PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE: INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Trabajo de Titulación

GENERACIÓN DE UNA SIMULACIÓN DE ATAQUE DE INGENIERÍA SOCIAL A TRAVÉS DE DISPOSITIVOS MÓVILES CON LA APLICACIÓN WHATSAPP.

AUTOR:

KAROL NICOLE NOVOA GALLARDO

QUITO DM, JUNIO DE 2024

INDICE

Índice de Figuras

Índice de Tablas

AGRADECIMIENTOS

En primer lugar, quiero expresar mi más profundo agradecimiento a Dios por regalarme la vida y salud necesarias para culminar mis estudios. A mis queridos padres, hermana, cuñado y sobrinos, gracias por estar siempre a mi lado, apoyándome en cada paso del camino hacia el éxito.

Quiero hacer una mención especial a mi padre, Marcelo Novoa, por su apoyo incondicional. Papá, tu respaldo en todos los aspectos y tus contantes palabras de ánimo han sido fundamentales para que no decayera a lo largo de mi carrera. Tu actitud positiva y la profunda confianza que siempre has tenido en mí son lo que hoy se refleja en este logro.

Este trabajo que presento hoy es un reflejo de su amor, sacrificio y constante aliento, y me llena de orgullo poder finalizar esta etapa y convertirme en una profesional.

CAPÍTULO I: INTRODUCCIÓN

1. MARCO REFERENCIAL

1.1. TEMA

Generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp.

1.2. JUSTIFICACIÓN

La ingeniería social, como técnica de manipulación psicológica y persuasión utilizada para engañar a las víctimas y obtener datos confidenciales o acceso a sistemas de información, representa una amenaza significativa en el entorno actual de las redes sociales y los dispositivos móviles. Los delincuentes recurren a esta práctica para obtener información personal, financiera o empresarial, lo que puede acarrear consecuencias graves tanto para los usuarios individuales como para las organizaciones. La falta de conciencia y preparación en materia de seguridad en línea, así como la ausencia de políticas de seguridad efectivas, contribuyen a agravar la vulnerabilidad ante estos ataques. En este sentido, la realización de una simulación de ataque de ingeniería social en redes sociales se vuelve fundamental para identificar y abordar las debilidades en la seguridad, mejorar las políticas de seguridad y concienciar a los usuarios sobre los riesgos asociados.

La relevancia de afrontar esta problemática inicia en la creciente prevalencia de los ataques de ingeniería social en el contexto de las redes sociales y el uso generalizado de dispositivos móviles. A medida que estas plataformas se vuelven más populares y se utilizan con mayor frecuencia para compartir información personal y empresarial, la amenaza de ataques se ha vuelto más pronunciada. Los usuarios de las redes sociales, en muchos casos, no están plenamente conscientes de las tácticas de manipulación que los delincuentes pueden utilizar para engañarlos y obtener acceso a información confidencial. Esta falta de conciencia y preparación en materia de seguridad en línea aumenta la vulnerabilidad de los usuarios y de las organizaciones frente a los ataques de ingeniería social.

Además, la problemática se agrava por el hecho de que muchas organizaciones no cuentan con políticas de seguridad adecuadas para prevenir o detectar ataques en las redes sociales. La ausencia de políticas de seguridad efectivas deja a las organizaciones expuestas a posibles vulnerabilidades y riesgos de seguridad. Asimismo, la falta de capacitación de los usuarios en

cuanto a la seguridad en línea y la ingeniería social contribuye aún más a aumentar la vulnerabilidad de la red.

Ante esta problemática, la generación de una simulación de ataque de ingeniería social en redes sociales se presenta como una estrategia clave para abordar las debilidades en la seguridad, mejorar las políticas de seguridad y concienciar a los usuarios sobre los riesgos asociados. La realización de esta simulación no solo permitirá identificar las vulnerabilidades en la seguridad, sino que también contribuirá a promover una cultura de seguridad en la comunidad de usuarios de las redes sociales. Además, la simulación de un ataque de ingeniería social puede ayudar a las organizaciones a cumplir con las normativas y requisitos legales, así como a proteger la reputación y la privacidad de los usuarios. Asimismo, esta estrategia puede ser una herramienta efectiva para valorar la efectividad de las estrategias de seguridad existentes y determinar si se necesitan cambios para mejorar la seguridad de la red.

Los beneficios esperados de llevar a cabo esta simulación son diversos y abarcan tanto a los usuarios individuales como a las organizaciones. En primer lugar, la identificación de las vulnerabilidades en la seguridad permitirá implementar medidas correctivas que fortalezcan la protección de la información y reduzcan la exposición a posibles ataques de ingeniería social. Asimismo, la concienciación de los usuarios sobre los riesgos asociados a la ingeniería social contribuirá a promover una cultura de seguridad en línea, fomentando prácticas seguras y responsables entre la comunidad de usuarios. Por otro lado, las organizaciones se verán beneficiadas al poder cumplir con las normativas y requisitos legales en materia de seguridad de la información, proteger la reputación y la privacidad de los usuarios, y evaluar la efectividad de las estrategias de seguridad existentes.

Además de los beneficios directos, la realización de esta simulación también puede tener implicaciones más amplias en el ámbito de la seguridad en línea y la protección de la información. Los resultados obtenidos a partir de la simulación podrían contribuir al desarrollo de buenas prácticas en materia de seguridad en línea, así como a la generación de conocimiento y conciencia sobre los riesgos asociados a la ingeniería social. Estos aportes podrían ser de utilidad para otras organizaciones y comunidades de usuarios que enfrentan desafíos similares en relación con la seguridad en línea y la protección de la información.

1.3. PLANTEAMIENTO DEL PROBLEMA

La creciente amenaza de los ataques de ingeniería social en el entorno de WhatsApp y los dispositivos móviles a nivel global es un problema que está afectando a una amplia variedad de usuarios y organizaciones en todo el mundo. Estos ataques tienen implicaciones significativas en la seguridad y protección de la información a gran escala en el contexto de WhatsApp, una de las redes sociales más utilizadas a nivel mundial. La falta de conciencia y preparación en materia de seguridad en línea, así como la ausencia de políticas de seguridad efectivas en el entorno específico de WhatsApp, contribuyen a agravar la vulnerabilidad de los usuarios y organizaciones frente a estas amenazas a nivel global. Es fundamental tomar medidas proactivas para abordar esta creciente preocupación y proteger la integridad de la información en el entorno digital de WhatsApp.

El problema se hace evidente en el entorno de WhatsApp debido a la carencia de políticas de seguridad adecuadas y la falta de capacitación de los usuarios en cuanto a la seguridad en línea y la ingeniería social en este contexto específico. Esto abarca la exposición a riesgos de seguridad en la red social WhatsApp y dispositivos móviles por parte de grupos de usuarios o comunidades con características y necesidades particulares. Por tanto, es fundamental implementar medidas específicas para abordar estas vulnerabilidades a nivel organizacional y comunitario en el contexto de WhatsApp, con el propósito de fortalecer la seguridad en línea y proteger la integridad de los datos en este entorno específico.

1.4. OBJETIVOS

1.4.1. GENERAL

Generar la simulación de un ataque de ingeniería social para concientizar a los usuarios sobre las vulnerabilidades existentes en el uso de las redes sociales en dispositivos móviles con la aplicación WhatsApp.

1.4.2. ESPÉCIFICOS

- Analizar los datos de las encuestas realizadas para identificar patrones de comportamiento y preferencias de los usuarios en redes sociales, para identificar vulnerabilidades en el uso de la aplicación WhatsApp.

- Ejecutar el plan de simulación para el ataque de ingeniería social que permita concientizar a los usuarios sobre las tácticas utilizadas por los atacantes, así como promover el buen uso y la seguridad en el entorno de WhatsApp.
- Evaluar la efectividad de las políticas de seguridad existentes en WhatsApp y dispositivos móviles a través de la simulación de ataques, con el objetivo de identificar áreas de mejora y proponer recomendaciones para fortalecer la protección de los usuarios.

1.5. ALCANCE

El alcance del proyecto se centrará en la red social WhatsApp, con el fin de delimitar el ámbito de la simulación y enfocar los esfuerzos en plataformas relevantes para el estudio.

Se puede considerar la segmentación de usuarios según características demográficas, intereses o comportamientos en línea, con el propósito de analizar la susceptibilidad a ataques de ingeniería social en grupos específicos.

El alcance del proyecto incluirá la definición de los métodos y técnicas a utilizar en la simulación, como el diseño de escenarios de ataque, la creación de perfiles falsos, la elaboración de mensajes persuasivos, entre otros.

Otro alcance también puede contemplar la evaluación de los resultados obtenidos a partir de la simulación, incluyendo el análisis de la efectividad de las políticas de seguridad existentes, la identificación de vulnerabilidades y la propuesta de recomendaciones para fortalecer la protección de los usuarios.

Es importante delimitar el alcance en términos de consideraciones éticas y legales, asegurando el desempeño de las normativas de privacidad y protección de información, así como el respeto a los derechos de los participantes en la simulación.

CAPÍTULO II: MARCO TEÓRICO

2. FUNDAMENTACIÓN TEÓRICA

Esta propuesta de innovación se basa en un marco que relaciona la tecnología, la seguridad de la información y el comportamiento humano. Esto facilita una mejor comprensión de la importancia y el impacto que conlleva la pérdida de confidencialidad, integridad y disponibilidad de la información. Este fundamento aporta mayor claridad sobre la situación y los riesgos que enfrentan los usuarios en este mundo tecnológico. Es un trabajo de investigación cumple la función de proporcionar el marco conceptual y la base de conocimientos relacionados con el tema de estudio. En el contexto de la investigación sobre la generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp, esta fundamentación teórica sería esencial para comprender y contextualizar conceptos clave como la ingeniería social, la seguridad informática, el uso de dispositivos móviles y las vulnerabilidades asociadas con la aplicación WhatsApp (Orihuela Quivaqui, 2022).

La fundamentación teórica sería útil para respaldar y justificar el estudio, así como para establecer conexiones con el trabajo previo realizado en el campo de la seguridad informática y la ingeniería social. Además de proporcionar el conocimiento necesario para diseñar y desarrollar una simulación efectiva de un ataque o irrupción de ingeniería social a través de dispositivos móviles utilizando la aplicación WhatsApp, al tiempo que permitiría evaluar y analizar los resultados de manera fundamentada (Orihuela Quivaqui, 2022).

2.1. Antecedentes de la Investigación

Según (Conde Mendoza, 2021) Titulado "Concientización en Ciberseguridad a través de ataques de ingeniería social" Este trabajo de investigación propone utilizar la filosofía de concientización como base para desarrollar un modelo de concientización en ciberseguridad, con el objetivo de optimizar el tratamiento de los riesgos procedentes de ataques de ingeniería social. Algunas ideas clave sobre cómo este trabajo podría ser útil para futuras investigaciones son, la propuesta de un enfoque alternativo: El artículo identifica que los enfoques actuales para gestionar los riesgos de ingeniería social se centran en grupos específicos, por lo que propone el modelo de concientización como una alternativa con un enfoque más general. Fundamentos teóricos robustos al basar su propuesta en la filosofía educativa de Paulo Freire, el trabajo aporta un marco teórico sólido y bien fundamentado para abordar el problema de los riesgos de ingeniería social.

La aplicación a la ciberseguridad, Si bien el modelo de concientización se originó en el campo de la educación, este trabajo demuestra cómo sus principios pueden ser adaptados y aplicados al contexto de la ciberseguridad y la gestión de riesgos.

Esta investigación sienta las bases para que futuras investigaciones puedan profundizar en el desarrollo, implementación y evaluación de modelos de concientización en ciberseguridad fundamentados en perspectivas educativas sólidas, con el fin de mejorar la gestión de riesgos procedentes de ataques de ingeniería social.

La investigación describe en detalle la filosofía de concientización y su aplicación como modelo para concientizar a las personas, con el fin de mejorar el manejo de los riesgos provenientes de ataques de ingeniería social. Esto podría ser relevante para el trabajo, ya que aborda directamente el tema de los ataques de ingeniería social y propone un marco teórico interesante, basado en la concientización de los usuarios, que podría influir en la efectividad de la simulación de ataque a través de WhatsApp y en las medidas de prevención que se deriven de ella.

Un segundo trabajo de investigación (Vallejo Rodriguez, 2020), la cual se denomina “Desarrollo de un simulador web aplicando las normas ISO/IEC 27002 enfocado en la ingeniería Social”, Esta investigación se enfocó en el desarrollo de un simulador web basado en las directrices de control de acceso establecidas en la norma ISO/IEC 27002. Estas pautas proporcionaron información sobre los estándares que deben seguirse en el desarrollo de aplicaciones web seguras contra ataques cibernéticos, las cuales deben implementarse de manera óptima para garantizar aplicaciones seguras y estandarizadas. El simulador web tiene como objetivo informar a la comunidad universitaria de la UTN sobre las principales amenazas, vulnerabilidades y riesgos presentes en Internet. Esto permite a los usuarios simular y conocer las técnicas más usadas de extorsión mediante la ingeniería social en escenarios controlados. La ingeniería social consiste en obtener acceso no autorizado a infraestructura e información a través del engaño y el fraude psicológico, específicamente dirigido a explotar las debilidades humanas con el fin de obtener accesos no autorizados, robar información y extorsionar.

Esta investigación sería de gran utilidad para esta investigación y futuras, ya que proporciona un ejemplo concreto de la aplicación de directrices de control de acceso del estándar ISO/IEC 27002 en el desarrollo de un simulador web. Esta información ayudaría a comprender cómo estas directrices pueden ser implementadas de manera práctica para garantizar la seguridad

de las aplicaciones web contra ataques cibernéticos, lo cual es relevante para la investigación sobre la generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp.

Además, el texto detalla la importancia de informar a la comunidad universitaria sobre las amenazas, vulnerabilidades y riesgos presentes en internet, así como el uso del simulador para simular y conocer las técnicas más comunes de extorsión mediante la ingeniería social en escenarios controlados. Esto te proporcionaría un precedente relevante para justificar la necesidad de la investigación y la utilidad de la simulación que se plantea desarrollar.

Asimismo, el texto aborda el marco teórico relacionado con la seguridad informática, la seguridad de la información, la ingeniería social y sus técnicas más utilizadas, lo cual te brindaría una base sólida para fundamentar el estudio y comprender el contexto en el que se desarrolla la investigación.

El propósito del proyecto realizado por (Camino Ruiz, 2020), tiene como objetivo examinar la seguridad de la red de la Unidad Educativa Salesiana Cardenal Spellman mediante el uso de técnicas y herramientas de Ingeniería Social. Estas técnicas pueden eludir las protecciones de hardware y software al dirigirse directamente al usuario objeto del ataque.

El proyecto incluye la creación de dos escenarios de prueba en diferentes áreas de la institución, utilizando las metodologías del Proyecto Piloto y la Cadena de Ataques Informáticos. En el primer escenario, el personal administrativo fue atacado con el Social-Engineer Toolkit (SET) para clonar páginas de acceso, logrando un éxito del 40%. En el segundo escenario, se emplearon técnicas de Phishing y Pretexting para enviar mensajes falsos a maestros, obteniendo un éxito del 29.6% por correo electrónico y 8% a través de WhatsApp.

Finalmente, el proyecto presenta recomendaciones para prevenir ataques de ingeniería social, abordar las vulnerabilidades identificadas y concienciar a la comunidad educativa sobre los riesgos asociados a la falta de conocimiento en la gestión de la información y la ausencia de políticas de seguridad.

Este análisis sería relevante para la investigación “Generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp”, ya que proporciona detalles sobre las técnicas específicas de ingeniería social utilizadas, los escenarios de

ataque simulados y los resultados obtenidos. Además, las recomendaciones ofrecidas pueden ser útiles para comprender las amenazas a la seguridad de la información en entornos educativos y proponer medidas de protección adecuadas.

En el marco de la cuarta investigación realizada por (Fernández Peña & Jinde Sisa, 2024), titulada "Estrategia para mitigar fraudes de Angler-Phishing basados en ingeniería social en plataformas de redes sociales", se enfoca en definir una estrategia para prevenir y reducir la incidencia de fraudes de Angler-Phishing basados en Ingeniería Social.

Para la anterior investigación, se utilizó una metodología de enfoque mixto para recopilar y analizar datos de usuarios de redes sociales, identificando soluciones viables para atenuar los riesgos de fraude, especialmente entre aquellos susceptibles a la ingeniería social y al angler-phishing. Como resultado relevante, se encontró que al aplicar una estrategia integral basada en la metodología OSSTMM para una efectiva integración de instrumentos de Tecnologías de la Información (TI), se logra prevenir y reducir la incidencia de ataques, fomentando la colaboración entre diversas soluciones tecnológicas, como autenticación de dos pasos, sistemas de detección de intrusiones y filtros de correo electrónico. Esta concordancia entre instrumentos fortalece la capacidad defensiva, siguiendo una aproximación estratégica que abarca distintas capas de seguridad.

Esta investigación sería relevante para el trabajo, ya que se enfoca específicamente en la mitigación de fraudes de Angler-Phishing basados en ingeniería social en plataformas de redes sociales. La estrategia propuesta, basada en la integración de múltiples instrumentos de TI, podría proporcionar un marco interesante para abordar los riesgos de seguridad en el contexto de la simulación de ataque a través de WhatsApp.

Esta investigación sirve como referencia para la investigación sobre la generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp ya que se centra en la prevención y reducción de la incidencia de fraudes de ingeniería social, específicamente en el contexto de las redes sociales y dispositivos móviles. Puedes utilizar la información proporcionada para comprender cómo se abordó un problema similar y cómo se aplicaron estrategias para mitigar los riesgos de fraude.

El estudio destaca la importancia de implementar una estrategia integral basada en la metodología OSSTMM (Open Source Security Testing Methodology Manual) para lograr una

integración efectiva de herramientas y tecnologías de la información. Esta estrategia ha demostrado ser eficaz para prevenir y reducir la incidencia de ataques. La integración de diversas soluciones tecnológicas, como la autenticación de dos factores, los sistemas de detección de intrusiones y los filtros de correo electrónico, fomenta la colaboración entre estas herramientas. Esta aproximación integral, que abarca múltiples capas de seguridad, fortalece significativamente la capacidad defensiva.

La investigación subraya la relevancia de implementar una estrategia holística, basada en la metodología OSSTMM, para lograr una integración efectiva de las tecnologías de la información. Esto ha demostrado ser efectivo para prevenir y reducir la incidencia de ataques, al aprovechar la sinergia entre diferentes soluciones de seguridad. Este hallazgo podría ser de gran interés para la investigación, ya que podrías explorar la posibilidad de aplicar una estrategia similar en el contexto de la simulación de a través de plataformas de mensajería como WhatsApp. De esta manera, podrías implementar una metodología integral que combine diversos instrumentos tecnológicos para prevenir y mitigar de manera efectiva los riesgos asociados a este tipo de amenazas.

2.2. Redes Sociales

Las redes sociales son plataformas en línea que permiten a los usuarios conectarse, compartir contenido, interactuar y construir comunidades virtuales. Las plataformas de redes sociales han transformado profundamente la manera en que las personas se comunican, comparte información y mantienen relaciones interpersonales en el entorno digital. Desde su aparición, las redes sociales han tenido un impacto considerable en diversos ámbitos de la sociedad, incluyendo la comunicación, el marketing, la política y la cultura. Las redes sociales han generado un cambio fundamental en la forma en que los individuos se relacionan y se expresan a través de medios digitales. Estas plataformas han permeado múltiples esferas de la sociedad, modificando significativamente la dinámica de la comunicación, el marketing, la participación política y las manifestaciones culturales (Altamiro, 2018).

Entre las numerosas redes sociales que existen, WhatsApp se destaca como una de las más populares y ampliamente utilizadas en todo el mundo. Aunque inicialmente se concibió como una aplicación de mensajería instantánea, WhatsApp ha evolucionado para incluir funciones de redes sociales, como la posibilidad de crear grupos, compartir actualizaciones de estado y establecer

conexiones con una amplia red de contactos. Por lo tanto, WhatsApp puede considerarse no solo como una plataforma de mensajería, sino también como una red social que facilita la interacción y el intercambio de información entre sus usuarios. (Altamiro, 2018)

2.2.1. Importancia y relevancia de las redes sociales en la actualidad.

Las redes sociales tienen una relevancia significativa en la sociedad actual, ya que desempeñan un papel fundamental en la comunicación, la interacción social, la difusión de información y la construcción de agrupaciones en línea. Estas plataformas han transformado la forma en que los individuos se conectan, comparten ideas, promueven causas, realizan negocios y acceden a contenido diverso. Además, las redes sociales han democratizado la generación de contenido, permitiendo que cualquier individuo o entidad pueda compartir su perspectiva e influir en un amplio público (Lopez Bonilla, 2024).

2.2.2. Características y Tipos de Redes Sociales:

Las redes sociales presentan una serie de características distintivas que las diferencian de otros medios de comunicación en línea. Estas características incluyen la posibilidad de crear perfiles personales, conectarse con otros usuarios, compartir contenido multimedia, participar en conversaciones públicas o privadas, y seguir o ser seguido por otros usuarios. Además, las redes sociales suelen ofrecer funciones de personalización, como la capacidad de crear listas de amigos, grupos temáticos o páginas de interés (Tascon & Quintana, 2018).

En cuanto a los tipos de redes sociales, estas pueden clasificarse en varias categorías según su función y estructura. Algunos ejemplos comunes incluyen las redes sociales generalistas, como Facebook, que abarcan una amplia gama de intereses y usuarios; las redes sociales profesionales, como LinkedIn, enfocadas en la conexión y colaboración laboral; las redes sociales de microblogging, como Twitter, que se centran en publicaciones breves y rápidas; las redes sociales visuales, como Instagram, que se basan en el contenido visual compartido; y las redes sociales de nicho, que se dirigen a audiencias específicas con intereses particulares, como Goodreads para amantes de la lectura o Strava para deportistas. Estas distintas categorías reflejan la diversidad de funciones y usos que las redes sociales ofrecen, adaptándose a las necesidades y preferencias variadas de sus usuarios (Tascon & Quintana, 2018).

2.3. Clasificación de las redes sociales.

La clasificación de las redes sociales se puede realizar en función de diversos criterios, como su propósito, audiencia objetivo y características distintivas. Por ejemplo, las redes sociales pueden ser categorizadas según su función, lo que incluye redes generalistas, profesionales, de microblogging, visuales y de nicho, cada una con enfoques y usos específicos. Asimismo, la clasificación según la audiencia puede abarcar redes sociales dirigidas a grupos demográficos particulares, intereses específicos o ámbitos profesionales, reflejando la diversidad de usuarios y propósitos que estas plataformas buscan atender. Esta variedad de clasificaciones permite comprender la amplitud y la especialización que caracterizan al panorama de las redes sociales, adaptándose a las necesidades y preferencias de los usuarios en diferentes contextos (Tejada Garitano & Castaño Garrido, 2019).

2.4. Impacto de las Redes Sociales:

El impacto de las redes sociales abarca una amplia gama de áreas, incluyendo la comunicación, la interacción social, el marketing, la política, la cultura y la sociedad en su conjunto. Estas plataformas han modificado la forma en que los usuarios se conectan, comparten datos, expresan sus opiniones y participan en discusiones públicas. Además, han generado cambios significativos en la dinámica de la difusión de noticias, la formación de comunidades en línea, la promoción de productos y servicios, así como en la participación ciudadana y el activismo social. El impacto de las redes sociales se extiende a múltiples aspectos de la vida moderna, ejerciendo una influencia profunda en la forma en que las personas se relacionan, se informan y participan en la sociedad (Tejada Garitano & Castaño Garrido, 2019)

En lo Social:

El impacto de las redes sociales en el ámbito social ha sido profundo, redefiniendo la manera en que las personas se relacionan, se comunican y forman comunidades. Estas plataformas han facilitado la conexión entre individuos de distintas regiones, permitiendo el establecimiento de relaciones personales y profesionales a través de fronteras geográficas. Además, han brindado espacios para la expresión personal, la difusión de ideas y la movilización en torno a causas sociales, lo que ha contribuido a amplificar voces y generar conciencia sobre temas relevantes (Fontecilla, 2021).

No obstante, las redes sociales también han planteado desafíos en el ámbito social, como la gestión de la privacidad, la difusión de información falsa y la creación de burbujas informativas que pueden polarizar opiniones. Asimismo, han impactado la dinámica de las relaciones interpersonales, generando cambios en la forma en que las personas se informan y establecen vínculos (Fontecilla, 2021).

En lo Económico:

El impacto de las redes sociales en el ámbito económico ha sido significativo, transformando la manera en que las empresas se relacionan con los consumidores, promocionan sus productos y servicios, y realizan estrategias de marketing. Estas plataformas han brindado a las empresas la oportunidad de llegar a audiencias más amplias, interactuar directamente con los clientes, y obtener retroalimentación en tiempo real. Además, han facilitado la creación de redes de negocios, la promoción de marcas y la generación de oportunidades de ventas a través de plataformas de comercio electrónico (Fontecilla, 2021).

Sin embargo, el impacto de las redes sociales en el ámbito económico también ha planteado desafíos, como la gestión de la reputación en línea, la competencia en un entorno digital saturado, y la necesidad de adaptarse a las tendencias cambiantes del comportamiento del consumidor en línea. Asimismo, ha surgido la preocupación sobre la privacidad de los datos y la seguridad en las transacciones comerciales realizadas a través de plataformas de redes sociales.

En lo Político:

El impacto de las redes sociales en el ámbito político ha sido significativo, transformando la manera en que se lleva a cabo la información política, la reciprocidad ciudadana y la influencia en la toma de decisiones. Estas plataformas han proporcionado canales para la difusión de información política, la movilización de votantes y la creación de discusiones públicas en torno a temas políticos relevantes. Además, han permitido a los ciudadanos expresar sus opiniones, organizarse en torno a causas políticas y ejercer presión sobre las autoridades (Fontecilla, 2021).

Sin embargo, el impacto de las redes sociales en el ámbito político también ha generado desafíos, como la propagación de desinformación, la polarización de opiniones y la influencia de intereses particulares en el discurso político. Asimismo, han surgido interrogantes sobre la

transparencia y la equidad en el uso de estas plataformas para la promoción de candidatos y la difusión de mensajes políticos (Fontecilla, 2021).

2.5. Consideraciones de Seguridad y Privacidad

Las consideraciones de seguridad y privacidad en el contexto de las redes sociales son de gran importancia, ya que estas plataformas enfrentan desafíos relacionados con el amparo de la información personal y la prevención de actividades maliciosas. La gestión adecuada de la seguridad y la privacidad en las redes sociales implica la implementación de medidas para proteger los datos de los usuarios, prevenir el acceso no acreditado a la información personal, y garantizar la confidencialidad de las interacciones en línea. Además, se deben considerar las implicaciones éticas y legales de la recopilación, el almacenamiento y el uso de los datos de los consumidores en el contexto de las redes sociales (Restrepo, 2023).

El equilibrio entre la facilitación de la interacción en línea y el amparo de la privacidad de los usuarios representa un desafío continuo para las plataformas de redes sociales, que deben adoptar políticas y tecnologías que salvaguarden la seguridad y la privacidad de manera efectiva. Asimismo, los usuarios también tienen un papel importante en la protección de su propia seguridad y privacidad al utilizar las redes sociales, a través de prácticas como el manejo seguro de contraseñas, la configuración adecuada de la privacidad de sus perfiles, y la evaluación crítica de la veracidad de la información compartida en línea (Restrepo, 2023).

2.6. Aspectos de seguridad y privacidad en las redes sociales.

Los aspectos de seguridad y privacidad en las redes sociales abarcan la importancia de salvaguardar la información personal de los usuarios y prevenir posibles amenazas en línea. Esto implica considerar medidas para salvaguardar los datos, Además, es crucial abordar las implicaciones éticas y legales relacionadas con la recopilación, almacenamiento y uso de los datos de los beneficiarios en el contexto de las redes sociales (Restrepo, 2023).

El equilibrio entre fomentar la interacción en línea y proteger la privacidad de los usuarios representa un desafío constante para las plataformas de redes sociales, que deben implementar políticas y tecnologías que garanticen la seguridad y la privacidad de manera efectiva. Además, los usuarios desempeñan un papel fundamental en la protección de su seguridad y privacidad al utilizar las redes sociales, a través de prácticas como el manejo seguro de contraseñas, la

configuración adecuada de la privacidad de sus perfiles y la evaluación crítica de la veracidad de la información compartida en línea (Restrepo, 2023).

2.7. Posibles riesgos y medidas de protección relacionadas con el uso de las redes sociales.

Los posibles riesgos y medidas de protección asociados con la utilización de las redes sociales abarcan la identificación de amenazas potenciales para los usuarios y la implementación de acciones preventivas para mitigar dichos riesgos. Esto implica reconocer posibles peligros como el acoso en línea, el robo de identidad, la difusión de información falsa y la exposición a contenido inapropiado. Para contrarrestar estos riesgos, es crucial adoptar medidas de protección, como configurar adecuadamente la privacidad de los perfiles, utilizar contraseñas seguras, educar a los usuarios sobre la detección de fraudes y promover un comportamiento responsable en línea (Restrepo, 2023).

Además, las plataformas de redes sociales también tienen la responsabilidad de implementar medidas de seguridad efectivas, como la encriptación de datos, la detección y eliminación de cuentas falsas o maliciosas, y la promoción de un entorno en línea seguro y respetuoso. Asimismo, la colaboración entre usuarios, plataformas y autoridades reguladoras es fundamental para abordar de manera integral los posibles riesgos mancomunados con el uso de las redes sociales (Restrepo, 2023).

2.8. Dispositivos Móviles

Los dispositivos móviles son aparatos electrónicos portátiles que permiten a los usuarios realizar diversas tareas, como hacer llamadas, enviar mensajes, acceder a internet, tomar fotografías, escuchar música, entre otros. Estos dispositivos incluyen teléfonos inteligentes, tabletas, relojes inteligentes y otros dispositivos portátiles con capacidades de conectividad inalámbrica (Fernández Robles & Marín Díaz, 2017).

2.9. Aplicación WhatsApp

WhatsApp es una diligencia de mensajería instantánea que ha transformado la manera en que las personas se comunican a través de dispositivos móviles. Fundada en 2009 por Brian Acton y Jan Koum, la plataforma permitía a los consumidores enviar imágenes, mensajes de texto, videos y documentos de forma gratuita a través de una conexión a internet. La adquisición de WhatsApp

por parte de Facebook Inc. en 2014 contribuyó a su expansión global y a la incorporación de nuevas funciones (Rubio Romero & Lamo de Espinosa, 2015).

Además de los mensajes de texto, la aplicación ofrece llamadas de voz y video llamadas, así como la opción de compartir estados de texto y multimedia que desaparecen después de 24 horas. WhatsApp se ha convertido en una herramienta de comunicación fundamental para millones de personas, tanto en su vida personal como en entornos profesionales, gracias a su facilidad de uso y su compatibilidad con diversos dispositivos y sistemas operativos (Cervantes Rosas & Alvites-Huamaní, 2021).

La aplicación ha continuado evolucionando, introduciendo características de seguridad y privacidad, como el cifrado de extremo a extremo, para salvaguardar la confidencialidad de las conversaciones. En la actualidad, WhatsApp sigue siendo una de las aplicaciones de mensajería más utilizadas a nivel mundial, con un golpe significativo en la forma en que los individuos se mantienen conectadas y colaboran en diferentes contextos. Explicación detallada de WhatsApp como una aplicación de mensajería instantánea.

2.10. Ingeniería Social

Es una estrategia que involucra el engaño y la manipulación psicológica para obtener información confidencial o persuadir a individuos a realizar ciertas acciones. Esta técnica se centra en explotar la confianza, la curiosidad o el miedo de las personas, en lugar de utilizar métodos técnicos, con el fin de obtener acceso a sistemas informáticos, datos sensibles o información privilegiada (Castellanos-Portela & Carvajal-Rodríguez, 2019).

La ingeniería social es una estrategia que se asienta en la operación psicológica y el engaño para obtener información personal o persuadir a individuos a realizar acciones específicas. En lugar de depender de métodos técnicos, esta técnica se centra en explotar la confianza, la curiosidad o el miedo de las personas. Se utiliza en el contexto de la seguridad informática para obtener acceso no autorizado a sistemas, datos sensibles o información privilegiada. Este enfoque destaca la importancia de la conciencia y la educación en la protección contra ataques de ingeniería social (Castellanos-Portela & Carvajal-Rodríguez, 2019).

2.10.1. Ataques utilizados en Ingeniería social

Existen varios tipos de ataques, entre ellos se incluyen:

- Phishing: es una técnica de ingeniería social que consiste en el envío de correos electrónicos fraudulentos que aparentan ser legítimos. El objetivo es engañar a las personas para que revelen información confidencial, como contraseñas, datos financieros o personales. Estos correos electrónicos suelen dirigirse a múltiples destinatarios y pueden incluir enlaces a sitios web falsos que imitan a empresas o instituciones legítimas, con el fin de robar información sensible. Este tipo de ataque se basa en la manipulación y el engaño para obtener acceso a datos privados (Benavides , Fuertes , & Sanchez , 2020).
- Pretexting: El pretexting es una táctica de ingeniería social que implica la creación de una situación ficticia o un pretexto para engañar a las personas y obtener información confidencial. Esto puede involucrar la fabricación de una identidad falsa o la presentación de una historia inventada con el fin de obtener datos personales, financieros o de seguridad. El pretexting se centra en la manipulación psicológica y la construcción de confianza para persuadir a las personas a revelar información sensible. Este tipo de ataque se basa en la astucia y la engañosa construcción de narrativas para obtener acceso a datos privados (Rodriguez Rincon, 2018).
- Baiting: El "baiting" es una estrategia de ingeniería social que implica la promesa de un incentivo, como un archivo descargable o un enlace atractivo, con el fin de engañar a los individuos y obtener acceso a sus sistemas o datos. Este tipo de ataque se basa en la tentación de los individuos para que realicen una acción específica, como descargar un archivo o hacer clic en un enlace, que puede resultar en la instalación de software malicioso o la revelación de información confidencial. El "baiting" se aprovecha de la curiosidad o el deseo de obtener algo valioso para comprometer la seguridad de los sistemas o la privacidad de los usuarios (Rodriguez Rincon, 2018).

  Ejemplo:

Una técnica de ciberataque común es cuando las personas encuentran un dispositivo o memoria USB tirado en el suelo. La mayoría de las personas caerán en la trampa y conectarán el dispositivo a su computadora, sin sospechar que contiene software malicioso. Esto permite que el malware se introduzca en el sistema. Aunque parece una técnica simple, la mayoría de las personas piensa que son afortunadas al encontrar un dispositivo "gratis" y no se dan cuenta del peligro que corren al conectarlo. (Platzi, 2024)

Estos tipos de ataques se basan en la manipulación psicológica y la explotación de la confianza para obtener acceso a información sensible o sistemas protegidos.

2.11. Comparación de Ataques de Ingenierías Social

Tabla 1

Métodos y Técnicas de Ingeniería Social

Técnica/Método	Descripción
PRETEXTING	Hacerse pasar por un contacto de confianza para ganar la confianza de la víctima y obtener información confidencial.
Phishing	Enviar mensajes engañosos solicitando datos personales o credenciales de acceso.
SMISHING	Envío de SMS con enlaces maliciosos, para obtener información privada.
VISHING	Utilizar llamadas de voz convincentes para obtener información de la víctima.
DUMPSTER DIVING	Explotar los lazos personales y la confianza que tiene la víctima en sus contactos.
SHOULDER SURFING	Identificar y aprovechar las debilidades o errores de la víctima para manipularla.

Fuente: (Institute, 2024)

Gracias a la información de la Tabla 1, proporciona una visión general de los principales métodos y técnicas utilizados por los atacantes. Esto permite analizar de manera más completa y profunda los desafíos y riesgos asociados a este tipo de amenazas.

2.12. Google Forms

Google Forms es una aplicación ofrecida por Google que permite crear y compartir de manera sencilla y eficiente formularios personalizados. Si bien la descripción oficial de Google sobre esta herramienta se enfoca en aspectos como la planificación de eventos, el envío de encuestas y la recopilación de información, el verdadero potencial de Google Forms va más allá de estos usos (Neri Ayala, Ramos y Yovera, & Caro Soto, 2020, pág. 05).

Esta aplicación se ha convertido en un recurso excepcionalmente utilizado gracias a su sencillez de uso y su accesibilidad a través de internet. Además de crear documentos de texto, Google Forms permite incluir recursos multimedia como imágenes, audio y vídeo, ampliando significativamente sus posibilidades de uso (Neri Ayala, Ramos y Yovera, & Caro Soto, 2020, pág. 05).

Más allá de la recopilación de información, Google Forms se puede emplear como una herramienta de evaluación, ofreciendo una variedad de configuraciones y gráficos para analizar los resultados obtenidos. Su facilidad de uso y la rapidez para acceder a los resultados son algunas de las principales ventajas que han convertido a Google Forms en una aplicación muy utilizada en diversos contextos.

2.13. Website como herramientas de Prevención de fraudes Electrónicos

Existen páginas web de concientización sobre fraudes electrónicos y robos de identidad, las cuales sirven para los siguientes propósitos:

2.13.1. Educación y concientización:

- Proporcionan información detallada sobre los diferentes tipos de fraude electrónico y robo de identidad, como estafas por correo electrónico, fraude con tarjetas de crédito, suplantación de identidad, entre otros.
- Buscan educar y concientizar a los consumidores sobre cómo reconocer señales de alerta y cómo protegerse contra estos delitos.

2.13.2. Prevención y protección:

- Ofrecen consejos prácticos y recomendaciones sobre mejores prácticas de seguridad para evitar ser víctima de fraudes electrónicos y robos de identidad.
- Brindan herramientas y recursos para que los usuarios puedan fortalecer su seguridad digital y proteger sus datos personales.

2.13.3. Asistencia a víctimas:

- Proporcionan guías paso a paso sobre cómo responder y recuperarse en caso de ser víctima de un incidente de fraude o robo de identidad.

- Informan sobre los derechos de los consumidores y los pasos a seguir para denunciar y mitigar los daños.
- Ofrecen servicios de apoyo y asistencia a las víctimas, como asesoramiento legal y emocional.

2.13.4. Reporte y denuncia:

- Facilitan canales y herramientas para que los usuarios puedan reportar casos de fraude electrónico y robo de identidad a las autoridades correspondientes.
- Permiten centralizar la información sobre incidentes denunciados, lo que ayuda a las agencias gubernamentales a monitorear tendencias y desarrollar estrategias de prevención más efectivas.

2.13.5. Investigación y análisis:

- Recopilan y analizan datos sobre los tipos de fraude y robo de identidad más comunes.
- Utilizan esta información para identificar patrones, comprender las técnicas utilizadas por los delincuentes y mejorar las medidas de seguridad y protección.

2.14. Fraude Electrónico en Ecuador

Según la investigación de (Santa Cruz & Hermoza, 2019), el fraude Electrónico o informático se refieren a todos aquellos comportamientos relacionados con la transmisión y/o procesamiento automático de datos que son considerados delitos penales en la legislación de los estados. Algunos autores definen los delitos informáticos como aquellos que utilizan la informática como medio o instrumento para cometer un delito, o cuando la información es el objetivo del delito.

En Ecuador, la tipificación de conductas relacionadas con el uso de medios informáticos es relativamente nueva, con antecedentes que se remontan al año 2002 con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Esta ley introdujo reformas al Código Penal ecuatoriano para criminalizar ciertas conductas como el acceso a información protegida, la destrucción de bases de datos, la falsificación electrónica, entre otros (Santa Cruz & Hermoza, 2019, pág. 04).

Posteriormente, con la entrada en vigor del Código Orgánico Integral Penal (COIP) en 2014, el número de conductas consideradas delitos informáticos se incrementó. Aunque el COIP no tiene una categoría específica de "delitos informáticos", existen varios artículos que pueden ser considerados como tales, como la pornografía con menores, el contacto sexual con menores por medios electrónicos, la violación a la intimidad, el acceso no consentido a sistemas informáticos, entre otros. A pesar de la creación de unidades especializadas en la Fiscalía General del Estado para combatir este tipo de criminalidad, existen desafíos, como la falta de fiscales, que ocasionan que muchas investigaciones se estanquen en la fase inicial por falta de evidencias, lo que aumenta la impunidad (Santa Cruz & Hermoza, 2019).

2.15. Concepto y comparación de bases de datos

Una base de datos es una colección organizada de información que se almacena y gestiona de forma sistemática. Está diseñada para permitir el acceso, la manipulación y el mantenimiento eficientes de los datos. Las bases de datos facilitan el almacenamiento de grandes cantidades de datos de manera estructurada, lo que permite a los usuarios y aplicaciones recuperar, actualizar y administrar esa información de manera rápida y precisa. Mediante el uso de un sistema que gestiona las bases de datos (SGBD), las bases de datos ofrecen funcionalidades avanzadas como la garantía de la integridad de los datos, la observación de ingreso o acceso, la realización de consultas complejas y la generación de informes. Las bases de datos son herramientas fundamentales para la gestión eficiente de la información en una amplia variedad de contextos (ver tabla 2) (Capacho Portilla & Nieto Bernal, 2017).

Tabla 2

Comparación de Bases de datos

Bas de datos	Tipo	Característica	Ventajas	Desventaja
MongoDB	NoSQL (Orientada a Documentos)	▪ Almacena datos en formato JSON. ▪ Escalabilidad horizontal ▪ Replicación y sharding incorporados	▪ Flexibilidad en el esquema de datos ▪ Alta Escalabilidad ▪ Alto rendimiento para lecturas y escrituras	▪ Menor soporte para transacciones complejas ▪ Mayor consumo de espacio de almacenamiento
PostgreSQL	SQL (Relacional)	▪ soporte completo para el estándar SQL ▪ Características avanzadas como transacciones ACID, índices, vistas, triggers, etc.	▪ Integridad de datos ▪ Amplia comunidad y documentación ▪ Escalabilidad vertical	▪ Menor rendimiento para algunas cargas de trabajo ▪ Configuración y administración más compleja
SQLite	SQL (Relacional)	▪ Sistema de base de datos autosuficiente ▪ Fácil de configurar e integrar Bajo consumo de recursos	▪ Muy ligero y sencillo de usar ▪ Buena opción para proyectos pequeños y móviles	▪ Limitaciones en el tamaño de la base de datos y número de usuarios concurrentes

				▪ Menor funcionalidad que otras bases de datos SQL
MYSQL	SQL (Relacional)	▪ Sistema de base de datos relacional líder en el mercado ▪ Soporte completo para SQL estándar ▪ Amplia comunidad y documentación	▪ Escalabilidad probada ▪ Alto rendimiento ▪ Facilidad de uso e implementación	▪ Menor funcionalidad avanzada que PostgreSQL ▪ Puede requerir más configuración para alta disponibilidad

Fuente: (Slideshare, 2024)

2.16. Lenguaje de Programación

Los lenguajes de programación que se utilizan comúnmente para el desarrollo de páginas web serán presentados en una tabla comparativa (ver tabla 3), pero tienen diferentes casos de uso. Son ideales para que cualquier aspirante a programador en el mercado aprenda a armar la estructura principal de una página web, incluyendo sus elementos, atributos y otros componentes.

Tabla 3

Comparación de Lenguajes de Programación

Lenguaje/tecnología	Características	Ventajas	Desventajas
ASP y ASP.NET	▪ Código en cualquier lenguaje compatible con CLR ▪ Capacidad de combinación con otros lenguajes ▪ Soporte MVC ▪ Plataforma específica de desarrollo	▪ Flexibilidad de usar diversos lenguajes ▪ Patrón de diseño MVC bien establecido	▪ Escaso soporte comunitario ▪ Plataforma específica puede limitar portabilidad
AJAX	▪ Técnica para crear aplicaciones web interactivas ▪ Utiliza DOM para visualización e interacción dinámica ▪ Usa tecnologías existentes ▪ Soportada por navegadores modernos	▪ Mejora la interactividad y respuesta de las aplicaciones web ▪ Aprovecha tecnologías ampliamente adoptadas	▪ Pierde el concepto tradicional de "volver a la página anterior" ▪ Puede desorientar al usuario con páginas con y sin AJAX
JSP	▪ Combina poder de Java en servidor y flexibilidad de HTML en cliente ▪ Permite crear clases para lógica de negocio y acceso a datos	▪ Integra Java y HTML de forma efectiva ▪ Permite una estructura organizada de la aplicación	▪ Gran parte de la lógica se ejecuta en el servidor, pudiendo sobrecargarlo
PHP	▪ Lenguaje de scripting para desarrollo web ▪ Integración con bases de datos y HTML ▪ Ampliamente utilizado en la web	▪ Fácil de aprender y usar ▪ Gran ecosistema y soporte comunitario ▪ Buena integración con bases de datos	▪ Rendimiento puede ser menor que otros lenguajes ▪ Algunas prácticas de codificación pueden llevar a vulnerabilidades
Python	▪ Lenguaje interpretado, de tipiado dinámico y fuerte ▪ Enfoque en programación sana y productiva	▪ Sintaxis clara y legible ▪ Amplia variedad de librerías y frameworks ▪ Excelente para desarrollo rápido de prototipos	▪ Algunas librerías por defecto no son del agrado de toda la comunidad

Fuente: (Linares, 2024)

CAPÍTULO III: MARCO METODOLÓGICO

3. Metodología de Investigación

Según (Galarza, 2020) la metodología de investigación se refiere al conjunto de procedimientos y técnicas que se utilizan para llevar a cabo una investigación de manera sistemática y rigurosa. Es el marco teórico y práctico que guía el proceso de investigación, desde la formulación del problema hasta la presentación de los resultados. Algunos elementos clave de la metodología incluyen el paradigma de investigación, el método de investigación (cualitativo, cuantitativo o mixto), las técnicas de recolección de datos, el análisis de datos, la validez y confiabilidad de los resultados, y las consideraciones éticas. La metodología de investigación proporciona un marco estructurado y rigurosamente diseñado para llevar a cabo una investigación efectiva y confiable, guiando al investigador a lo largo de todas las etapas del proceso de investigación.

3.1. Tipo de Investigación

La propuesta metodológica para esta tesis se basa en una combinación de investigación documental y de campo, lo cual permitirá generar un marco sólido y robusto para el desarrollo del proyecto.

3.1.1. Investigación Aplicada

Es una investigación aplicada, su diseñó es de manera ética y responsable ya que se enfoca en:

Problema práctico a abordar: La necesidad de concientizar a los estudiantes sobre los riesgos de entregar datos personales y hacer clic en enlaces web sospechosos.

Objetivo aplicado: Desarrollar estrategias o intervenciones efectivas para educar a los estudiantes y motivarlos a proteger su información personal en entornos digitales.

Metodología apropiada:

- Se realizará una encuesta a los estudiantes para comprender sus conocimientos, actitudes y comportamientos actuales.
- Se diseñará un programa de concientización, utilizando medios y técnicas que respeten la ética y la privacidad de los participantes.

- Se evaluará el impacto del programa en los conocimientos, actitudes y prácticas de los estudiantes para mejorar la propuesta.

Enfoque en la aplicación práctica:

- Los resultados de la investigación deben servir para desarrollar estrategias, materiales educativos o intervenciones concretas que puedan ser implementadas en la universidad.
- El objetivo final sería lograr un cambio positivo en el comportamiento de los estudiantes en cuanto a la protección de sus datos personales.

Consideraciones éticas:

- Obtener el consentimiento informado de los participantes en todas las etapas de la investigación.
- Respetar la privacidad y confidencialidad de la información recopilada.
- Asegurarse de que las actividades de concientización no impliquen engaño o prácticas que puedan poner en riesgo a los estudiantes.

3.1.2. Investigación documental:

El componente documental de la investigación se enfocará en la revisión exhaustiva de fuentes de información secundarias relacionadas con el tema de estudio. Algunas de las principales fuentes a consultar serán:

- Artículos científicos y académicos sobre ingeniería social, ataques a través de dispositivos móviles y la aplicación WhatsApp.

- Informes, estudios y publicaciones de organizaciones especializadas en ciberseguridad, que aporten datos, tendencias y mejores prácticas en esta área.

- Marcos legales y regulatorios aplicables a la investigación, tanto a nivel nacional como internacional.

El objetivo de esta fase documental será recopilar información, antecedentes y conocimientos previos que sirvan como fundamento teórico y contextual para el desarrollo de la tesis. Esto permitirá tener una sólida base de información secundaria que respalde y enriquezca la investigación.

3.1.3. Investigación de campo:

Por otra parte, la investigación de campo se centrará en la aplicación de una encuesta a usuarios de la universidad. Los datos recopilados en el trabajo de campo complementarán los hallazgos de la revisión documental, brindando una visión más completa del fenómeno que se está estudiando. Esto permitirá generar un análisis integral que combine tanto información secundaria como primaria.

Al integrar estos dos enfoques metodológicos (documental y de campo), se podrá desarrollar un marco sólido y robusto para la investigación sobre la simulación de ataque través de WhatsApp. Es importante mantener un enfoque ético y responsable a lo largo de todo el proceso, priorizando la seguridad y el bienestar de los participantes. Este abordaje metodológico permitirá cumplir con los objetivos de la investigación, generando resultados confiables y de alto impacto en el ámbito académico y práctico.

3.2. Enfoque de la Investigación

De acuerdo a la investigación el enfoque de la investigación es cuantitativo ya que la recolección de datos mencionado en la metodología incluye la aplicación de una encuesta a los usuarios de la universidad la cual puede ser medida y graficada.

- Al recopilar datos a través de una encuesta, se estará obteniendo información en formato numérico y estadístico sobre los hábitos, percepciones y conocimientos de los participantes.
- Estos datos cuantitativos permitirán medir, cuantificar y analizar patrones, tendencias y relaciones entre variables.
- Una vez recolectados los datos de la encuesta, se podrá proceder a analizarlos utilizando técnicas y herramientas cuantitativas. Esto puede incluir análisis estadísticos, cálculo de porcentajes, elaboración de gráficos y tablas, entre otros.
- El análisis cuantitativo de los datos te permitirá identificar y establecer relaciones, tendencias y hallazgos medibles.

3.3. Población y Muestra

3.3.1. Población

La población para el desarrollo de esta tesis está conformada por un total de 200 usuarios de la Pontificia Universidad Católica del Ecuador.

Características de la población:

- Tamaño de la población: 200 usuarios.

- Ubicación geográfica: La población se encuentra ubicada en Quito.

- Perfil de los usuarios: La población incluye usuarios de diversas edades, géneros, niveles socioeconómicos y niveles de conocimiento tecnológico.

- Criterios de inclusión: Todos los participantes deben ser usuarios activos de la aplicación móvil WhatsApp.

Relevancia de la población:

- La población de 200 usuarios de WhatsApp es relevante y representativa para los objetivos de la investigación, ya que permitirá recopilar información valiosa sobre los hábitos, percepciones y conocimientos de los usuarios en torno a los riesgos de ingeniería social en esta aplicación de mensajería.

- Al ser una población de tamaño moderado, se podrá realizar un análisis más profundo y detallado de los datos recopilados, lo cual enriquecerá los hallazgos y las conclusiones de la tesis.

- La diversidad de perfiles dentro de la población brindará una visión más amplia y representativa del fenómeno estudiado.

3.3.2. Muestra

Para seleccionar a los participantes de la encuesta dentro de esta población de 200 usuarios, se utilizará un muestreo aleatorio simple. Esto permitirá que cada usuario tenga la misma probabilidad de ser seleccionado, lo cual aumentará la representatividad de la muestra.

Entendiendo, si la población de la investigación se considera infinita, es decir, no se conoce el número total de usuarios de WhatsApp, se calcula el tamaño de la muestra de manera diferente.

Para calcular el tamaño de muestra cuando la población es infinita, puedes utilizar la siguiente fórmula:

$$n = [(z^2 * N * p * q) / (e^2 * (N - 1) + (z^2 * p * q))]$$

Donde:

N= Población = 415

Z = Nivel de confianza (normalmente 95%, que es 1.96)

p = Probabilidad de éxito (0.5 si no se conoce)

e = Margen de error o precisión (normalmente 5% o 0.05)

q = probabilidad de Fracaso = (1-q) =0.5

Aplicando los valores:

Bien, con los datos proporcionados, procedemos a calcular el tamaño de muestra utilizando la fórmula:

$$n = [(z^2 * N * p * q) / (e^2 * (N - 1) + (z^2 * p * q))]$$

Datos:

N = 413 (Población)

z = 1.96 (Nivel de confianza del 95%)

p = 0.5

q = 0.5

e = 0.05 (Margen de error del 5%)

Sustituyendo los valores en la fórmula:

$$n = [(1.96^2 * 415 * 0.5 * 0.5) / (0.05^2 * (415 - 1) + (1.96^2 * 0.5 * 0.5))]$$

$$n = [(3.8416 * 415 * 0.25) / (0.0025 * 414 + 0.9604)]$$

$$n = [399.332 / 1.9954]$$

n = 200.01

Por lo tanto, el tamaño de muestra recomendado con los datos proporcionados es de 200.01 personas.

Redondeando el resultado, el tamaño de muestra sería de aproximadamente 200 usuarios.

Algunos aspectos a tener en cuenta:

Nivel de confianza: Utilizamos un nivel de confianza del 95%, que es el más comúnmente usado. Puedes ajustarlo según tus necesidades.

Probabilidad de éxito: Al no tener una estimación previa, asumimos una probabilidad de 0.5, que es la más conservadora.

Margen de error: Usamos un margen de error del 5%, que es un valor estándar. Puedes ajustarlo según tus requerimientos.

Al tener una población finita de 413 Personas, la muestra de 200 usuarios representará adecuadamente a los usuarios de la universidad con WhatsApp, con un nivel de confianza del 95% y un margen de error del 5%.

3.4. Técnicas y herramientas de Recolección de Datos

Según (Galarza, 2020) en la investigación, existen diversas técnicas y herramientas que se pueden utilizar para la recolección de datos. Algunas de las más comunes incluyen:

- **Encuestas:** Esta técnica implica la recopilación de información a través de cuestionarios estructurados, ya sea en formato físico o digital, que se distribuyen a una muestra representativa de la población objetivo.
- **Entrevistas:** Las entrevistas permiten obtener información más detallada y en profundidad a través de la interacción directa con los participantes. Pueden ser de tipo estructurado, semiestructurado o no estructurado.
- **Observación:** La observación implica el registro sistemático de comportamientos, actividades y eventos relevantes para la investigación. Puede ser observación participante o no participante.
- **Análisis de documentos:** El análisis de documentos, ya sean físicos o digitales, permite recopilar información relevante a partir de fuentes existentes, como informes, registros, artículos y publicaciones.

- **Herramientas tecnológicas:** Diversas herramientas tecnológicas, como encuestas en línea, aplicaciones móviles, sensores y dispositivos de seguimiento, pueden facilitar la recolección de datos de manera eficiente y automatizada.

CAPÍTULO IV: DESARROLLO DE LA SIMULACIÓN

4. Estrategia

La estrategia de recolección de datos involucra la planificación y organización de las diferentes técnicas y herramientas que se utilizarán para obtener la información necesaria para la investigación. La estrategia de recolección de datos en esta investigación se centra en la implementación de encuestas para evaluar la efectividad de la simulación de ataques a través de dispositivos móviles utilizando la aplicación WhatsApp

4.1. Encuesta

Las encuestas se diseñaron para recopilar información sobre la percepción y el comportamiento de los usuarios ante los ataques simulados a través de WhatsApp en dispositivos móviles. Estas encuestas se aplicó una muestra representativa de la población objetivo

Ítems 01 ¿Estaría usted de acuerdo en autorizar el uso de sus datos con fines educativos e investigación?

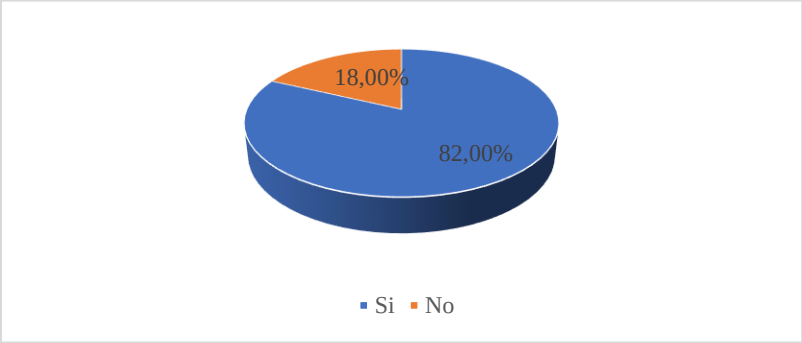
Tabla 4

¿Estaría usted de acuerdo en autorizar el uso de sus datos con fines educativos e investigación?

Si	%	No	%	Total
164	82	36	18	200

Figura 1

¿Estaría usted de acuerdo en autorizar el uso de sus datos con fines educativos e investigación?



Gracias a la información de la tabla 4, la gran mayoría de las personas encuestadas, 164 de 200, estarían de acuerdo en autorizar el uso de sus datos con fines educativos e investigación. Esto representa el 82% de la muestra. Un grupo más pequeño, 36 de 200 personas, no estarían de acuerdo con dicha autorización. Esto representa el 18% de la muestra. El alto porcentaje de aceptación (82%) sugiere que la mayoría de los encuestados estarían dispuestos a colaborar y permitir el uso de sus datos para fines educativos e investigación. Esto podría facilitar el desarrollo de estudios y proyectos que requieran el uso de información personal con propósitos legítimos.

Consideraciones éticas: Sin embargo, es importante tener en cuenta las preocupaciones de la minoría (18%) que no desean autorizar el uso de sus datos. Esto destaca la necesidad de implementar procesos de consentimiento informado y garantizar la protección adecuada de la privacidad y confidencialidad de los datos.

Ítems 02 Género

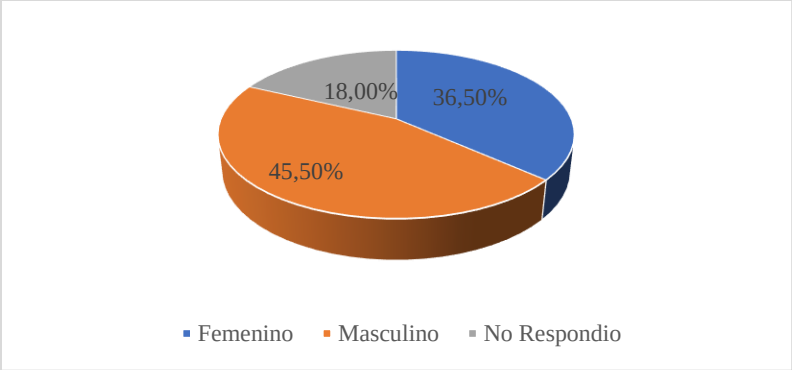
Tabla 5

Género

Femenino	%	Masculino	%	No Respondió	%
73	36.5	91	45.5	36	18

Figura 2

Género



Gracias a la información de la tabla 5 se evidencia que la muestra está compuesta por una mayoría de participantes de género Masculino, representando el 45.5% del total, mientras que los participantes de género Femenino constituyen el 36.5%. La mayor proporción de participantes de

género Masculino puede reflejar la composición o tendencias del grupo objetivo de la investigación. Sin embargo, es importante considerar si esta distribución de género es representativa de la población a la que se pretende generalizar los hallazgos. Dado que existe una diferencia significativa en la composición de género de la muestra, sería relevante analizar si existen patrones, comportamientos o percepciones distintas entre hombres y mujeres en relación a los temas abordados sobre ataques de ingeniería social a través de dispositivos móviles. Los resultados segmentados por género pueden aportar valiosos insights para diseñar estrategias de prevención y mitigación de ataques más efectivas y adaptadas a las necesidades específicas de hombres y mujeres. Se puede evidenciar que un 18% de los usuarios no quisieron responder.

Ítems 03 Edad

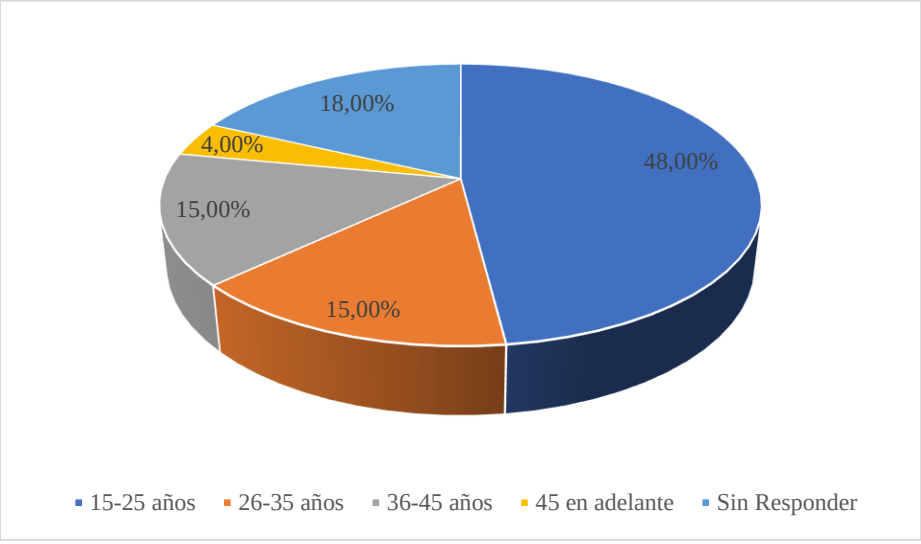
Tabla 6

Edad

Rango de edad	Cantidad	%
15-25 años	96	48
26-35 años	30	15
36-45 años	30	15
45 en adelante	8	4
Sin Responder	36	18

Figura 3

Edad



La información de la tabla 6 se demuestra el predominio del rango de 15-25 años, El rango de 15-25 años representa el 48% del total de datos, siendo el grupo más numeroso. Este resultado sugiere que la investigación probablemente se enfoca en población joven o adolescente. La presencia los rangos de 26-35 años (15%) y 36-45 años (15%) también tienen una representación significativa, esto indica que la investigación podría beneficiarse al considerar la perspectiva de otros grupos etarios, más allá del predominante de 15-25 años. Al analizar las diferencias y similitudes entre los distintos grupos de edad puede aportar una visión más completa a la investigación. El grupo de 45 años en adelante esta con solo el 4% del total, el grupo de 45 años en adelante es el menos representado, se puede apreciar que de las 200 personas 36 no dieron respuesta de la edad.

Ítems 04 Tipo de premio que te gustaría ganar

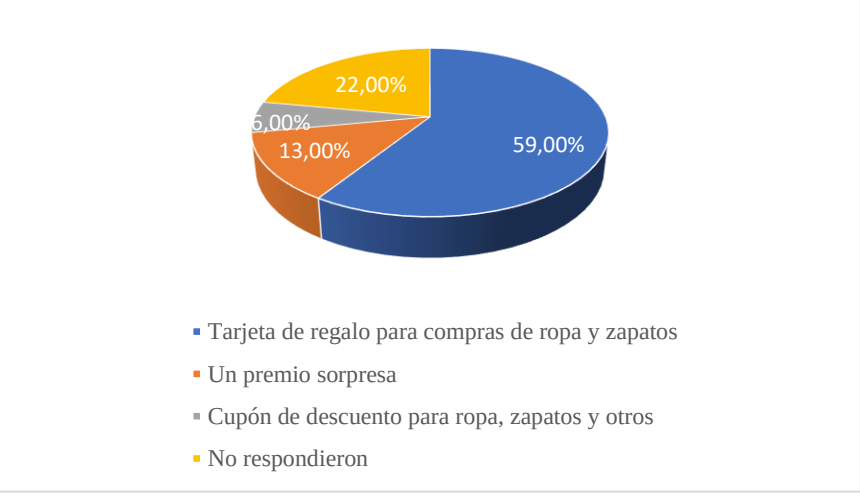
Tabla 7

Tipo de premio que te gustaría ganar

Tipo de premio	Cantidad	%
Tarjeta de regalo para compras de ropa y zapatos	125	59
Un premio sorpresa	27	13
Cupón de descuento para ropa, zapatos y otros	12	6
No respondieron	36	22

Figura 4

Tipo de premio que te gustaría ganar



La tabla 7 evidencia que la opción predominante es la "Tarjeta de regalo para compras de ropa y zapatos", lo cual representa un 59% del total de premios ofrecidos. Por otro lado, los "Premios sorpresa" y los "Cupones de descuento" representan un 13% y 6% respectivamente. Esta distribución de premios sugiere que el objetivo principal de esta encuesta es obtener información y datos de las personas que optan por la tarjeta de regalo, probablemente con fines de realizar engaños de marketing o ventas dirigidas. Los premios sorpresa y los cupones de descuento podrían estar sirviendo como señuelos para atraer a los participantes y obtener sus datos personales o de contacto, lo cual se consideraría una práctica de ingeniería social. Adicional también se puede evidenciar que el 22% no hubo respuesta por parte de los participantes.

Ítems 05 ¿Cuál de las siguientes marcas de ropa prefieres Masculino?

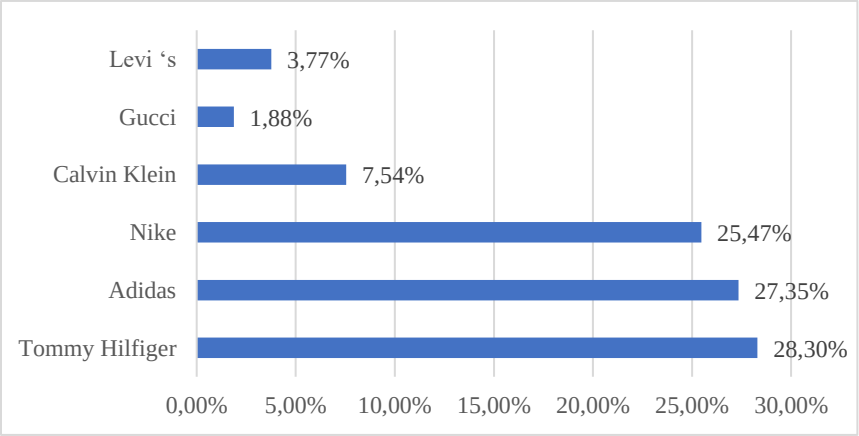
Tabla 8

¿Cuál de las siguientes marcas de ropa prefieres Masculino?

Marca	Cantidad	%
Tommy Hilfiger	26	28.3
Adidas	25	27.35
Nike	24	25.47
Calvin Klein	10	7.54
Gucci	2	1.88
Levi ‘s	4	3.77

Figura 5

¿Cuál de las siguientes marcas de ropa prefieres Masculino?



Gracias a la tabla 8 se puede evidenciar que la marca de ropa preferida es Tommy Hilfiger, con 30 menciones y 28.3% del total. Adidas es la segunda marca más popular, con 29 menciones y 27.35%, Nike ocupa el tercer lugar con 27 menciones y 25.47%, Calvin Klein, Levi's y Gucci tienen una presencia menor, con 7.54%, 3.77% y 1.88% respectivamente y el 5.66% de los participantes, es decir 6 personas, no respondieron a esta pregunta. Esta información detallada proporciona una visión clara de las preferencias de marcas de ropa entre los participantes. La distribución muestra un liderazgo de Tommy Hilfiger, seguido de cerca por Adidas y Nike. Es importante tener en cuenta que el porcentaje de no respuesta, aunque bajo, puede reflejar algunas limitaciones o sesgos en la muestra, la información tabulada ofrece una base sólida para comprender las tendencias de preferencia de marcas de ropa en este grupo de participantes.

Ítems 06 ¿Cuál de las siguientes marcas de ropa prefieres Femenino?

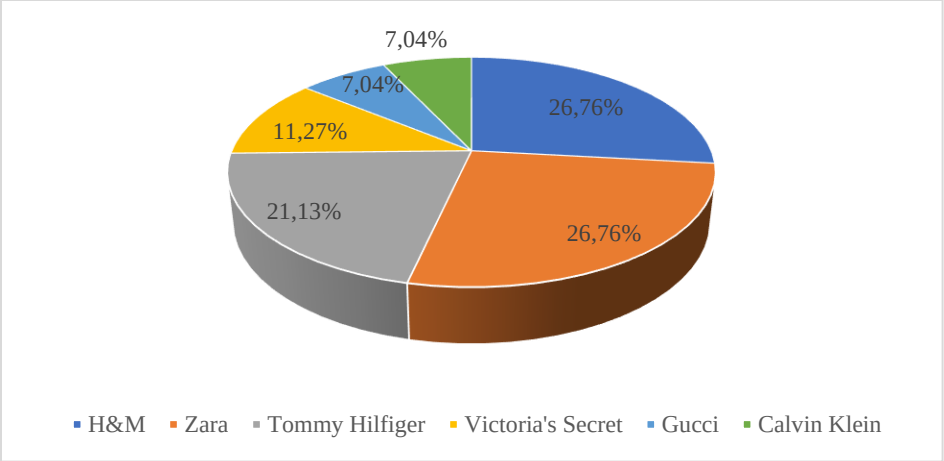
Tabla 9

¿Cuál de las siguientes marcas de ropa prefieres Femenino?

Marca	Cantidad	Porcentaje
H&M	17	26.76%
Zara	19	26.76%
Tommy Hilfiger	18	21.13%
Victoria's Secret	9	11.27%
Gucci	5	7.04%
Calvin Klein	5	7.04%

Figura 6

¿Cuál de las siguientes marcas de ropa prefieres Femenino?



La tabla 9 muestra las preferencias de marcas de ropa femenina. Las marcas más preferidas son Zara y H&M, ambas con 26.76% de preferencia. Le sigue Tommy Hilfiger con 21.13%. Las marcas menos preferidas son Gucci y Calvin Klein, con 7.04% cada una.

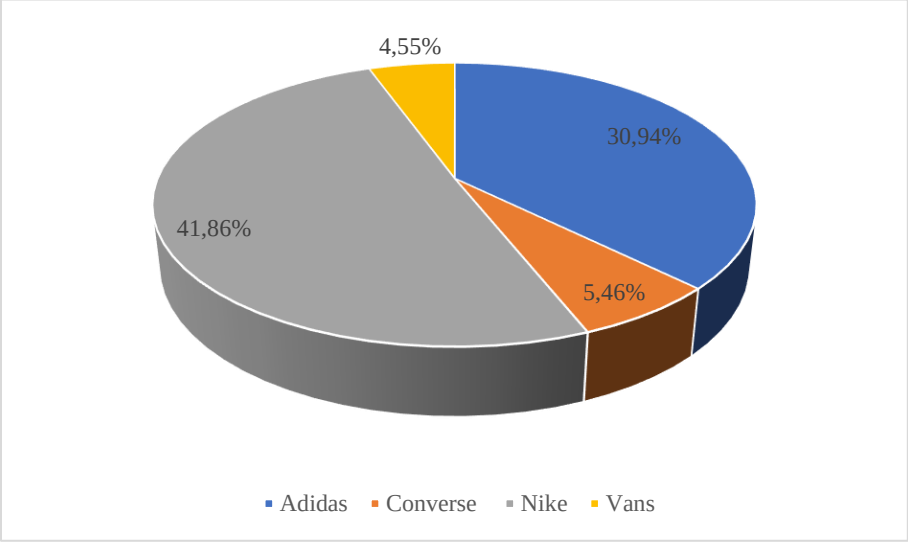
Ítems 07 ¿Cuál de las siguientes marcas de zapatos prefieres? Masculino

Tabla 10

¿Cuál de las siguientes marcas de zapatos prefieres? Masculino

Marca	Cantidad	Porcentaje
Adidas	34	30.94%
Converse	6	5.46%
Nike	46	41.86%
Vans	5	4.55%

Figura 7 ¿Cuál de las siguientes marcas de zapatos prefieres? Masculino



La tabla 10 indica que la marca con mayor cantidad de unidades es Nike con 46, representando el 41.86% del total. La segunda marca con mayor cantidad es Adidas con 34 unidades, que equivale al 30.94% del total. Converse tiene 6 unidades, lo que representa el 5.46% del total. Vans tiene la menor cantidad con 5 unidades, siendo el 4.55% del total. Las marcas con mayor presencia son Nike y Adidas, abarcando la mayor parte del mercado representado en estos datos. Las marcas Converse y Vans tienen una participación más baja en comparación.

Ítems 08 ¿Cuál de las siguientes marcas de zapatos prefieres? Femenino

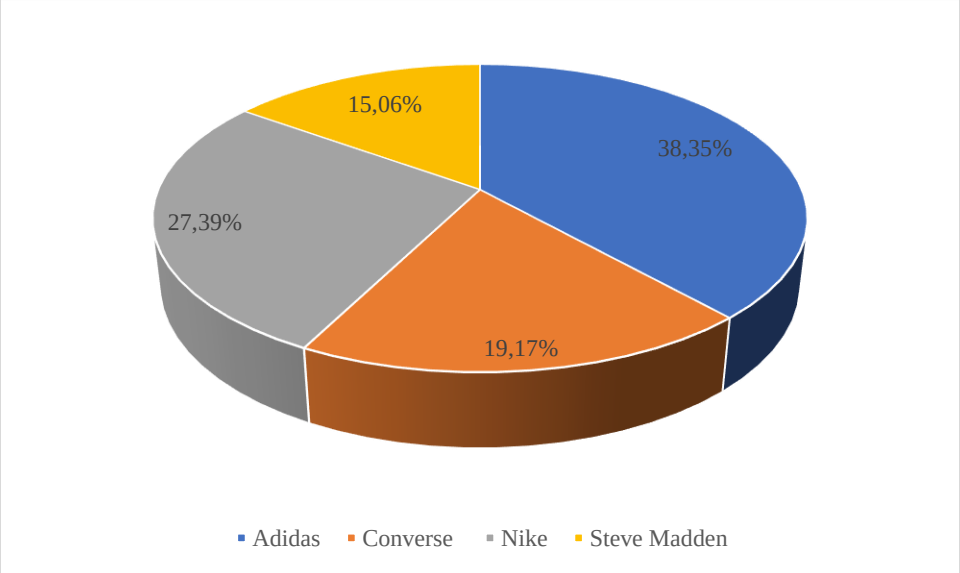
Tabla 11

¿Cuál de las siguientes marcas de zapatos prefieres? Femenino

Marca	Cantidad	Porcentaje
Adidas	28	38.35
Converse	14	19.17
Nike	20	27.39
Steve Madden	11	15.06

Figura 8

¿Cuál de las siguientes marcas de zapatos prefieres? Femenino



Gracias a la información de la tabla 11, se pudo comprobar que la marca con mayor cantidad y porcentaje es Adidas, con 28 usuarios que le llaman la atención esta marca que representan el 38.35% del total. Converse es la segunda marca con 14 pts., equivalente al 19.17% del total. Nike ocupa el tercer lugar con 20 pts., que corresponden al 27.39% del total. Steve Madden es la marca con menor cantidad, con 11 unidades, que representan el 15.06% del total.

Ítems 09 ¿Cuál de las siguientes marcas de parlantes prefieres?

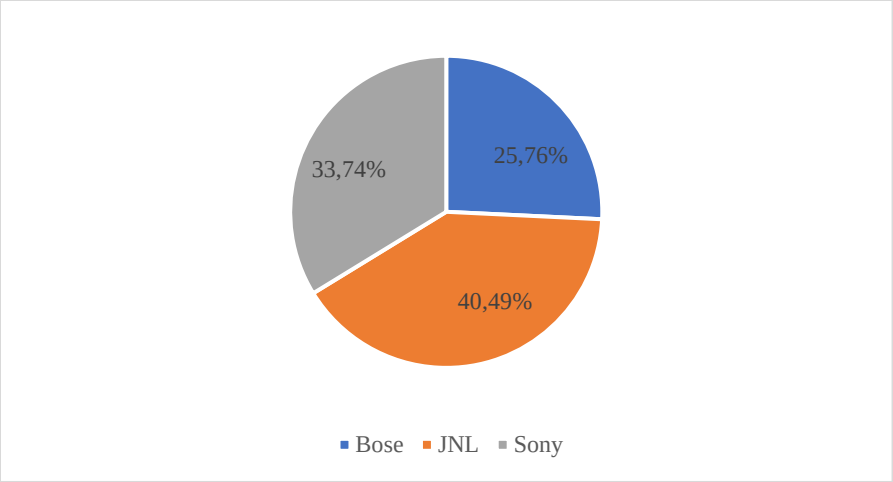
Tabla 12

¿Cuál de las siguientes marcas de parlantes prefieres?

Marca	Cantidad	Porcentaje
Bose	42	25.7668712
JNL	66	40.4907975
Sony	55	33.7423313

Figura 9

¿Cuál de las siguientes marcas de parlantes prefieres?



La tabla 12 indica que la marca preferida: La marca de parlantes preferida por los encuestados es JNL, con 66 menciones y un porcentaje del 40.49%. La segunda marca preferida es Sony, con 55 menciones y un porcentaje del 33.74%. La tercera marca preferida es Bose, con 42 menciones y un porcentaje del 25.77%. Los datos muestran una clara preferencia por la marca JNL, seguida por Sony y Bose. La diferencia entre las tres marcas es significativa, con JNL liderando con una mayor cantidad de menciones. Tendencias del mercado: Estos resultados pueden reflejar las tendencias de preferencia de marcas de parlantes en el mercado objetivo. La predominancia de JNL sugiere que esta marca es la más popular y atractiva para los consumidores encuestados lo que puede permitir utilizar esta como un señuelo para aplicar la Ingeniería social.

Conocer las preferencias de marca de parlantes de los participantes puede ser relevante para el desarrollo de la simulación de ataque de ingeniería social. Utilizar elementos relacionados en las marcas preferidas puede aumentar la efectividad y realismo de la simulación. Los datos

muestran que la marca de parlantes preferida por los encuestados es JNL, seguida por Sony y Bose. Esta información puede ser valiosa para orientar el diseño y la implementación de la simulación de ataque de ingeniería social a través de dispositivos móviles y la aplicación WhatsApp.

4.2. Análisis General

La muestra está compuesta por una mayoría de participantes de género masculino (45.5%), seguidos de participantes de género femenino (36.5%) y un 18% que no respondieron. El rango de edad predominante es de 15 a 25 años (48%), seguido de los rangos de 26-35 años (15%) y 36-45 años (15%). El grupo de 45 años en adelante es el menos representado (4%). La gran mayoría de los encuestados (82%) estarían de acuerdo en autorizar la utilización de sus datos con fines educativos e investigación, lo cual facilita el desarrollo del estudio.

La preferencia mayoritaria (59%) por tarjetas de regalo para compras de ropa y zapatos como premio sugiere que este incentivo podría ser utilizado como señuelo en la simulación de ataque de ingeniería social. Los premios sorpresa (13%) y los cupones de descuento (6%) también podrían servir como atractivos para atraer a los participantes y obtener información personal. Es importante analizar si la oferta de estos premios influye en la disposición de los usuarios a proporcionar datos o a caer en el engaño, lo cual constituiría una práctica de ingeniería social.

Las marcas preferidas por los participantes masculinos son Tommy Hilfiger, Adidas y Nike, lo que refleja las tendencias de consumo de este grupo. Conocer estas preferencias de marcas puede ser útil para diseñar escenarios de ataque de ingeniería social más realistas y efectivos, al utilizar elementos familiares y atractivos para los participantes. Las marcas preferidas por las participantes femeninas son H&M, Zara y Tommy Hilfiger, mostrando diferencias en las preferencias de género. Al igual que en el caso de los hombres, esta información sobre las marcas de ropa preferidas por las mujeres puede ser valiosa para el desarrollo de la simulación de ataque.

Las marcas de zapatos preferidas por los participantes masculinos son Nike, Adidas y Converse, con una clara predominancia de Nike. Estos hallazgos pueden guiar el diseño de la simulación de ataque, al utilizar elementos relacionados con las marcas de zapatos más populares entre los hombres.

Las participantes femeninas prefieren principalmente las marcas Adidas, Nike y Converse para sus zapatos. Al igual que con la preferencia de marcas de ropa, estos datos pueden informar el desarrollo de la simulación de ataque de ingeniería social dirigida a mujeres.

La marca de parlantes preferida por los encuestados es JNL, con un 40.49% de menciones. Le siguen Sony con un 33.74% y Bose con un 25.77%. Esto muestra una clara preferencia por la marca JNL, que es significativamente más alta que las otras dos. Estos datos sobre las preferencias de marca pueden ser relevantes para el desarrollo de una simulación de ataque de ingeniería social. Utilizar elementos relacionados con las marcas preferidas, como JNL, puede aumentar la efectividad y realismo de la simulación.

En general, el análisis profundo de los resultados de la herramienta de recolección de datos revela información valiosa sobre las características, preferencias y tendencias de los participantes. Estos insights pueden ser utilizados para diseñar una simulación de ataque de ingeniería social a través de WhatsApp que sea más realista, efectiva y adaptada a las necesidades y características específicas de la población objetivo. Sin embargo, es importante considerar las limitaciones de la muestra y atestiguar la protección de la privacidad de los participantes, especialmente de aquellos que no autorizaron el uso de sus datos. La alta aceptación de los usuarios para autorizar el uso de sus datos sugiere una predisposición favorable hacia los fines educativos e investigativos de la tesis. La predominancia de participantes jóvenes (15-25 años) indica que el estudio se enfoca en este grupo etario, lo cual podría ser relevante para analizar su vulnerabilidad ante ataques de ingeniería social. La preferencia por premios como tarjetas de regalo y cupones de descuento podría ser utilizada como señuelo para atraer a los participantes y obtener información personal, lo cual constituiría una práctica de ingeniería social.

Los resultados proporcionan datos valiosos para diseñar y desarrollar la simulación de ataque a través de WhatsApp, adaptándola a las características y preferencias de la muestra objetivo. El conocimiento de las marcas y premios preferidos por los participantes puede ser utilizado para diseñar escenarios de ataque más realistas y efectivos.

CAPÍTULO V IMPLEMENTACIÓN DE LA SIMULACIÓN

5. Simulación

5.1. Simulación de Ataque

Para comprobar la eficacia de ataques de engaño con ingeniería social, y comprender mejor el funcionamiento de los mismos, se llevará a cabo una simulación de un robo de información, utilizando para ello plataformas que se describirán.

5.1.1. Selección de Herramientas

A continuación, se selecciona las herramientas y opciones necesarias para el método de desarrollo a crear:

5.1.1.1. Bases de Datos

Para llevar a cabo el proyecto de tesis "Generación de una simulación de ataque de ingeniería social a través de dispositivos móviles con la aplicación WhatsApp", es fundamental contar con una base de datos que permita almacenar y gestionar eficientemente la información recopilada. MySQL se perfila como una excelente opción para este proyecto de investigación por varias razones:

Adecuado para el alcance del proyecto ya que implica un número relativamente pequeño de tablas, MySQL se adapta bien a estas necesidades gracias a su simplicidad y facilidad de uso. Es conocido por su alto rendimiento en cargas de trabajo de lectura y escritura, lo cual es fundamental para registrar y consultar los datos de la simulación. Además, ofrece una escalabilidad contrastada, permitiendo que el sistema pueda crecer a medida que se recopile más información. También posee una extensa comunidad de desarrolladores y la documentación exhaustiva de MySQL facilitan el aprendizaje y la resolución de problemas, lo cual es valioso en un el proyecto de tesis. Se integra de manera sencilla con una variedad de herramientas y lenguajes de programación, lo que permitirá una conexión y procesamiento eficiente de los datos de la simulación. En comparación con otras opciones de bases de datos más avanzadas, MySQL generalmente requiere menos configuración y mantenimiento, lo cual es beneficioso en un proyecto de tesis donde el enfoque debe estar en la investigación y el análisis.

Figura 10

MySQL

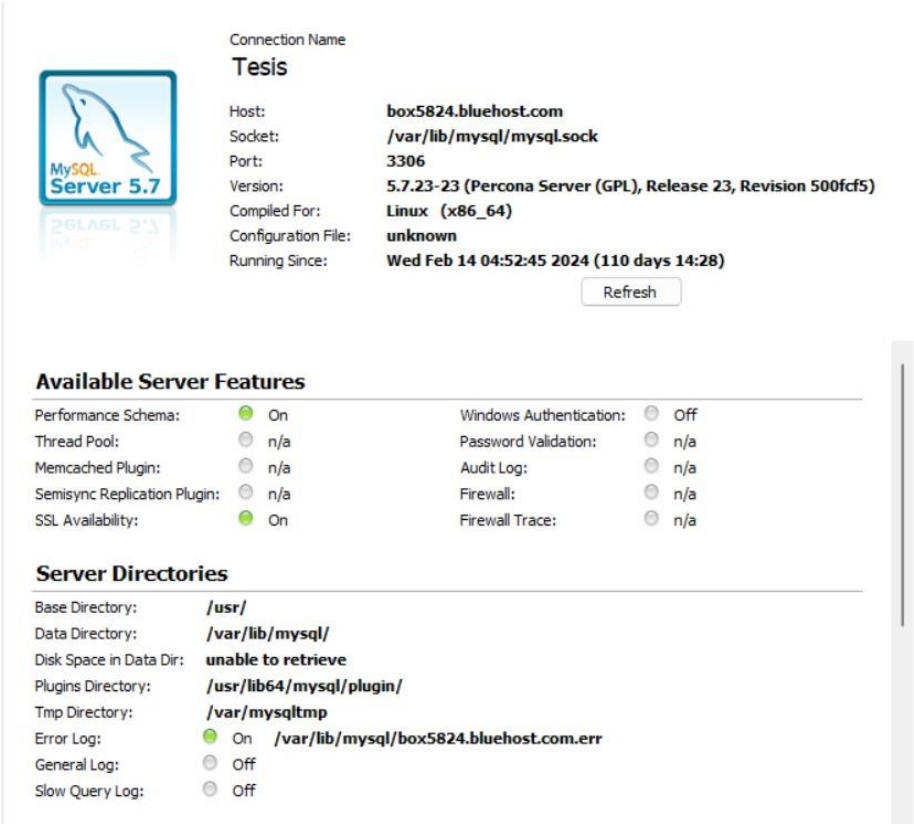
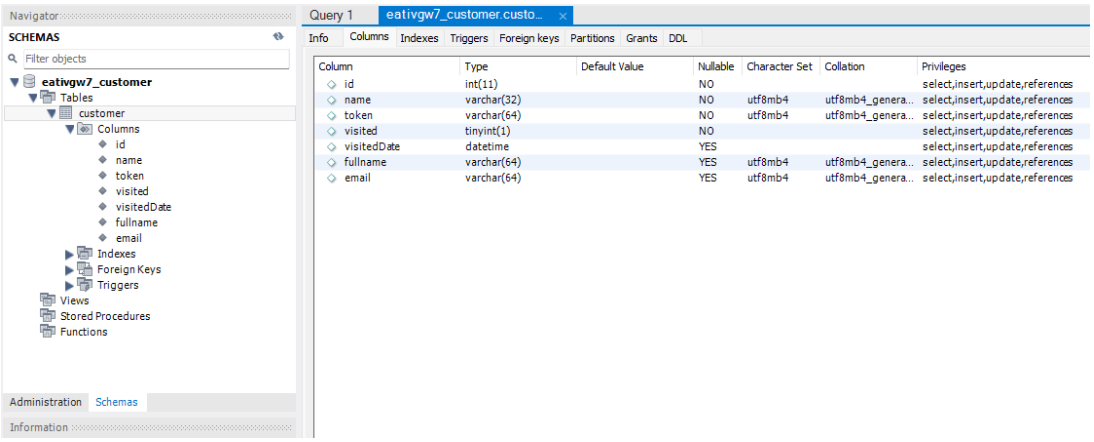


Figura 11

MySQL



5.1.1.2.Lenguaje de Programación

Para el desarrollo de las herramientas de envió de link y recolección de los datos de ingeniería social se necesita una herramienta sencilla y amigable, la cual se plantean los siguientes lenguajes de programación:

Para la generación y envío automatizado de enlaces de ingeniería social a través de WhatsApp, Python sería un excelente lenguaje de programación, cuenta con librerías y herramientas robustas para la automatización de tareas, como el envío de mensajes y archivos a través de la API de WhatsApp. Con Python, se desarrolló scripts y programas que simulen de forma eficiente el envío masivo de enlaces maliciosos a través de WhatsApp, lo cual es clave para la investigación. Python tiene una sintaxis clara y legible, lo que facilitaría el desarrollo y mantenimiento de la simulación. Además, Python cuenta con una amplia comunidad y ecosistema, lo que te permitiría encontrar recursos, bibliotecas y ejemplos que aceleren el desarrollo del proyecto de investigación ver (Anexo A).

Para la creación de un formulario web que reciba la información recopilada durante los ataques de ingeniería social, PHP es una excelente opción.es un lenguaje ampliamente utilizado y aceptado para el desarrollo de aplicaciones web, lo que te permitiría crear un formulario robusto y escalable. Se podría integrar fácilmente el formulario web con una base de datos para almacenar y procesar los datos recopilados durante la simulación de los ataques. Tiene una curva de aprendizaje relativamente sencilla, lo que facilitaría el desarrollo del formulario y su integración con el resto del proyecto Ver (Anexo B, Anexo C, Anexo D).

Código Fuente Python Anexo A

A continuación, una descripción de cada línea de código:

- `import webbrowser as web`: Esta línea importa el módulo `webbrowser` y lo asigna a la variable `web`. Este módulo permite abrir un navegador web desde el programa.
- `import pandas as pd`: Esta línea importa el módulo `pandas`, que es una biblioteca muy utilizada para el manejo y análisis de datos. Se le asigna el alias `pd`.
- `import pyautogui as pg`: Esta línea importa el módulo `pyautogui`, que permite controlar el mouse y el teclado de forma programática.

- `import time`: Esta línea importa el módulo `time`, que proporciona funciones para trabajar con el tiempo, como pausar la ejecución del programa.
- `path = 'C:\\Users\\Karol NG\\Desktop\\Karol\\PUCE\\Titulación\\Telefonos.xlsx'`: Esta línea define la ruta del archivo Excel que contiene los datos que se utilizarán.
- `data = pd.read_excel(path, sheet_name= "Hoja1")`: Esta línea lee el archivo Excel especificado en la variable `path` y lo carga en la variable `data`. Se indica que la hoja de cálculo a leer es "Hoja1".
- Líneas 9-13: Estas líneas se encuentran dentro de un bucle `for` que recorre cada fila del archivo Excel.
- `celular = data.loc[i, "Cel"].astype(str)`: Esta línea obtiene el valor de la columna "Cel" (celular) de la fila actual y lo convierte a una cadena de texto.
- `nombre = data.loc[i, "Nombre"]`: Esta línea obtiene el valor de la columna "Nombre" de la fila actual.
- `token = data.loc[i, "Token"].astype(str)`: Esta línea obtiene el valor de la columna "Token" de la fila actual y lo convierte a una cadena de texto.
- `urlbase = "https://giftcard.meventos.ec/?token="`: Esta línea define la URL base que se utilizará para abrir el navegador.
- Lineas 15-21: Estas líneas construyen el mensaje de WhatsApp que se enviará.
- `web.open("https://web.whatsapp.com/send?phone=" + celular +"&text="+ mensaje)`: Esta línea abre el navegador web y carga la URL de WhatsApp con el número de teléfono y el mensaje a enviar.
- `time.sleep(8)`: Esta línea detiene la ejecución del programa durante 8 segundos.
- `time.sleep(1)`: Esta línea detiene la ejecución del programa durante 1 segundo.
- `pg.click(1800, 954)`: Esta línea simula un clic del mouse en las coordenadas (1800, 954) de la pantalla.
- `time.sleep(1.5)`: Esta línea detiene la ejecución del programa durante 1.5 segundos.
- `pg.hotkey("ctrl", "w")`: Esta línea simula la combinación de teclas Ctrl+W, que cierra la pestaña del navegador.
- `time.sleep(1)`: Esta línea detiene la ejecución del programa durante 1 segundo.

Código Php (Anexo B, Anexo C, Anexo D, Anexo E, Anexo F)

Código Index.php Anexo B

- `$request = $_SERVER['REQUEST_URI'];`: Esta línea obtiene la URI (Identificador de Recursos Uniforme) de la solicitud actual del usuario. Esto incluye la ruta y los parámetros de consulta.
- `$path = parse_url($request, PHP_URL_PATH);`: Esta línea utiliza la función `parse_url()` para extraer solo la ruta de la URI de la solicitud. Esto se almacena en la variable `$path`.
- `$viewDir = '/public/views/';`: Esta línea define la ruta relativa al directorio donde se encuentran los archivos de vista (como archivos HTML o PHP).
- Lineas 5-14: Estas líneas contienen una declaración `switch` que maneja diferentes rutas de solicitud.
- Líneas 7-9: Si la ruta es vacía (`"`) o la raíz (`'/'`), se carga el archivo `index.html` ubicado en el directorio de vistas.
- Líneas 11-12: Si la ruta es `/fail`, se carga el archivo `myfail.html` ubicado en el directorio de vistas.
- 14-16: Si la ruta no coincide con ninguno de los casos anteriores, se establece el código de respuesta HTTP a 404 (No encontrado) y se carga el archivo `404.php` ubicado en el directorio de vistas.

Este código PHP está manejando las solicitudes del usuario y redirigiendo a diferentes archivos de vista (HTML o PHP) según la ruta solicitada. El objetivo es tener una estructura organizada y flexible para manejar las diferentes páginas de la aplicación.

Código Index.html (Anexo C)

A continuación, una explicación detallada de cada una de las secciones y líneas de código del archivo HTML proporcionado:

- `<!DOCTYPE html>`: Declara que este documento es un documento HTML5.
- `<html lang="es">`: Expresa que el idioma principal del documento es español.
- `<head>`: Contiene la información de metadatos y recursos externos del documento.

- `<body>`: Contiene el los detalles visibles de la página web.
- `<header>`: Contiene el logotipo y el botón "Reclama tu GIFTCARD".
- `<img>`: Muestra el logotipo de la campaña.
- `<button>`: Crea un botón que abre el modal cuando se hace clic en él.
- `<div class="container">`: Envuelve el contenido principal de la página.
- `<div class="fondo-div">`: Contiene el valor de la GiftCard.
- `<p class="note">`: Muestra notas informativas sobre la campaña.
- `<button class="b-gift">`: Crea otro botón que abre el modal cuando se hace clic en él.
- `<div class="modal" id="myModal">`: Crea el modal, que es un cuadro de diálogo emergente.
- `<div class="modal-header">`: Contiene el título y el botón de cierre del modal.
- `<div class="modal-body">`: Contiene el formulario para ingresar información.
- `<form id="giftCardForm">`: Crea el formulario para que el usuario ingrese su nombre y correo electrónico.
- `<script>`: Contiene funciones JavaScript para: Obtener el token de la URL, Enviar el token al servidor para actualizar la base de datos, Obtener los datos del formulario, Enviar los datos del formulario al servidor PHP para actualizar la base de datos, `<script>`: Contiene un controlador de eventos para el formulario, que evita el envío del formulario, actualiza los datos en la base de datos y redirige al usuario a la página "fail".

Este código HTML crea una página web con un header, un contenido principal y un modal. El modal contiene un formulario que recopila información del usuario y la envía al servidor para actualizarla en la base de datos. El JavaScript en la página se encomienda de manejar la lógica de la aplicación.

Figura 12

Página web

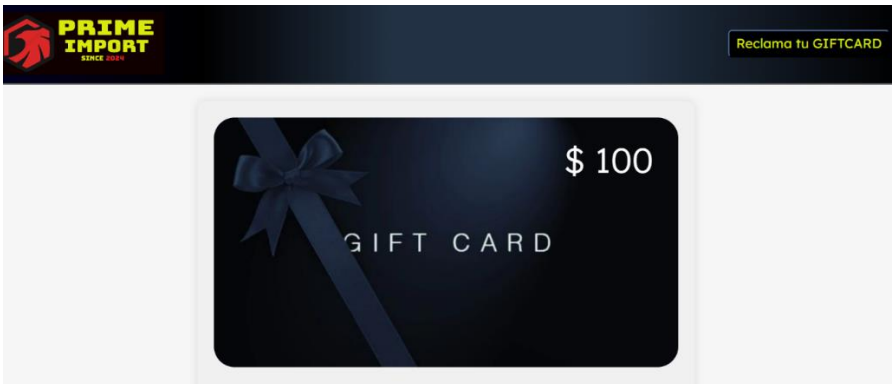
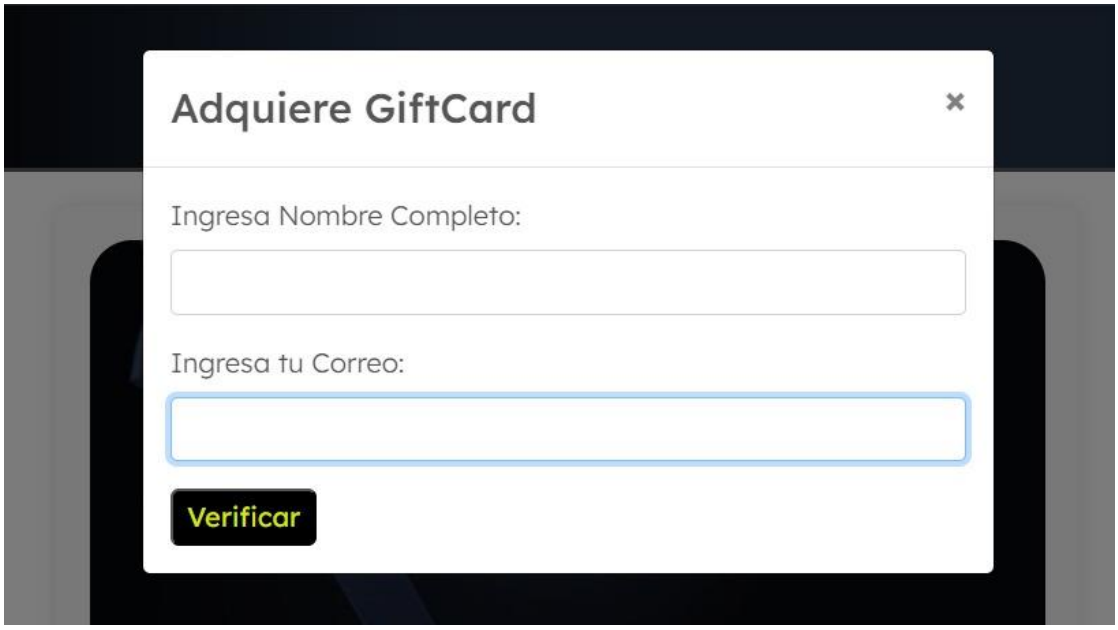


Figura 13

Modal



Código connection.php (Anexo D)

El siguiente código permite la conexión a la base de datos MYSQL:

- `$servername = "XXX.XXX.XXX.XXX";`: Define el nombre del servidor de la base de datos.

- `$username = "xxxxxxxxxx";`: Define el nombre de usuario de la base de datos.
- `$password = "xxxxxxxxxx";`: Define la contraseña de la base de datos.
- `$database = "xxxxxxxxxx";`: Define el nombre de la base de datos a la que se va a conectar.
- `$conn = new mysqli($servername, $username, $password, $database);`: Crea una nueva conexión a la base de datos utilizando los parámetros de configuración definidos anteriormente.
- `if ($conn->connect_error) { ... }`: Verifica si la conexión a la base de datos fue exitosa. Si hubo algun error, se visualiza el mensaje de error y termina la ejecución del script.

Este código PHP establece la conexión a una base de datos MySQL utilizando los datos de configuración proporcionados. Es una buena práctica tener estos datos en un archivo de configuración separado para mantener la seguridad y la portabilidad del código.

Cuando la conexión se establece correctamente, el código está listo para realizar operaciones en la base de datos, como insertar, actualizar, eliminar o consultar datos. Normalmente, este código de conexión se incluiría en otros archivos PHP que contengan las funciones y consultas específicas para interactuar con la base de datos.

Código register.php (Anexo E)

- `require_once('./connection.php');`: Esta incluye el archivo `connection.php`, que coge la configuración de conexión a la base de datos.
- `global $conn;`: Esta línea hace que la variable `$conn` (que se definió en el archivo `connection.php`) esté disponible en el ámbito global de este script.
- `$token = $_POST['token'];`: Esta línea obtiene el valor del parámetro `token` enviado a través de una solicitud POST.
- `$sql = "UPDATE customer SET visitedDate = NOW(), visited = 1 WHERE token = '$token'";`: Esta línea construye la consulta SQL para actualizar la tabla `customer`. Establece el campo `visitedDate` a la fecha y hora actual y el campo `visited` a 1 (verdadero), donde el valor de `token` coincida con el valor recibido.
- Lineas 8-12: Estas líneas ejecutan la consulta SQL y manejan el resultado:

- `if ($conn->query($sql) === TRUE) { ... }`: Verifica si la consulta se ejecutó correctamente. Si es así, imprime un mensaje de éxito.
- `else { ... }`: Si hubo un error, imprime el mensaje de error.
- `$conn->close();`: Esta línea cierra la conexión de la data.

Este código PHP recibe un token a través de una solicitud POST, actualiza un registro en la tabla `customer` de la base de datos para marcar que ese token ha sido visitado, y luego cierra la conexión a la base de datos. El objetivo de este script es registrar el uso de un token o código de regalo en la base de datos del sistema.

Código register.php (Anexo F)

- `require_once('./connection.php');`: Esta línea incluye el archivo `connection.php`, que contiene la configuración de conexión a la base de datos.
- `global $conn;`: Esta línea hace que la variable `$conn` (que se definió en el archivo `connection.php`) esté disponible en el ámbito global de este script.
- Líneas 4-6: Estas líneas obtienen los datos enviados a través de una solicitud POST:
- `$token = $_POST['token'];`: Obtiene el valor del parámetro `token` de la solicitud.
- `$fullName = $_POST['fullName'];`: Obtiene el valor del parámetro `fullName` de la solicitud.
- `$email = $_POST['email'];`: Obtiene el valor del parámetro `email` de la solicitud.
- `$sql = "UPDATE customer SET fullName = '$fullName', email = '$email' WHERE token = '$token'";`: Esta línea construye la consulta SQL para actualizar la tabla `customer`. Establece los campos `fullName` y `email` con los valores recibidos, donde el valor de `token` coincida con el valor recibido.
- Lineas 10-14: Estas líneas ejecutan la consulta SQL y manejan el resultado:
- `if ($conn->query($sql) === TRUE) { ... }`: Verifica si la consulta se ejecutó correctamente. Si es así, imprime un mensaje de éxito.
- `else { ... }`: Si hubo un error, imprime el mensaje de error.
- `$conn->close();`: Esta línea cierra la conexión a la data.

En resumen, este código PHP recibe un token, un nombre completo y un correo electrónico a través de una solicitud POST, y actualiza un registro en la tabla `customer` de la base de datos con esos datos. Luego, cierra la conexión a la base de datos. El objetivo de este script es actualizar la información del usuario asociada a un token o código de regalo en la base de datos del sistema.

Código myfail.html (Anexo G)

- `<!DOCTYPE html>`: Declara que este documento es un documento HTML5.
- `<html lang="es">`: Indica que el idioma principal del documento es español.
- `<head>`: Contiene la información de metadatos y los estilos CSS del documento.
- `<body>`: Contiene el datos visible de la página web.
- `body { ... }`: Define el estilo del cuerpo de la página, incluyendo la fuente, el color de fondo y el alineamiento del texto.
- `h1 { ... }`: Define el estilo del encabezado principal.
- `p { ... }`: Define el estilo de los párrafos.
- `.warning { ... }`: Define el estilo de los elementos con la clase "warning".
- `.tips { ... }`: Define el estilo de la sección de consejos.
- `ul { ... }`: Define el estilo de la lista de consejos.
- `li { ... }`: Define el estilo de los elementos de la lista.
- `<h1>`: Muestra el título principal de la página.
- `<p class="warning">`: Muestra un mensaje de advertencia en rojo.
- `<p>`: Muestra un párrafo introductorio.
- `<div class="tips">`: Contiene la sección de consejos.
- `<ul>`: Crea una lista con los consejos.
- `<li>`: Muestra cada uno de los consejos.

Este código HTML crea una página web sencilla que tiene como objetivo concientizar a los usuarios sobre la importancia de la seguridad de los datos personales. El diseño utiliza una paleta de colores clara y un estilo minimalista para enfocar la atención en los mensajes clave.

Los estilos CSS definen el aspecto visual de la página, como el tipo de fuente, los colores, el espaciado y el alineamiento del contenido. La sección de "consejos" se presenta de manera resaltada dentro de un cuadro con sombra para llamar la atención del usuario.

En general, este código HTML y CSS crea una página web informativa y de fácil lectura, que puede ser utilizada para adiestrar a los usuarios sobre las mejores prácticas de seguridad de datos.

Figura 14

Página Web

5.1.1.3.Métodos y Técnicas de Ingeniería Social

Gracias a las investigaciones previas se pudo seleccionar el método SMISHING como método de ingeniería social a aplicar, por el cual los cumplimientos de las metas serian óptimos.

El método de Smishing, que se basa en el envío de mensajes de texto o WhatsApp engañosos para obtener información personal o causar daños, se ha vuelto cada vez más relevante en los últimos años. Esto se debe a varios factores:

- Ubicuidad de los Smartphone: La mayoría de las personas, incluyendo estudiantes, utilizan constantemente sus teléfonos móviles, lo que los hace vulnerables a este tipo de ataques a través de mensajes de texto.

- Eficacia del Smishing: Los atacantes aprovechan la tendencia de las personas a confiar más en los mensajes que en otros canales digitales, lo que aumenta la eficacia de los ataques de Smishing.

- Facilidad de ejecución: Desde la perspectiva de los atacantes, el Smishing es relativamente sencillo de implementar en comparación con otros métodos de ingeniería social, lo que lo convierte en una amenaza cada vez más presente.

Importancia de concientizar a los estudiantes y Usuarios de WhatsApp:

La concientización de los usuarios sobre los riesgos del Smishing es fundamental por varias razones:

- Población vulnerable: Los estudiantes, al ser usuarios jóvenes y con mayor familiaridad con la tecnología, pueden ser un blanco atractivo para los ciberdelincuentes que utilizan este método.

- Impacto a largo plazo: Educar a los estudiantes sobre el Smishing les brindará herramientas para reconocer y evitar este tipo de ataques, lo que les ayudará a protegerse a lo largo de sus carreras y vidas profesionales.

- Efecto multiplicador: Al concientizar a los estudiantes, ellos pueden convertirse en agentes de cambio, compartiendo sus conocimientos y promoviendo una cultura de seguridad digital entre sus compañeros, familiares y comunidad.

5.1.2. Tipo de Mensajes para obtener la información

Existen diferentes tipos de mensajes que se pueden utilizar para transmitir un engaño a los usuarios de WhatsApp, aquí se presentan algunos tipos de mensajes que se pueden utilizar en el método de ingeniería social a través de WhatsApp:

5.1.2.1.Mensajes de urgencia o emergencia:

- "Hola, necesito tu ayuda de inmediato. Es una situación de emergencia."
- "Disculpa, tengo una urgencia y necesito que me hagas un favor rápido."

5.1.2.2.Mensajes de supuesta amistad o familiaridad:

- "Hola, soy [nombre], tu viejo amigo del colegio. ¿Cómo has estado?"
- "Hola [nombre], soy [nombre], tu primo. ¿Tienes un momento para hablar?"

5.1.2.3.Mensajes de supuesta autoridad o cargo:

- "Soy [cargo] de la empresa y necesito que me proporciones algunos datos de manera urgente."

- "Hola, soy [nombre] de [empresa/organización] y tengo una solicitud importante para ti."

5.1.2.4.Mensajes con engaños o pretextos:

- "Hola, soy de [empresa] y tenemos un problema con tu cuenta. Necesito que me proporciones algunos datos."
- "Disculpa, se ha producido un error en nuestro sistema y necesitamos que verifiques algunos detalles."

5.1.2.5.Mensajes Promocionales o de Premios

- Por tiempo limitado, ofrecemos un 20% de descuento en nuestra suscripción anual y acceso gratuito a nuestras guías de capacitación
- Felicitaciones tenemos el placer de comunicarte que has ganado un bono de [Valor], para la compra en línea de [Mercadería].

Para esta investigación se seleccionó el mensaje de tipo Promocional o de premios, la cual gracias a la encuesta se pudo comprobar las marcas más utilizadas por los usuarios y se aplicó el siguiente mensaje personalizado.

Figura 15

Mensaje de engaño

5.1.3. Análisis de los Resultados

En base a las tabulaciones de los resultados de la base de datos en la simulación de ataque de Ingeniería social resultó la siguiente tabla:

Tabla 13

Resultados Obtenidos

Población Objeto de estudio	Población que participo en el cuestionario	%	Población que no participo en el cuestionario	%	Población que visito la página	%	Población que Ingreso los datos del Fraude	%
200	164	82. %	36	18 %	20	10 %	6	3 %

Figura 16 Resultados Obtenidos

Con base en los resultados de las tabulaciones proporcionadas, se puede realizar el siguiente análisis:

5.1.3.1.Población objeto de estudio:

- La población objeto de estudio es de 200 personas.

5.1.3.2.Participación en el cuestionario:

- 164 personas (82%) participaron en el cuestionario.
- 36 personas (18%) no participaron en el cuestionario.

5.1.3.3.Visitas a la página web:

- 20 personas (10%) visitaron la página web.
- 180 personas (90%) no visitaron la página web.

5.1.3.4.Ingreso de datos sobre fraude:

- *6 personas (3%) ingresaron datos sobre fraude en la página web.*
- *194 personas (97%) no ingresaron datos sobre fraude.*

5.1.3.5.Análisis general

La participación en el cuestionario fue alta, con un 82% de la población objeto de estudio respondiendo. No obstante, solo el 10% de la población visitó la página web, lo que indica que la mayoría de las personas no interactuaron con la herramienta en línea. Esto puede deberse a diversas razones, como desconfianza hacia los enlaces web o falta de empatía hacia este tipo de comunicaciones. Por otro lado, el hecho de que solo el 3% de la población objeto de estudio ingresó datos sobre fraude en la página web debe verse como un resultado positivo. Esto sugiere que solo una pequeña minoría de la población es propensa a este tipo de ataques de ingeniería social y, por lo tanto, es susceptible de caer víctima de fraudes. Este bajo porcentaje refleja que la gran mayoría de la población tiene conciencia y habilidades para evitar ser víctimas de este tipo de delitos.

Sin embargo, aún es importante analizar las razones por las cuales la mayoría de la población no visitó la página web. Esto permitiría identificar oportunidades de mejora, como simplificar el proceso, aumentar la promoción y visibilidad de la herramienta, o desarrollar estrategias complementarias para fomentar la participación y la recopilación de información relevante sobre fraude, sin comprometer la seguridad de los usuarios.

Conclusiones

El análisis de los datos recopilados a través de las encuestas realizadas permitió identificar patrones de comportamiento y preferencias de los usuarios en el uso de redes sociales. La información obtenida en las encuestas reveló vulnerabilidades clave en el uso de la aplicación WhatsApp por parte de los participantes, lo que facilitó el diseño y la implementación de la simulación del ataque de ingeniería social. Los hallazgos de las encuestas proporcionaron valiosos insumos para comprender mejor las áreas de riesgo y los puntos débiles en el manejo de la seguridad por parte de los usuarios en el entorno digital.

La ejecución del plan de simulación del ataque de ingeniería social en WhatsApp permitió concientizar a los usuarios sobre las tácticas y técnicas empleadas por los atacantes para engañar y manipular a las víctimas. La exposición de los usuarios a este escenario simulado les brindó la oportunidad de comprender en primera persona los mecanismos utilizados por los ciberdelincuentes, lo que fomentó una mayor conciencia sobre la importancia del buen uso y la seguridad en la aplicación WhatsApp. La simulación demostró ser una herramienta efectiva para promover cambios en el comportamiento y las prácticas de los usuarios, motivándolos a adoptar medidas de seguridad más sólidas en el entorno de las redes sociales.

La simulación de ataques en WhatsApp y dispositivos móviles permitió evaluar la efectividad de los ataques y la facilidad de engaño en un grupo minoritario de la población objeto de estudio, revelando áreas de mejora clave. A partir de estos hallazgos, se proponen recomendaciones concretas para fortalecer la protección de los usuarios, como el refuerzo de los mecanismos de autenticación, la mejora de las opciones de privacidad, la implementación oportuna de actualizaciones de seguridad, el fortalecimiento de los sistemas de detección y respuesta a amenazas, y el desarrollo de campañas de concientización. Estas medidas buscan brindar a los usuarios un entorno más seguro y confiable al utilizar la aplicación de mensajería, garantizando la salvaguarda de su seguridad y privacidad en el ecosistema digital.

Recomendaciones

Realizar encuestas y estudios de campo periódicos para monitorear la evolución de los patrones de comportamiento y preferencias de los usuarios en el uso de redes sociales y aplicaciones como WhatsApp. También profundizar en el análisis de los datos recopilados a través de las encuestas, haciendo uso de técnicas de minería de datos y análisis de tendencias, con el fin de identificar vulnerabilidades emergentes. Establecer un sistema de alerta temprana que permita detectar y anticipar posibles cambios en las prácticas de los usuarios que puedan incrementar los riesgos de seguridad.

Incorporar la simulación de ataques de ingeniería social en programas de capacitación y sensibilización dirigidos a los usuarios de WhatsApp y otras redes sociales. También se puede desarrollar materiales educativos, como guías, infográficos y video tutoriales, que permitan a los usuarios comprender de manera práctica las tácticas utilizadas por los atacantes y cómo protegerse. El promover la participación activa de los usuarios en los procesos de simulación, fomentando su involucramiento y retroalimentación para mejorar la efectividad de las actividades de concientización.

Realizar evaluaciones periódicas de las políticas de seguridad implementadas por WhatsApp y los fabricantes de dispositivos móviles, a través de la simulación de ataques. Establecer un canal de comunicación y colaboración constante entre los investigadores, los proveedores de servicios y las autoridades competentes, con el fin de identificar y atender de manera oportuna las áreas de mejora en materia de seguridad. Proponer e impulsar la adopción de nuevas medidas de seguridad, como el fortalecimiento de los mecanismos de autenticación, el cifrado de extremo a extremo y la implementación de soluciones de detección y respuesta a incidentes.

Bibliografía

Galarza, C. R. (2020). *Los alcances de una investigación.* Santiago: CienciAmérica (2020) Vol. 9 (3).

Altamiro, V. (2018). *Recursos para la gestión de la comunicación online.* Tenerife: Universidad de Vigo.

Benavides , E., Fuertes , W., & Sánchez , S. (2020). *Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura.* Quito: Universidad de las Fuerzas Armadas.

Camino Ruiz, E. S. (2020). *Análisis y evaluación de la seguridad en la red de la Unidad Educativa Salesiana Cardenal Spellman, utilizando herramientas de Ingeniería social, y recomendar medidas preventivas.* Quito: Universidad Politécnica Salesiana.

Capacho Portilla, J. R., & Nieto Bernal, W. (2017). *Diseño de base de datos.* Barranquilla: Universidad del Norte.

Castellanos-Portela, J. A., & Carvajal-Rodríguez, H. D. (2019). *Ataque controlado de ingeniería social usando códigos QR.* Bogota: Universidad Católica de colombia.

Cervantes Rosas, C. M., & Alvites-Huamaní, C. G. (2021). *WhatsApp como recurso educativo y tecnológico en la educación.* Hamut´ay: Universidad César Vallejo.

Conde Mendoza, J. P. (2021). *Concientización en Ciberseguridad a través de ataques de ingeniería social.* La paz: Universidad Mayor de San Andrés.

Fernández Peña, F. O., & Jinde Sisa, A. H. (2024). *Estrategia para mitigar fraudes de angler-phishing basados en ingeniería social en plataformas de redes sociales.* Ambato: Universidad Técnica de Ambato.

Fernández Robles, B., & Marín Díaz, V. (2017). *Dispositivos móviles y realidad aumentada en el aprendizaje del alumnado universitario.* Sevilla: Universidad de Sevilla.

Fontecilla, H. B. (2021). *El impacto de las redes sociales en las personas y en la sociedad: redes sociales, redil social, ¿o telaraña?* Madrid: Universidad Autónoma de Madrid.

Institute, L. (23 de 05 de 2024). Obtenido de https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

Linares, v. (22 de 05 de 2024). Obtenido de https://es.scribd.com/document/523921014/Cuadro-Comparativo-Lenguajes-de-Programación

López Bonilla, E. (2024). *Interacción en redes sociales y comunicación oral-escrita de estudiantes-docentes de la escuela de turismo de la Universidad Autónoma de Chiriquí, 2023.* Chiriqui: Universidad Autonoma de Chiriqui.

Neri Ayala, A. C., Ramos y Yovera, S. E., & Caro Soto, F. G. (2020). *Herramientas google en el aprendizaje de matemática financiera en los estudiantes universitarios.* Lima: Universidad Nacional José Faustino Sánchez Carrión.

Restrepo, H. A. (2023). *Comercio electrónico: Importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra online y en redes sociales en Colombia.* Medellin: Universidad Nacional Abierta y a Distancia UNAD.

Rodríguez Rincon, E. Y. (2018). *Metodologías de ingeniería social.* Catalunya: Universidad Oberta de Ctalunya.

Rubio Romero, J., & Lamo de Espinosa, M. P. (2015). *El fenómeno WhatsApp en el contexto de la comunicación personal: una aproximación a través de los jóvenes universitarios.* Madrid: Universidad Antonio de Nebrija.

Santa Cruz, H., & Hermoza, M. (2019). *Los delitos informáticos y su tipificación en la legislación penal Ecuatoriana.* Ibarra: Pontificia Universidad Católica del Ecuador.

Slideshare. (22 de 05 de 2024). *Slideshare*. Obtenido de https://es.slideshare.net/JonathanAdielEhuanPe/cuadro-comparativo-de-las-bases-de-datospdf

Tascon, M., & Quintana, Y. (2018). *Ciberactivismo: Las nuevas revoluciones de las multitudes conectadas.* Madrid: Los Libros de la Catarata 2012.

Tejada Garitano, E., & Castaño Garrido, C. M. (2019). *Los hábitos de uso en las redes sociales de los preadolescentes.* Leioa: Universidad del País Vasco.

Vallejo Rodriguez, F. W. (2020). *Desarrollo de un simulador web aplicando las normas ISO/IEC 27002 enfocado en la ingeniería Social*. Ibarra: Universidad Técnica del Norte.

Anexos

Anexo A Código Fuente Python Envió WhatsApp

```
import webbrowser as web

import pandas as pd

import pyautogui as pg

import time

path = 'C:\\Users\\Karol NG\\Desktop\\Karol\\PUCE\\Titulación\\Telefonos.xlsx'

data = pd.read_excel(path, sheet_name= "Hoja1")

for i in range(len(data)):

    celular = data.loc[i, "Cel"].astype(str)

    nombre = data.loc[i, "Nombre"]

    token = data.loc[i, "Token"].astype(str)

    urlbase = "https://giftcard.meventos.ec/?token="

    mensaje = (

    "🎉 Hola " + nombre + " 🎉\n"

    "Prime Import tiene una gran noticia para ti: ¡Has ganado una GiftCard de 💵 $100 💵! 🎁\n"

    "Las marcas donde puedes usar tu premio son:\n"

    "👟 Adidas\n"

    "👔 Tommy Hilfiger\n"

    "👟 Nike\n"

    "%0a%0a"

    "Para reclamar tu premio, ingresa al siguiente enlace: " + urlbase + token + " 🔗"

     )

    web.open("https://web.whatsapp.com/send?phone=" + celular +"&text="+ mensaje)

    time.sleep(8)

    time.sleep(1)

    pg.click(1800, 954)

    time.sleep(1.5)

    pg.hotkey("ctrl", "w")

    time.sleep(1)
```

Anexo B Código Index.php

```
<?php

$request = $_SERVER['REQUEST_URI'];

$path = parse_url($request, PHP_URL_PATH);

$viewDir = '/public/views/';

switch ($path) {

    case '':

    case '/':

        require __DIR__ . $viewDir . 'index.html';

        break;

    case '/fail':

        require __DIR__ . $viewDir . 'myfail.html';

        break;

    default:

        http_response_code(404);

        require __DIR__ . $viewDir . '404.php';

}
```

Anexo C Código Index.html

```
<!DOCTYPE HTML>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Campaña de GiftCards</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
    <link rel="stylesheet" href="/public/styles/style.css">
</head>
<body>
<header>
    <img src="/public/assets/images/logo_.png" alt="Banner" class="banner-image">
   <button id="header-button" class="b-gif"  data-toggle="modal" data-target="#myModal">Reclama tu GIFTCARD</button>
</header>
<div class="container">
  <div class="fondo-div">
      <div class="gift-values">
          <div class="price-container">
             <p class="card-value">$ 100</p>
          </div>
      </div>
  </div>
    <p class="note">¡Importamos Estilo!</p>
    <p class="note">No te quedes sin tu GiftCard</p>
    <p class="note">La GiftCard es válida para marcas seleccionadas Addidas Tommy Hilfiger y Nike</p>
    <button class="b-gift" data-toggle="modal" data-target="#myModal">Reclama tu GIFTCARD</button>
    <p class="note">Nota: Para generar el token de la tarjeta de regalo, es posible que se requiera validar ciertos datos. ¡Asegúrate de proporcionar la información correcta!</p>
</div>
<!-- The Modal -->
<div class="modal" id="myModal">
```

```
  <div class="modal-dialog">
    <div class="modal-content">
      <!-- Modal Header -->
      <div class="modal-header">
        <h4 class="modal-title">Adquiere GiftCard</h4>
        <button type="button" class="close" data-dismiss="modal">&times;</button>
      </div>
      <!-- Modal Body -->
      <div class="modal-body">
        <form id="giftCardForm">
          <div class="form-group">
            <label for="nombre">Ingresa Nombre Completo:</label>
            <input type="text" class="form-control" id="fullName" required>
          </div>
          <div class="form-group">
            <label for="email">Ingresa tu Correo:</label>
            <input type="email" class="form-control" id="email" required>
          </div>
          <button type="submit" class="b-gift">Verificar</button>
        </form>
      </div>
    </div>
  </div>
</div>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.0/umd/popper.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.js"></script>
<script>
    // Función para obtener el valor del token de la URL
    function obtenerToken() {
        var urlActual = window.location.href;
        var url = new URL(urlActual);
```

```
        var params = new URLSearchParams(url.search);
        var token = params.get("token");
        return token;
    }
    // Obtener el token y asignarlo a una variable
    var tokenGanador = obtenerToken();
    // Mostrar el token en la consola para verificar
    console.log("El token del ganador es: " + tokenGanador);
    // Enviar el token al servidor para actualizar la base de datos
    function actualizarBaseDeDatos(token) {
        // Configurar la solicitud AJAX
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
            if (this.readyState === 4 && this.status === 200) {
                console.log("Respuesta del servidor:", this.responseText);
            }
        };
        xhttp.open("POST", "/database/register_visit.php", true);
        xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
        xhttp.send("token=" + token);
    }
    // Llamar a la función para actualizar la base de datos
    actualizarBaseDeDatos(tokenGanador);
</script>
<script>
    // Función para obtener los valores de los campos de formulario
    function obtenerDatosFormulario() {
        var fullName = document.getElementById("fullName").value;
        var email = document.getElementById("email").value;
        return { fullName: fullName, email: email };
    }
    // Enviar los datos al servidor PHP para actualizar la base de datos
```

```
    function actualizarDatos() {
        // Obtener los datos del formulario
        console.log("actualizando...");
        var datos = obtenerDatosFormulario();
        console.log("datos: " +datos.email)
        // Obtener el token de la URL
        var token = obtenerToken();
        console.log("token: " + token);
        // Configurar la solicitud AJAX
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
            if (this.readyState === 4 && this.status === 200) {
                console.log("Respuesta del servidor:", this.responseText);
            }
        };
        xhttp.open("POST", "/database/save_customer_data.php", true);
        xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
        xhttp.send("token=" + token + "&fullName=" + datos.fullName + "&email=" + datos.email);
    }
    // Controlador de eventos para el botón "Enviar"
    document.getElementById("giftCardForm").addEventListener("submit", function(event) {
        console.log("verificando...")
        event.preventDefault(); // Evitar el envío del formulario
        // Llamar a la función para actualizar los datos en la base de datos
        actualizarDatos();
        // Cerrar el modal después de enviar
        $('#myModal').modal('hide');
        window.location.href = "fail"
    });
</script>
</body>
</html>
```

Anexo D Código connection.php

```
<?php

// Configuración de conexión a la base de datos

$servername = "162.241.253.222";

$username = "eativgw7_myuser";

$password = "mypass12345678.";

$database = "eativgw7_customer";


$conn = new mysqli($servername, $username, $password, $database);


// Verificar la conexión

if ($conn->connect_error) {

    die("Conexión fallida: " . $conn->connect_error);

}
```

Anexo E Código register.php

```
<?php

require_once('./connection.php');

global $conn;

// Obtener el token de la solicitud POST

$token = $_POST['token'];

// Actualizar la base de datos

$sql = "UPDATE customer SET visitedDate = NOW(), visited = 1 WHERE token = '$token'";

if ($conn->query($sql) === TRUE) {

    echo "Registro actualizado correctamente";

} else {

    echo "Error al actualizar el registro: " . $conn->error;

}

// Cerrar la conexión

$conn->close();
```

Anexo F Código register.php

```
<?php

require_once('./connection.php');

global $conn;

// Obtener el token de la solicitud POST

$token = $_POST['token'];

// Actualizar la base de datos

$sql = "UPDATE customer SET visitedDate = NOW(), visited = 1 WHERE token = '$token'";

if ($conn->query($sql) === TRUE) {

    echo "Registro actualizado correctamente";

} else {

    echo "Error al actualizar el registro: " . $conn->error;

}

// Cerrar la conexión

$conn->close();
```

Anexo G Código myfail.html

```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Concientización sobre Seguridad de Datos</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            text-align: center;
            background-color: #f8f9fa;
            padding: 20px;
        }
        h1 {
            margin-top: 50px;
        }
        p {
            color: #6c757d;
            margin: 20px 0;
        }
        .warning {
            color: #dc3545;
            font-weight: bold;
        }
        .tips {
            text-align: left;
            display: inline-block;
            margin-top: 30px;
            padding: 20px;
            border: 1px solid #ddd;
            background-color: #ffffff;
```

```
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
        }
        ul {
            list-style-type: none;
            padding: 0;
        }
        li {
            margin-bottom: 10px;
        }
    </style>
</head>
<body>
    <h1>¡Protege tus Datos Personales!</h1>
    <p class="warning">¡Ten cuidado con los enlaces y formularios desconocidos!</p>
    <p>La seguridad de tu información personal es muy importante. Aquí tienes algunos consejos para evitar comprometer tus datos:</p>

    <div class="tips">
        <ul>
            <li><strong>No hagas clic en enlaces sospechosos:</strong> Antes de hacer clic en un enlace, asegúrate de que proviene de una fuente confiable.</li>
            <li><strong>Verifica la URL:</strong> Asegúrate de que la dirección web sea correcta y segura. Las URL seguras comienzan con "https://".</li>
            <li><strong>No ingreses datos personales en formularios desconocidos:</strong> Asegúrate de que el sitio web es legítimo antes de proporcionar información personal o financiera.</li>
            <li><strong>Usa contraseñas fuertes:</strong> Crea contraseñas que sean difíciles de adivinar y utiliza una combinación de letras, números y caracteres especiales.</li>
            <li><strong>Actualiza tu software de seguridad:</strong> Mantén tu antivirus y otros programas de seguridad actualizados para protegerte contra amenazas nuevas.</li>
        </ul>
    </div>
</body>
</html>
```