



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\\_Lab\\_6](https://github.com/AlexTheLion99/sis_737_Lab_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

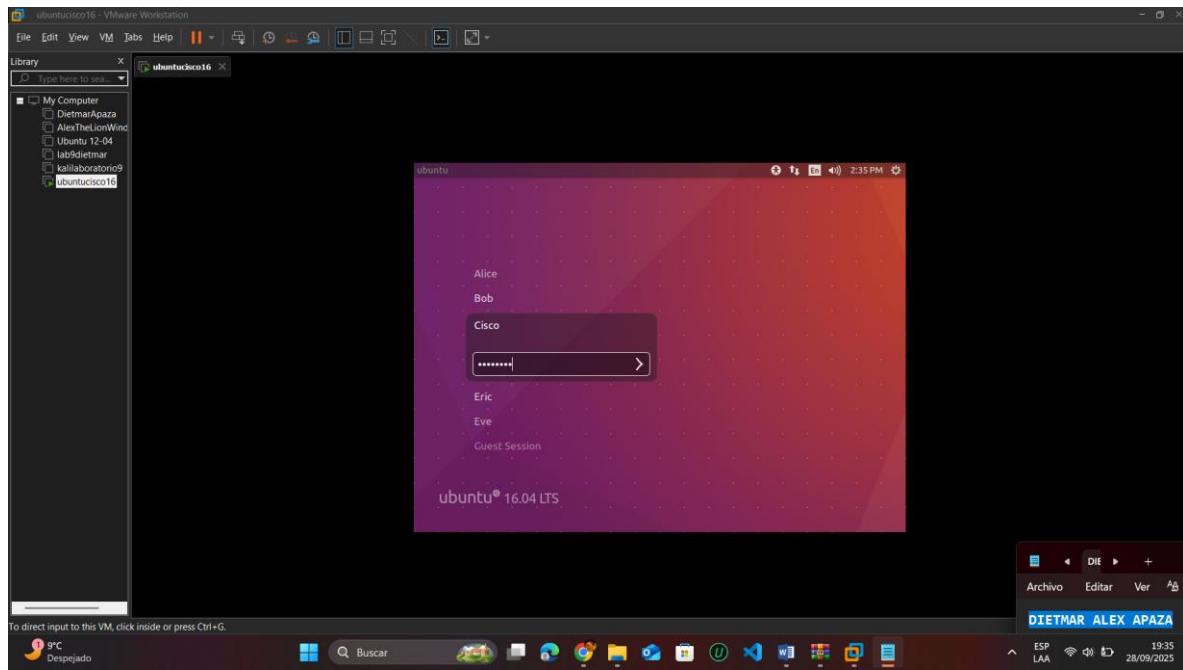
**Recursos:** Computadora de escritorio con Ubuntu CISCO 16.04.4 LTS instalado en una máquina virtual de VirtualBox o VMware.

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

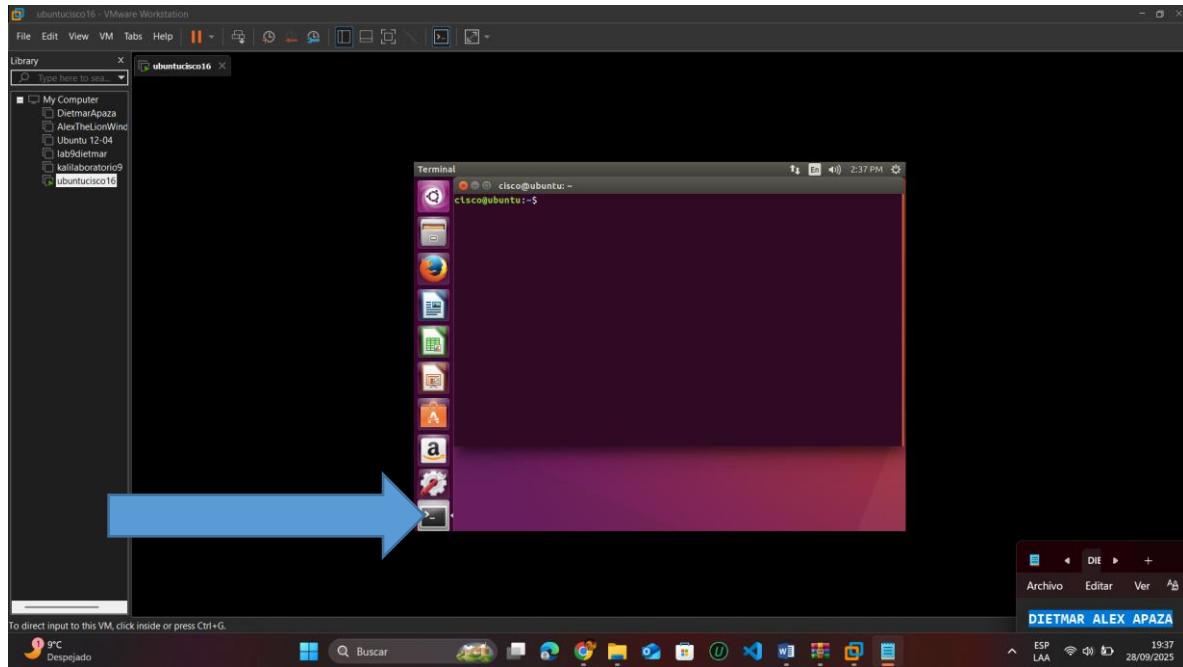
a. Inicie sesión en Ubuntu con las siguientes credenciales:

**Usuario:** cisco

**Contraseña:** password



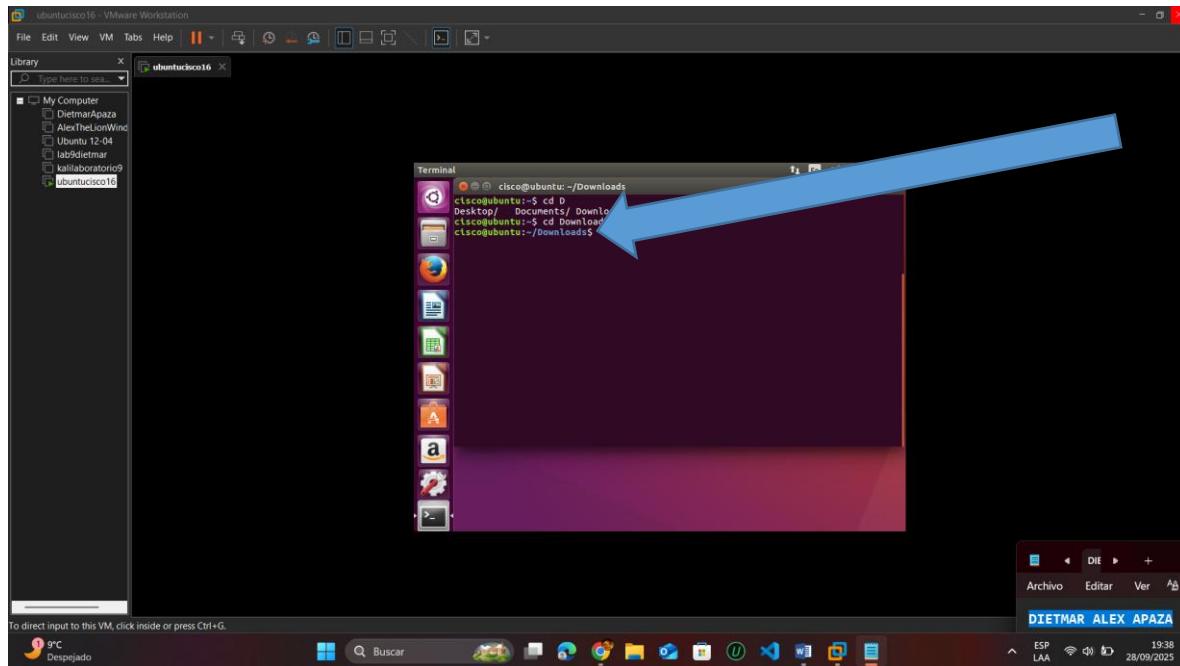
b. Haga clic en el icono de terminal para abrir un terminal.



## Paso 2: Ejecute Steghide.

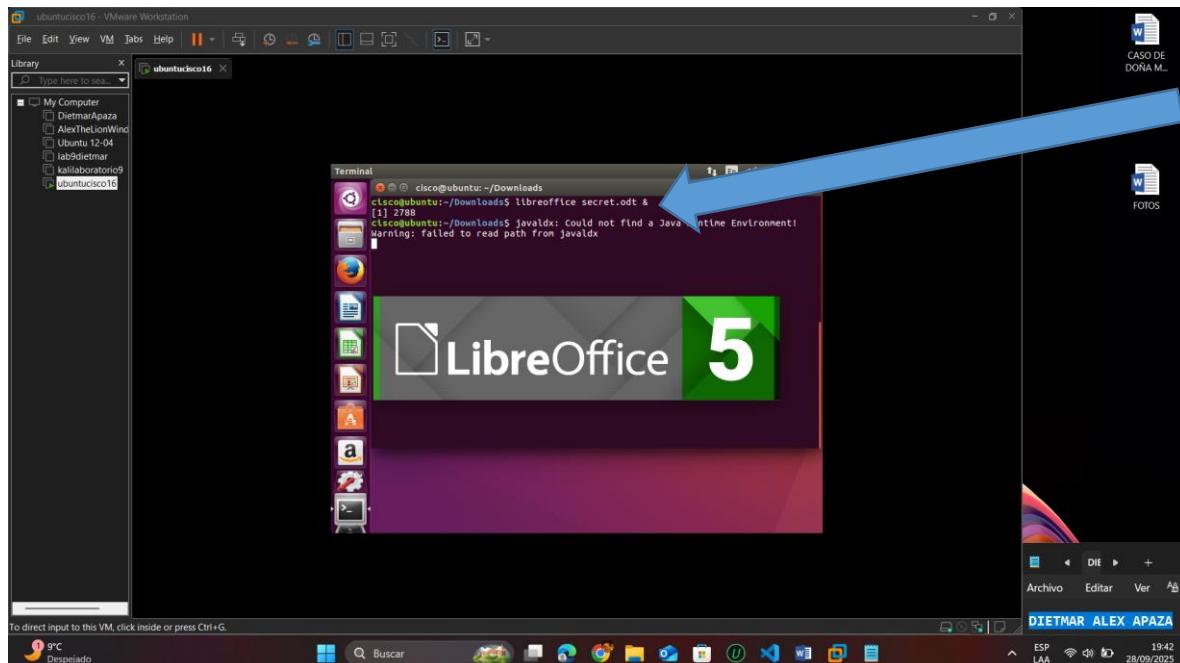
- En la petición de ingreso de comando, ingrese el siguiente comando para cambiar el directorio de descargas:

cisco@ubuntu:~\$ cd Downloads/



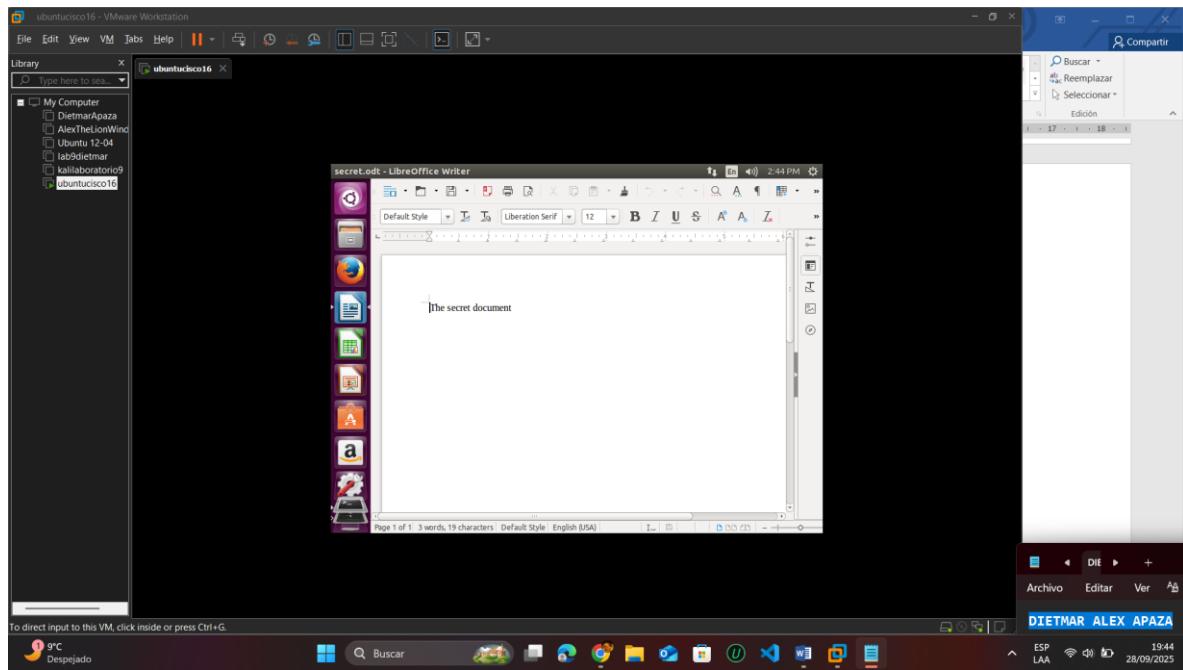
b. Introduzca libreoffice secret.odt & en la petición de ingreso.

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

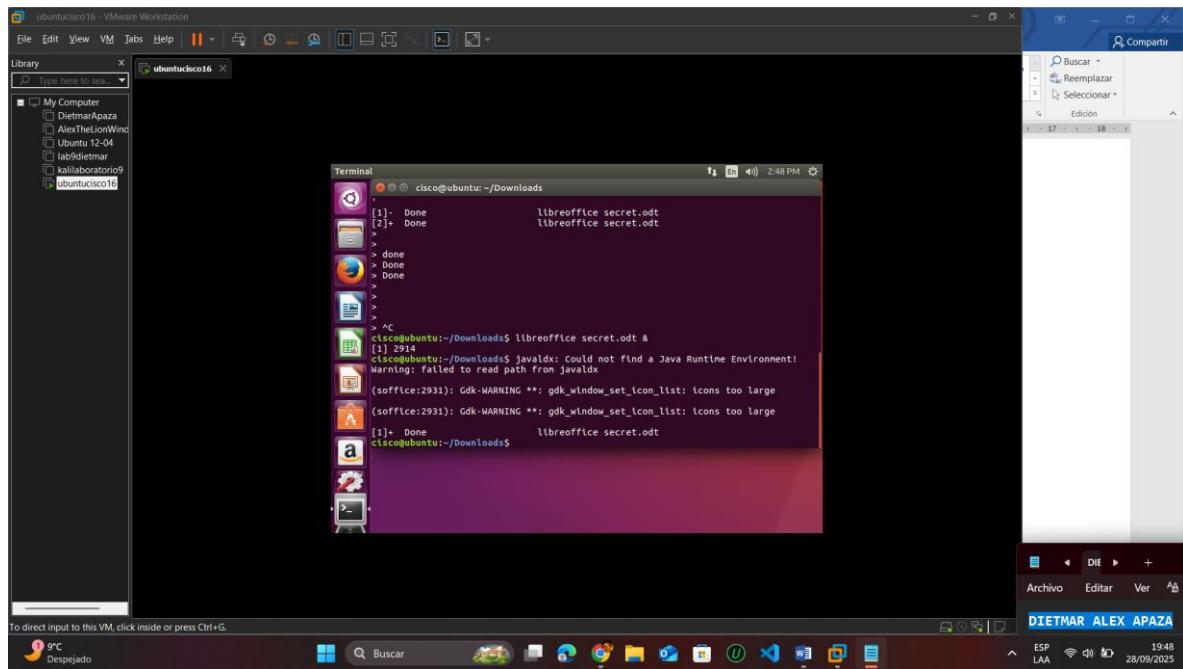


¿Cuál es el mensaje en el archivo secret.odt?

R.- The secret document

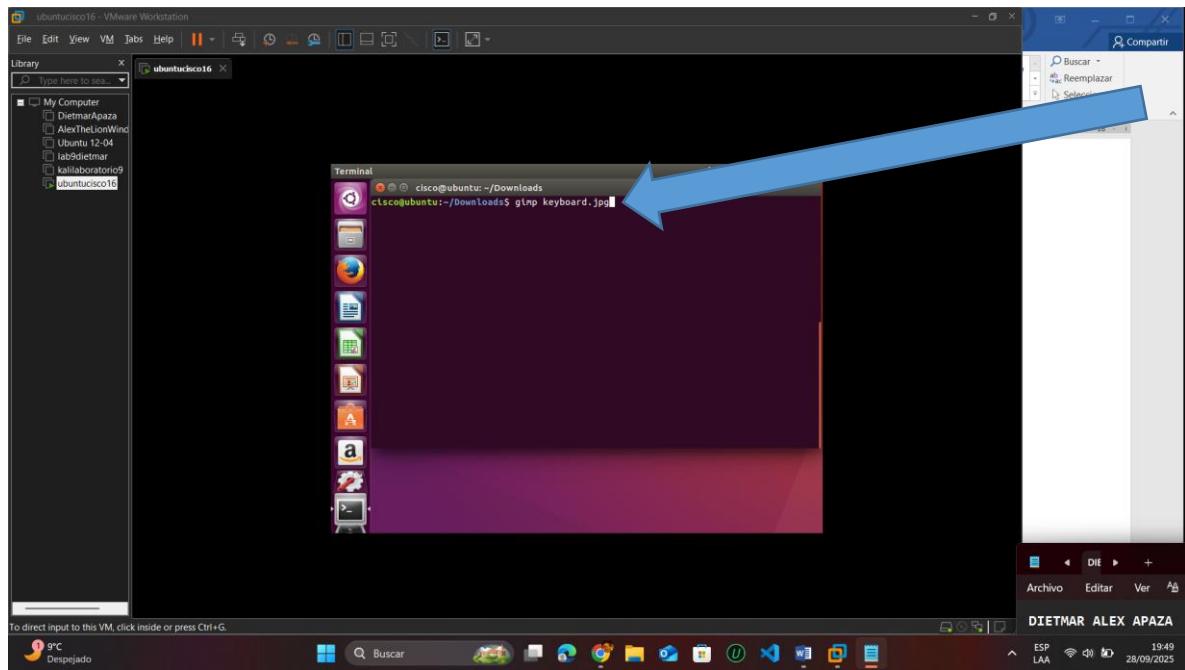


c. Cierre el archivo secret.odt cuando haya terminado.

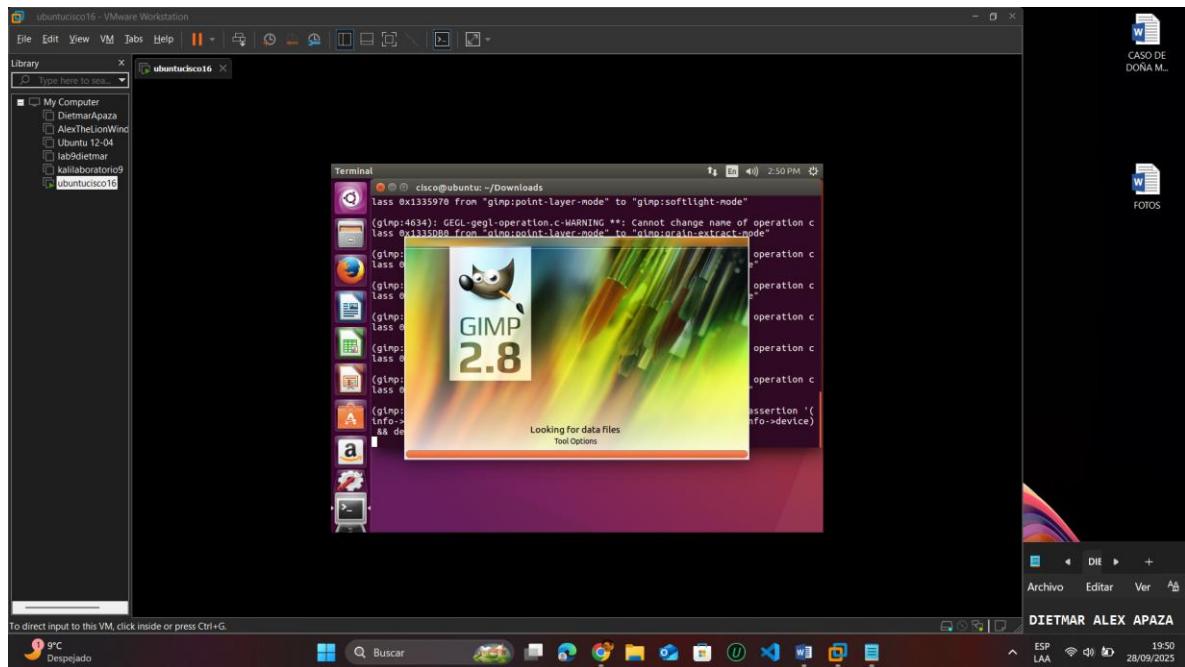


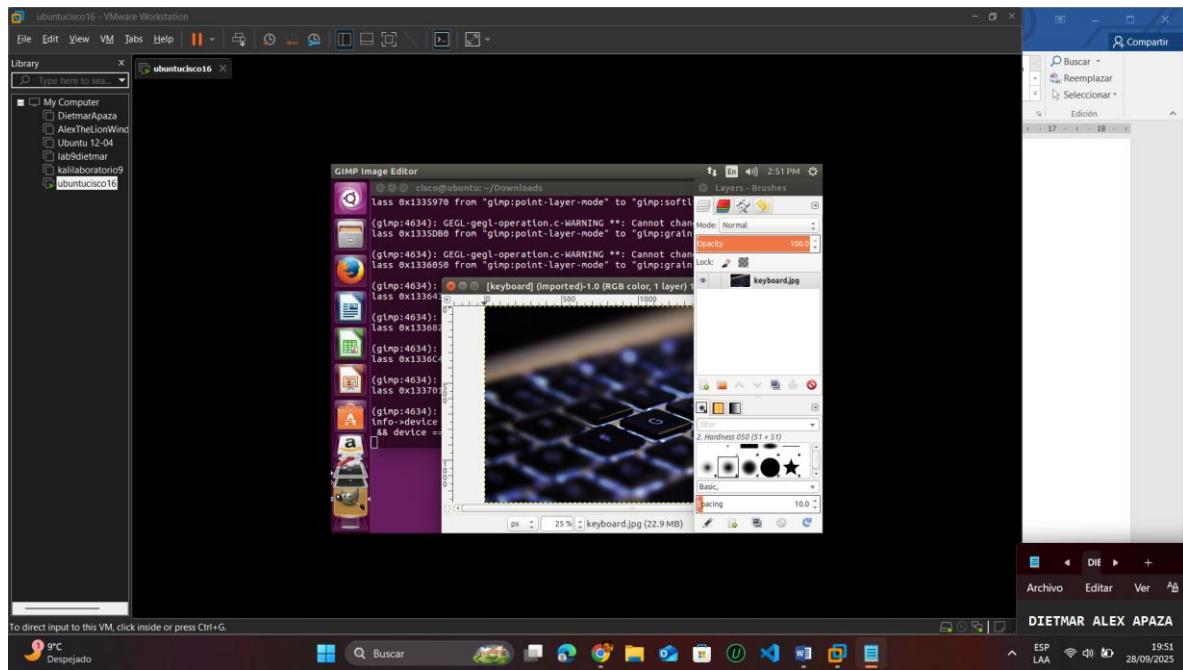
d. Introduzca **gimp keyboard.jpg &** en la petición de ingreso para ver el archivo de imagen

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

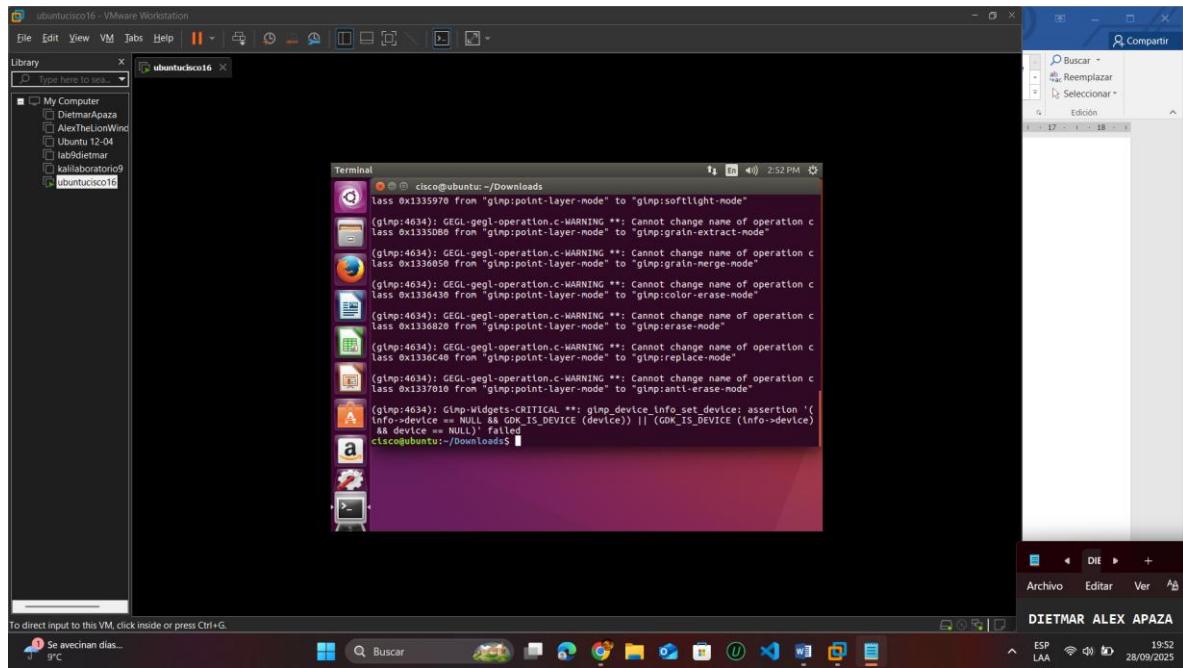


El comando abrirá la imagen que está en Download

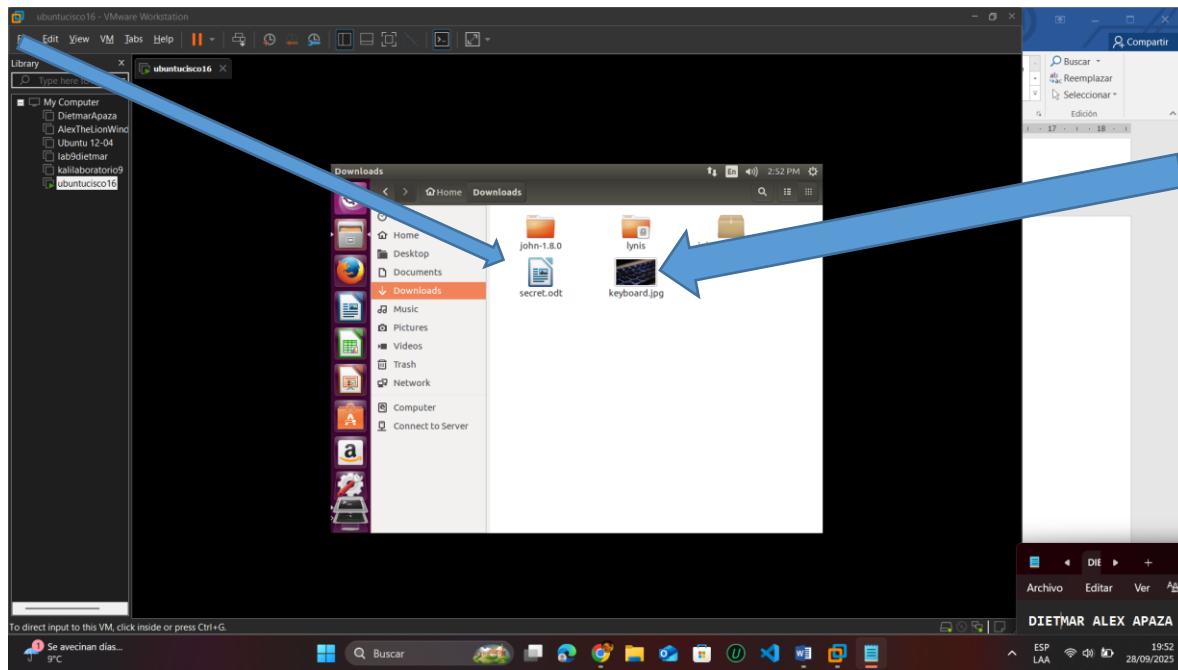




e. Cierre el archivo keyboard.jpg cuando haya terminado.

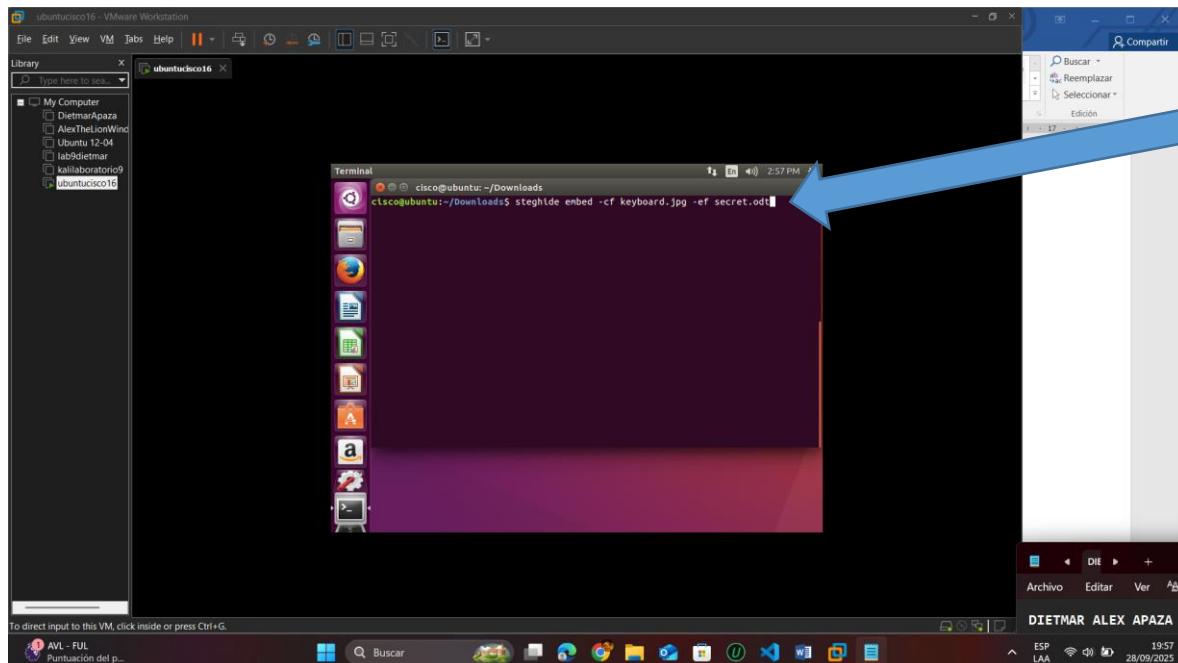


Puede visualizar estos archivos si ingresa a la carpeta Donwloads



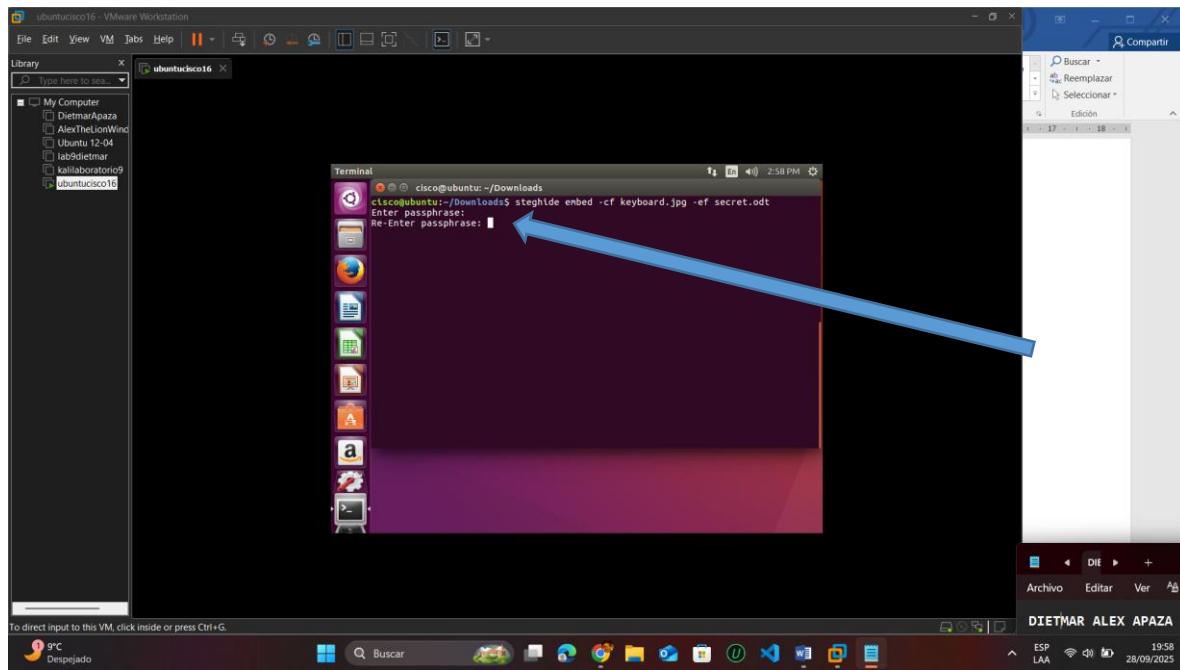
f. En la petición de ingreso de comando, introduzca el siguiente comando:

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

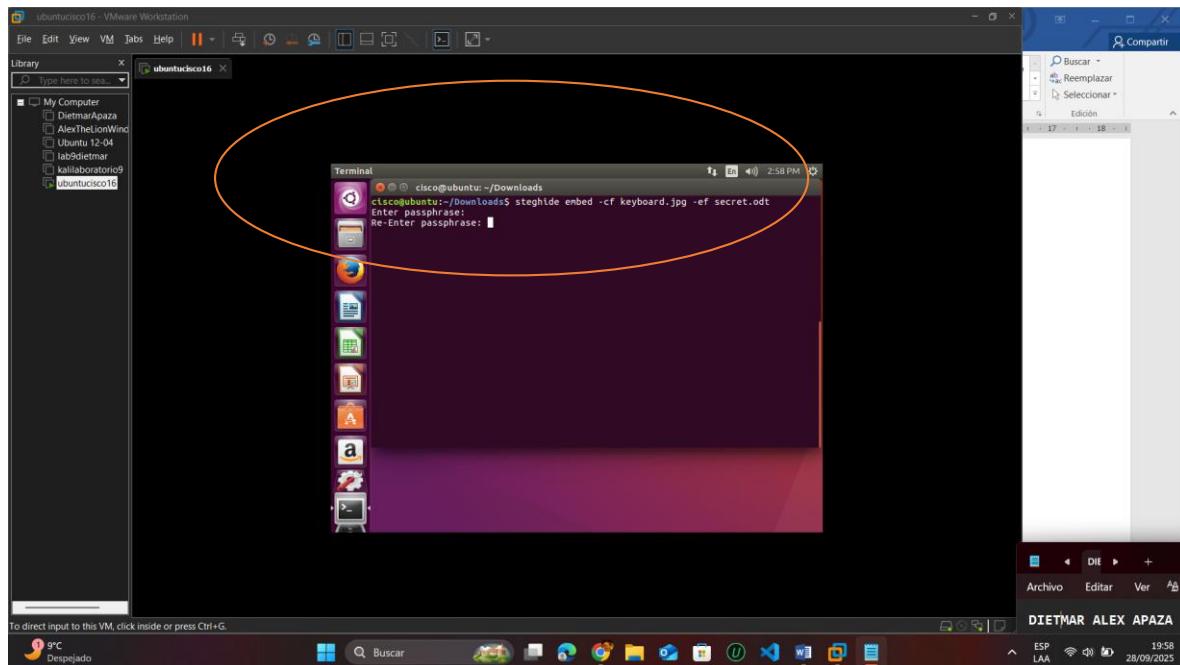


Este comando acepta el archivo JPEG llamado «keyboard.jpg» y lo utiliza como transportista para incorporar el documento, secret.odt en él.

**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.



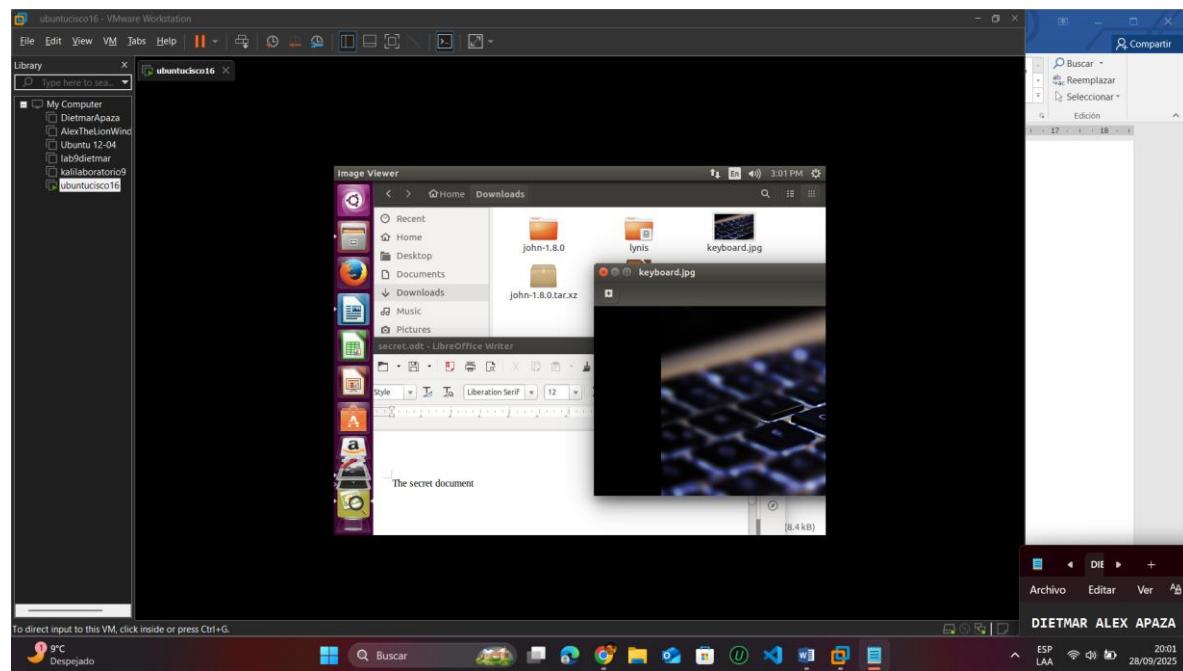
**i.** Abra los archivos secret.odt y keyboard.jpg. ¿Se modificaron estos archivos?

R.-

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

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

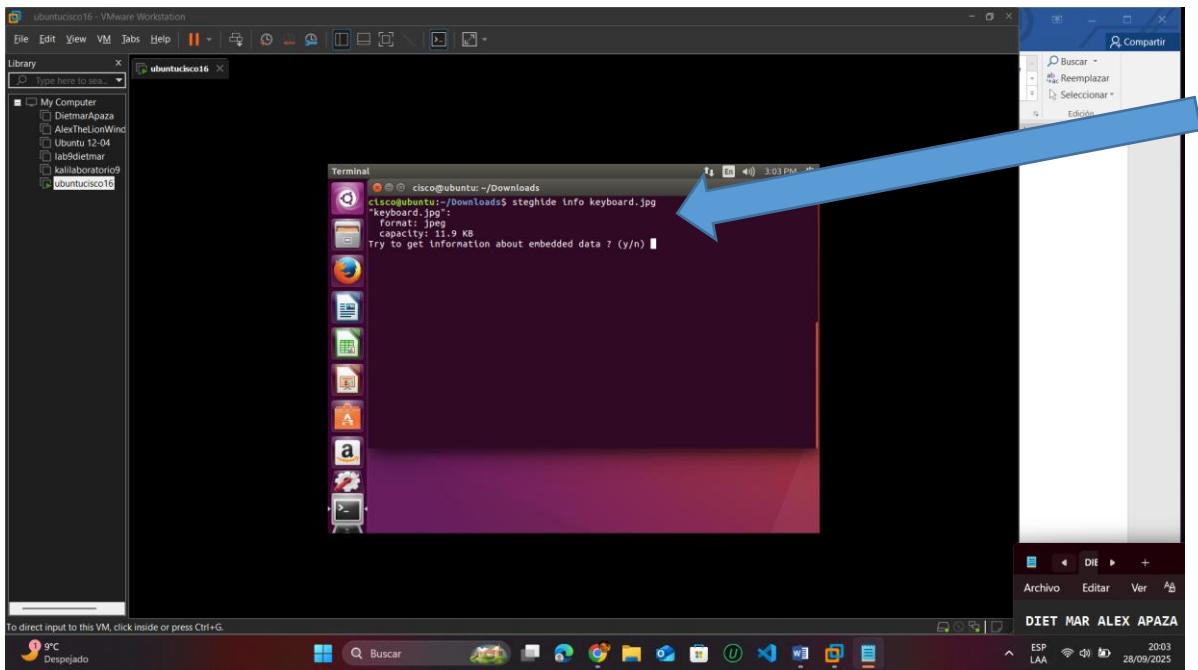
Puede abrirlos mediante comandos o también desde la carpeta Downloads



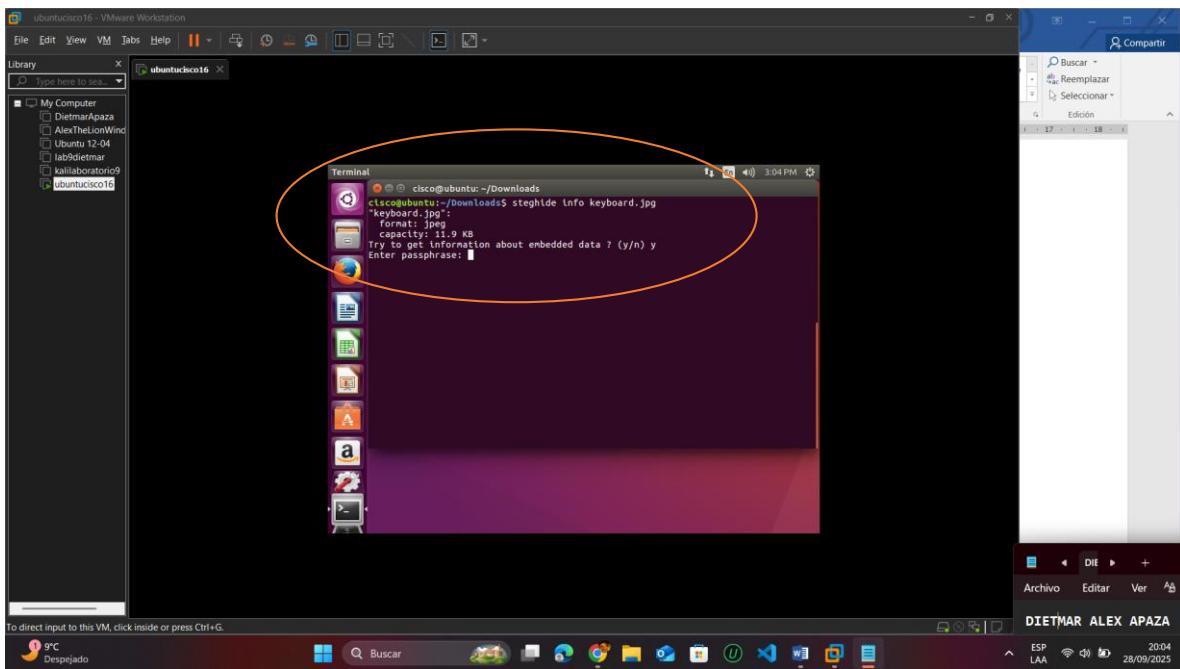
**Paso 3:** Verifique el archivo oculto.

a. Escriba el siguiente comando en el terminal.

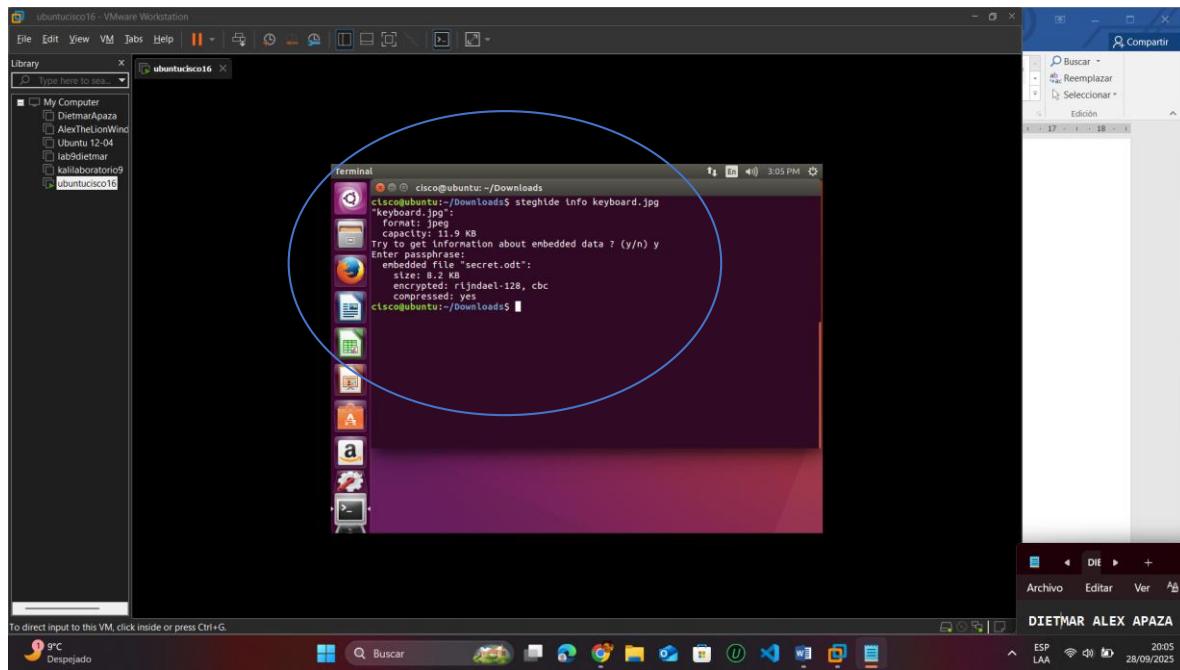
```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
```



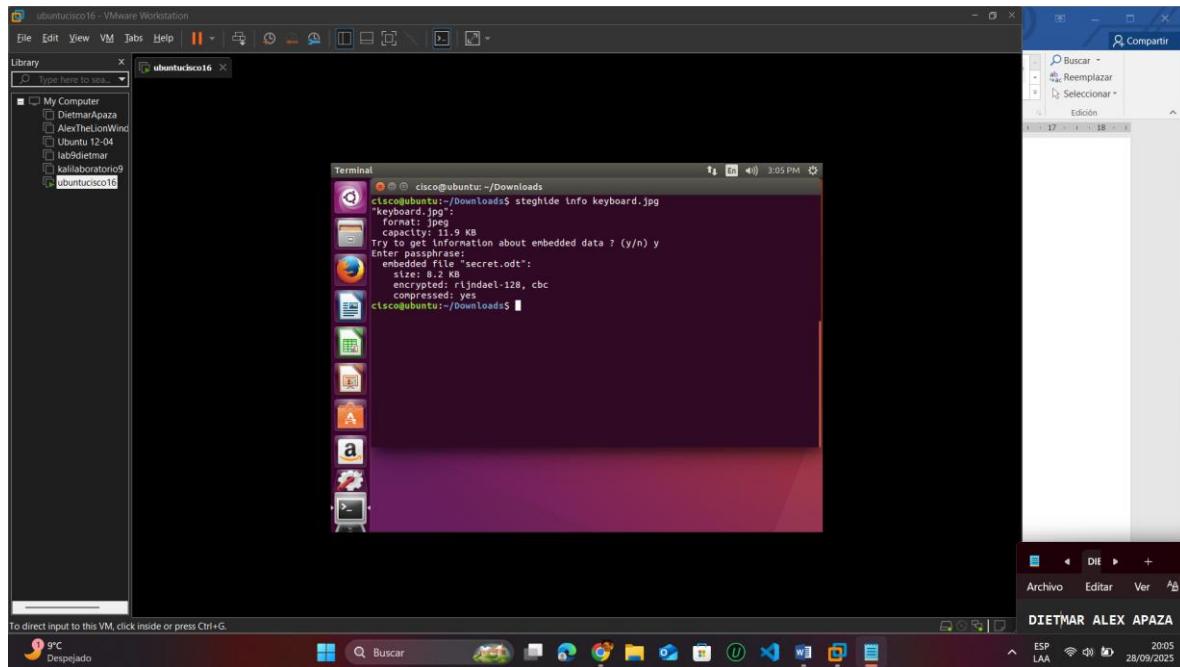
**b.** Escriba y en la petición de ingreso. (No presione Intro).



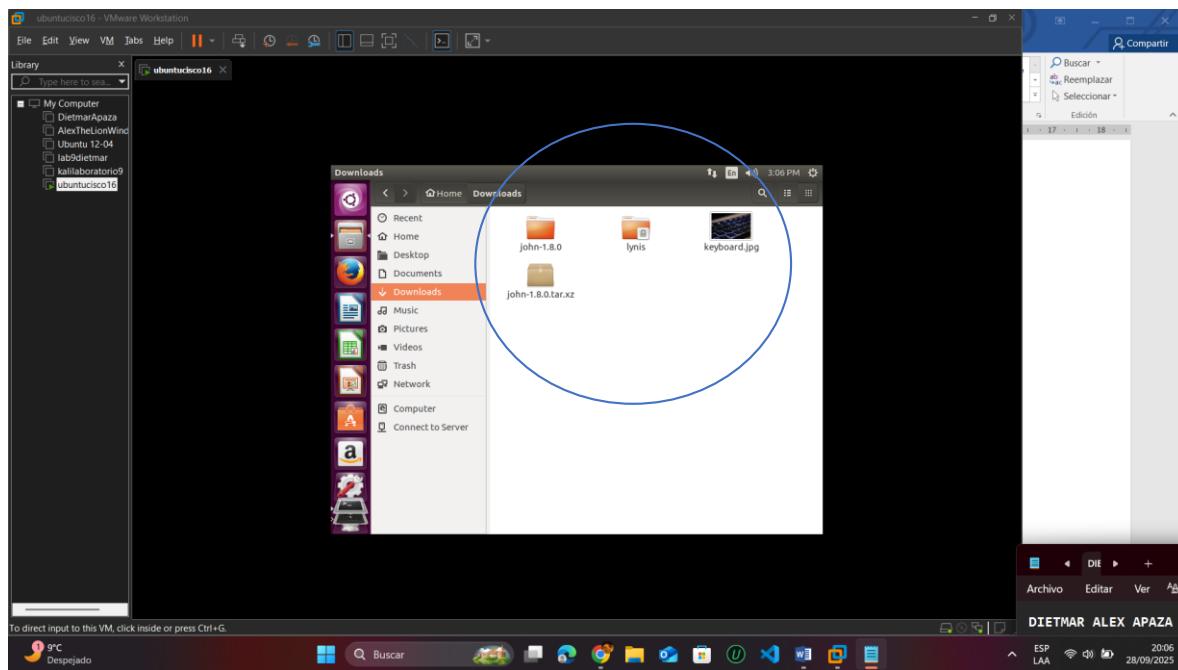
**c.** Introduzca la contraseña Cisco y presione Intro.



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



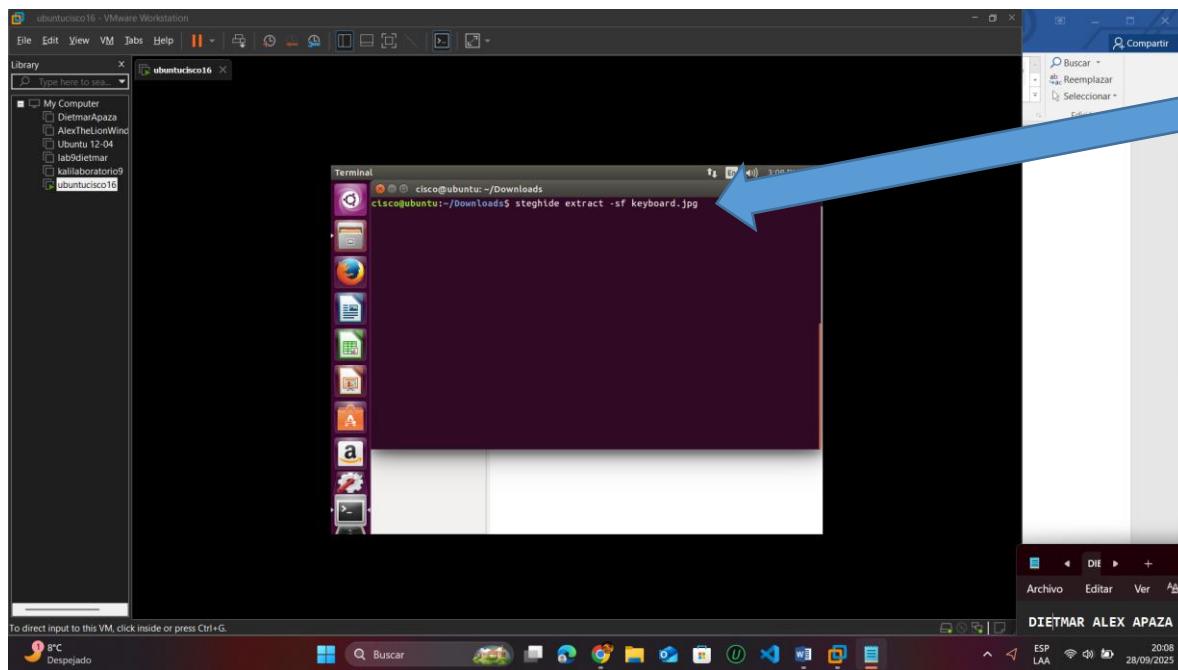
Elimine el archivo secret.odt , esto representa que únicamente ahora cuenta con la imagen y dentro de ella el archivo que oculta.



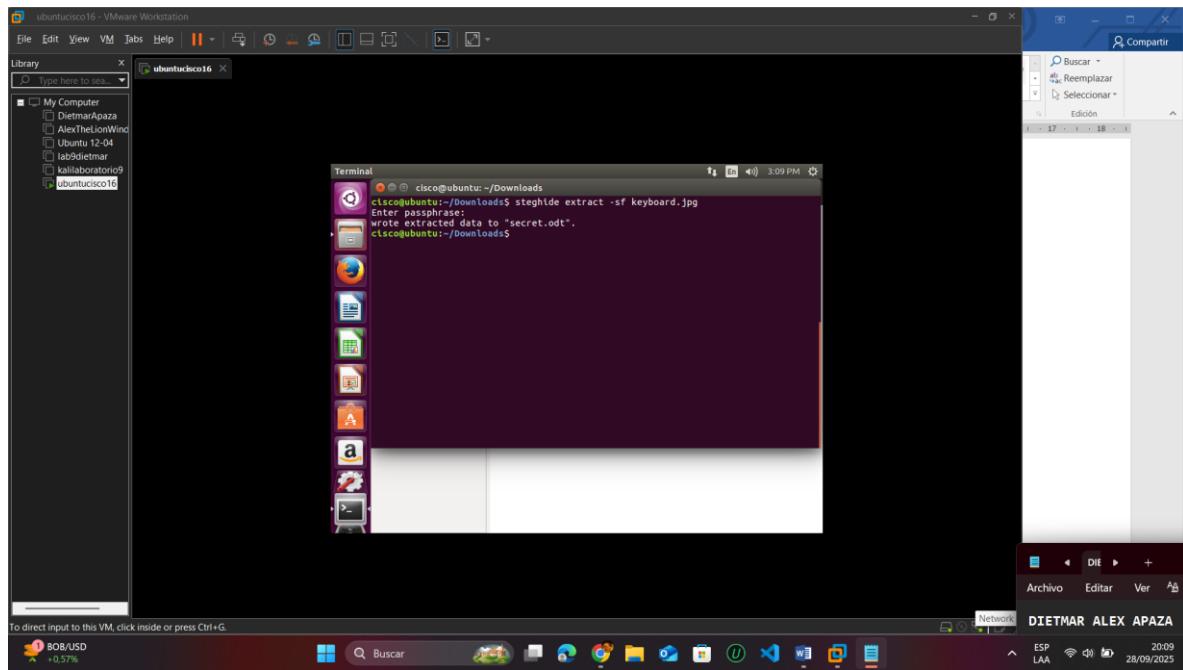
**Paso 4:** Extraiga el archivo oculto.

a. Escriba el siguiente comando en el terminal.

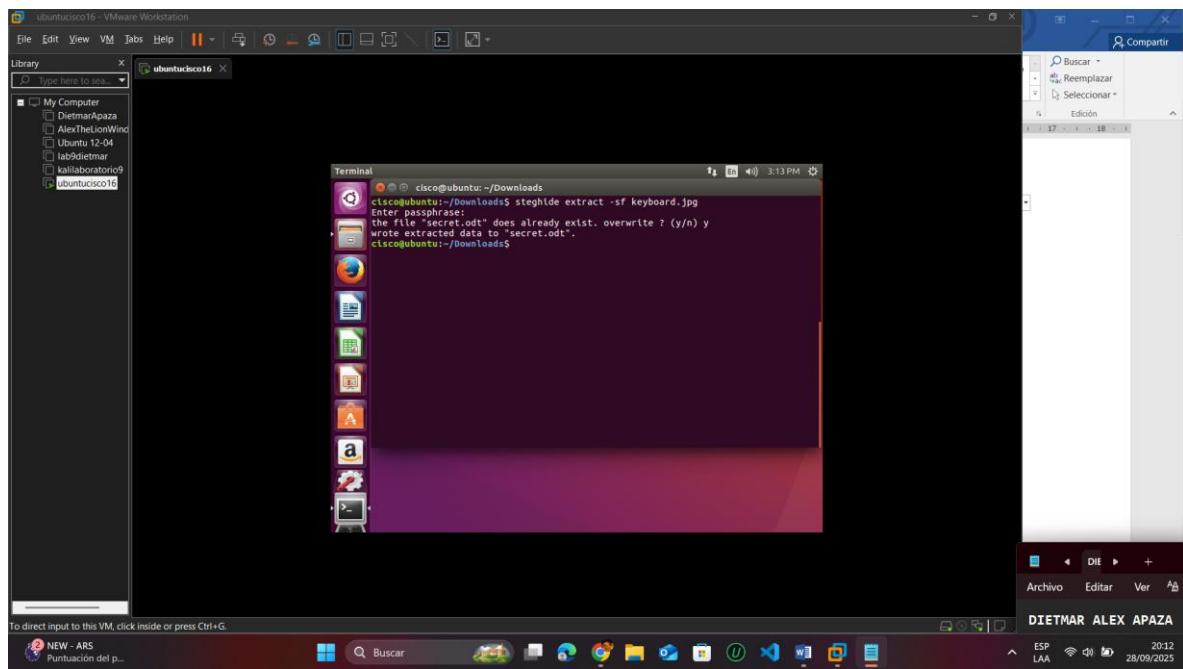
```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```



b. Introduzca la contraseña Cisco y presione Intro.

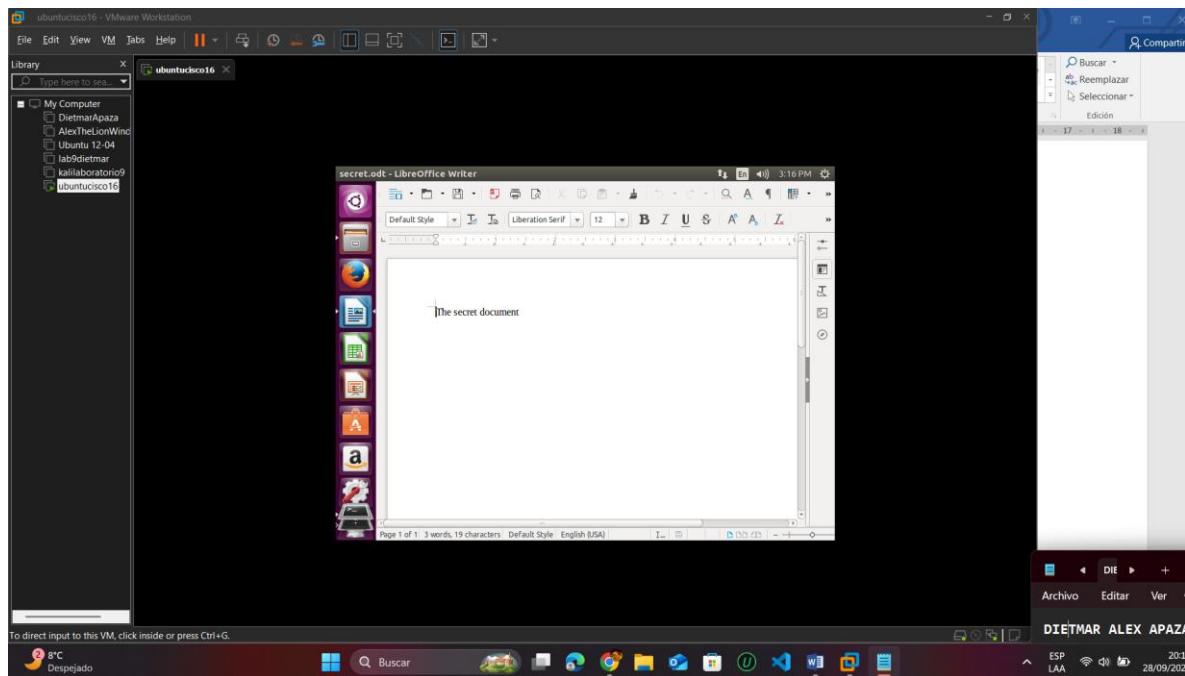
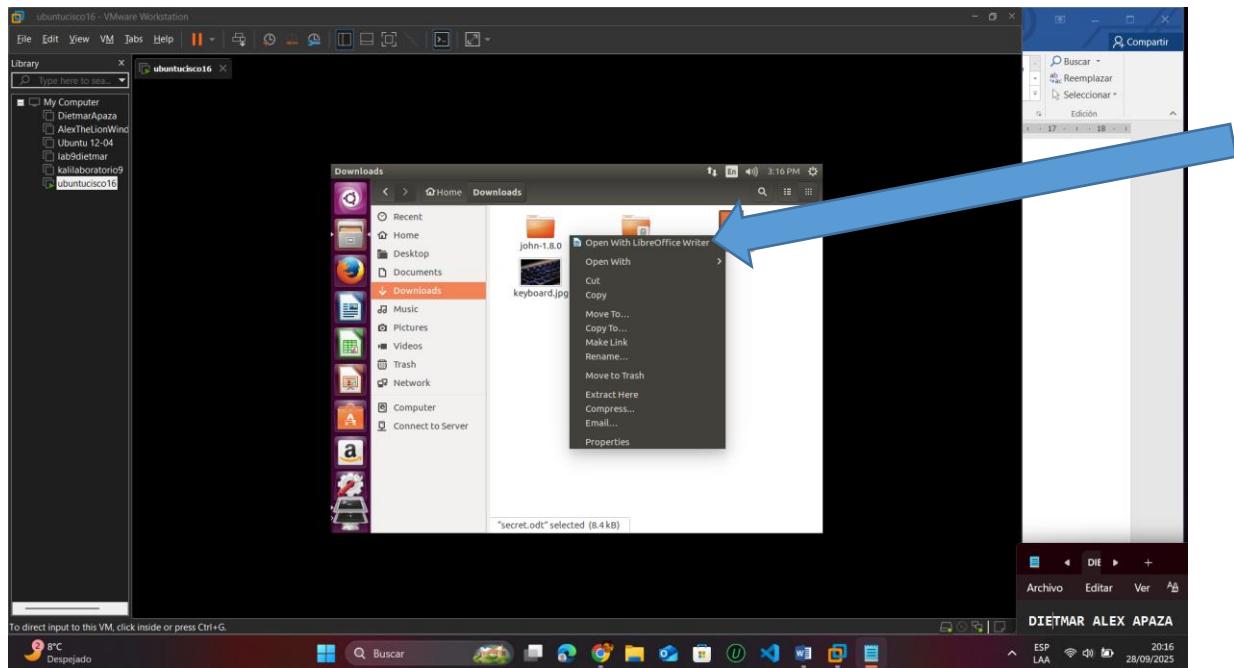


c. Introduzca y , el archivo secret.odt será extraído nuevamente de la imagen que lo transporta.



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?

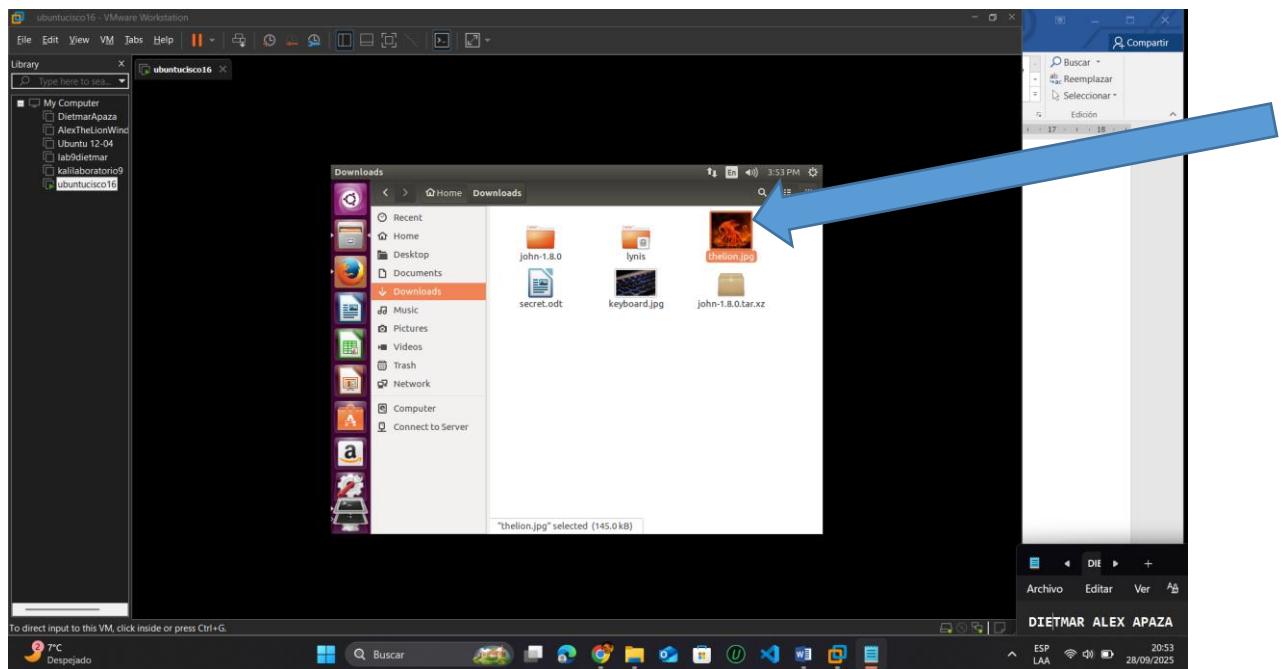
R.- Sí, el contenido del archivo `secret.odt` no cambia durante el proceso.

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

# EVALUACIÓN

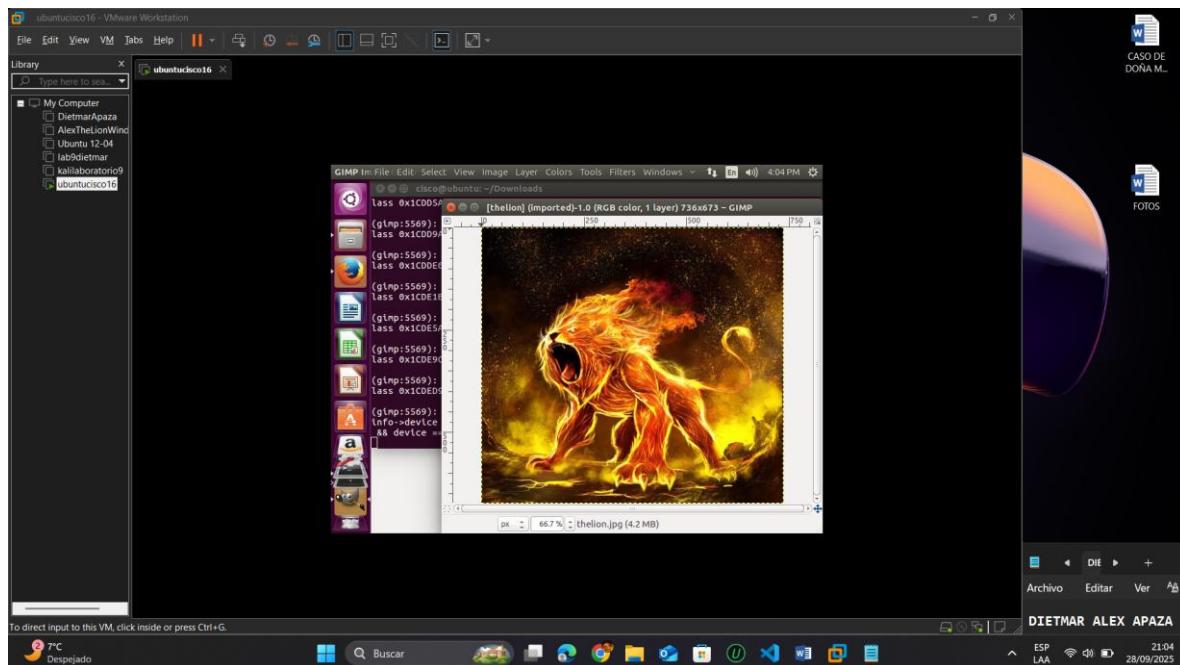
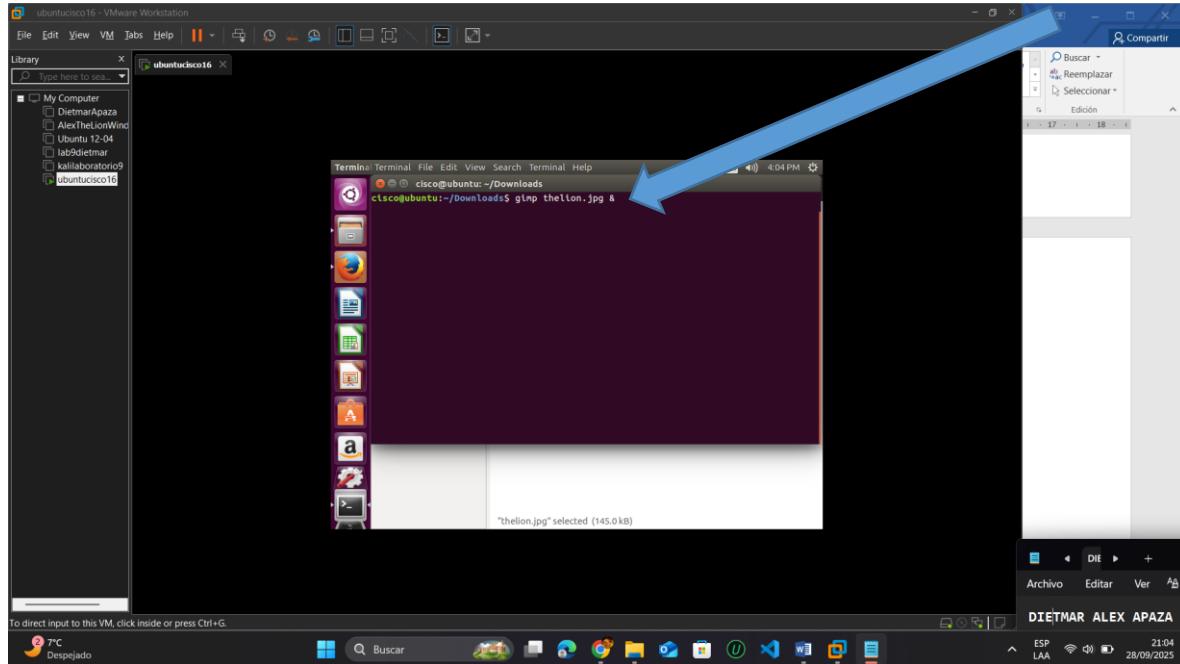
1.- Copie una imagen nueva a la pc con ubuntu y adjunte a ella un archivo de texto en el que estará su nombre completo y CI, use como contraseña sistemas2024s2 y muestre que la extracción funciona. (Deberá hacer capturas de todo este proceso)

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



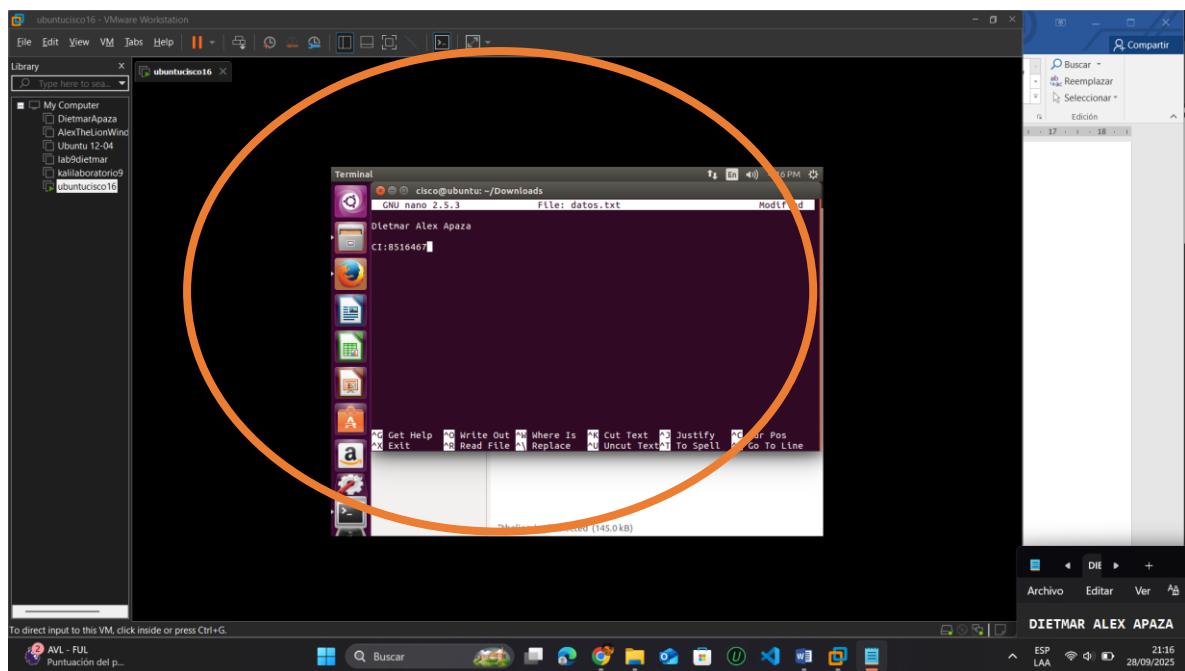
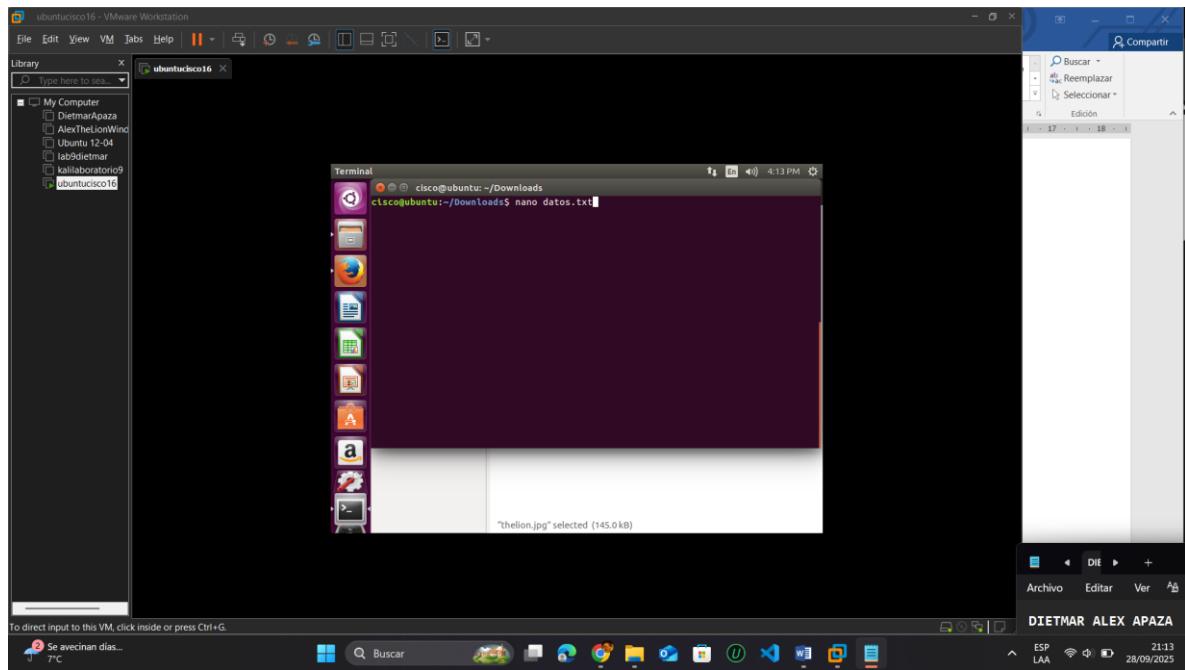
Introduzca **gimp thelion.jpg &** en la petición de ingreso para ver el archivo de imagen

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

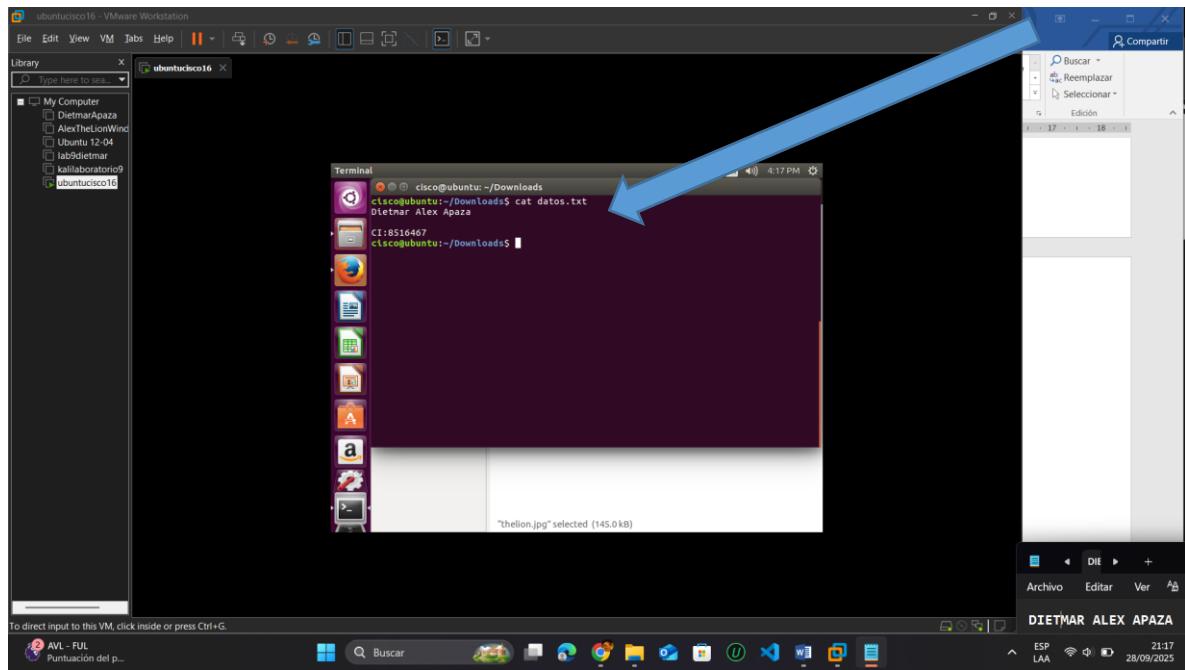


Creamos un archivo.txt con el el siguiente comando: nano datos.txt

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



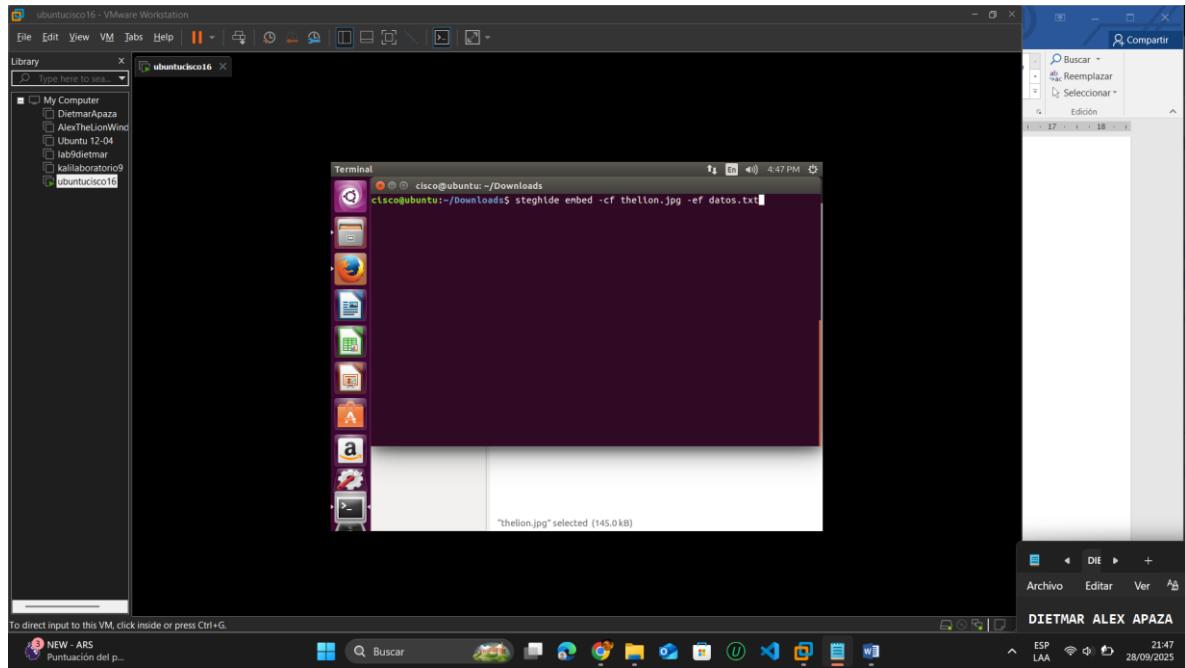
Para verificar ingresamos el código de: cat datos.txt

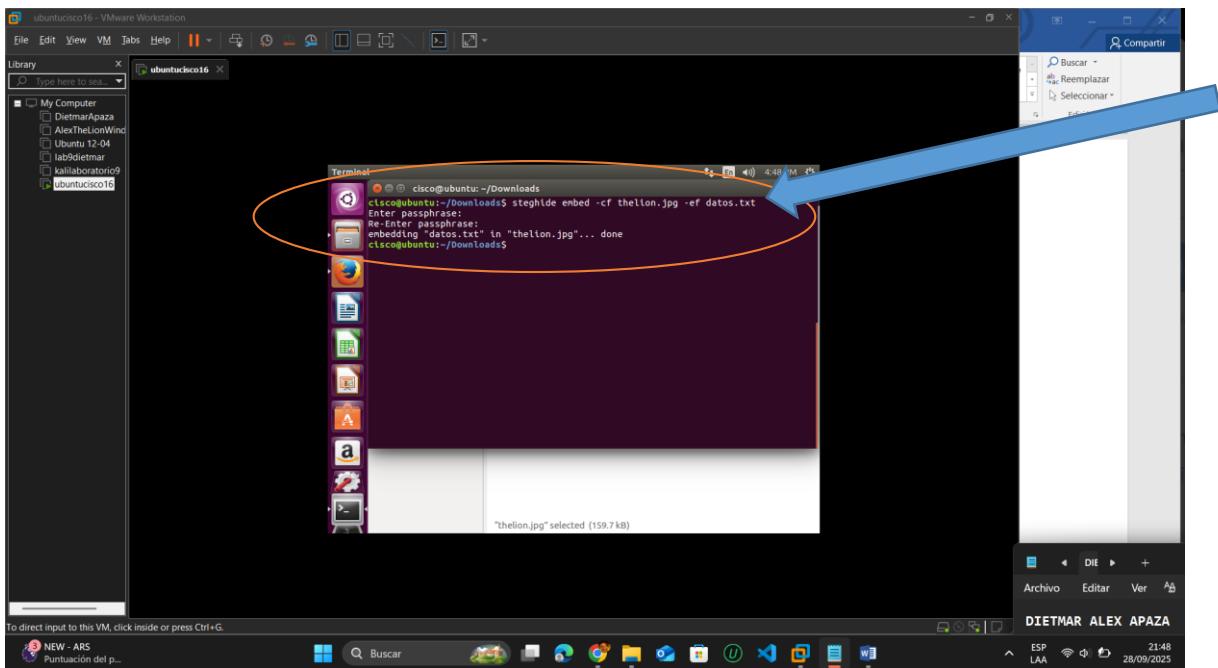


En la petición de ingreso de comando, introduzca el siguiente comando:

```
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.





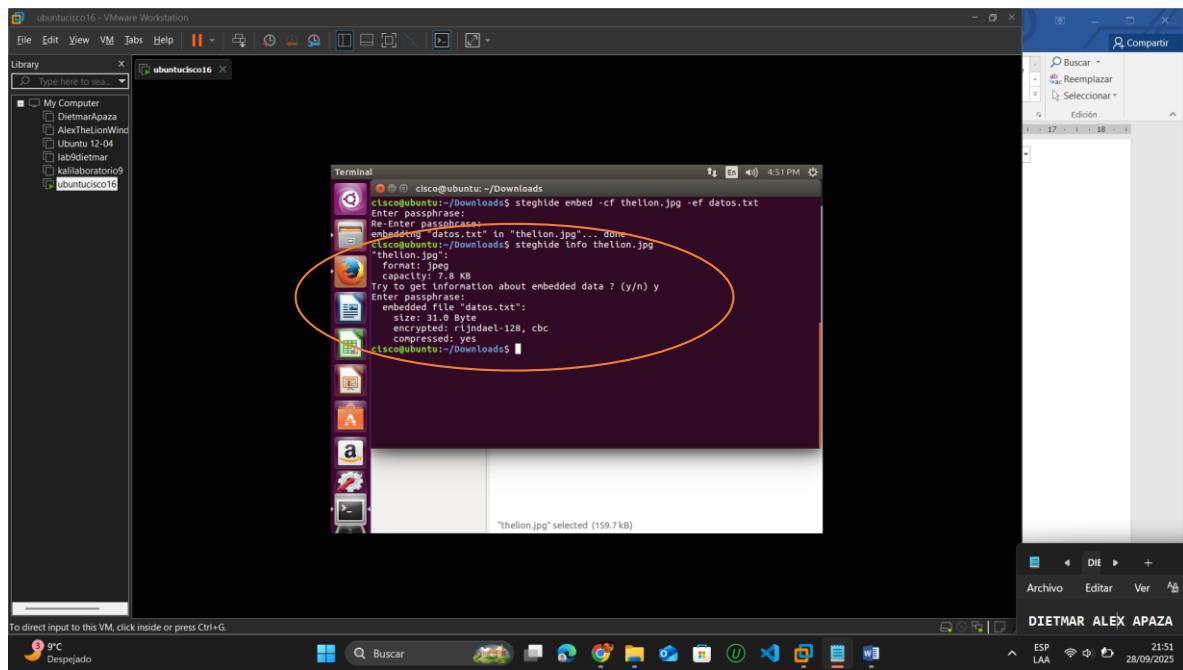
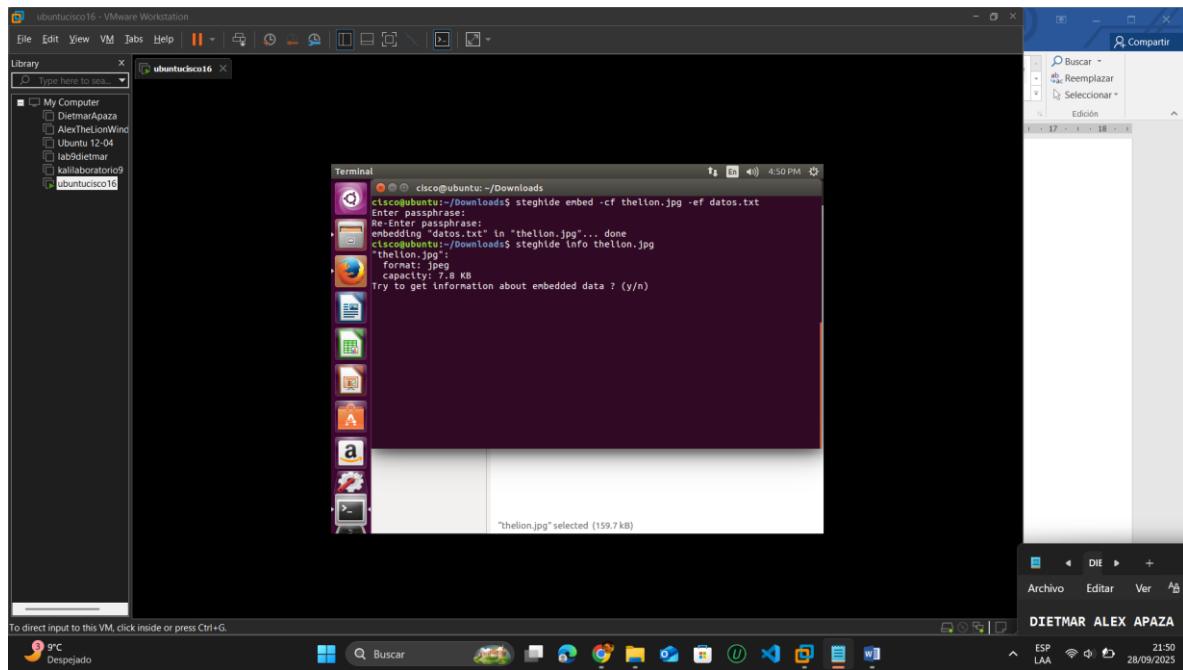
## Verificar el archivo oculto.

Escriba el siguiente comando en el terminal.

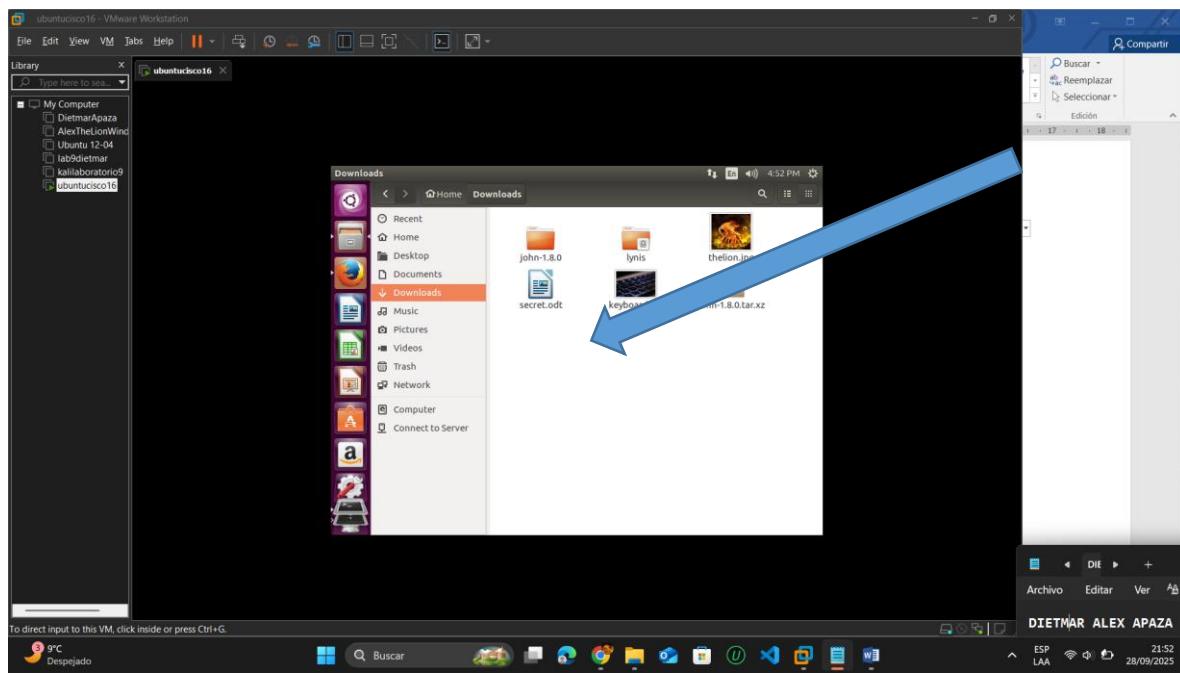
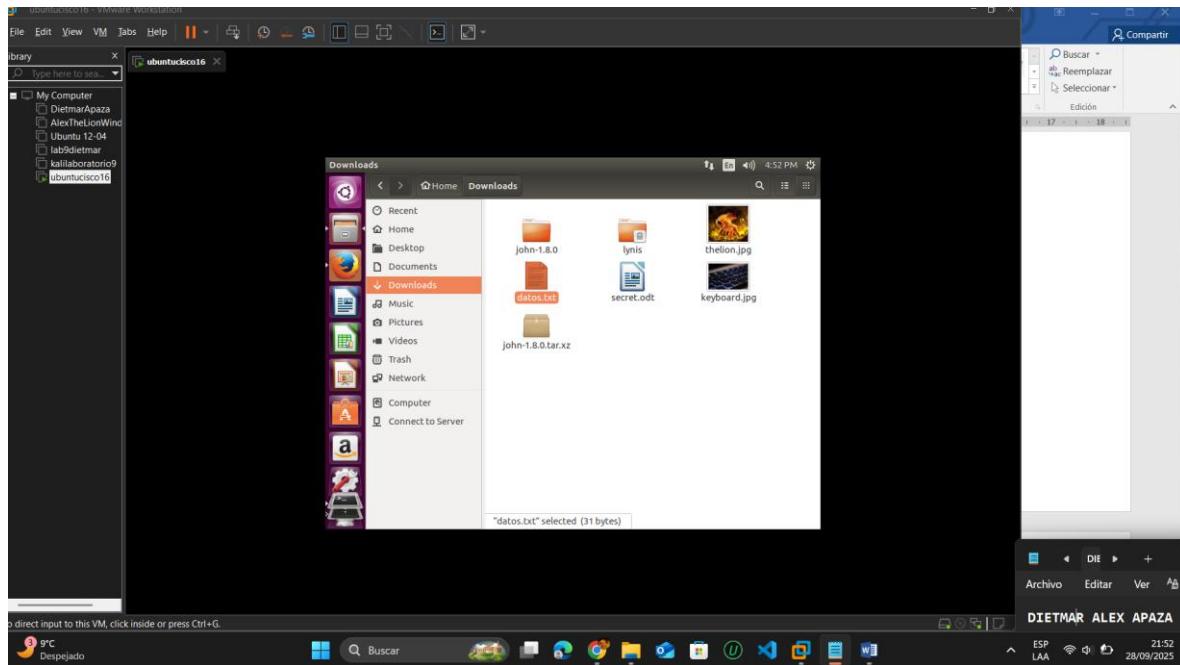
```
cisco@ubuntu:~/Downloads$ steghide info thelion.jpg
```

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.



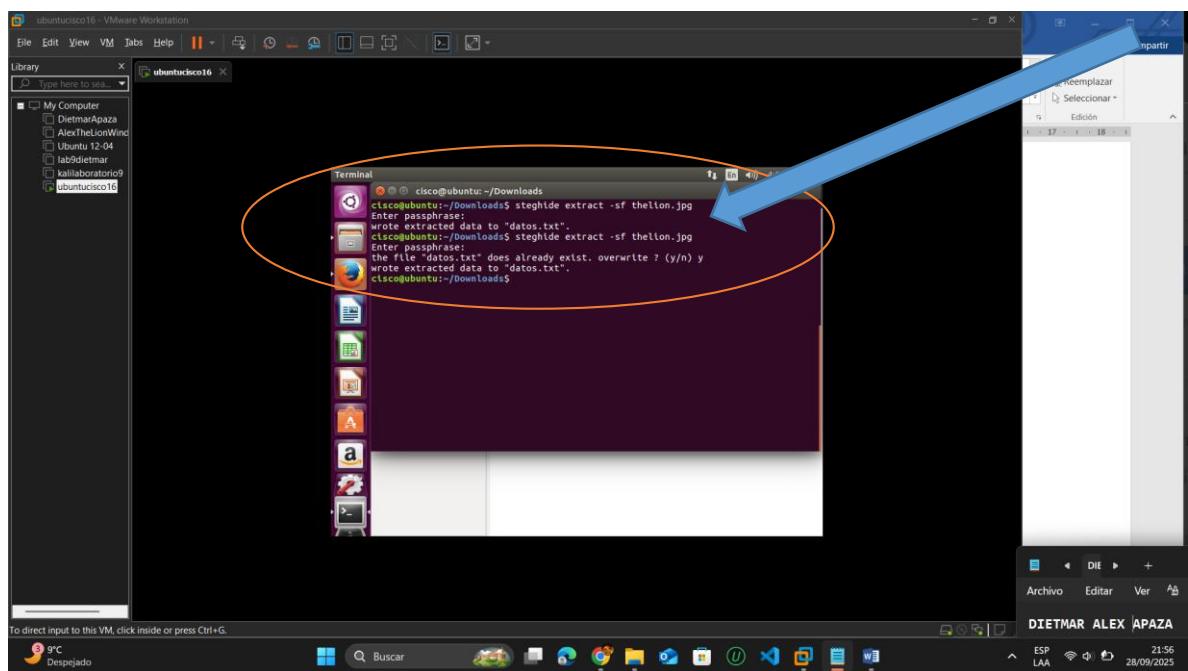
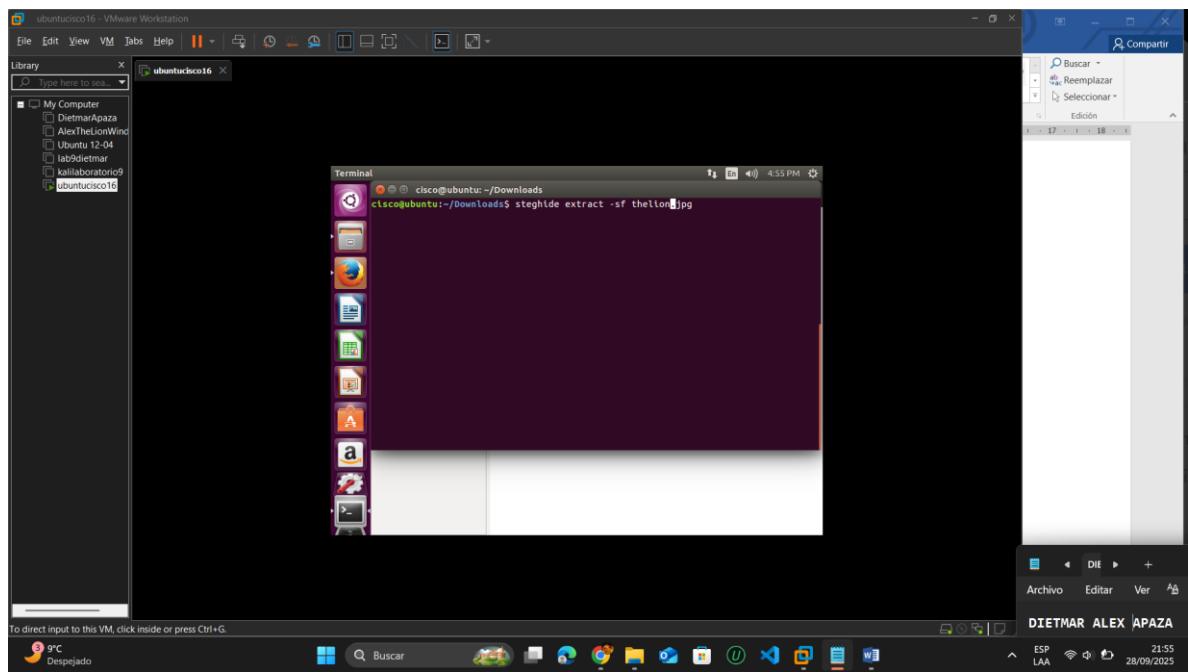
## Extraiga el archivo oculto.

Escriba el siguiente comando en el terminal.

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

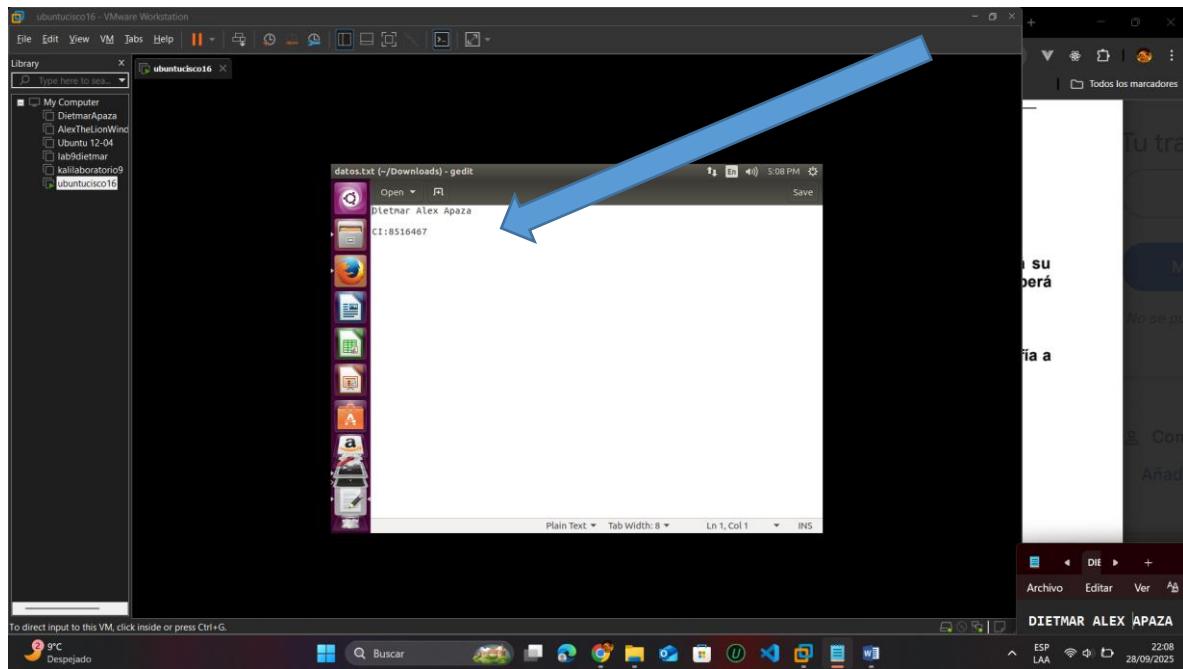
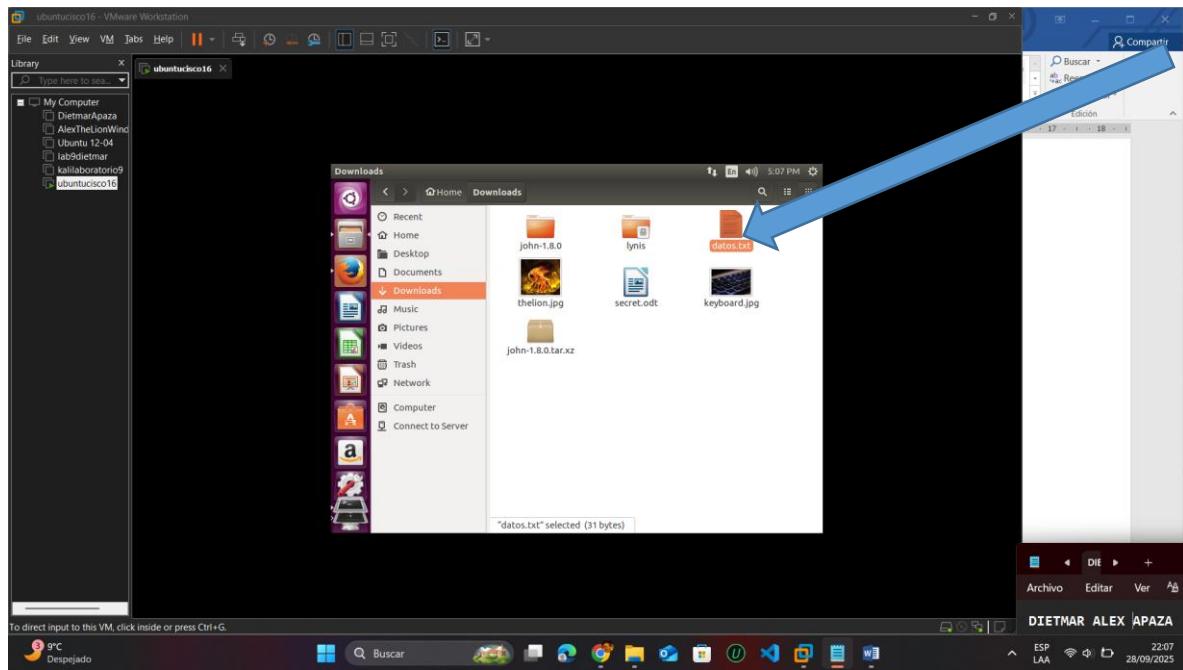
Ingresamos la contraseña: **sistemas204s2**

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.



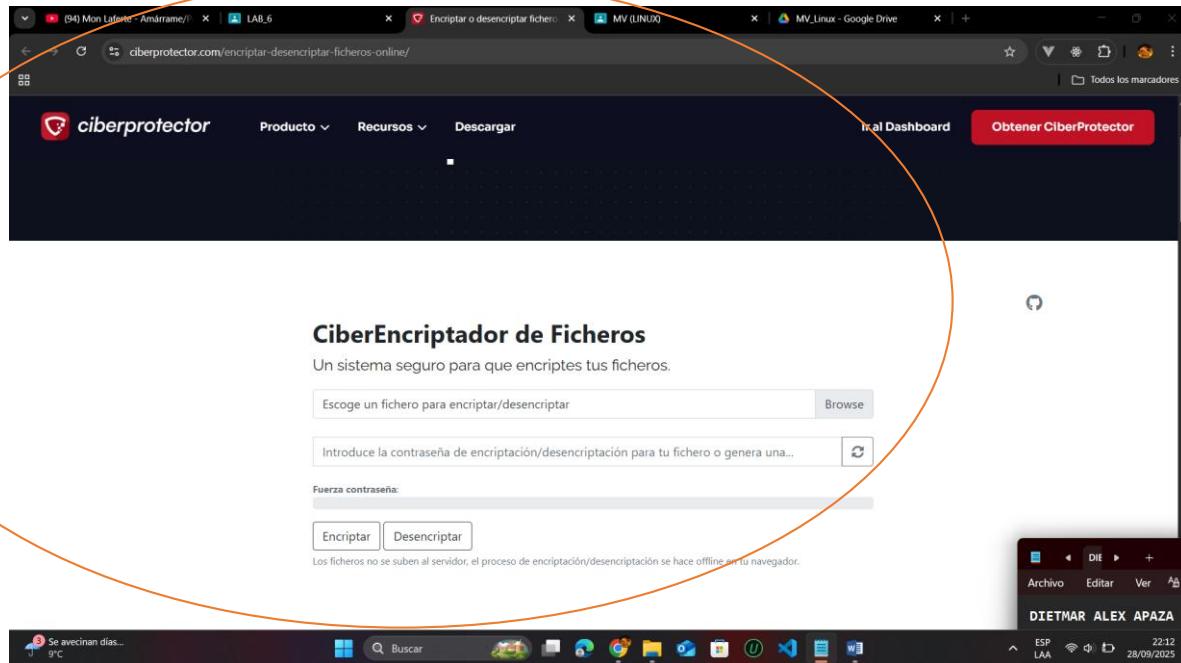
**2.- Realice la demostración para cifrar/descrifrar un archivo, un mensaje en texto plano y la esteganografía a una imagen. Utilice las siguientes webs para ello**

### **1.- Encriptar y desencriptar archivos**

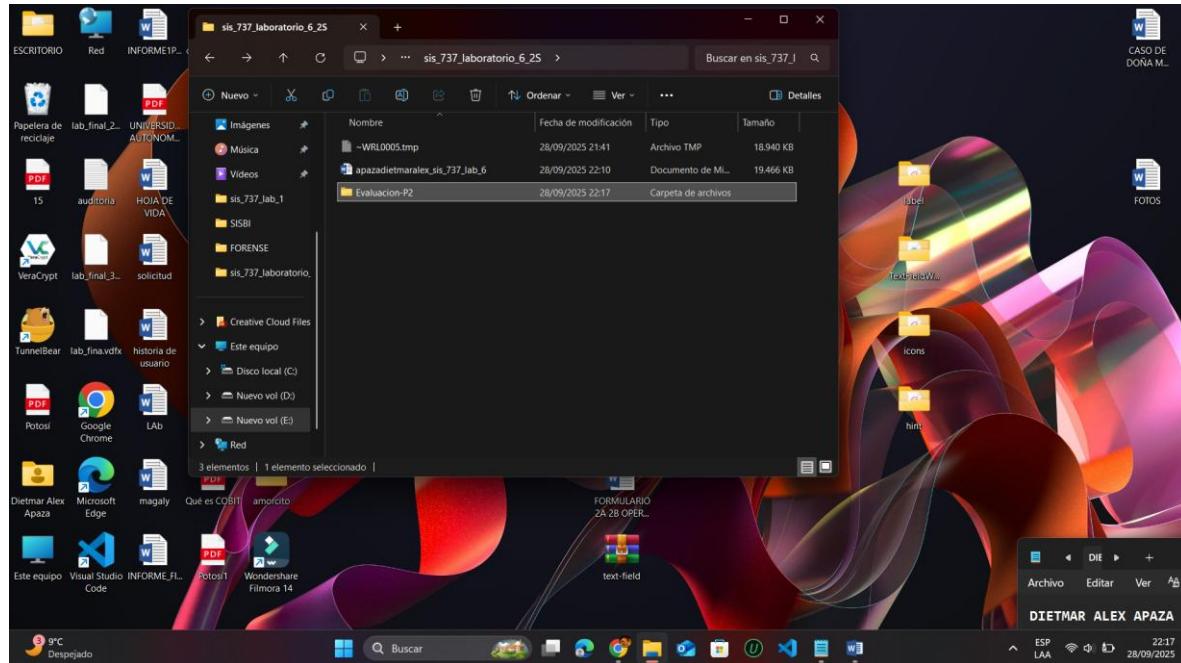
<https://ciberprotector.com/encryptar-desencriptar-ficheros-online/>

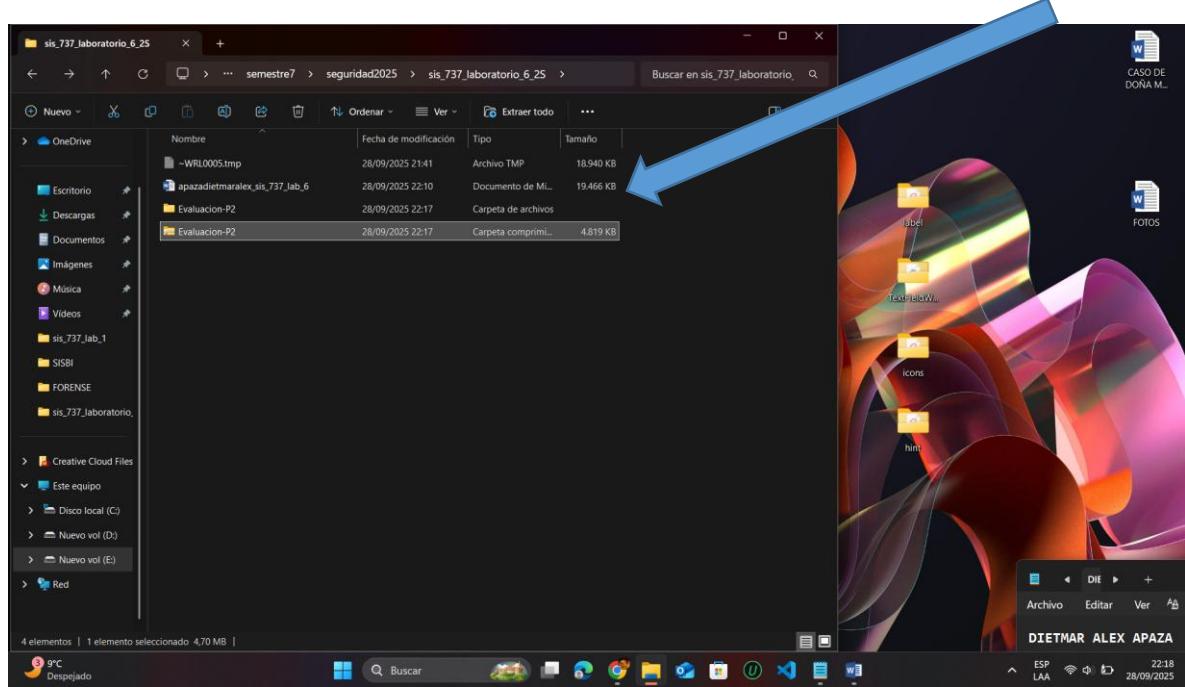
## Encriptar archivo

Ingresamos al link para realizar la encriptación de un archivo

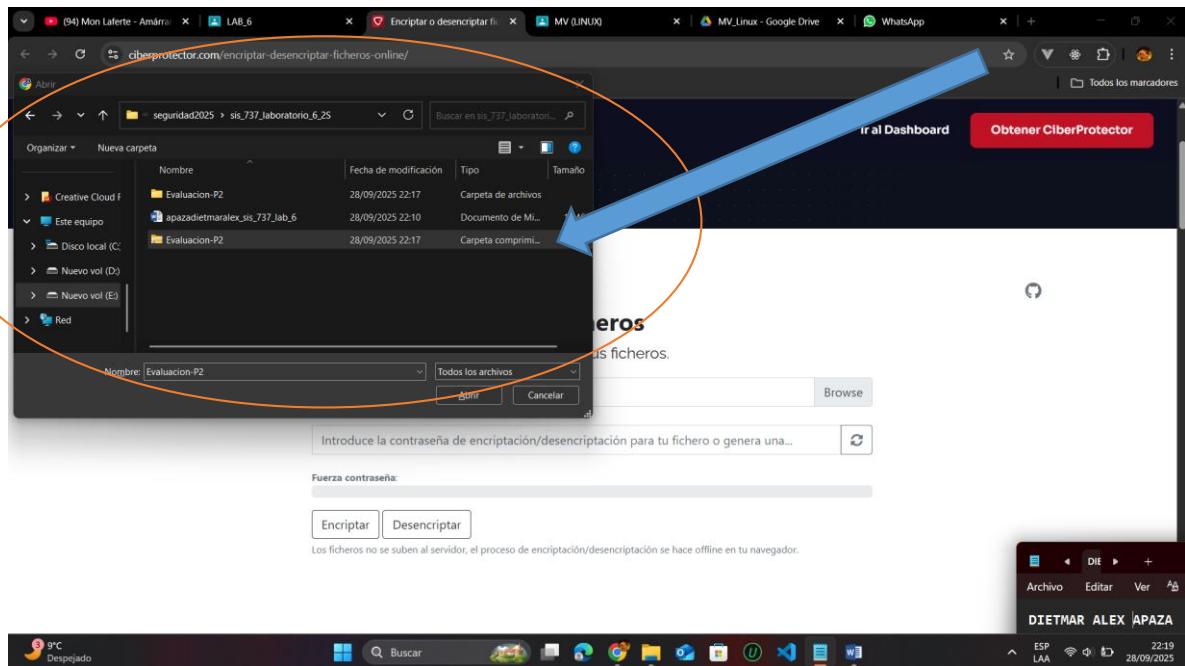


Creamos un archivo llamado “Evaluacion-P2” y lo convertimos en un archivo.ZIP dentro del archivo se encontrara documentos que deseamos encriptar.

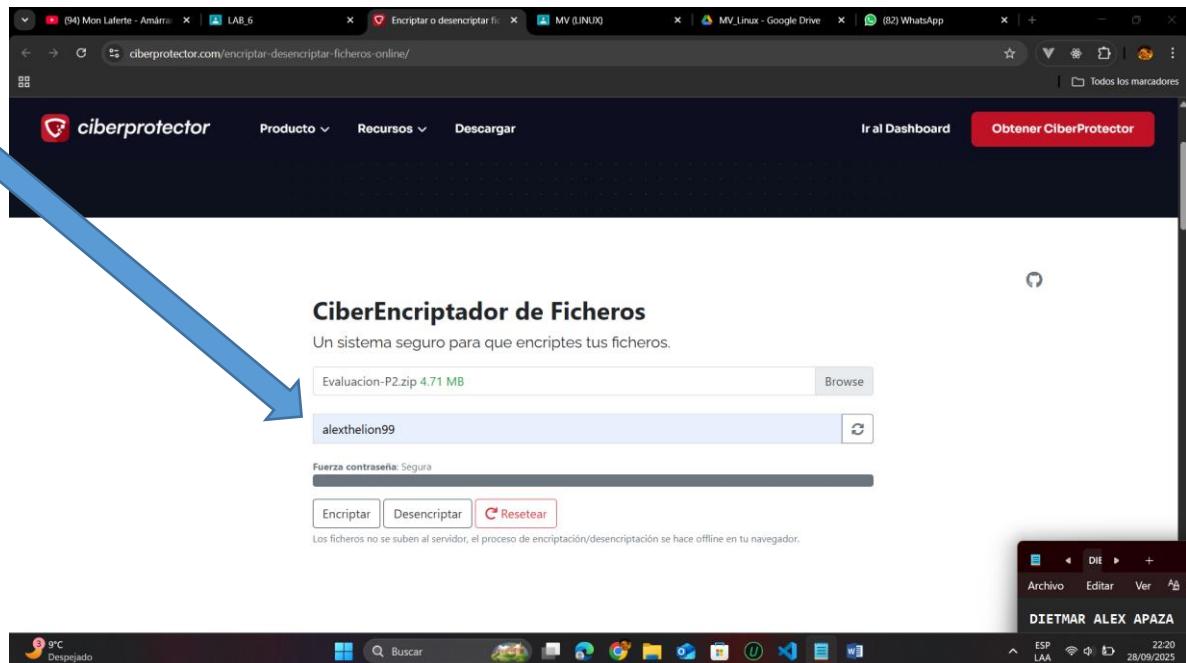




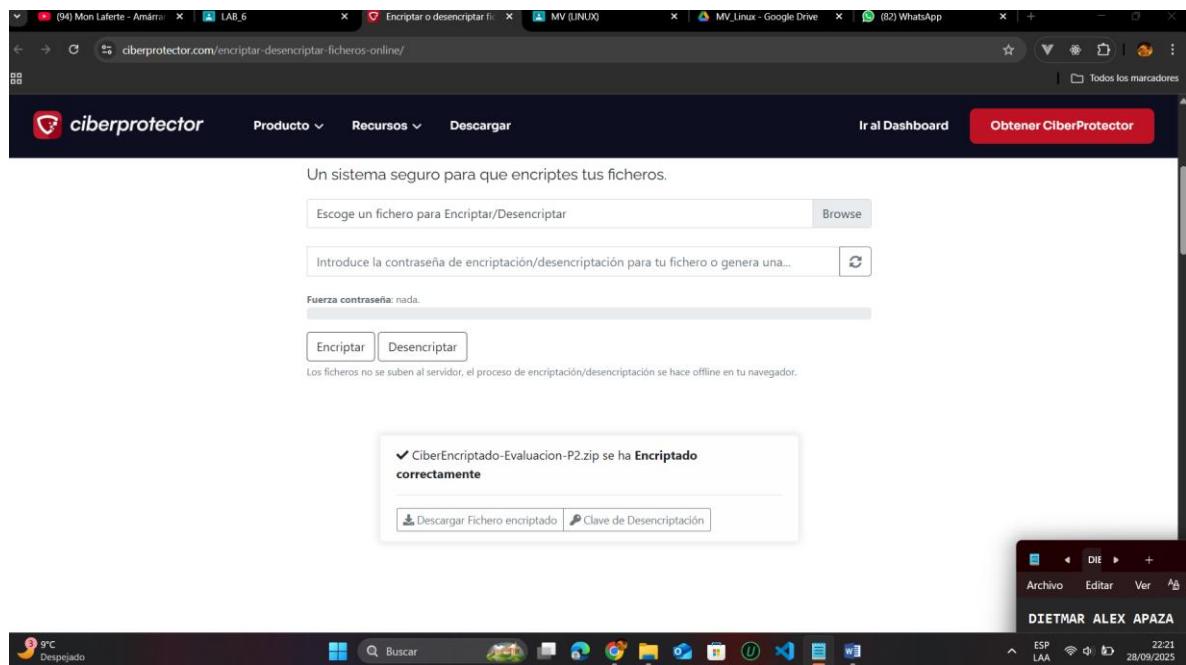
Sube el archivo Evaluacion-P2.ZIP



Establece una contraseña segura: alexthelion99

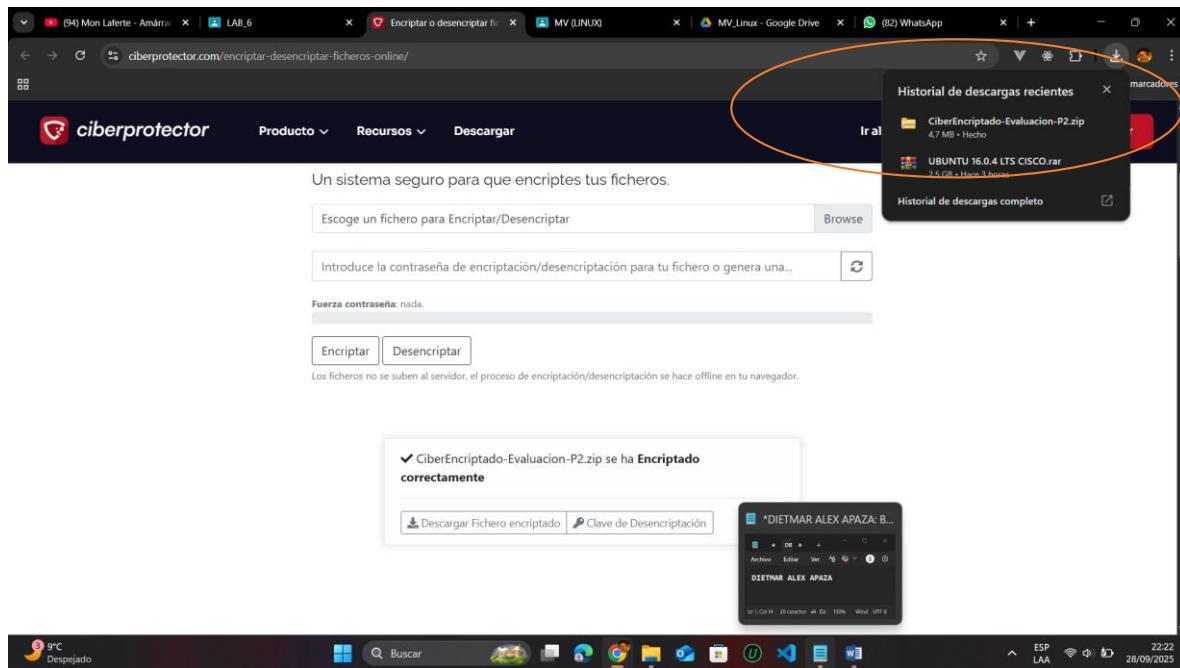


The screenshot shows the CiberEncryptador de Ficheros interface. A large blue arrow points from the top left towards the interface. The interface has a dark header with the Ciberprotector logo and navigation links. Below the header, there's a section for "CiberEncryptador de Ficheros" with a subtext "Un sistema seguro para que encriptes tus ficheros.". A file input field contains "Evaluacion-P2.zip 4.71 MB" and a password input field contains "alexthelion99". A progress bar indicates "Fuerza contraseña: Segura". At the bottom are "Encriptar", "Desencriptar", and "Resetear" buttons. A note at the bottom states: "Los ficheros no se suben al servidor, el proceso de encriptación/desencriptación se hace offline en tu navegador." The taskbar at the bottom shows various open windows and system icons.

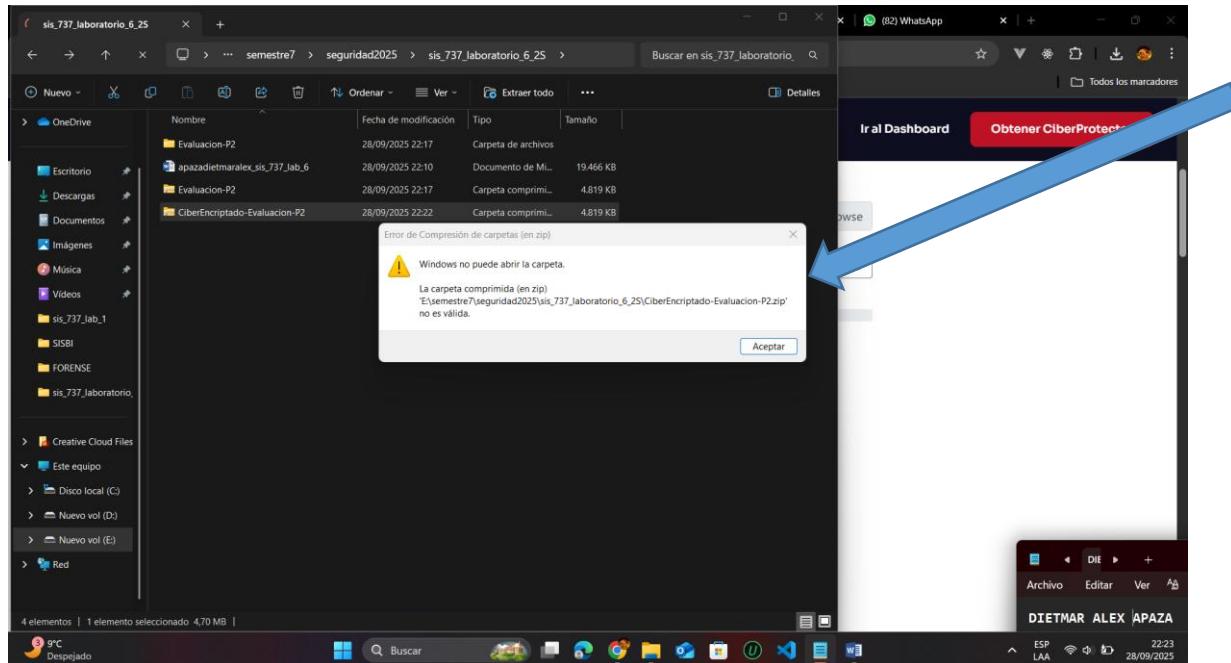
  


This screenshot shows the same interface after the file has been encrypted. A message box in the center says: "✓ CiberEncryptado-Evaluacion-P2.zip se ha **Encriptado** correctamente". Below it are two buttons: "Descargar Fichero encriptado" and "Clave de Desencriptación". The taskbar at the bottom remains the same as in the previous screenshot.

Descarga el archivo encryptado.

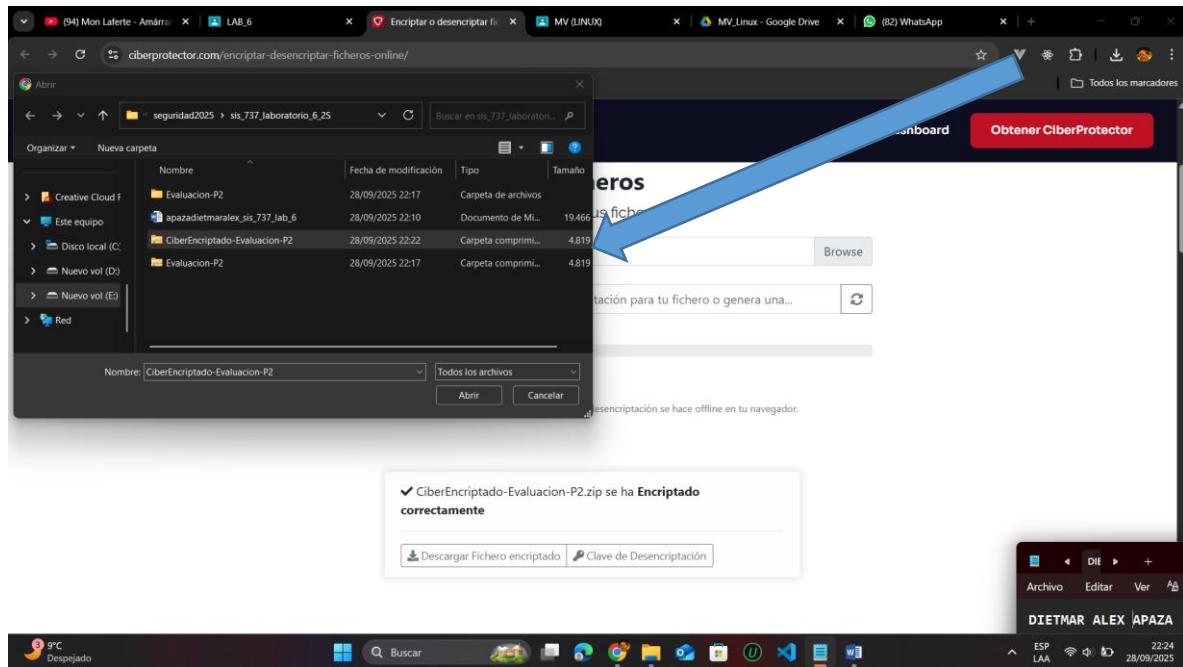


Una vez descargado el archivo encriptado ya no es el resultado esperado como se muestra en la imagen

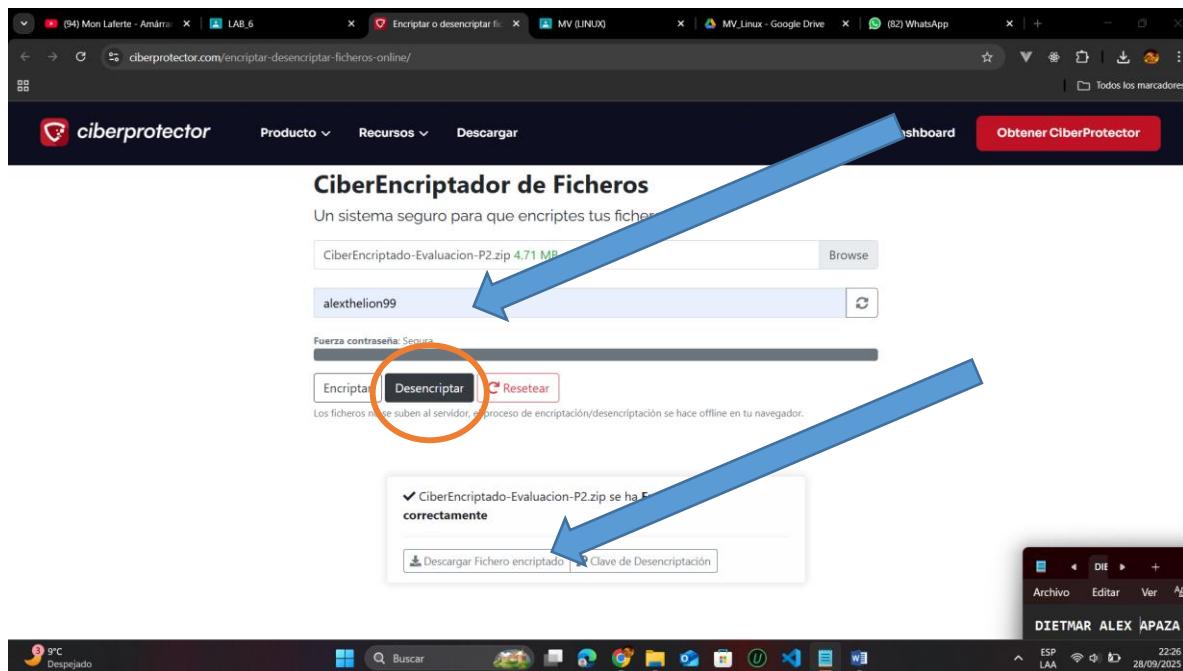


## Desencriptar archivo

Para desencriptar el archivo subimos el archivo que encriptamos anteriormente.



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

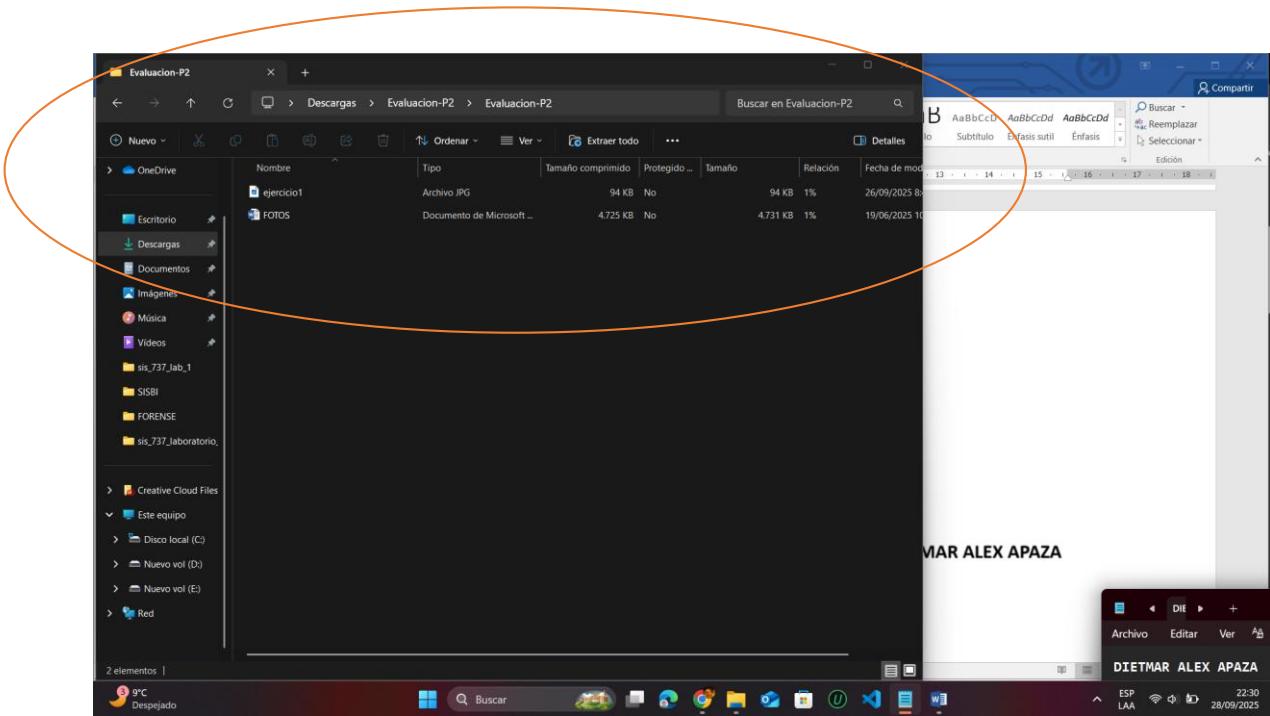


Una ves desencriptado procedemos a descargar el archivo y verificar si esta correctamente solucionado.

The screenshot shows a Windows desktop environment with several open windows:

- CiberProtector Website:** A browser window displaying the CiberProtector website at <https://ciberprotector.com/encryptar-desencriptar-ficheros-online/>. The page shows two successful operations:
  - Evaluacion-P2.zip se ha **Desencriptado correctamente**. A "Descargar Fichero Desencriptado" button is present.
  - CiberEncriptado-Evaluacion-P2.zip se ha **Encriptado correctamente**. A "Descargar Fichero encriptado" and "Clave de Desencriptación" button are present.
- Task Manager:** A small window titled "DIE" showing system status: DIETMAR ALEX APAZA, ESP, LAA, 22:27, 28/09/2025.
- File Explorer:** A window titled "Evaluacion-P2" showing the contents of a folder. The folder contains one item: "Evaluacion-P2" (Carpeta de archivos). The file list table has columns: Nombre, Tipo, Tamaño comprimido, Protegido..., Tamaño, Relación, and Fecha de mod. The date 28/09/2025 is visible.
- Task Manager:** Another small window titled "DIE" showing system status: DIETMAR ALEX APAZA, ESP, LAA, 22:29, 28/09/2025.

Resultado de la desencriptacion.



## 2.- Encriptar y desencriptar texto

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

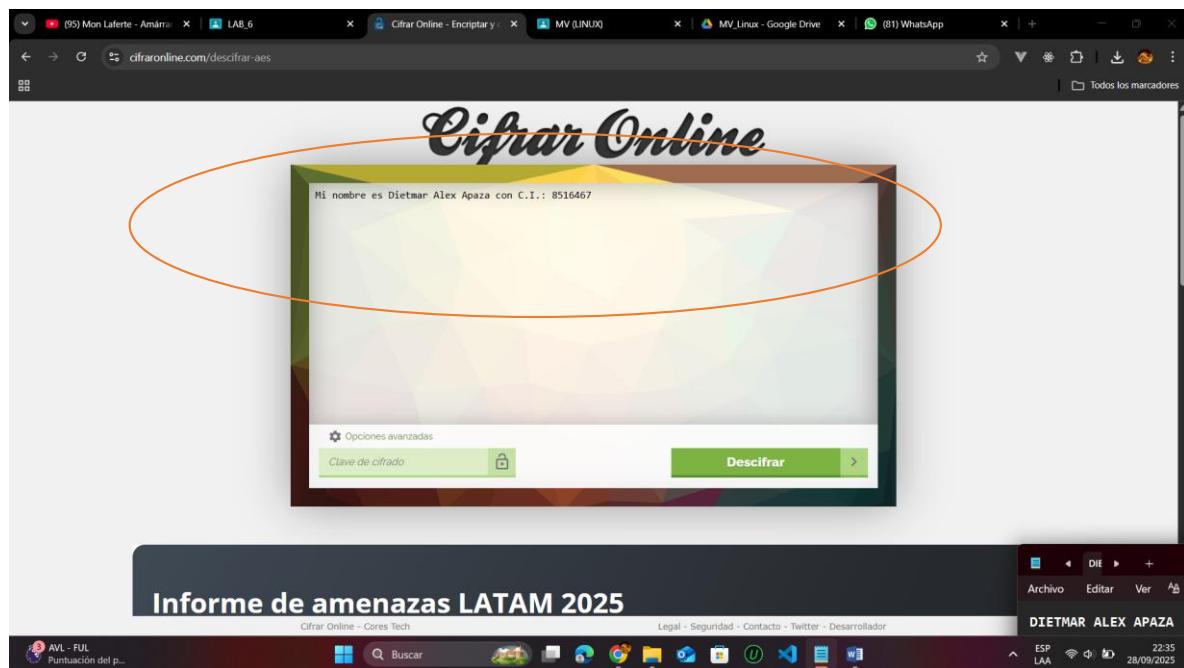
Primero ingresamos al link para poder realizar el desafío.

A screenshot of a web browser displaying the 'Cifrar Online' website. The URL in the address bar is 'https://cifraronline.com/descifrar-aes'. The main content area shows a large input field for text and a green 'Descifrar' button. Below the input field is a green button labeled 'Clave de cifrado'. The status bar at the bottom of the browser window displays the user's name 'DIETMAR ALEX APAZA'.

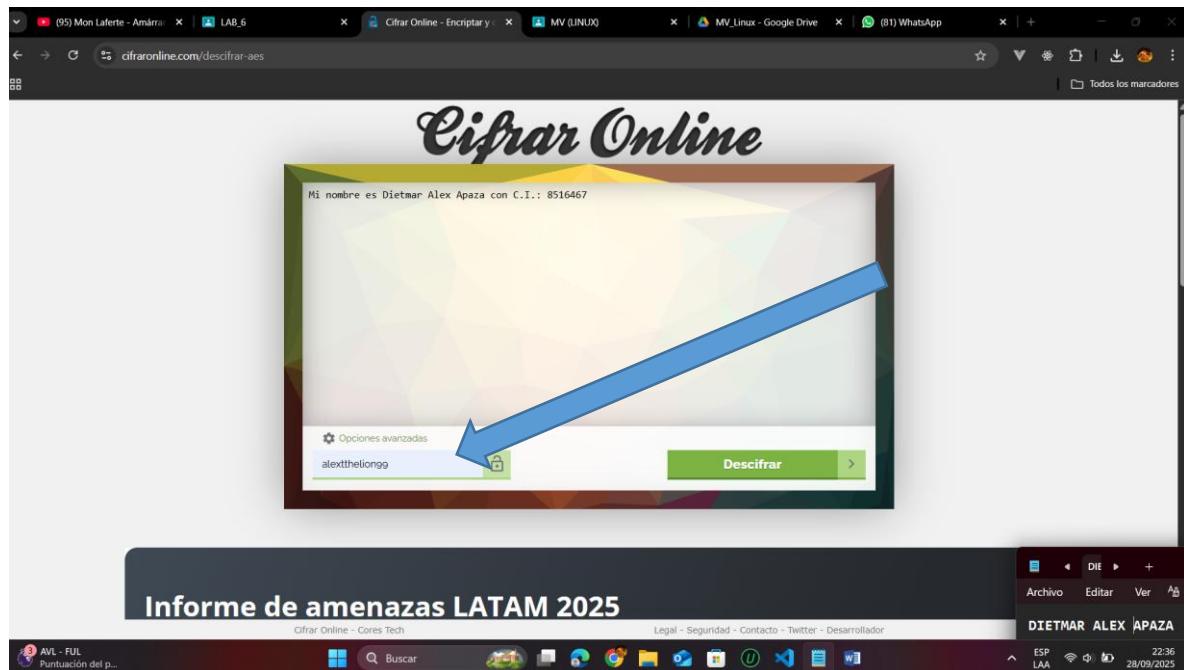
Pasos para Encriptar:

Seleccionar la opción "**Encriptar**".

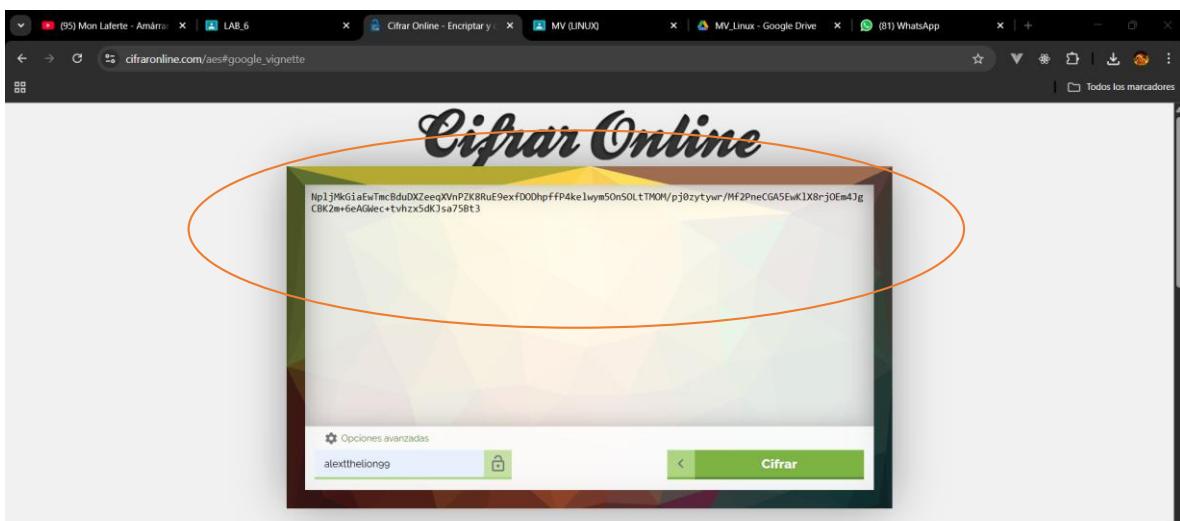
En el campo de **Texto plano**, escribir el mensaje que deseas cifrar.



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:

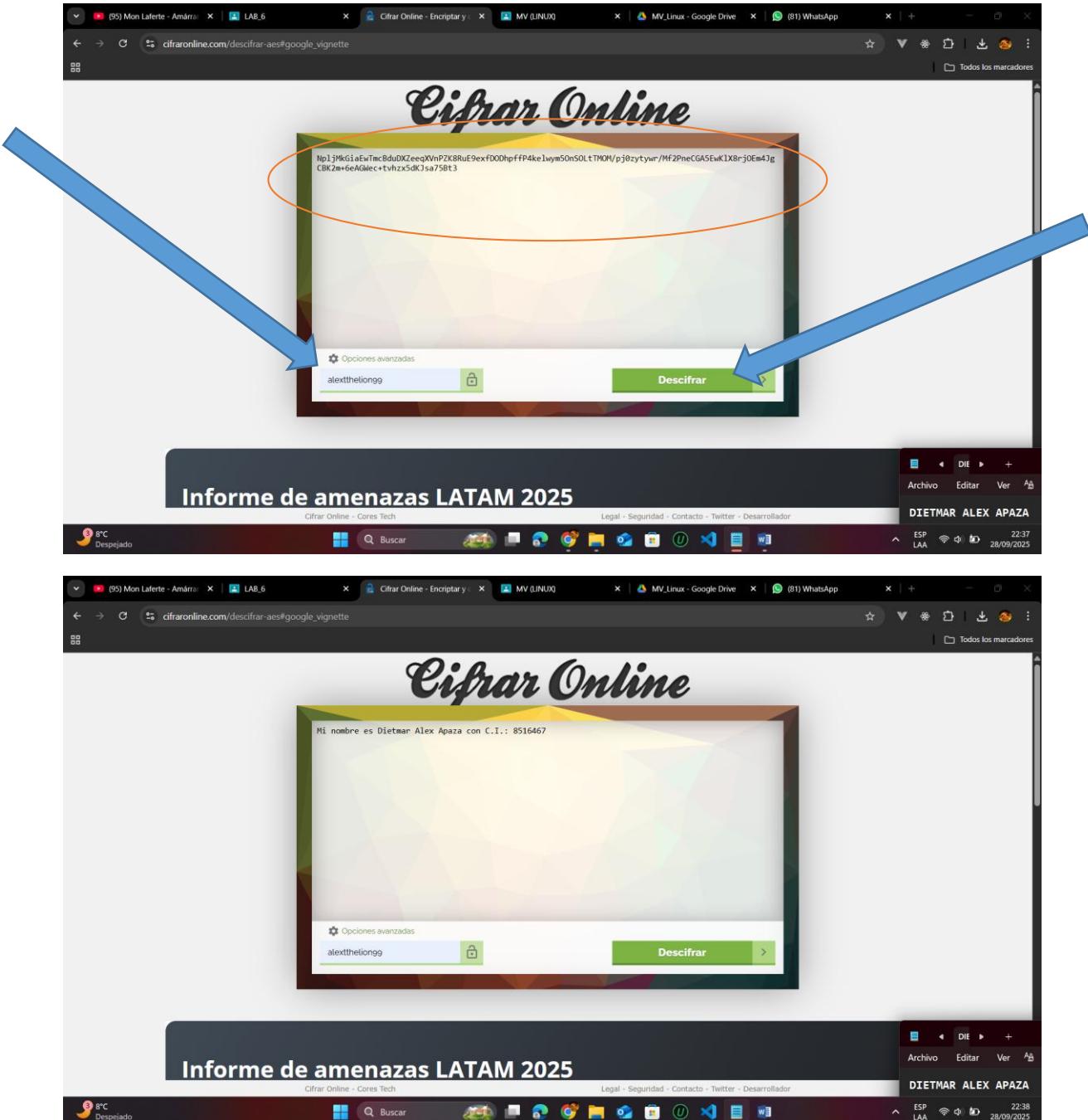
Seleccionar la opción "**Desencriptar**" en el mismo sitio.

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)



#### Steganographic Encoder

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU audio file. The changes to the file should be invisible to any casual observer. Once you submit, you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this may fail silently. You may wish to find the capacity of the file below before embedding data in it.

Select a JPEG, AU or WAV file to upload:

Seleccionar archivo Ningún archivo seleccionado

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):

Just find capacity of this file

Text

File payload  Seleccionar archivo Ningún archivo seleccionado

Once you've encoded, try to [decode a file](#), or [compare the differences](#) between your original file and the file you've just decoded.

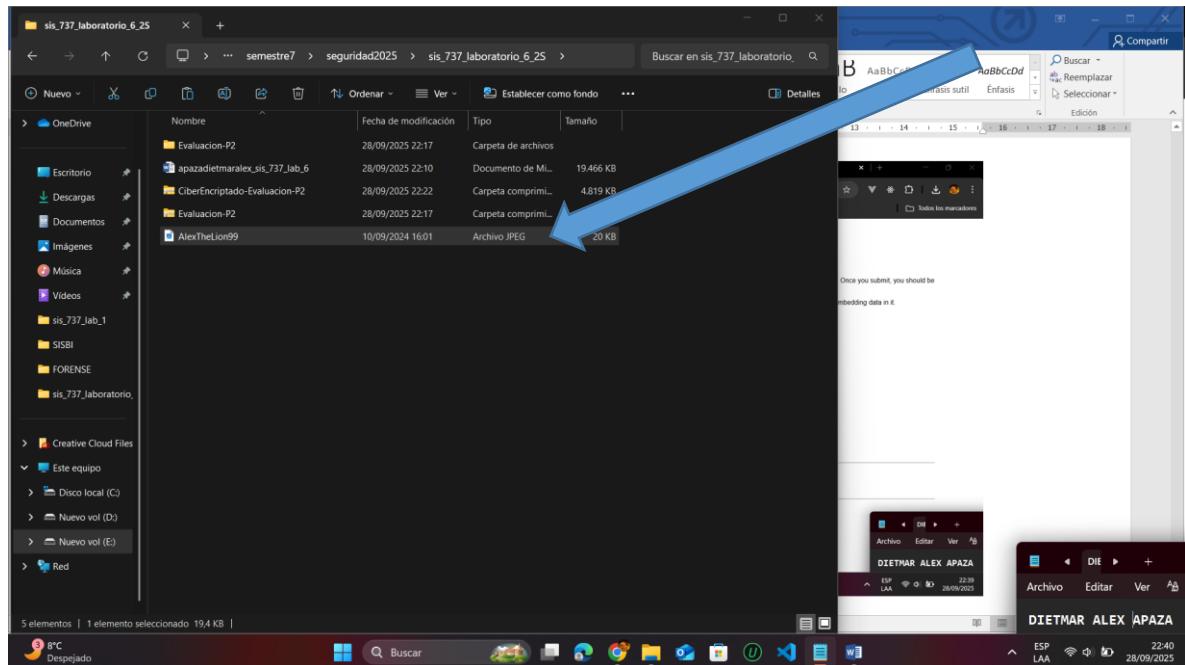
These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)

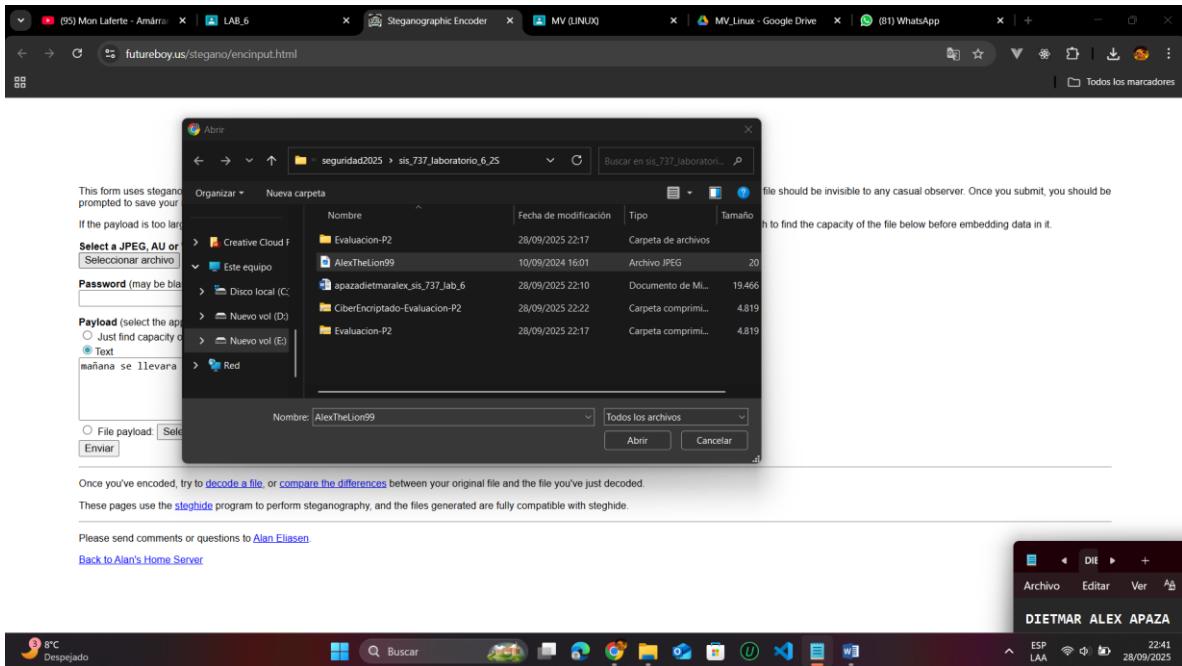
[Back to Alan's Home Server](#)



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

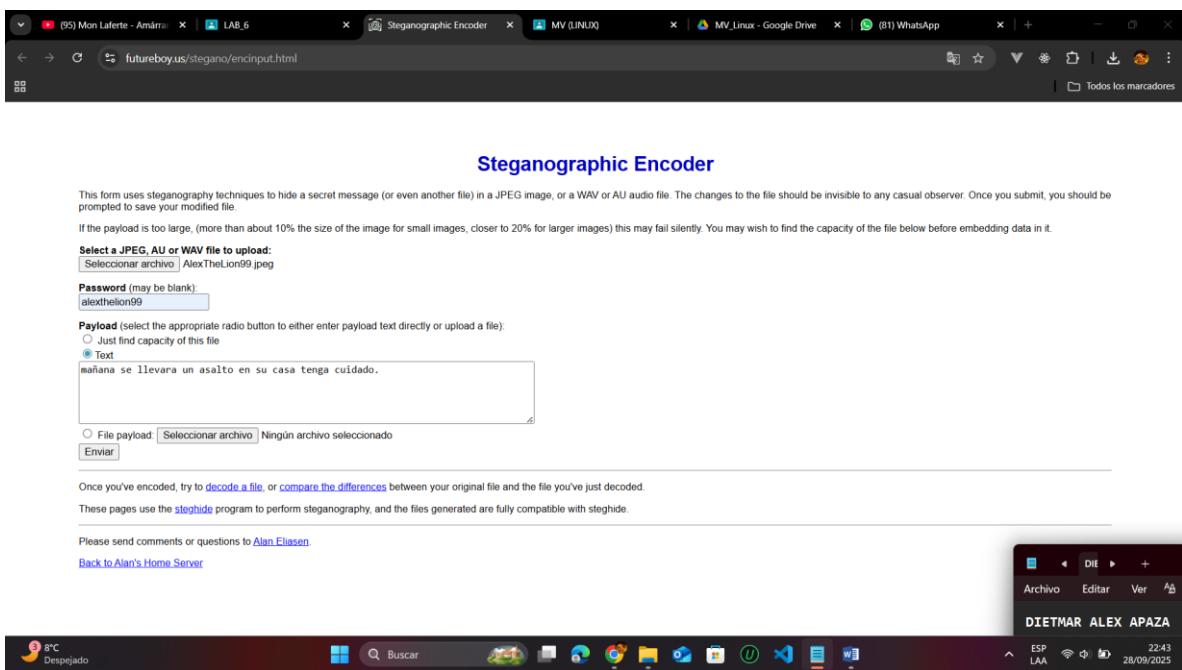


Primeramente añadimos el archivo



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

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



Hacer clic en "**Enviar**".

**Steganographic Encoder**

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU audio file. The changes to the file should be invisible to any casual observer. Once you submit, you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this may fail silently. You may wish to find the capacity of the file below before embedding data in it.

Select a JPEG, AU or WAV file to upload:  
 Seleccionar archivo | AlexTheLion99.jpeg

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):  
 Just find capacity of this file  
 Text

File payload:  Ningún archivo seleccionado

Once you've encoded, try to [decode a file](#), or [compare the differences](#) between your original file and the file you've just decoded.  
 These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)  
[Back to Alan's Home Server](#)

DIETMAR ALEX APAZA

Descargar la imagen resultante con el mensaje oculto incrustado.

**Steganographic Encoder**

This form uses steganography techniques to hide a secret message (or even another file) in a JPEG image, or a WAV or AU audio file. The changes to the file should be invisible to any casual observer. Once you submit, you should be prompted to save your modified file.

If the payload is too large, (more than about 10% the size of the image for small images, closer to 20% for larger images) this may fail silently. You may wish to find the capacity of the file below before embedding data in it.

Select a JPEG, AU or WAV file to upload:  
 Seleccionar archivo | AlexTheLion99.jpeg

Password (may be blank):

Payload (select the appropriate radio button to either enter payload text directly or upload a file):  
 Just find capacity of this file  
 Text

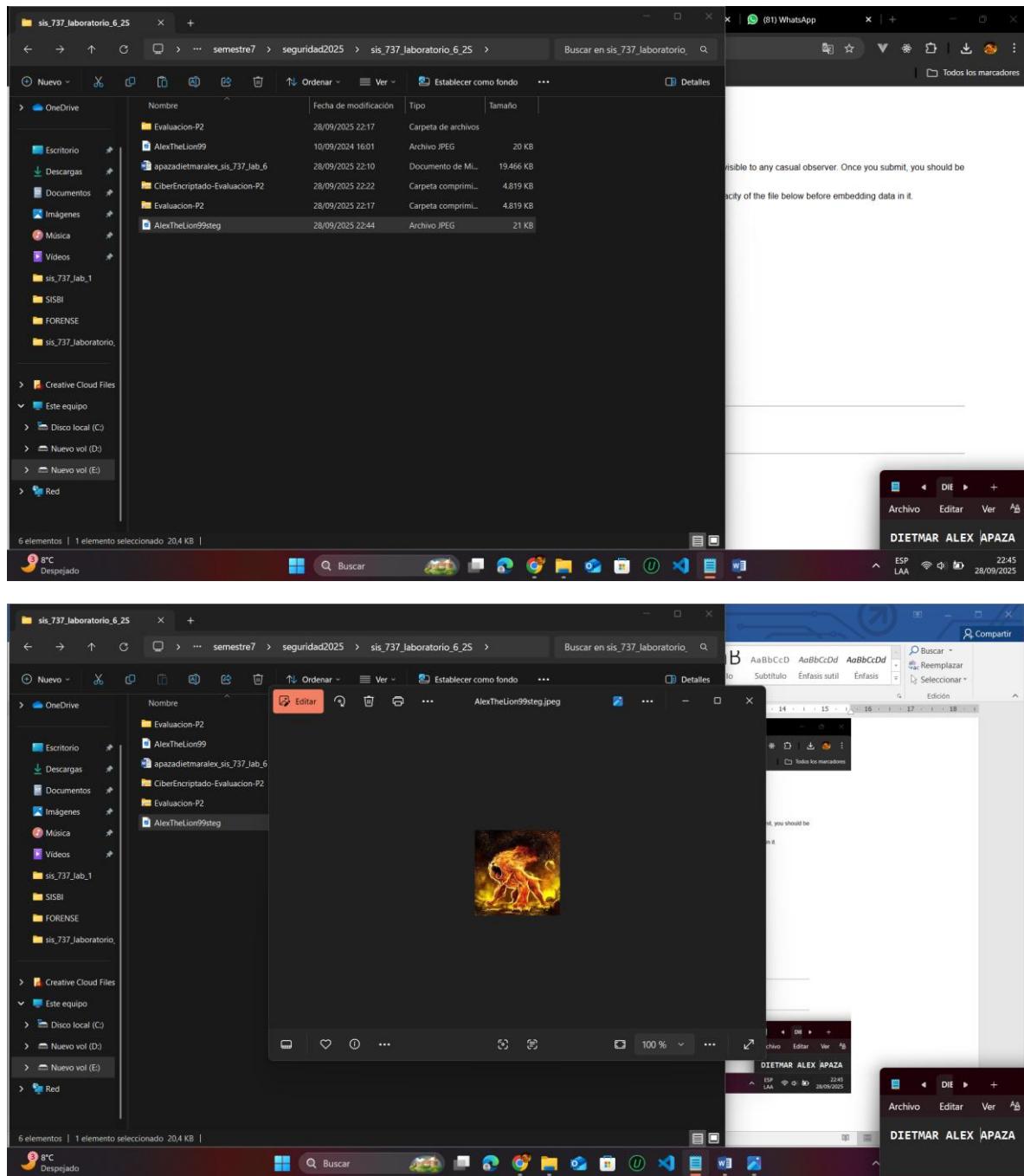
File payload:  Ningún archivo seleccionado

Once you've encoded, try to [decode a file](#), or [compare the differences](#) between your original file and the file you've just decoded.  
 These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)  
[Back to Alan's Home Server](#)

DIETMAR ALEX APAZA

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)



## Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Seleccionar archivo | Ningún archivo seleccionado

Password (may be blank):

View raw output as MIME-type: text/plain

Guess the payload

Prompt to save (you must guess the file type yourself.)

Enviar

To use this form, you must first [encode a file](#).

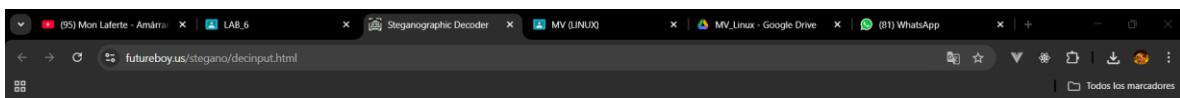
These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)

[Back to Alan's Home Server](#)



Subir la imagen que tiene el mensaje oculto.



## Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Seleccionar archivo | Ningún archivo seleccionado

Password (may be blank):

View raw output as MIME-type: text/plain

Guess the payload

Prompt to save (you must guess the file type yourself.)

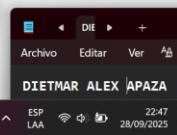
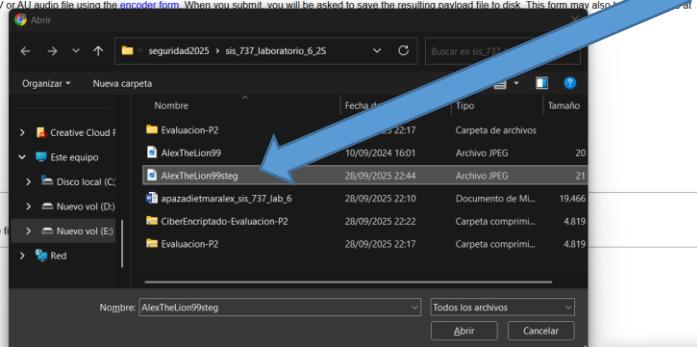
Enviar

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)

[Back to Alan's Home Server](#)



Ingresar la clave de codificación si se usó una.



## Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Seleccionar archivo | AlexTheLion99steg.jpeg

Password (may be blank):

alexthelion99

View raw output as MIME-type: text/plain

Guess the payload

Prompt to save (you must guess the file type yourself.)

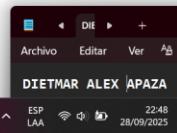
Enviar

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)

[Back to Alan's Home Server](#)



Hacer clic en "Enviar".



## Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Seleccionar archivo | AlexTheLion99steg.jpeg

Password (may be blank):

alexthelion99

View raw output as MIME-type: text/plain

Guess the payload

Prompt to save (you must guess the file type yourself.)

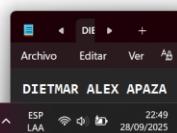
Enviar

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#)

[Back to Alan's Home Server](#)



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

