

## **PRACTICA\_01\_SEGURIDAD DE SISTEMAS**

Nombre: Jacob Santos Ayaviri Condori

C.I. 13229452



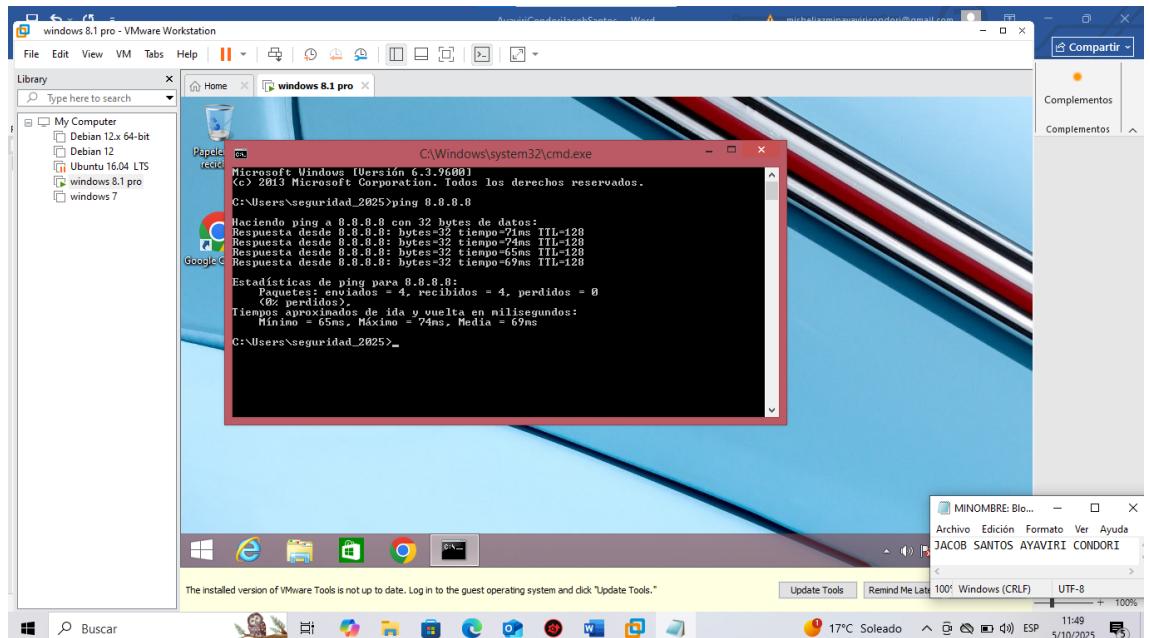
Git hub

Name: Ayaviri\_Condori\_Jacob\_Santos

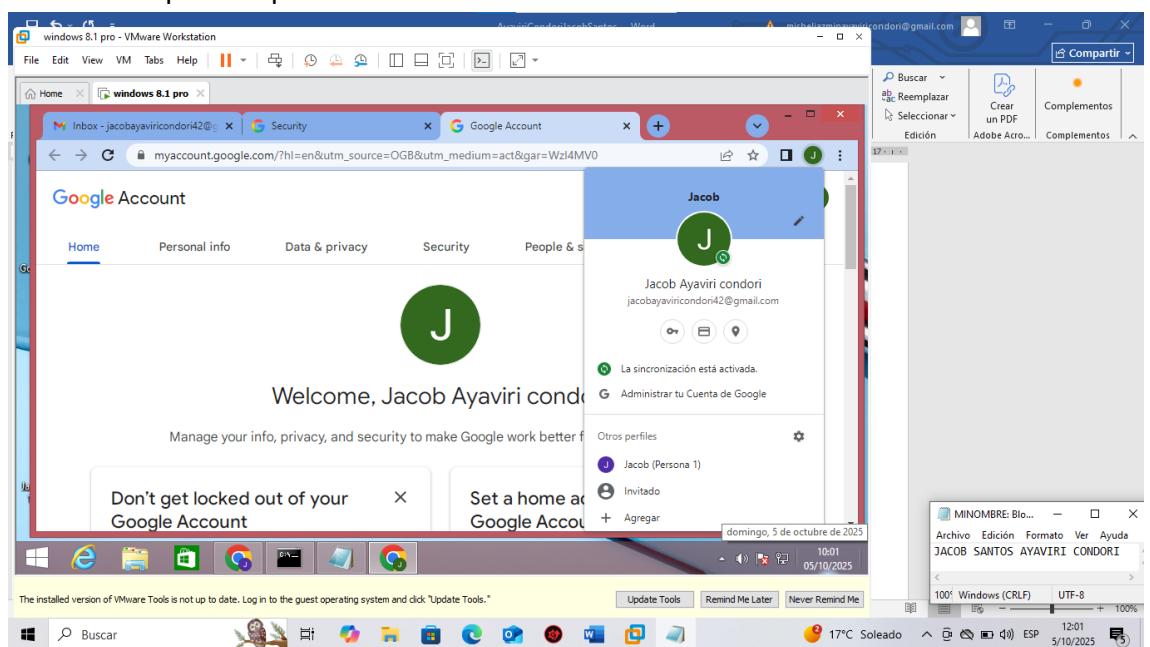
Link: [https://github.com/jacob-santos-0/Practica\\_01\\_seguridad\\_1\\_2025.git](https://github.com/jacob-santos-0/Practica_01_seguridad_1_2025.git)

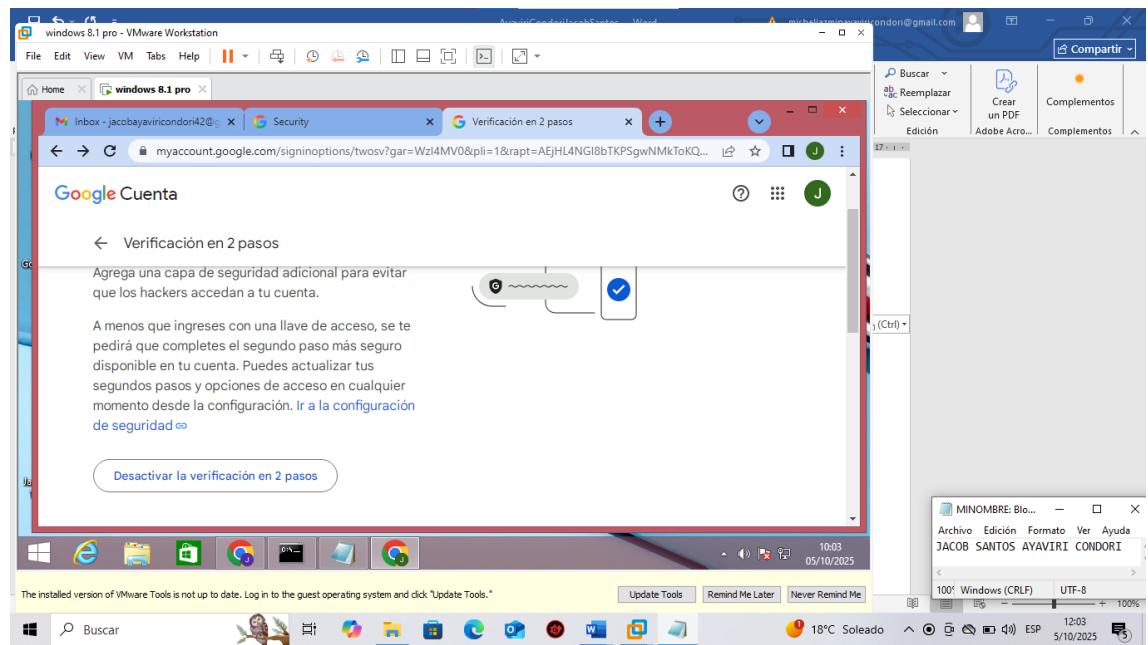
## MODIFICAR PARAMETROS DEL CORREO

### 1. Conexión a internet

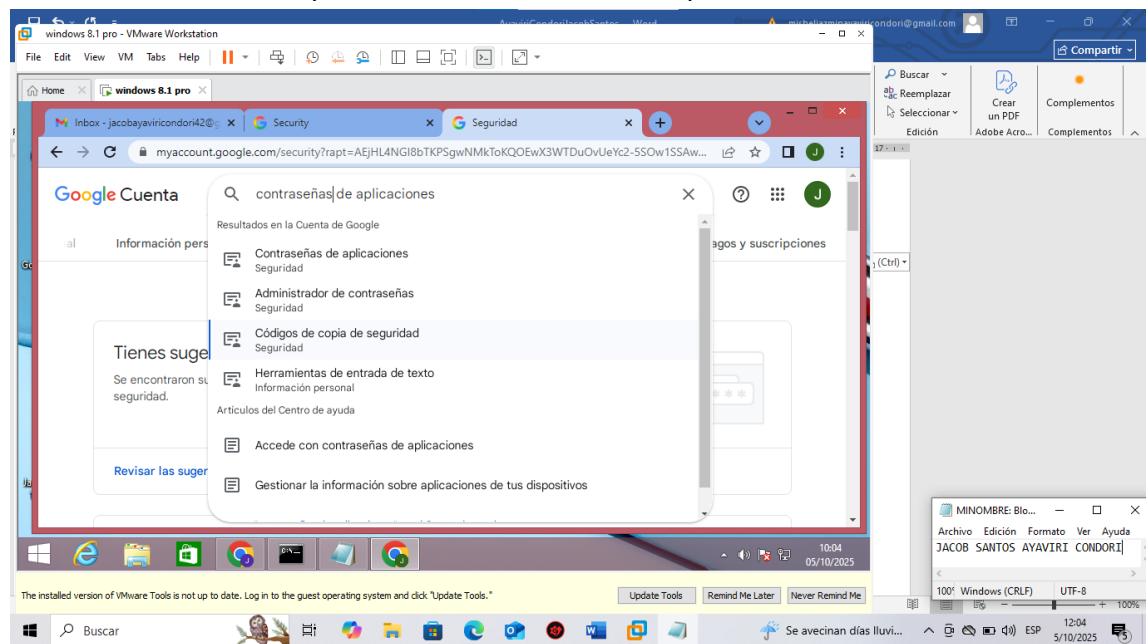


### 2. Ir a administración de tu cuenta Google, luego a seguridad y activamos la verificación por dos pasos

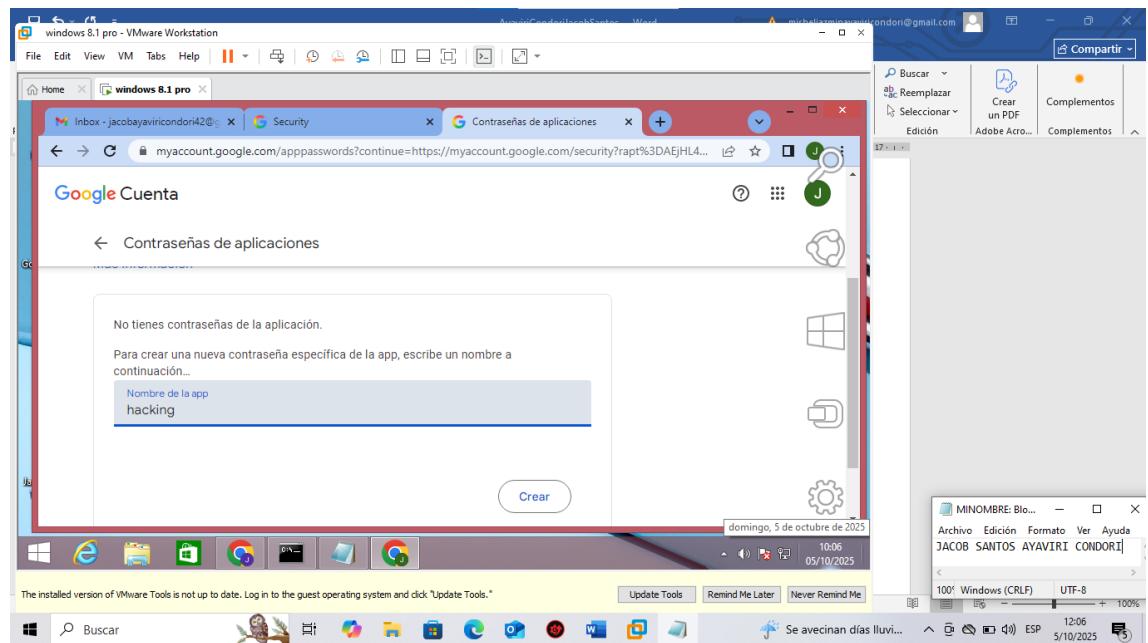




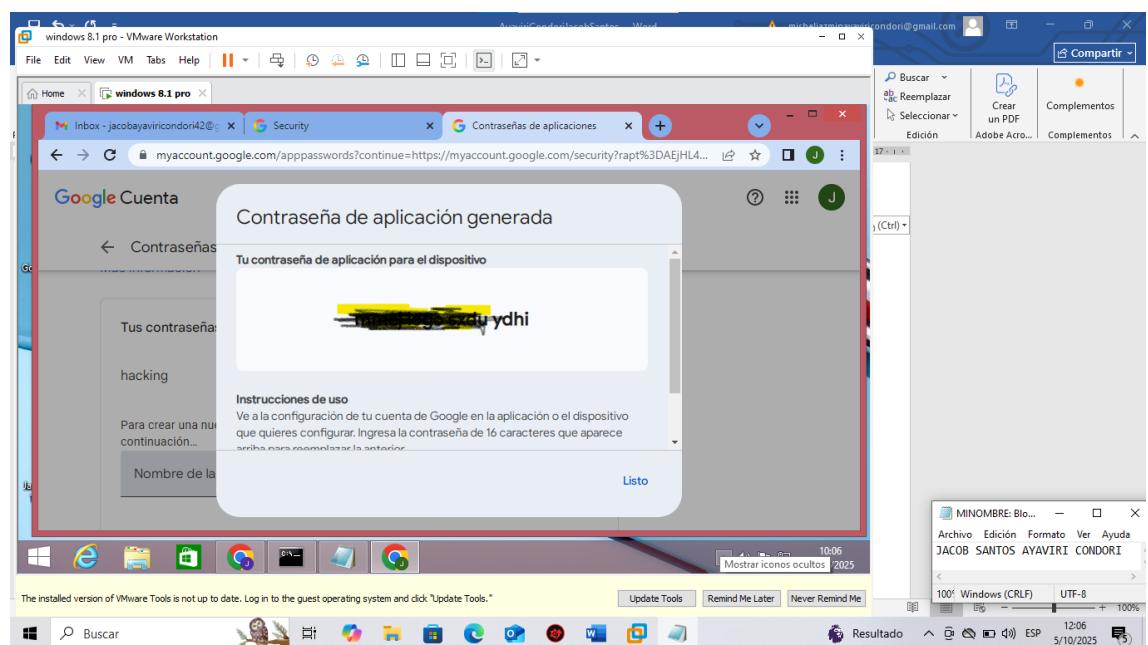
## Vinculamos el numero y buscamos contraseñas de aplicaciones



## Ponemos el nombre hacking y crear

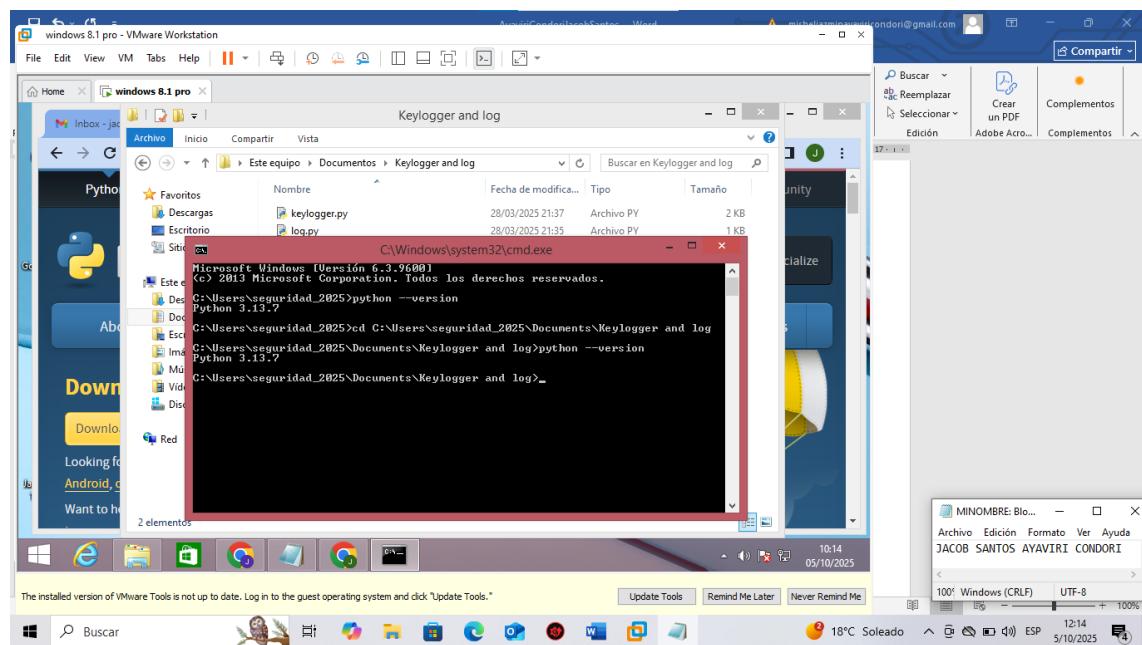


## Contraseñaaaaa

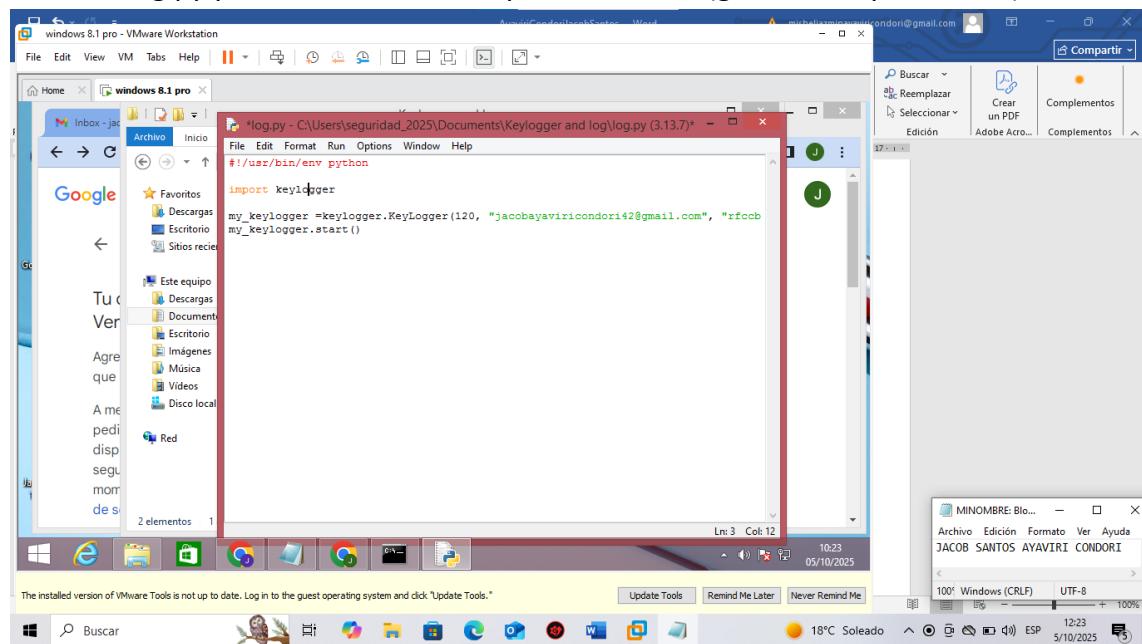


## ACTUALIZAR LOS PARAMETROS

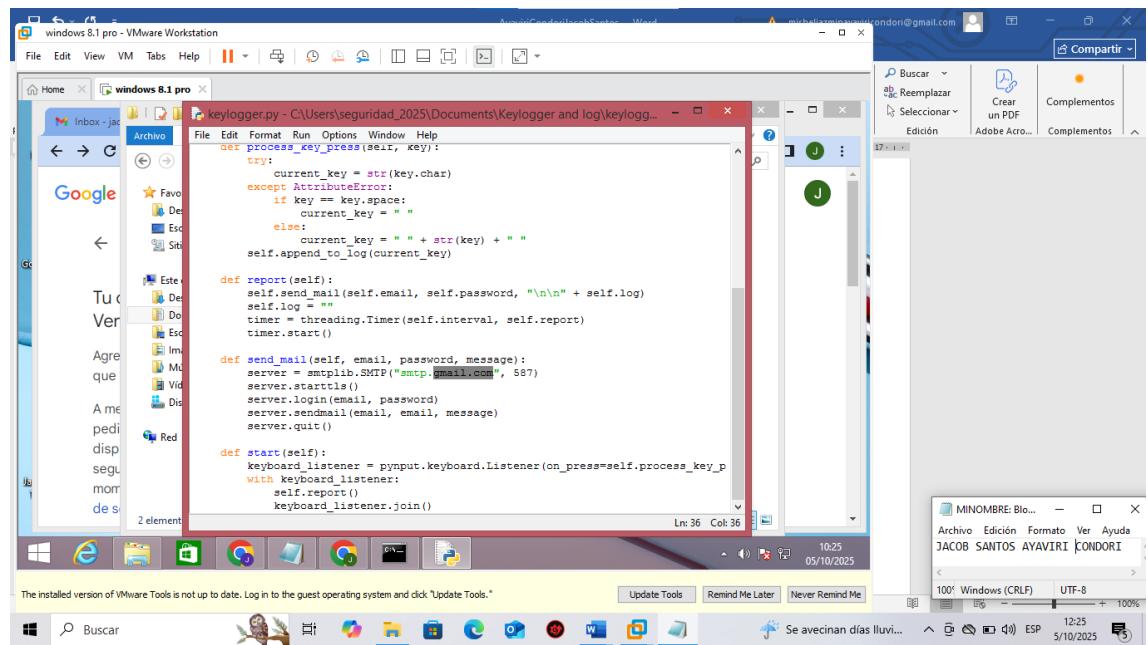
3. Vamos a la carpeta Keylogger and log y verificamos que tenga phyton instalado



Abrimos log.py y cambiamos el Gmail y la contraseña (guardamos y cerramos)

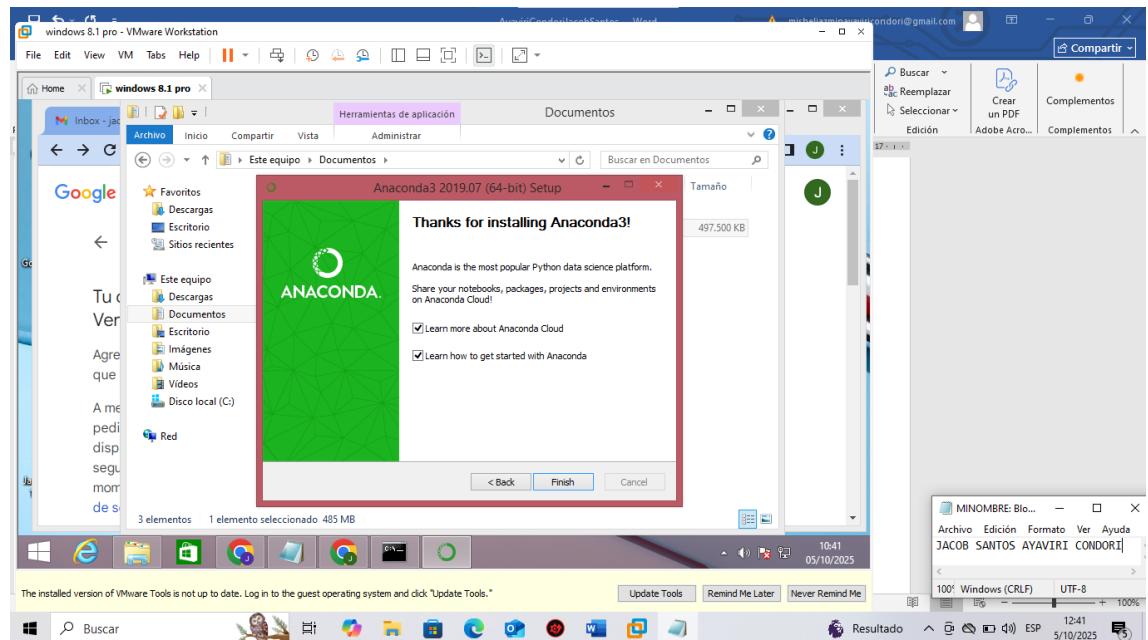


Abrimos keylogger.py y verificamos que tenga lo opción de Gmail.com

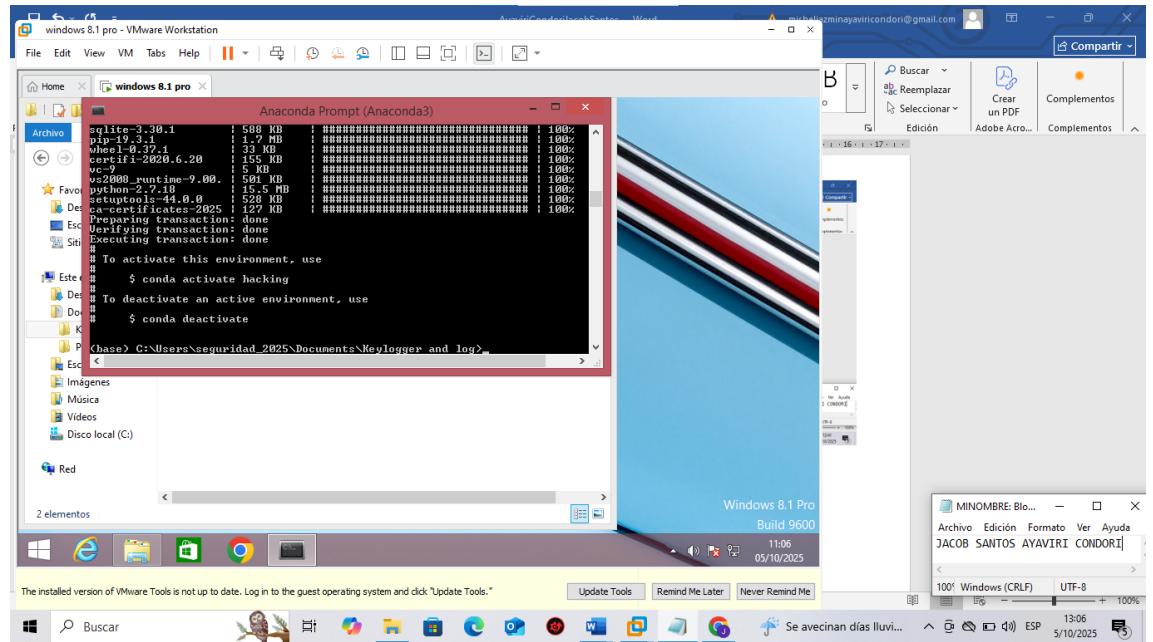


## EMPAQUETAMOS EL ARCHIVO EJECUTABLE

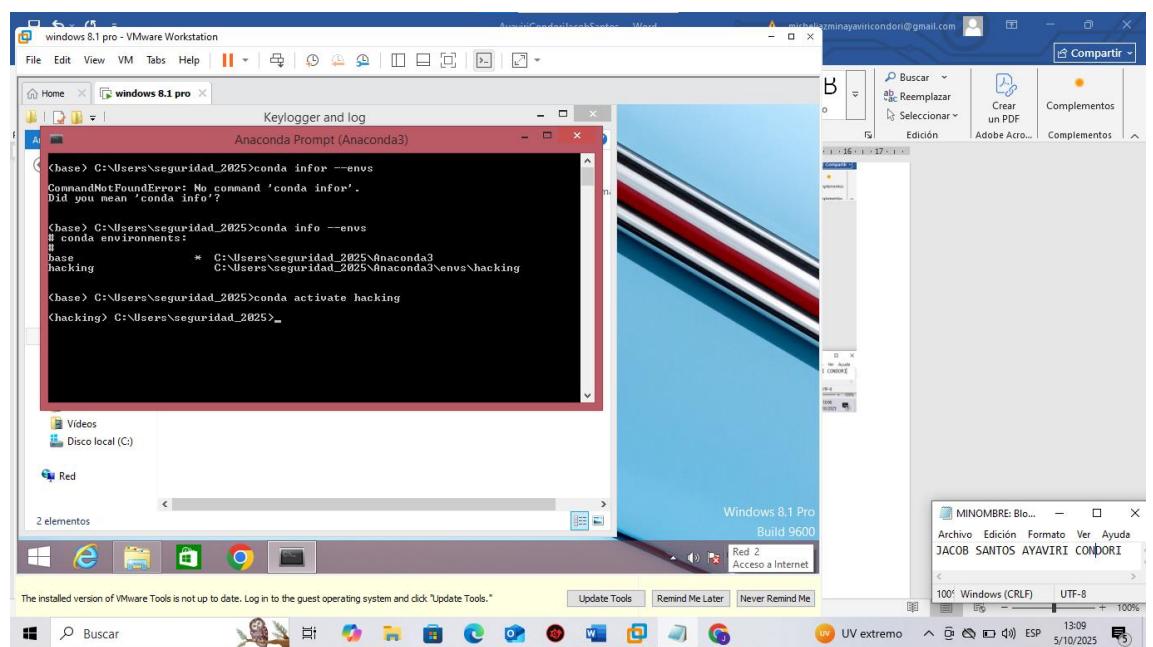
### 4. Abrimos CMD y activamos el entorno de Python 2 (instalamosssssssss)



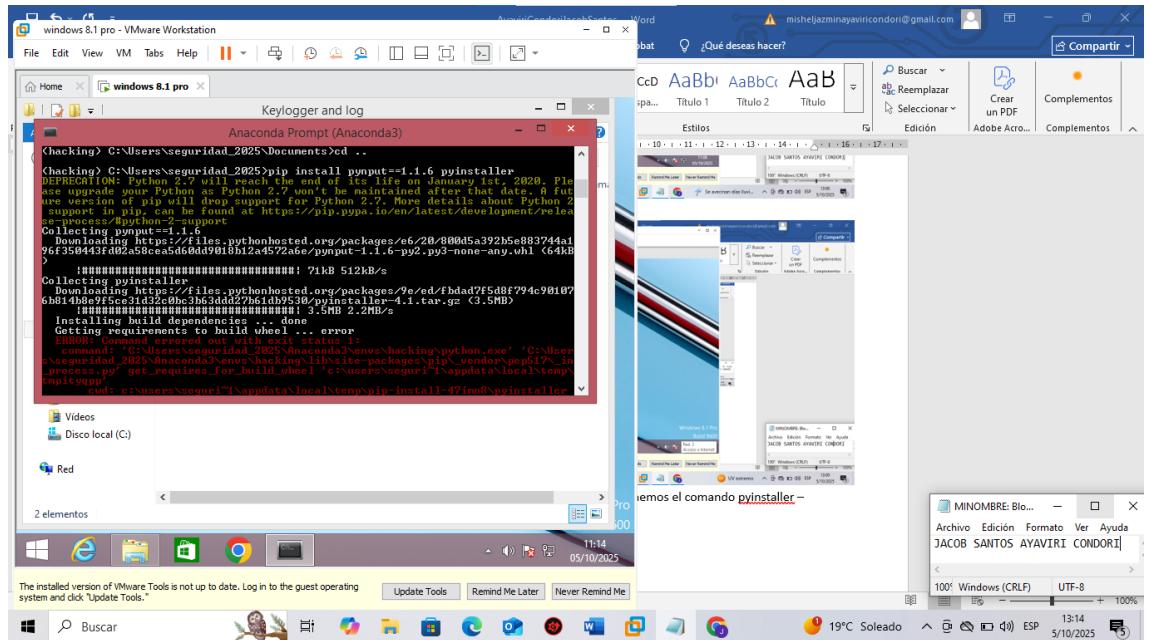
Abrimos anaconda 3 y creamos hacking



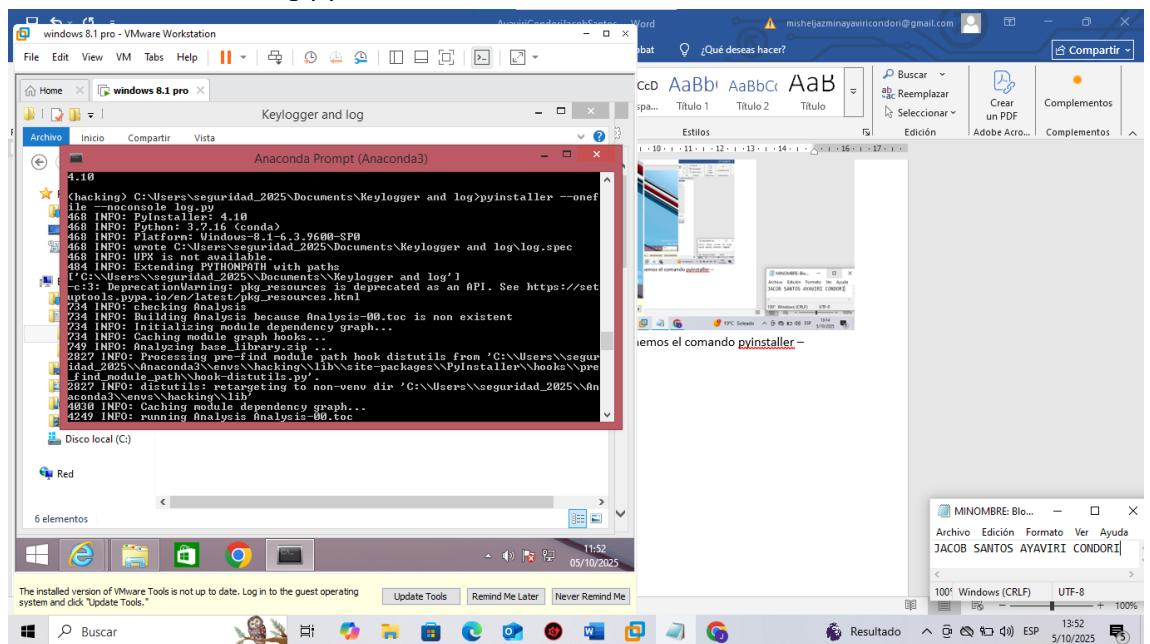
Activamosssss



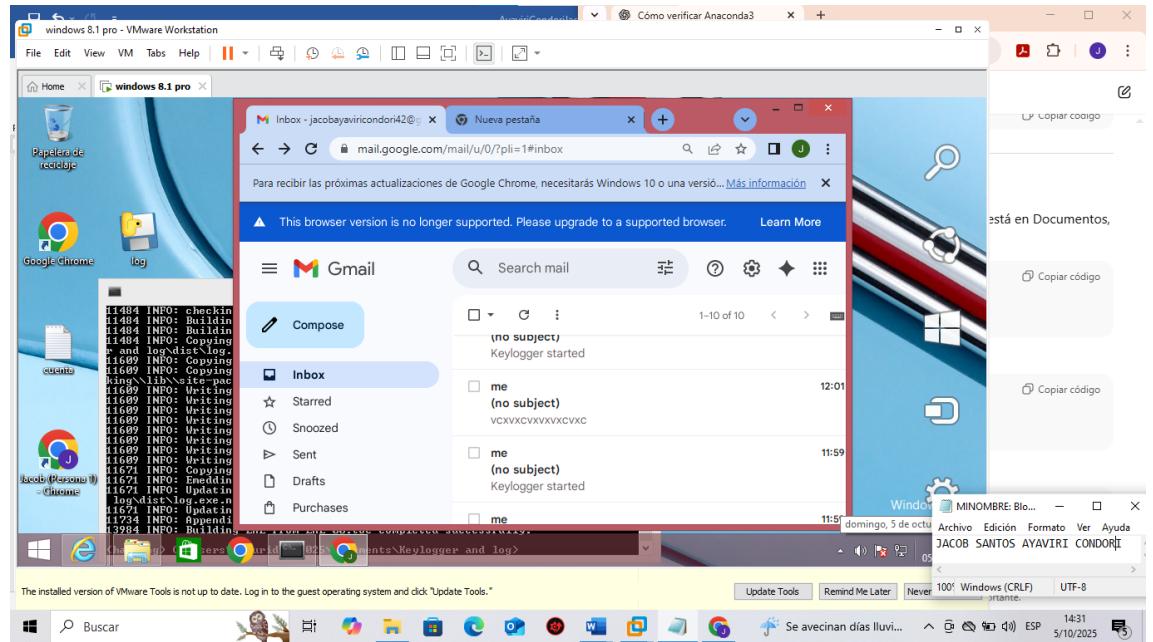
## Instalamos: pip install pynput==1.1.6 pyinstaller



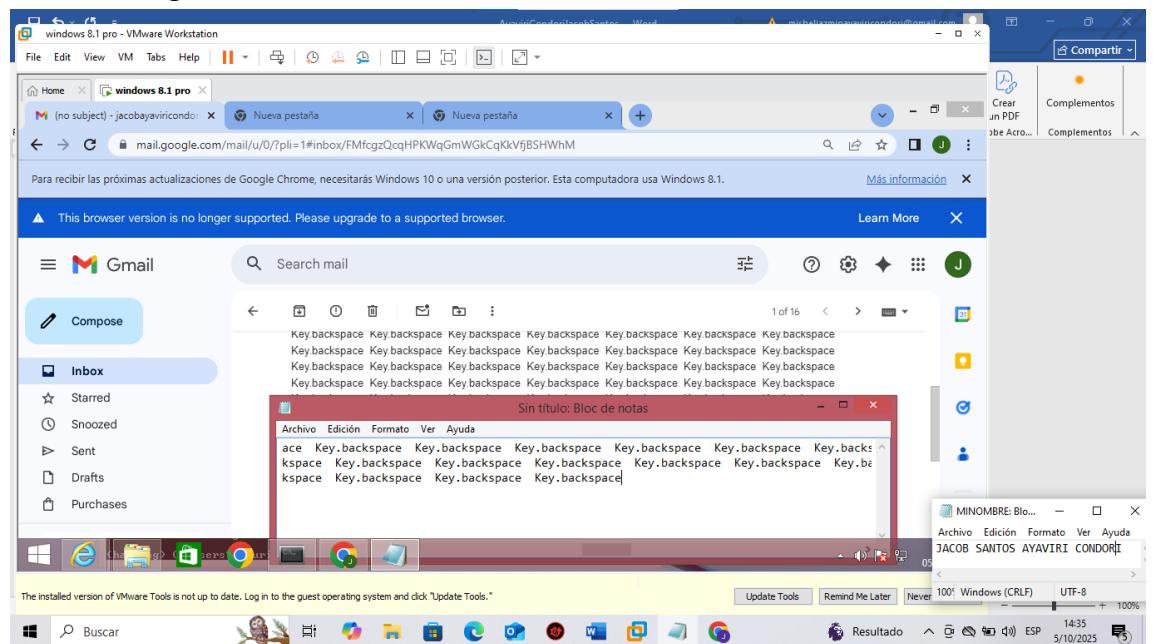
Entramos al archivo keylogger.py y log.py, y ponemos el comando pyinstaller –onefile –noconsole log.py



Arrastramos log.py al escritorio y abrimos el correo



Cada 120 segundo



EVALUACION N1

## Me registro en Twilio

Cómo verificar Anaconda3 Phone Numbers | Twilio Console Search Results - Twilio Help Center

Página de inicio de Twilio prueba Ensayo : \$15.50 Mejora Saltar a... Administración Comprar un número →

Números activos

Filtros de inventario Filtros de configuración

Número URL de voz

Filtrar Restablecer filtros

No tienes ningún número de teléfono de Twilio.

Compre un nuevo número Twilio o transfiera un número

Enviar OTP o 2FA?

Obtenga más información

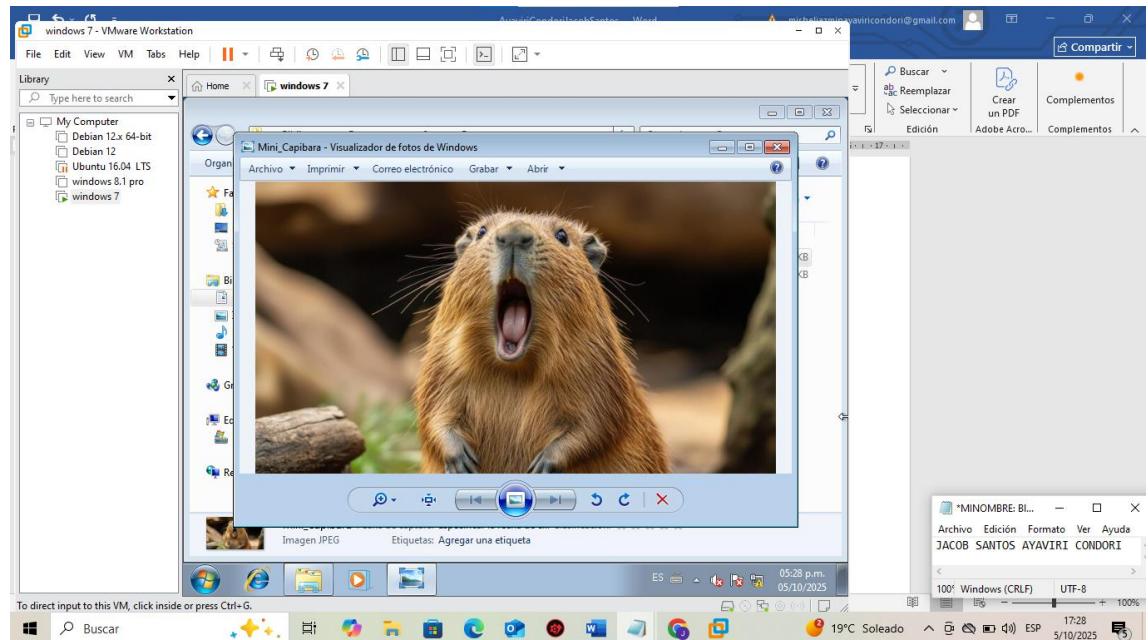
JACOB SANTOS AYAVIRI CONDORI

100% Windows (CRLF) 16:08 5/10/2025

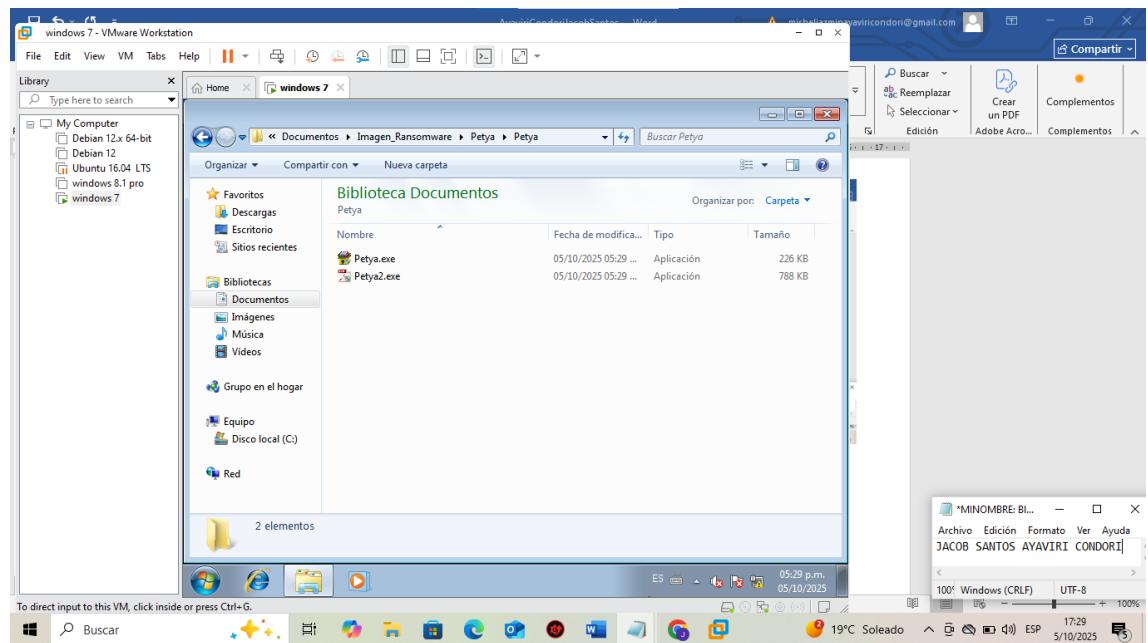
## PARTE 2

### COMUFLAJE DE MALWARE

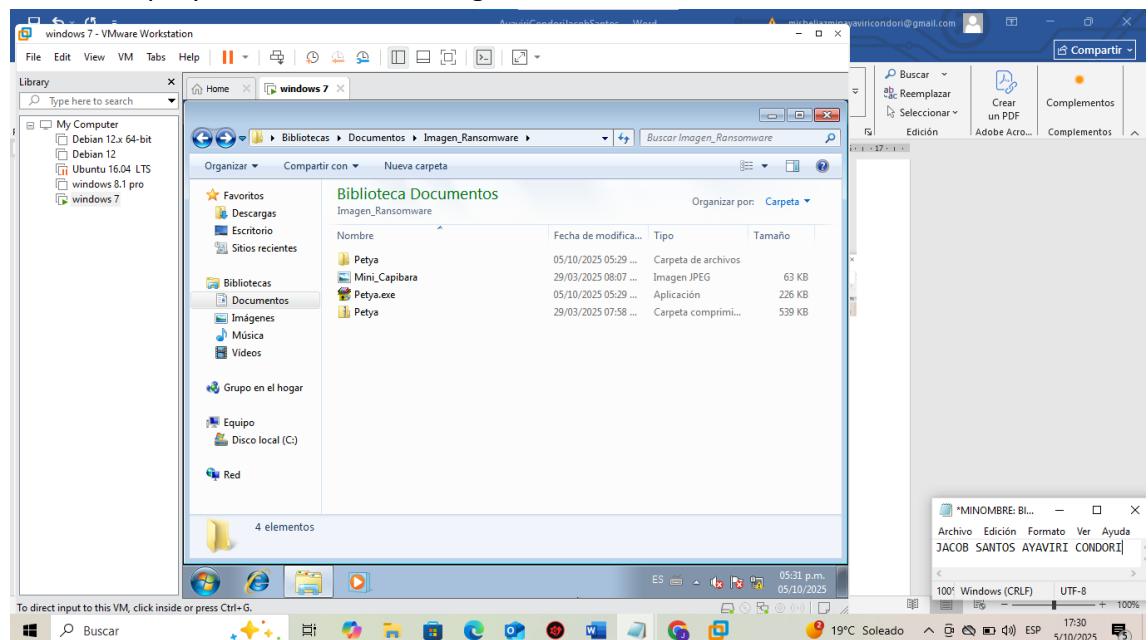
#### 1. Ir a la imagen



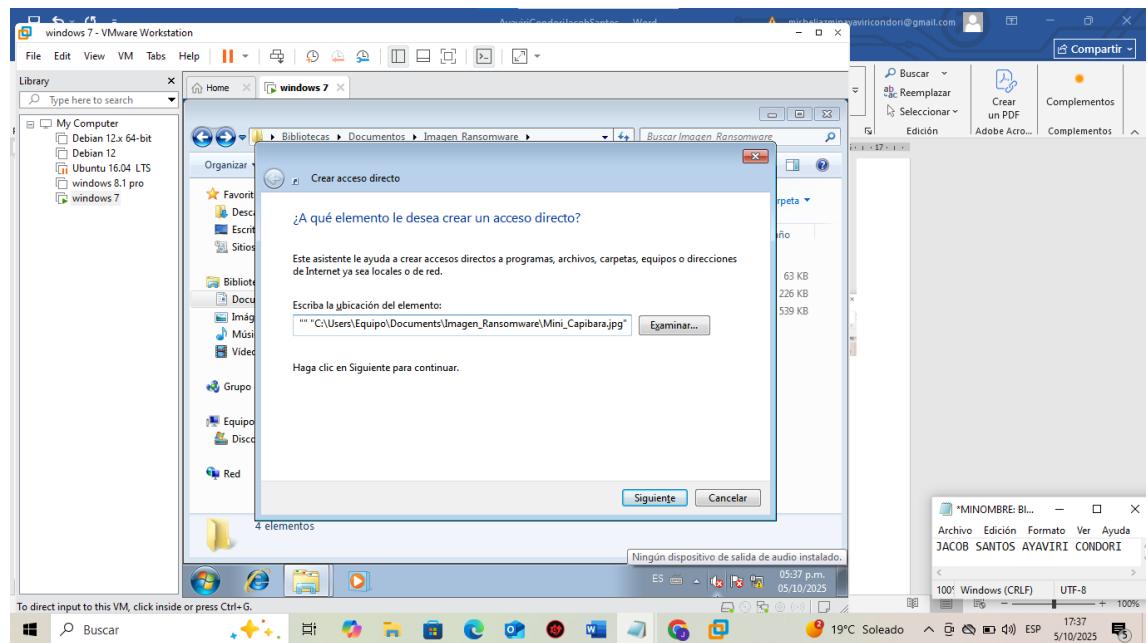
Extraemos petya



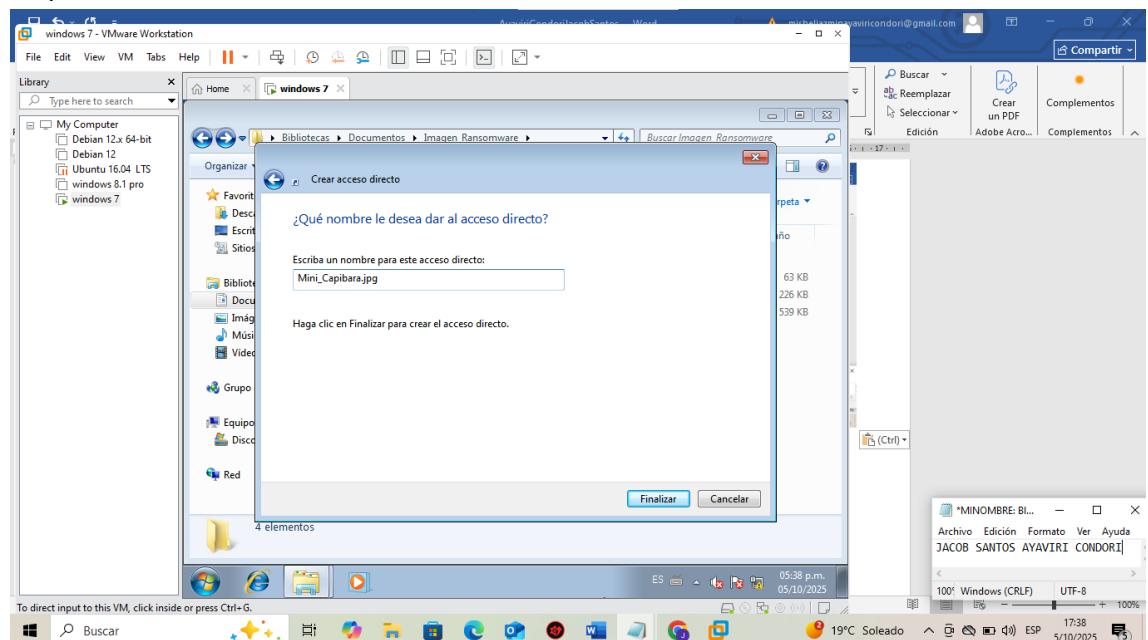
Movemos petya.exe a donde la imagen



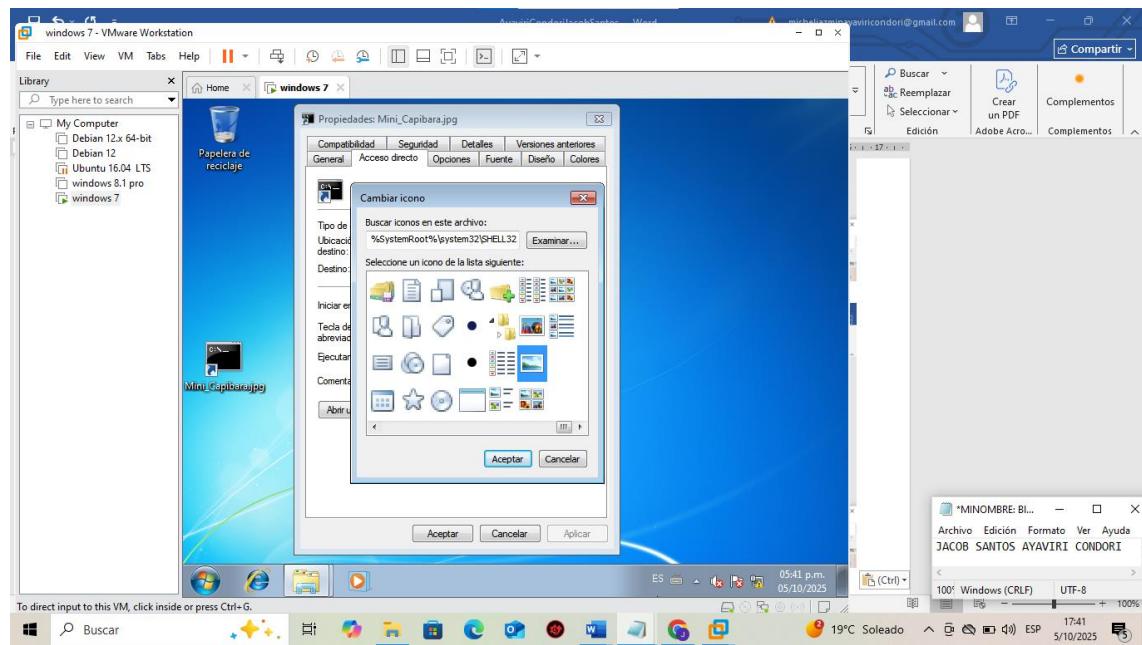
Nos vamos al escritorio y creamos un acceso directo



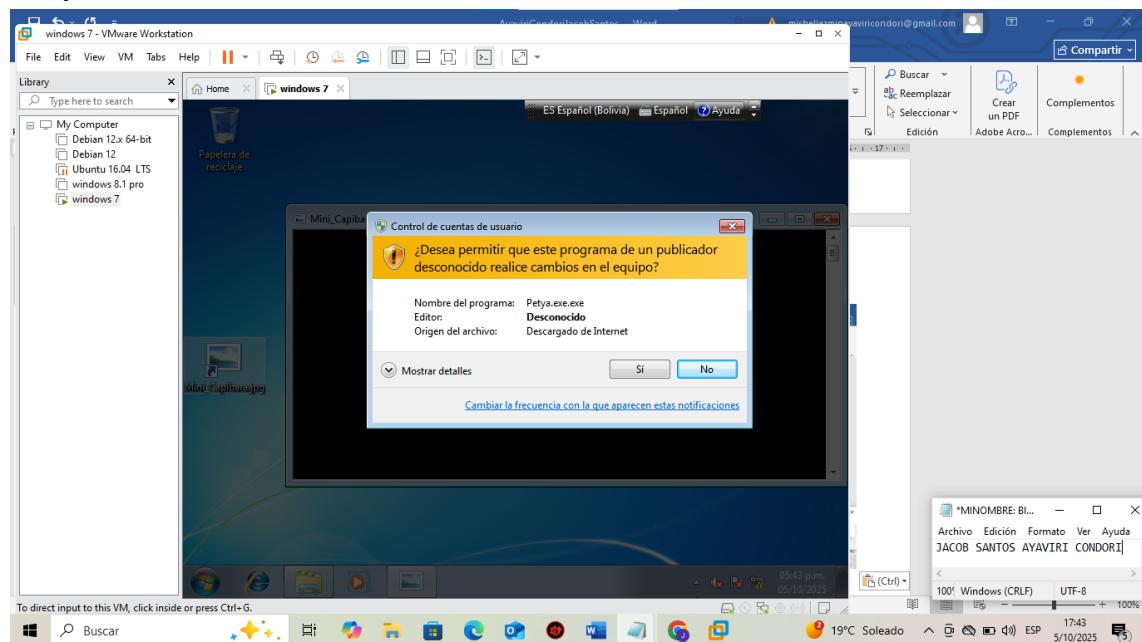
## Le ponemos nombre



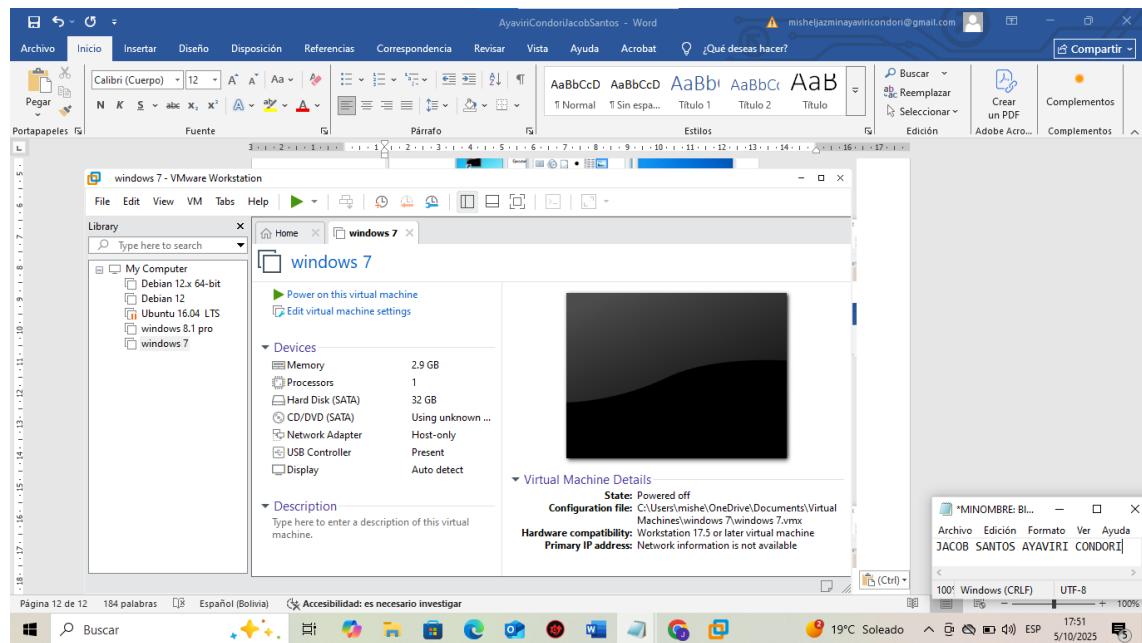
## Cambiamos el icono



## Lo ejecutamos

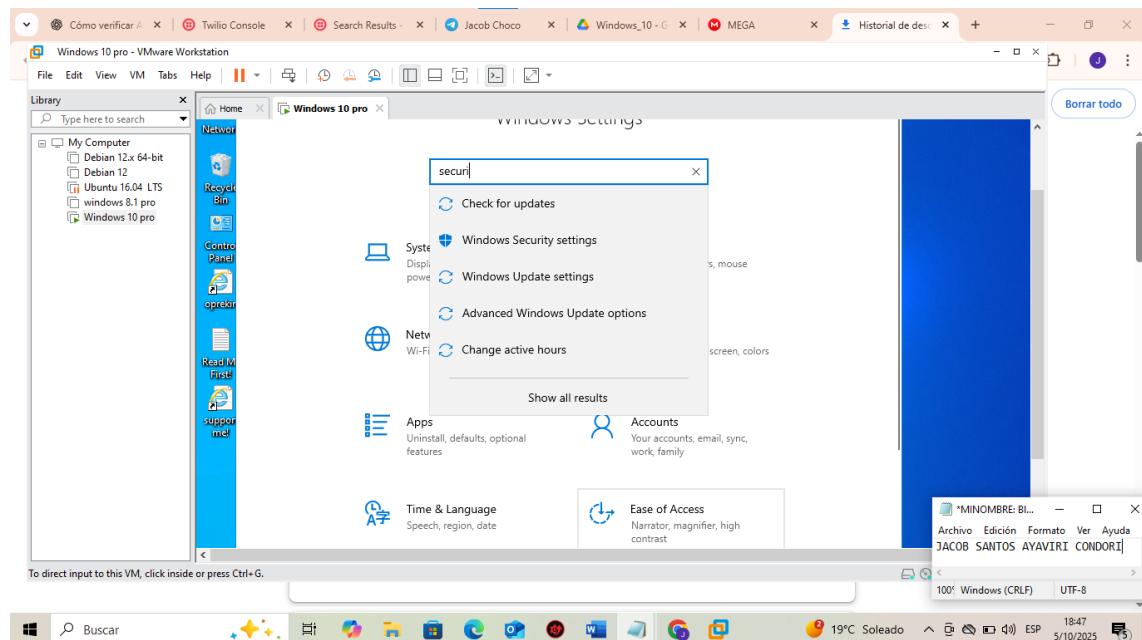


Final

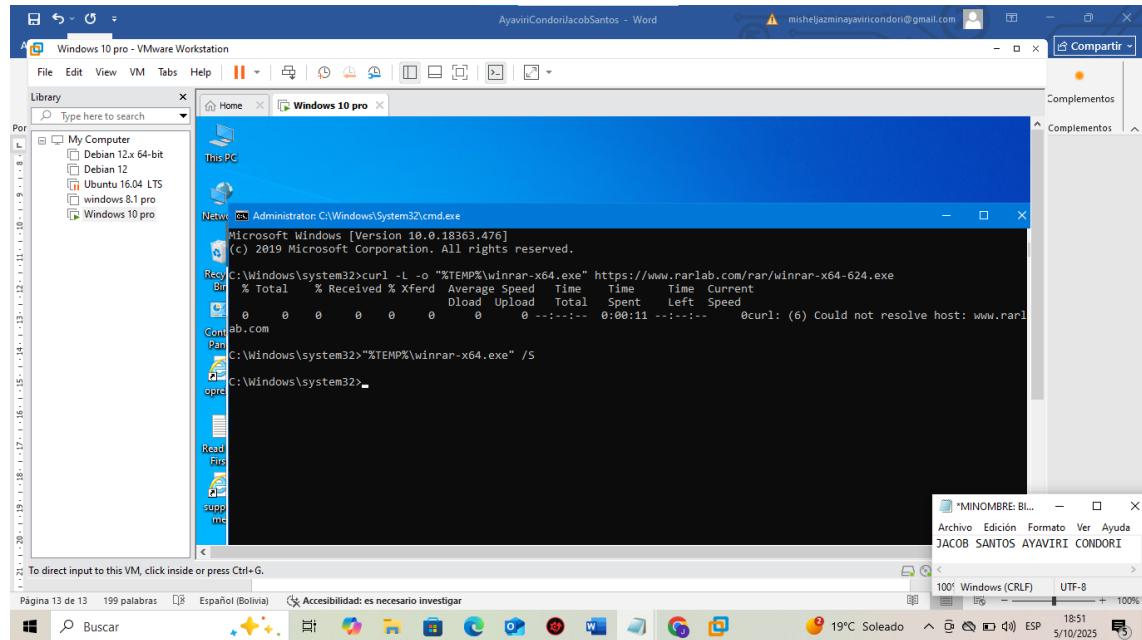


## EVALUACION 2

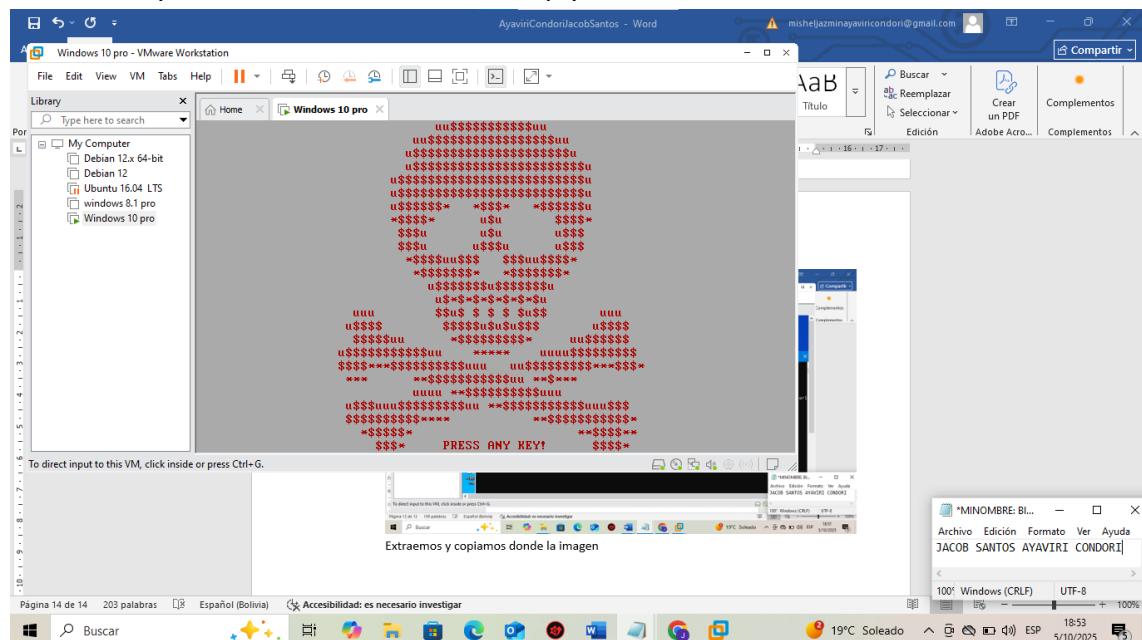
### Desactivar todos las medidas de seguridad de Windows



Instalamos winrar



## Extraemos y con solo extraer el archivo zip ya se murió el sistema



## EXPLICACION

A pesar de que en Windows 7 y en Windows 10 tenian los mismos archivos de imagen y petya, en Windows 10 el sistema quedo muerto inmediatamente a solo extraer el zip (toda la seguridad estaba desactivada), mientras que en Windows 7 permitio hacer interacciones como hacer un acceso directo y ejecutarlo