

# UNIVERSIDAD TÉCNICA DE COTOPAXI

# **CARRERA**

Ingeniería en Sistemas de Información

## **ASIGNATURA**

Control y Auditoria Informática

# **ESTUDIANTE**

Stalin Jaime

# **INGENIERO**

Rubio Jorge Bladimir

# CICLO ACADEMICO

ABRIL 2025 - AGOSTO 2025

**Tema:** Informe de clonación manual de Sitio Web (Phishing)

#### Introducción

Este informe se explicará el procedimiento de clonación manual de una página web con propósitos de aprendizaje, como un ejercicio práctico hacia a la ingeniería de sistemas de información y la ciberseguridad. El objetivo es entender el funcionamiento de los ataques de phishing y cómo evitarlos.

#### **Objetivo**

Comprender y aplicar el proceso de clonación manual de un sitio web para fines educativos.

#### Desarrollo

#### Herramientas que se van a utilizar

Un navegador web en mi caso (Brave)

Editor de texto (Visual Studio Code)

Framework (Django)

DBeaver(Para ver los datos guardados)

#### **Procedimiento**

#### Sitio seleccionando

El sitio seleccionado es el siguiente es la pagina web de la compañía de productos tía el apartado que vamos a clonar esta en el siguiente en lace.

Link: https://www.tia.com.ec/customer/account/login/

## Inspección de código fuente

Bueno, después de hacer el primer intento de phishing, que consistía en copiar y pegar el código, al momento de copiar el código nuevamente, pero esta vez en lugar de pegarlo en el Bloc de notas lo pegué en el editor de texto que utilicé, lo que sucedió fue que las líneas de código se transformaron en un texto enorme. Lo que pude investigar es que esto se debe al comportamiento del editor mismo.

### Descarga de recursos

Bueno, para esto solo copié las direcciones de las imágenes. Un punto negativo de esto es que cualquiera puede copiarlas, aunque deberían ser exclusivas únicamente para la empresa.

#### Cambios en el formulario

Bueno, no hubo cambios en la funcionalidad del formulario el único cambio fue en el diseño, pero se hizo todo lo posible para mejorarlo.

#### Resultados

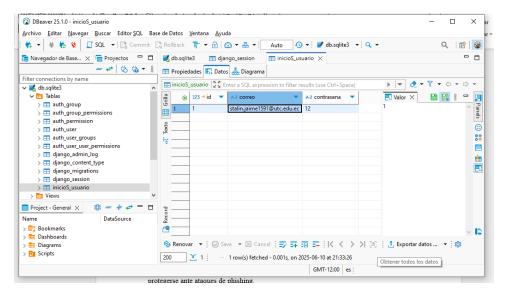
Se logró clonar el sitio seleccionado lo mejor que se pudo.

Se almacenaron los datos en la BDD.

#### Anexos







## Conclusión

La actividad permitió entender cómo se puede clonar manualmente una página web y cómo se pueden capturar datos mediante formularios, lo cual resalta la importancia de protegerse ante ataques de phishing.

## Recomendación

Se recomienda verificar siempre la autenticidad de los sitios web antes de ingresar información personal, y utilizar autenticación en dos pasos para mayor seguridad.