

PRACTICA_01_SEGURIDAD DE SISTEMAS

Nombre: Jacob Santos Ayaviri Condori

C.I. 13229452



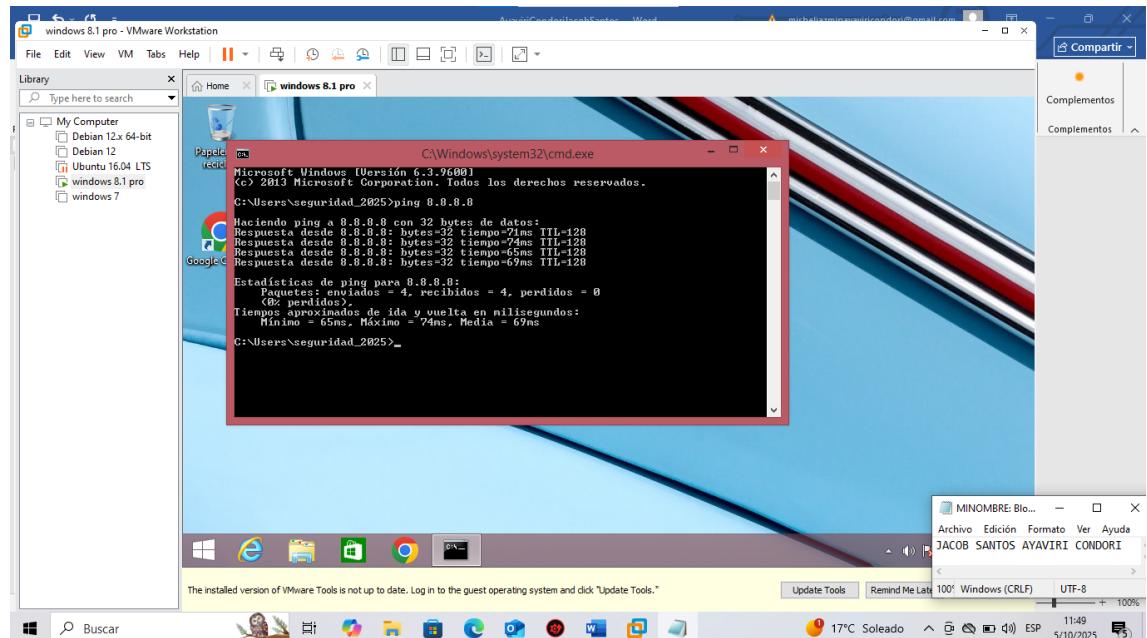
Name: Ayaviri_Condori_Jacob_Santos

Link: https://github.com/jacob-santos-0/Practica_01_seguridad_1_2025.git

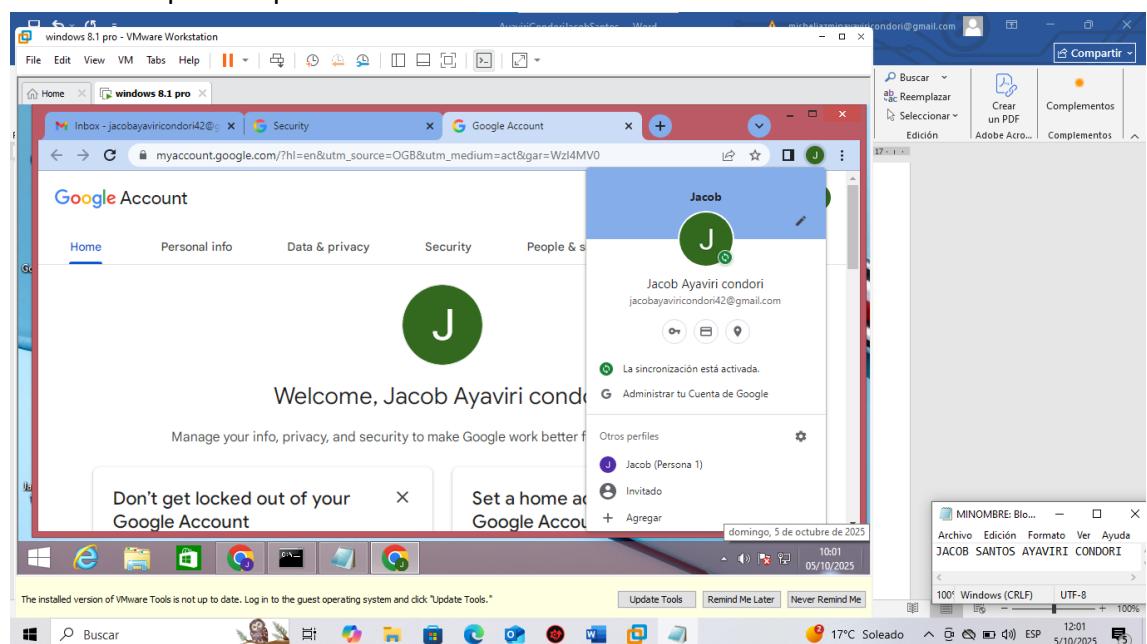
The screenshot shows a GitHub repository page. At the top, there are navigation links: Code (highlighted), Issues, Pull requests, Actions, Projects, Wiki, Security, Insights, and Settings. Below the header, the repository name is 'Practica_01_seguridad_1_2025' (Public). It shows 1 Branch and 0 Tags. A search bar, an 'Add file' button, and a 'Code' dropdown are also present. The main area displays a commit from 'jacob-santos-0' with the message 'pruebo'. The commit was made 2 minutes ago by user '4e1e729'. The commit history includes three files: 'AyaviriCondoriJacobSantos.docx', 'ayaviri_Condori_Jacob_Santos.pdf', and '~\$aviriCondoriJacobSantos.docx', all modified 7 minutes ago. At the bottom, there's a section for 'README' with a 'Create README' button and a note: 'Help people interested in this repository understand your project by adding a README.'

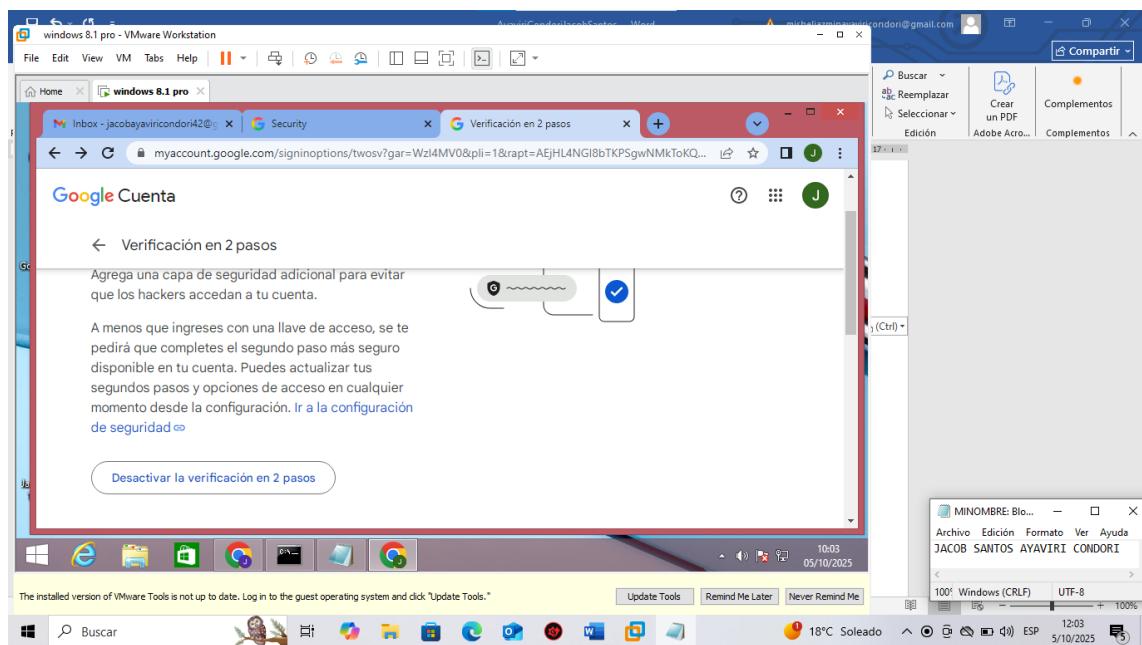
MODIFICAR PARAMETROS DEL CORREO

1. Conexión a internet

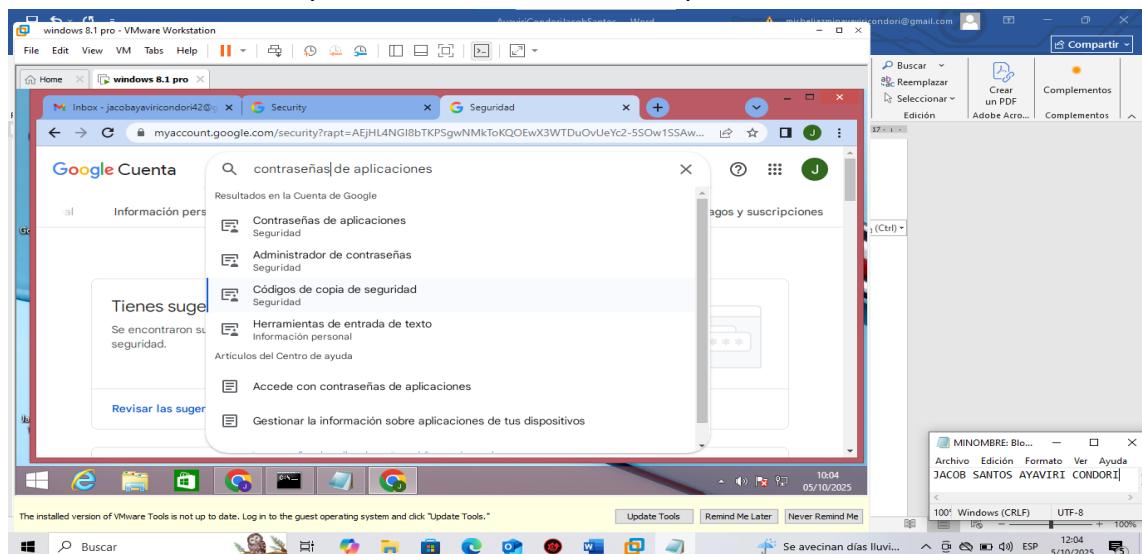


2. Ir a administración de tu cuenta Google, luego a seguridad y activamos la verificación por dos pasos

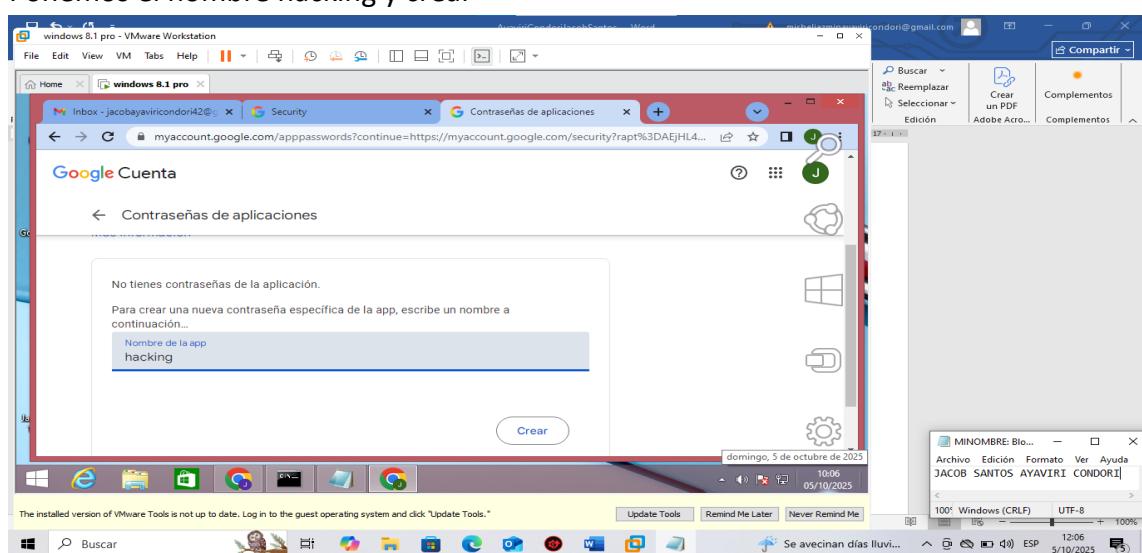




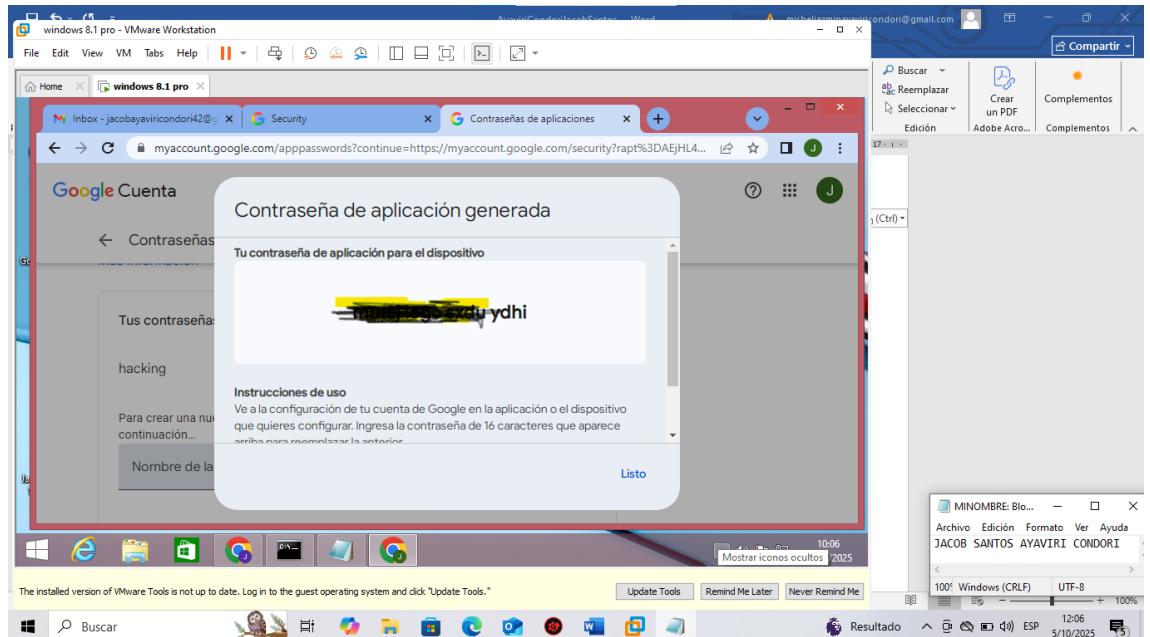
Vinculamos el numero y buscamos contraseñas de aplicaciones



Ponemos el nombre hacking y crear

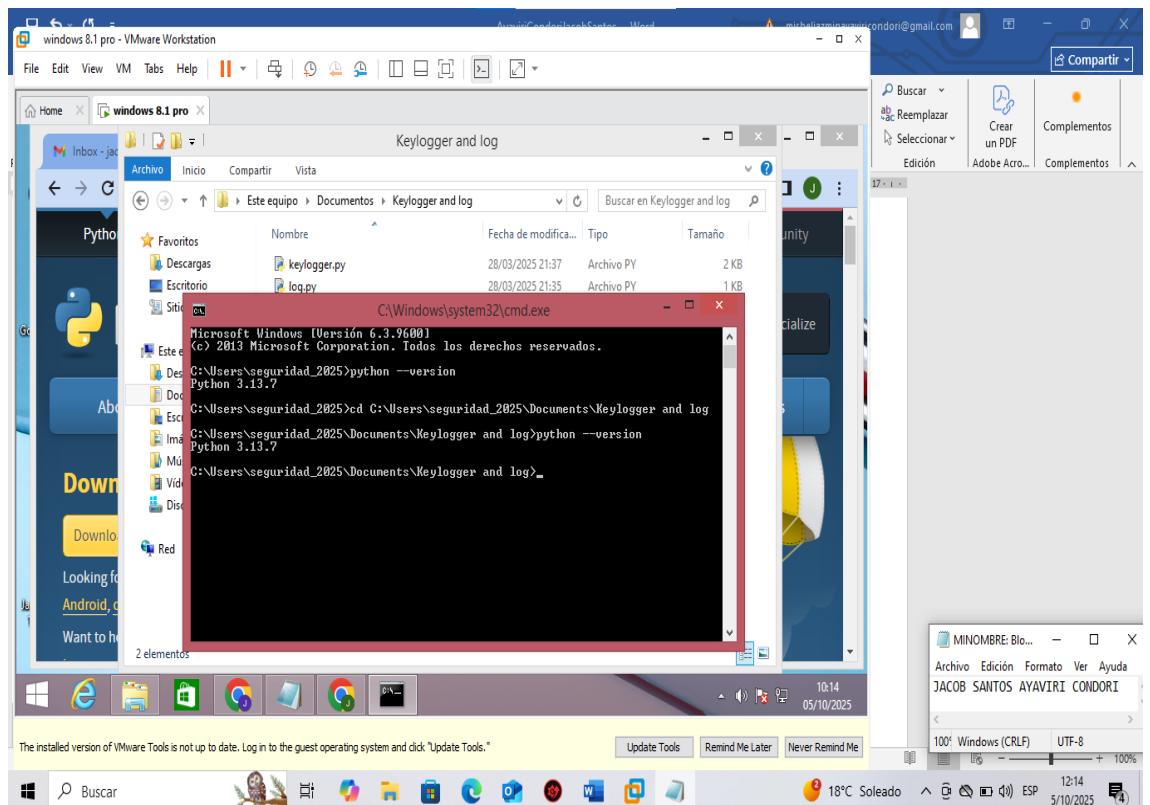


Contraseñaaaaa

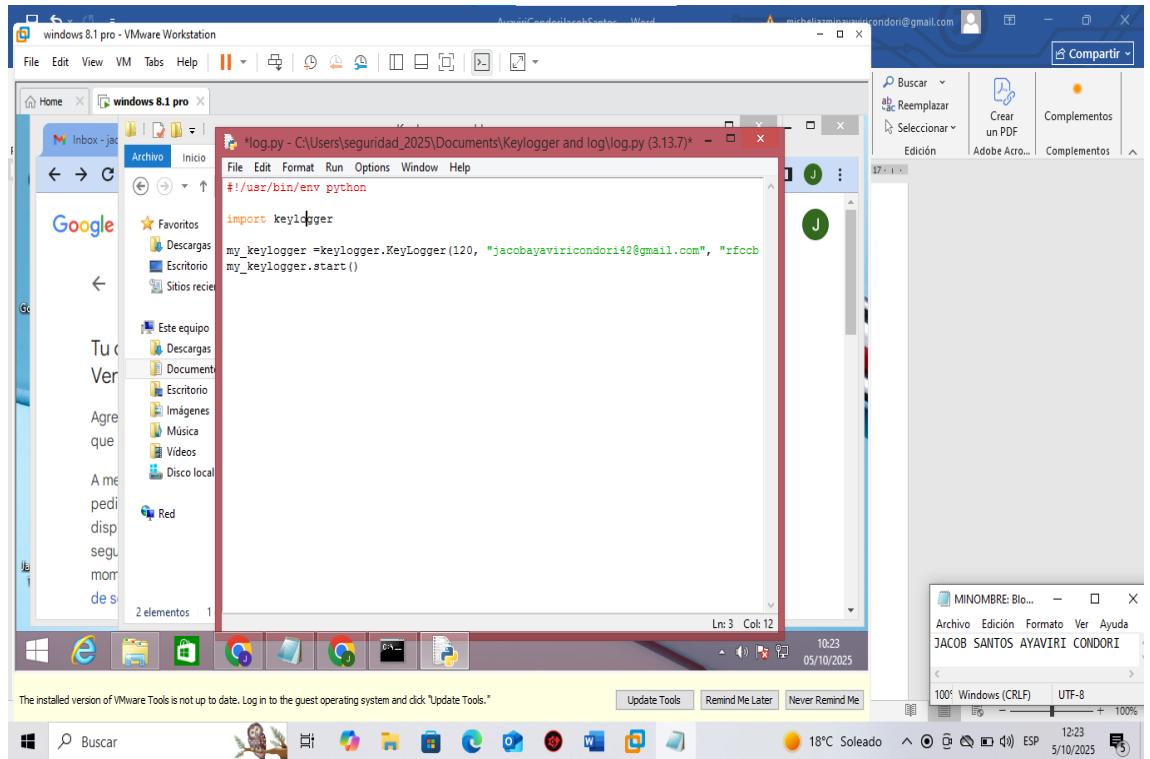


ACTUALIZAR LOS PARAMETROS

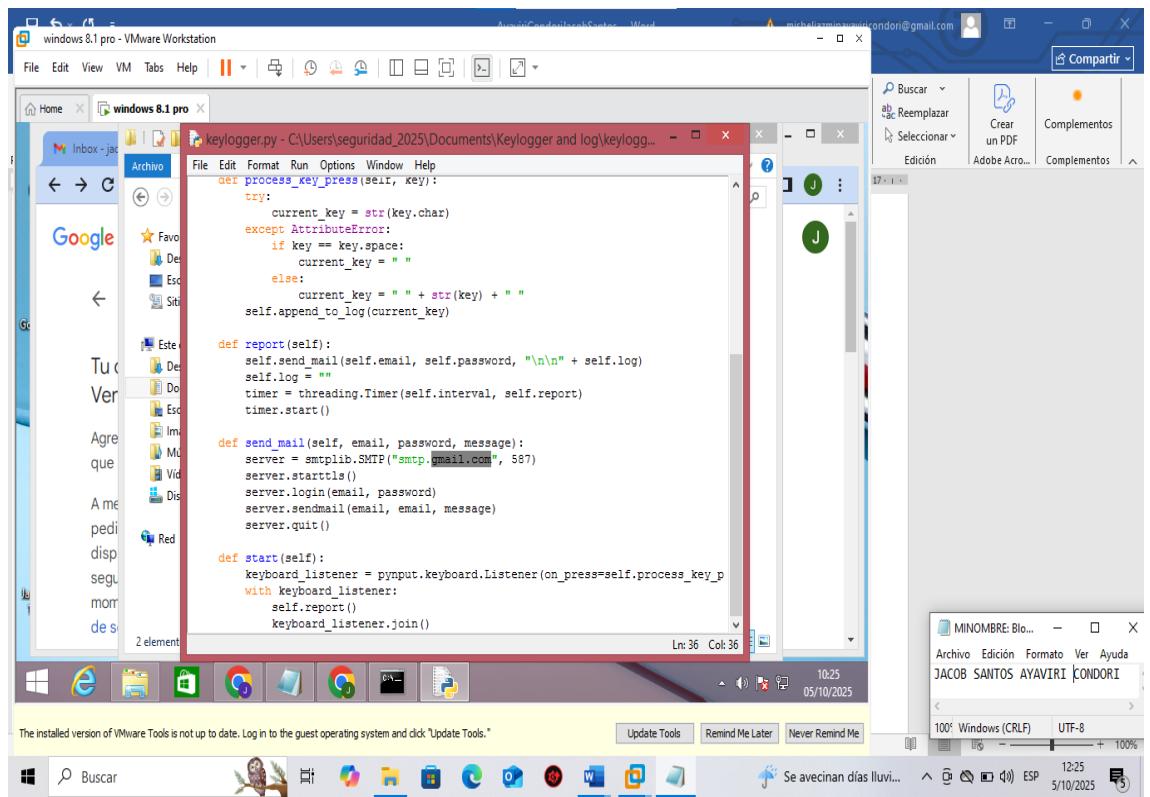
3. Vamos a la carpeta Keylogger and log y verificamos que tenga python instalado



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

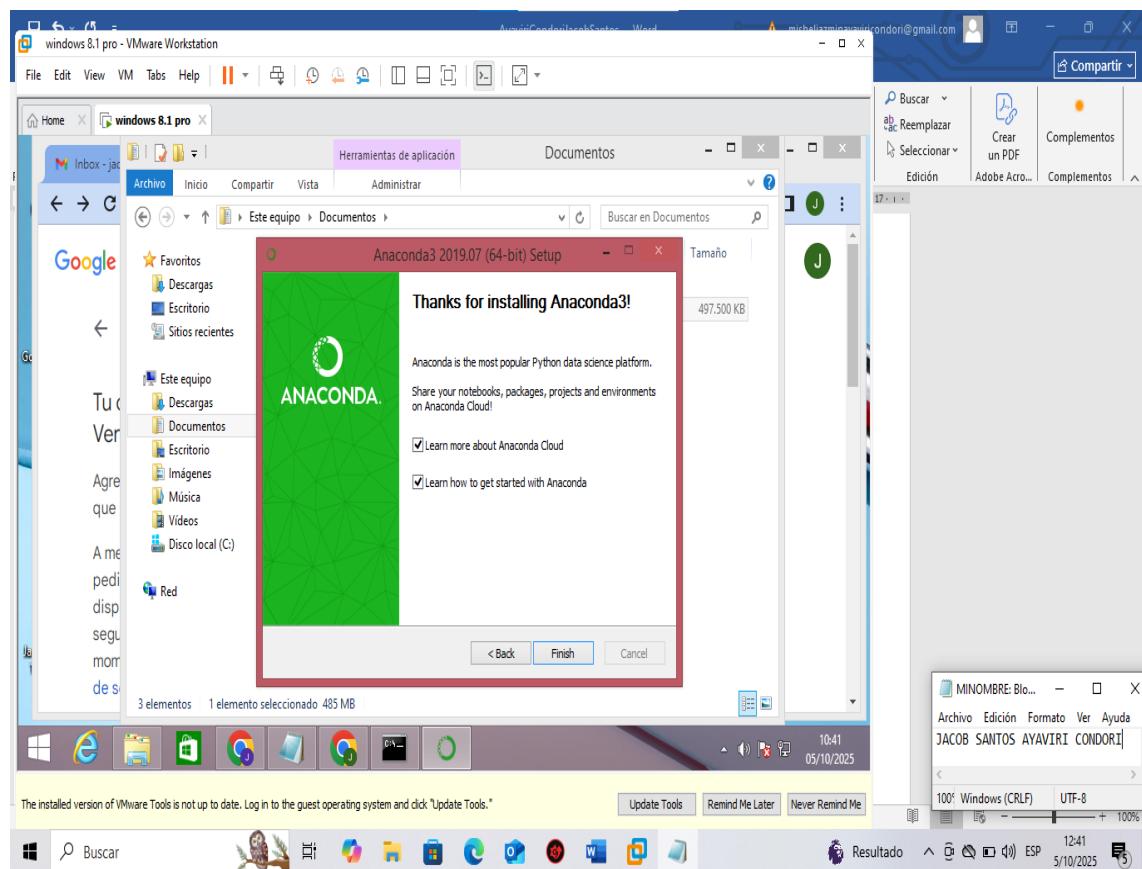


Abrimos keylogger.py y verificamos que tenga lo opción de Gmail.com

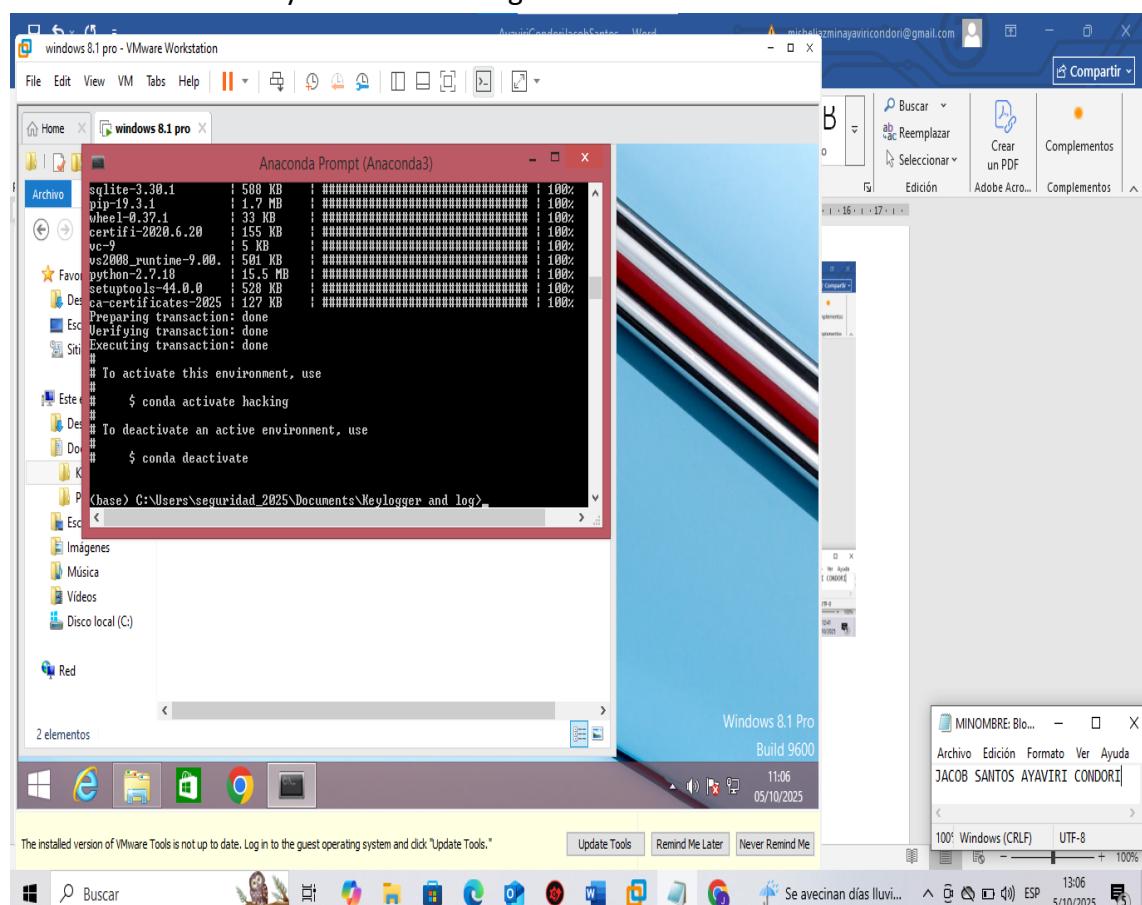


EMPAQUETAMOS EL ARCHIVO EJECUTABLE

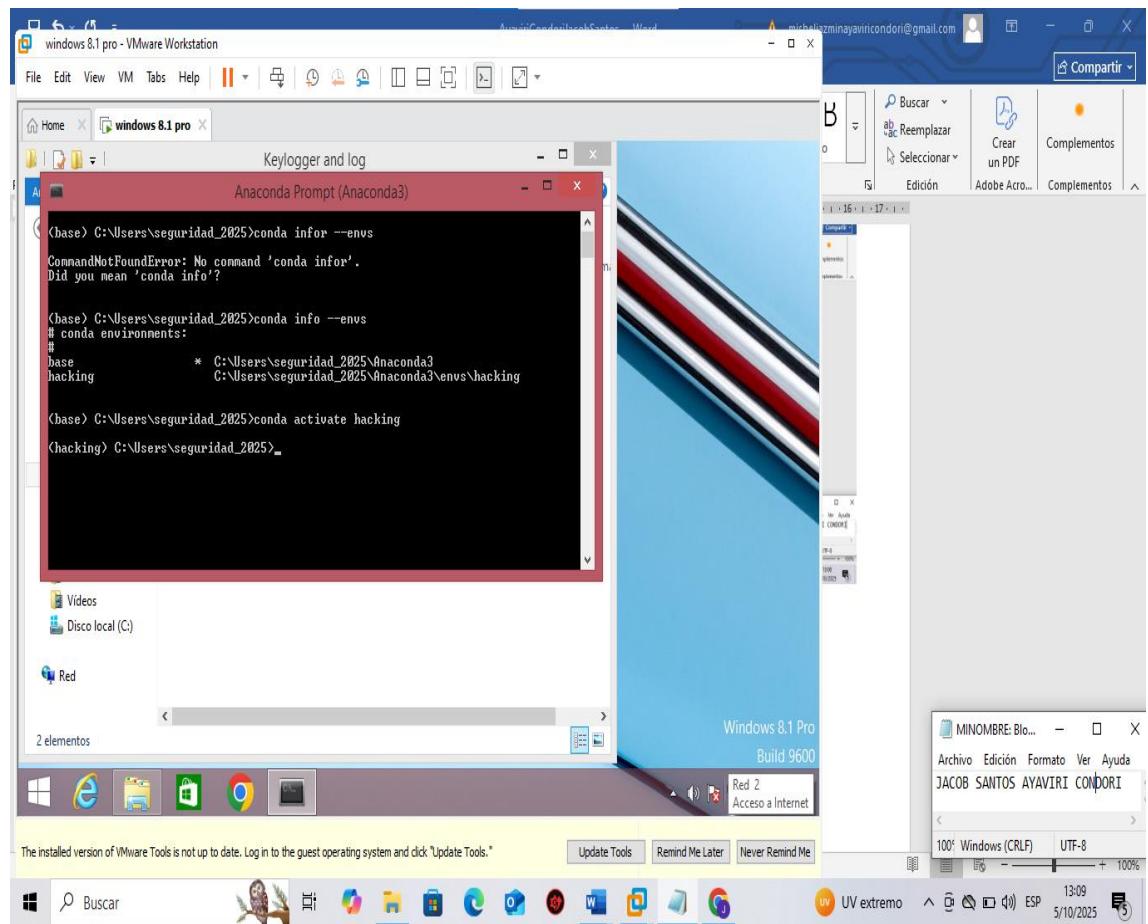
4. Abrimos CMD y activamos el entorno de Python 2 (instalamosssssssss)



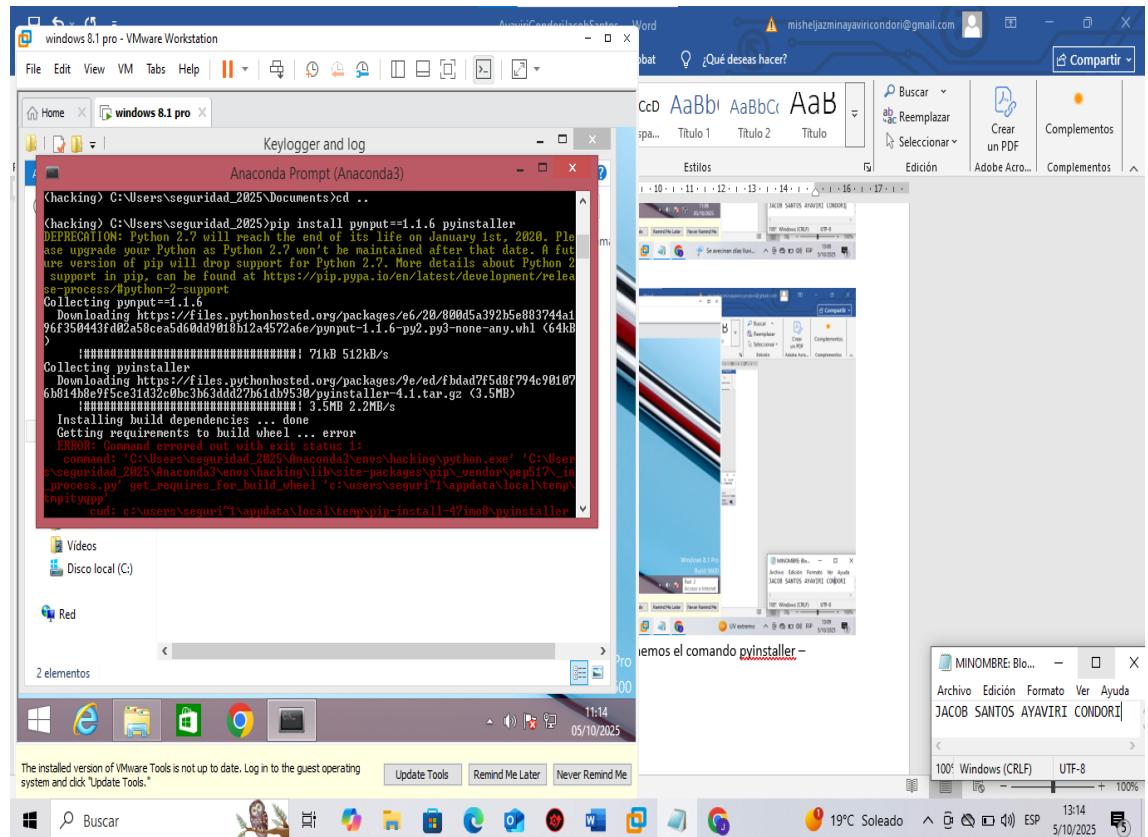
Abrimos anaconda 3 y creamos hacking



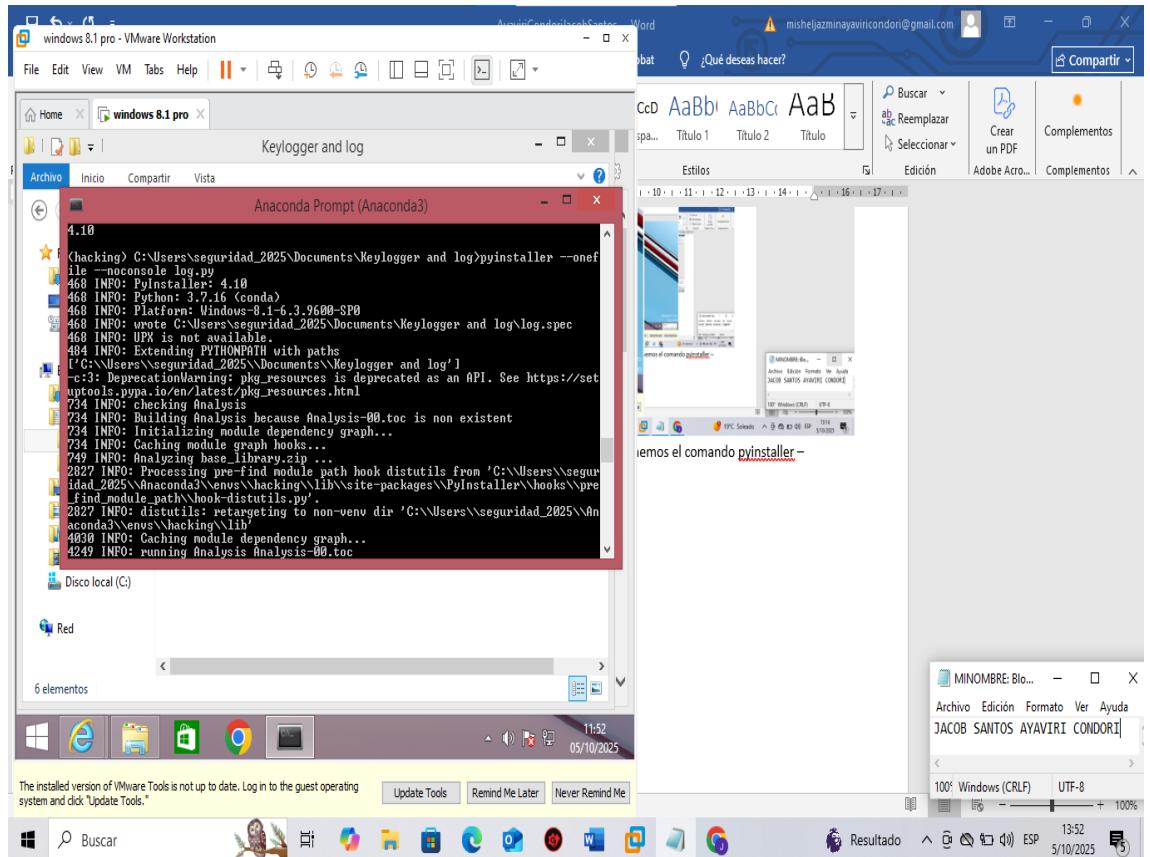
Activamossss



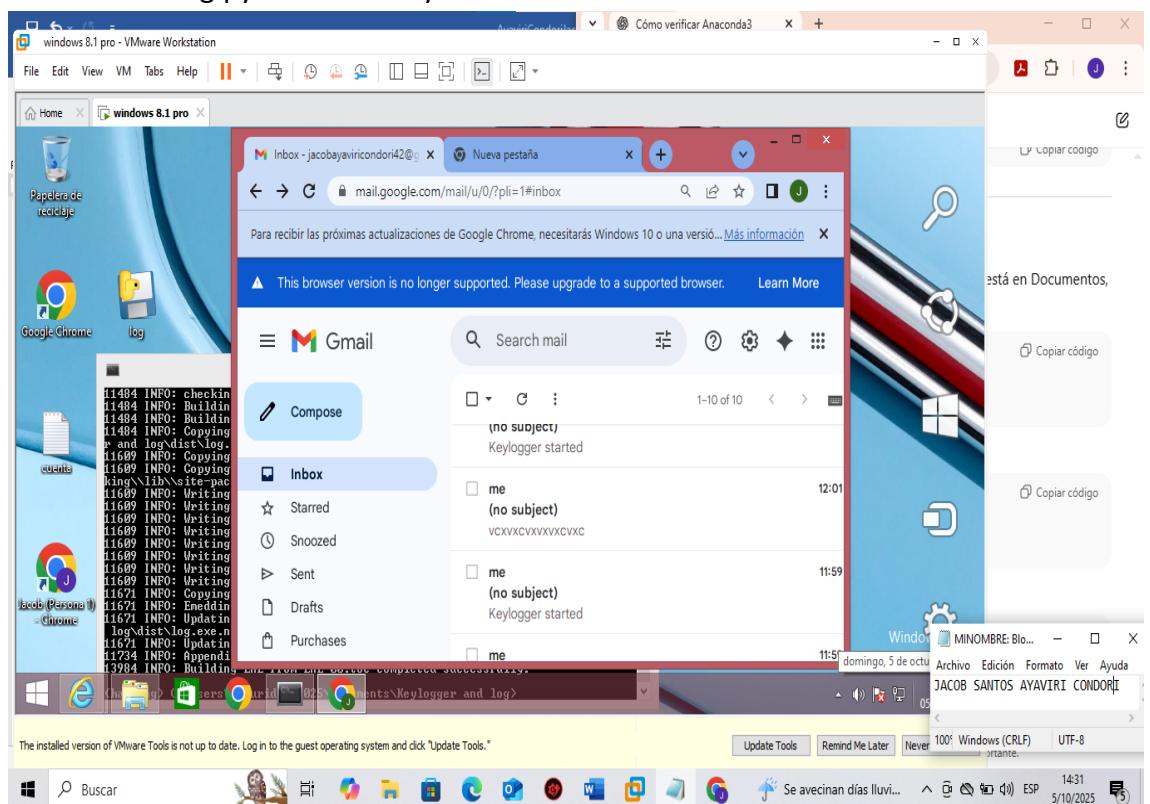
Instalamos: pip install pyngput==1.1.6 pyinstaller



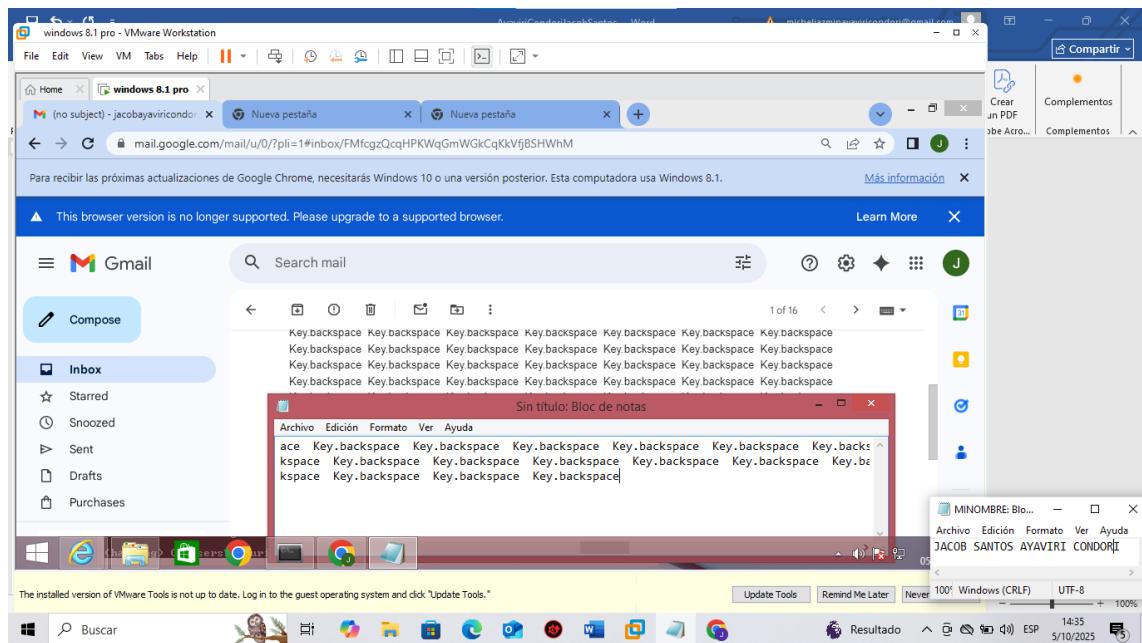
Entramos al archivo keylogger.py y log.py, y ponemos el comando pyinstaller –onefile –noconsole log.py



Arrastramos log.py al escritorio y abrimos el correo



Cada 120 segundo



EVALUACION N1

Me registro en Twilio

Página de inicio de Twilio

Ensayo : \$15.50 Mejora

Administración

Comprar un número →

Números activos

No tienes ningún número de teléfono de Twilio.

Compre un nuevo número Twilio o transfiera un número

¿Enviar OTP o 2FA?

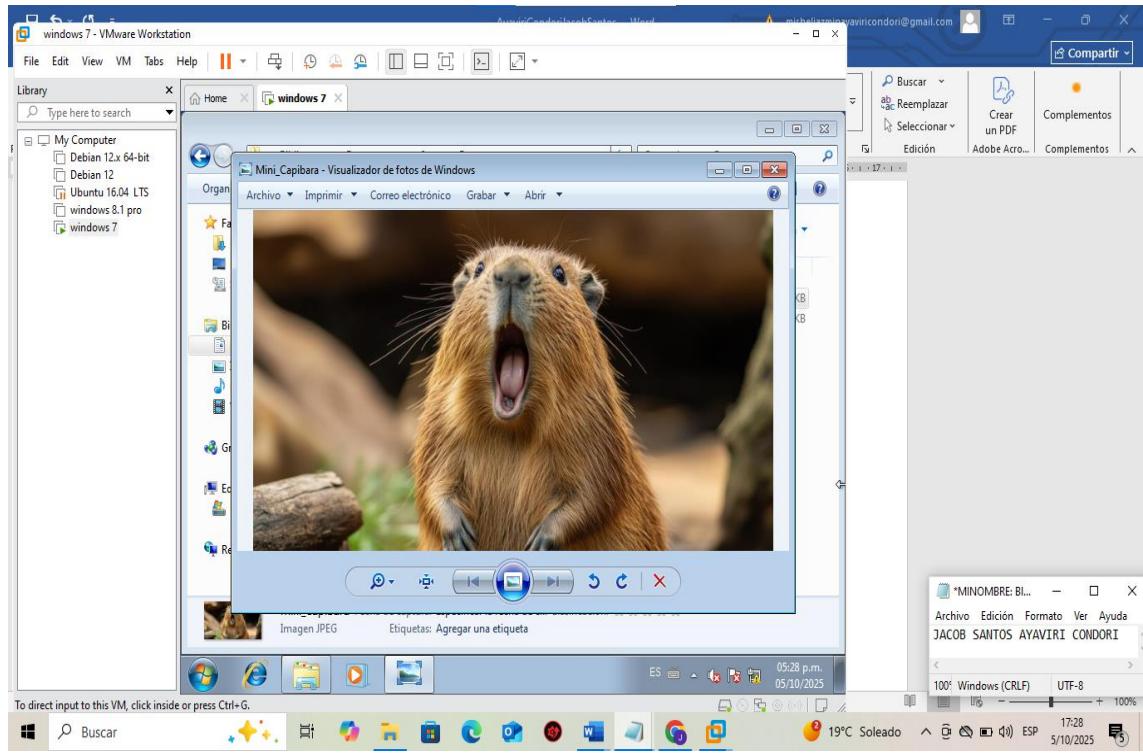
Obtenga más info

UV extremo

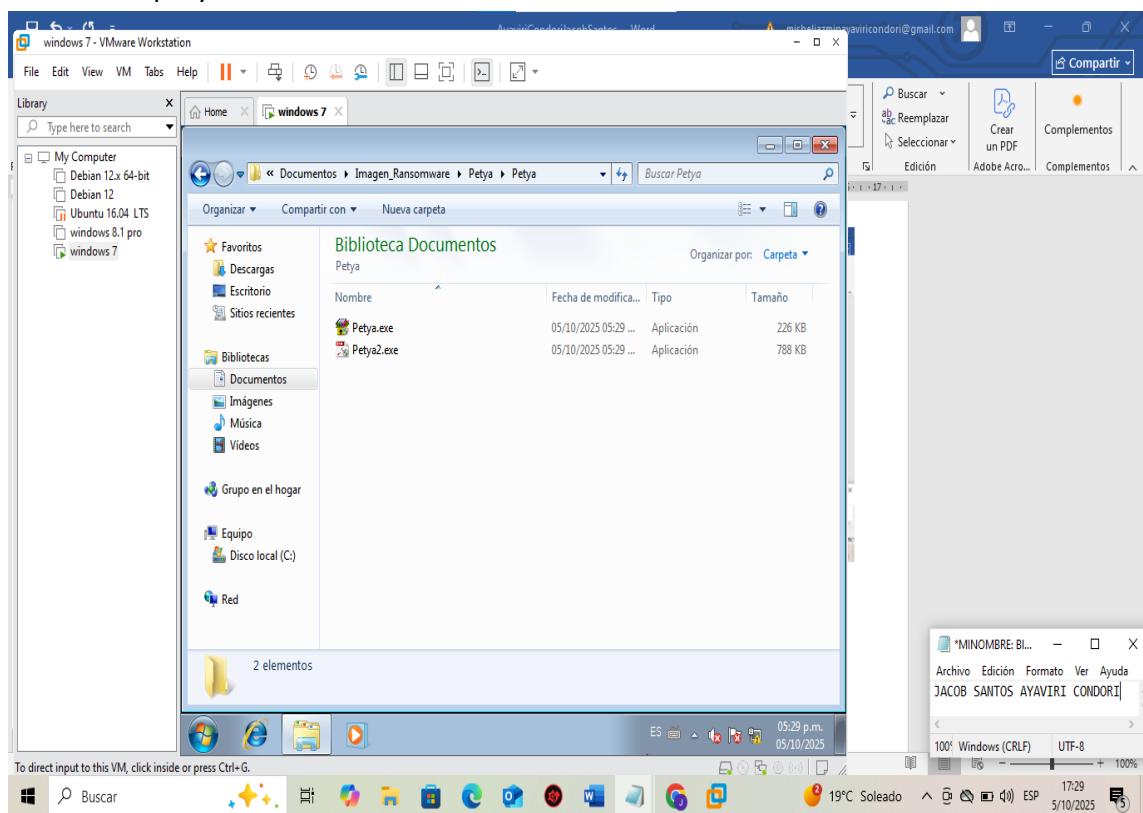
PARTE 2

COMUFLAJE DE MALWARE

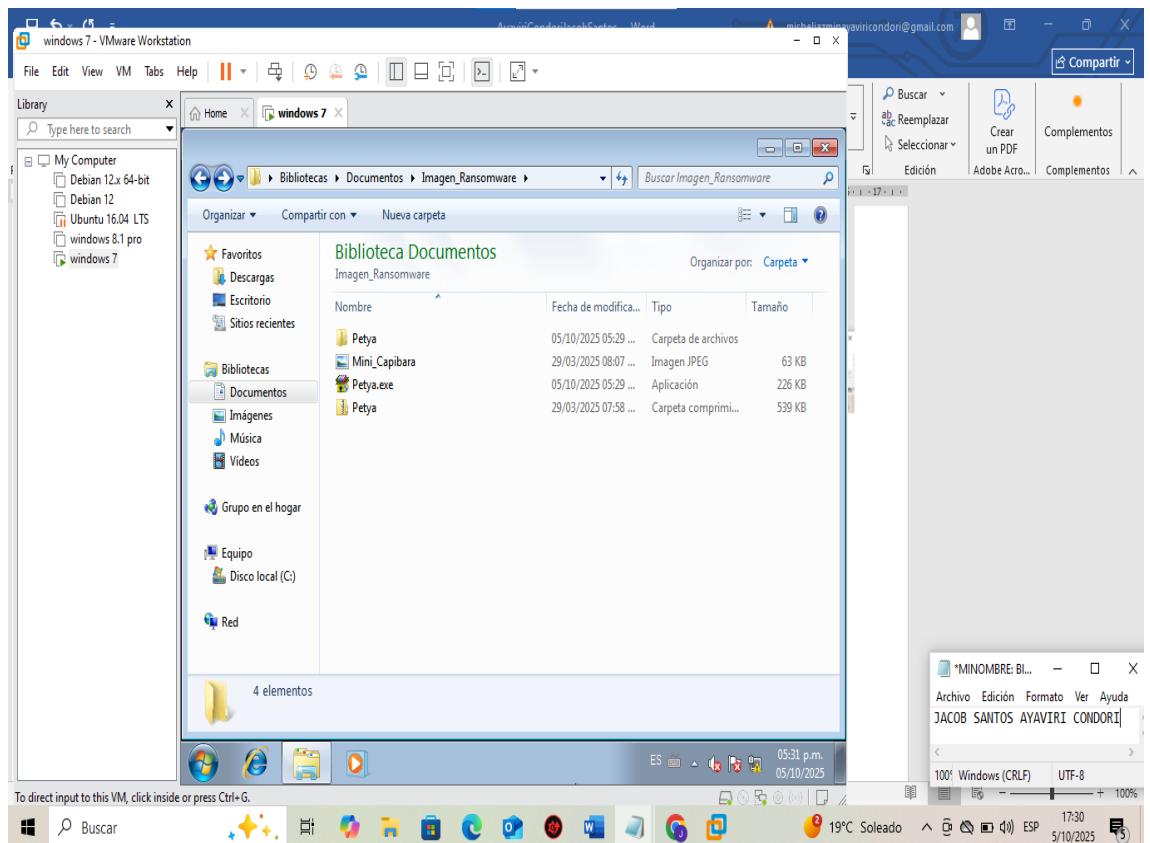
1. Ir a la imagen



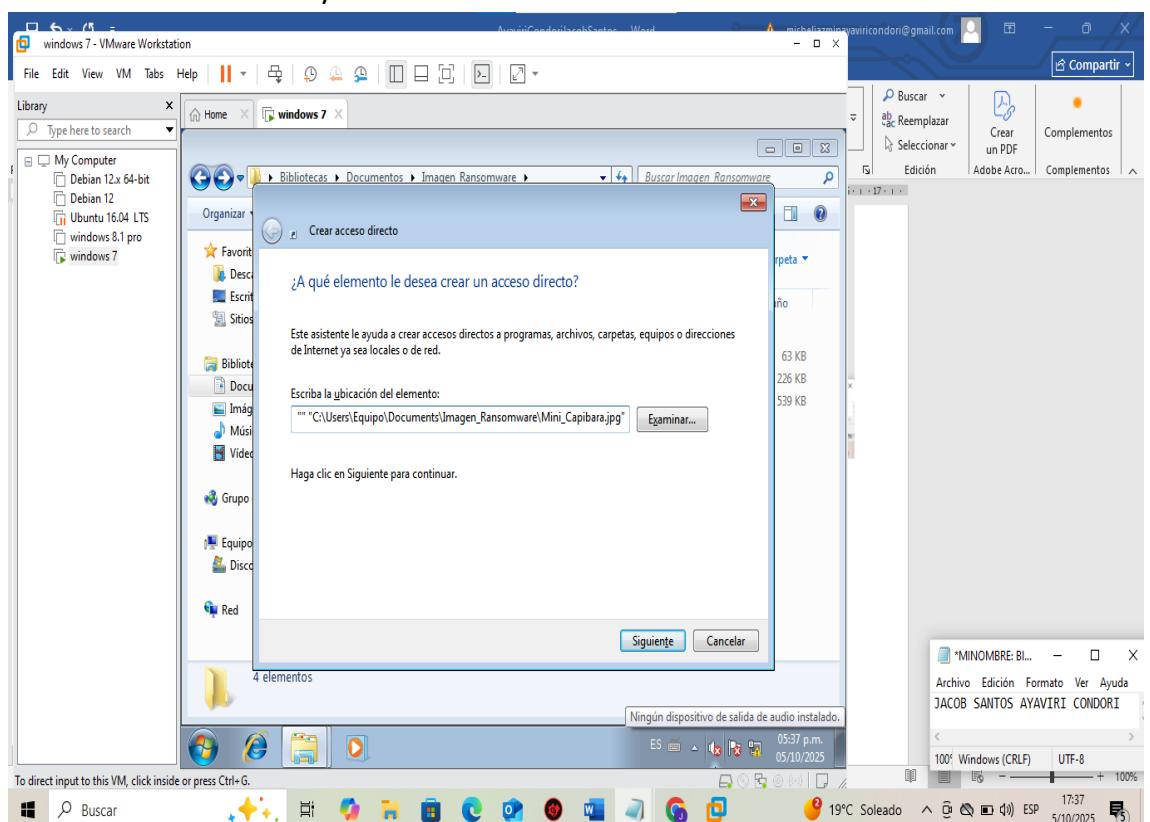
Extraemos petya



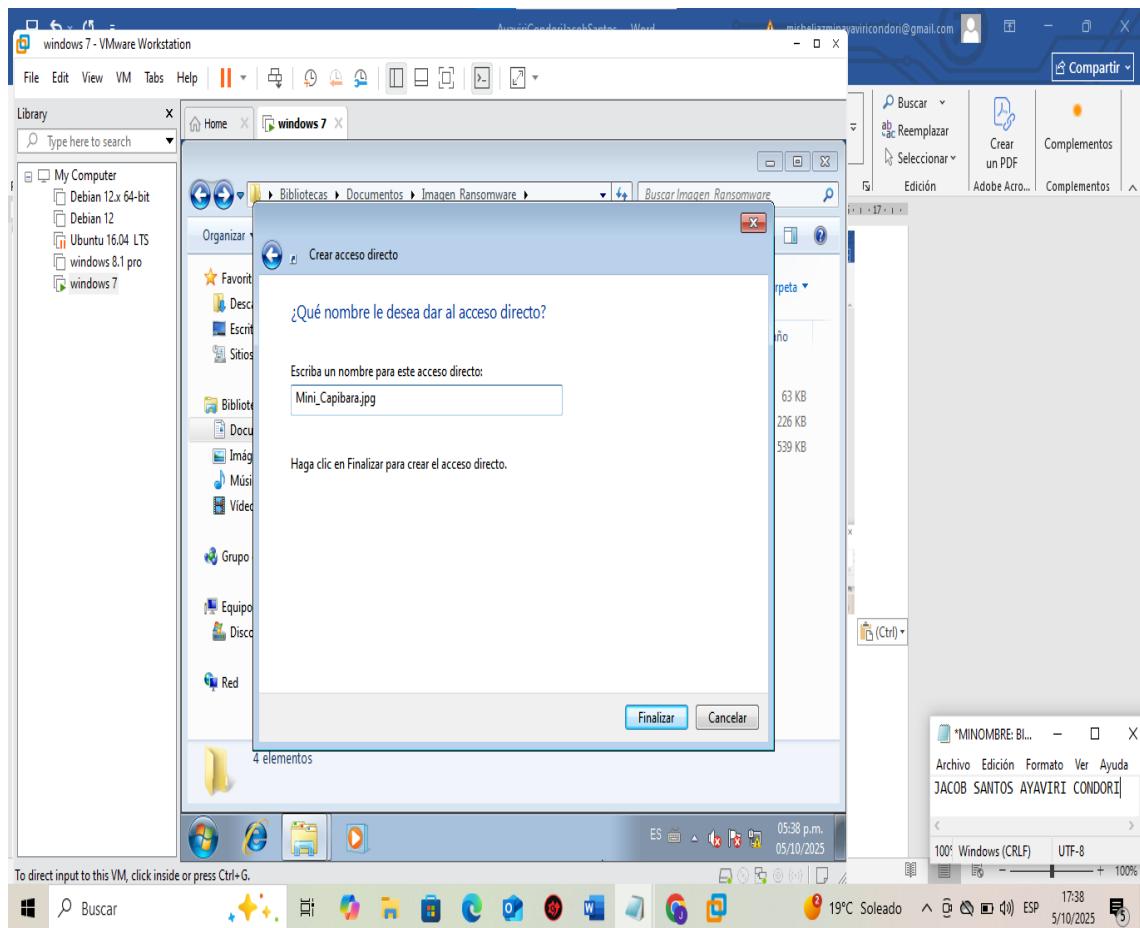
Movemos petya.exe a donde la imagen



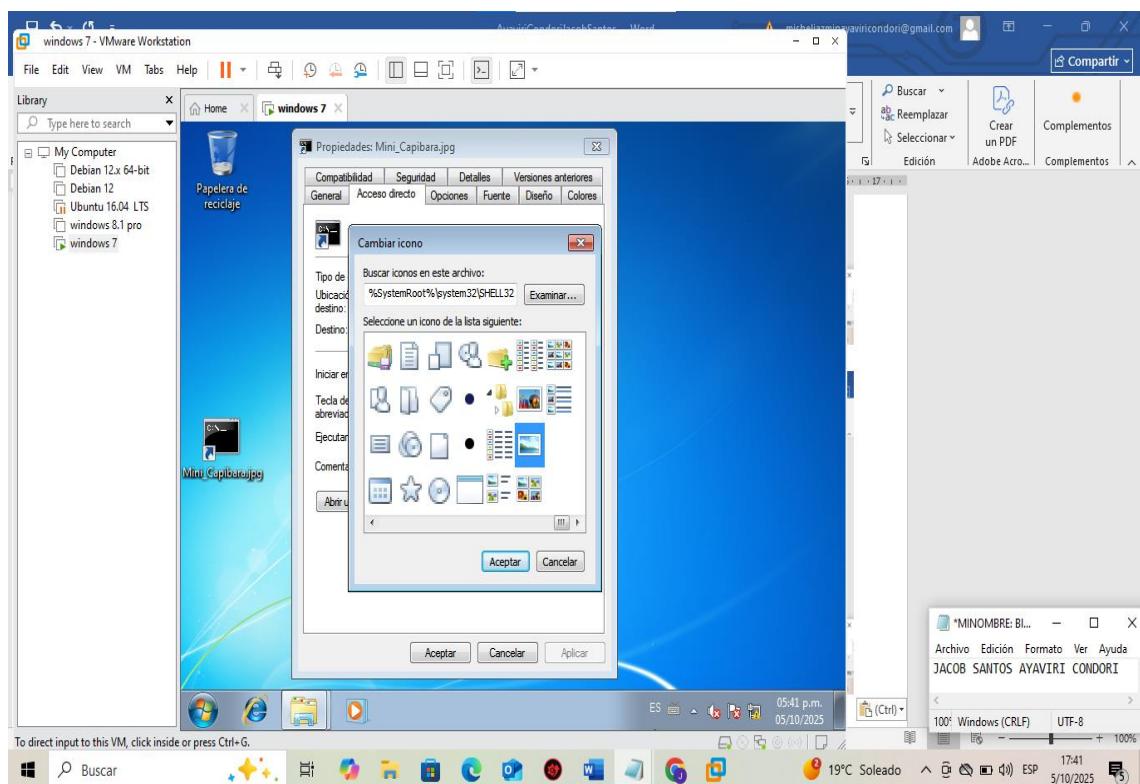
Nos vamos al escritorio y creamos un acceso directo



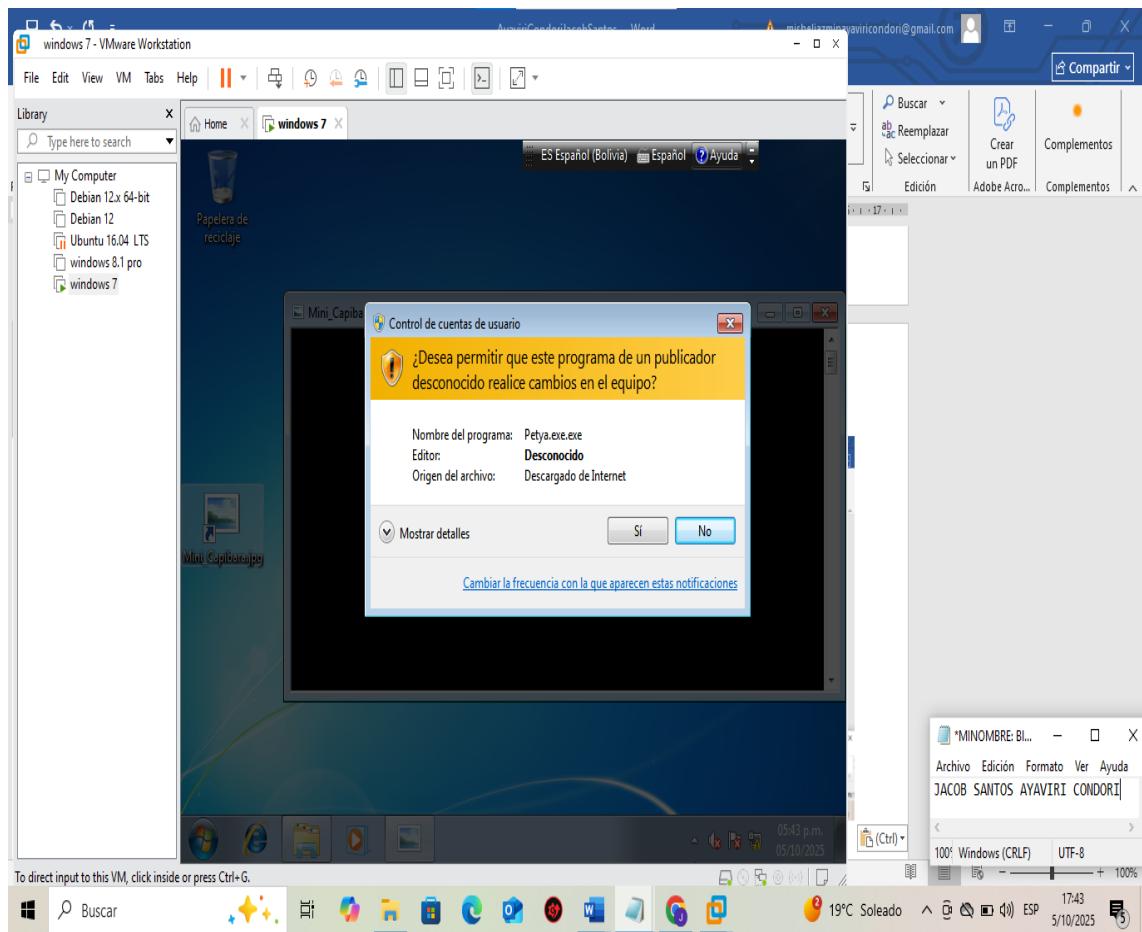
Le ponemos nombre



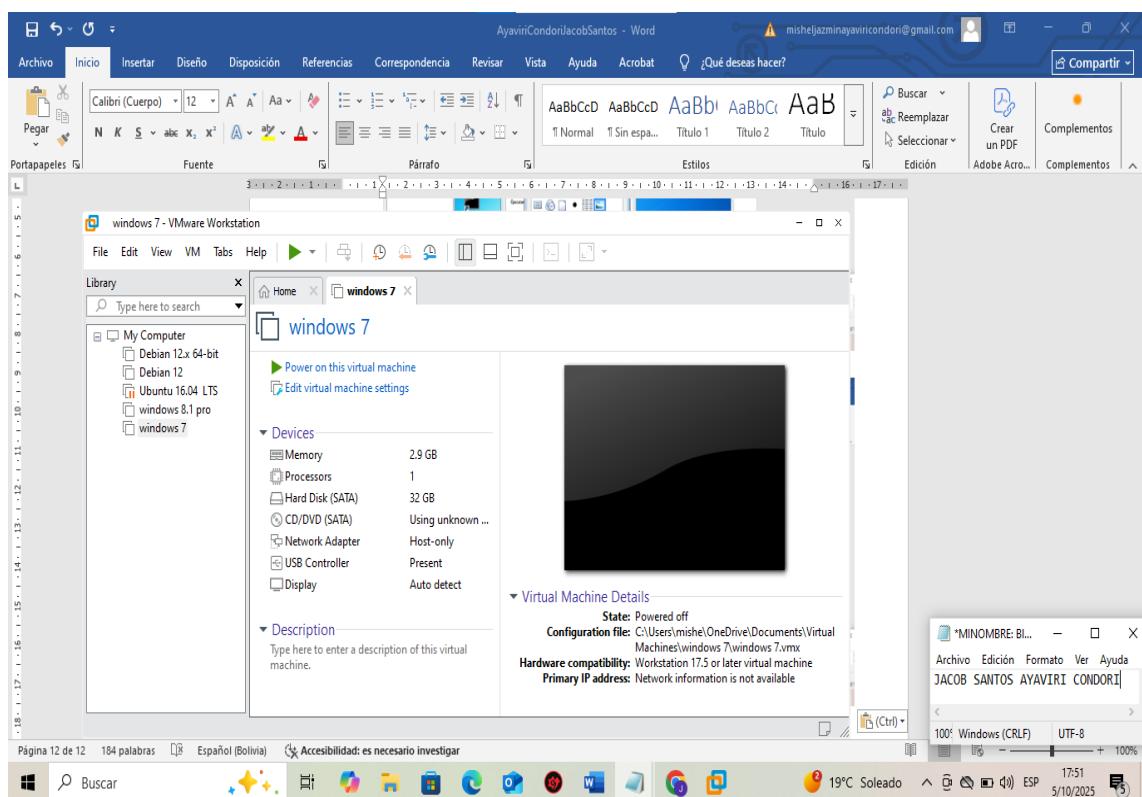
Cambiamos el icono



Lo ejecutamos

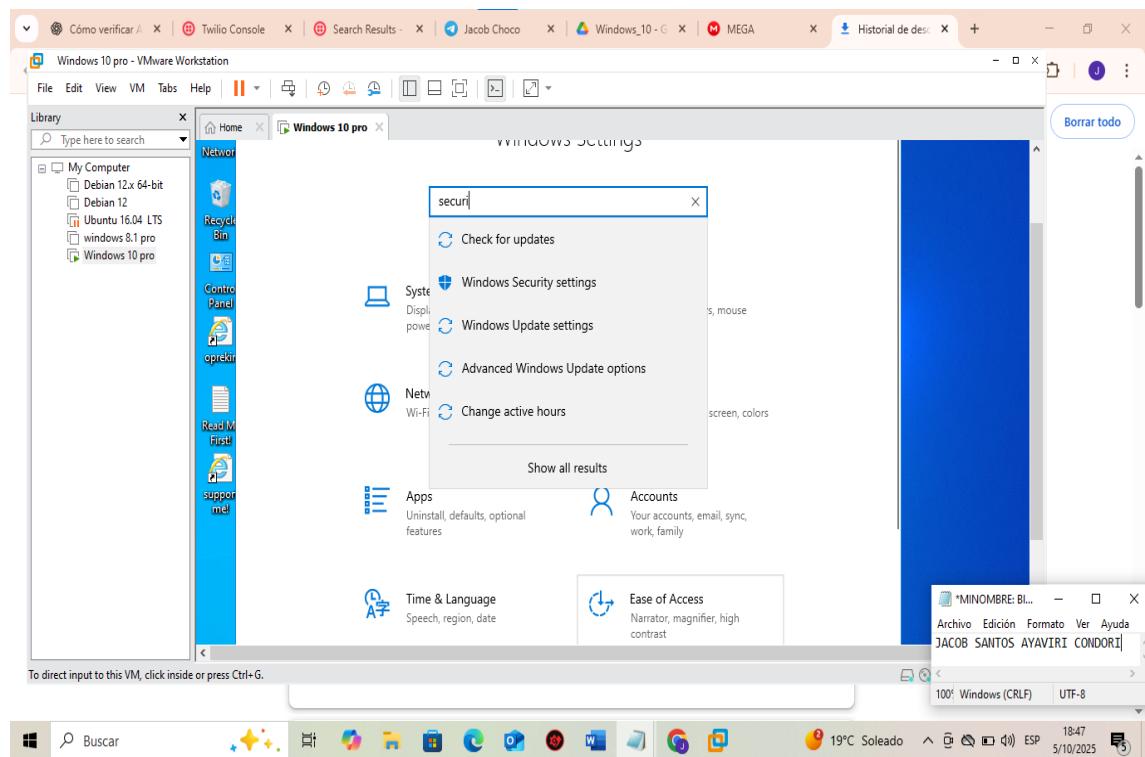


Final

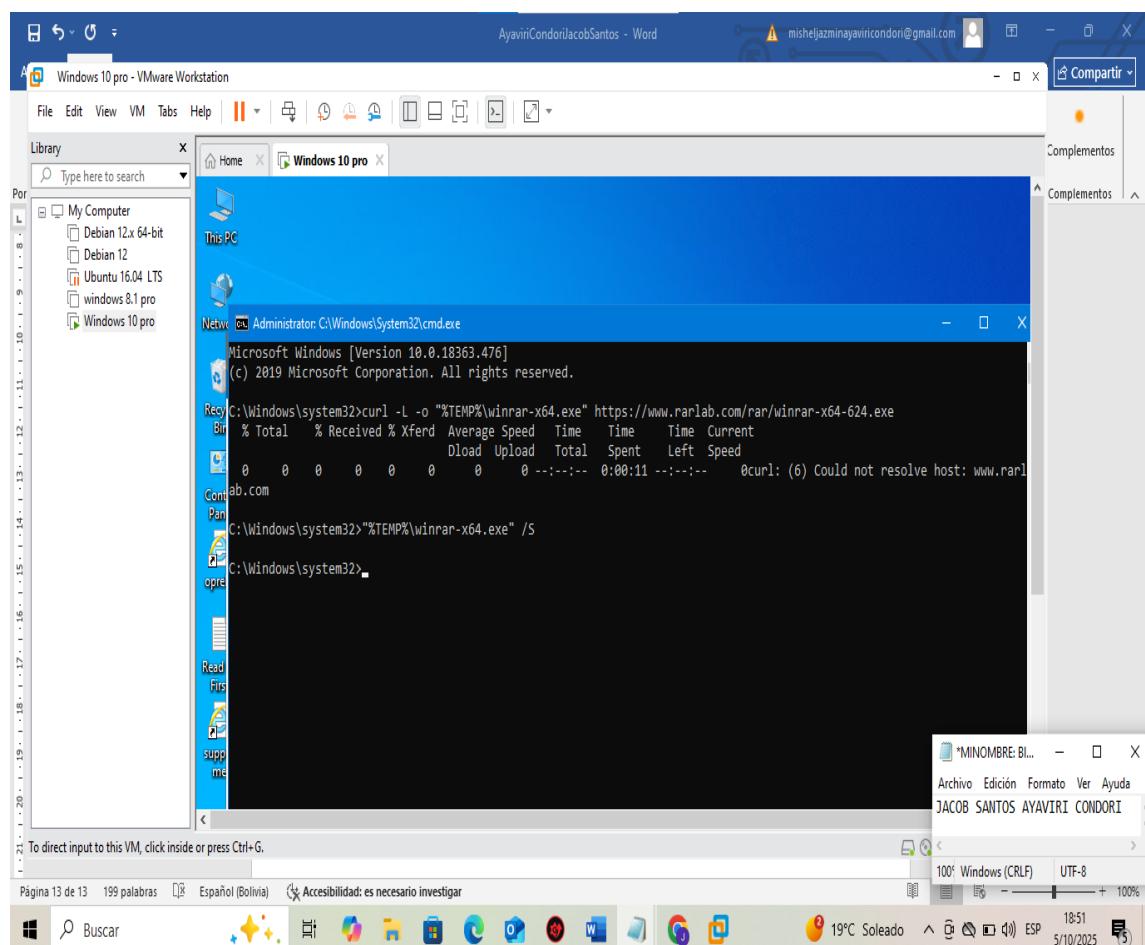


EVALUACION 2

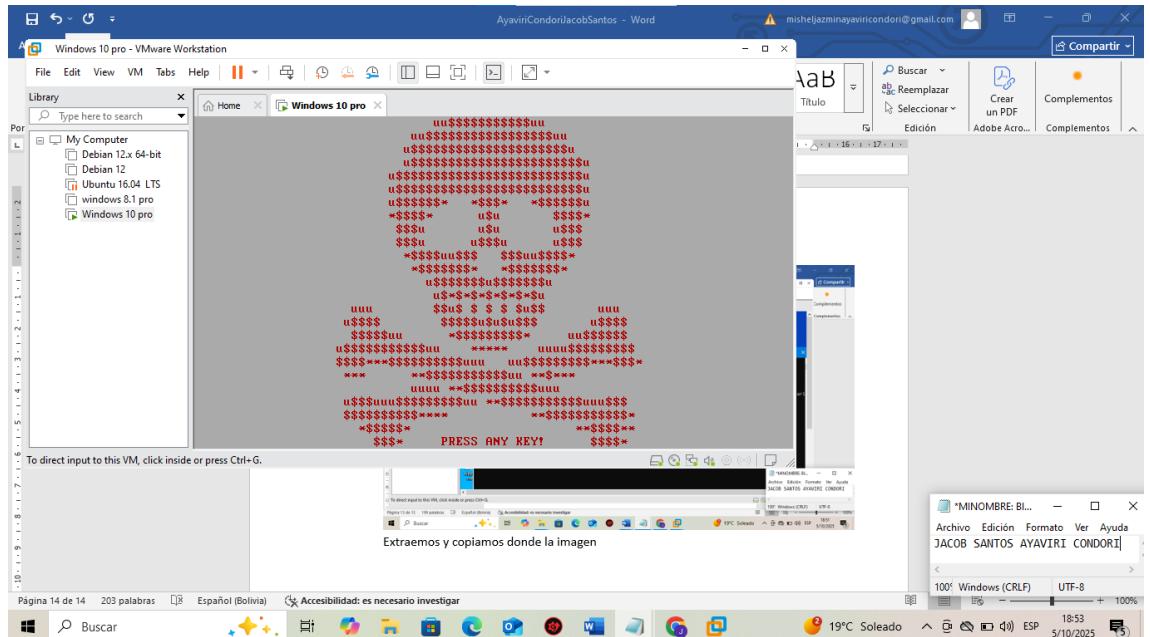
Desactivar todos las medidas de seguridad de Windows



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