PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE:

INGENIERÍA EN TECNOLOGIAS DE LA INFORMACIÓN

Trabajo de Titulación

Tema:

Simulación de ataques de phishing utilizando Gophish y Zphisher en un grupo pequeño de estudiantes de la Pontificia Universidad Católica del Ecuador y análisis del impacto generado.

AUTOR:

Miguel Andrade

Tutor: Fabián Ignacio de la Cruz Domínguez

QUITO, diciembre 2024

Dedicatoria

Este trabajo de titulación se lo dedico a Milene Andrade, mi madre, y a mis abuelitos, Eufemia Morales y Marino Velepucha, por haber confiado siempre en mí y por enseñarme que nunca debo rendirme, por más difícil que sea la situación. Además, les agradezco profundamente por haberme inculcado, desde muy pequeño, esta pasión por el estudio. Este trabajo es para ustedes.

Agradecimiento

En primer lugar, quiero agradecer a mi madre por nunca haberme dejado solo, incluso en los momentos más difíciles. En aquellos momentos en los que quise rendirme, ella estuvo ahí brindándome ánimo; cuando creí que no lo lograría, me alentó a seguir adelante. Muchas gracias, madre. También quiero agradecer a mis abuelitos, Eufemia Morales y Marino Velepucha, quienes, pese a la distancia, siempre me han hecho sentir como si estuvieran cerca. Gracias por incentivarme a estudiar y superarme a mí mismo, por todo su apoyo y su infinito cariño. A mi padre Wilmer Andrade, a mis hermanos, Laddy Andrade, Tomas Andrade, Analía Andrade y a mi abuelita Herminia Andrade, les agradezco por cuidarme, estar siempre pendientes de mí y darme la fuerza y la motivación para seguir adelante todos los días.

Quiero agradecer también a mis tíos, María Alexandra Andrade, Diana Velepucha y Víctor Velepucha, por siempre haberme apoyado en mis estudios. A mi tío Luis Andrade, le agradezco por el inmenso cariño que me tiene y por haberme ayudado tanto en una de las etapas más duras de mi vida. A mis mejores amigos, Adrián Carrión, Josué Estrella y Nara Cevallos, les agradezco por estar conmigo en los momentos más difíciles, no solo de mi carrera, sino de mi vida. Gracias por su apoyo incondicional.

Por último, quiero expresar mi agradecimiento a Maruja Calle. Aunque coincidimos muy poco tiempo en esta vida, siempre la apreciaré y estaré agradecido por la hospitalidad y el cuidado que me brindó durante mi estancia en Guayaquil. También agradezco a María Calle y Diego Mora por haberme abierto las puertas de su hogar. A Elsa Calle, quien fue mi compañera en esta lucha contra el cáncer, lamento profundamente que ya no esté con nosotros, pero siempre la llevaré en mi corazón.

Agradezco de todo corazón a los doctores Ricardo Mosquera, Javier Ladines, Mayhua Lam, Fabián Villarroel y a todo el equipo médico que hizo todo lo posible para salvarme del cáncer y que, hasta el día de hoy, continúan ayudándome a llevar una vida plena.

A todos ustedes, gracias. Sin su apoyo, este gran logro no hubiera sido posible.

1. Contenido

índice de figuras

CAPÍTULO I – INTRODUCCION

En este capítulo se abordan temas fundamentales para este trabajo de titulación, como la justificación, donde se expone la razón principal por la cual se seleccionó el tema del phishing como objeto de estudio. Además, se desarrolla el planteamiento del problema, en el que se explica de manera breve cómo se formuló dicha problemática. También se presentan los objetivos que se buscan alcanzar, tanto generales como específicos, y se detalla el alcance que tendrá esta investigación dentro del contexto académico.

1.1. Justificación

En los últimos años, con el crecimiento exponencial de la tecnología, se ha producido un aumento del número de ciberataques, siendo el phishing uno de los más destacados. No obstante, las medidas de seguridad digital han avanzado, pero esta amenaza se ha convertido en una de las técnicas más efectivas utilizadas por los ciberdelincuentes. La información confidencial que manejan y las vulnerabilidades de seguridad que suelen presentar las instituciones académicas los convierten en un objetivo frecuente de estos ataques. Por otro lado, la población estudiantil es especialmente susceptible ante estas amenazas, puesto que están expuestos diariamente a múltiples plataformas tecnológicas y, en muchos casos, desconocen las técnicas para identificarlas y mitigarlas. Esto los convierte en objetivos fáciles, así que es fundamental concienciar y formar en ciberseguridad en el entorno educativo.

1.2. Planteamiento del problema

Tanto Gophish como Zphisher son herramientas que permiten crear campañas y simulaciones realistas de este tipo de ciberataques, y con las que se llevará a cabo este estudio. Este análisis se llevará a cabo con una pequeña muestra (grupo pequeño) de estudiantes de la Pontificia Universidad Católica del Ecuador para evaluar sus respuestas ante los ataques simulados. Mediante este análisis, es posible evaluar el impacto de los llamados ataques de phishing desde las perspectivas de la vulnerabilidad y grado de conocimiento de estas amenazas por parte de los estudiantes.

1.3. Objetivos

1.3.1. Objetivo general

Simular ataques de phishing utilizando Gophish y Zphisher de un grupo pequeño de estudiantes de la Universidad Católica del Ecuador, analizar y evaluar el impacto generado por este tipo de ataque en los estudiantes.

1.3.2. Objetivos específicos

1. Realizar campañas phishing de correos falsos y páginas web falsas con Gophish y Zphisher.
2. Evaluar el grado de efectividad de los ataques de phishing en función de la cantidad de usuarios afectados.
3. Analizar mediante encuestas el nivel de conocimiento de los estudiantes sobre el phishing.

1.4. Alcance

Este estudio tendrá lugar en la Pontificia Universidad Católica del Ecuador con un grupo reducido de estudiantes como participantes previos a su consentimiento, a quienes se les realizarán simulaciones de ataques de phishing con las herramientas Gophish y Zphisher. Asimismo, antes de comenzar la investigación, se recogerán datos mediante una encuesta inicial para evaluar sus conocimientos sobre esta clase de ciberataques. De este modo, se establecerá una línea de base que permitirá evaluar el grado de concienciación y capacitación sobre ciberseguridad**.**

1.5. Resumen de contenido

Por su parte, el presente estudio se compone de cuatro capítulos estructurados del siguiente modo:

El capítulo I detalla el motivo del estudio, planteando la problemática, definiendo los objetivos y delimitando el alcance de la investigación.

En el capítulo II figura el marco teórico y conceptual donde se fundamenta el estudio proporcionando los conocimientos necesarios acerca de qué es el phishing, cuáles es la funcionalidad de las herramientas utilizadas para simularlas y las consecuencias que tienen la educación superior.

En el capítulo III figurará todo el proceso de desarrollo del trabajo de titulación, junto con las fases y las herramientas empleadas para la simulación de phishing. Por último, se incluirán los resultados de la encuesta.

Finalmente, en el capítulo IV constarán las conclusiones y recomendaciones resultantes de este trabajo de titulación.

CAPÍTULO II- MARCO TEÓRICO

En este capítulo se abordarán conceptos fundamentales para una comprensión adecuada del trabajo de titulación sobre el phishing, incluyendo conceptos técnicos y aspectos legales, así como investigaciones relacionadas al phishing.

2.1. Marco conceptual

Gracias a la creciente incorporación de la tecnología en casi todos los ámbitos de la cotidianidad (salud, social, educativo y empresarial), la ciberseguridad se ha convertido en un tema fundamental. Sin embargo, el aumento en el uso de herramientas digitales ha generado un aumento en la frecuencia y la complejidad de los ciberataques. el El phishing es una de las técnicas más utilizadas por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial como contraseñas, datos bancarios o información personal. Consiste en enviar mensajes que parecen legítimos para suplantar la identidad de entidades o personas de confianza.

Del reporte realizado por Verizon, 2024 Data Breach Investigations Report (DBIR), se evidencia que el 73 % de los ataques de ingeniería social están asociados al phishing, demostrando su impacto y efectividad. Si bien las herramientas de seguridad han experimentado un gran avance, este método sigue siendo eficaz dado que se centra en el factor humano, identificado como el punto más vulnerable en la ciberseguridad.

Esta situación es especialmente preocupante en el ámbito educativo, donde la población estudiantil es particularmente vulnerable. Dado que la interacción con la tecnología es constante, no siempre tienen los conocimientos y herramientas necesarias para identificar y prevenir este tipo de ciberataques. Por esta razón, es importante llevar a cabo estudios que mejoren la ciberseguridad en las universidades mediante simulaciones de phishing. Identificar las principales áreas de vulnerabilidad y contribuir al desarrollo de programas de capacitación en ciberseguridad dentro de la institución es posible analizando el impacto de estas simulaciones en los estudiantes de la Pontificia Universidad Católica del Ecuador.

2.2. Marco Teórico

2.2.1. Ciberseguridad

"La ciberseguridad engloba una serie de procesos, soluciones tecnológicas y procedimientos recomendados destinados a proteger tus sistemas y redes críticos contra ciberataques" (Microsoft, nd). Es crucial salvaguardar la información confidencial de organizaciones e individuos, dado que cada vez más datos se almacenan en soporte digital, convirtiéndolos en un blanco más vulnerable a los ciberataques. La ciberseguridad va más allá de las medidas tecnológicas, involucra la educación y sensibilización de los usuarios en el manejo de la información para que puedan hacer frente a las amenazas cibernéticas. Por tanto, al fomentar una cultura de la concienciación y la seguridad, disminuye el riesgo de que los usuarios resulten víctimas de las ciber amenazas y se refuerza la protección general de la confidencialidad de la información.

2.2.2. Phishing

Phishing es un método de ciberataque ejecutado por delincuentes que utilizan direcciones de correo electrónico fraudulentas y páginas web engañosas para manipular a los usuarios y obtener información confidencial mediante la descarga de software malicioso. Su efectividad se basa en la desinformación y la falta de concienciación de los usuarios sobre estas amenazas, hecho que aumenta la probabilidad de ser víctima de este tipo de estafa.

2.2.2.1. Tipos de phishing

Este tipo de ciberataque tiene como objetivo engañar a las víctimas para obtener información confidencial como contraseñas, datos bancarios o credenciales de acceso. Mediante diferentes canales y estrategias, los atacantes se aprovechan de la confianza y de la falta de conocimiento de los usuarios. En este apartado se identificarán sus principales modalidades, organizadas según el método empleado y la finalidad del ataque:

- **Phishing tradicional:** El phishing tradicional es el método más común y utiliza correos electrónicos fraudulentos para captar la atención de las víctimas. A menudo, este tipo de mensajes intentan suplantar la identidad de entes de confianza, como proveedores de servicios, empresas o bancos, solicitando a los internautas que hicieran doble clic en enlaces o les piden que proporcionen información confidencial. El éxito de este tipo de ataque proviene de la destreza del actor malicioso al imitar el estilo y el contenido de los emails originales (Trend Micro, n.d.).
- **Spear Phishing:** Este tipo de phishing consiste en un ataque dirigido a personas o grupos en concreto. En comparación con el phishing habitual que se lleva a cabo de manera masiva, esta clase de ciberataque malicioso se vale de información previamente extraída de las potenciales víctimas con el fin de hacer que los correos parezcan confiables y legítimos. Como, por ejemplo, el atacante se hace pasar por un nivel superior o compañero de trabajo, lo que consigue que las víctimas les faciliten información sensible o lleven a cabo acciones específicas como transacciones bancarias. (Fortinet, 2021).
- **Whaling:** Es una variante del phishing y está orientada a miembros de alta dirección, grandes ejecutivos o personal con acceso a información sensible. Este método de malicia consiste en un diseño convincente y enfoque sofisticado con el objetivo de que parezca una comunicación real por parte de organizaciones financieras o legales. El objetivo de los atacantes es extraer información confidencial, como detalles empresariales críticos o datos financieros de alto valor. (Malwarebytes, nd).
- **Smishing:** Utiliza mensajes de texto (SMS) como vía principal para llevar a efecto la malicia. Esta técnica suele incluir links engañosos que inducen a las personas a realizar acciones como descargar aplicaciones malignas o conducen a sitios web falsos. El smishing se caracteriza por ser peligroso ya que los usuarios tienden a confiar más en los mensajes de texto porque los perciben menos susceptibles y maliciosos a las estafas que los emails. (EasyDMARC, nd).
- **Vishing:** Es un tipo de phishing que se ejecuta mediante llamadas telefónicas. Los delincuentes suplantan la identidad de personas que laboran en servicios gubernamentales, entes financieros u otras empresas de confianza para manipular a las víctimas de que realicen transferencias monetarias o compartan información confidencial. Este tipo de ataque combina técnicas de presión psicológica para persuadir a las víctimas con tácticas de ingeniería social. (Trend Micro, n.d.).

- **Pharming:** El pharming es una técnica avanzada que redirige a las víctimas a sitios web maliciosos manipulando el sistema de nombres de dominio (DNS). Incluso cuando los usuarios ingresan la URL correcta, son llevados a una página fraudulenta que simula el sitio original. Este tipo de ataque compromete la seguridad de las personas, lo hace de manera silenciosa y es particularmente peligroso debido a la dificultad de detección. (Fortinet, 2021).

2.2.3. Simulaciones de phishing

El phishing y sus simulaciones permiten educar a las personas con el objetivo de aumentar su percepción de esta amenaza dentro de un marco de seguridad protegido. Gracias a estas simulaciones, es posible evaluar la susceptibilidad y seguridad de las personas, lo que permite la evaluación de la idoneidad de las malicias y de las actividades de capacitación en cuanto a protección cibernética. Gophish y Zphisher son herramientas esenciales para desarrollar campañas de phishing que ayuden a cumplir estos objetivos preventivos y educativos.

2.2.3.1. Phishing y sus herramientas de simulación

- **Gophish:** Se trata de una plataforma de código abierto utilizada ampliamente para el gestionamiento y creación de campañas simuladas de phishing. Gracias a su intuitiva interfaz, resulta muy fácil a los administradores establecer campañas personalizadas, enviar emails de prueba y realizar un análisis del comportamiento de las personas a través de indicadores clave, incluyendo la cantidad de clics en enlaces fraudulentos y el total de cuentas de usuarios ingresados en páginas maliciosas. Todas estas características convierten a Gophish en una herramienta primordial en la medición del nivel de concienciación sobre asuntos de ciberseguridad, especialmente en ámbitos organizacionales y educativos. (Gophish, nd).
- **Zphisher:** Este tipo de ciberataque tiene como finalidad manipular a las víctimas para obtener información confidencial, como contraseñas, datos bancarios o credenciales de acceso aprovechando la confianza o el desconocimiento de los usuarios. En función del método empleado y el objetivo del ataque, se clasifican las principales modalidades de phishing.

2.2.3.2. Técnicas de simulación de phishing

- **Simulación de Páginas Web Falsas:** Esta técnica consiste en crear páginas web falsas que redirigen a los usuarios a sitios web similares a plataformas oficiales con el objetivo oculto de obtener información confidencial. Además, es importante destacar que Zphisher es una herramienta muy útil para crear sitios web fraudulentos realistas basados en plantillas predeterminadas, lo que permite analizar cómo responden sus usuarios a esta clase de engaños (Gaikwad, 2023).
- **Simulación de Smishing (Mensajes de Texto):** Por su parte, el Smishing es un método mediante el cual se envían de forma engañosa mensajes de texto que contienen enlaces que direccionan a la víctima a sitios web maliciosos o le indican qué información debe proporcionar. Con este método se evalúan las debilidades de los usuarios dependientes de aparatos móviles, el cual son susceptibles de ser víctimas de ciberataques cada vez con más frecuencia (Trend Micro, n.d.).
- **Simulación de Vishing (Llamadas Telefónicas Fraudulentas):** Los atacantes simulan ser agentes de instituciones de confianza gracias a la técnica del vishing a fin de persuadir a los usuarios que proporcionen contraseñas u otros datos sensibles o que realicen transferencias financieras. Aunque es relativamente poco frecuente, su efecto en la sensibilización de los usuarios frente a las estrategias avanzadas de ingeniería social ha quedado demostrado (Verizon, 2024).
- **Simulación Híbrida:** Mediante esta técnica se integran correos electrónicos con vínculos a páginas web fraudulentas o mensajes de texto destinados engañar a las personas para que interactúen dentro de plataformas maliciosas. La finalidad consiste en replicar las tácticas empleadas por los ciberdelincuentes en la etapa actual (Kumar, Gupta, & Singh, 2023).
- **Simulación Gamificada:** La Gamificación, por su parte, consiste en combinar escenarios interactivos con sistemas de puntuación y retroalimentación instantánea. A través de este enfoque, se promueve que los usuarios participen activamente, lo que aumenta en ellos su comprensión y capacidad de identificación de amenazas cibernéticas. Son particularmente útiles en contextos educativos, como herramienta que promueve el aprendizaje dinámico (Dhamija, Tygar, & Hearst, 2006).

2.2.3.3. Aplicación y comparación en la investigación

Tanto Zphisher como Gophish tienen como objetivo principal facilitar simulaciones de phishing, y las particularidades de ambos programas las hacen complementarias en aspectos diferentes. Zphisher se centra en la creación de páginas web fraudulentas que imitan a los sitios reales, convirtiéndolo en una herramienta ideal para estudiar cómo las personas interactúan con interfaces falsas, mientras que Gophish sobresale por su gran eficacia en campañas de phishing por emails, ofreciendo un análisis profundo sobre las interacciones de las personas.

En este proyecto de titulación se emplearán ambas herramientas para crear escenarios de phishing diseñados para un grupo de estudiantes de la Pontificia Universidad Católica del Ecuador. Gracias a estos escenarios se permitirá conocer su nivel de exposición frente a este tipo de ciberataques y recolectar datos que contribuyan al diseño de medidas educativas destinadas a la sensibilización y prevención en materia de seguridad cibernética.

2.2.4. Concienciación y Educación sobre Seguridad Cibernética

En la actualidad, los ciberataques, como el phishing, son una amenaza que está creciendo tanto para organizaciones como para personas. Estos métodos de fraude se valen de las vulnerabilidades de los humanos para tener acceso a información comprometida y confidencial, poniendo en riesgo la seguridad de los datos y sistemas. Por tanto, es fundamental educar y concienciar a los usuarios sobre la seguridad cibernética para prevenir estos riesgos y proteger la información corporativa y personal. Según estudios recientes, las personas con mayor conocimiento tienen considerablemente menos probabilidades de ser objeto de ataques de ingeniería social, como los emails falsos asociados al phishing (Verizon, 2024).

2.2.4.1. La capacitación y su importancia

Para protegerse de las tácticas de ataque que están en constante evolución., los usuarios deben recibir capacitación en ciberseguridad. A través de programas educativos sólidos, las personas logran desarrollar destrezas fundamentales, como identificar spam,

prevenir la apertura de enlaces fraudulentos y saber cómo denunciar intentos de ciberataques. Al desarrollar estas habilidades, no solo se reduce el riesgo individual, también se contribuye colectivamente a fortalecer la seguridad en empresas y planteles educativos (Cloudflare, n.d.).

Esta formación aporta beneficios concretos, entre los que destacan la reducción significativa de incidentes de seguridad, así como de los costes derivados de una posible recuperación de datos. De acuerdo con el reporte de IBM (2024), un 95 % de las ciber brechas se deben a errores humanos, razón por la cual es fundamental capacitar a los ciber usuarios en la prevención de fallos asociados al phishing y diversas amenazas cibernéticas.

2.2.4.2. Eficacia en la capacitación

Diversos estudios empíricos revelan que complementar simulaciones de ciberataques con iniciativas de concienciación fortalece significativamente la capacidad de los internautas para identificar y protegerse contra el phishing. De hecho, análisis recientes han revelado que las tasas de clics a enlaces dudosos han disminuido significativamente gracias a la ejecución de campañas educativas fundamentadas en simulaciones reales (Kumar et al., 2023). Gophish y Zphisher son herramientas destacadas en este contexto, capaces de realizar simulaciones realistas que incrementan tanto la efectividad del aprendizaje como las medidas de concienciación en ciberseguridad.

2.2.4.3. Aplicación en el contexto educativo

Es fundamental en el ámbito educativo, ya que procesos como la enseñanza y el aprendizaje se están digitalizando cada vez más. Los estudiantes, por su uso frecuente de las redes y plataformas digitales, son un objetivo recurrente para atacantes cibernéticos, puesto que, al no recibir una formación sólida en ciberseguridad, suelen carecer de conocimientos necesarios para proteger sus datos.

El propósito de este estudio es comprobar la eficacia de las actividades de simulación de phishing empleadas como herramientas pedagógicas orientadas a reforzar los conocimientos y habilidades para hacer frente a estas ciber amenazas. El análisis se centrará

concretamente en un grupo de alumnos de la Pontificia Universidad Católica del Ecuador. A partir de los resultados obtenidos, se diseñarán nuevas estrategias educativas para minimizar los riesgos derivados del phishing de manera que se fortalezca la ciberseguridad entre el grupo seleccionado.

2.2.5. El impacto del phishing en la Ciberseguridad

El uso de este phishing se ha popularizado como una de las ciber amenazas más usadas y maliciosas en este entorno. Esta amenaza no solo compromete datos sensibles, sino que también repercute en considerables pérdidas reputacionales, operativas y económicas tanto para organizaciones como para personas. Este tipo, al utilizar técnicas de ingeniería social, explota las deficiencias humanas, por lo tanto, es difícil prevenirlo mediante métodos exclusivamente técnicos.

Para desarrollar estrategias eficaces especialmente en el ámbito educativo, es fundamental comprender el impacto del phishing. Este proyecto de investigación busca analizar cómo pueden utilizarse las simulaciones de ataques de phishing para detectar los puntos vulnerables en los individuos y reforzar su capacidad de protección ante estos ataques.

Las recientes estadísticas ponen de manifiesto la magnitud del perjuicio del phishing en la ciberseguridad:

- Según el *2024 Data Breach Investigations Report* de Verizon, el 36% de las brechas de seguridad reportadas en el último año estuvieron relacionadas con ataques de phishing.
- IBM (2024) señala que el 95% de las filtraciones de datos tienen como origen principal un error humano, generalmente derivado de tácticas de phishing.
- Una investigación de Trend Micro (2023) reporta que el 86% de las organizaciones consideran al phishing como la amenaza más significativa dentro del panorama de la ciberseguridad actual.

2.2.5.1. Consecuencias del phishing

Las consecuencias derivadas de los ataques de phishing pueden agruparse en tres categorías principales:

- **Económicas:** Según el informe de IBM (2024), una brecha de seguridad derivada de un ataque de phishing tiene un costo promedio superior a los $4.65 millones por incidente. Este monto incluye gastos asociados a la recuperación de información, interrupciones en las actividades operativas y posibles multas legales. Las pequeñas y medianas empresas son especialmente vulnerables, ya que suelen carecer de los recursos necesarios para implementar medidas de mitigación efectivas.
- **Operativas:** Las entidades que se ven afectadas por ataques de phishing sufren perturbaciones en sus procesos internos, ya sea por la pérdida temporal de conexión a determinados sistemas sensibles o por la urgencia de verificar el incidente. Estos problemas no solo perjudican a la productividad, sino que también pueden afectar a la confianza de los socios comerciales externos, clientes o empleados (Verizon, 2024).
- **Reputacionales:** Estos ataques pueden tener un impacto negativo a largo plazo en la reputación de las organizaciones, además de los costes financieros que conllevan. El robo no autorizado de información confidencial puede deteriorar la confianza de los socios estratégicos y clientes, perjudicar la imagen pública y poner en peligro la sostenibilidad de la organización (Cloudflare, nd).

2.2.6. Marco ético y legal

La implementación de simulaciones de ciberataques de phishing desde un enfoque académico requiere una consideración cuidadosa de aspectos legales y éticos para proteger a los participantes y asegurar el cumplimiento de las regulaciones actuales. Dicho marco legal y ético establece las pautas que garantizan los derechos de las personas implicadas, preservan la confidencialidad de la información recabada y aseguran la fiabilidad de todo el proceso investigativo.

2.2.6.1. Consideraciones éticas

La investigación ética es crucial cuando se llevan a cabo simulaciones de ataques cuyas implicaciones psicológicas o académicas para los participantes podrían ser significativas. Estas son algunas de las principales consideraciones éticas:

- **Consentimiento informado:** Es esencial obtener el consentimiento previo y explícito de los participantes, proporcionándoles información detallada sobre los objetivos de la investigación, las actividades a realizar y los posibles riesgos y beneficios. Según la Declaración de Helsinki (1964), los participantes tienen el derecho fundamental de decidir libremente si desean participar en estudios que puedan afectar su bienestar emocional o físico.
- **Protección de datos personales:** Tratar información confidencial en simulaciones de phishing exige garantizar el anonimato y la confidencialidad de la información recopilada. De acuerdo con normativas como la Ley Orgánica de Protección de Datos Personales de Ecuador (2021) y el Reglamento General de Protección de Datos (RGPD) en Europa, el uso de los datos personales debe limitarse únicamente a fines investigativos en los que se garantice la protección frente a intentos indebidos de acceso.
- **Minimización del impacto psicológico:** Para evitar efectos adversos en los participantes, es imprescindible que los ataques simulados se diseñen de manera adecuada. Es preciso minimizar cualquier posible ansiedad, desconfianza o estrés, especialmente en contextos de educación, ya que es fundamental preservar la seguridad psicológica.

2.2.6.2. Regulaciones legales

Es fundamental cumplir con las normativas y leyes relacionadas con la ciberseguridad y la protección de datos para garantizar que los estudios sean legítimos y éticos. En este sentido, es importante tener en cuenta que entre las normativas relevantes se encuentran las siguientes:

- **Leyes locales de protección de datos**: La Ley Orgánica de Protección de Datos Personales (2021) en Ecuador establece normas para el almacenamiento, transferencia de datos personales y uso, requiriendo el consentimiento explícito de los titulares. Quienes incumplan esta normativa se enfrentarán a sanciones.
- **Legalidad de las simulaciones de phishing**: Dichas simulaciones deben realizarse únicamente en entornos protegidos con fines educativos y cumpliendo con las debidas autorizaciones y medidas de seguridad. Estas prácticas sin el consentimiento adecuado por parte de los usuarios pueden ser considerados como conductas de ciberataque ilegales. Por lo tanto, en este estudio se tomarán las medidas legales y éticas para certificar que las simulaciones de phishing realizadas con Zphisher y Gophish, se realicen de manera responsable y segura. Para ello se debe requerir con la debida autorización de los participantes, certificar la confidencialidad de la información recolectada y elaborar los ataques simulados de forma que se evite causar algún tipo de daño psicológico. Además, se debe garantizar a los participantes que se cumplirá según lo estipulado en la Ley Orgánica de Protección de Datos Personales de Ecuador.

2.2.7. Investigaciones previas y falta de estudio en contextos educativos.

El efecto del phishing en la seguridad cibernética ha sido tema de numerosos estudios a nivel mundial, ya que se ha convertido en una de las principales ciber amenazas. Sin embargo, la mayoría de estas investigaciones se han centrado en regiones o ámbitos corporativos con avanzados desarrollos tecnológicos, lo que ha dejado rezagadas a otras áreas como en América Latina, y concretamente en Ecuador, en donde la labor investigativa en este tema sigue siendo limitada. A continuación, se muestran algunos trabajos relevantes que sustentan este estudio.

- **Simulaciones de phishing y concienciación:** En 2023, Kumar et al. realizaron simulaciones de phishing en un ambiente empresarial usando herramientas como Gophish. La investigación reveló que los cursos de formación basados en simulaciones disminuyeron la posibilidad de que los empleados sufran ciber ataques de este tipo en un 40%. Si bien esta metodología ha mostrado gran efectividad en

entornos corporativos, su aplicación en ámbitos educativos, especialmente en Latino América, todavía es limitada.

- **Análisis de herramientas de simulación:** Gaikwad (2023) realizó un análisis comparativo de diversas herramientas utilizadas para la simulación de phishing. La investigación destacó que Gophish es especialmente efectiva para simular ataques vía correo electrónico, en tanto que Zphisher resulta ser un método eficiente para la creación de sitios web engañosos. No obstante, este estudio se centró en aplicaciones técnicas generales sin abordar su uso en contextos educativos particulares, siendo el ecuatoriano uno de ellos.
- **Factores psicológicos y sociales en el phishing:** Dhamija et al. (2006) identificaron varios factores psicológicos que aumentan la probabilidad de caer en ataques de phishing, entre ellos la presión de tiempo y la falta de conocimientos básicos en ciberseguridad. Aunque estos descubrimientos son importantes, no se han explorado ni validado en grupos específicos, como estudiantes universitarios en Ecuador, quienes pueden tener características socioculturales y tecnológicas particulares que influyan en su vulnerabilidad.
- **Estudio sobre el phishing en América Latina**: Según un informe publicado por Kaspersky LATAM, en los últimos 12 meses se detectaron más de 697 millones de intentos de phishing en América Latina, lo que representa un aumento del 140% en comparación con el año anterior. Este incremento está relacionado con el uso de inteligencia artificial por parte de los atacantes para crear mensajes fraudulentos más persuasivos.
- **Investigación sobre el phishing en Ecuador:** La Universidad Regional Autónoma de los Andes realizó un análisis sobre el phishing como delito informático en Ecuador, evaluando su evolución, regulación y las acciones necesarias para un tratamiento más efectivo de este problema.
- **Análisis de riesgos informáticos en canales electrónicos:** Según una investigación de la Universidad Politécnica Salesiana, analiza que el phishing representa una creciente amenaza en los medios electrónicos, y afecta tanto a organizaciones como a personas comprometiéndolas a actividades financieras y económicas.
- **Estudio jurídico sobre el phishing en Ecuador:** Investigadores de la Universidad Nacional de Loja analizaron el delito informático del phishing en Ecuador y

destacaron dos aspectos: la falta de normativas específicas y la importancia de reformar el marco legal actual para abordar este problema.

2.2.7.1. Carencia de estudios en el ámbito educativo

Pese a progresos significativos en la investigación contra el phishing, continúan identificándose brechas que fundamentan la necesidad de llevar a cabo este estudio, especialmente en el escenario local ecuatoriano.

Los estudios disponibles se han centrado exclusivamente en contextos empresariales o académicos internacionales, lo que ha dejado al descubierto la necesidad de analizar la forma en que los estudiantes universitarios interpretan y actúan ante los ataques de phishing. Por tanto, este estudio se propone evaluar cuál es la eficacia de las simulaciones en una muestra de alumnos de la Pontificia Universidad Católica del Ecuador.

2.2.7.2. Falta de investigaciones sobre impacto en América Latina

Las simulaciones de phishing son recursos habituales en la formación en ciberseguridad de los países desarrollados. Sin embargo, en América Latina, en particular Ecuador, existe una escasa evidencia del efecto que estas estrategias tienen en las prácticas digitales y la percepción en los estudiantes. El objetivo de este trabajo es estudiar los beneficios y desafíos de la implementación de simulaciones en el contexto educativo.

2.2.7.3. Relevancia sociocultural del phishing en Ecuador

Ecuador ha experimentado un aumento considerable en la adopción de plataformas digitales, lo que resulta en una mayor exposición a ciber amenazas, siendo los ataques de phishing particularmente relevantes. No obstante, carecemos de estudios que analicen cómo las particularidades culturales y tecnológicas propias del país influyen en las posibilidades de sufrir estos ataques. La investigación de estos factores permitirá crear estrategias efectivas de prevención adaptadas al contexto ecuatoriano.

2.2.8. Metodología

Podríamos definir la metodología como el conjunto de métodos, técnicas y estrategias utilizados para realizar una investigación de manera planificada y ordenada. Se centra en garantizar que los datos obtenidos sean coherentes, válidos y puedan reproducirse. Además, permite abordar el problema de investigación de forma lógica y estructurada. De acuerdo con Hernández Sampieri et al. (2014), define a la metodología como un sistema de métodos y procedimientos que se emplean en una investigación para lograr objetivos y responder a preguntas de investigación

2.2.8.1. Metodología cuantitativa

La metodología cuantitativa es un método de investigación centrado en la recopilación y el análisis de datos numéricos. Este enfoque permite entender fenómenos, encontrar patrones y comprobar hipótesis. Se basa en principios claros y ordenados, lo que ayuda a medir variables con precisión y analizar cómo se relacionan entre sí (Hernández Sampieri et al., 2014). Este tipo de metodología se usa mucho en áreas como las ciencias sociales, la educación y la tecnología porque permite sacar conclusiones que se pueden aplicar a un grupo más grande de personas.

2.2.8.2. Características principales de la metodología cuantitativa.

Esta metodología tiene algunas características principales como las siguientes:

- **Uso de datos numéricos:** Este tipo de metodología trabaja con datos que se expresan en números, lo que facilita su análisis y permite obtener resultados más claros y objetivos (Hernández Sampieri et al., 2014).
- **Enfoque objetivo:** Se busca evitar opiniones o interpretaciones personales, centrándose en datos concretos y medibles que se puedan comprobar (Hernández Sampieri et al., 2014).

- **Estructura planificada:** Todo el proceso sigue un plan organizado que incluye pasos como formular hipótesis, definir variables y establecer cómo se recogerán y analizarán los datos (Hernández Sampieri et al., 2014).
- **Medición de variables:** Se analizan variables específicas, las cuales se miden para entender su comportamiento o la relación que tienen entre ellas (Creswell, 2014).
- **Análisis estadístico:** Se usan herramientas y cálculos estadísticos para entender los datos, encontrar patrones y comprobar las hipótesis planteadas (Creswell, 2014).
- **Generalización de resultados:** Si la muestra estudiada representa bien a toda la población, los resultados obtenidos pueden aplicarse a más personas o situaciones similares (Hernández Sampieri et al., 2014).
- **Reproducibilidad:** Los pasos de la investigación están bien explicados, lo que permite que otros puedan repetir el estudio en diferentes contextos o con otras muestras (Creswell, 2014).
- **Relación entre variables:** Permite estudiar cómo una variable está conectada con otra, ya sea identificando relaciones o analizando si una causa a la otra (Hernández Sampieri et al., 2014).

2.2.8.3. Tipos de diseños cuantitativa

Algunos tipos de diseño en la metodología cuantitativa son los siguientes:

- **Descriptivo:** Los diseños descriptivos sirven para observar y describir fenómenos, mostrando sus características y frecuencia sin que el investigador cambie nada o manipule las variables (Hernández Sampieri et al., 2014).
- **Diseños correlacionales:** Estos diseños se usan para analizar la relación entre dos o más variables, buscando saber si están conectadas de alguna manera, pero sin afirmar que una causa la otra.
- **Diseños experimentales y cuasi-experimentales:** En este tipo de diseños, el investigador modifica una variable (llamada independiente) para ver cómo afecta a otra (llamada dependiente). Esto ayuda a probar hipótesis y entender relaciones causales (Creswell, 2014).

CAPÍTULO III: METODOLOGÍA APLICADA Y DESARROLLO

En el presente capítulo se explicará la metodología que se utilizará para desarrollar esta investigación, así como las diferentes fases en las que se llevará a cabo. Se describirá el enfoque de la investigación, el diseño elegido, las herramientas que se usarán y los pasos necesarios para recolectar y analizar los datos. Además, se detallará quiénes serán los participantes del estudio, cómo se seleccionarán y cuáles serán las normas éticas que se aplicarán para proteger su privacidad y derechos. Este capítulo será clave para entender cómo se logrará cumplir con los objetivos planteados y obtener resultados confiables.

3.1. Diseño de la investigación

Para este trabajo de titulación se empleará un diseño descriptivo dentro de la metodología cuantitativa. Este diseño permitirá analizar el nivel de conocimiento que los estudiantes poseen sobre el phishing antes de la simulación, y posteriormente comparar estos resultados con los datos obtenidos a través de estas. Este enfoque facilitará identificar posibles cambios en el nivel de comprensión y respuesta de los participantes frente a las amenazas simuladas.

3.2. Herramientas de recolección de datos

3.2.1. Simulación de phishing

Las siguientes herramientas serán usadas para la simulación de los ataques de phishing:

- **Gophish:** Se utilizará para crear campañas de phishing de correos electrónicos y para medir las métricas claves como lo son las tasas de clics y aperturas.
- **Zphisher:** Con esta herramienta se crearán páginas web falsas que se implementarán en los correos creados con gophish para determinar cuántos estudiantes ingresan sus credenciales.

3.2.2. Encuestas

Se realizará una encuesta previa la cual tendrá dos funciones, la primera será medir el nivel de conocimiento de los estudiantes acerca del phishing y la segunda será obtener el correo electrónico al cual se enviará el correo falso. La encuesta se realizará con la siguiente herramienta:

- **Google forms:** Esta herramienta nos permitirá crear una encuesta además nos permitirá visualizar los datos recolectados.
- **Gmail:** Por medio de esta enviaremos los correos electrónicos a los estudiantes.

3.3. Población y muestra

- **Población:** Estudiantes de la Pontificia Universidad Católica del Ecuador.
- **Muestra:** Se obtendrán los datos de un grupo pequeño de 20 estudiantes.

3.4. Consentimiento informado

Ya que el presente trabajo de titulación contiene simulaciones de ataques de phishing los resultados podrían verse afectados si se menciona directamente la implicación del estudio, ya que los estudiantes estarán alertas y es posible que no se tome en cuenta los correos falsos. Por lo que en la encuesta habrá un apartado de consentimiento informado general donde no se mencionara específicamente los ataques, sino más bien los objetivos generales de este plan de titulación como lo son la evaluación de conocimiento relacionados con la ciberseguridad y en este caso, el phishing.

3.5. Etapa inicial

3.5.1. Creación de la encuesta

Primero se creó una encuesta en Google forms que nos permitirá obtener datos sobre el nivel de conocimiento de los estudiantes sobre el phishing, además por este medio se solicitará un correo electrónico al cual será enviado la simulación de phishing. El cuestionario contiene las siguientes preguntas:

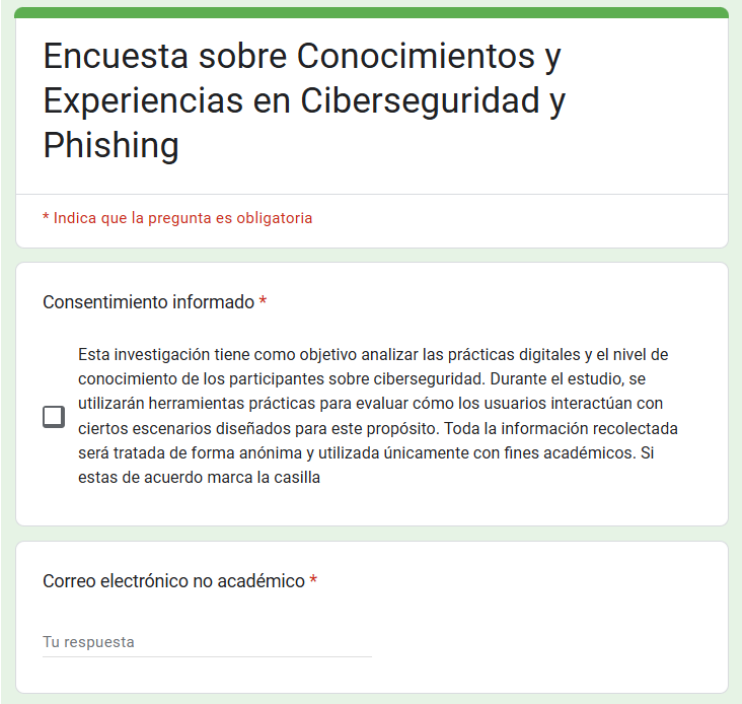

Figura 1. Muestra la parte inicial de la encuesta

En la Figura 1 se puede observar el inicio de la encuesta que es una parte muy importante ya que contiene el consentimiento informado que es crucial para evitar problemas legales y éticos ya que el presente trabajo es sobre una simulación de un ataque donde se puede conseguir información sensible. Posteriormente también se puede observar otra parte importante de la encuesta que es donde se solicita un correo electrónico que es indispensable para poder llevar a cabo las simulaciones de phishing.

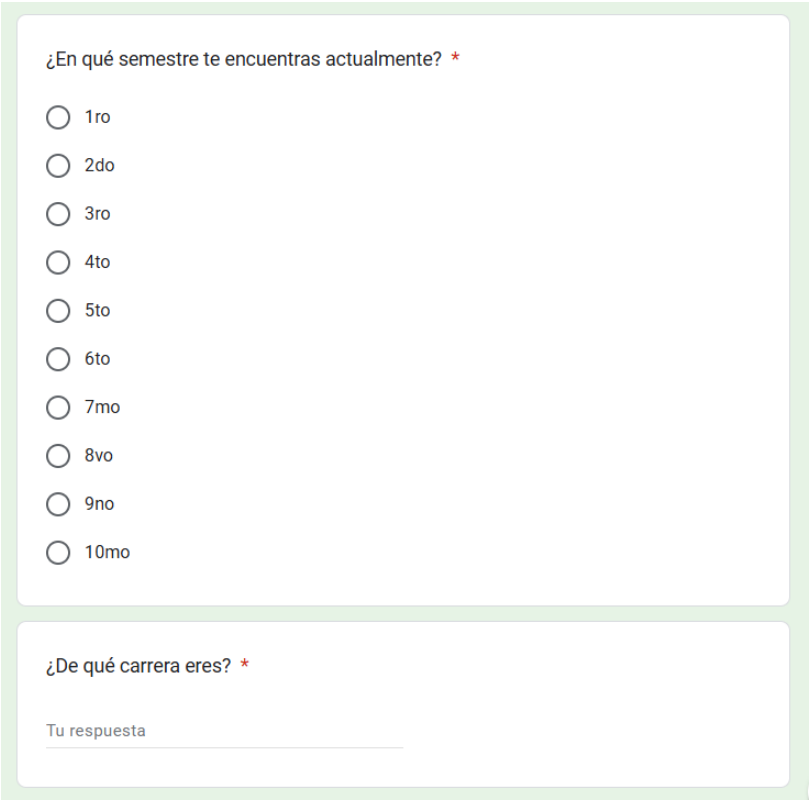

Figura 2. Parte dos de la encuesta

En la Figura 2 se incluye la siguiente parte de la encuesta donde se solicitan datos demográficos como el semestre actual y la carrera del estudiante. Esta información nos servirá para observar si es que el nivel de conocimiento sobre el phishing mejora a medida en que se avanza en la formación académica además de saber si el tipo de carrera tiene alguna influencia sobre este conocimiento.

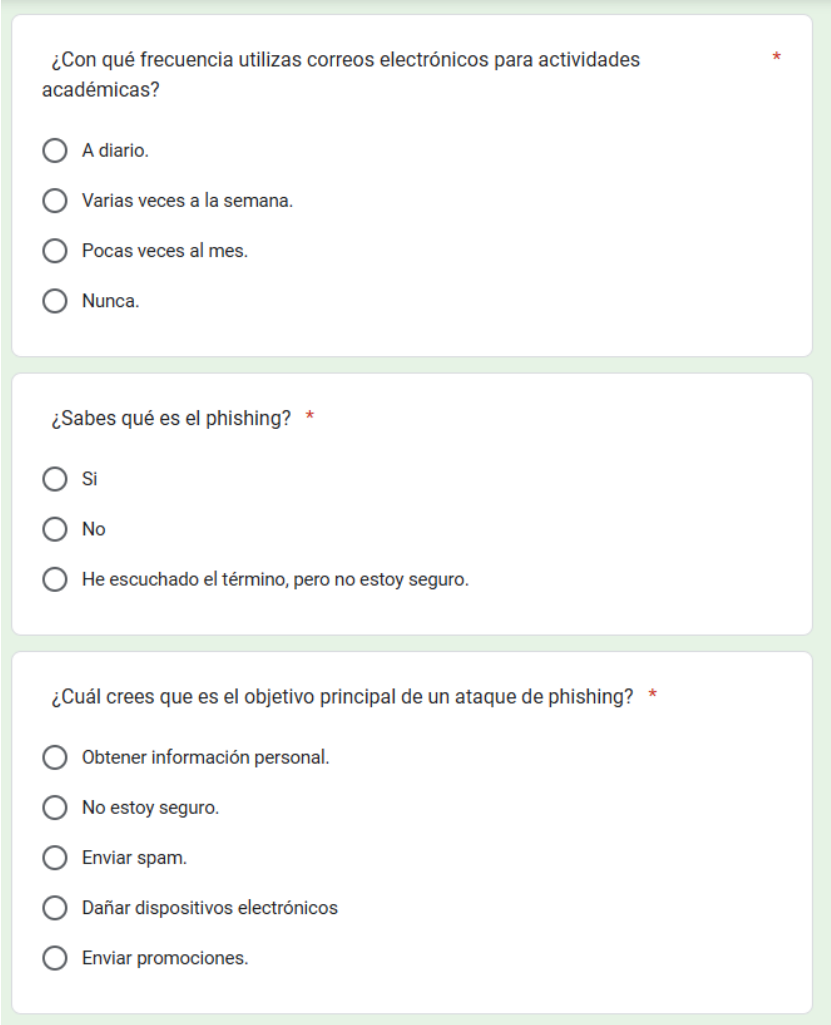

Figura 3. Muestra la parte tres de la encuesta

En la Figura 3 se presentan interrogantes sobre el conocimiento del encuestado en áreas de ciberataques en especial sobre el phishing.

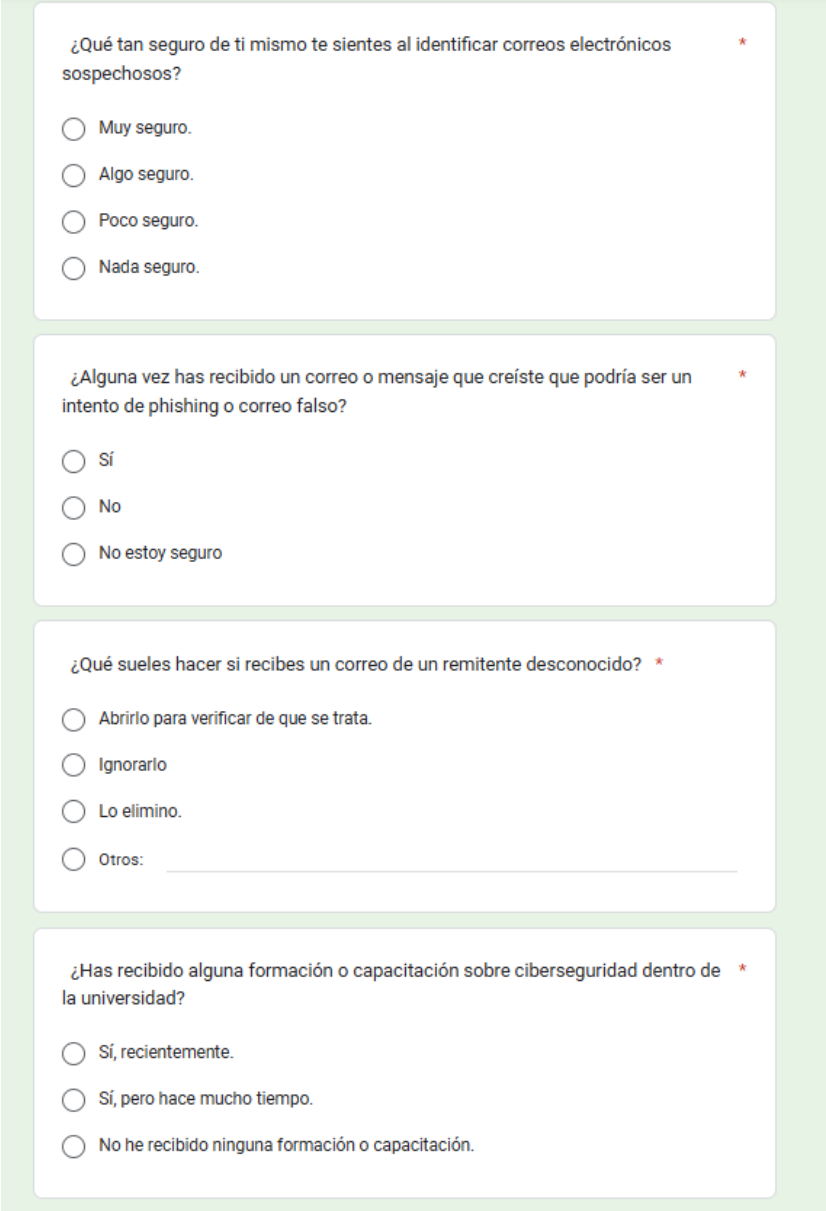

Figura 4. Muestra la parte final de la encuesta

En la Figura y 4 se muestran las preguntas sobre el nivel de conocimiento en este tipo de ataques que servirá para analizar la efectividad de dichos ataques.

3.5.2. Aplicación de la encuesta en los estudiantes de la Pontificia Universidad Católica del Ecuador y obtención de correos electrónicos.

Se realizó una encuesta a los estudiantes de la universidad, y como resultado se recopilaron varios correos electrónicos. Para proteger la confidencialidad y la seguridad de

los participantes, estos correos estarán parcialmente cubiertos con una línea roja en los registros mostrados. Estos datos son esenciales para llevar a cabo la siguiente etapa de simulación de phishing.

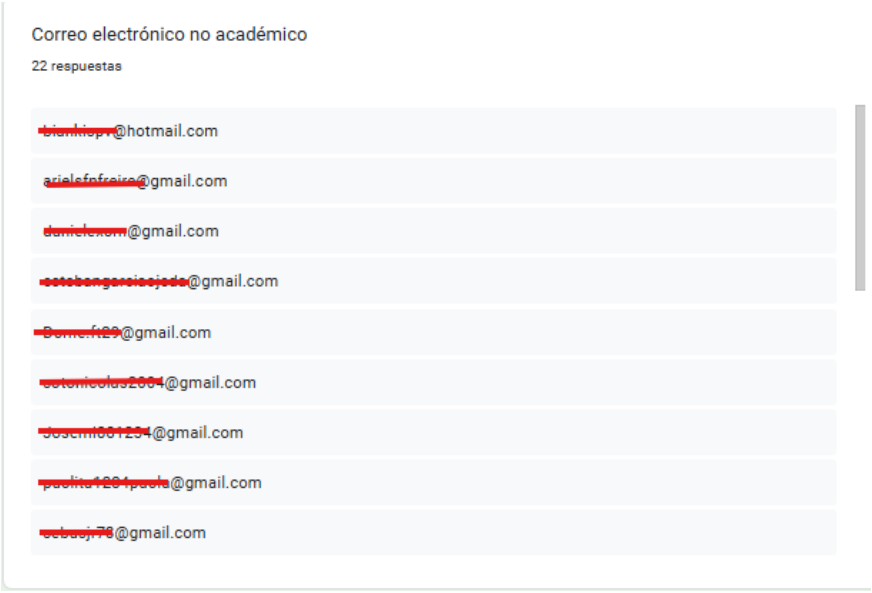

Figura 5. Muestra parte de los correos recolectados en la encuesta

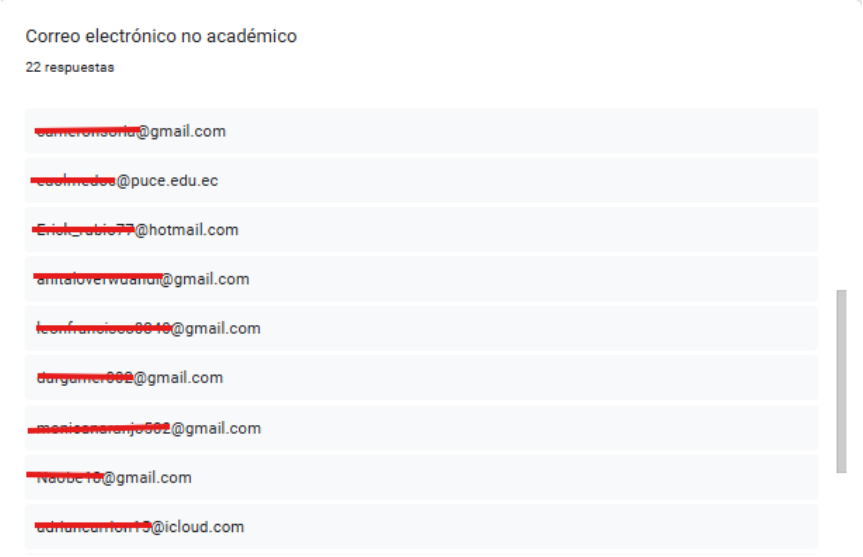

Figura 6. Muestra parte de los correos recolectados en la encuesta

Figura 7. Muestra parte de los correos recolectados en la encuesta

Las figuras 5, 6 y 7 presentan los correos electrónicos recolectados durante la encuesta, los cuales serán utilizados en la fase de simulación de phishing. Estos correos se han manejado con cuidado para proteger la confidencialidad de los participantes.

3.6. Simulación de phishing

3.6.1. Configuración de Gophish

Primero, se configuró un nuevo perfil desde el cual se enviarán todos los correos electrónicos falsos.

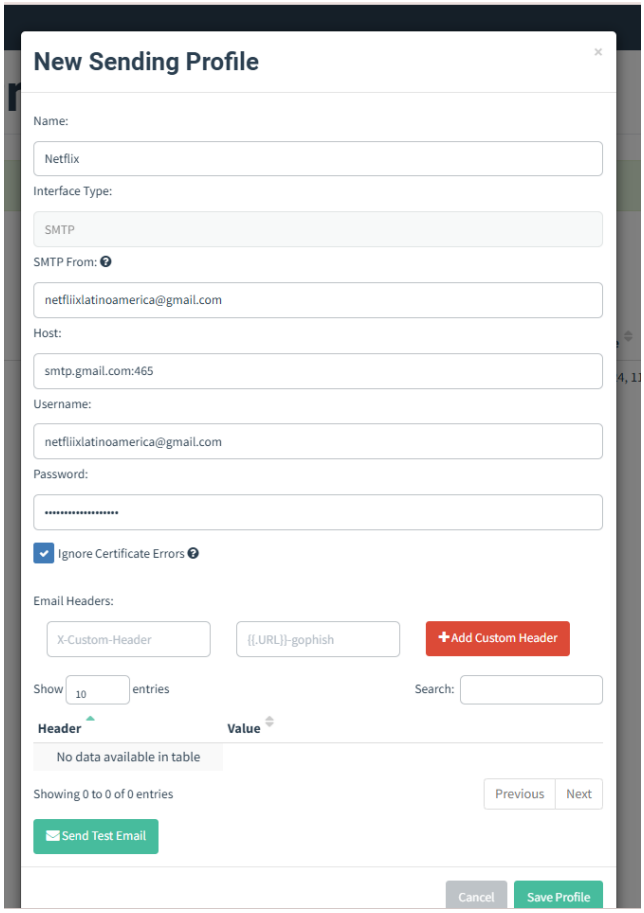

Figura 8. Configuración del perfil de envío en gophish

Para el presente trabajo de titulación, se decidió suplantar la identidad de la plataforma Netflix con el objetivo de realizar una simulación de phishing. Para ello, se configuró la dirección de correo electrónico “netfliixlatinoamerica@gmail.com”, que será

utilizada como remitente principal de todos los mensajes falsos enviados durante la investigación. En la Figura 8 se muestra claramente el correo electrónico desde el cual se distribuirán los mensajes simulados a los participantes seleccionados.

3.6.2. Configuración de Zphisher

Para la configuración del entorno que se utilizará en Zphisher, primero se seleccionará la página que será clonada, que en este caso corresponde a Netflix.

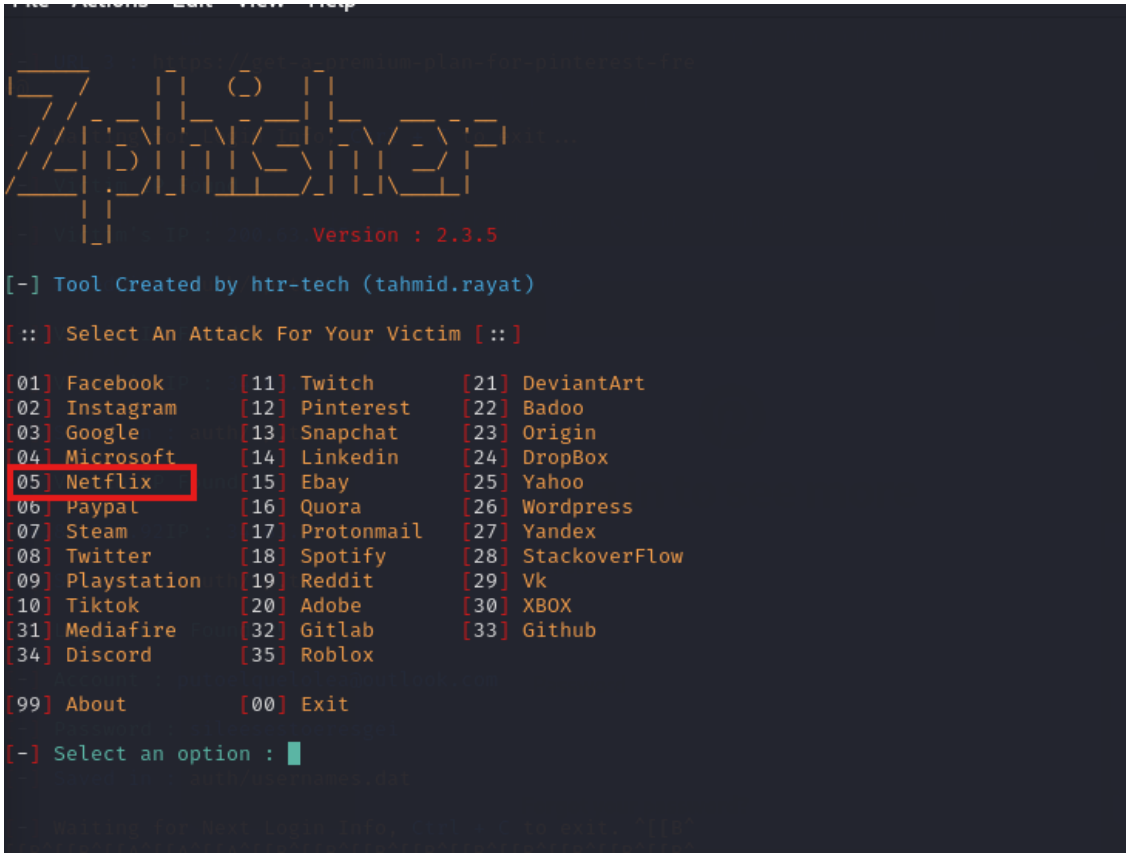

Figura 9. Muestra las opciones de duplicación de páginas de Zphisher

En la Figura 9 se presentan las diferentes opciones de clonación de páginas que ofrece Zphisher. En este caso, se seleccionará la opción "05", que corresponde a la plataforma Netflix.

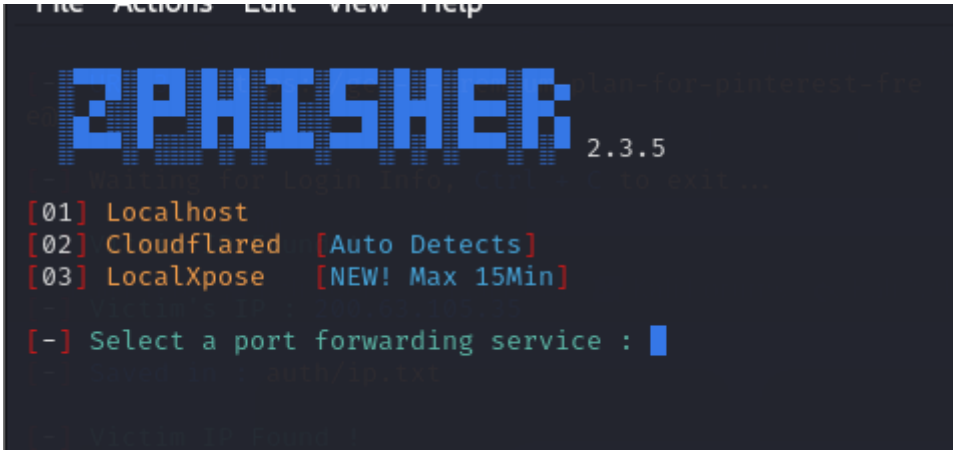

Figura 10. Muestra las opciones alojamiento de la página duplicada

De las tres opciones de alojamiento que ofrece el programa, se seleccionará la opción "02", ya que las opciones "01" y "02" son locales y no cumplirían con los objetivos del presente trabajo. La opción "02" permitirá que los usuarios interactúen con el enlace fuera de la red local. En la Figura 7 se muestran las tres opciones mencionadas

Figura 11. Muestra la url de la página web falsa creada en zphisher

En la Figura 11 se muestra la dirección "https://ton-quality-game-smooth.trycloudflare.com" correspondiente a la página web falsa de Netflix que se utilizará posteriormente en Gophish. Este enlace malicioso será incluido en los correos electrónicos enviados durante la campaña de phishing creada en Gophish.

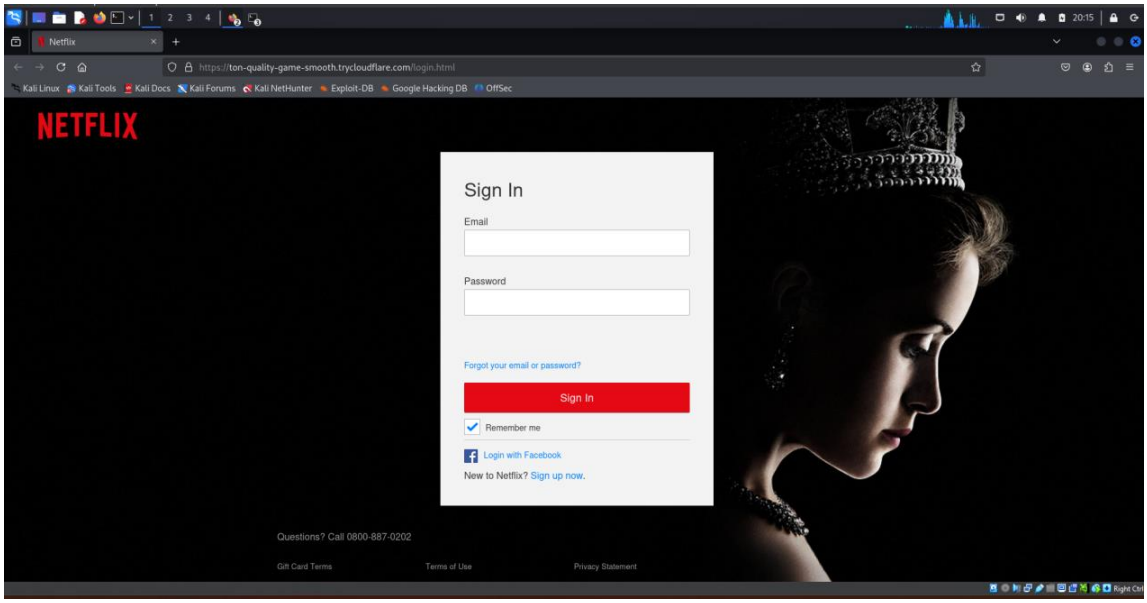

Figura 12. Muestra la página web falsa creada en Zphisher.

En la Figura 12 se presenta la página web falsa diseñada para la simulación de phishing. Esta página replica de manera casi exacta la apariencia de la plataforma oficial de Netflix, con el objetivo de engañar a los usuarios seleccionados para la simulación. Sin embargo, la principal diferencia radica en la URL, que en este caso corresponde a "https://ton-quality-game-smooth.trycloudflare.com", la misma que fue detallada previamente en la Figura 8. Este enlace malicioso será fundamental para evaluar la efectividad de la simulación.

3.6.3. Creación de la plantilla de correo electrónico en Gophish

El primer paso consiste en configurar la página a la que serán redirigidos los usuarios una vez que accedan al enlace falso. Esta configuración se realizará en el apartado denominado "Landing Pages" dentro de la plataforma Gophish. Este proceso es fundamental, ya que permite establecer el destino final al que los participantes llegarán tras interactuar con el enlace malicioso, asegurando que la simulación cumpla con los objetivos planteados en el presente trabajo.

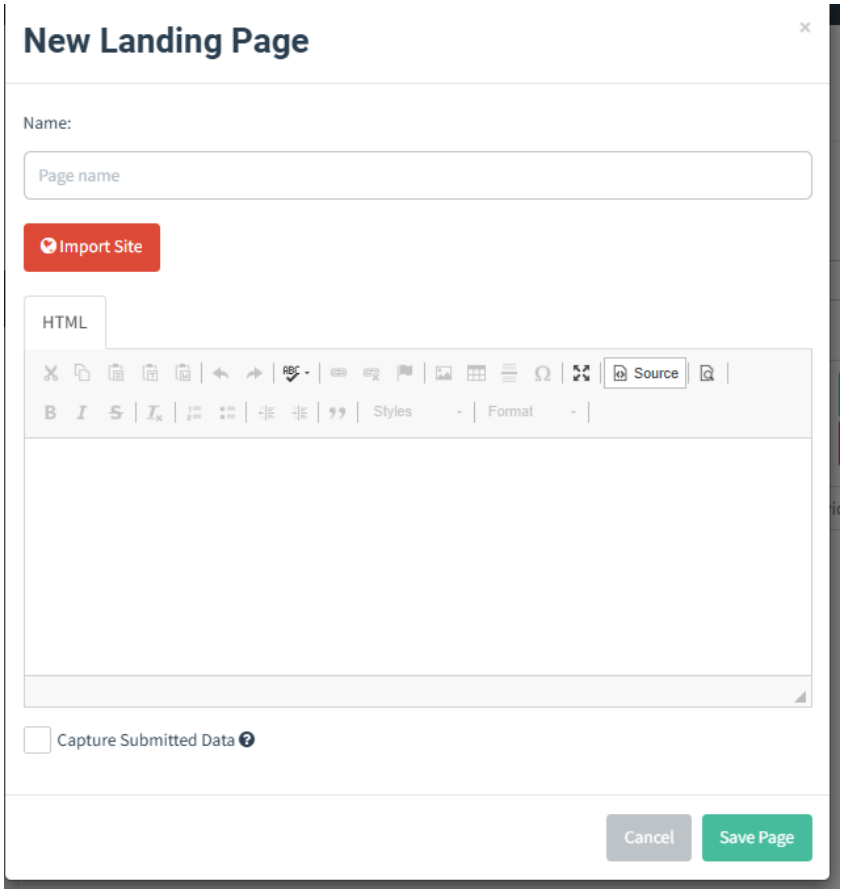

Figura 13. Muestra el "landing page" ventana de configuración Gophish.

Como se muestra en la Figura 13, en la pestaña de configuración de Gophish se configurará la URL de redirección que verán los usuarios tras interactuar con la página web falsificada. Aquí se le dará el nombre de "Netflix" para facilitar su identificación dentro de la interfaz. Dentro del campo "Import Site", se introducirá la dirección de inicio de sesión de la página falsa creada anteriormente en Zphisher, que corresponde a «https://ton-quality-game-smooth.trycloudflare.com». Es crucial realizar este paso para garantizar la coherencia y el cumplimiento de los objetivos de la presente investigación.

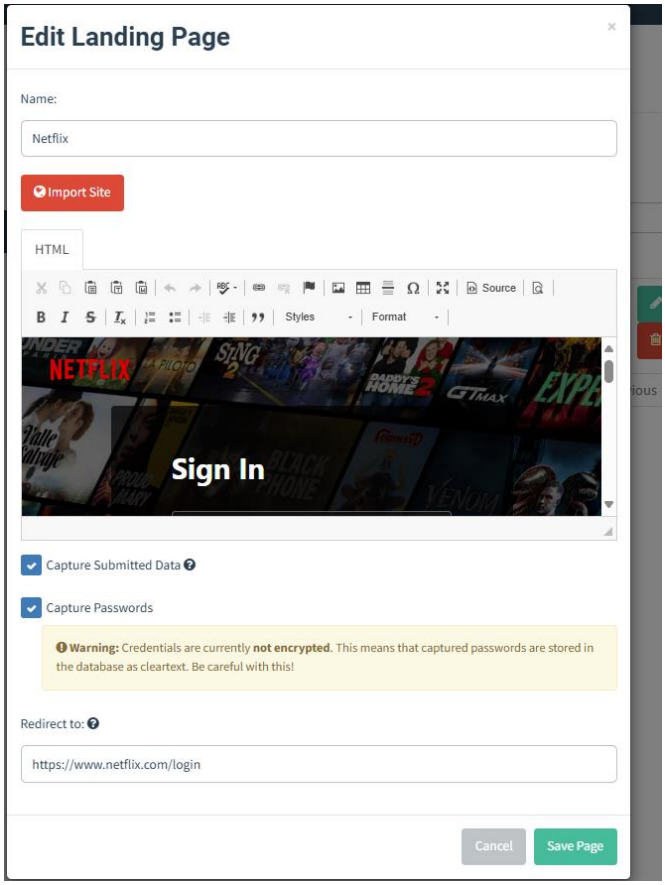

Figura 14. Muestra la configuración del "Landing Page"

Tras finalizar la configuración de la pestaña, se guardarán los cambios para asegurarse de que todo esté establecido correctamente. La Figura 14 presenta la pestaña configurada, en la que se puede apreciar una visión previa del sitio al que los usuarios serán redirigidos tras interactuar con la URL falsa. Gracias a esta opción, se puede verificar que el diseño y la funcionalidad de la página cumpla con los parámetros establecidos para la simulación de phishing, lo que asegura una experiencia realista para los participantes del análisis.

Tras esto, se pasará a configurar la plantilla del email que se enviará mientras se lleva a cabo la simulación de phishing. Dicho proceso se realizará en la pestaña "Email Templates" perteneciente a la plataforma Gophish, elaborada especialmente para personalizar y crear correos electrónicos. Aquí se trabajará en el contenido del mensaje, incluidos los textos y elementos visuales, que tiene como objetivo atraer la atención de los receptores y conseguir

que interactúen con el sitio web falso. Se requiere de este proceso para garantizar que el email resulte creíble y logre los objetivos deseados del presente trabajo de investigación.

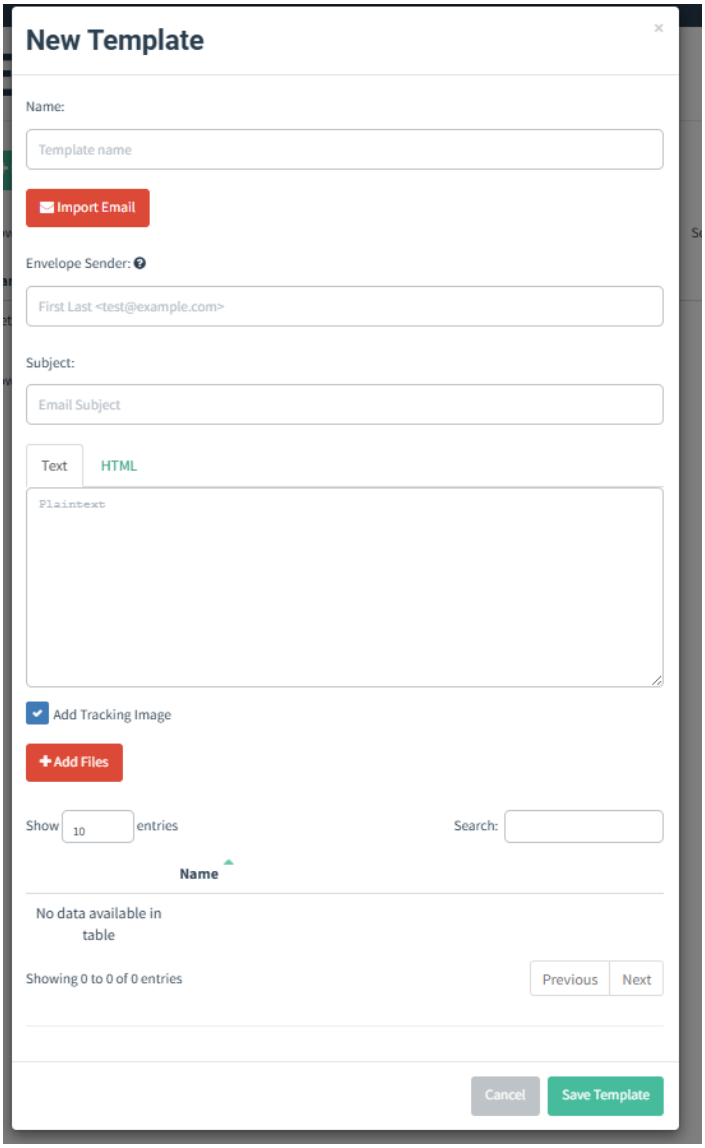

Figura 15. Muestra en Gophish la ventana de "Email Templates"

Como se muestra en la Figura 15, se utilizará un botón llamado "Import Email" para cargar una plantilla previamente diseñada de correo electrónico. Para este proceso, se utilizará dicha función para importar una plantilla que simule los correos electrónicos oficiales de Netflix. Esta función permite reducir el tiempo necesario para diseñar el correo y garantizar que el mensaje mantenga un formato convincente y profesional, lo que aumenta

la precisión de la simulación de phishing realizado en esta investigación.

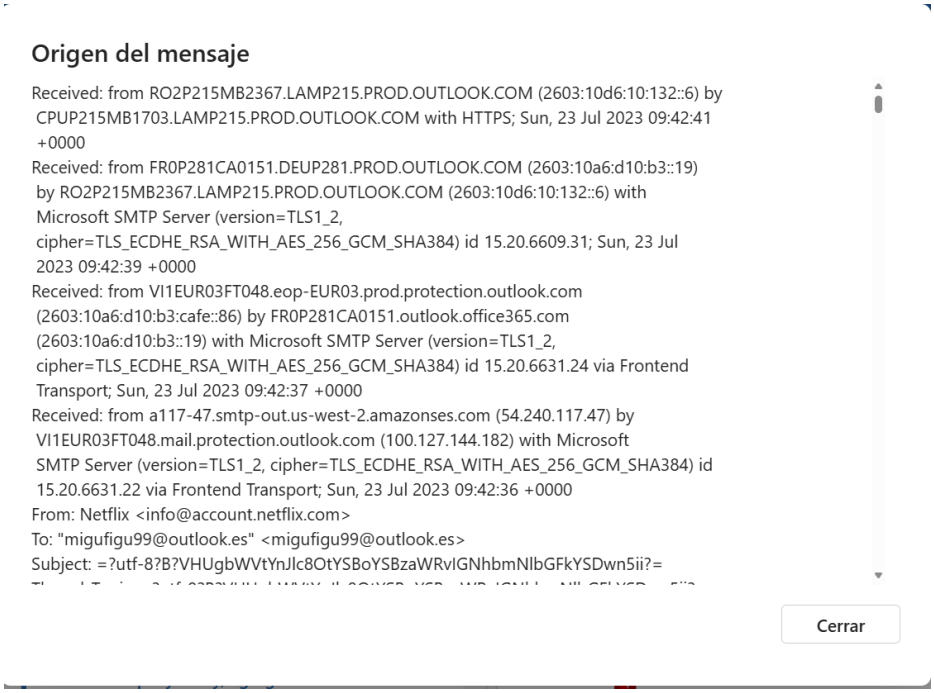

Figura 16. Muestra la plantilla del correo de Netflix y parte del código html

Tal y como se observa en la Figura 16, el código presentado se insertará en el apartado "Import Email". Gracias a este código, se establece la estructura y el contenido del email que será utilizado en la simulación fraudulenta. Este paso es crucial para que el correo simulado se asemeje lo máximo posible a los emails legítimos de Netflix y, por tanto, para que el ataque de phishing simulado sea más creíble y efectivo en esta investigación.

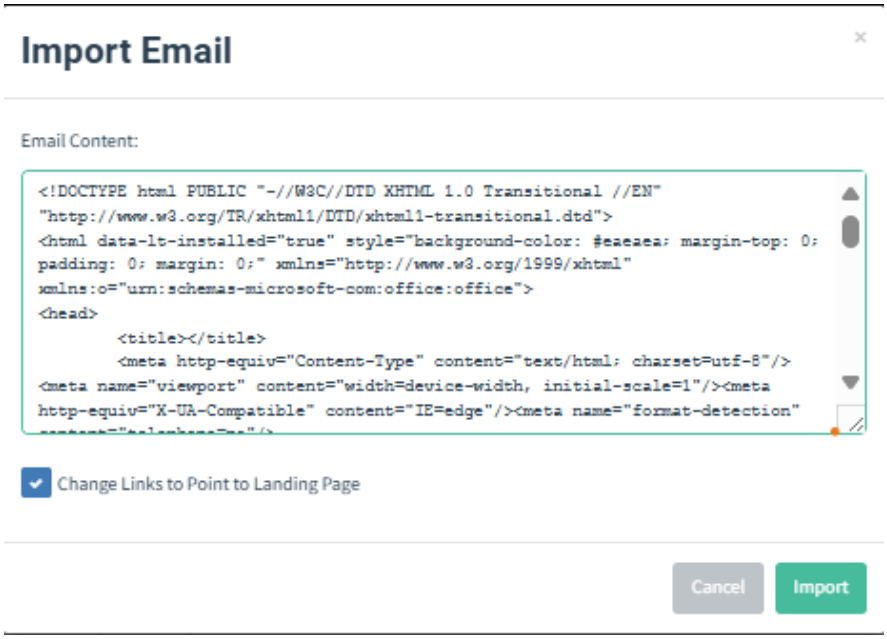

Figura 17. Muestra el código html de la plantilla del correo en el "Import Email"

La Figura 17 presenta el código HTML de la plantilla del correo obtenida de un email legítimo de Netflix, el mismo que se utilizará para simular un ataque de phishing.

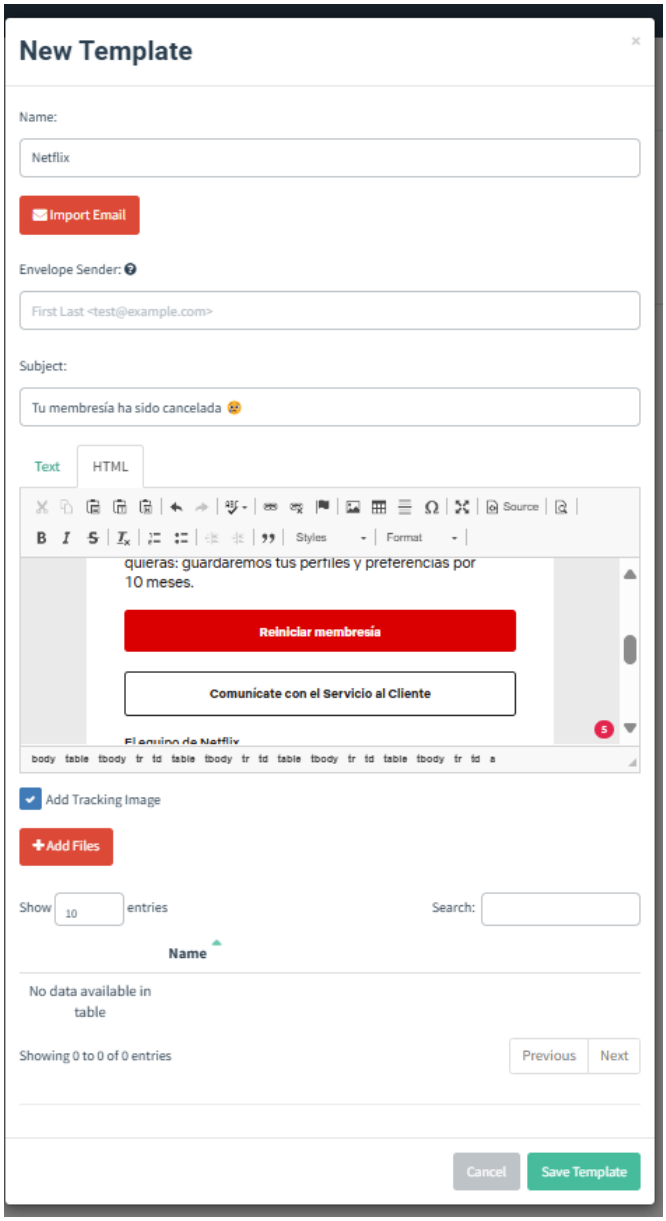

Figura 18. Muestra la configuración del "Email Template"

Como se puede observar en la figura 18, en la pestaña "Email Template" se puede observar una vista preliminar del correo electrónico que se enviará a los estudiantes. Dicha funcionalidad sirve para verificar el aspecto final del mensaje, incluida la configuración del formato, texto e incluso elementos gráficos. Este paso es fundamental para garantizar que el email tenga un aspecto convincente y profesional, basado con los objetivos de la simulación de phishing planteados en esta investigación. Asimismo, ofrece la posibilidad de efectuar ajustes si se localizan inconsistencias o errores antes de continuar el proceso del envío masivo.

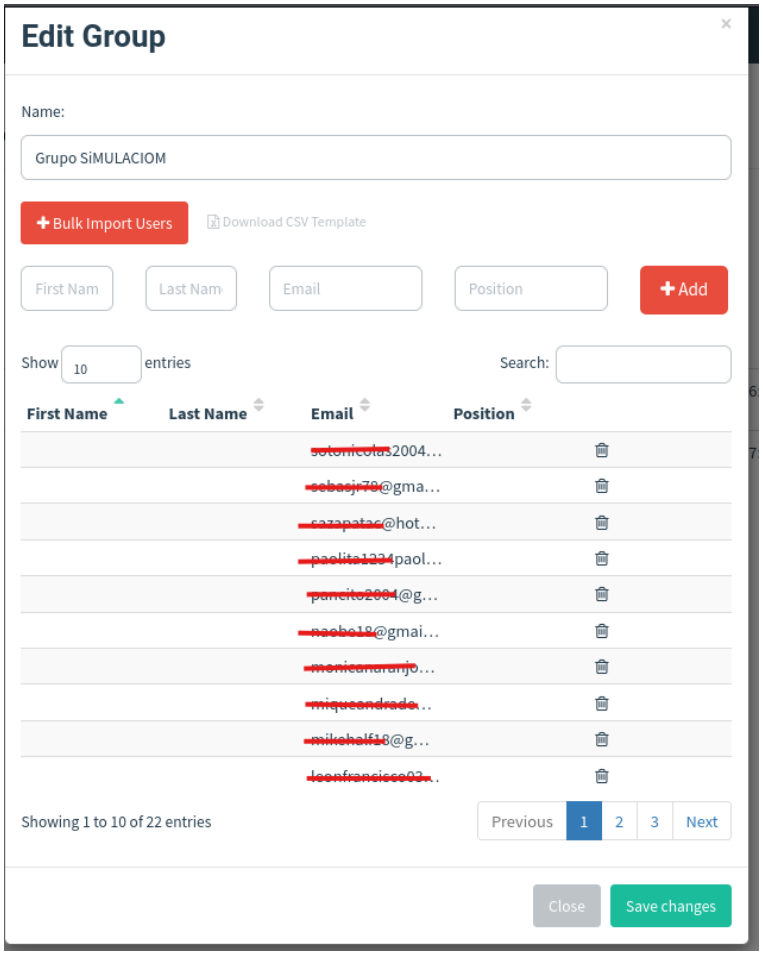

Figura 19. Muestra los correos de los estudiantes a los que se les enviara el correo malicioso en la pestaña de "New Group" de Gophsih

Tal y como se muestra en la Figura 19, en el apartado "Campaigns" se creará una nueva campaña de phishing. Aquí se configurarán distintos parámetros esenciales que garantizarán la adecuada funcionalidad de esta, entre ellos el URL del servidor donde se almacenará la página fraudulenta. Para este estudio, utilizaremos la dirección IP pública "192.168.100.145:80" como principal enlace. Este proceso es esencial porque vincula todos los elementos configurados previamente, como la página falsa y la plantilla de correo, garantizando que la campaña pueda ejecutarse de manera efectiva en el marco de la presente investigación.

3.7. Prueba antes del lanzamiento

Es fundamental cerciorarse de que todos los parámetros estén correctamente configurados antes de lanzar la campaña. En este sentido, el correo de prueba se enviará a

una dirección determinada. De este modo, se podrá verificar cuál será la apariencia del mensaje cuando los usuarios lo abran. Durante este proceso, nos aseguraremos de que todos los enlaces y elementos del mensaje funcionen correctamente, garantizando así una experiencia real y el cumplimiento eficaz de los objetivos de la simulación. Esta fase es esencial para detectar y corregir errores antes de continuar con el envío a los demás usuarios. La Figura 20 muestra cómo aparecerá el correo que recibirán los usuarios.

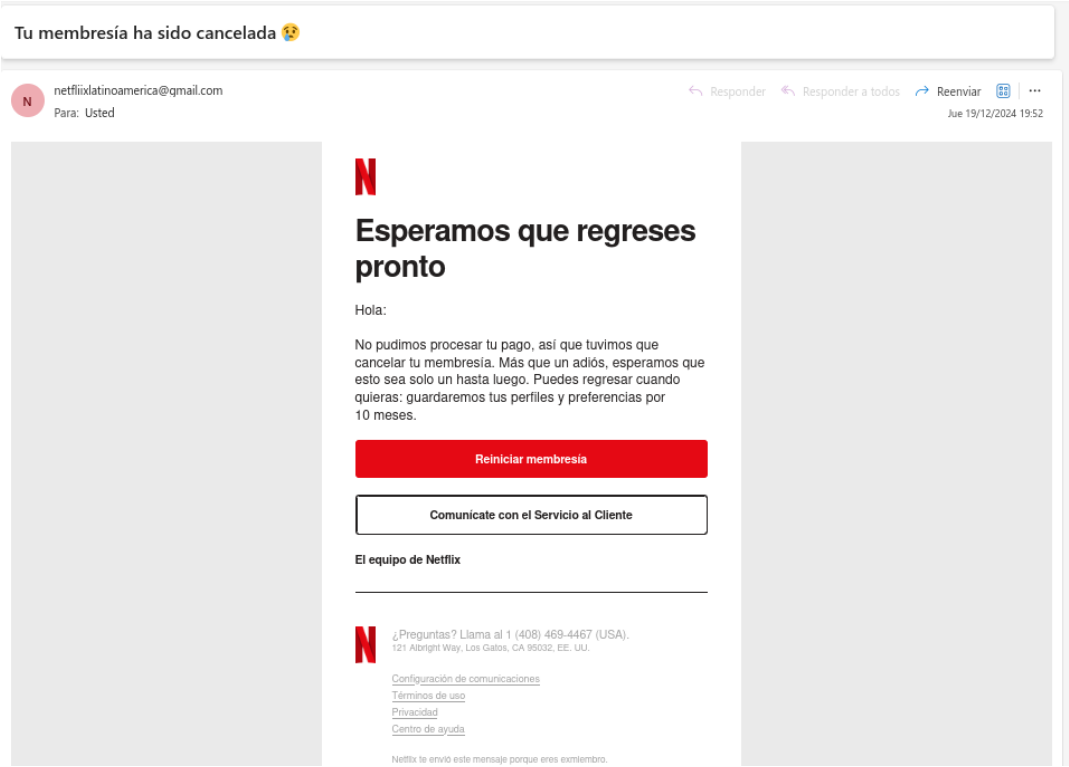

Figura 20. Muestra el correo electrónico de prueba enviado

Una vez hecho esto, nos aseguramos de que el enlace incluido en el correo redirija correctamente a la dirección web creada previamente en Zphisher para la página falsa de Netflix. Para garantizar que el enlace malicioso esté activo y cumpla su propósito en la simulación de phishing, este paso es esencial. Además, se comprobará que la página falsa mantenga su diseño y funcionalidad esperada, proporcionando una experiencia realista a los usuarios que interactúen con ella.

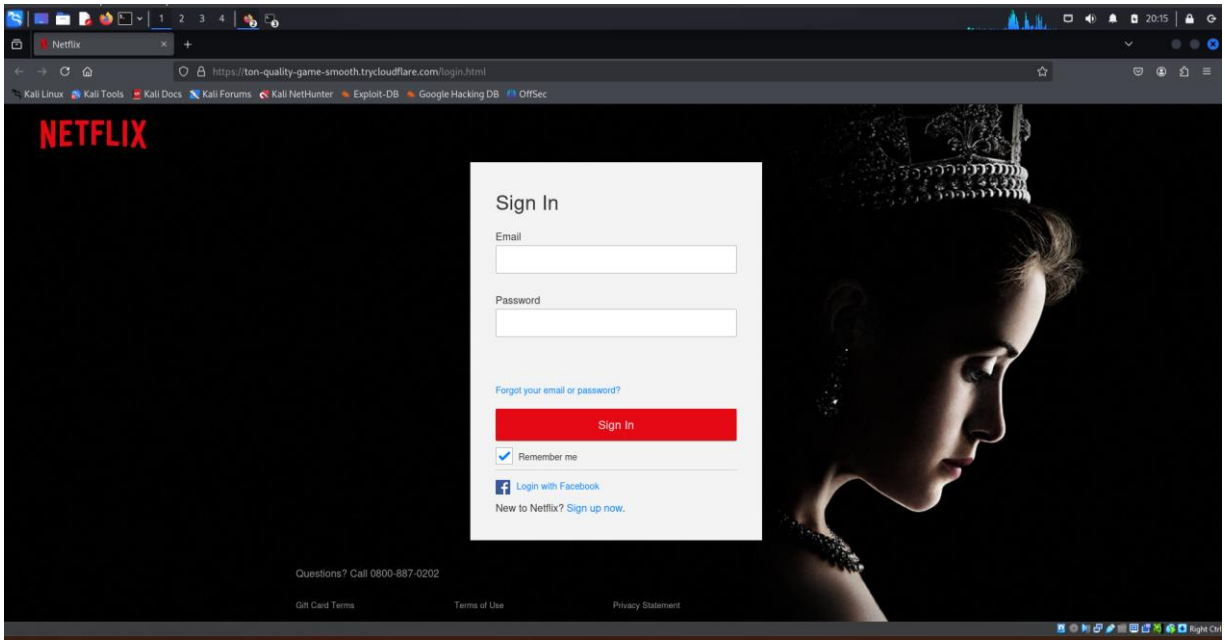

Figura 21. Muestra la página web falsa creada en zphisher

La Figura 21 muestra que el enlace fraudulento redirige correctamente a la página web falsa de Netflix creada en Zphisher. Esto confirma que la configuración del enlace y su funcionalidad son las deseadas, por lo que se puede avanzar con la campaña de phishing. Desde este punto, se enviará los correos electrónicos simulados al grupo de estudiantes seleccionados para participar en este trabajo.

3.8. Lanzamiento de la simulación

Una vez finalizado este proceso, crearemos una nueva campaña en el apartado "Campaigns" de Gophish. En este paso, integraremos todos los elementos configurados en los pasos anteriores, como la página de redirección (Landing Page), la plantilla de correo electrónico (Email Template) y el conjunto de destinatarios. Durante este proceso, se recopilan las configuraciones realizadas previamente, garantizando así que la campaña esté lista a ejecutarse.

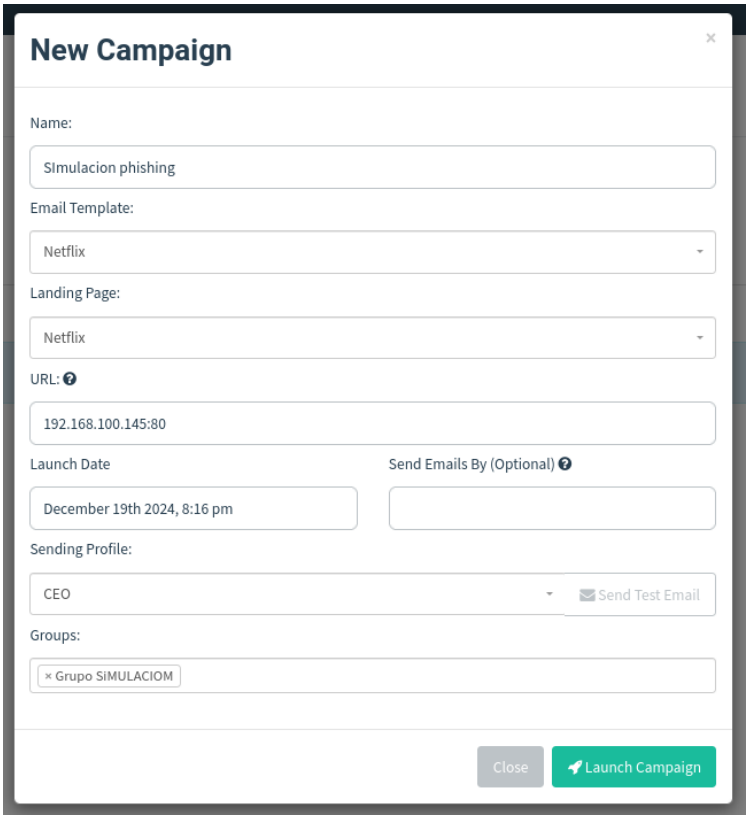

Figura 22. Muestra la pestaña de "New Campaign" configurada.

La configuración final para crear la campaña en Gophish se muestra en la Figura 22. En este apartado se comprueba todos los parámetros establecidos preliminarmente, como la página de redirección, la plantilla de correo y el grupo de destinatarios seleccionados, son correctos. Hecho lo anterior, se enviará la campaña de phishing una vez confirmado que todo está correctamente configurado. Una vez enviado, solo queda esperar los resultados para hacer un análisis del impacto y la efectividad de la simulación según los objetivos de este trabajo.

3.9. Etapa final

3.9.1. Análisis de los resultados obtenidos por Gophish

Cuando la ejecución de la campaña se haya finalizado, se podrán analizar los datos obtenidos a través de la interfaz de Gophish. La información recopilada incluye el número total de correos abiertos por los destinatarios, el número de veces que los usuarios hicieron

clic en el enlace malicioso, la cantidad de correos electrónicos enviados, y las veces en las que se ingresaron datos en la página web fraudulenta de Netflix. Dicha información es esencial para determinar la efectividad de la campaña de phishing y evaluar el alcance de la interacción de los usuarios con los elementos diseñados en este trabajo investigativo.

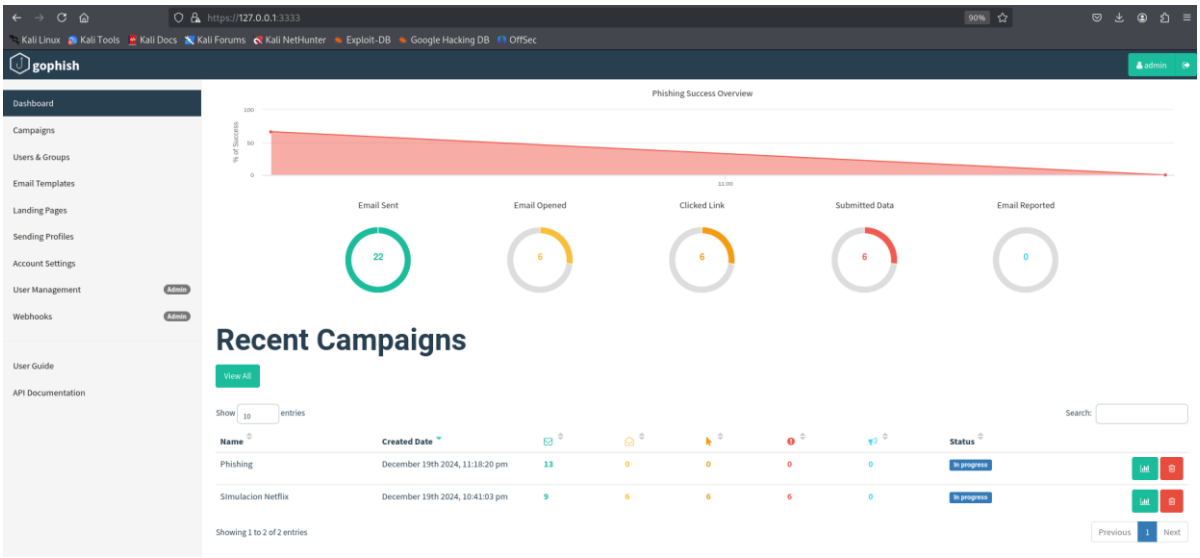

Figura 23. Muestra en Gophish las métricas de la campaña de phishing

Tal y como se observa en la Figura 23, de la muestra de los 22 correos electrónicos enviados, 6 personas interactuaron con el enlace malicioso, lo que representa un 27 % del total de destinatarios. Sin embargo, este resultado no supera la mitad del total, por lo que sigue siendo un dato significativo, ya que indica que una parte considerable de los usuarios fue susceptible a la simulación de phishing. Dicho resultado muestra el impacto que puede tener este tipo de ciber ataque, y pone en manifiesto la necesidad de implementar medidas preventivas y educativas para disminuir el riesgo de que los individuos sean víctimas de phishing en situaciones reales.

Figura 24. Muestra en Gophish los detalles de la campana de phishing

Los datos recopilados durante la campaña se presentan de manera más detallada en la Figura 24. Entre los datos destacados se incluye la identificación de los usuarios que ingresaron datos en la página web falsa y las personas que interactuaron con el enlace fraudulento. Esta información detallada permite realizar un estudio más profundo del comportamiento de los usuarios, lo que resulta fundamental para analizar la efectividad de la simulación e identificar los potenciales riesgos relacionados con la falta de prevención ante los ataques de phishing. Dichos resultados serán primordiales para las conclusiones del presente trabajo.

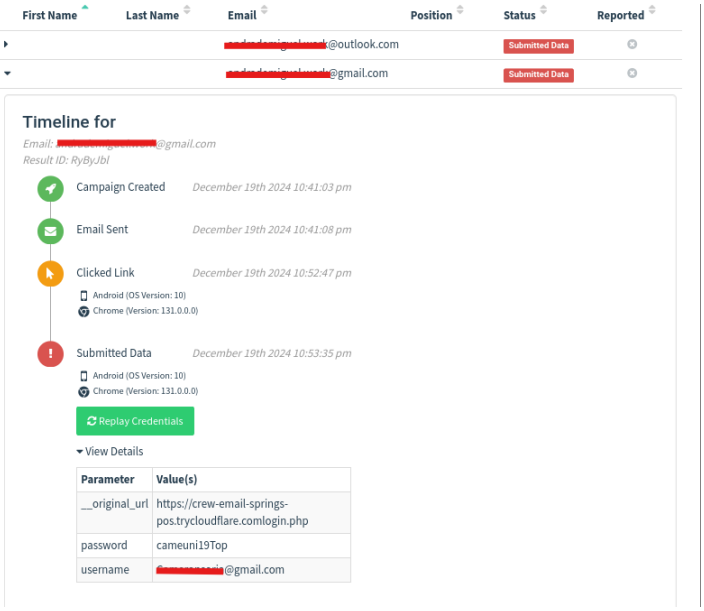

Figura 25. Muestra los detalles de los datos capturados de un estudiante.

Como se puede observar en la Figura 25, la página web falsa capturó información detallada de un estudiante que interactuó con ella. Además, se observa que el estudiante ingresó información sensible, como su nombre de usuario y contraseña, confirmando la efectividad del ciberataque simulado. Este resultado subraya la vulnerabilidad de los usuarios ante este tipo de amenazas.

3.9.2. Análisis obtenido por la encuesta

Figura 26. Resultado de los datos de la pregunta "¿En qué semestre se encuentra el estudiante?"

La Figura 26 muestra la distribución de los estudiantes según el semestre en el que se encuentran actualmente. De acuerdo con los datos obtenidos, el 31.8% de los estudiantes pertenece al octavo semestre, siendo este el grupo más representativo. Le siguen los estudiantes de quinto semestre, con un 22.7%, y los de sexto semestre, con un 18.2%.

Por otro lado, los estudiantes de tercer semestre representan el 13.6%, mientras que los de primer semestre constituyen el grupo más pequeño, con un 4.5%. No se registraron datos para los semestres segundo, cuarto, séptimo u otros niveles.

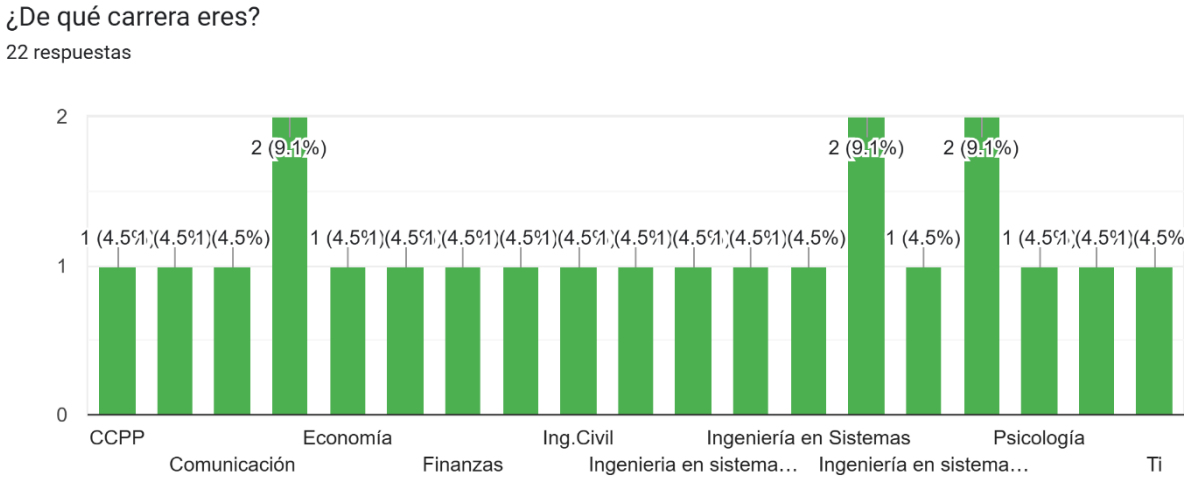

Figura 27. Resultado de los datos de la pregunta "¿De qué carrera eres?"

La figura 27 muestra la distribución de los estudiantes según sus carreras. Los datos indican que las carreras con mayor representación son Economía, Ingeniería en Sistemas y Psicología, cada una con un 9.1% (2 estudiantes).

El resto de las carreras, como Ciencias Políticas (CCPP), Comunicación, Finanzas, Ingeniería Civil, Ingeniería en Sistemas (otros grupos) y Tecnologías de la Información (TI), tienen una representación del 4.5%

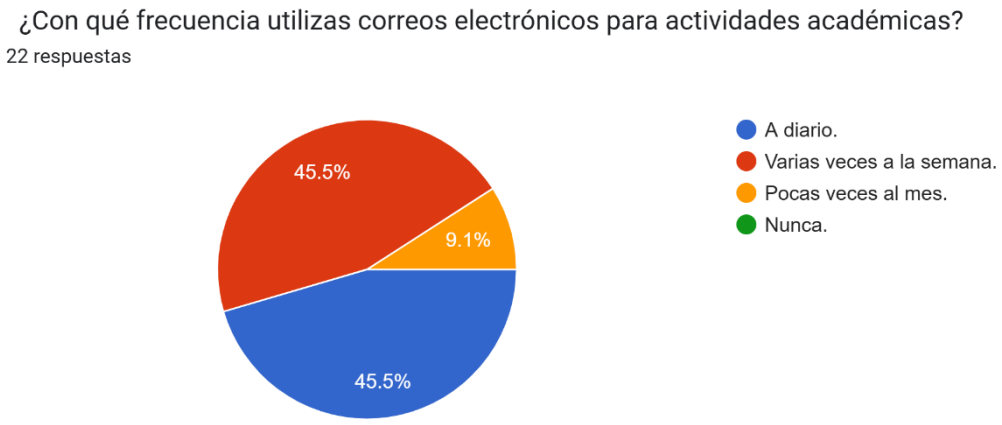

Figura 28. Resultado de los datos de la pregunta "¿Con que frecuencia utilizas correos electrónicos para actividades académicas?"

La figura 28 muestra los resultados sobre la frecuencia de uso de correos electrónicos por parte de los estudiantes para actividades académicas. Se observa que el 45.5% de los encuestados utiliza correos electrónicos a diario, mientras que otro 45.5% lo hace varias veces a la semana, lo que refleja un uso constante y regular de esta herramienta en el ámbito educativo.

Por otro lado, el 9.1% de los participantes señaló que utiliza correos electrónicos pocas veces al mes, y ningún estudiante indicó que nunca los utiliza. Estos resultados destacan la importancia del correo electrónico como medio de comunicación clave en actividades académicas, ya que la mayoría de los encuestados lo emplea de manera frecuente.

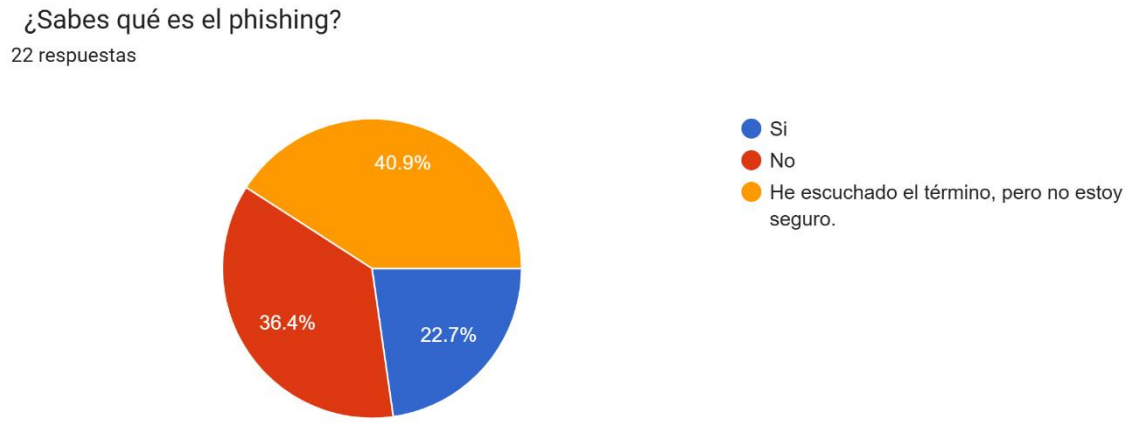

Figura 29. Resultado de los datos de la pregunta "¿Sabes que es el phishing?"

La figura 29 muestra los resultados sobre el conocimiento de los estudiantes acerca del término "phishing". Los datos reflejan que el 40.9% de los encuestados ha escuchado el término, pero no está seguro de su significado, lo que indica una falta de claridad sobre el concepto. Por otro lado, el 36.4% indicó que no sabe qué es el phishing, mientras que solo el 22.7% afirmó saber lo que significa.

Estos resultados sugieren que la mayoría de los estudiantes no tiene un conocimiento claro o suficiente sobre el phishing, lo que resalta la necesidad de realizar actividades educativas y de sensibilización para mejorar su comprensión sobre esta amenaza cibernética.

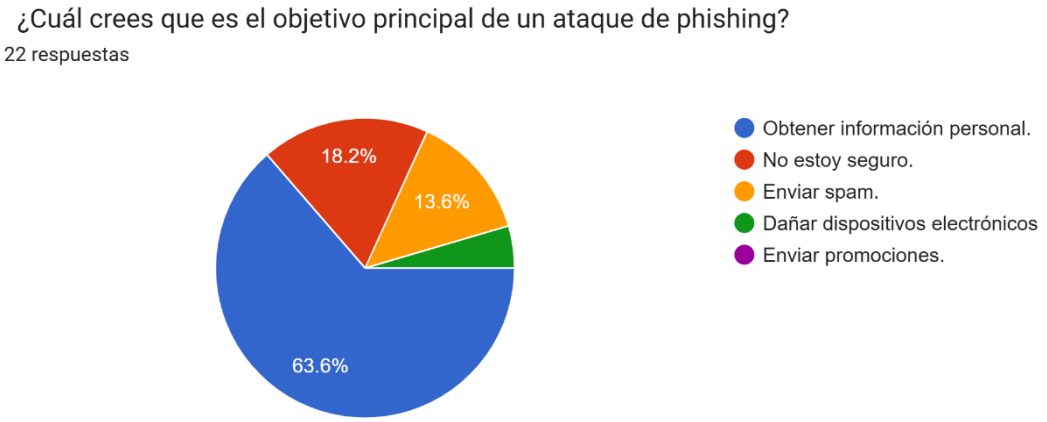

Figura 30. Resultado de los datos de la pregunta "¿Cuál crees que es el objetivo principal de un ataque de phishing?"

La Figura 30 refleja las respuestas de los estudiantes sobre lo que consideran el objetivo principal de un ataque de phishing. El 63.6% identificó correctamente que el propósito principal es obtener información personal, demostrando un nivel de conocimiento adecuado en este aspecto.

Por otro lado, el 18.2% indicó que no está seguro del objetivo, lo que muestra cierta falta de claridad sobre el tema. Un 13.6% cree que el phishing tiene como finalidad enviar spam, mientras que un pequeño porcentaje considera que su objetivo es dañar dispositivos electrónicos o enviar promociones.

Estos datos indican que, aunque la mayoría de los estudiantes reconoce el propósito central del phishing, aún existe un porcentaje significativo que necesita mayor sensibilización y formación para comprender completamente las amenazas y riesgos asociados a este tipo de ataque.

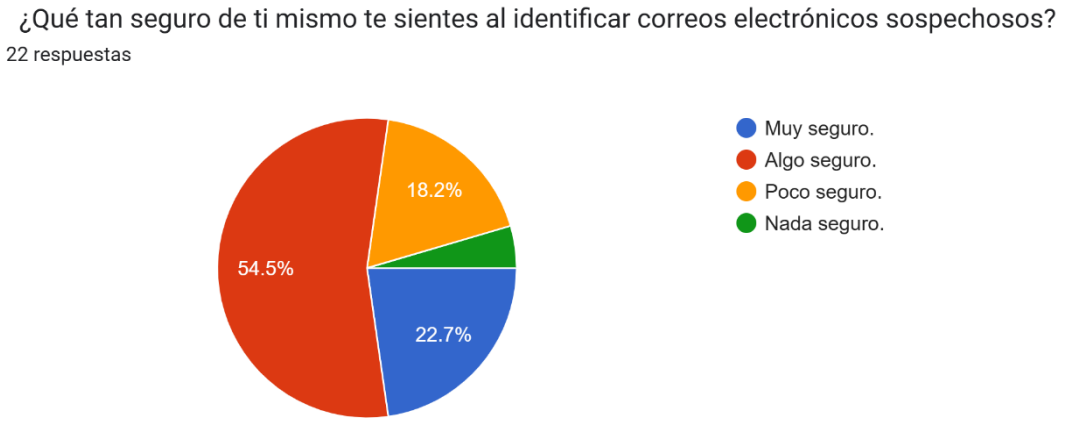

Figura 31. Resultado de los datos de la pregunta "¿Qué tan seguro te sientes al identificar correos electrónicos sospechosos?"

La Figura 31 muestra las respuestas de los estudiantes sobre su nivel de confianza al identificar correos electrónicos sospechosos. El 54.5% de los encuestados indicó sentirse poco seguro, mientras que el 22.7% señaló estar muy seguro en esta tarea. Por otro lado, un 18.2% expresó sentirse algo seguro, y un pequeño 4.5% mencionó que no se siente nada seguro.

Estos resultados evidencian que más de la mitad de los estudiantes tienen dificultades para identificar correos electrónicos sospechosos, lo que resalta la necesidad de implementar capacitaciones o simulaciones que refuercen sus habilidades para detectar amenazas cibernéticas.

Figura 32. Resultado de los datos de la pregunta "¿Alguna vez has recibido un correo o mensaje que creíste que podría ser un intento de phishing o correo falso?"

La Figura 32 refleja las respuestas de los estudiantes sobre si han recibido correos o mensajes que podrían ser intentos de phishing o correos falsos. El 81.8% de los encuestados afirmó haber recibido este tipo de mensajes, mientras que el 18.2% indicó que no. Ninguno de los participantes expresó no estar seguro al respecto.

Estos resultados indican que la gran mayoría de los estudiantes han estado expuestos a posibles intentos de phishing, lo que subraya la importancia de educarlos sobre cómo identificar y responder ante estas amenazas cibernéticas. La experiencia previa con este tipo de mensajes puede ser un punto de partida útil para fortalecer sus habilidades de detección.

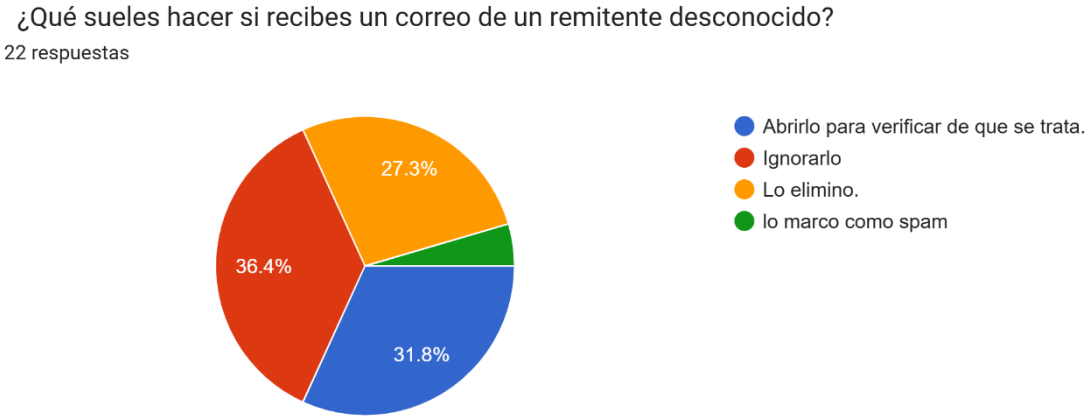

Figura 33. Resultado de los datos de la pregunta "¿Qué sueles hacer si recibes un correo de un remitente desconocido?"

La Figura 33 muestra las respuestas de los estudiantes sobre lo que suelen hacer al recibir un correo de un remitente desconocido. El 36.4% de los encuestados indicó que prefiere ignorar este tipo de correos, mientras que el 31.8% mencionó que lo abre para verificar de qué se trata.

Por otro lado, el 27.3% opta por eliminar el correo, y un pequeño 4.5% señaló que lo marca como spam.

Estos datos reflejan que una parte significativa de los estudiantes toma decisiones que podrían exponerlos a riesgos, como abrir correos desconocidos. Esto pone de manifiesto la importancia de sensibilizar a los estudiantes sobre prácticas seguras al gestionar correos electrónicos para reducir la vulnerabilidad frente a intentos de phishing.

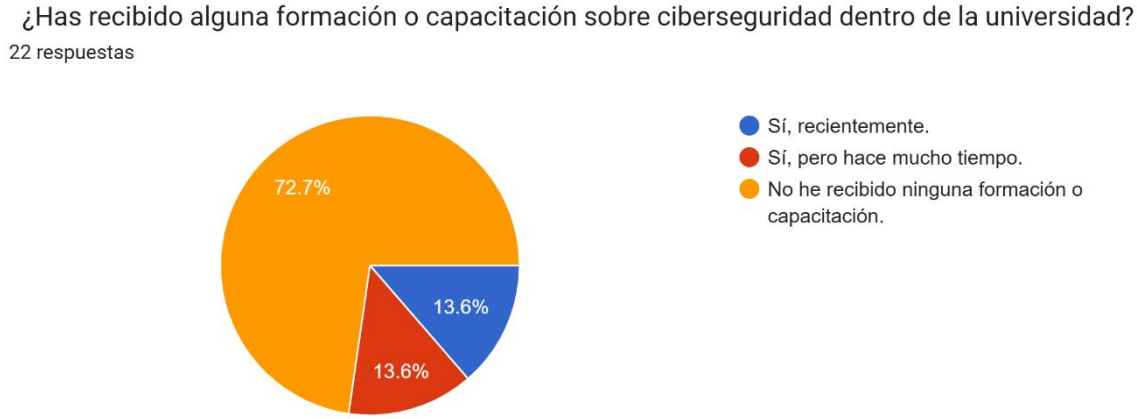

Figura 34. Resultado de los datos de la pregunta "¿Has recibido alguna formación o capacitación sobre ciberseguridad dentro de la universidad?"

La figura 34 presenta los resultados sobre si los estudiantes han recibido formación o capacitación en ciberseguridad dentro de la universidad. Un 72.7% de los encuestados indicó que no ha recibido ninguna formación o capacitación, lo que representa la gran mayoría. Por otro lado, un 13.6% señaló que sí recibió capacitación, pero hace mucho tiempo, mientras que otro 13.6% mencionó haber recibido formación recientemente.

Estos resultados reflejan una clara falta de formación actualizada en ciberseguridad para los estudiantes. Esto subraya la importancia de implementar programas educativos

dentro de la universidad para aumentar la sensibilización y mejorar la preparación de los estudiantes frente a amenazas cibernéticas, como el phishing.

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

En el presente capitulo abordaremos las conclusiones y recomendaciones a las que se llegaron en el proceso de realización de este trabajo de titulación.

4.1. Conclusiones

- Los resultados evidencian que una gran parte de los estudiantes encuestados no cuenta con un conocimiento claro sobre lo que es el phishing, ya que solo el 22.7% afirmó saber con certeza qué significa este término.
- Más del 70% de los estudiantes indicó que no ha recibido ninguna capacitación en ciberseguridad dentro de la universidad. Esto pone en evidencia la carencia de programas educativos específicos que aborden este tipo de amenazas
- Gophish puede ser una buena opción para campañas de phishing que incluyan grupos pequeños de personas, pero no es una herramienta muy eficaz a la hora de realizar phishing de manera masiva.
- Gophish y Zphisher resultaron ser herramientas muy útiles para llevar a cabo simulaciones de ataques de phishing que se sienten reales. Estas herramientas permiten personalizar tanto los correos electrónicos como las páginas web, lo que ayuda a crear escenarios similares a los ataques reales y hace más fácil analizar qué tan vulnerables son los usuarios.
- Ambas herramientas cuentan con interfaces relativamente sencillas que las hacen accesibles para usuarios con conocimientos básicos en ciberseguridad. Sin embargo, Gophish requiere una configuración inicial más detallada, especialmente para la integración de correos electrónicos.
- A pesar de su utilidad, estas herramientas enfrentan desafíos, como la posibilidad de que los correos enviados sean detectados como spam o bloqueados por proveedores de correo. Además, su uso debe estar estrictamente limitado a entornos controlados y con fines éticos, para evitar malentendidos o usos indebidos.

4.2. Recomendaciones

- Desarrollar e implementar talleres y cursos sobre ciberseguridad, con énfasis en la identificación y prevención de ataques de phishing. Esto ayudará a fortalecer las habilidades de los estudiantes para detectar correos sospechosos y reducir su vulnerabilidad.
- Se recomienda realizar simulaciones de ataques de phishing de forma regular para evaluar el nivel de susceptibilidad de los estudiantes.
- Si se requiere más nivel de sofisticación en las campañas de phishing se recomienda comprar un dominio, así mismo como la creación de la página web desde cero.
- Se recomienda dedicar tiempo a configurar adecuadamente Gophish, incluyendo el uso de dominios personalizados y certificados SSL válidos, para evitar que los correos sean detectados como spam y garantizar una experiencia más realista.
- Dado que Zphisher facilita la creación de páginas web falsas, es crucial limitar su uso a entornos educativos o de investigación, garantizando que no se utilice con fines maliciosos.
- Dado que ambas herramientas dependen de tecnologías que evolucionan constantemente, se recomienda mantenerse al día con las actualizaciones y buscar soporte en comunidades especializadas para resolver problemas técnicos.
- Fomentar la importancia de la ciberseguridad en la institución educativa, no solo con simulaciones, sino también mediante charlas, talleres y recursos educativos accesibles a toda la comunidad.
- Explorar simulaciones adicionales, como el envío de mensajes SMS falsos (smishing) o llamadas telefónicas simuladas (vishing), para educar sobre otras formas comunes de phishing.
- Implementar encuestas post-simulación para recopilar las percepciones de los participantes y medir el impacto educativo de las simulaciones.

Bibliografía

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. Recuperado de https://www.verizon.com/business/resources/Tde5/reports/2024-dbir-data-breach-investigations-report.pdf

Cloudflare. (n.d.). What is cyber security?. Recuperado de https://www.cloudflare.com/es-es/learning/security/what-is-cyber-security/

Microsoft. (n.d.). *What is cybersecurity?*. Microsoft. Recuperado de https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity?msockid=0ee0018e68a463c806d4149969646216

IBM. (2024, 17 de mayo). *¿Qué es el phishing?* Recuperado de https://www.ibm.com/es-es/topics/phishing

IBM. (n.d.). *Simulación de phishing*. Recuperado de https://www.ibm.com/mx-es/think/topics/phishing-simulation#:~:text=Una%20simulaci%C3%B3n%20de%20phishing%20es%20un%20ejercicio%20de,reconocer%20y%20responder%20a%20un%20ataque%20de%20phishing.

Gophish. (n.d.). *Open-Source Phishing Framework*. Recuperado de https://getgophish.com/#features

Gaikwad, H. (2023, 14 de septiembre). *Zphisher - Automated Phishing Tool in Kali Linux*. Scaler Topics. Recuperado de https://www.scaler.com/topics/zphisher/

Trend Micro. (n.d.). Types of phishing attacks. Retrieved from https://www.trendmicro.com

Fortinet. (2021). Cyber glossary: Types of phishing attacks. Retrieved from https://www.fortinet.com

EasyDMARC. (n.d.). 12 types of phishing attacks and how to identify them. Retrieved from https://easydmarc.com

Malwarebytes. (n.d.). Phishing. Retrieved from https://www.malwarebytes.com

Gaikwad, H. (2023, 14 de septiembre). *Zphisher - Automated Phishing Tool in Kali Linux*. Scaler Topics. Recuperado de https://www.scaler.com/topics/zphisher/

Gophish. (n.d.). Open-Source Phishing Framework. Recuperado de https://getgophish.com/#features

Kumar, S., Gupta, A., & Singh, R. (2023). *The impact of phishing simulation training on user awareness*. *Journal of Cybersecurity Education*, 25(3), 45-60.

Declaración de Helsinki. (1964). *Principios éticos para las investigaciones médicas en seres humanos*. Recuperado de https://www.wma.net/policies-

post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

Ley Orgánica de Protección de Datos Personales. (2021). *Registro Oficial Suplemento 459*. Ecuador.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 581-590. Recuperado de https://dl.acm.org/doi/10.1145/1124772.1124861

Reporte de ciberseguridad en Ecuador. (2023). *Amenazas cibernéticas en América Latina*. *CyberSecure Ecuador*, 45(2), 30-40.

Kaspersky LATAM. (2023). *Aumentan en 140% las estafas mediante mensajes falsos en América Latina*. Recuperado de https://latam.kaspersky.com/about/press-releases

Universidad Regional Autónoma de los Andes. (2013). *El phishing como delito informático: análisis y medidas en Ecuador*. Recuperado de https://dspace.uniandes.edu.ec

Universidad Politécnica Salesiana. (2023). *Riesgos informáticos asociados al phishing en canales electrónicos*. Recuperado de https://dspace.ups.edu.ec

Universidad Nacional de Loja. (2023). *Phishing y cibercrimen: análisis jurídico en Ecuador*. Recuperado de https://dspace.unl.edu.ec

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6ta ed.). McGraw-Hill.

Babbie, E. (2020). The Practice of Social Research (15th ed.). Cengage Learning.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

Flick, U. (2015). Introducing Research Methodology: A Beginner's Guide to Doing a Research Project (2nd ed.). SAGE Publications.