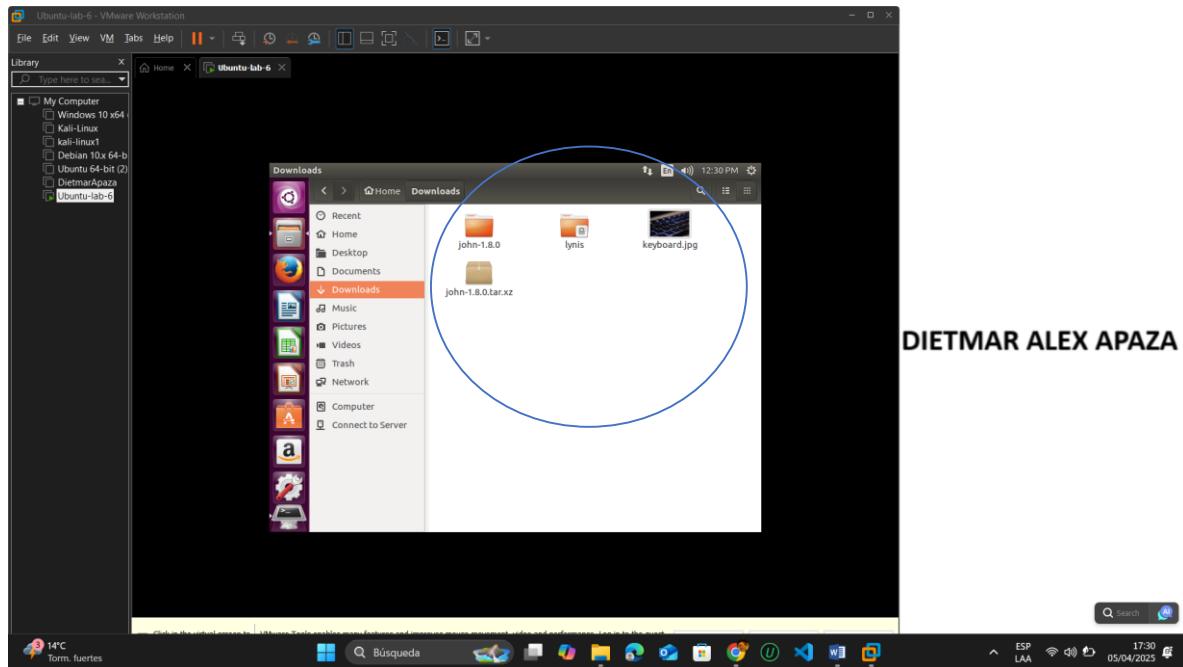


d. Los resultados a continuación muestran que el archivo, secret.odt, está cifrado y comprimido.



DIETMAR ALEX APAZA

Elimine el archivo secret.odt , esto representa que únicamente ahora cuenta con la imagen y dentro de ella el archivo que oculta.

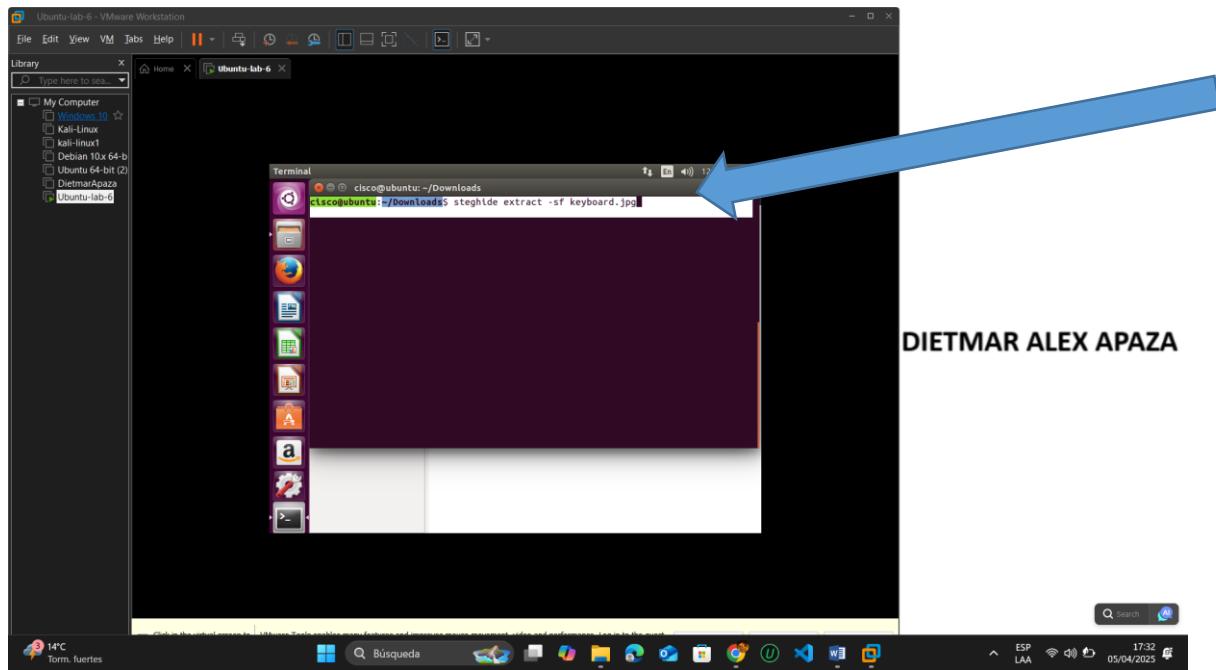


DIETMAR ALEX APAZA

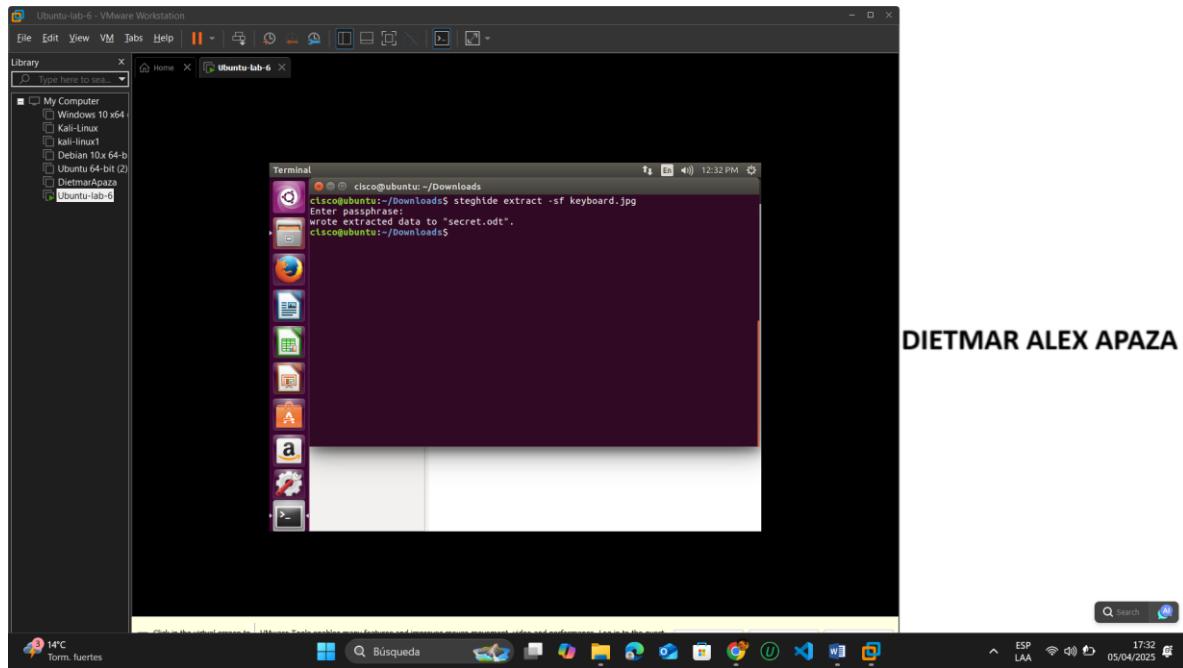
**Paso 4:** Extraiga el archivo oculto.

a. Escriba el siguiente comando en el terminal.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```



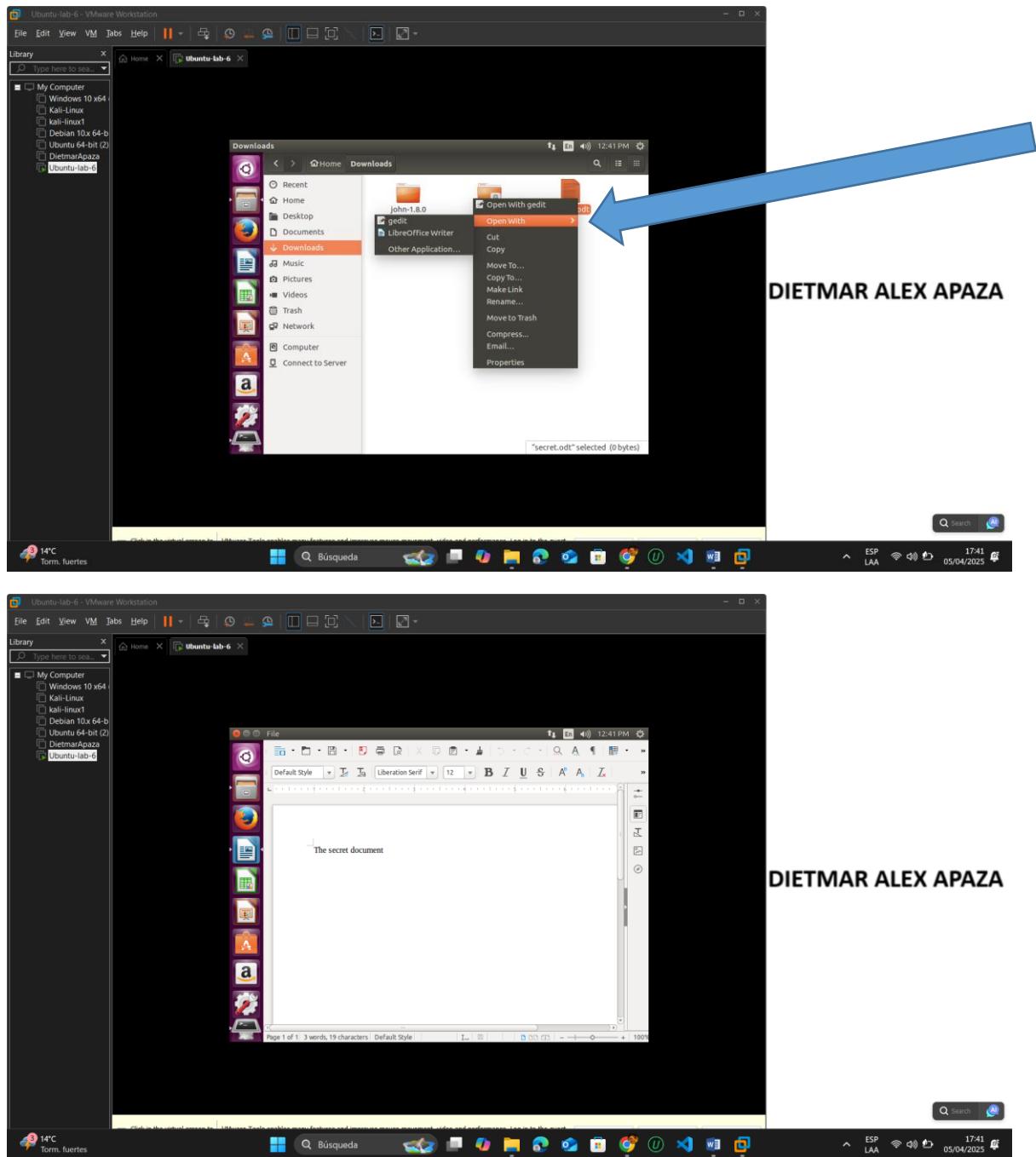
b. Introduzca la contraseña Cisco y presione Intro.



c. Introduzca y , el archivo secret.odt será extraído nuevamente de la imagen que lo transporta.

d. Ha extraído el archivo. Abra el archivo extraído secret.odt con LibreOffice.

¿Podría abrir el archivo desde la imagen?



¿El mensaje secreto es el mismo que antes?

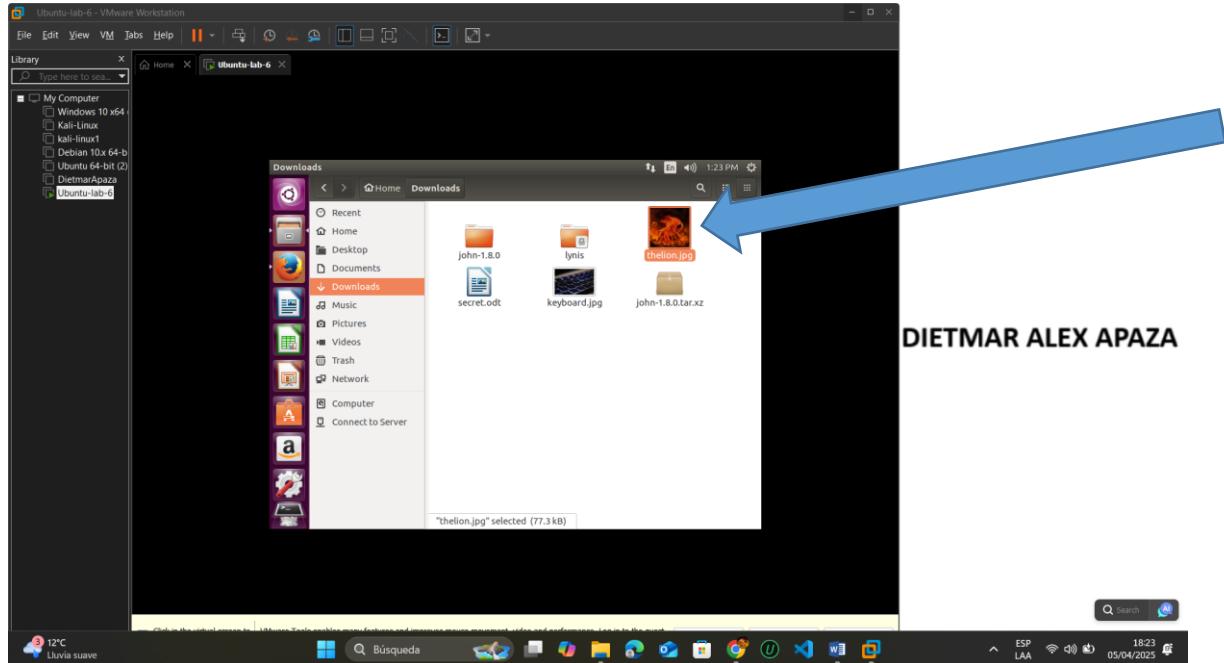
R.- Sí, el contenido del archivo `secret.odt` no cambia durante el proceso.

Aunque esté comprimido y cifrado dentro de la imagen, al ser extraído correctamente, su contenido es idéntico al original.

# EVALUACIÓN

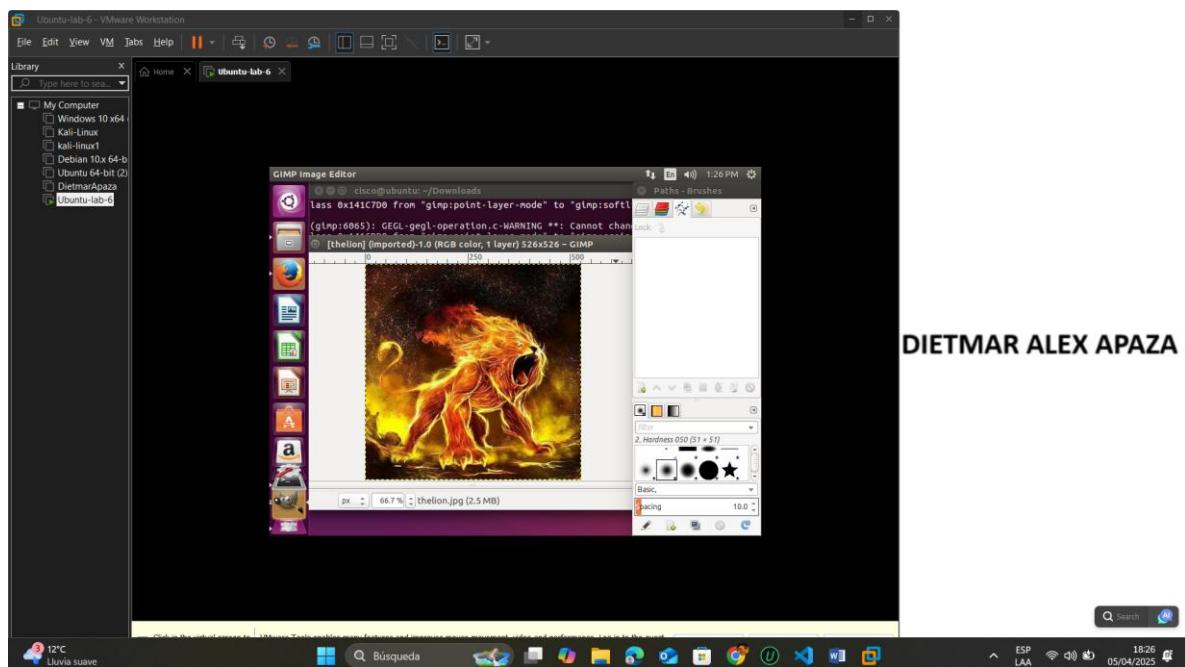
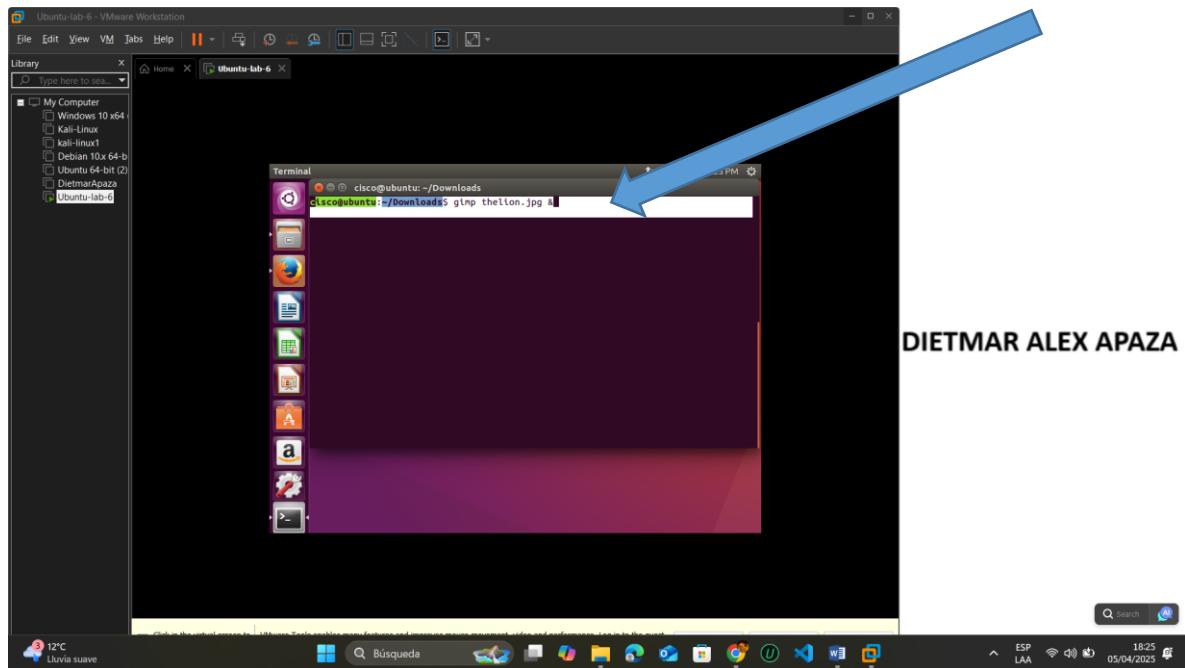
1.- Copie una imagen nueva a la pc con ubuntu y adjunte a ella un archivo de texto en el que estará su nombre completo y CI, use como contraseña sistemas2024s2 y muestre que la extracción funciona. (Deberá hacer capturas de todo este proceso)

- Descargamos una imagen de la web con el nombre de “thelion.jpg”



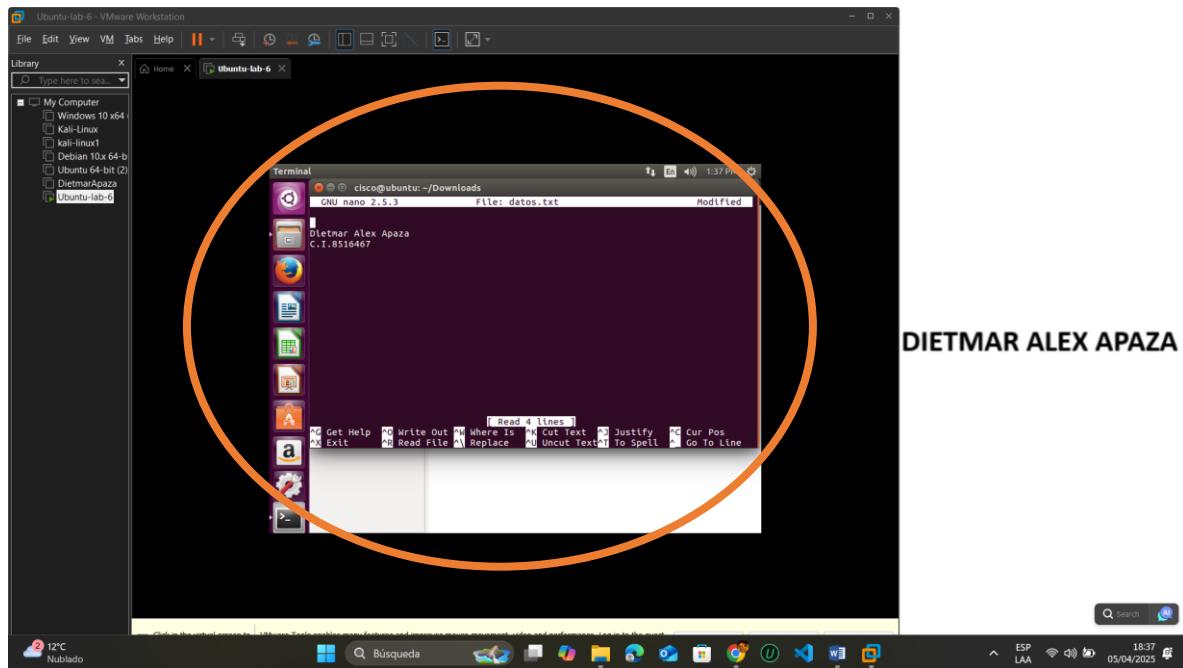
Introduzca **gimp thelion.jpg &** en la petición de ingreso para ver el archivo de imagen

cisco@ubuntu:~/Downloads\$ **gimp thelion.jpg &**

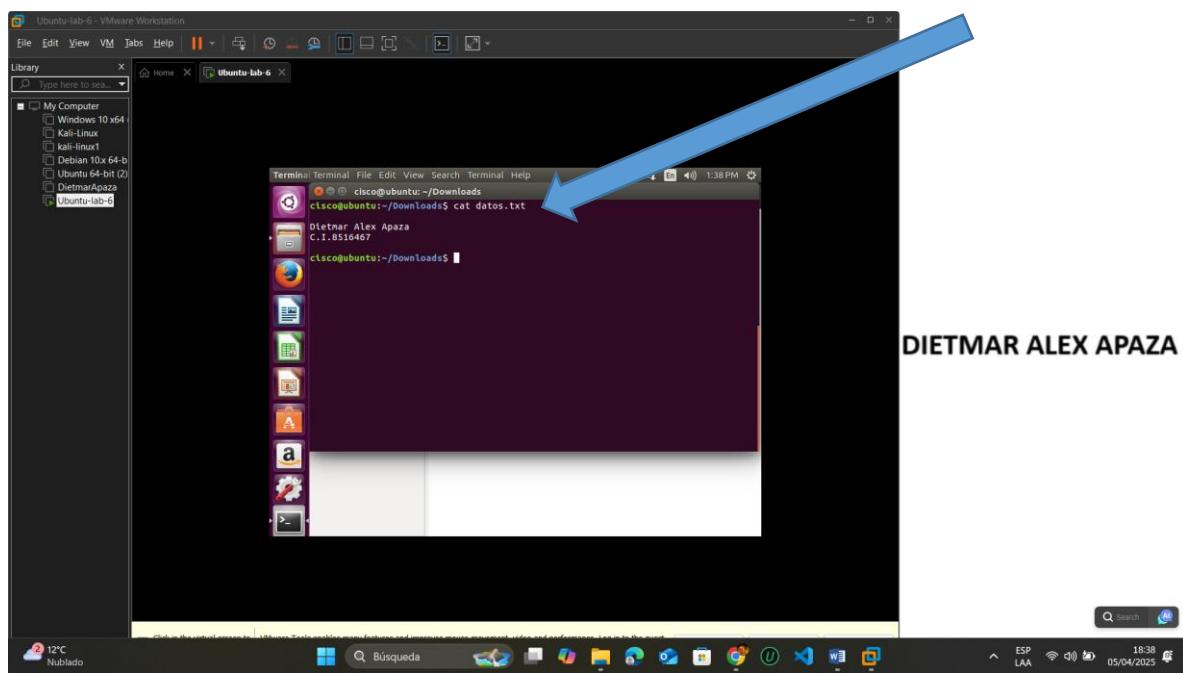


Creamos un archivo.txt con el el siguiente comando: nano datos.txt

Dentro del archivo ingresamos nuestro nombre completo y C.I.



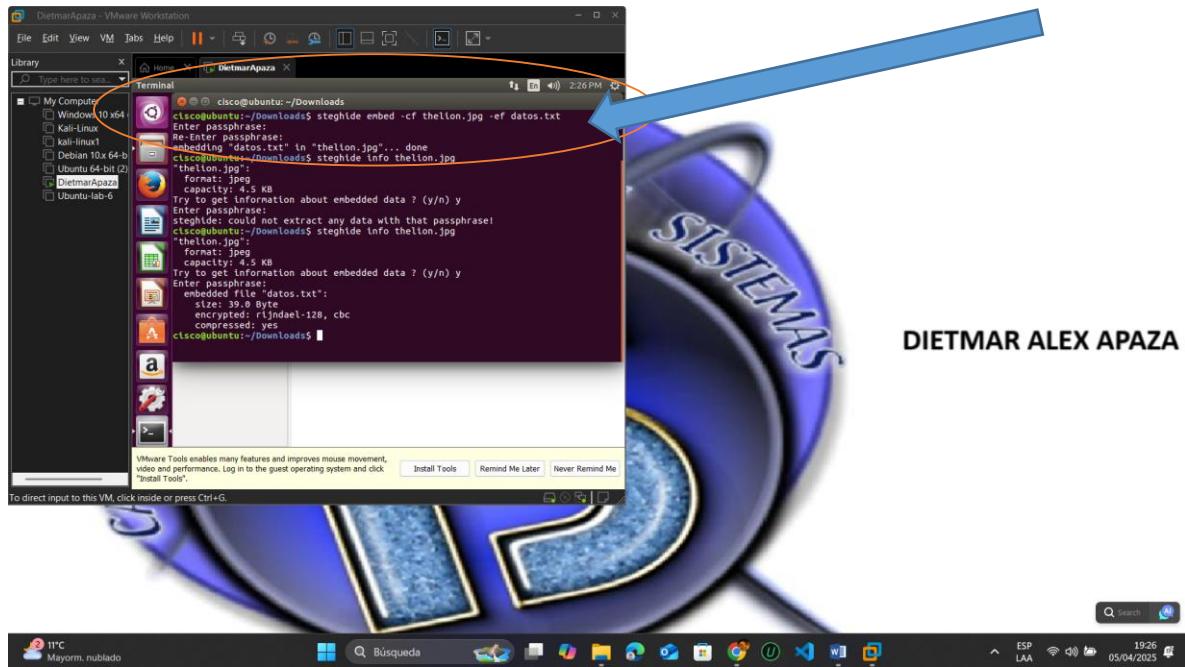
Para verificar ingresamos el código de: cat datos.txt



En la petición de ingreso de comando, introduzca el siguiente comando:

```
cisco@ubuntu:~/Downloads$ steghide embed -cf thelion.jpg -ef datos.txt
```

Cuando se le solicite una contraseña, la contraseña será: **sistemas2024s2**. Reintroduzca la contraseña cuando se le solicite.



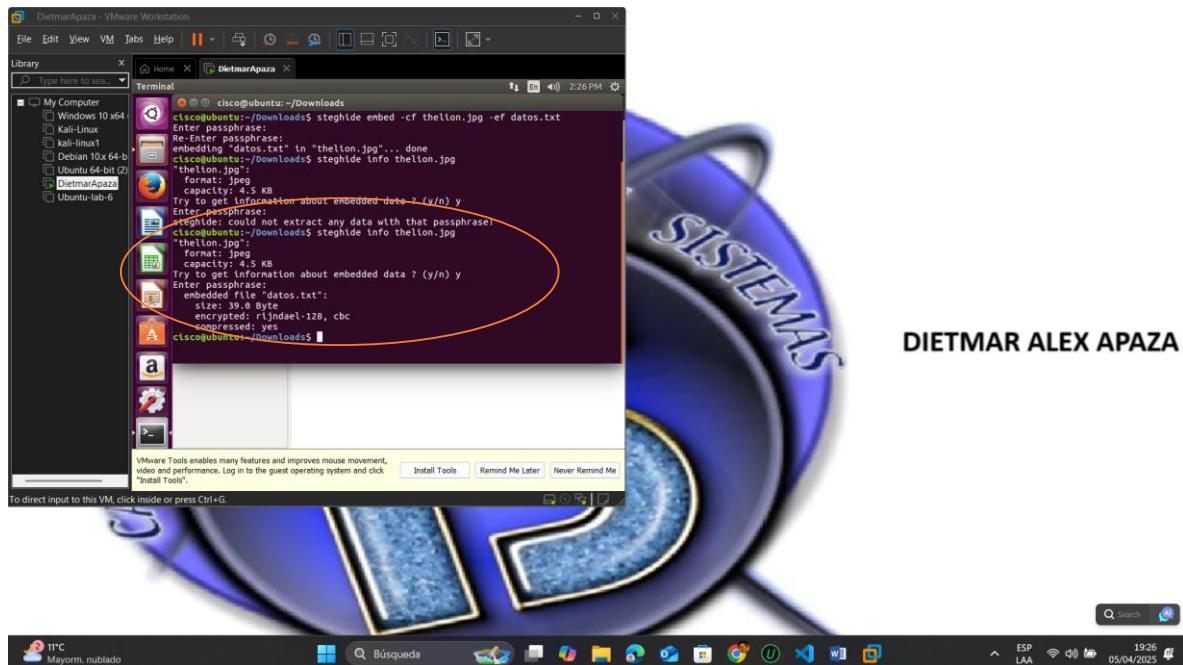
## Verificar el archivo oculto.

Escriba el siguiente comando en el terminal.

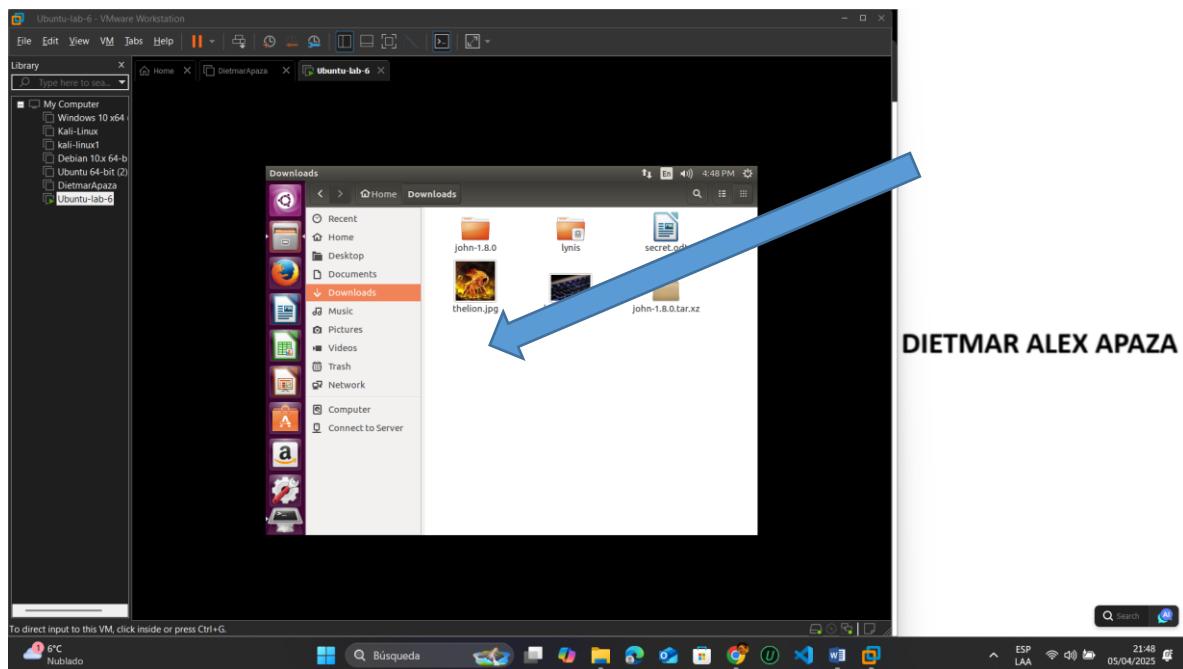
```
cisco@ubuntu:~/Downloads$ steghide info thelion.jpg
```

Escriba y en la petición de ingreso. (No presione Intro).

La contraseña será **sistemas2024s2**



Elimine el archivo **datos.txt**, esto representa que únicamente ahora cuenta con la imagen y dentro de ella el archivo que oculta.



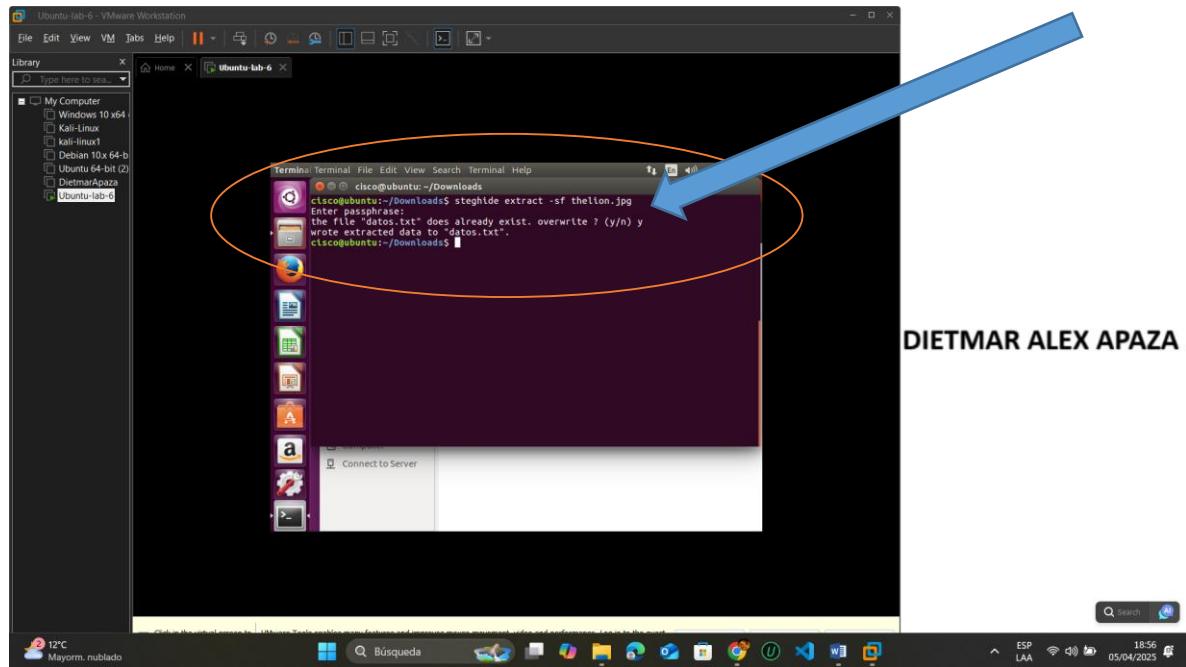
### Extraiga el archivo oculto.

Escriba el siguiente comando en el terminal.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf thelion.jpg
```

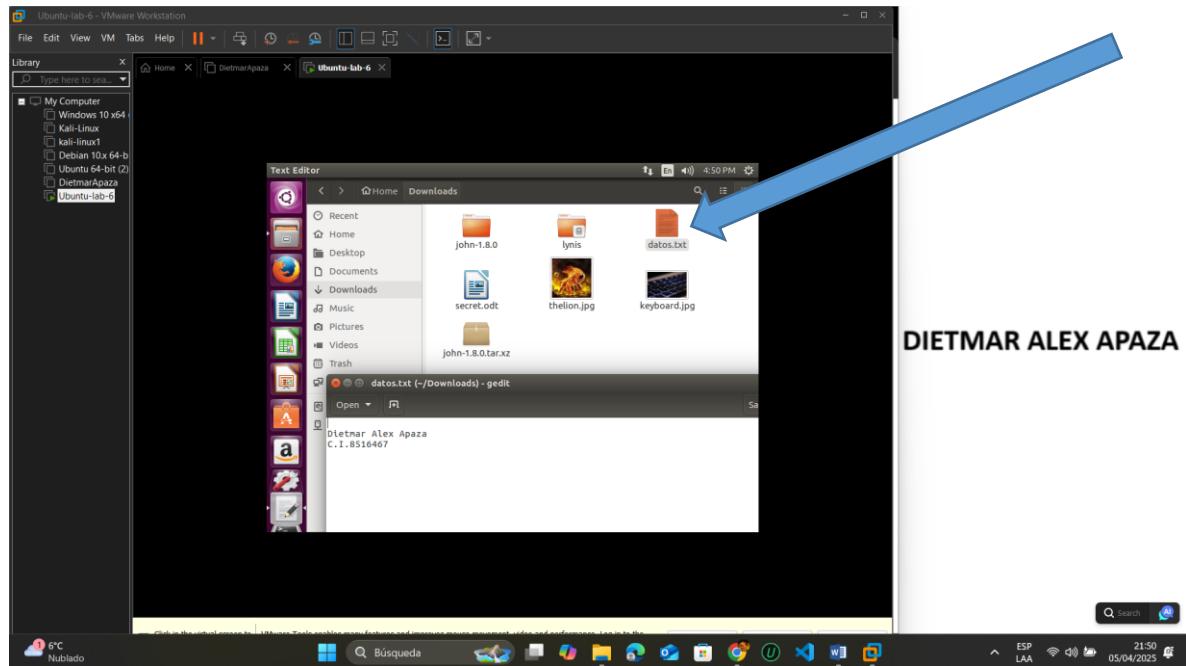
Ingresamos la contraseña: **sistemas204s2**

Introduzca y , el archivo secret.odt será extraído nuevamente de la imagen que lo transporta.



Una vez extraído el archivo. Abrir el archivo extraído datos.txt.

Como se ve en la imagen se extrajo correctamente y muestra toda la información que guardamos en el archivo.



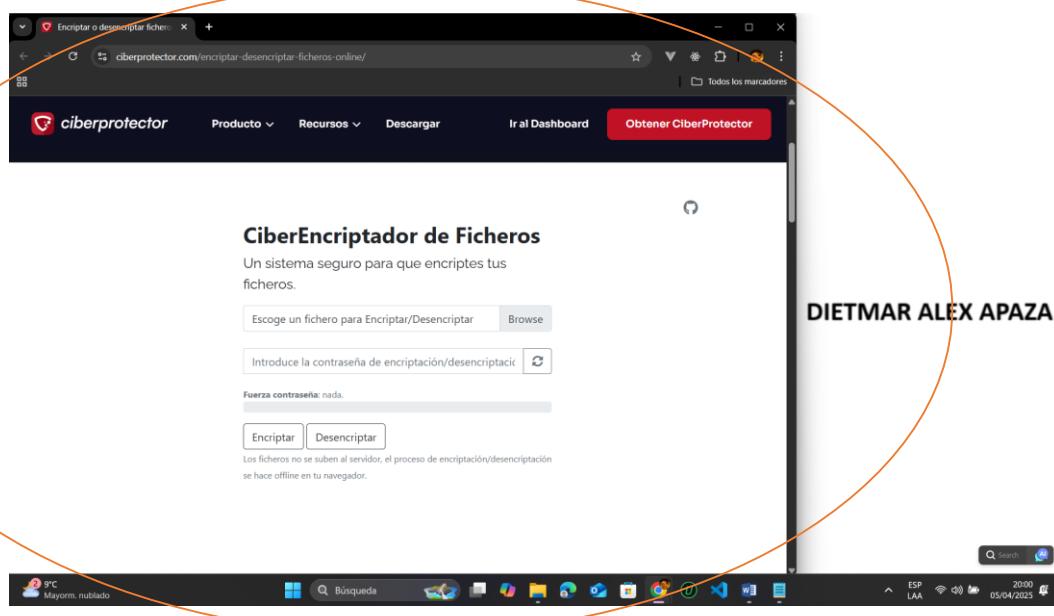
**2.- Realice la demostración para cifrar/descrifrar un archivo, un mensaje en texto plano y la esteganografía a una imagen. Utilice las siguientes webs para ello**

**1.- Encriptar y desencriptar archivos**

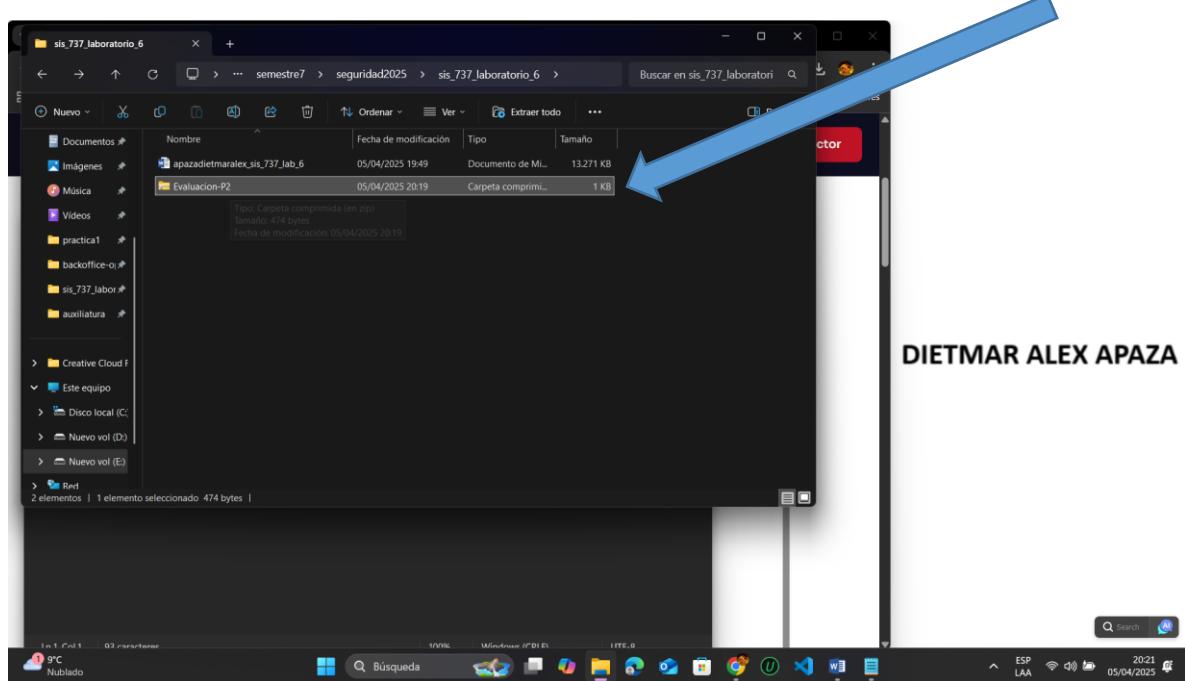
<https://ciberprotector.com/encriptar-desencriptar-ficheros-online/>

**Encriptar archivo**

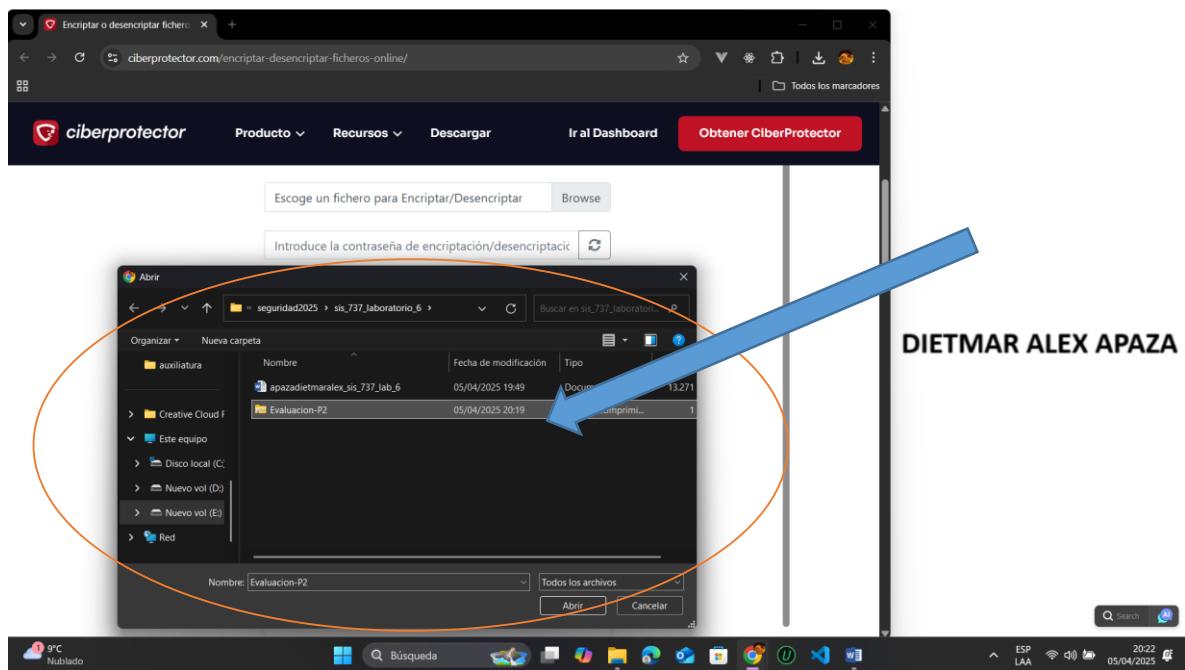
Ingresamos al link para realizar la encriptación de un archivo



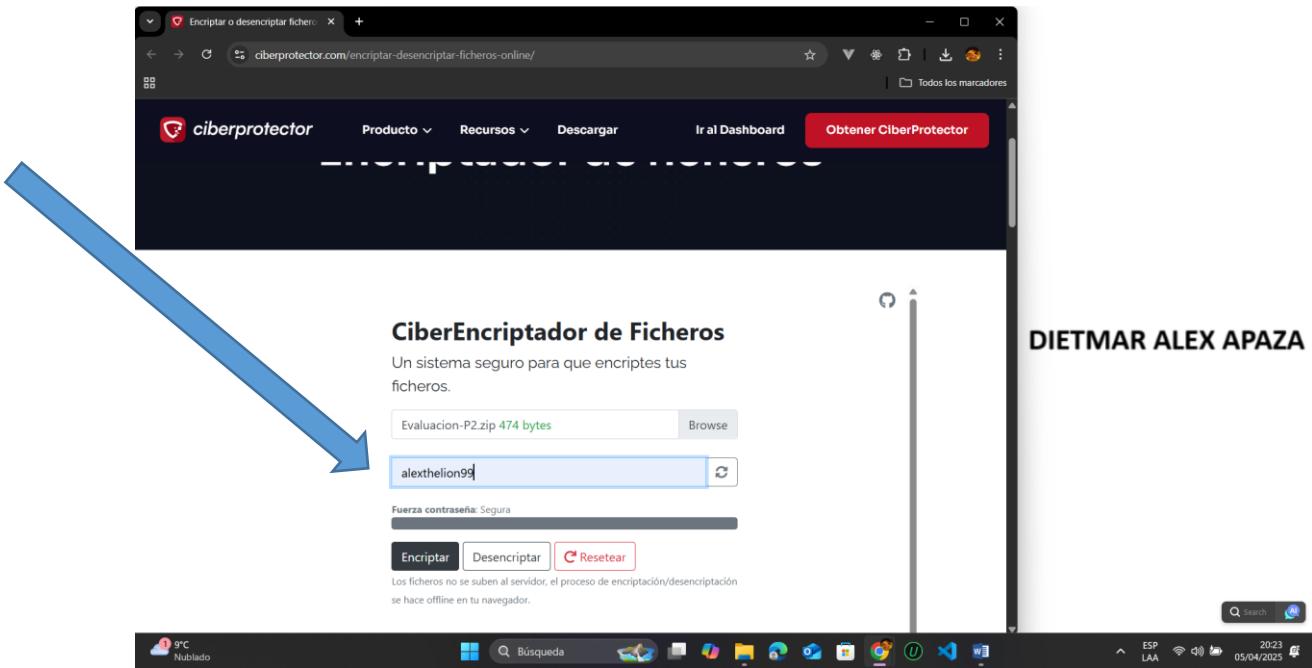
Creamos un archivo llamado “Evaluacion-P2” y lo convertimos en un archivo.ZIP dentro del archivo se encontrara documentos que deseamos encriptar.



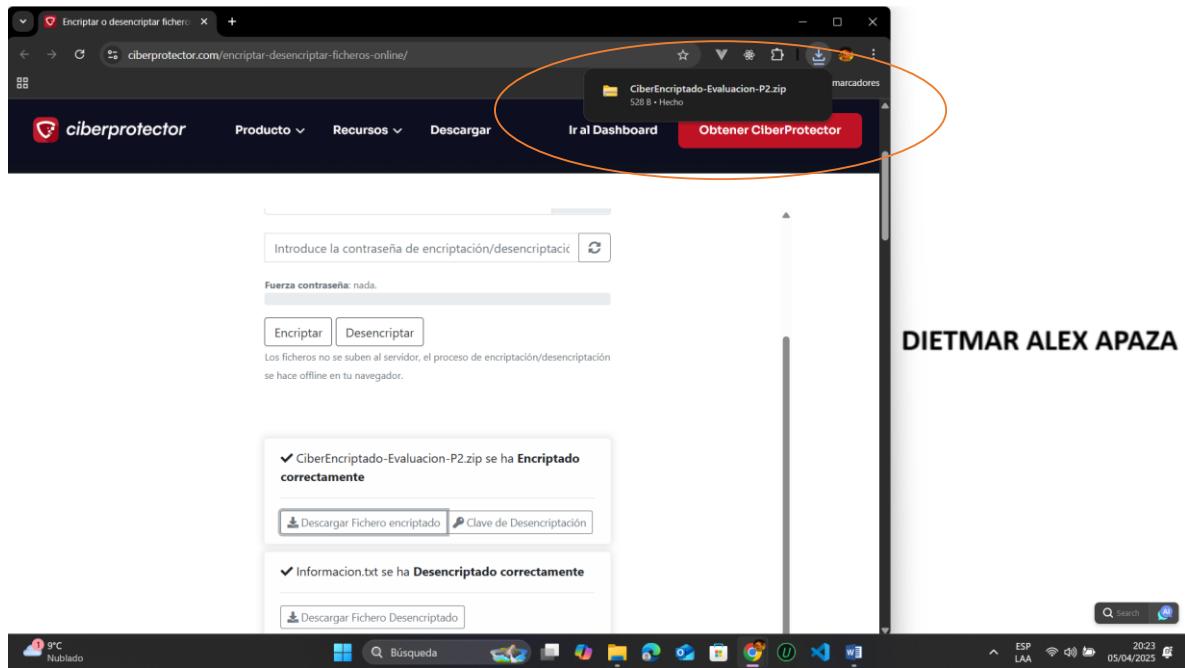
Sube el archivo Evaluacion-P2.ZIP



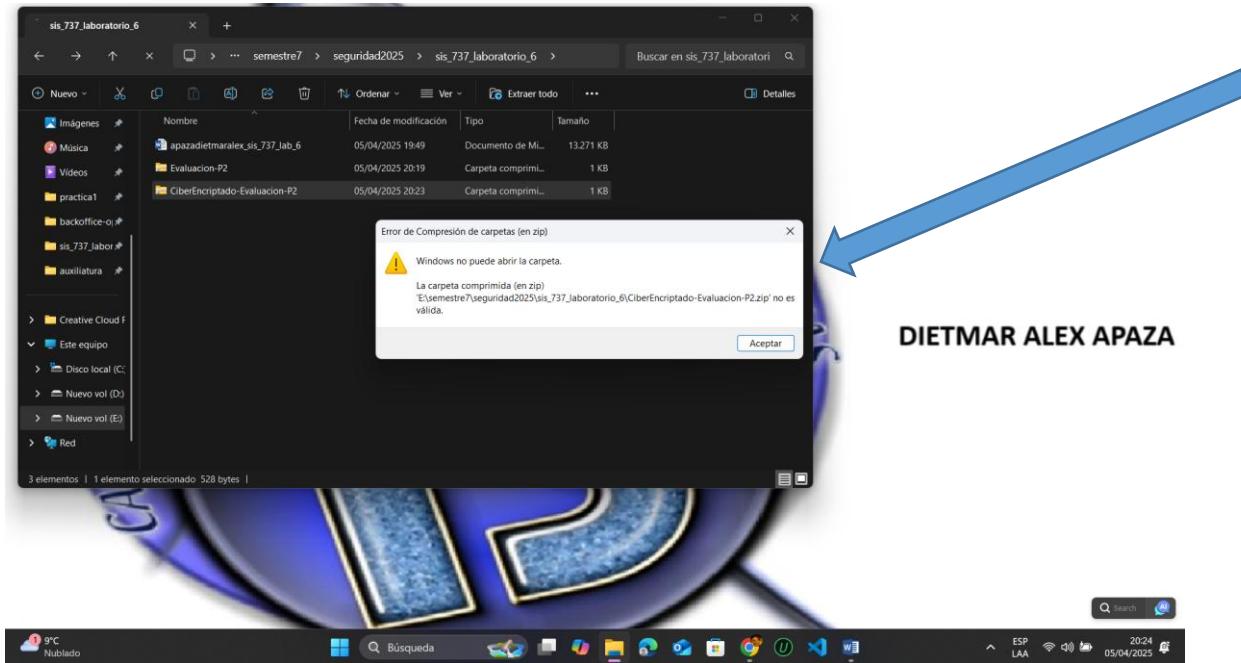
Establece una contraseña segura: alexthelion99



Descarga el archivo encryptado.

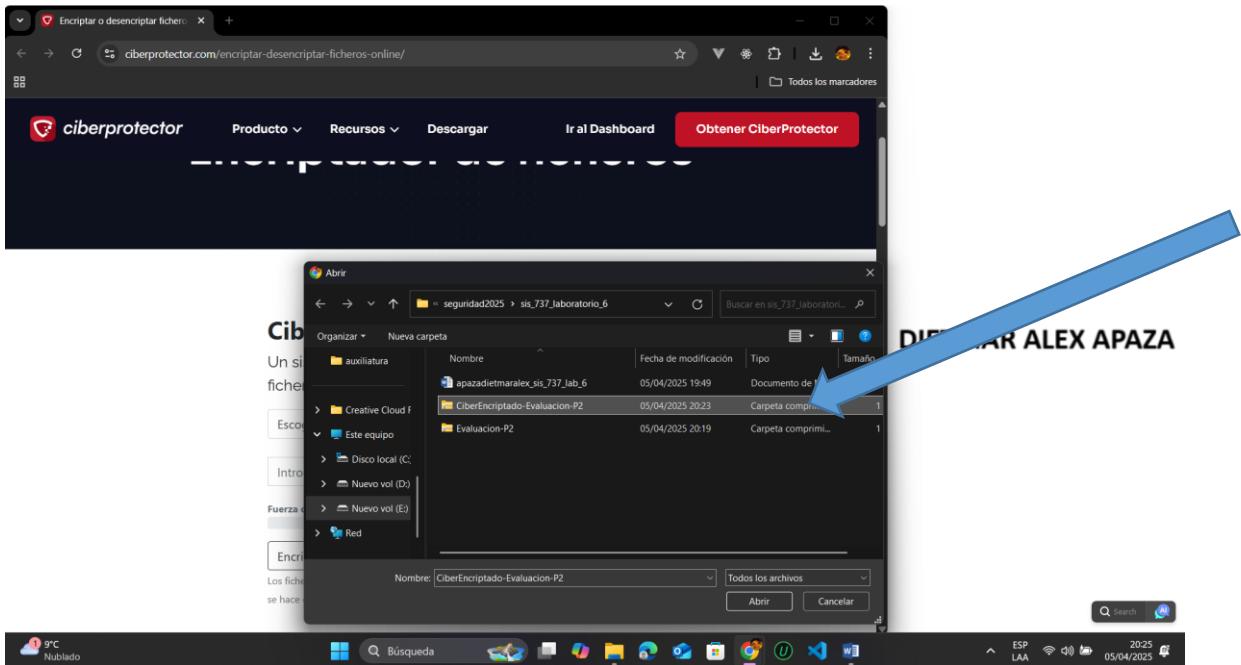


Una vez descargado el archivo encriptado ya no es el resultado esperado como se muestra en la imagen

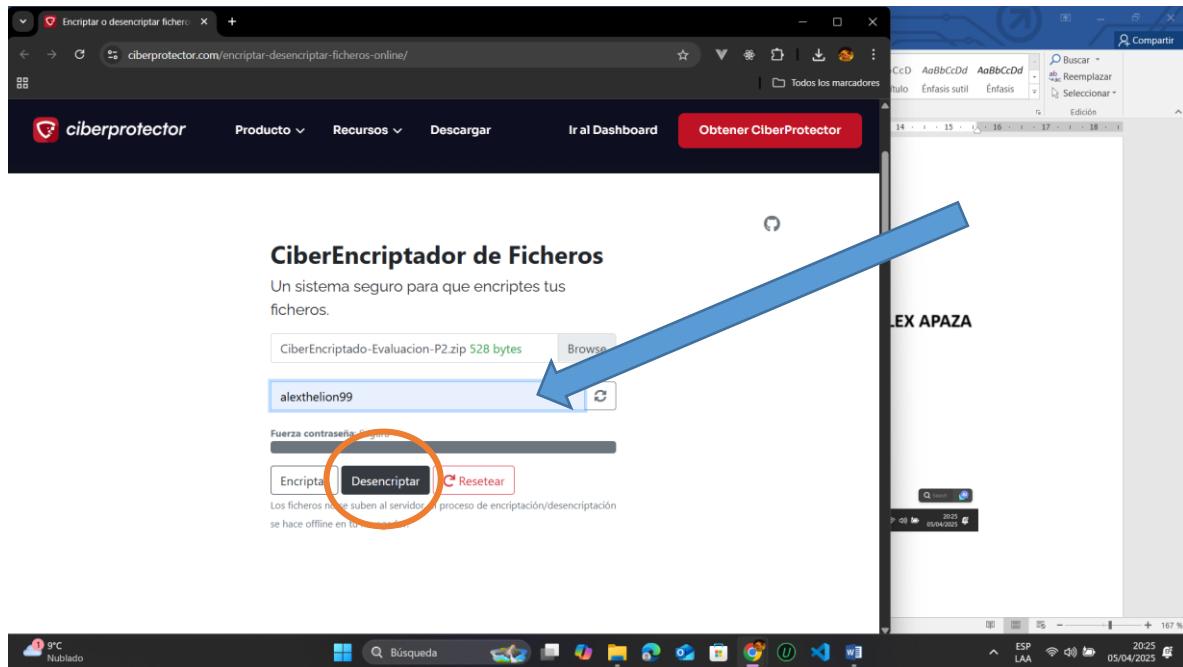


## Desencriptar archivo

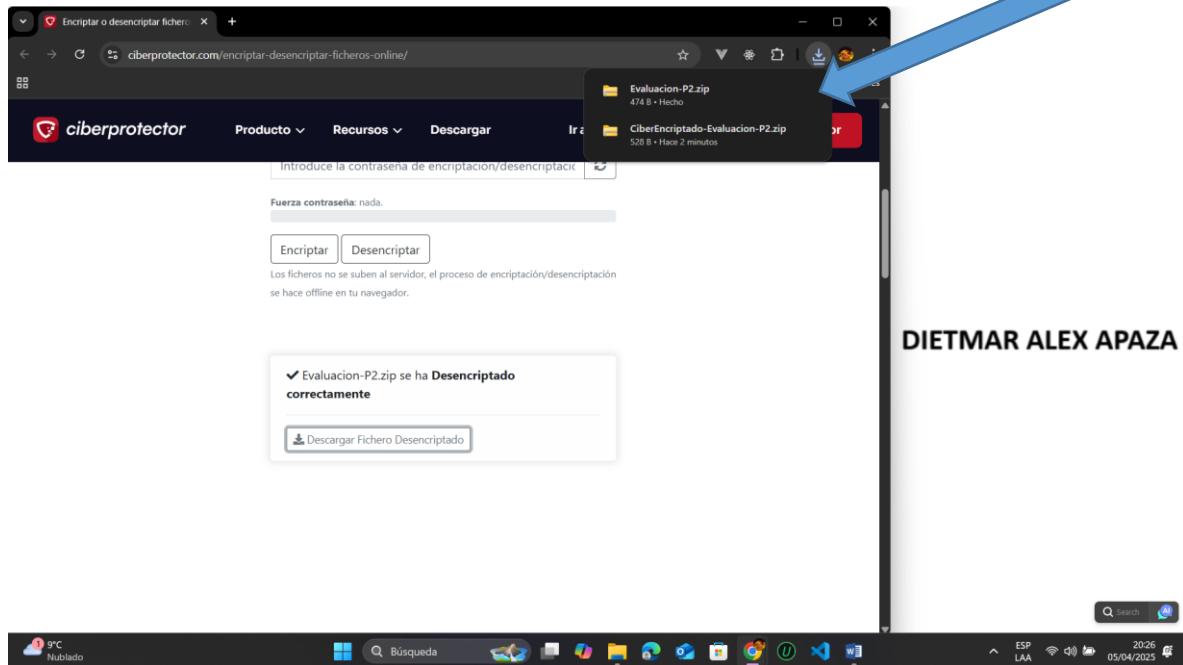
Para desencriptar el archivo subimos el archivo que encriptamos anteriormente.



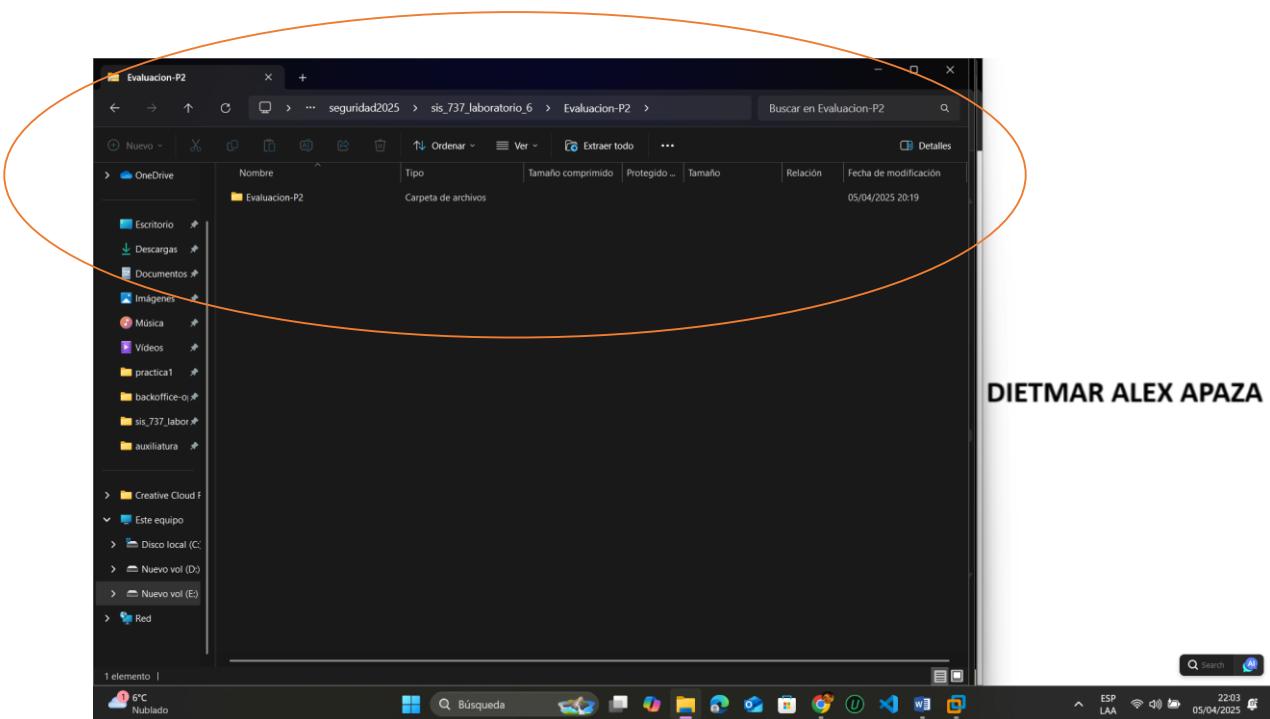
Ingresar la contraseña y presionar en el botón donde dice desencriptar.



Una ves desencriptado procedemos a descargar el archivo y verificar si esta correctamente solucionado.



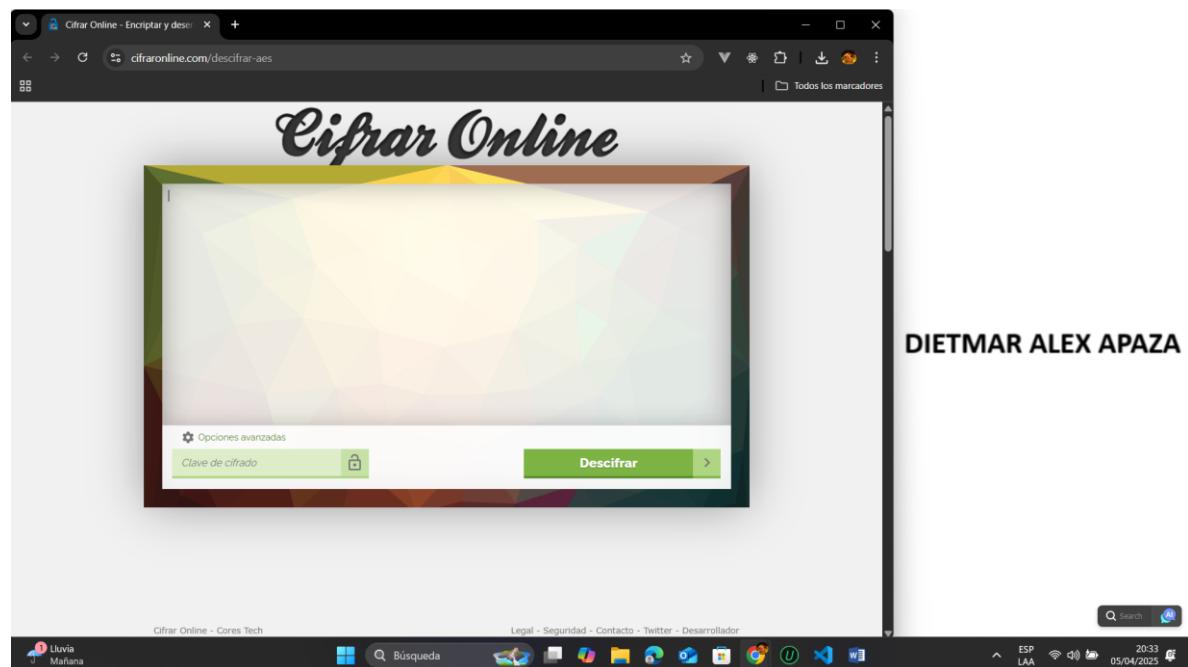
Resultado de la desencriptacion.



## 2.- Encriptar y desencriptar texto

<https://cifraronline.com/descifrar-aes>

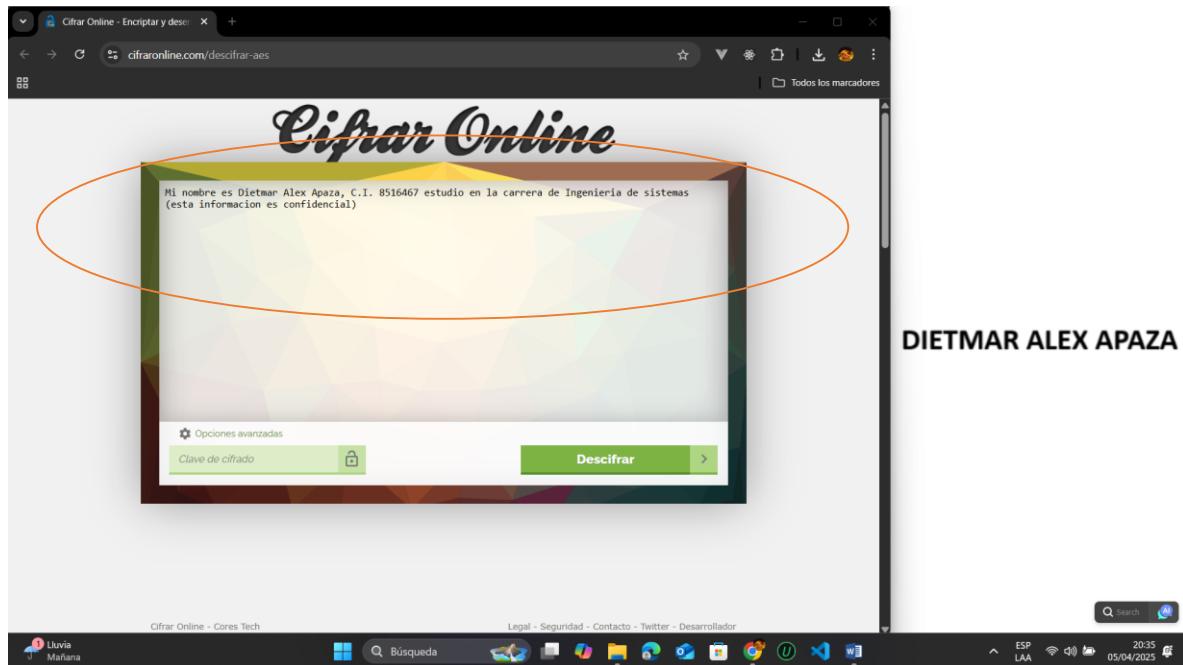
Primero ingresamos al link para poder realizar el desafío.



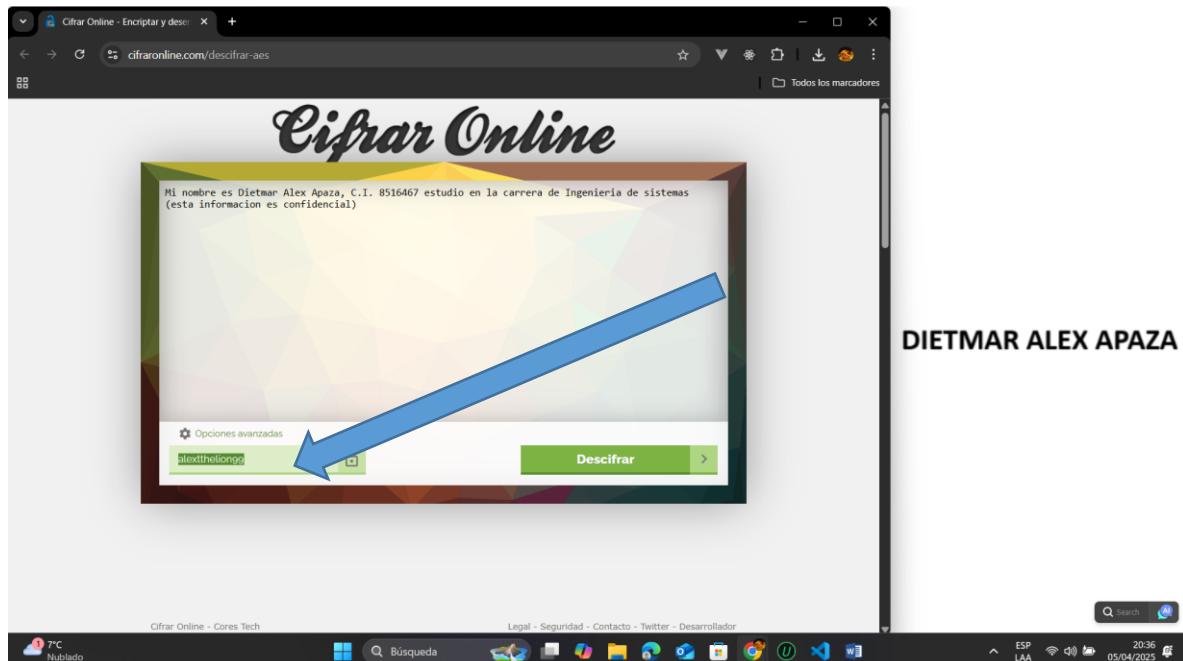
Pasos para Encriptar:

Seleccionar la opción "**Encriptar**".

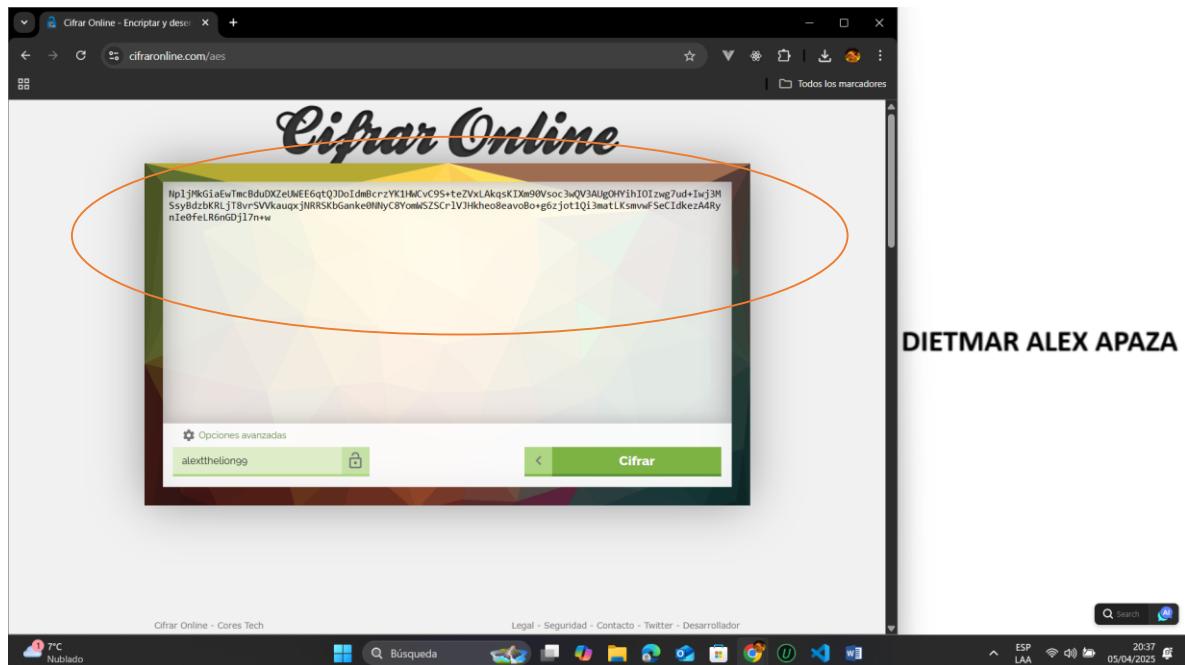
En el campo de **Texto plano**, escribir el mensaje que deseas cifrar.



En el campo de **Contraseña o clave**, ingresar una **contraseña segura** (preferiblemente larga, con mayúsculas, minúsculas, números y símbolos).



Hacer clic en "**Cifrar**".



### Pasos para Desencriptar:

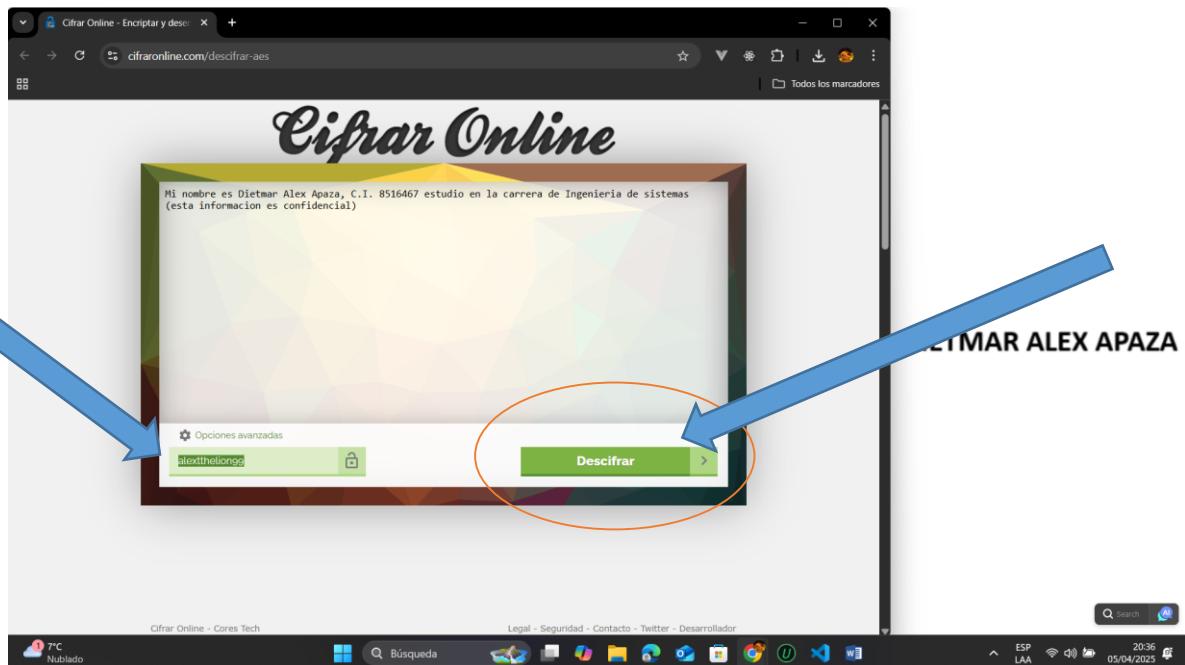
Seleccionar la opción "**Desencriptar**" en el mismo sitio.

Pegar el **texto cifrado** en el campo correspondiente.

Ingresar la **misma contraseña** usada para cifrar.

Hacer clic en "**Descifrar**".

Verás el mensaje original si la contraseña es correcta.



### Recomendación: Usar una Contraseña Segura

Utiliza generadores de contraseñas como LastPass Password Generator o Bitwarden Generator.

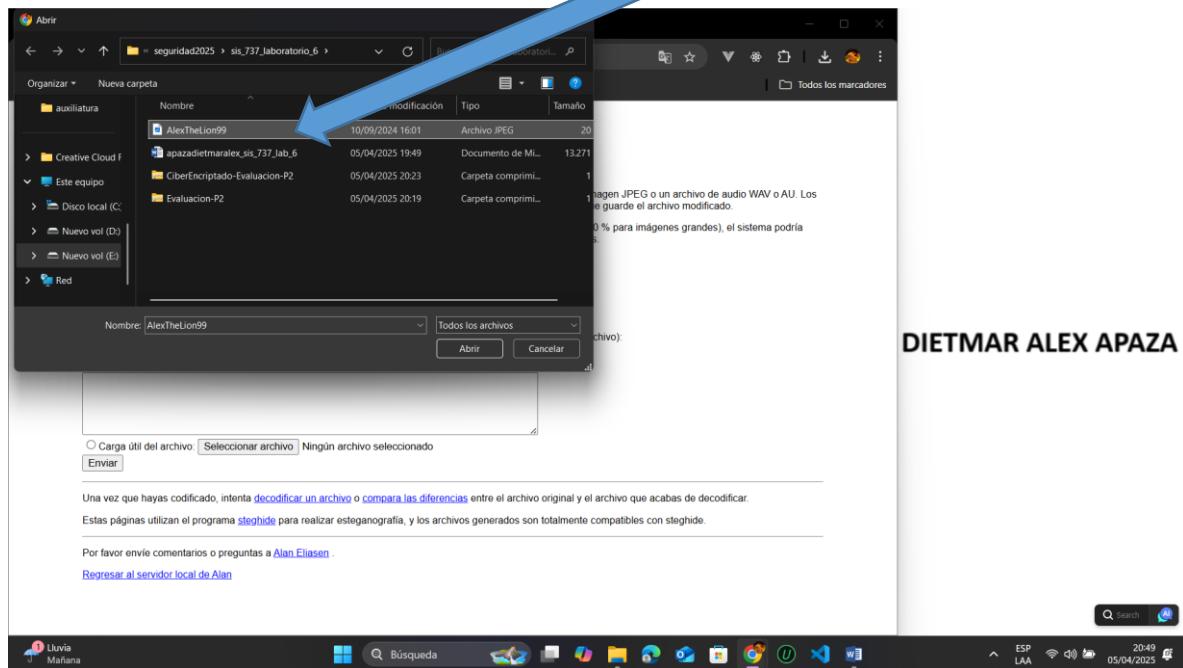
Ejemplo de contraseña segura: Xr@29#dlPQ8z!rK0

### 3.- Esteganografía (ocultar)

Ingresar al sitio: [futureboy.us/stegano/encinput.html](http://futureboy.us/stegano/encinput.html)

The screenshot shows a Windows desktop environment. A browser window is open to the 'Codificador esteganográfico' page at [futureboy.us/stegano/encinput.html](http://futureboy.us/stegano/encinput.html). The form has a title 'Codificador esteganográfico'. It includes instructions about using steganography to hide messages in images or audio files. There are fields for selecting a JPEG, AU, or WAV file ('Seleccione un archivo JPEG, AU o WAV para cargar') and a password ('Contraseña'). Below these are options for 'Carga útil' (useful load) with radio buttons for 'Solo encuentra la capacidad de este archivo' (selected) and 'Texto', followed by a large text input area. At the bottom, there are buttons for 'Carga útil del archivo' (useful load of the file), 'Seleccionar archivo' (select file), and 'Enviar' (Send). The status bar at the bottom of the browser shows 'DIETMAR ALEX APAZA' and various system icons.

Subir la imagen base en el campo "Choose file".



DIETMAR ALEX APAZA

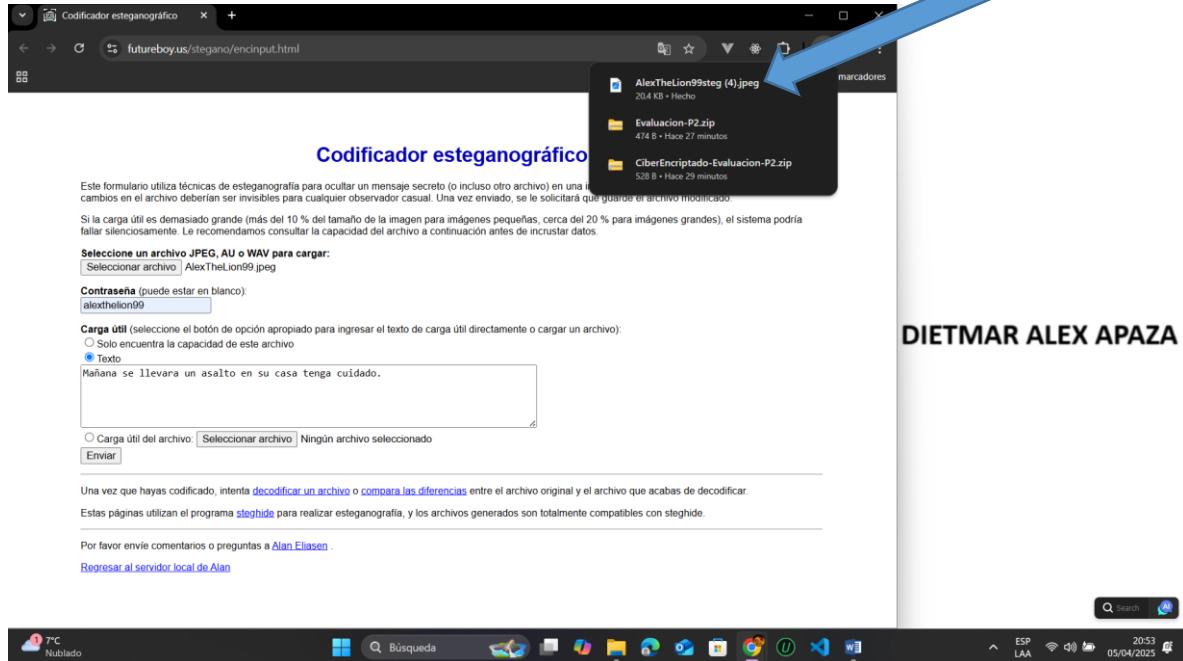
En el campo "**Message**", escribir el mensaje que deseas ocultar.

Añadir una **clave de codificación** para mayor seguridad.

Hacer clic en "**Enviar**".

DIETMAR ALEX APAZA

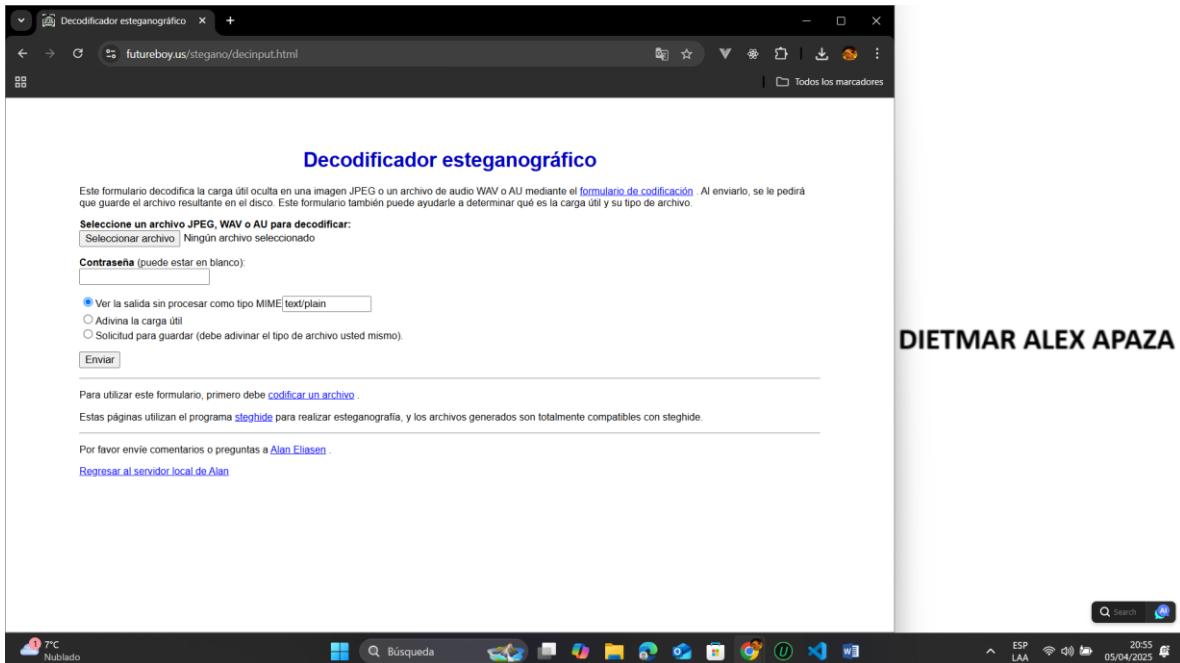
Descargar la imagen resultante con el mensaje oculto incrustado.



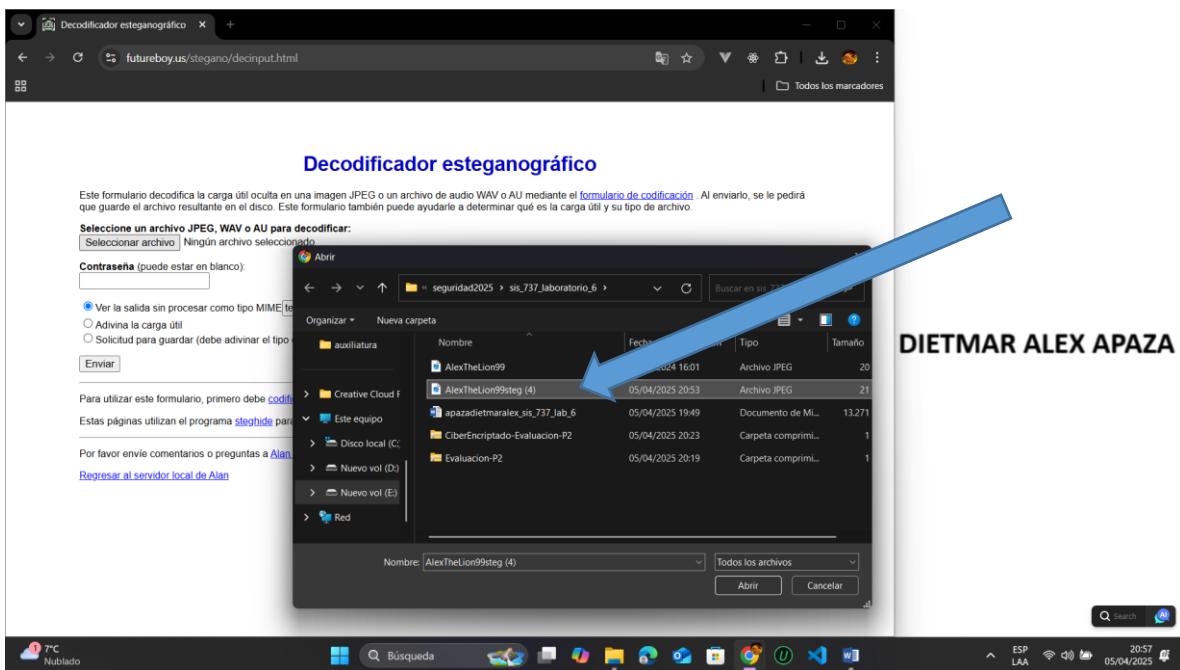
En la imagen que esta ocultado el texto plano no se puede ver a simple vista. Hasta que logremos decifrar la imagen.

#### 4.- Esteganografía (mostrar)

Ingresar al sitio: [futureboy.us/stegano/decinput.html](http://futureboy.us/stegano/decinput.html)

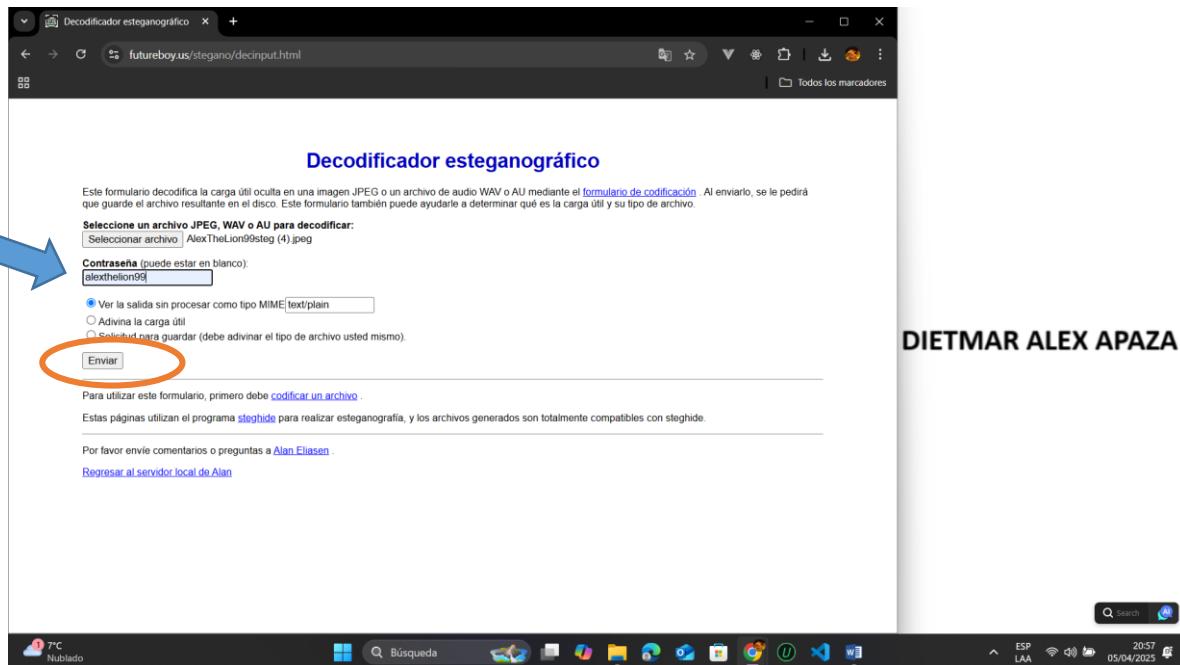


Subir la imagen que tiene el mensaje oculto.



Ingresar la clave de codificación si se usó una.

Hacer clic en "Enviar".



**Decodificador esteganográfico**

Este formulario decodifica la carga útil oculta en una imagen JPEG o un archivo de audio WAV o AU mediante el [formulario de codificación](#). Al enviarlo, se le pedirá que guarde el archivo resultante en el disco. Este formulario también puede ayudarle a determinar qué es la carga útil y su tipo de archivo.

**Seleccione un archivo JPEG, WAV o AU para decodificar:**

**Contraseña** (puede estar en blanco):

Ver la salida sin procesar como tipo MIME:   
 Adivina la carga útil  
 Solicitud para guardar (debe adivinar el tipo de archivo usted mismo).

**Enviar**

Para utilizar este formulario, primero debe [codificar un archivo](#).  
Estas páginas utilizan el programa [steghide](#) para realizar esteganografía, y los archivos generados son totalmente compatibles con steghide.

Por favor envíe comentarios o preguntas a [Alan Eliasen](#).  
[Regresar al servidor local de Alan](#)

DIETMAR ALEX APAZA

Una vez realizado los pasos si la contraseña es la correcta. El sitio mostrará el mensaje oculto extraído de la imagen.

