# Fundamentos de Ciberseguridad y Retos CTF

Ensayo Reflexivo y Práctica Guiada

Juan Julián Paniagua Rico

1 de diciembre de 2025

# 1. Ensayo Reflexivo: La Seguridad de los Datos en la Era Digital

## 1.1. La Importancia de la "Inseguridad"

En el mundo actual, la creencia de que un sistema puede ser completamente seguro es una falacia que ha sido desmentida repetidamente por la realidad. Durante el taller de ciberseguridad, quedó evidenciado que ningún sistema es 100 % seguro, no por deficiencias técnicas exclusivamente, sino por la naturaleza misma de la tecnología y, más importante aún, por el factor humano.

Los vectores de ataque demostrados en el taller revelaron que la seguridad no es un estado absoluto, sino un proceso continuo de adaptación y mejora. La seguridad perfecta es un objetivo inalcanzable porque la tecnología evoluciona constantemente, y con ella surgen nuevas vulnerabilidades. Cada actualización, cada nueva funcionalidad, cada integración de sistemas representa una potencial superficie de ataque que debe ser evaluada y protegida.

El factor humano emerge como el eslabón más débil en la cadena de seguridad. La ingeniería social, demostrada en múltiples ocasiones durante el taller, aprovecha la psicología humana: la confianza, la curiosidad, el miedo o la urgencia son explotados por atacantes para vulnerar sistemas que técnicamente podrían ser robustos. Un empleado que comparte credenciales, un usuario que hace clic en un enlace malicioso o un administrador que configura incorrectamente un firewall pueden comprometer años de inversión en infraestructura de seguridad. Por ello, la educación continua en ciberseguridad no es opcional sino imperativa para toda organización que maneje datos sensibles.

## 1.2. CTFs como Herramienta de Aprendizaje

Las competencias Capture The Flag representan una metodología de aprendizaje transformadora para la formación de profesionales en seguridad informática. Más allá de la adquisición de habilidades técnicas específicas, los CTFs desarrollan competencias fundamentales que definen a un profesional de élite en este campo.

En primer lugar, los CTFs cultivan el pensamiento crítico y analítico. Enfrentarse a un reto CTF requiere descomponer problemas complejos en componentes manejables, identificar patrones ocultos y formular hipótesis que deben ser probadas metódicamente. Esta capacidad de análisis estructurado es esencial no solo para resolver vulnerabilidades, sino para diseñar sistemas seguros desde su concepción.

Además, estas competencias fomentan la resiliencia y la persistencia. En el mundo real de la ciberseguridad, los problemas rara vez se resuelven al primer intento. Los CTFs enseñan

que el fracaso es parte del proceso de aprendizaje, que cada intento fallido proporciona información valiosa y que la perseverancia es tan importante como el conocimiento técnico. Esta mentalidad de crecimiento es invaluable en un campo donde las amenazas evolucionan constantemente.

Finalmente, los CTFs promueven el aprendizaje autodidacta y la actualización continua. La naturaleza diversa de los retos obliga a los participantes a investigar, experimentar con nuevas herramientas y mantenerse al día con las últimas tendencias en seguridad. Esta curiosidad intelectual y capacidad de autoaprendizaje son características distintivas de los profesionales más exitosos en ciberseguridad.

## 1.3. Interés Personal: Criptografía

De todas las categorías presentadas durante el taller, la criptografía fue la que más captó mi atención por su elegancia matemática y su relevancia crítica en la era digital. La criptografía no es simplemente el arte de ocultar información; es la ciencia que sustenta la confianza en el mundo digital moderno.

Lo fascinante de la criptografía radica en cómo conceptos matemáticos abstractos se traducen en protecciones tangibles para nuestra privacidad y seguridad. Desde los cifrados clásicos como el ROT13 hasta los sistemas de clave pública que protegen nuestras transacciones bancarias, la criptografía representa la batalla constante entre quienes buscan proteger información y quienes intentan acceder a ella.

Además, la criptografía plantea desafíos intelectuales únicos. Requiere comprender tanto la teoría matemática subyacente como las implicaciones prácticas de su implementación. Un algoritmo criptográfico puede ser teóricamente perfecto pero fallar en la práctica debido a errores de implementación o gestión incorrecta de claves. Esta intersección entre teoría y práctica la convierte en un campo de estudio infinitamente rico y relevante para el futuro de la tecnología, especialmente ante amenazas emergentes como la computación cuántica.

# 2. Práctica Guiada: Mi Primer CTF en picoCTF

## 2.1. Reto 1: Python Wrangling

**Categoría:** General Skills
**Dificultad:** Easy
**Flag obtenida:** `picoCTF{4p0110_1n_7h3_h0us3_67c6cc96}`

### 2.1.1. Descripción del Reto

Este reto introduce el uso de scripts de Python para operaciones básicas de criptografía. El desafío consiste en ejecutar un script de Python que requiere una contraseña para descifrar un archivo y obtener la flag.

### 2.1.2. Proceso de Resolución

Para resolver este reto seguí los siguientes pasos:

1. Descargué los archivos proporcionados: el script Python (`ende.py`), el archivo cifrado (`pw.txt`) y el archivo con la contraseña (`flag.txt.en`).
2. Revisé el código fuente del script para entender su funcionamiento. El script usa las librerías `sys`, `base64` y `cryptography.fernet` para operaciones de cifrado/descifrado.
3. Ejecuté el comando en la terminal: `python3 ende.py -d flag.txt.en`
4. El script solicitó la contraseña, la cual ingresé desde el archivo correspondiente: `67c6cc9667cc9667cc9`
5. El script descifró exitosamente el archivo y mostró la flag.

### 2.1.3. Capturas de Pantalla

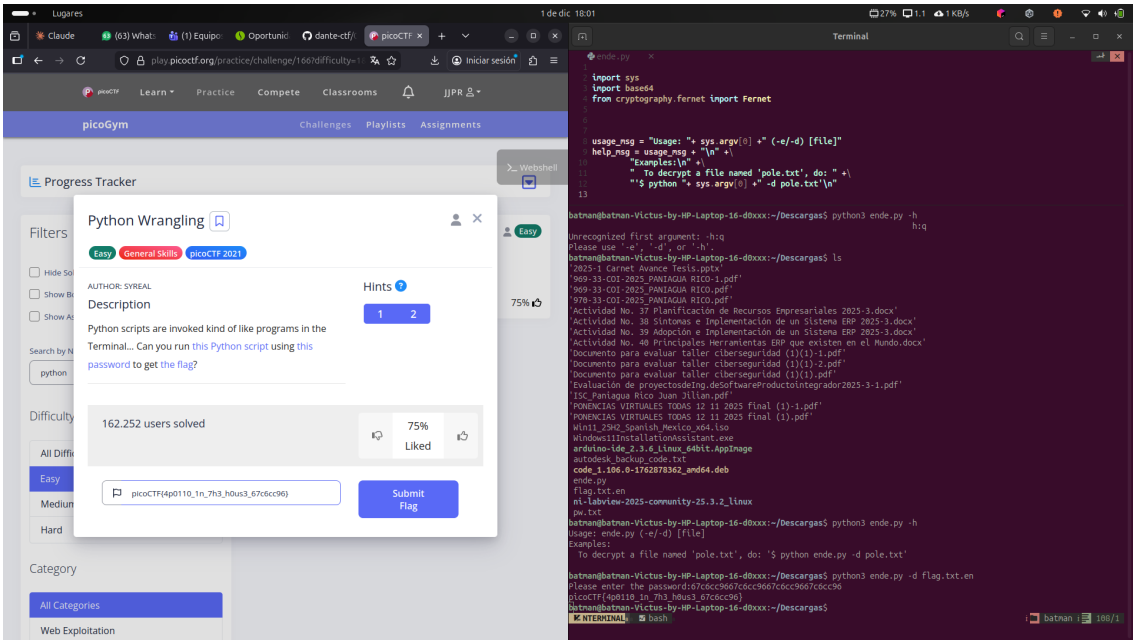


Figura 1: Vista del reto Python Wrangling en picoCTF mostrando la descripción y el proceso de resolución en la terminal

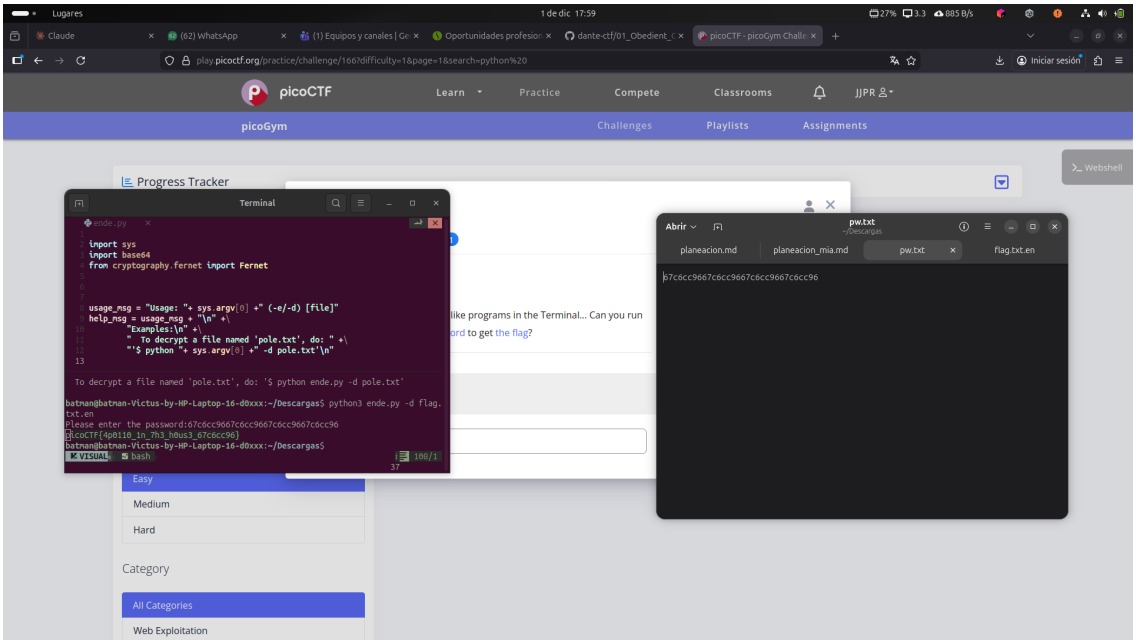


Figura 2: Ejecución exitosa del script de descifrado mostrando la flag obtenida: picoCTF{4p0110_1n_7h3_h0us3_67c6cc96}

#### 2.1.4. Aprendizajes

Este reto me enseñó la importancia de leer y comprender el código fuente antes de ejecutarlo. También reforzó conocimientos básicos sobre el uso de la línea de comandos, manejo de argumentos en scripts de Python y conceptos fundamentales de criptografía simétrica. La experiencia práctica con la librería Fernet de Python fue particularmente valiosa para entender cómo se implementan sistemas de cifrado en aplicaciones reales.

## 3. Conclusiones

El taller de ciberseguridad y la práctica en picoCTF han consolidado la comprensión de que la seguridad informática es un campo multidimensional que requiere tanto conocimiento técnico como habilidades analíticas y una mentalidad de aprendizaje continuo. Los CTFs no solo son herramientas educativas efectivas, sino que simulan escenarios del mundo real donde la creatividad, la persistencia y el pensamiento crítico son tan valiosos como el dominio técnico.

La experiencia práctica de resolver retos reales refuerza la teoría aprendida y demuestra que la ciberseguridad es accesible para quienes estén dispuestos a invertir tiempo y esfuerzo en el aprendizaje autodidacta. El camino hacia la maestría en este campo está pavimentado con desafíos, fracasos y, eventualmente, victorias que construyen tanto habilidad técnica como confianza profesional.