Pontificia Universidad Católica del Ecuador | Sede Ambato

ESCUELA DE INGENIERÍAS

Tema:

HERRAMIENTAS DE ATAQUES DE INGENIERÍA SOCIAL Y ESTRATEGIAS PARA SU PREVENCIÓN

Proyecto de investigación previo a la obtención del título de Ingeniera en Tecnologías de la Información

Líneas de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Autora:

Fátima Ariana Manzano Moscoso

Director:

Mg. Enrique Xavier Garcés Freire

Ambato – Ecuador

Agosto 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **FÁTIMA ARIANA MANZANO MOSCOSO**, con cédula de identidad. **1850182880**, autora del trabajo de graduación titulado: "HERRAMIENTAS DE ATAQUES DE INGENIERÍA SOCIAL Y ESTRATEGIAS PARA SU PREVENCIÓN", previa a la obtención del título profesional de **INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN**, en la escuela de **INGENIERÍAS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontifica Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, agosto 2024

Fátima Ariana Manzano Moscoso

CC. 1850182880

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

HERRAMIENTAS DE ATAQUES DE INGENIERÍA SOCIAL Y ESTRATEGIAS PARA SU PREVENCIÓN

Líneas de investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Autora:

Fátima Ariana Manzano Moscoso

Enrique Xavier Garcés Freire, Ing. Mg. f._____

CC. 1803226016

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____

CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____

DIRECTOR ESCUELA DE INGENIERÍAS

Ana Cecilia Parra Ramos, Ab. Mg. f._____

SECRETARIA GENERAL PUCESA (S)

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Agosto 2024

DEDICATORIA

Todo este proyecto, está dedicado a mis padres, quienes con esfuerzo todos los días, me dieron la mejor educación, y no descansaron hasta convertirme en profesional. Alex y Adriana, mis pilares fundamentales siempre, les quiero dedicar este pedacito de mi vida. Aquellas personas que estuvieron para mí en cada uno de los momentos más difíciles de este proceso, desde el principio hasta el final, mis amigos, mis hermanas, mi familia, mis profesores, que con palabras de aliento me permitieron todos los días convencerme de seguir adelante. A mi Max, que estuvo conmigo desde el primer día de clases de la universidad, acompañándome, hasta el último día en el que terminé este proyecto de titulación. Y a mi compañero de vida, mi pequeño gran amor Juan Di, que estuvo ahí para escucharme llorar, reír y frustrarme, siempre tuvo las palabras justas para poder darme ánimos y seguir.

AGRADECIMIENTO

Quiero agradecer principalmente a mis padres, Alex y Adriana, quienes fueron mi soporte, y mi más grande motivación para seguir adelante, a mis dos hermanitas, Estefanía y Sofía, mis pequeñas alegrías cuando ya no podía más. A mi tutor de este proyecto, Enrique Garcés, quien, me guío durante todo este proceso, desde el principio ha sido más que un mentor, un amigo a quién acudir.

A toda mi familia, mis abuelitos, mis tíos, por siempre estar ahí para darme un consejo, un abrazo, palabras de ánimo. A todos mis profesores, quienes hicieron que la universidad sea como un segundo hogar para mí. Por último, quisiera agradecer a todos mis amigos, aquellos que estuvieron desde el principio, y con quienes reí, y lloré muchas veces, gracias por no dejarme caer. Mi Kelly bella, que es como una hermana para mí, al Pitty, con quien muchas veces hablamos de dejar la carrera, pero hoy por fin la estamos terminando. Mi Juan Di, gracias por escucharme siempre, y por estar ahí cuando me desesperaba, y darme ánimos, para poder estar aquí. Muchas gracias.

RESUMEN

La investigación se centra en el estudio de las herramientas de ataques de ingeniería social y estrategias para su prevención en el contexto de las Tecnologías de la Información y Comunicación. La necesidad de este estudio surge de la creciente importancia de proteger la información personal y empresarial frente a las sofisticadas técnicas de ingeniería social utilizadas por ciberdelincuentes. El objetivo principal de la investigación es proporcionar una guía detallada y específica para los emprendedores del Servicio de Integración Laboral (SIL) de Tungurahua, con el fin de proteger sus datos y activos comerciales de posibles ataques.

La metodología empleada en este estudio combina enfoques cualitativos y cuantitativos, con la aplicación de la metodología Kanban para una gestión eficiente del proyecto. Se identifican las herramientas utilizadas en los ataques de ingeniería social, se realizan pruebas de ataques simulados en el grupo de emprendedores del SIL para recopilar datos relevantes y se proponen estrategias concretas para prevenir estos ataques. Se destaca la importancia de la educación y concientización de los usuarios, la implementación de políticas de seguridad y la difusión de los ataques más comunes como medidas clave para la prevención.

Los resultados obtenidos resaltan la efectividad de las estrategias propuestas para proteger a los emprendedores del SIL de Tungurahua de posibles ataques de ingeniería social. Se espera que este estudio no solo mejore la seguridad cibernética de este grupo vulnerable, sino que también sirva como modelo para futuras investigaciones en el campo de la prevención de amenazas cibernéticas.

Palabras clave: ingeniería social, ciberseguridad, emprendedores, prevención de ataques, concientización.

ABSTRACT

The research focuses on the study of social engineering attack tools and strategies for their prevention within the context of Information and Communication Technologies. The need for this study stems from the growing importance of safeguarding personal and business information against sophisticated social engineering techniques employed by cybercriminals. The primary objective of this research is to provide a detailed and specific guide for entrepreneurs affiliated with the Tungurahua Labor Integration Service (SIL), to protect their data and business assets from potential attacks.

The methodology used in this study integrates both qualitative and quantitative approaches, applying the Kanban methodology to ensure efficient project management. The tools used in social engineering attacks are identified, and simulated attack tests are conducted on the group of SIL entrepreneurs to collect relevant data.

The results underscore the effectiveness of the strategies proposed to protect Tungurahua's SIL entrepreneurs from possible social engineering attacks. It is anticipated that this study will not only enhance the cybersecurity of this vulnerable group, but also serve as a model for future research in the field of cyber threat prevention.

Keywords: *social engineering, cybersecurity, entrepreneurs, attack prevention, awareness.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

INTRODUCCIÓN

La era digital contemporánea ha cambiado profundamente la forma en que se interactúa con la información y entre las personas. La omnipresencia de la tecnología ha traído consigo una serie de beneficios, pero también ha generado nuevos desafíos, especialmente en lo que respecta a la seguridad cibernética. En este contexto, la ingeniería social ha surgido como una herramienta poderosa y peligrosa en manos de actores malintencionados que buscan comprometer la integridad de los sistemas y la privacidad de los individuos. Este estudio se sumerge en el mundo de la ingeniería social, explorando sus diversas herramientas y estrategias para prevenir y mitigar los riesgos asociados, con un enfoque particular en el ámbito empresarial de los emprendedores.

La ingeniería social, en el contexto de la seguridad cibernética, se refiere al uso de técnicas psicológicas y manipulativas para engañar a personas y obtener información confidencial o acceso a sistemas protegidos. Esta práctica no es nueva, pero ha evolucionado significativamente en la era digital, aprovechando la interconexión global y la abundancia de información personal en línea. Desde el clásico *phishing* hasta tácticas más sofisticadas como la suplantación de identidad, la ingeniería social representa una seria amenaza para la seguridad cibernética en todos los niveles, desde usuarios individuales hasta grandes corporaciones.

En la revisión de proyectos internacionales, se han realizado muchas investigaciones sobre la ingeniería social y su impacto en la seguridad cibernética. Según Anderson (2013) encontró que los ataques de ingeniería social costaron a las empresas de todo el mundo 2,7 billones de dólares en 2010. El estudio también encontró que los ataques de ingeniería social se están volviendo cada vez más sofisticados, lo que los hace más difíciles de detectar y prevenir.

En Ecuador, se han realizado algunas investigaciones sobre la ingeniería social y su impacto en la seguridad cibernética. El estudio de Hinojosa (2010) encontró que los ataques de *phishing* son los más comunes en el país. Las personas que tienen

más probabilidades de ser víctimas de ataques de ingeniería social son aquellas que tienen poca educación en seguridad cibernética.

Este caso práctico de Prado (2021) muestra cómo los ciberdelincuentes pueden utilizar la ingeniería social para robar información confidencial. El estudio propone una metodología para la generación y ejecución de campañas de ingeniería social.

Dentro de la situación problemática del actual panorama digital, los emprendedores están en una situación particularmente susceptible a los ataques de ingeniería social. Motivados por el deseo de expandir sus negocios en línea, estos individuos a menudo comparten una cantidad significativa de información personal y comercial en diversas plataformas, incluyendo redes sociales y sitios web. Esta práctica los expone a una serie de riesgos, desde el robo de identidad hasta extorsiones financieras, que pueden tener consecuencias devastadoras para sus empresas y su reputación.

La constante evolución de las herramientas de ingeniería social presenta un desafío adicional. Los métodos utilizados por los ciberdelincuentes se vuelven cada vez más comunes y difíciles de detectar, lo que hace casi imposible aún más la protección de los datos y la prevención de ataques.

El problema científico central que guía esta investigación radica en la necesidad de comprender en profundidad las herramientas de ingeniería social utilizadas en ciberataques, así como en el desarrollo de estrategias efectivas para prevenir y mitigar los riesgos asociados. La falta de un conocimiento integral sobre estas herramientas, combinada con la ausencia de estrategias de prevención sólidas, contribuye significativamente a la vulnerabilidad de los emprendedores y sus activos comerciales frente a las amenazas cibernéticas.

Como idea a defender este estudio busca llenar ese vacío de conocimiento al proporcionar una guía integral para los emprendedores del Servicio de Integración Laboral (SIL) de Tungurahua, les ayuda a protegerse de las amenazas de ingeniería social que enfrentan en su día a día.

Objetivo general: El objetivo general es analizar las herramientas de ataques de ingeniería social y desarrollar estrategias efectivas para su prevención en el contexto de los emprendedores del SIL de Tungurahua.

Objetivos específicos:

1.- Realizar un estado del arte sobre las herramientas utilizadas en ingeniería social y las estrategias para prevenir estos ataques.
2.- Pruebas similares de ataques de ingeniería social en el grupo de emprendedores del SIL de Tungurahua para recopilar datos relevantes.
3.- Proporcionar una guía detallada de estrategias para la prevención de ataques de ingeniería social dirigida específicamente a los emprendedores del SIL.

Este estudio se basa en la metodología Kanban, una metodología ágil ampliamente utilizada para gestionar y visualizar el flujo de trabajo en proyectos. Al aplicar esta metodología al estudio de los ataques de ingeniería social y las estrategias de prevención, esperamos obtener resultados claros y estructurados que faciliten la comprensión y la implementación de medidas preventivas. Su aplicación en el estudio de ataques de ingeniería social y estrategias para su prevención permitirá:

- Crear un tablero que represente las diferentes etapas de investigación, análisis y desarrollo de estrategias.
- Aplicar el principio *To do, Do*, y *Done*.
- Representar cada tarea como una tarjeta Kanban que incluya: revisión de la literatura, recopilación de datos, análisis de ataques de ingeniería social y desarrollo de estrategias.

La importancia de esta investigación radica en su contribución a la seguridad cibernética de los emprendedores del SIL de Tungurahua, un grupo vulnerable que enfrenta constantemente amenazas de ingeniería social. Al proporcionar una guía práctica y específica, este estudio tiene el potencial de proteger no solo los activos comerciales de estos emprendedores, sino también su privacidad personal en un entorno digital cada vez más peligroso.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Acercamiento teórico a la ingeniería social, técnicas y repercusiones

Hoy en día se puede definir a la Ingeniería Social, como un conjunto de técnicas de manipulación a individuos con el fin de obtener información confidencial, acceder a sistemas protegidos o inducir determinadas acciones. Grande y Guadrón (2015), mencionan que “El fin del atacante que aplica ingeniería social es el de explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, el atacante puede utilizar herramientas tecnológicas o incluso los encuentros cara a cara para obtener la información que necesita.” (pág. 02) A diferencia de los ataques informáticos que aprovechan vulnerabilidades técnicas, la ingeniería social se centra en explotar las debilidades humanas, como la confianza, la curiosidad o el miedo, para alcanzar sus objetivos.

El primer individuo en emplear el concepto de Ingeniería Social dentro del ámbito de la seguridad cibernética fue Kevin Mitnick, ampliamente reconocido como uno de los mejores expertos en *hacking* del mundo hasta la fecha. Grande y Guadrón (2015) afirman que:

> Mitnick sostiene que la Ingeniería Social implica la aplicación de tácticas por parte de los *hackers* con el propósito de engañar a un usuario autorizado de los sistemas informáticos de una empresa, con el fin de obtener información confidencial o inducir acciones que inadvertidamente generen vulnerabilidades de seguridad que puedan ser explotadas. (pág. 02)

Además de lo que indican los escritores, es importante mencionar que los ataques de Ingeniería Social han evolucionado, y hoy en día no se centran solamente en atacar empresas, si no, se ha expandido a la población en general que puede llegar a ser más vulnerable en este ámbito, más susceptible a manipulaciones y estafas en la red como los pequeños emprendedores y comerciantes que usan el internet como su principal medio de difusión.

> Según Sancho (2023), a pesar de que existen medidas de seguridad para prevenir los ataques de Ingeniería social, como la capacitación y la concientización sobre la importancia de proteger la información, muchos usuarios continúan siendo víctimas de estas tácticas. Esto puede deberse a la falta de conocimiento o a la falta de implementación de políticas de seguridad efectivas. (pág. 04)

Esto se debe específicamente a que hace falta mucha más difusión de las formas más comunes en las que la seguridad cibernética se ve afectada, y trata de concientizar a la población que sin importar el tipo de datos que sean subidos a la red, pueden resultar en su contra, hoy en día es muy común ver a pequeños emprendedores, compartir diferentes tipos de datos, ya no solo personales, sino que también bancarios y esto puede llevar a futuras estafas, extorsiones, o incluso suplantación de identidad

Técnicas de ingeniería social

Existen diferentes técnicas que usan los ciberdelincuentes según lo expuesto por Grande y Guadrón (2015):

- ***Baiting:*** esta técnica juega mucho con la psique humana. El atacante puede dejar un dispositivo que contenga un virus o *malware*, como una memoria USB, en algún área para que cualquier persona de la organización pueda encontrarla. La víctima seguramente la conectará a su computadora para revisar que pueda tener la memoria y en ese momento es cuando el *malware* puede ser inyectado al sistema.
- ***Phishing:*** los atacantes tratan de utilizar diferentes niveles de influencia a través de correos electrónicos que aparentan ser de una compañía legítima, como un banco, una institución de gobierno. Generar miedo a través de un correo electrónico, hace que la persona tome decisiones basadas en sus emociones más que en su sentido común.
- **IVR o *Phone Phishing:*** esta técnica utiliza una copia del sistema IVR (Respuesta de Voz Interactiva, por sus siglas en inglés) de un banco o

cualquier otra institución. La víctima es manipulada (por lo general, con un ataque de *phishing*) para que realice una llamada telefónica a un número gratuito para, por ejemplo, hacer una verificación de la información de su cuenta bancaria.

- ***Quid Pro Quo:*** esta técnica se basa en que el atacante promete algún beneficio a la víctima a cambio de información sensible de la organización o del mismo usuario. Por ejemplo, el atacante podría haber investigado alguna carencia sobre algún sistema de uso diario en la organización y puede llamar a un usuario haciéndose pasar por personal de soporte técnico para solventar ese problema, pero para hacerlo, le pide a cambio las credenciales de inicio de sesión a dicho sistema.
- ***Pretexting:*** el atacante muestra un buen pretexto o incluso, un buen escenario para poder robar información importante y sensible a la víctima, al contrario del *phishing* que lo que busca es generar miedo en la mayoría de los casos, el *pretexting* busca ganarse la confianza de la víctima.
- ***Farming:*** con esta técnica, el atacante busca crear una relación personal con la víctima, creando un entorno de confianza basado en la información que el atacante ha investigado de su objetivo, donde las principales fuentes de información son las redes sociales. (pág. 03)

Las técnicas que mencionan los autores se pueden usar de un sinfín de formas diferentes, y estas mismas pueden llegar a tener diferentes riegos como son el robo de información personal, pérdida de dinero, acceso a sistemas informáticos e incluso llegando al daño de la reputación de un individuo o empresa.

Repercusiones: Después de conocer las tácticas que los ciberdelincuentes utilizan, es apropiado conocer las repercusiones expuestas por Gómez (2017) de la Policía Nacional del Ecuador.

1. Manipulación psicológica de las personas para extraer información y así cometer un fraude por los ciber-delincuentes.

2. Aprovechamiento malicioso de la buena voluntad de las personas, para usarlos como puerta de ingreso para el robo de información.
3. Atraimiento de víctimas mediante publicidades a páginas web falsas y así robar su información y saldos de cuentas.
4. Engaño y la manipulación de usuarios a través del correo electrónico, llamadas telefónicas y las redes sociales para obtener información confidencial de personas o de la misma Institución Policial.

El autor resalta la manipulación y el engaño como principal repercusión que los ciberdelincuentes repercuten a la ciudadanía, además que es importante conocer que no solo pequeños emprendimientos, o medianas y grandes empresas pueden llegar a sufrir este tipo de ataques, sino que incluso la Policía Nacional no está libre de caer en algún tipo de estos ataques de seguridad cibernética.

> La pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital. En un lapso de tres meses, experimentamos una aceleración de la transformación digital que se había anticipado que ocurriría en tres años, según datos del Informe del Banco Interamericano de Desarrollo (2020). (pág. 28)

La era digital tuvo un salto enorme, avances significativos en muy poco tiempo, pero de igual forma, los peligros se hacen cada vez más grandes y sofisticados, como consumidores de todas las plataformas que existen en la red, se aprenderían que los datos personales de las personas, de empresas, de pequeños y grandes negocios, hoy en día corren mucho más riesgo de estafas, extorciones e incluso suplantación de identidades.

En la actualidad, la ingeniería social afecta notablemente a los pequeños emprendedores y negocios. A través de técnicas sofisticadas, como el *phishing* y la suplantación de identidad, los estafadores aprovechan la vulnerabilidad de aquellos con menos recursos y conocimientos en ciberseguridad. Esto crea un clima de desconfianza y riesgo para estas personas. Es esencial concienciar y educar a los

dueños de pequeños emprendimientos sobre las amenazas cibernéticas y la necesidad urgente de implementar medidas de protección adecuadas.

En Ecuador en los últimos años, los ataques a la seguridad cibernética han crecido de manera exponencial, como señala García (2022):

> Muestra un aumento alarmante de casos, escalando de 682 en 2020 a 1.852 en 2021, y continuando con 393 hasta la fecha en 2022 de la presente investigación. Este incremento se atribuye a la falta de cultura digital en el país, donde, aunque un alto porcentaje de la población (75.6%) utiliza internet, solo una pequeña fracción (10%) posee conocimientos digitales suficientes. (pág. 08)

Transgresiones habituales como la toma indebida y la usurpación de identidad, sancionadas por el Código Integral Penal (COIP) de Ecuador, indican la urgencia de una sensibilización y enseñanza más amplia en cuanto a la seguridad cibernética, puesto que es importante educar a la población en lo que se refiere a seguridad informática, cosas simples como cambiar contraseñas cada cierto tiempo, o no tener información muy personal a la vista y alcance de todo el mundo, son cosas básicas que todas las personas aplicaría en sus datos en línea.

1.2. Herramientas de *software* y físicas en ingeniería social

Existe un sinfín de herramientas que los ciberdelincuentes usan para realizar ingeniería social, anteriormente se expuso técnicas que se usan para realizar estos tipos de ataques, ahora se va a abordar las diferentes herramientas que se usa, siendo una de estas principales las redes sociales, existen varios riesgos al momento de exponer datos personales en internet, como los que exponen Paesani y Stucher (2017) que suceden en las redes sociales:

- Abrir los sitios para que cualquiera los pueda ver.
- Dar información personal. Subir fotografías, propias o ajenas, que reflejen situaciones de intimidad.

- Hacerse ‘amigos’ de gente que no conocen.
- Encontrarse en persona con ‘amigos’ que sólo conocieron en la Red. (pág. 77)

Se puso en práctica ataques cibernéticos usando ingeniería social en la facultad de ciencias administrativas de la universidad de Guayaquil, los resultados obtenidos por Urritia y Hernández (2022) mencionan que:

> Existe un mediano conocimiento sobre el manejo de la información personal frente a una encuesta, las personas utilizan como principal red social *facebook* por lo que ejecución del *phishing* fue efectiva en cuanto a la obtención de datos personales y claves de acceso, con la creación del punto de acceso falso se puedo obtener un número considerable de suscritores a la red permitiendo receptar paquetes con claves, datos personales y cuentas bancarias, la solución sería la capacitación y mejoramiento de políticas y procedimientos al momento de tratar la información institucional y personal. (pág. 15)

En la actualidad, la ingeniería social ha tenido un gran impacto en los pequeños emprendedores y negocios. Con la popularización de las redes sociales y el acceso a Internet, los estafadores han desarrollado formas cada vez más sofisticadas de engañar a personas y empresas menos protegidas. Desde correos electrónicos fraudulentos hasta intentos de robo de identidad, la ingeniería social ha creado un ambiente de desconfianza y vulnerabilidad para aquellos que no tienen los recursos o conocimientos necesarios en materia de ciberseguridad. Esto destaca la importancia urgente de educar a los pequeños empresarios sobre las amenazas cibernéticas y la necesidad de implementar medidas de seguridad para proteger sus operaciones comerciales.

Dentro del mundo de los ciberdelincuentes, se encuentran diferentes herramientas, de las que se habla a continuación son las que se usan para atacar el *software*, según la función que tenga, como por ejemplo para descifrar contraseñas García (2019) en su trabajo describe algunas, como son:

- ***John the Ripper:*** es una aplicación de *software* libre y código abierto para desencriptar contraseñas por fuerza bruta, para ello utiliza un diccionario de contraseñas, el cual se puede descargar por Internet o aprovechar el que incluye la propia aplicación. Para poder desencriptar la contraseña necesita que las diferentes partes de la contraseña pertenezcan al diccionario y para ello explota que gran parte de las contraseñas comparten una serie de palabras y características similares.
- ***Ophcrack:*** es una herramienta gratuita utilizada para crackear contraseñas de *Windows* usando *Rainbow tables*. Es una gran implementación del método *Rainbow tables* puesto que está hecho por los inventores de este. *Orphcrack* viene con una GUI y funciona en múltiples plataformas.
- ***Aircrack NG:*** es un kit completo de herramientas para conseguir acceso a redes *WiFi* con seguridad. Este se enfoca en cuatro áreas, el monitoreo de la red para capturar paquetes, ataque a base de inyección de paquetes, el testeo de la red y la parte final del crackeo para obtener la contraseña de acceso. (pág. 46)

El uso de herramientas informáticas diseñadas para descifrar contraseñas se vuelve esencial para los ingenieros sociales que buscan acceder a información confidencial protegida por contraseñas. Estos programas ofrecen una solución efectiva para superar las barreras de seguridad digital, permitiendo el acceso a datos protegidos de manera más rápida y eficiente. En el mercado actual, existe una variedad de opciones disponibles, cada una adaptada para diferentes necesidades y niveles de seguridad, lo que brinda a los usuarios la flexibilidad necesaria para lograr sus objetivos con éxito.

Hoy en día, el uso de *software* especializado para recopilar información se ha vuelto esencial en diversos ámbitos, desde la academia hasta el mundo empresarial. Estas herramientas son fundamentales para recolectar, organizar y analizar grandes cantidades de datos de manera eficiente y ordenada. Algunas de estas herramientas que expone Gil (2022) son:

- **Maltego:** Es una aplicación de inteligencia y análisis forense de código abierto. Algunos consideran a Maltego como una herramienta de inteligencia de código abierto. Ofrece una interfaz para minar y recopilar información en un formato fácil de entender. Junto con sus bibliotecas de gráficos, Maltego permite identificar relaciones clave entre información e identificar relaciones previamente desconocidas entre ellas. Maltego está desarrollado por Paterva y es utilizado por profesionales de seguridad e investigadores forenses para recopilar y analizar inteligencia de código abierto.
- ***Creepy:*** Se trata de una herramienta de geolocalización. Recopila información relacionada con posibles ubicaciones a través de diferentes redes sociales. Permite la extracción de información de cuentas como *Twitter, Flicklr, Facebook*, etc. Posteriormente representa esta información en un mapa y es posible exportarla a formatos CSV o KML para su posterior utilización.
- ***Harvester:*** Excelente herramienta para obtener información relacionada con el correo electrónico y el dominio. Este está incluido en Kali y puede ser muy útil para obtener información
- ***Recon-ng:*** Es una gran herramienta para la recopilación de información de destino. Está incluida en el repositorio de Kali. El poder de esta herramienta radica en el enfoque 59 modular y en que la información es recopilada en una base de datos, dándole un gran potencial. (pág. 58)

El uso de herramientas diseñadas específicamente para llevar a cabo ataques de *phishing* plantea una seria preocupación en el ámbito de la seguridad cibernética. Estos programas permiten a los ciberdelincuentes crear y enviar correos electrónicos fraudulentos en masa, con el propósito de engañar a los usuarios para que divulguen información sensible como contraseñas, datos financieros o detalles personales.

Con características avanzadas de personalización y suplantación de identidad, estos *softwares* hacen que los ataques sean más efectivos y difíciles de detectar para los sistemas de seguridad. La disponibilidad de tales herramientas en los

mercados clandestinos en línea destaca la necesidad de implementar medidas preventivas sólidas y educar a los usuarios sobre los peligros del *phishing* en internet.

Dentro de los motores de búsqueda más comunes y grandes de internet, tenemos Google, sin embargo, para poder buscar información mucho más específica, tenemos a Google Dorks, como lo dice García (2019) en su trabajo “son las búsquedas avanzadas que se pueden realizar mediante el famoso buscador Google que permiten obtener resultados sorprendentes por malas configuraciones o poco seguras de los diferentes *websites.* Estás búsquedas consisten en búsquedas estructuradas que encuentran resultados que en las búsquedas habituales no se encontrarían.”

Para comprender de mejor manera Gil (2022) desglosa diferentes tipos de *softwares* que son más comunes para realizar ataques de *phishing* como son:

- ***Social-Engineer Toolkit:*** El *Social-Engineer Toolkit* (SET) está diseñado específicamente para realizar ataques avanzados contra el ser humano. SET fue diseñado para ser lanzado con el lanzamiento de https://www.social-engineer.org y rápidamente se ha convertido en una herramienta estándar en un arsenal de probadores de penetración. SET fue escrito por David Kennedy y con mucha ayuda de la comunidad ha ido 60 incorporando ataques disponiendo de un conjunto de herramientas de explotación. Los ataques integrados en el kit de herramientas están diseñados para ser ataques dirigidos y enfocados contra una persona u organización utilizada durante una prueba de penetración.
- ***King Phisher:*** Es una de las herramientas de generación de campañas de *phishing* de código abierto más conocidas. King Phisher está escrito en *Python* y es una herramienta que se utiliza para simular ataques de *phishing* en el mundo real y para evaluar y promover la conciencia de la ciberseguridad y el phishing de una organización.
- ***Gophish:*** Es un simulador de *phishing* de código abierto escrito en GO, que ayuda a las organizaciones a evaluar la susceptibilidad a los ataques

de *phishing* al simplificar el proceso de creación, lanzamiento y revisión de los resultados de una campaña. *Gophish* ayuda en la creación de plantillas de correo electrónico, páginas de destino y listas de destinatarios, y ayuda al envío de perfiles. Permite lanzar campañas y generar y ver informes sobre aperturas de correo electrónico, clics en enlaces, credenciales enviadas y más

- ***WifiPhisher***: Una herramienta de *phishing* que tiene la capacidad de asociarse con una red *WiFi* cercana y obtener una posición de intermediario. Puede hacer esto de diferentes maneras: mediante la creación de una red inalámbrica falsa para imitar una legítima o mediante transmisión de identificador de conjunto de servicios o por sus siglas en inglés SSID que parecen familiares para los usuarios.
- ***HiddenEye:*** Es una herramienta todo en uno que presenta una funcionalidad interesante como *keylogge*r y rastreo de ubicación. También ofrece una serie de ataques diferentes, como *phishing*, recopilación de información, ingeniería social y otros. Es compatible con las principales redes sociales y sitios web comerciales como *Google, Facebook, Twitter, Instagram* y *LinkedIn*, y se pueden utilizar como vectores de ataque. Dispone de varias opciones de tunelización disponibles para lanzar campañas de *phishing*. (pág. 60)

Las herramientas físicas empleadas en ingeniería social son diversas y van desde dispositivos de espionaje como micrófonos ocultos y cámaras de vigilancia encubiertas hasta grabadoras de voz y dispositivos de seguimiento GPS. Estos instrumentos se utilizan discretamente para recopilar información confidencial o comprometedora, lo que facilita la manipulación o el engaño de individuos u organizaciones. En el trabajo de García (2019) expone diferentes herramientas que se suele usar como:

- **Ganzúas:** Son utensilios que se usan para abrir cerraduras y permitir acceso aquello que está protegido.
- **Cuchillo *shove:*** Es uno de los medios más rápidos para abrir puertas de casas y/o oficinas que utilizan una cerradura de pestillo en el pomo

- **Llaves *bumping:*** son unas llaves diseñadas para abrir cerraduras sin la necesidad de la llave de la cerradura. La llave *bumping* se introduce en la cerradura y mediante un golpe esta se adapta al diseño de la cerradura permitiéndole abrir la puerta sin forzarla. Está técnica es comúnmente usada por los cerrajeros, aunque recientemente han aumentado los robos de viviendas usando estas llaves. (pág. 42)

Las cámaras y dispositivos de grabación se han vuelto esenciales en la práctica de la ingeniería social, según Gil (2022) “Las cámaras pueden ser una herramienta útil para los ingenieros sociales cuando es necesario capturar información rápidamente” (pág. 55) puesto que permiten recopilar información de manera discreta y eficaz. Desde cámaras ocultas hasta grabadoras de voz camufladas en objetos cotidianos, estos dispositivos brindan la capacidad de capturar imágenes y sonidos de forma sigilosa durante las interacciones con personas o entornos específicos. Su uso puede ser variado, desde obtener pruebas concretas hasta recopilar información estratégica o documentar situaciones relevantes

1.3. Estrategias para la prevención de ataques de ingeniería social

Las malas prácticas cibernéticas son las principales causantes que exista mucha inseguridad cibernética, el desconocimiento de los usuarios los hace potencialmente víctimas de los ciberdelincuentes como comenta Fernández (2024):

> La capacitación del usuario final se enfoca en el factor de ciberseguridad más impredecible: las personas. Si no se siguen las buenas prácticas de seguridad, cualquier 6 individuo puede introducir accidentalmente un virus en un sistema que, de otra manera, sería seguro. Instruir a los usuarios sobre la eliminación de archivos adjuntos de correos electrónicos sospechosos, la precaución al conectar unidades USB no identificadas y otras lecciones fundamentales es esencial para la seguridad de cualquier organización. Este enfoque educativo contribuye significativamente a la prevención de amenazas y fortalece la conciencia de los usuarios en cuanto a la

> importancia de su papel en la protección de la ciberseguridad de la organización. (pág.22)

Para protegerse de manera efectiva contra la ingeniería social, especialmente en el caso de los pequeños emprendedores, es crucial implementar estrategias sólidas y prácticas de prevención. Estos pequeños emprendedores, a menudo carecen de los recursos y la experiencia necesarios en ciberseguridad, lo que los convierte en blancos fáciles para los estafadores que emplean tácticas de manipulación psicológica. Una estrategia fundamental implica educar y concienciar sobre las diversas formas de ingeniería social y cómo identificarlas.

Además, es esencial establecer políticas de seguridad claras y capacitar a los empleados para que puedan reconocer y reportar posibles amenazas. La implementación de medidas de autenticación multifactorial y el uso de herramientas de seguridad informática confiables también son pasos clave para fortalecer la defensa contra estos ataques cada vez más sofisticados.

Según comenta el autor Gil (2022) en su obra: “Una táctica defensiva comúnmente sugerida contra los ataques de ingeniería social es garantizar que todos los empleados reciban formación (obligatoria) para reconocer y lidiar contra los ataques de ingeniería social.” (pág. 66) Hoy en día es sumamente importante la educación de las personas en lo que se refiere a la seguridad cibernética, dentro y fuera de un área de trabajo, puesto que de forma personal ellos también están expuestos a distintos ataques de estos ciberdelincuentes, usando información personal encontrada en redes sociales.

Dentro de lo que involucra a redes sociales como se describió anteriormente, son las principales herramientas de los ciberdelincuentes, para ganarse la confianza de la posible víctima y cumplir con su objetivo, que puede ser robar información, o incluso llegar a la extorción. Otra de las principales herramientas es los correros electrónicos, puesto que estos son más fáciles de manipular, y más probable en la que las personas pueden llegar a ser víctimas. Para tratar de mitigar esta gran amenaza Gil (2022) propone las siguientes soluciones:

- ***OpenPGP*:** Es un protocolo de cifrado que se utiliza para encriptar mensajes, archivos y para demostrar la autenticidad del remitente mediante una firma digital. Se realiza mediante una clave privada y otra pública, la cual es compartida con terceros y puede ser visible para todos.
- **Protocolo S/MIME:** Por sus siglas que significan extensiones seguras multipropósitos al correo de Internet. Es una tecnología que permite cifrar correos electrónicos. S/MIME está basado en la criptografía asimétrica y la finalidad es proteger correos electrónicos frente a accesos no deseados. También permite firmar digitalmente correos electrónicos para autenticarse como el remitente legítimo de los mensajes, lo cual la 66 convierte en una eficaz arma contra los numerosos ataques de *phishing* que se producen cada día en Internet.
- **SPF/DKIM/DMARC:** Los protocolos de autenticación SPF (por sus siglas en inglés *sun protection factor* o factor de protección solar), DKIM (por sus siglas en inglés *domain keys identified mails)* y DMARC (por sus siglas en inglés *Domain-based Message Authentification Reporting and Conformance*) pueden ayudar a evitar que se manden correos suplantando la identidad del emisor. También sirven para dar más seguridad a los servidores de destino de los correos y así evitar, dentro de lo posible, que sean marcados como *SPAM*. (pág. 65)

De igual manera existen buenas prácticas para evitar ser víctimas de algún tipo de ataque, como señala la Escuela Europea de Negocios (2020):

1. Evitar compartir información en redes sociales.
2. Instalar un *firewall*, además, de un *software* que contrarreste el *malware*.
3. Evitar los correos de fuentes sospechosas o de fuentes tentadoras.
4. Realiza las actualizaciones de *software* y antivirus.
5. Realiza un monitoreo constante de redes sociales y situación financiera, en busca de algo fuera de lugar.
6. Gestionar con cuidado las contraseñas de sitios con información personal.
7. Evitar las redes *Wi-Fi* públicas.

8. Adquirir más información sobre la seguridad de la información o ciberseguridad.

Es esencial tener un entendimiento amplio de las distintas tácticas de prevención para defenderse de los ataques de ingeniería social en la era digital. Desde estar atentos a posibles engaños en las redes sociales hasta garantizar que nuestro *software* este siempre actualizados para cerrar posibles vulnerabilidades, cada medida de seguridad juega un papel importante en la protección contra los ciberataques. Además, cuidar meticulosamente nuestras contraseñas, se asegura de que sean sólidas y únicas para cada cuenta, refuerza aún más la seguridad de nuestros datos personales y empresariales. Al incorporar estas prácticas en nuestra rutina diaria, se puede reducir de manera significativa nuestra vulnerabilidad ante las amenazas en línea y promover un entorno digital más seguro y protegido.

Los enfoques *antiphishing* son de igual manera muy necesario e importantes conocer, así comparte Rosero (2021):

Las técnicas están categorizadas de la siguiente manera:

- **Enfoque de detección:** consiste en dos formas, la primera es el entrenamiento del usuario, se lo educa en lo referente a los ataques de phishing, esto permite que pueda distinguir entre mensajes malignos y no malignos. La segunda forma es la clasificación por *software*, el *software* realiza la tarea de clasificar mensajes de *phishing* en vez del usuario, para reducir la brecha del error humano o la ignorancia de este.
- **Enfoque defensa ofensiva:** el objetivo es generar campañas de *phishing* que no sean válidas, esto se logra desbordando el sitio *web* malicioso con credenciales no válidas, de esta manera el atacante tendrá un tiempo complicado para encontrar las credenciales originales
- **Enfoque de corrección:** al detectarse la campaña se comienza con el proceso de corrección, esto se realiza dando de baja los recursos de *phishing*; se lo logra reportando los ataques a los proveedores de servicios.

- **Enfoque de prevención:** dependiendo del contexto puede significar: prevención para evitar que los usuarios se conviertan en víctimas. En este enfoque se utilizan las técnicas de detección; prevención de los atacantes para comenzar campañas de *phishing*, consiste en demandas y sanciones legales para los atacantes por medio de los entes legales correspondientes. (pág. 15)

La lucha contra los ataques cibernéticos, como el *phishing*, se aborda mediante diversos enfoques que incluyen la detección, la defensa ofensiva, la corrección y la prevención. En el enfoque de detección, se enfatiza la importancia de educar a los usuarios sobre las señales de *phishing* y utilizar software especializado para filtrar mensajes maliciosos. La defensa ofensiva busca dificultar el trabajo de los atacantes inundando los sitios web maliciosos con información falsa. Por su parte, el enfoque de corrección implica tomar medidas una vez que se detecta un ataque, como eliminar recursos de *phishing* y notificar a los proveedores de servicios.

Finalmente, el enfoque de prevención busca evitar que los usuarios sean víctimas y perseguir legalmente a los perpetradores. Es esencial comprender estas estrategias de prevención para protegerse contra la ingeniería social y mantener la seguridad en línea.

Para los pequeños emprendedores, es importante implementar estrategias efectivas para evitar los ataques de ingeniería social, lo cual es vital para protegerse contra las amenazas en línea debido a su situación vulnerable y recursos limitados en ciberseguridad. Estas medidas se convierten en un escudo protector fundamental para salvaguardar la integridad de sus operaciones comerciales.

Al estar al tanto de los riesgos y adoptar medidas preventivas, como educarse sobre las tácticas de ingeniería social, utilizar herramientas de seguridad cibernética y establecer políticas claras de protección de datos, los pequeños emprendedores pueden fortalecer su resiliencia ante posibles ataques y conservar la confianza de sus clientes y socios comerciales en un entorno digital que se vuelve cada vez más desafiante.

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la empresa o institución

El Servicio de Integración Laboral (SIL) en Tungurahua es un proyecto que fue implementado en conjunto con la Federación Nacional de ecuatorianos con Discapacidad Física (FENEFID) y la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) en 2006, esta misma representa una valiosa iniciativa gubernamental sin costo alguno que se dedica a respaldar a personas con discapacidades en su búsqueda de empleo. Ubicada estratégicamente en las oficinas de la 12 de Noviembre y Mera, Centro Comercial Ambato, Oficina 10, esta institución trabaja arduamente para crear oportunidades laborales adaptadas a las necesidades específicas de este grupo.

El SIL desempeña diversas funciones esenciales para alcanzar su objetivo de facilitar la integración laboral de las personas con discapacidad. Por un lado, funciona como un enlace entre los trabajadores y los individuos con discapacidad, identificando oportunidades laborales apropiadas y colaborando con las empresas para crear ambientes de trabajo inclusivos y adaptados a las necesidades de cada persona.

Además, el SIL ofrece una amplia gama de servicios de apoyo tanto a los trabajadores, como a personas que laboran con algún tipo de discapacidad. Para el efecto, proporciona orientación y recursos con la finalidad de facilitar la contratación e integración de personas con discapacidad en sus equipos, a quienes brindan asesoramiento y preparación en habilidades laborales, ayuda en la búsqueda de empleo, apoyo para adaptarse a cada entorno de trabajo y seguimiento continuo para garantizar su éxito y desarrollo profesional a largo plazo.

El Servicio de Integración Laboral en Tungurahua cumple una función fundamental como entidad pública, actuando como un mediador entre trabajadores y empleadores. Ofrece servicios integrales para garantizar que todas las personas, sin importar sus capacidades, tengan la oportunidad de contribuir significativamente

al mercado laboral, a la sociedad en general y a utilizar estas herramientas tecnológicas en beneficio de su seguridad.

En la investigación de Núñez (2023) comenta que “el SIL desde hace varios años ha trabajado con la PUCESA a través de proyectos de vinculación enfocados en programas de capacitación en distintas áreas, así como con proyectos de investigación que han beneficiado a las personas con discapacidad” (pág. 24) es por ello por lo que el presente trabajo está enfocado en mencionados usuarios para fortalecer el conocimiento sobre la seguridad cibernética.

2.2 Metodología de investigación

La metodología de investigación se refiere al conjunto de procedimientos y técnicas empleados para realizar un estudio de forma estructurada y exacta. Esta metodología establece las pautas para recopilar, analizar e interpretar datos, además de definir los pasos necesarios para responder a la pregunta de investigación. Proporciona una guía que ayuda para obtener resultados válidos y confiables.

Existen diferentes enfoques dentro de la metodología de investigación, estas mismas son de importancia, para poder analizar, recopilar, y exponer los resultados de una investigación previa, este proyecto se enfoca en los siguientes:

Enfoque de investigación

El presente trabajo tiene como objetivo analizar e investigar las diferentes herramientas en las que actualmente muchas personas son víctimas de ingeniería social, y así de esta manera, poder propiciar a los usuarios una guía con diferentes estrategias que pueden servir para la protección de sus datos dentro de internet.

Es por ello por lo que los enfoques mixtos son la mejor opción para poder obtener todos los datos necesarios de aquellas personas vulnerables a los diferentes tipos

de ataques de ingeniería social, y así de igual forma comprender un poco más cuales son las necesidades primordiales que estas personas cumplirían.

Al ser una mezcla de la investigación cuantitativa y cualitativa potencia ambos enfoques para poder tener un mejor resultado en la investigación del presente trabajo, como lo afirma Otero (2018) en su trabajo “la investigación mixta no tiene como meta remplazar a la investigación cuantitativa ni a la investigación cualitativa, sino utilizar las fortalezas de ambos tipos de indagación combinándolas y tratando de minimizar sus debilidades potenciales” (pág. 22) así demostrando que este enfoque es el más efectivo para el presente trabajo.

Dentro del presente trabajo se realizaron diversas entrevistas a personas que tienen más experiencia en el campo de la seguridad cibernética y a aquellas personas que pueden llegar a ser vulnerables frente a estos ataques, estas entrevistas son de suma importancia como lo expone Oviedo (2019) “las entrevistas ayudan a captar matices y las opiniones de las personas de manera efectiva.” (pág. 26.)

Como parte de la recolección de datos se implementaron encuestas, para conocer un poco más sobre el nivel de conocimiento de los usuarios en cuanto a que hacer si son víctimas de estos ataques, o incluso conocer si es que han tenido algún tipo de capacitación sobre este problema de seguridad cibernética. Como expone Otero (2018) la importancia de este tipo de recolección de datos recae en que se “diseñaría unos instrumentos que le permita medir los datos de la muestra. Estos en algunos casos pueden ser a través de análisis estadísticos, como también, la aplicación de entrevistas abiertas, encuestas entre otros ajustados a naturaleza cualitativa. Toda investigación sería planificada en su proceso.” (pág. 10)

Tipo de investigación

El presente proyecto tiene en consideración dos tipos de investigación esenciales: Investigación de Campo e Investigación Bibliográfica. Cada una de estas es de suma importancia puesto que así se compararía los diferentes autores con sus

ideas, teniendo en cuenta a la población con la que se va a trabajar. Esta combinación hace que se tenga ambos puntos de vista y así poder obtener un resultado mucho más efectivo.

Dentro de la investigación de campo, se realizó entrevistas a diferentes personas para poder recopilar datos, tanto de gente que ya es experta en el tema de seguridad cibernética, como aquellas personas vulnerables que no tienen mucho conocimiento sobre cómo protegerse. De igual manera se realizó una encuesta, para poder llegar de una forma más sencilla a aquellas personas con discapacidad en las que va a ir enfocada la guía final, esta misma se diseñó para obtener información sobre cuanto conocen estas personas de los ataques de ingeniería social, y poder realizar un mejor trabajo partiendo desde ahí.

Así también, la investigación bibliográfica es esencial dentro de cualquier investigación, como cuenta Otero (2018) “esta búsqueda facilita identificar conceptos claves relacionados con la idea de investigación, así mismo que puede proporcionar elementos que faciliten la recolección de datos y el análisis de estos a través de diferentes métodos que permitan el entendimiento de estos y avanzar en su interpretación.” (pág. 18)

Población

La población con la que se trabajó para conocer sobre sus conocimientos, pensamientos y experiencias personales dentro de la seguridad cibernética, son personas con diferentes discapacidades que se encuentran dentro del SIL de Tungurahua, debido que a estas personas es a las que se les quiere ayudar en un futuro con la guía ya terminada y así que puedan protegerse de una forma más efectiva en el entorno informático. A estas personas se llegó gracias a la entrevista con la Psicóloga Mercedes Santana, analista promotora laboral del SIL.

También se ha tomado en consideración a dos especialistas en el tema de seguridad informática para poder tener un punto de vista más técnico al momento de analizar la información previamente consultada.

A continuación, la población se detalla en el siguiente cuadro:

Cuadro 1. Población entrevistada y encuestada

Entrevistado	Cargo
Mercedes Santana	Analista Promotora del SIL
Héctor Robayo	Analista de TICS de la Gobernación de Tungurahua
Liliana Mena	Coordinadora del programa de maestrías en ciberseguridad PUCESA
Encuestados	
12 personas con discapacidad	Miembros del proyecto SIL de Tungurahua

Fuente: elaboración propia

La tabla anterior se usó para tener en cuenta cuál es el número de personas con las que se va a trabajar, que pueden llegar a ser vulnerables frente a un ataque, y de igual manera para determinar cuántas personas que si conocen sobre el tema de seguridad cibernética dan sobre este tipo de problemas que afronta la población más vulnerable.

Instrumentos

En lo que se refiere a los diferentes instrumentos que se aplicaron para el presente trabajo, se recopiló la información de la siguiente manera: Entrevistas y Encuestas. Estos dos instrumentos fueron de suma importancia para obtener diferentes perspectivas de los usuarios, sus conocimientos de los ataques de ingeniería social, los diferentes problemas que hayan atravesado y si conocen sobre qué hacer en caso de ser víctima de este tipo de ataques y para analizar la opinión de diferentes expertos en el tema.

- Entrevista*:* Para el presente trabajo se tomó en consideración 2 tipos de entrevistas, la primera fue a la psicóloga Mercedes Santana Analista Promotora del SIL, que se encuentra en el anexo 1 para poder recopilar la mayor cantidad de información que la persona que está a cargo de los trabajadores con capacidades especiales conoce acerca de la ingeniería social, y sobre la cantidad de miembros del SIL con los que se puede llegar a trabajar. La siguiente entrevista se realizó al ingeniero Héctor

Robayo Analista de TICS de la Gobernación de Tungurahua, que se encuentra en el anexo 2, quien, desde su punto de vista mucho más experimentado, da su opinión acerca de las diferentes herramientas que usan los delincuentes cibernéticos al momento de realizar estos ataques. Y por último también se entrevistó a la magister Liliana Mena Coordinadora del programa de maestrías en ciberseguridad PUCESA que se encuentra en el anexo 3, quien también compartió sus conocimientos sobre las diferentes medidas de seguridad que se puede llegar a implementar en las instituciones.

- Encuesta: La encuesta para recopilación de datos que se encuentra en el anexo 4, tiene como objetivo conocer, diferentes aspectos sobre la población vulnerable, en que situaciones pueden estar fallando al momento de protegerse en la red, y si es que llegaran a ser víctimas de este tipo de ataques, que se haría para denunciar en nuestro país, está misma es de vital importancia puesto que con esto sabremos el nivel de educación en seguridad cibernética que posee la población del SIL de Tungurahua.

Los medios empleados en este estudio, como las entrevistas y encuestas, han sido esenciales para recopilar datos precisos y detallados. Las entrevistas brindaron perspectivas valiosas de expertos y profesionales, ofreciendo una visión amplia sobre la ingeniería social y sus implicaciones. Las encuestas, por otro lado, sumaron datos cuantitativos que enriquecieron la comprensión de las percepciones y prácticas de la población vulnerable ante los ataques cibernéticos. Estos medios no solo facilitaron un análisis exhaustivo, sino que también ayudaron a identificar áreas de mejora y soluciones para fortalecer la seguridad cibernética en la comunidad del SIL de Tungurahua. El uso efectivo de estos medios fue vital para el desarrollo del estudio y para promover la protección y concienciación en seguridad.

2.3 Metodología de desarrollo

La metodología óptima para el desarrollo de este proyecto es Kanban, puesto que según Garcés (2023) esta metodología “busca optimizar la producción e

incrementar la productividad, lo que lo convierte en un sistema eficiente que reduce el desperdicio de producción y los tiempos muertos.” (pág. 735) es un método eficiente y efectivo que busca aprovechar todo el tiempo que se tenga para desarrollar el proyecto mediante diferentes tipos de tareas.

Kanban, frente a otro tipo de metodologías se base en cuatro diferentes tipos de principio que según Olic (2015) son:

- La calidad es fundamental, por lo que es crucial que las actividades salgan bien desde el principio, sin margen para errores, lo que garantiza la calidad.

- No se desperdicia nada, puesto que Kanban se centra en hacer lo necesario de manera correcta; en resumen, no se implementa algo a menos que se esté seguro de su necesidad.

- Kanban fomenta la mejora continua, no solo dirige y gestiona un proyecto, sino que también se esfuerza por mejorar a lo largo del tiempo de acuerdo con los objetivos establecidos.

- Prioriza las tareas según las necesidades del momento, lo que significa que es adaptable y flexible.

Para poder comenzar con la preparación de la metodología se va a realizar una tabla con diferentes columnas como lo explica Garcés (2023) Tiene tres columnas, en las cuales el proyecto va a ir avanzando en sus diferentes etapas como son: Por hacer, Haciendo y Terminada. Como lo explica Garcés (2023) en su trabajo “Cuando una idea es tomada de la columna de ideas se traslada a las siguientes columnas y, en algunos casos, dependiendo de su alcance y complicación, se genera un nuevo tablero Kanban para un mayor control particular del proyecto.” (pág. 736).

Figura 1. Tablero de Kanban

Fuente: tomado a partir de Arriaga (2018)

Este tablero contiene las etapas en las que se va a dividir el presente proyecto, más, sin embargo, no define las etapas por las que va a pasar, esto quiere decir que se analizarían previamente cada uno de los requerimientos que se necesita al finalizar el trabajo, y por lo tanto después de hacer ese análisis se llegó a la conclusión que tendrá cuatro etapas importantes: Análisis, Ataques, Desarrollo y por último Evaluación y Validación

Análisis

Conforme al esquema anteriormente descrito a continuación se va a definir el desarrollo de la siguiente etapa, dentro del análisis del problema

Cuadro 2. Tablero Kanban de la Fase de Análisis

TO – DO	DOING	DONE
Analizar los resultados de la encuesta realizada al grupo vulnerable SIL de Tungurahua Analizar las entrevistas a los diferentes expertos en seguridad cibernética e ingeniería social y a la persona encarga del SIL. Buscar bibliografía sobre los ataques de ingeniería social en Ecuador y como denunciarlos		

Fuente: elaboración propia

Tarea 1: Se realizó una encuesta a la población vulnerable en la que se va a enfocar el proyecto que es el SIL de Tungurahua anexo 4, con un total de diez preguntas,

entre cerradas y abiertas a doce personas pertenecientes al grupo de personas discapacitadas, a continuación, se expondrá de manera detallada, cada una de las preguntas y de las respuestas que fueron obtenidas en esta misma:

Pregunta 1. ¿Ha sido víctima de algún tipo de estafa en línea en el pasado? Respuestas: El cincuenta por ciento de la población encuestada contesto que si ha sido víctima y el otro cincuenta por ciento respondió que no han sido víctimas.

Pregunta 2. ¿Ha sido víctima o conoce a alguien que haya pasado por alguna de las siguientes situaciones? Respuestas: Del total de la población encuestada tres personas dijeron que han sido víctimas o conocen a alguien que les hayan clonado el perfil en redes sociales, dos personas contestaron que han recibido correos electrónicos fraudulentos, a tres personas les han hecho extorción por llamada telefónica, solamente una persona ha sido víctima de robo de datos bancarios, y tres personas contestaron que ninguna de las anteriores.

Pregunta 3. ¿Qué medidas tomas habitualmente para proteger tu información personal y financiera en línea? en caso de no tomar ninguna medida colocar (NINGUNA) Respuestas: Cinco encuestados respondieron que NINGUNA, tres personas contestaron que usan contraseñas, una persona contesto que no confiar en nada ni nadie, otra persona dice que no enviar datos delicados, como claves, una persona dice que no contestar llamadas extrañas, y una persona contesto que siempre cambiar las claves.

Pregunta 4. ¿Ha recibido capacitación sobre cómo prevenir ataques de ingeniería social? Respuestas: El cien por ciento de los encuestados contestaron que no han recibido ninguna capacitación sobre este tema.

Pregunta 5. ¿Está al tanto de los pasos a seguir en caso de ser víctima de algún tipo de estafa en la web? Respuestas: Ninguna persona contesto que está totalmente informado, una sola persona contesto que tiene una idea general, y once personas contestaron que no están informados.

Pregunta 6. En caso de ser víctima, ¿Sabe cómo denunciar este hecho a las autoridades? Respuestas: Una sola persona contesto que sí y once personas contestaron que no sabrían como denunciar.

Pregunta 7. ¿Utilizas medidas adicionales de seguridad, como la autenticación de dos pasos, en tus dispositivos electrónicos? Respuestas: Dos personas contestaron que sí, y diez personas respondieron que no utilizan ninguna medida adicional de seguridad.

Pregunta 8. ¿Has recibido correos electrónicos o mensajes sospechosos solicitando información personal o financiera? Respuestas: Una persona contesto que sí, con frecuencia, seis personas respondieron que sí, ocasionalmente, y cinco personas contestaron que no.

Pregunta 9. ¿Consideras importante que las instituciones educativas incluyan formación sobre seguridad en línea y prevención de estafas en sus programas? Respuestas: Siete personas dijeron que sí, es crucial, sin embargo, tres personas contestaron que sí, pero no es prioritario, y dos personas contestaron que no están seguras.

Pregunta 10. ¿Crees que sería obligatoria la capacitación sobre medidas de prevención contra cualquier tipo de ataque? Respuestas: Ocho personas contestaron que sí, dos personas contestaron que no, dos personas contesto que no es obligatorio, pero si necesario.

La encuesta llevada a cabo entre la población vulnerable, dentro del marco del proyecto SIL de Tungurahua, proporciona una visión clara acerca de las vivencias y percepciones en relación con la seguridad en línea. Los resultados muestran una división equitativa en cuanto a la incidencia de estafas en línea, con el cincuenta por ciento de los encuestados admitiendo haber sido víctimas en el pasado. Además, se evidencia una falta notable de capacitación en asuntos de seguridad, dado que ningún participante ha recibido formación sobre la prevención de ataques

de ingeniería social, y solo una persona afirma estar informada sobre los pasos a seguir en caso de ser víctima de una estafa en línea.

También resalta el hecho de que la mayoría de los encuestados no emplean medidas adicionales de seguridad en sus dispositivos electrónicos, lo que subraya la importancia de promover una mayor conciencia y educación en esta área.

Por otro lado, se nota una conciencia generalizada sobre la importancia de la educación en seguridad en línea, con la mayoría de los encuestados expresando que las instituciones educativas incorporarían formación sobre este tema en sus programas. Sin embargo, también se percibe cierta indecisión en cuanto a la obligatoriedad de dicha capacitación, con algunas respuestas sugiriendo que no es una prioridad absoluta. Estos hallazgos enfatizan la necesidad urgente de implementar programas de educación y sensibilización sobre seguridad en línea, así como la importancia de establecer políticas que fomenten la capacitación obligatoria en medidas de prevención contra cualquier tipo de ataque, con el fin de proteger a la población vulnerable ante las amenazas en el mundo digital.

Tarea 2.1: Según la entrevista realizada a la psicóloga Mercedes Santana anexo 1, analista promotora laboral del SIL de Tungurahua, con un total de diez preguntas comenta que actualmente hay un total de 20 emprendedores activos que están dentro del programa, y supo manifestar que se puede llegar a realizar un muestreo con 10 personas como mínimo que estarían dispuestas a realizar encuestas y entrevistas debido a sus diferentes condiciones.

Dentro de la entrevista se le hicieron varias preguntas para conocer el nivel de conocimiento sobre ingeniería social, y de igual manera para saber si es que alguna vez han sufrido algún tipo de ataque. Supo manifestar que nunca han recibido una capacitación sobre ciberseguridad. De igual manera afirmó conocer sobre las estafas y suplantaciones de identidad que existen en redes sociales.

De la misma forma comentó que no está acostumbrada a cambiar periódicamente la contraseña de acceso personal a sus redes sociales, si es que le llegara un

correo electrónico falsificado, con el cual quisieran robarle información, comentó que no sabría como identificarlo, también dijo que ningún emprendedor que está en el programa actualmente le ha comentado sobre algún problema de ciberseguridad, así mismo invita a que se realice la investigación en la institución para poder conocer más sobre este tema y las precauciones que se tomarían. Mercedes comenta que dentro del SIL no ha tenido problemas sobre clonación de perfiles o estafas más, sin embargo, si conoce gente externa al programa que ha sufrido de este tipo de ataques de ingeniería social.

En relación con el conocimiento sobre ingeniería social y ataques cibernéticos, se revela que nunca han recibido capacitación al respecto. A pesar de estar consciente de los riesgos de estafas y suplantaciones de identidad en redes sociales, Mercedes confiesa que no suele cambiar regularmente sus contraseñas y no se siente segura para distinguir correos electrónicos fraudulentos. Aunque no ha experimentado contratiempos de seguridad informática dentro del SIL, reconoce casos externos de clonación de perfiles y fraudes entre individuos ajenos al programa, lo que indica la necesidad de investigar y adoptar medidas preventivas adicionales en la institución.

Tarea 2.2: Según la entrevista realizada al Magister Héctor Robayo anexo 2, analista de TICS de la Gobernación de Tungurahua, con un total de diez preguntas, comentó que él considera el *phishing* como la técnica más común utilizada actualmente por los ciberdelincuentes, y de igual manera estos ataques son los que más frecuentemente usan en contra de los entornos empresariales.

En referente a los principales riesgos y consecuencias asociados con los ataques de ingeniería social para los grupos vulnerables, dijo que la perdida de información y la obtención de datos personales de las personas, son los principales riesgos, puesto que al momento que un ciberdelincuente obtiene información sensible y privada, puede comenzar con las extorciones por llamadas telefónicas, o incluso la suplantación de identidad.

Algunas de las medidas o estrategias que considera más efectivas para prevenir los ataques de ingeniería social en grupos vulnerables, son las capacitaciones a la población en general, tener el conocimiento para aplicar y mantener el *firewall,* implementar e invertir en un buen antivirus, y de igual manera aplicar políticas de seguridad en una empresa. De igual manera la capacitación permanente desde el ingreso a cualquier empresa, o lugar de trabajo sobre los peligros de la ingeniería social, es una estrategia que puede ayudar a prevenir futuros ataques, comentó el Ingeniero.

También se habló que no conoce cuales son los pasos para denunciar un ataque de ciberseguridad en Ecuador, pero que si fuera una información que todas las personas conocerían, para saber que hacer en caso de ser víctimas de este tipo de ataques. Comenta que las redes sociales hoy en día juegan un papel muy importante en la ejecución de ataques de ingeniería social, puesto que es un punto u objetivo en el cual los ciberdelincuentes lo ven como vulnerables, y como la forma más sencilla de obtener información personal.

Una de las medidas de seguridad adicional que puede implementarse en los entornos de trabajo remoto para proteger a los empleados contra los ataques de ingeniería social es la capacitación para el uso de antivirus, y agregar políticas de seguridad. Para finalizar hablo sobre cómo pueden las organizaciones evaluar su nivel de vulnerabilidad frente a los ataques de ingeniería social y las acciones pueden tomar para mejorar su seguridad son mediante auditorias periódicos controles permanentes.

Esta entrevista ofrece un análisis detallado sobre los riesgos relacionados con los ataques de ingeniería social y las estrategias para prevenirlos. Reconoce al *phishing* como la táctica más frecuentemente utilizada por los ciberdelincuentes, particularmente dirigida a entornos empresariales. Destaca la amenaza de pérdida de información y la vulnerabilidad de los datos personales para los grupos vulnerables, subrayando la importancia de una formación continua y la adopción de medidas de seguridad como el uso de antivirus y la aplicación de políticas de protección en las empresas.

Así mismo, enfatiza la necesidad de conocer los procedimientos para denunciar los ataques de ciberseguridad en Ecuador y la importancia de sensibilizar sobre los riesgos de la ingeniería social, especialmente en el ámbito de las redes sociales. Sugiere la capacitación en el uso de antivirus y la implementación de políticas de seguridad como medidas adicionales en los entornos de trabajo remoto, y recomienda auditorías periódicas como un medio para evaluar y fortalecer la seguridad contra los ataques de ingeniería social.

Tarea 2.3: Según la entrevista realizada a la Magister Liliana Mena coordinadora del programa de maestrías en ciberseguridad PUCESA anexo 3, cuenta que ella considera que las técnicas más usadas por los ciberdelincuentes en la actualidad son el *phishing* a través de mensajes de texto y el *vishing* a través de llamadas telefónicas. Y dentro de los entornos empresariales afirma que el *phishing* es el que más se da.

Los principales riesgos asociados con los ataques de ingeniería social para los grupos vulnerables puede ser el robo de la información, suplantación de identidad, robo de datos bancarios. De igual manera comenta que una medida muy efectiva para prevenir los ataques de ingeniería social, son las capacitaciones al personal sobre cuáles son los ataques más comunes que existe, los riesgos a lo que se exponen las personas al momento de navegar en internet, socializar a las personas los riesgos de las redes sociales al momento de compartir su información personal.

Para poder adaptar las capacitaciones en ciberseguridad a la población vulnerable en la que está enfocada este proyecto que es el SIL de Tungurahua, habla que como primer paso se hiciera un estudio de las discapacidades que poseen las personas que están dentro de este programa, puesto que existen diferentes requerimientos para cada una de ellas, y de igual manera dar una capacitación en general sobre el riesgo de ser muy confiados en el internet de hoy en día.

Dice que es muy importante establecer políticas y procedimientos internos para prevenir los ataques de ingeniería social en organizaciones porque a partir de las políticas y de aplicar las normativas, las instituciones van a tener enfoques desde

donde actuar, porque en estas mismas políticas iría descrito como van las contraseñas, o aspectos de a qué información se le va a dar acceso al usuario, los roles.

Al igual que en la entrevista anterior comenta que no conoce cuales son los pasos para denunciar un ataque de ciberseguridad en Ecuador, puesto que igual en el país de lo que se escucha de las veces que se acude a la policía por llamadas telefónicas amenazantes, de mensajes de igual manera amenazantes o por correo electrónico, de robo de información, o de acoso, no se da el debido seguimiento, pero que si sería importante conocer cómo hacer la denuncia y como se va a dar continuidad a este proceso.

Las redes sociales juegan un papel muy importante en la ejecución de ataques de ingeniería social, porque hoy en día la mayoría de personas manejan redes sociales, pero no saben cómo realmente cuidarse, y en ese aspecto si se daría mayor socialización, y el cómo se pueden proteger las personas es que no se tomaría tanto a la ligera o como un juego el publicar demasiada información, puesto que hoy con la inteligencia artificial es mucho más sencillo con una foto de una persona, buscar datos en internet, número de teléfono, dirección del domicilio.

Colocar contraseñas más seguras, que no sean tan fáciles de adivinar, usar los controles de seguridad que ya vienen en las redes sociales como es la verificación en dos pasos, que hay veces en la que no se verifica, pero con esto se podría saber quién accede de manera ilegítima a cualquier perfil de cualquier red social.

Algunas de las medidas de seguridad adicionales que puede implementar en entornos de trabajo remoto son las VPNs, porque tiene un grado grande de seguridad, trabajar siempre usando sitios seguros, usando el https que un sitio seguro. Para finalizar cuenta que las organizaciones pueden evaluar su nivel de vulnerabilidad usando diferentes herramientas que existen de manera online, para conocer qué tan seguros están los equipos de una empresa.

Tarea 3: Los ataques de ciberseguridad han crecido mucho, sobre todo en época de pandemia según el departamento de seguridad de las TIC de la Policía Nacional del Ecuador afirma que “en el 2017 se registraron 8421 casos; subieron a 9571 y 10 279 en 2018 y 2019. La tendencia se mantiene. Los más frecuentes son las estafas digitales con modalidades como la suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos.” (pág. 3) Es muy preocupante la forma en la que han subido este tipo de ataques, puesto que desde la pandemia la era digital ha ido creciendo de una manera exponencial.

Según la Policía Nacional del Ecuador comenta que:

> Desde que entró en vigor el Código Orgánico Integral Penal (COIP), el 10 de agosto del 2014, contempla y sanciona los delitos informáticos como, por ejemplo: la revelación ilegal de base de datos, la interceptación ilegal de datos, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos y los accesos no consentidos a un sistema telemático o de telecomunicaciones, la pornografía infantil, el acoso sexual. (pág. 01)

Así mismo como se menciona en el párrafo anterior estos delitos ya se contemplan en el código orgánico integral penal, lo que quiere decir que, si se puede ir a denunciar cualquier tipo de ataque, únicamente presentando la cédula como comenta la Policía Nacional se puede “acercarse a denunciar en los Servicios de Atención Ciudadana de la Fiscalía más cercana a su lugar de residencia. En Quito existen siete Unidades de Servicio de Atención al Integral (SAI) donde receptan las denuncias (Fiscalía de Pichincha, Quitumbe, Mena 2, Tres Manuelas, Carcelén, Tumbaco, Los Chillos.” (pág. 01) Este trámite es completamente gratuito y no es necesario ir con un abogado.

Ataques

Para comenzar con la fase de ataques de ingeniería social, se observó el análisis previamente detallado, y a continuación se muestra una actualización del tablero, con las tareas a desarrollar en esta fase.

Cuadro 3. Tablero Kanban de la Fase de Ataques

TO – DO	DOING	DONE
Documentar diferentes ejemplos de ataques de ingeniería social reales Documentar una simulación de ataque de ingeniería social		Analizar los resultados de la encuesta realizada al grupo vulnerable SIL de Tungurahua Analizar las entrevistas a los diferentes expertos en seguridad cibernética e ingeniería social y a la persona encarga del SIL. Buscar bibliografía sobre los ataques de ingeniería social en Ecuador y como denunciarlos

Fuente: elaboración propia

Tarea 1: Actualmente, los ataques de ingeniería social se han convertido en una parte habitual de la vida diaria de las personas, se solicitó a un grupo de gente enviar capturas de las diferentes formas en las que han intentado hacerles ingeniería social, una vez socializado, y con la aceptación y permiso de estas mismas, a continuación, se presentan diferentes tipos de ejemplos de ataques de ingeniería social.

Figura 2. Ejemplo de Mensaje fraudulento

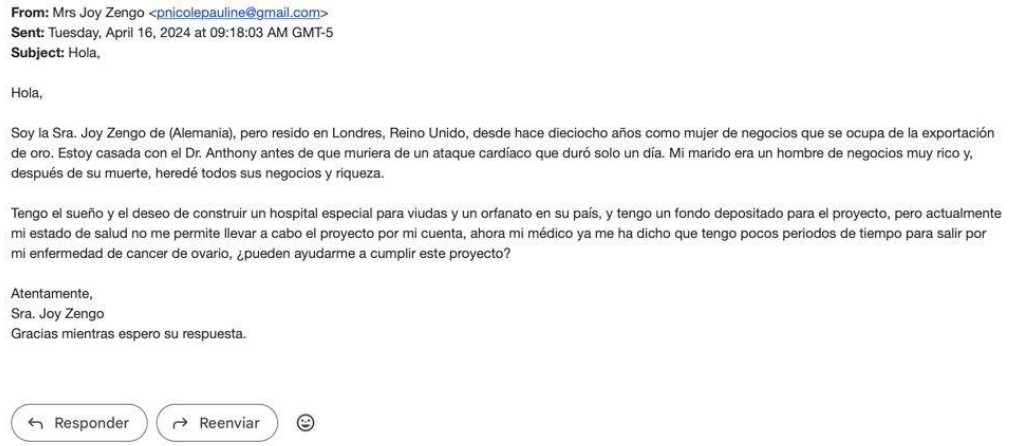
Fuente: tomado a partir de Gaibor (2024)

Como se observa en la figura 2, el mensaje intenta engañar al destinatario haciéndole creer que ha sido seleccionado para un trabajo legítimo en Facebook (Meta). Este es un intento de obtener información financiera o personal del destinatario. Las siguientes son señales importantes de que se trata de una estafa:

- Es muy típico de estafas que ofrecen altas ganancias por poco trabajo.
- La frase “SÓLO POR TIEMPO LIMITADO” crea urgencia.
- Es un mensaje no solicitado porque el remitente no está en los contactos del destinatario.
- En lugar de proporcionar una dirección de correo electrónico o un enlace a un sitio web oficial, algo común en las estafas para evitar rastros fácilmente verificables, proporcione un número de WhatsApp.

Lo más recomendado en estos casos es ignorar el mensaje y reportar como spam o mensaje no deseado, para así de esta forma, poder alertar a las empresas que esa dirección de correo, o número telefónico, está enviando mensajes sospechosos.

Figura 3. Correo electrónico fraudulento



Fuente: tomado a partir de Semblantes (2024)

En la figura 3, se puede observar que el mensaje intenta engañar al destinatario haciéndole creer que existe una oportunidad de participar en un proyecto solidario, aprovechando la emotiva historia para ganarse su confianza. En particular, se trata de una estafa de "herencia" o "fondo caritativo" en la que la heredera

supuestamente rica necesita ayuda para transferir dinero o completar un proyecto. La mayoría de las veces, estas estafas tienen como objetivo obtener dinero o información personal de las víctimas. Las siguientes son señales importantes de que se trata de una estafa:

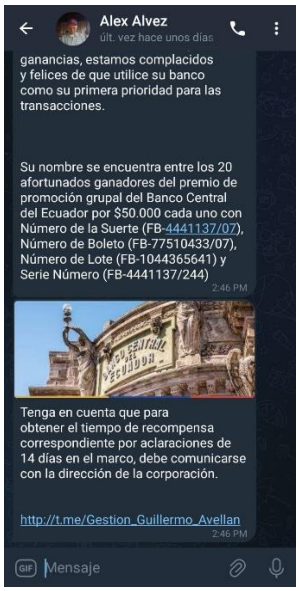
- Una historia emotiva y detallada sobre una situación personal trágica (muerte de marido, por cáncer) para provocar empatía.
- Prometer una gran cantidad de dinero o un fondo para un proyecto caritativo.
- El hecho de que el destinatario no sepa quién es el remitente
- Se puede concluir que el remitente eventualmente le solicitará información personal o dinero para facilitar el proceso

La red social más común en la que los ciberdelincuentes intentan estafar personas es la red de *Telegram*, toman su usuario de cualquier grupo, o canal en el que se pueda ver los miembros, y comienzan a enviar, diferentes ofertas de trabajo con dinero fácil en poco tiempo

Figura 4. Mensaje con intención de estafar

Fuente: tomado a partir de Muñoz (2024)

Figura 5. Mensaje con intención de estafar



Fuente: tomado a partir de Muñoz (2024)

El mensaje de texto que se muestra en la figura 4 y 5, intenta engañar al usuario para que haga clic en un enlace que lo llevará a un sitio web falso que parece ser el sitio web del Banco Central del Ecuador. Los ciberdelincuentes pueden utilizar la información que se proporciona en un sitio web falso para robar dinero o identidad. Las señales que indican que el mensaje es phishing son:

- El mensaje no está dirigido al nombre del usuario.
- El mensaje contiene errores gramaticales u ortográficos.
- El mensaje hace que el usuario sienta miedo o urgencia de actuar rápidamente.
- El mensaje solicita que el usuario revele datos personales o financieros.
- El enlace incluido en el mensaje no es una dirección web legítima del Banco Central del Ecuador

Muchas veces las personas caen en este tipo de estafas, les dan dinero a los usuarios por tareas simples, como ver videos en línea, luego, poco a poco le dan cada vez menos recompensa, a no ser qué invite a más personas, o que se les pague para que la comisión por cumplir tareas aumente.

Figura 6. Mensaje fraudulento

Fuente: tomado a partir de Muñoz (2024)

Como se puede observar en la figura 6, los ciberdelincuentes, le otorgan dinero a la víctima, con el afán de que esta misma confíe en ellos, es en este momento en el que la manipulación de estas personas ataca.

Figura 7. Mensaje con intención de estafar

Fuente: tomado a partir de Muñoz (2024)

En la figura 7, se puede observar que se ofrece dinero a cambio de invertir, y de hacer ciertas actividades como ver videos, tienen una estructura detalla, y por esto

las personas que no tienen conocimiento de este tipo de estafas, pueden llegar a ser víctimas.

Figura 8. Publicidad engañosa

Fuente: tomado a partir de Muñoz (2024)

Este tipo de publicidades como se muestra en la figura 8, es muy común para hacer que las personas den su información personal, como correo electrónico, para supuestamente ganar sumas de dinero grande en poco tiempo

Figura 9. Amenazas para solicitar dinero

Fuente: tomado a partir de Muñoz (2024)

Como se puede observar en la figura 9, al momento de proporcionar información personal a este tipo de ciberdelincuentes, comienzan con las amenazas como se puede ver en la figura 9 y 10, en la cual, si no dan el dinero requerido, recurren a la extorción para poder conseguir su propósito.

Figura 10. Amenaza vía correo electrónico

Fuente: (Muñoz, M. 2024)

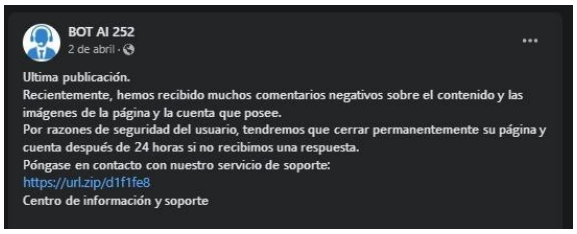
Facebook, es una de las redes sociales más grandes del mundo, casi todas las personas poseen un perfil dentro de esta red, y por lo tanto también es una de las herramientas, más comunes utilizadas por los ciberdelincuentes.

Figura 11. Páginas fraudulentas en *Facebook*

Fuente: tomado a partir de Muñoz (2024)

Este tipo de páginas que se puede observar en la figura 11, son creadas para robar la información personal como número de teléfono, dirección del domicilio, correo electrónico, fotos privadas, de Facebook de los usuarios.

Figura 12. Ejemplo de publicación fraudulenta



Fuente: tomado a partir de Muñoz (2024)

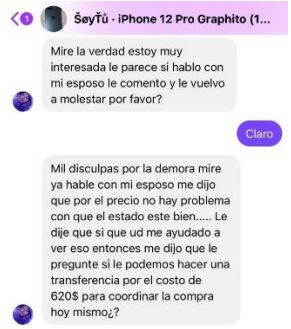
Como se puede observar en la figura 12, hacen este tipo de publicación, esperando que las personas del clic en el enlace, por el medio en el que comienzan a robar toda la información del perfil de la víctima.

Continuando con la red social Facebook, dentro de esta se encuentra *Market Place,* un sitio en el que los emprendedores, pueden publicar sus productos para la compra y venta de estos mismo, la mayoría de estas personas tiene el mismo modo de operar para intentar estafar a los usuarios, como se muestra en las figuras 13, 14 y 15.

Figura 13. Intento de estafa en *Market Place*

Fuente: tomado a partir de Semblantes (2024)

Figura 14. Intento de estafa en *Market Place*



Fuente: tomado a partir de Semblantes (2024)

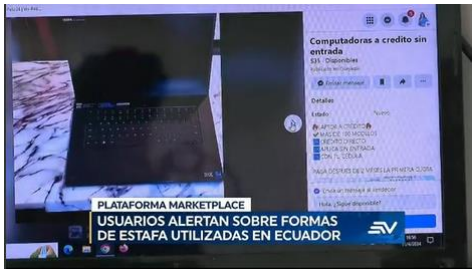
Figura 15. Intento de estafa en *Market Place*

Fuente: tomado a partir de Semblantes (2024)

Como se puede observar es estos ejemplos, la mayoría de estas personas, alude a que consultaría con su esposo/sa y de la misma manera el método de pago por transferencia, para evitar esto, se recomienda a los usuarios, aceptar la transferencia únicamente si se trata del mismo banco que posea el emprendedor, para evitar que el pago no llegue.

El medio de comunicación Ecuavisa, emitió una noticia en la cual dio a conocer como los ciberdelincuentes, usan *Market Place* para estafar a los vendedores que se encuentran dentro de esta aplicación, el modo de operación de estas personas es el siguiente: el comprador al momento de hacer una transferencia ingresa todos los datos de manera correcta para realizar el pago, pero ingresa un número de la mitad de la cuenta diferente, al momento de emitir el comprobante el número de cuenta no se puede visualizar de manera completa, por ende la transferencia rebota, y es devuelta al mismo comprador, es por eso que se recomienda a los vendedores, asegurarse que las transferencias si les haya llegado a sus cuentas, por eso es preferible que el vendedor y el comprador, tengan la misma entidad bancaria.

Figura 16. Noticia de estafa



Fuente: tomado a partir de Ecuavisa (2024)

Figura 17. Método de estafa

Fuente: tomado a partir de Ecuavisa (2024)

Figura 18. Muestra del método de estafa

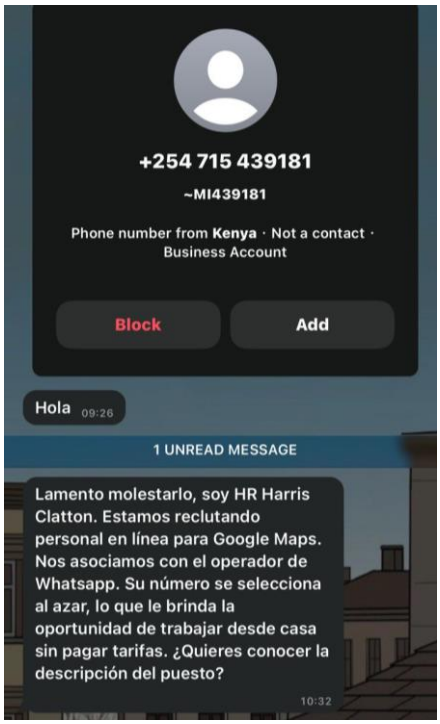
Fuente: tomado a partir de Ecuavisa (2024)

Figura 19. Método de Estafa

Fuente: tomado a partir de Ecuavisa (2024)

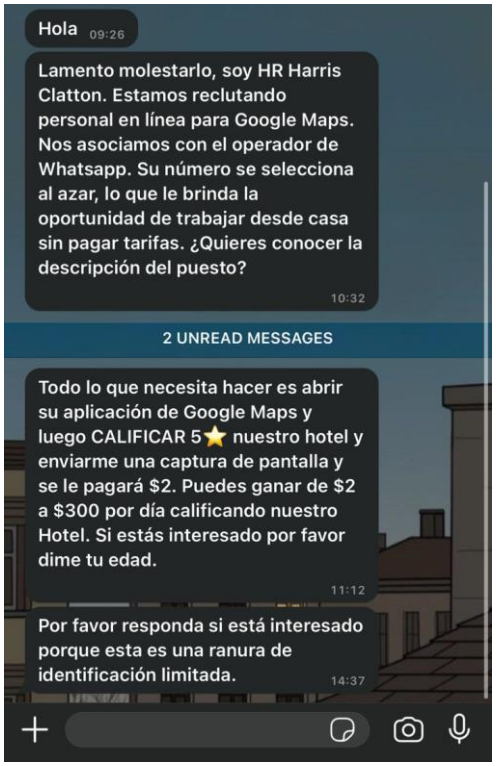
Siguiendo con el servicio de mensajería *WhatsApp,* muchas veces los usuarios colocan su número de celular para registrarse en diferentes páginas, posteriormente, con la información recaudada, comienzan a enviar mensajes, ofreciendo diferentes servicios, haciéndose pasar por agentes de *Google, Instagram,* entre otros, como se puede observar en las figuras 16, 17 y 18.

Figura 20. Ejemplo de mensaje fraudulento



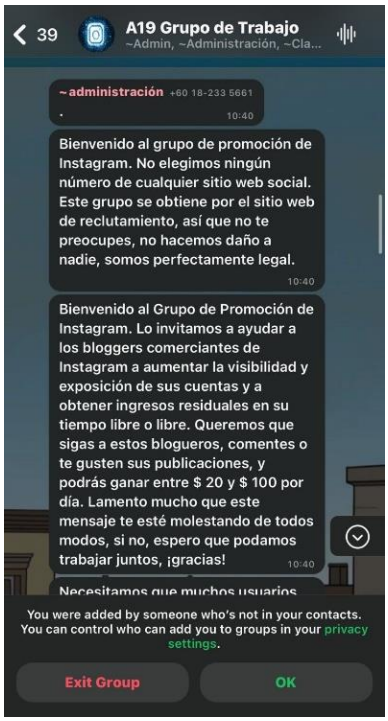
Fuente: tomado a partir de Altamirano (2024)

Figura 21. Ejemplo de mensaje fraudulento



Fuente: tomado a partir de Altamirano (2024)

Figura 22. Ejemplo de mensaje fraudulento



Fuente: tomado a partir de Altamirano (2024)

Como se pudo observar la mayor parte de estos ciberdelincuentes, dicen trabajar para grandes empresas, y ofrecen dinero, lo ideal en estos casos es ignorar los mensajes, denunciar como *spam*, dentro de la misma aplicación, y bloquear el número para evitar que estos tipos de mensajes sigan llegando.

Figura 23. Ejemplo de mensaje en Instagram

Fuente: elaboración propia

Figura 24. Ejemplo de mensaje en Instagram

Fuente: elaboración propia

Para concluir esta parte, en la figura 19 y 20, se puede encontrar ejemplos de supuestas propuestas de negocios con marcas reconocidas, o usando inteligencia artificial, mediante el servicio de mensajería de *Instagram,* incluso pueden llegar a poner el nombre del usuario para intentar manipular mejor al usuario.

Como se pudo observar en esta tarea los ciberdelincuentes encuentran las formas de engañar a las personas, ofreciendo trabajos muy fáciles con remuneraciones altas, en caso de no continuar dando dinero a estas personas, o invitando a más personas, comienzan con las amenazas, es importante conocer cuáles son los factores más comunes que usan estas personas para evitar ser víctimas de estos ataques de ingeniería social.

Tarea 2: Para esta tarea se solicitó previamente el permiso de la persona involucrada, con un acuerdo firmado que se puede observar en el anexo 5, para comenzar, los únicos datos que se conocía de la víctima eran los siguientes:

-Nombre: Adriana Moscoso
- Propietaria de la Empresa: Rodamientos Bower 4

Objetivo: Robar la contraseña del sitio web de Facebook personal, para extorsionar
Información Disponible: Nombre de Propietaria, y nombre de la empresa.

Posibles Herramientas:

- Google Dorks
- Set Took kit

Red Social para atacar:

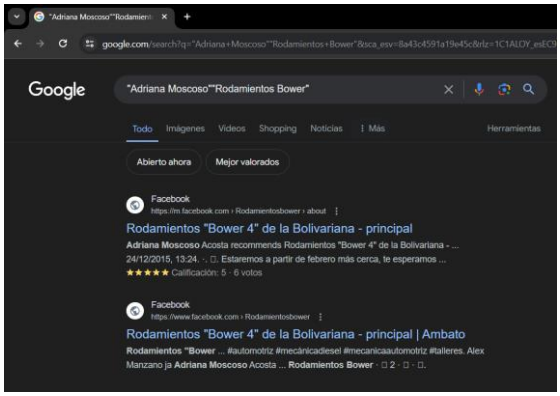
- Facebook

Medio:

- Creación de correo manipulando a la persona, para que entregue voluntariamente el acceso a las cuentas, y después extorsionar, para solicitar dinero, para devolver el acceso

Experimento:
Se usó Google Dorks, para poder comenzar a buscar información

Figura 25. Búsqueda de información de la víctima con Google Dorks



Fuente: elaboración propia

Se logró encontrar una página de Facebook de la cual se obtuvo los siguientes datos:

- Dirección de domicilio
- Número de teléfono fijo: (03) 240-8618
- Correo electrónico: rodamientosbower4@gmail.com

- Otros sitios web: https://www.instagram.com/rodamientosbower4?igsh=ODA1NTc5OTg5Nw%3D%3D
- Número de Celular

Con estos datos se procedió a comprar un chip nuevo y activarlo, para poder comenzar con la interacción con el posible objetivo con la creación de WhatsApp *Business* y cerciorarse de la persona con la que se va a tener interacción, de igual manera la creación de un nuevo correo electrónico

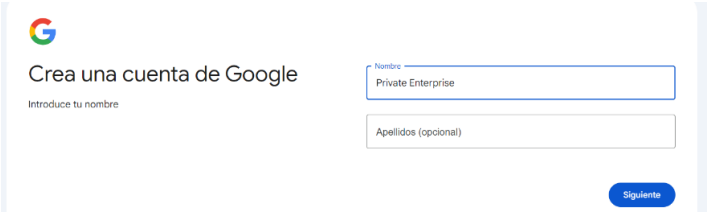
Figura 26. Nuevo número para el experimento

Fuente: elaboración propia

Figura 27. Creación de WhatsApp *Business*

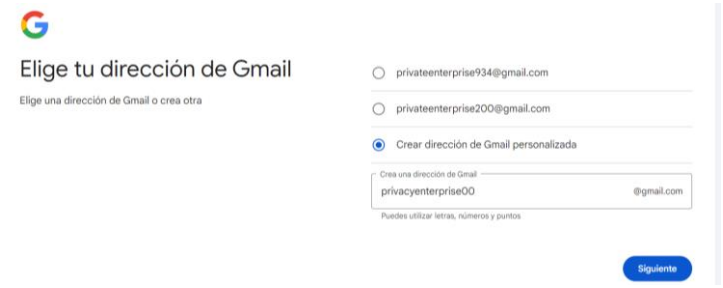
Fuente: elaboración propia

Figura 28. Creación de una cuenta de correo en Gmail



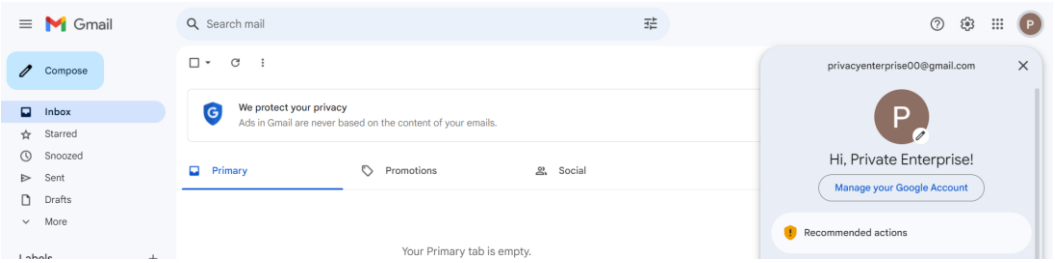
Fuente: elaboración propia

Figura 29. Elección de dirección de correo



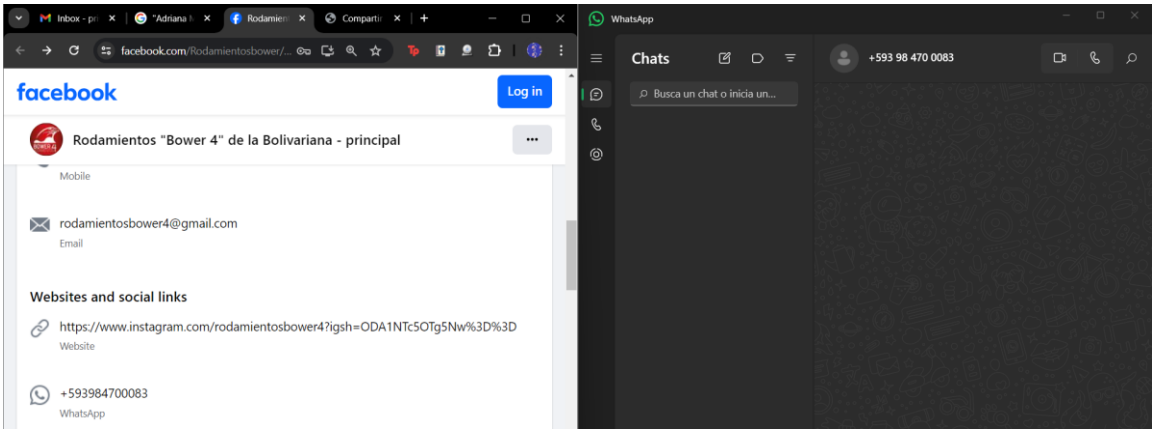
Fuente: elaboración propia

Figura 30. Vista principal del nuevo correo



Fuente: elaboración propia

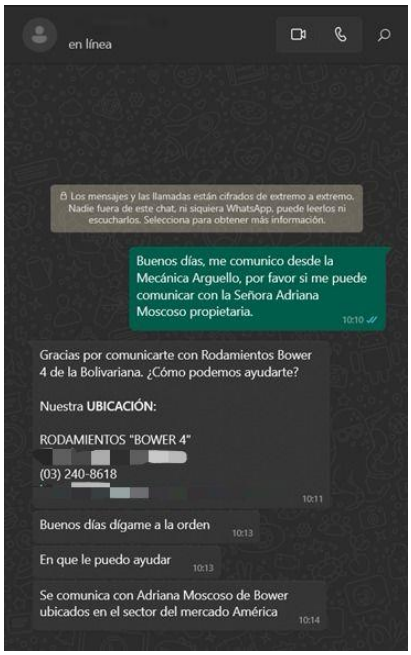
Figura 31. Contacto al número de celular



Fuente: elaboración propia

Dentro de la página de Facebook que se encontró se hizo una investigación de los productos que la empresa vende, y se procede a hacer el contacto con la víctima, para poder crear un vínculo

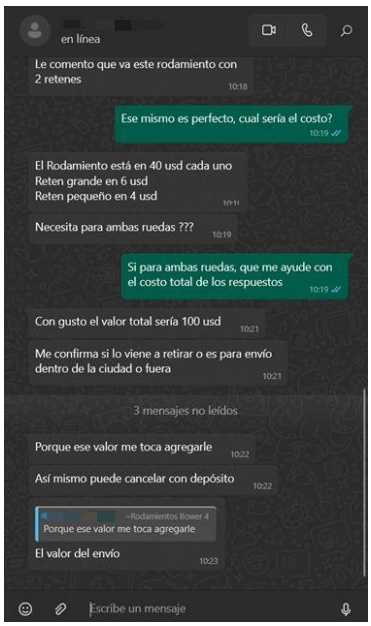
Figura 32. Contacto con la víctima por WhatsApp



Fuente: elaboración propia

Como se puede observar la persona proporción su nombre de manera rápida, con la información de la empresa, se procede a solicitar diferentes repuestos, para obtener información bancaria

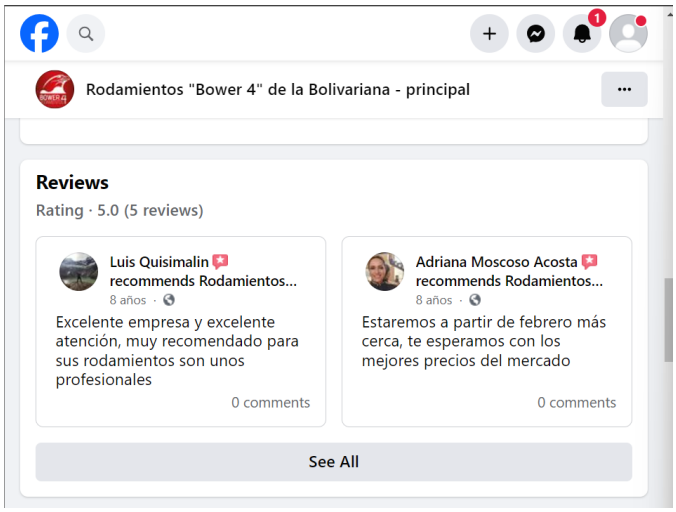
Figura 33. Contacto con la víctima por WhatsApp



Fuente: elaboración propia

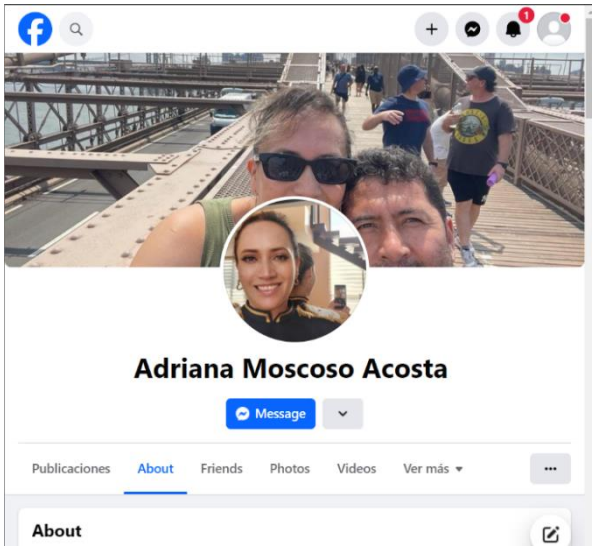
Para poder continuar con la investigación de la víctima, se crea una cuenta de Facebook, con el mismo nombre de la cuenta de WhatsApp. Dentro de esta cuenta, se comienza con la investigación, y se encuentra ya el perfil personal de la Propietaria.

Figura 34. Búsqueda de la persona en Facebook



Fuente: elaboración propia

Figura 35. Investigación de información



Fuente: elaboración propia

La información encontrada de este perfil es la siguiente:

Su segundo apellido es: Acosta

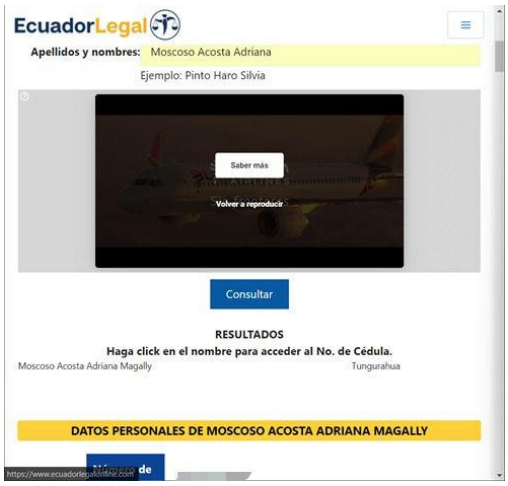
Está casada con: Alex Manzano

Ha estudiado Economía en la UNIANDES – UTPL

Tiene dos hijas

Con el segundo apellido, se procedió a buscar en la página Ecuador Legal, el número de cédula y sus nombres completos, de esta manera se tendrá mucha más información de la víctima

Figura 36. Búsqueda de cédula



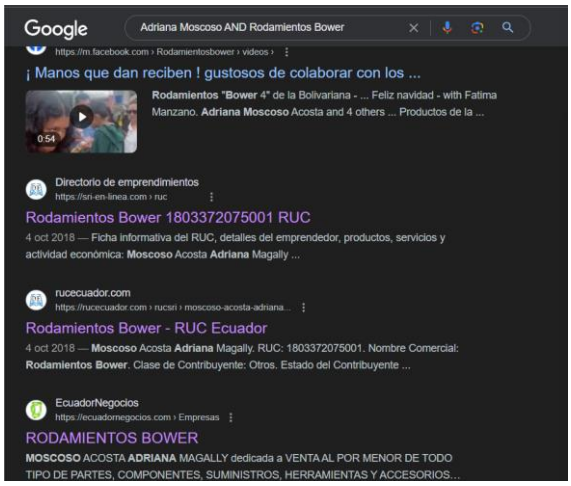
Fuente: elaboración propia

Nombres Completos: Moscoso Acosta Adriana Magally

Número de Cédula: 18XXXXXXXX

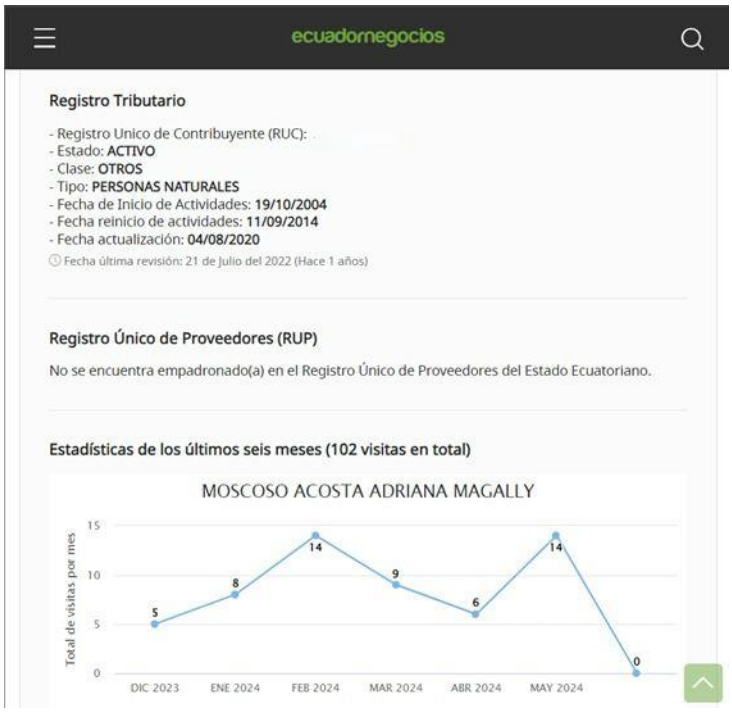
Continuando con Google Docks, se consulta más datos sobre esta persona y estos son los resultados:

Figura 37. Búsqueda de Información con Google Docks



Fuente: elaboración propia

Figura 38. Información encontrada



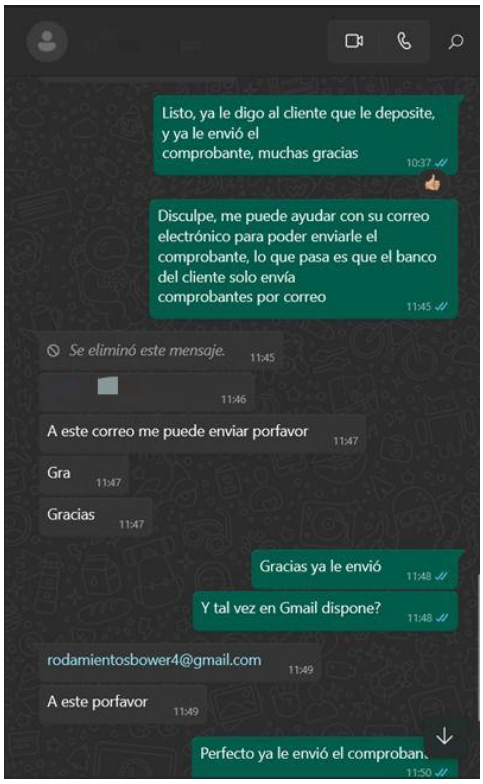
Fuente: elaboración propia

Figura 39. Información encontrada

Fuente: elaboración propia

Para continuar con una campaña de phishing, se va a requerir el correo personal de la víctima, y con los datos anteriormente recolectados, se creó una cuenta de correo en el servicio que tiene que ya proporcionó

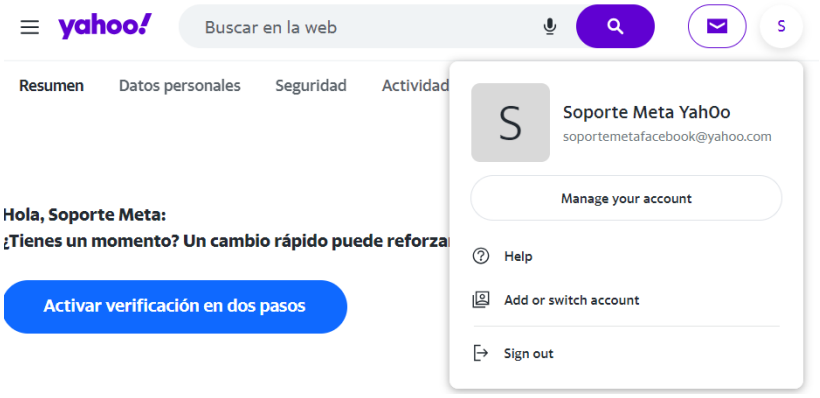
Figura 40. Contacto con la víctima



Fuente: elaboración propia

Se crea una cuenta en *Yahoo*, la cual se va a hacer pasar por soporte técnico de Facebook, ligado con Yahoo, para continuar por otra red con la cual no se ha tenido contacto con la víctima.

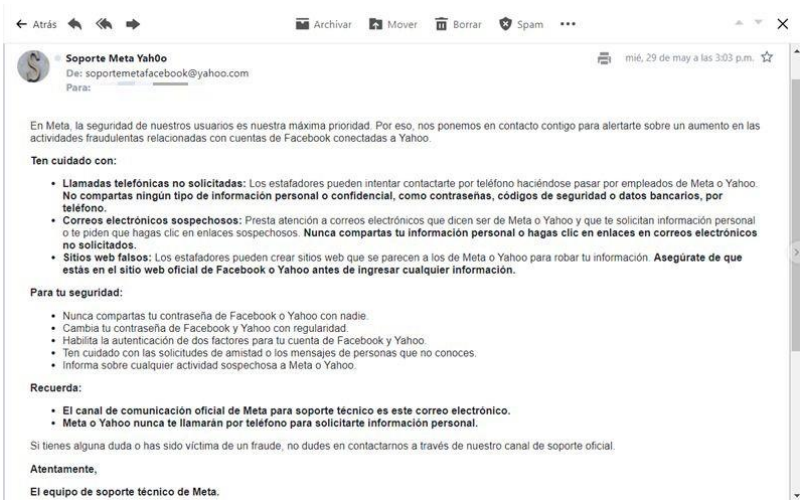
Figura 41. Creación de Correo electrónico en Yahoo



Fuente: elaboración propia

Con el correo electrónico de la víctima se procede a enviar correos para que confíe en esa dirección de correo de a poco, esto mismo durante una semana, para tener constancia.

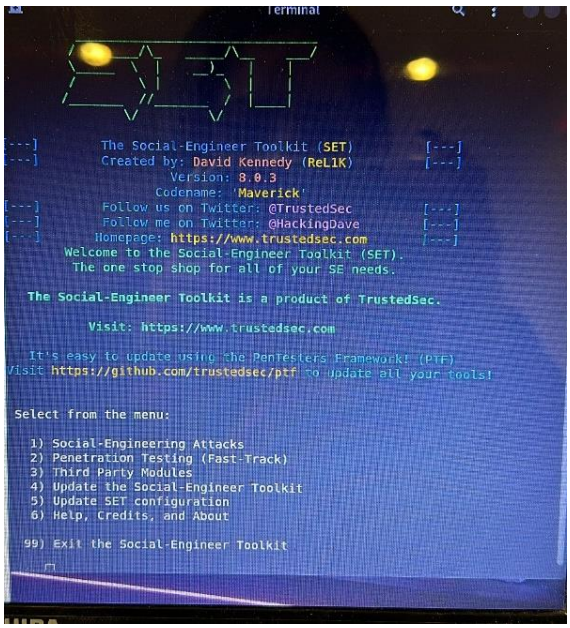
Figura 42. Contacto con la víctima por correo



Fuente: elaboración propia

Ahora continuando con la herramienta *set took kit*, se va a crear un anzuelo, para poder quitarle los accesos a la víctima de su Facebook personal. Se abre la herramienta en una computadora que tenga el sistema operativo de Kali Linux.

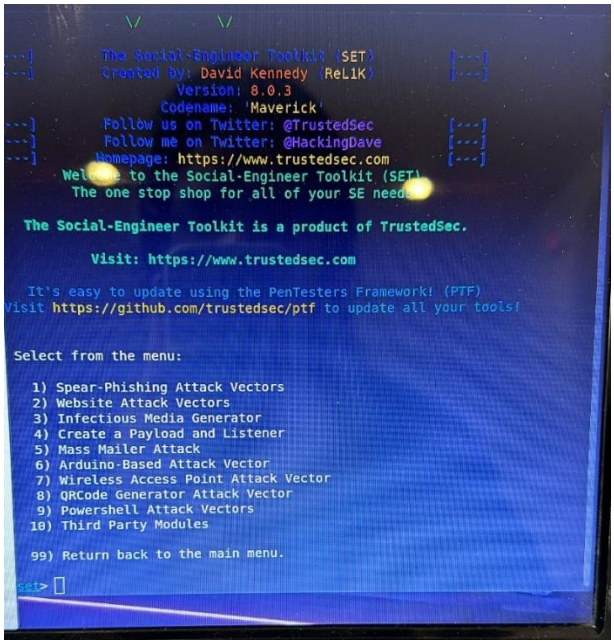
Figura 43. Set Tool Kit primera vista



Fuente: elaboración propia

Se coloca la primera opción que dice *Social Engineering Attacks* para hacer un ataque de ingeniería social, el cual desplegara diferentes opciones que se pueden usar de muchas maneras para vulnerar a las personas.

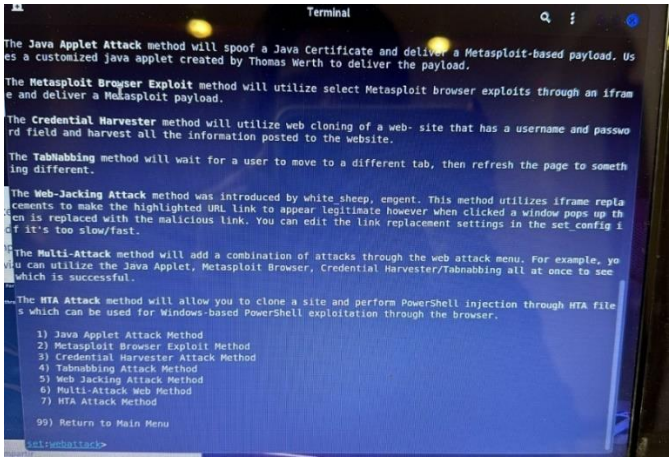
Figura 44. *Set Tool Kit* segundo menú



Fuente: elaboración propia

Una vez desplegado el menú se escoge la opción número dos, que corresponde a *Website Attack* Vector que en español quiere decir, vector de ataque a sitio web, la cual desplegara un menú en la cual se encuentren opciones para atacar sitios web

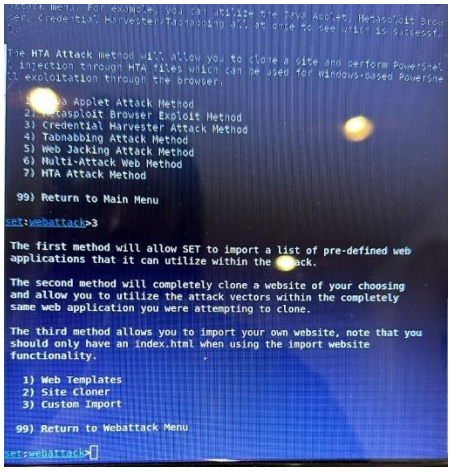
Figura 45. *Set Tool Kit* tercer menú



Fuente: elaboración propia

Después se va a seleccionar la opción número tres, *Credential Harvester Attack Method* o en español, el método de ataque para recolectar credenciales, esta opción lo que va a ser es que va a clonar un sitio web, para de esta manera poder capturar o pescar los datos que la víctima ingrese, como son la contraseña y el correo electrónico.

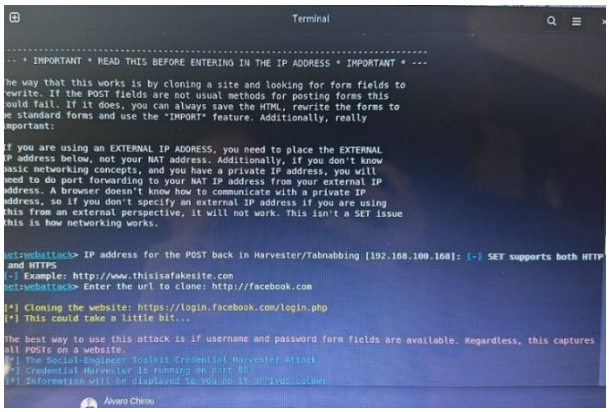
Figura 46. *Set Tool Kit* cuarto menú



Fuente: elaboración propia

Ahora del menú desplegado se va a escoger la opción número 2 "*Site Cloner*" o clonador del sitio, lo que va a hacer esta opción es que va a clonar completamente cualquier sitio web, en este caso Facebook, después de esto se ingresaría la dirección ip del equipo Kali y la dirección del sitio web, que este caso sería: http://facebook.com

Figura 47. Set Tool Kit Clonación de página web



Fuente: elaboración propia

Ahora con la dirección IP la máquina que tiene *Kali Linux* se va a poder hacer que la víctima entre a la página clonada de Facebook, y así poder capturar sus datos personales. Para verificar que el usuario confía en el correo electrónico anteriormente mencionado se va a solicitar que actualice sus datos, como es el número de cédula.

Figura 48. Contacto con la víctima por correo electrónico

Fuente: elaboración propia

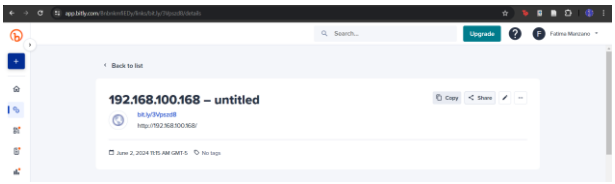
Verificamos que la víctima contestó al correo electrónico correctamente comparando su información y confirmando que confía en la dirección de correo electrónico con la cual se procederá a intentar robar su clave de acceso.

Figura 49. Contestación de la víctima proporcionando datos

Fuente: Elaboración Propia

Ahora sabiendo que la víctima confía en el correo electrónico que se hace pasar por el soporte técnico de Meta, lo que se va a hacer es enviar nuevamente otro correo, pero ahora solicitando que ingrese en el link que se le va a enviar para poder capturar sus datos personales. Se usa esta herramienta para acortar links, y así de esta manera poder enviar a la víctima un link mucho más creíble para que pueda confiar.

Figura 50. Creación del link



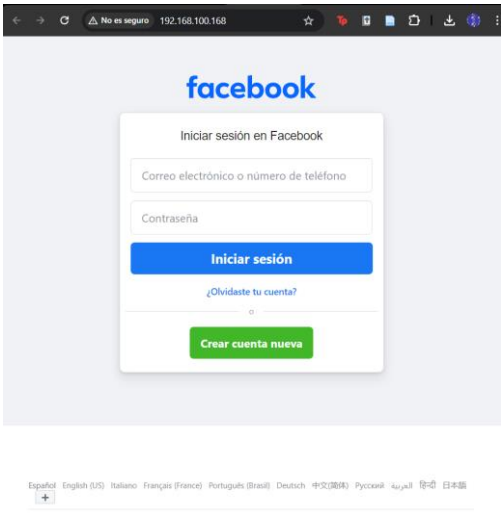
Fuente: elaboración propia

Figura 51. Correo de phishing

Fuente: elaboración propia

El correo que se puede observar en la figura 51, es un ejemplo de correo de *phishing*, al momento de ingresar en el enlace la víctima verá la página que se muestra en la figura 52.

Figura 52. Vista del sitio web clonado

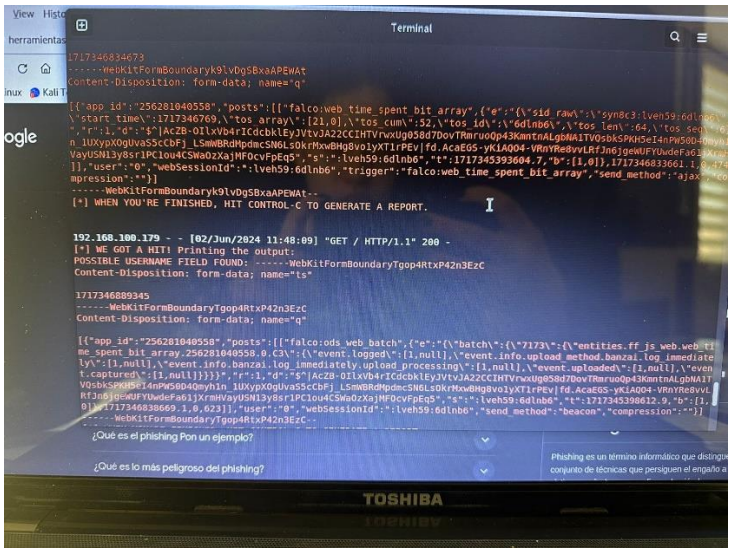


Fuente: elaboración propia

Al momento que la víctima ingresa en el link de la página web clonada, enseguida en la máquina que tiene Kali Linux y está corriendo la herramienta *Set Tool Kit,*

aparecerá una alerta que una persona ingresó, y aparecerá la dirección IP del dispositivo desde el que se ha ingresado, el día y la hora.

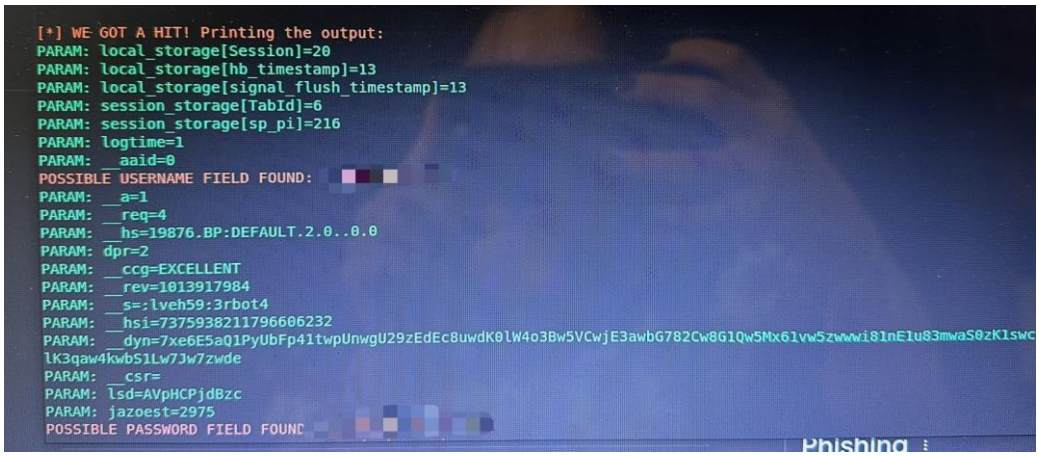
Figura 53. Herramienta *Set Tool Kit*



Fuente: elaboración propia

Después de esto, la herramienta desplegará una lista en la que se encontrará el correo electrónico, como *user name*, y la contraseña de acceso a su cuenta de Facebook personal.

Figura 54. Captura de clave de acceso a Facebook



Fuente: elaboración propia

Una vez terminado el experimento se socializó con la víctima y se le dio a conocer como su correo electrónico y contraseña de acceso a Facebook fueron robados, y se le enseño todos los fallos que ha tenido en este tiempo en el que ha durado, de

igual manera se le regreso la contraseña que proporcionó al sitio web clonado, y se le recomendó que cambiará la contraseña, así como también se le explicó que ninguno de sus datos sería expuesto en el presente trabajo.

Algunos fallos de seguridad fueron encontrados, y se evidencia que la ingeniería social manipula a las personas para poder conseguir su confianza para después poder lograr su cometido que en este caso sería interceptar su acceso personal a la red social, con este acceso posteriormente el ciberdelincuente puede llegar a suplantar la identidad de esta persona y comenzar a solicitar dinero a los contactos de esta misma, o simplemente comenzar a extorsionar a la víctima para que le de dinero, a cambio de devolverle el acceso a su red social personal.

Desarrollo

Al comenzar con la fase de desarrollo, se toma en cuenta el análisis de las encuestas, y las entrevistas, y los diferentes ataques reales de los que se tomó en cuenta para este proyecto, a continuación, se muestra una actualización del tablero, como las tareas a desarrollar en esta fase.

Cuadro 4. Tablero Kanban de la Fase de Desarrollo

TO – DO	DOING	DONE
Consultar la importancia de las guías frente a otras opciones Consultar las partes de una guía de ayuda Consultar sobre el cumplimiento de accesibilidad en personas vulnerables Diseñar el contenido de la guía en base a la información analizada		Analizar los resultados de la encuesta realizada al grupo vulnerable SIL de Tungurahua Analizar las entrevistas a los diferentes expertos en seguridad cibernética e ingeniería social y a la persona encarga del SIL. Buscar bibliografía sobre los ataques de ingeniería social en Ecuador y como denunciarlos Documentar diferentes ejemplos de ataques de ingeniería social reales Documentar una simulación de ataque de ingeniería social

Fuente: elaboración propia

Tarea 1: A diferencia de otras opciones, como manuales o instrucciones, las guías ofrecen ventajas significativas que las hacen fundamentales para el éxito en diferentes entornos de proyectos, algunas de las razones por que las guías son importantes según Moser (2023) son:

1.- Orientación y claridad en la dirección: Las guías brindan una dirección clara y precisa, estableciendo objetivos, pasos y procedimientos específicos a seguir. Esto permite a los usuarios concentrar sus esfuerzos de manera efectiva y evitar confusiones o desviaciones del camino trazado.
2.- Estandarización y coherencia: Las guías fomentan la estandarización y coherencia en la ejecución de tareas o procesos. Al definir un conjunto común de prácticas y criterios, se garantiza la calidad y fiabilidad de los resultados, minimizando la variabilidad y la incertidumbre.

3.- Mejora en la toma de decisiones: Las guías facilitan la toma de decisiones informadas al proporcionar información relevante, análisis y recomendaciones basadas en evidencia y experiencia acumulada. Esto permite a los usuarios tomar decisiones acertadas y bien fundamentadas, optimizando sus acciones y maximizando sus posibilidades de éxito.

4.- Reducción de errores y riesgos: Las guías contribuyen a la reducción de errores y riesgos al establecer protocolos y medidas de seguridad adecuadas. Al seguir las indicaciones de la guía, se minimizan las posibilidades de cometer errores o sufrir accidentes, protegiendo tanto a las personas como a los recursos involucrados.

5.- Eficiencia y ahorro de tiempo: Las guías optimizan el uso del tiempo y los recursos al proporcionar un camino directo y eficiente para alcanzar los objetivos. Al evitar confusiones, redundancias y errores, se agiliza el desarrollo de las actividades y se maximiza la productividad.

6.- Facilidad de uso y accesibilidad: Las guías, ya sea en formato físico o digital, son herramientas accesibles y fáciles de utilizar. Su lenguaje claro, conciso y estructurado permite una comprensión rápida y sencilla, incluso para usuarios con diferentes niveles de conocimiento o experiencia.

7.- Adaptabilidad y versatilidad: Las guías pueden adaptarse a diferentes contextos, necesidades y objetivos específicos. Su flexibilidad permite

personalizarlas y ajustarlas a las circunstancias particulares de cada caso, maximizando su utilidad y aplicabilidad.

8.- Fomento del aprendizaje y la mejora continua: Las guías sirven como instrumentos de aprendizaje y mejora continua al documentar las mejores prácticas y lecciones aprendidas. Al compartir y utilizar estas guías, se promueve el intercambio de conocimientos y la búsqueda constante de la excelencia.

Tarea 2: A pesar de que las guías varían en términos de formato y contenido, suelen tener una estructura básica que facilita su entendimiento y utilización. Los elementos esenciales de una guía según la Universidad de California (2024) son:

- Introducción: Esta sección presenta el tema de la guía, sus metas, alcance y audiencia. Proporciona una visión general del contenido y sitúa al lector en la importancia y pertinencia del tema.

- Desarrollo: El desarrollo constituye la parte fundamental de la guía, donde se detalla el contenido principal de manera organizada y detallada. Puede contener secciones sobre conceptos clave, pasos a seguir, procedimientos específicos, ejemplos, recursos adicionales y referencias bibliográficas.

- Conclusión: La conclusión resume los puntos clave de la guía, reafirma su relevancia y ofrece recomendaciones para su aplicación práctica. Puede incluir un llamado a la acción o invitar a una reflexión sobre el tema abordado.

- Anexos: Los anexos proporcionan información adicional que enriquece el contenido de la guía. Pueden incluir diagramas, tablas, formularios, glosarios, y demás recursos complementarios.

Las guías, con su estructura organizada y sus múltiples ventajas, se convierten en herramientas indispensables para navegar por un mundo complejo y cambiante. Su capacidad para guiar, estandarizar, facilitar la toma de decisiones, reducir riesgos,

optimizar recursos, fomentar el aprendizaje y la mejora continua las convierte en elementos esenciales para el éxito en diversos ámbitos.

Tarea 3: En un mundo cada vez más diverso e inclusivo, resulta esencial que las guías y materiales informativos estén disponibles para todas las personas, independientemente de sus habilidades físicas, sensoriales o cognitivas. Para lograrlo, se emplean diferentes normas y recomendaciones destinadas a garantizar la accesibilidad de la información escrita, con el propósito de hacerla comprensible y útil para todos los usuarios. Según la *World Wide Web Consortium* (2021) enumera algunas de las principales normas de accesibilidad que deben considerarse al redactar una guía enfocada en personas con diversas discapacidades:

1. Claridad y Legibilidad:

Contraste de Colores: Se sugiere utilizar una combinación de colores que garantice un contraste adecuado entre el texto y el fondo, permitiendo una lectura clara para personas con visión limitada o daltonismo.

Tamaño de Letra: Es importante emplear un tamaño de letra lo suficientemente grande para asegurar su legibilidad, teniendo en cuenta las necesidades de personas con problemas de visión. Se recomienda un tamaño mínimo de 12 puntos para el texto normal y 16 puntos para los títulos.

Tipo de Letra: Se aconseja utilizar una tipografía clara y sin adornos excesivos, evitando fuentes con distracciones. Las tipografías como *Arial, Verdana o Tahoma* suelen ser más legibles

Interlineado: Mantener un interlineado adecuado entre las líneas de texto para facilitar su lectura y evitar la fatiga visual. Se recomienda un interlineado de al menos 1,5 veces el tamaño de la letra.

El uso de múltiples colores en una guía accesible puede ser beneficioso para:

• Mejorar la legibilidad.
• Resaltar información clave.
• Crear una experiencia visual agradable.

Sin embargo, es crucial utilizar los colores con precaución para evitar:

• Dificultades de lectura.
• Confusión visual.

2. Estructura y Organización:

Organización Lógica: La guía estaría estructurada de manera coherente y lógica, dividiéndola en secciones claramente identificadas. Se recomienda utilizar encabezados y subtítulos descriptivos para facilitar la navegación.

Lenguaje Sencillo: Se emplearía un lenguaje claro y directo, evitando términos técnicos que puedan resultar difíciles de entender para algunos lectores.

Oraciones Cortas: Es recomendable utilizar oraciones simples y estructuradas de manera sencilla para facilitar la comprensión, especialmente para personas con dificultades de aprendizaje o cognitivas.

3. Recursos Visuales:

Imágenes: Incluir imágenes descriptivas que complementen el texto y faciliten la comprensión de la información. Hay que asegurar que estas imágenes cuenten con descripciones alternativas claras y concisas para personas con discapacidad visual.

Diagramas y Gráficos: Utilizar diagramas y gráficos simples y claros que ilustren conceptos complejos o procesos secuenciales. Asegurarse de que estos elementos

sean accesibles para personas con discapacidad visual mediante la inclusión de descripciones textuales o alternativas.

4. Formato y Extensión:

Formato Digital: La guía debe ofrecerse en un formato digital accesible, como PDF o HTML, para permitir su lectura en diferentes dispositivos y con lectores de pantalla Extensión: Se recomienda limitar la extensión de la guía a lo necesario para transmitir la información de manera clara y concisa, evitando textos demasiado largos o densos que puedan resultar abrumadores para algunos lectores.

5. Compatibilidad con Tecnologías de Asistencia:

Teclado: Es fundamental garantizar que la guía sea navegable y operable únicamente con el teclado, facilitando su uso por personas con movilidad limitada o que utilizan tecnologías de asistencia como teclados adaptados o lectores de pantalla

Lectores de Pantalla: La guía sería compatible con lectores de pantalla, permitiendo que las personas con discapacidad visual accedan a la información mediante la conversión del texto a audio.

Tarea 4: El contenido de la guía se dividirá en secciones de la siguiente forma:

- **Introducción:** En este apartado se le explicará al usuario, sobre los peligros de la era actual digital en la que se vive, y por qué es importante conocer sobre la ingeniería social, y sus estrategias para prevenir.
- **Desarrollo:** Se dividirá en cinco secciones importantes:
    - **Sección 1.**- Definición de ingeniería social
    - **Sección 2.**- Técnicas comunes de ingeniería social
    - **Sección 3.**- Vulnerabilidad en la Población
    - **Sección 4.**- Estrategias de Prevención
        - **4.1.- Conciencia y Educación**

        - Conocer métodos
        - Mantenerse al día de las últimas amenazas
        - Conozca las estafas en las redes sociales
    - **4.2.- Protección Personal**
        - Cuidar la información personal
        - Precaución con correos electrónicos, enlaces y archivos adjuntos
        - Identificar correos electrónicos fraudulentos
        - Proteja sus contraseñas
        - Creación de contraseñas seguras
        - Mantenga su computadora actualizada
    - **4.3.- Vigilancia y Reportes**
        - Supervise mensajes de texto y solicitudes urgentes
        - Evite llamadas telefónicas de números desconocidos
        - Confía en tu intuición
        - Reporta y Denuncia ataques de ingeniería social
    - **4.4.- Protección adicional**
        - Utilice *software* antivirus y antimalware de calidad
        - Permita la autenticación de dos pasos
        - Considere usar una red privada virtual
- **Sección 5.**- Ejemplos de Ataques Reales y Simulación
- **Conclusiones y Recomendaciones**

De igual manera la guía contará con anexos de fotografías e ilustraciones en sus diferentes secciones, para una mejor compresión de la guía en general, revisar el anexo 6 del trabajo, donde se encontrará de forma completa todo el contenido.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Resultados

Los resultados se visualizan en la guía que se encuentra en el anexo número 6, la cual está dentro de la fase de desarrollo del capítulo 2, la guía lleva el nombre de “Blindaje Contra Ataques de Ingeniería Social”.

3.2. Evaluación y validación

Para concluir, la fase de evaluación y validación, al cumplir con las tareas de la fase de desarrollo, se puede dar paso a esta fase, a continuación, se muestra una actualización del tablero, con la tarea a desarrollarse.

Cuadro 5. Tablero Kanban de la Fase de Evaluación y Validación

TO – DO	DOING	DONE
Solicitar a dos profesionales en el área de ciberseguridad que lean la guía y la rúbrica de calificación de esta misma. Realizar los cambios a la guía sugeridos por los expertos Revisar la rúbrica de calificación con la validación de los profesionales		Analizar los resultados de la encuesta realizada al grupo vulnerable SIL de Tungurahua. Analizar las entrevistas a los diferentes expertos en seguridad cibernética e ingeniería social y a la persona encarga del SIL. Buscar bibliografía sobre los ataques de ingeniería social en Ecuador y como denunciarlos. Documentar diferentes ejemplos de ataques de ingeniería social reales Documentar una simulación de ataque de ingeniería social Consultar la importancia de las guías frente a otras opciones Consultar las partes de una guía de ayuda Consultar sobre el cumplimiento de accesibilidad en personas vulnerables. Diseñar el contenido de la guía en base a la información analizada

Fuente: elaboración propia

Tarea 1: Se solicitó a dos profesionales en el tema de Ciberseguridad que hagan una evaluación del contenido de la guía según la rúbrica de calificación, estos mismos fueron:

- Magister Héctor Robayo, analista de TICS de la Gobernación de Tungurahua.
- Magister Verónica Pailiacho, docente de la Escuela de ingenierías de la Pontificia Universidad Católica del Ecuador sede Ambato.

Figura 55. Rubrica de calificación

Rubrica de Calificación

Tipo de Documento: Guía con estrategias para prevenir ingeniería social

Objetivo: Evaluar la accesibilidad, comprensión e integridad de la guía

Instrucciones: Después de haber leído la guía, seleccione una calificación con un visto o una X para marcar cada criterio. Incluya comentarios para justificar su respuesta

Criterio	Descripción	No	En algunos casos	La mayoría de las veces	Siempre
Accesibilidad	¿La guía es accesible para todas las personas?				
Accesibilidad	¿Se utiliza un lenguaje claro y sencillo?				
Accesibilidad	¿Se utilizan imágenes y gráficos con texto alternativo?				
Accesibilidad	¿La guía es compatible con diferentes tecnologías de asistencia?				
Comprensión	¿La guía es fácil de entender?				
Comprensión	¿La información está organizada de forma lógica?				
Comprensión	¿Se utilizan ejemplos y casos prácticos?				
Comprensión	¿El lenguaje es claro y conciso?				
Integridad	¿La guía contiene toda la información necesaria?				
Integridad	¿La guía cubre todos los temas relevantes?				
Integridad	¿La información es precisa y actualizada?				
Integridad	¿La guía proporciona recursos adicionales?				

Fuente: elaboración propia

Tarea 2: Se realizaron todos los cambios que cada uno de los expertos sugirió para que la guía sea un producto accesible, y de fácil compresión para todos los usuarios.

Tarea 3: Como último paso, se va a revisar la rúbrica de la calificación de los profesionales, para realizar la validación final de la guía. Magister Héctor Robayo, analista de TICS de la Gobernación de Tungurahua.

Figura 56. Rubrica de calificación llenada

Rubrica de Calificación

Tipo de Documento: Guía con estrategias para prevenir ingeniería social

Objetivo: Evaluar la accesibilidad, comprensión e integridad de la guía

Instrucciones: Después de haber leído la guía, seleccione una calificación con un visto o una X para marcar cada criterio. Incluya comentarios para justificar su respuesta

Criterio	Descripción	No	En algunos casos	La mayoría de las veces	Siempre
Accesibilidad	¿La guía es accesible para todas las personas?				X
Accesibilidad	¿Se utiliza un lenguaje claro y sencillo?				X
Accesibilidad	¿Se utilizan imágenes y gráficos con texto alternativo?				X
Accesibilidad	¿La guía es compatible con diferentes tecnologías de asistencia?				X
Comprensión	¿La guía es fácil de entender?				X
Comprensión	¿La información está organizada de forma lógica?				X
Comprensión	¿Se utilizan ejemplos y casos prácticos?				X
Comprensión	¿El lenguaje es claro y conciso?				X
Integridad	¿La guía contiene toda la información necesaria?				X
Integridad	¿La guía cubre todos los temas relevantes?				X
Integridad	¿La información es precisa y actualizada?				X
Integridad	¿La guía proporciona recursos adicionales?				X

Fuente: tomado a partir de Robayo (2024)

Figura 57. Rubrica de calificación validada

Pregunta de Evaluación	Comentario Justificativo
¿La guía es accesible para todas las personas?	La guía está diseñada teniendo en cuenta la accesibilidad universal, permitiendo que cualquier persona, independientemente de sus capacidades, pueda entender y aplicar la información proporcionada.
¿Se utiliza un lenguaje claro y sencillo?	El documento utiliza un lenguaje claro y sencillo, evitando tecnicismos innecesarios, lo que facilita la comprensión por parte de todos los usuarios.
¿Se utilizan imágenes y gráficos con texto alternativo?	La guía incluye imágenes y gráficos acompañados de texto alternativo, asegurando que la información visual sea accesible para personas con discapacidades visuales.
¿La guía es compatible con diferentes tecnologías de asistencia?	La guía está optimizada para ser compatible con diversas tecnologías de asistencia, como lectores de pantalla, lo cual garantiza su accesibilidad para usuarios con discapacidades.
¿La guía es fácil de entender?	La estructura y el lenguaje de la guía la hacen fácil de entender, incluso para aquellos que no tienen conocimientos previos sobre el tema.
¿La información está organizada de forma lógica?	La información se presenta de manera lógica y secuencial, facilitando la navegación y comprensión del contenido.
¿Se utilizan ejemplos y casos prácticos?	La guía incluye ejemplos y casos prácticos que ilustran los conceptos, haciendo más fácil su aplicación en situaciones reales.
¿El lenguaje es claro y conciso?	El documento utiliza un lenguaje claro y conciso, evitando redundancias y simplificando la comunicación.
¿La guía contiene toda la información necesaria?	La guía proporciona toda la información necesaria para entender y prevenir ataques de ingeniería social, cubriendo todos los aspectos relevantes del tema.
¿La guía cubre todos los temas relevantes?	Se abordan todos los temas pertinentes relacionados con la ingeniería social, proporcionando un enfoque integral sobre cómo protegerse de estos ataques.
¿La información es precisa y actualizada?	La información es precisa y está actualizada, reflejando las prácticas y conocimientos más recientes en materia de seguridad contra ingeniería social.
¿La guía proporciona recursos adicionales?	La guía incluye recursos adicionales, como referencias, que permiten a los lectores profundizar en el tema.

La guía "BLINDAJE CONTRA ATAQUES DE INGENIERÍA SOCIAL" es un recurso integral y accesible que satisface todos los estándares de evaluación. Gracias a su lenguaje sencillo, la inclusión de ejemplos prácticos y su estructura lógica, se convierte en una referencia valiosa para quienes desean protegerse de los ataques de ingeniería social. Se sugiere emplear esta guía como herramienta de comunicación y formación en el ámbito institucional y empresarial para promover una cultura de seguridad y protección de la información.

HECTOR VLADIMIR ROBAYO VILLARROEL

Firmado digitalmente por HECTOR VLADIMIR ROBAYO VILLARROEL
Fecha: 2024.06.12 14:17:43 -05'00'

Ing. Vladimir Robayo
Analista TI - Gobernación de Tungurahua

Fuente: tomado a partir de Robayo (2024)

Interpretación:

o Los criterios de accesibilidad, compresión e integridad cumplen con todo lo establecido anteriormente.
o Determina el Magister en Ciberseguridad Vladimir Robayo que la guía es un recurso integral y accesible que satisface todos los estándares de evaluación. Y es de fácil compresión para todas las personas.
o La guía está validada por el profesional

- Magister Verónica Pailiacho, docente de la Escuela de ingenierías de la Pontificia Universidad Católica del Ecuador sede Ambato

Figura 58. Rubrica de calificación llenada

Rubrica de Calificación

Tipo de Documento: Guía con estrategias para prevenir ingeniería social

Objetivo: Evaluar la accesibilidad, comprensión e integridad de la guía

Instrucciones: Después de haber leído la guía, seleccione una calificación con un visto o una X para marcar cada criterio. Incluya comentarios para justificar su respuesta

Criterio	Descripción	No	En algunos casos	La mayoría de las veces	Siempre
Accesibilidad	¿La guía es accesible para todas las personas?				X
Accesibilidad	¿Se utiliza un lenguaje claro y sencillo?				X
Accesibilidad	¿Se utilizan imágenes y gráficos con texto alternativo?				X
Accesibilidad	¿La guía es compatible con diferentes tecnologías de asistencia?				X
Comprensión	¿La guía es fácil de entender?				X
Comprensión	¿La información está organizada de forma lógica?				X
Comprensión	¿Se utilizan ejemplos y casos prácticos?				X
Comprensión	¿El lenguaje es claro y conciso?				X
Integridad	¿La guía contiene toda la información necesaria?				X
Integridad	¿La guía cubre todos los temas relevantes?				X
Integridad	¿La información es precisa y actualizada?				X
Integridad	¿La guía proporciona recursos adicionales?				X

Fuente tomado a partir de Pailiacho (2024)

Figura 59. Validación completa

Una vez revisada la guía se ha determinado que cumple con los parámetros accesibilidad, comprensión e integridad de la información.

Mg. Verónica Pailiacho

Directora del Proyecto de Investigación

Contenido digital accesible para la protección de

información personal digital en personas con discapacidad.

Fuente: tomado a partir de Pailiacho (2024)

Interpretación:

- Cada uno de los criterios de accesibilidad, comprensión e integridad están completos dentro de la guía.
- Determina la Magister Verónica Pailiacho que la presente guía cuenta con todas las características de accesibilidad para todas las personas, incluyendo las personas que tengan algún tipo de discapacidad.
- La guía está validada por la profesional.

CONCLUSIONES

- Según la bibliografía revisada y analizada en el proyecto se puede concluir que la ingeniería social se ha consolidado como una de las técnicas más efectivas para vulnerar la seguridad de las organizaciones. El *phishing*, el *vishing* y la suplantación de identidad son las técnicas de ingeniería social más comunes que los diferentes autores citados anteriormente concuerdan. Cada una de estas estrategias utiliza diferentes aspectos de la interacción humana para recopilar datos confidenciales.

- Según el experimento que se realizó, las personas tienen diferentes niveles de vulnerabilidad a los ataques de ingeniería social. El ataque simulado, como los correos de phishing, lograron recopilar datos confidenciales. Los hallazgos muestran que los emprendedores carecen de capacitación y conciencia sobre temas de seguridad informática, lo que los hace vulnerables a los atacantes. La recopilación de datos demostró que los métodos que aprovechaban la falta de procedimientos de verificación de identidad y el desconocimiento de protocolos de seguridad básicos fueron los más efectivos.

- La prevención de estos ataques depende de la educación y concientización de los usuarios, la implementación de políticas de seguridad, y la difusión de los ataques más comunes que usan los ciberdelincuentes, son algunas de las estrategias que se lograron encontrar en la investigación previa. Se ha creado una guía detallada que aborda los problemas de vulnerabilidad más importantes que se descubrieron durante las pruebas. Esta misma cumple con los requerimientos de accesibilidad, para las personas con discapacidad, en base a la investigación previa.

RECOMENDACIONES

- Crear y llevar a cabo programas de capacitación periódicos para enseñar a los empresarios técnicas de ingeniería social y medidas preventivas. Para mejorar la capacidad de respuesta y la resistencia a los ataques, estos programas incorporarían simulaciones de ataques.

- Crear y hacer cumplir políticas de seguridad claras que incluyan verificación de identidad, autenticación de solicitudes de información y administración de contraseñas. Es necesario revisar y actualizar periódicamente estas políticas para adaptarlas a nuevas amenazas.

- Invierta en tecnologías de seguridad que ayuden a detectar y detener ataques de ingeniería social. El software de detección de phishing, los filtros de correo electrónico avanzados y los sistemas de autenticación pueden ser parte de esto.

- Crear una cultura en la organización que valore la seguridad de los datos. Esto implica no sólo capacitación y políticas, sino también liderazgo y creación de un entorno donde los emprendedores se sientan empoderados y responsables de proteger sus propios datos y los de la organización.

- Implementar un sistema de seguimiento continuo para evaluar la efectividad de las estrategias de prevención y realizar las modificaciones necesarias. Esto incluye realizar auditorías de seguridad periódicas y actualizar guías de prevención en respuesta a nuevas amenazas detectadas.

BIBLIOGRAFÍA

Anderson, R. (2013). Measuring the Cost of Cybercrime. *Springer EBooks*, 265–300. Obtenido de https://bit.ly/3R4eI8A

Arriaga, L. (2018). Revista Digital INESEM. Obtenido de Qué es Kanban, el método de moda para desarrollar proyectos de éxito. Obtenido de https://bit.ly/4biQ6lv

BID. (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Obtenido de https://bit.ly/4cBKxzA

Departamento de Seguridad de las TIC. Delitos informáticos en ECUADOR. Policía Nacional del Ecuador. Obtenido de https://bit.ly/3UFZdpd

Escuela Europea de Negocios (2020). 10 mejores Prácticas de ciberseguridad para las organizaciones. Obtenido de https://bit.ly/3vVVprw

Garcés, E., Pailiacho V. (2020). Kanban como herramienta de gestión para actividades en grupos de investigación informáticos. Puce Ibarra. Obtenido de https://bit.ly/3SV9Ipu

García, G. (2022). Delitos Informáticos en Ecuador. Notimundo.

García, J. (2019). Estudio de metodologías de ingeniería social. Uoc.edu. Obtenido de https://bit.ly/3vDlGLc

Gil, L. (2022). Estudio de los ataques y su defensa en la Ingeniería Social. Uned.es; Universidad Nacional de Educación a Distancia (España). Escuela Técnica Superior de Ingeniería Informática. Departamento de Sistemas de Comunicación y Control. Obtenido de https://bit.ly/4aK0sKJ

Grande, C., Guadrón, R. (2015). Ingeniería Social: El Ataque Silencioso. Repositorio Digital de la Ciencia y Cultura de El Salvador REDICCES. Obtenido de https://bit.ly/4autwW8

Gómez, K. (2017). Ingeniería Social, sus repercusiones y recomendaciones. Policia.gob.ec; Policía Nacional del Ecuador. Obtenido de https://bit.ly/3IYaNGR

Hinojosa, G. (2010). Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del Ecuador. *Uisek.edu.ec*. Obtenido de https://bit.ly/3uJUjOFbi

Moser, G., Stevens, G. (2023). The how-to guide to writing and publishing a book. CreateSpace Independent Publishing Platform.

Núñez, P. (2023). APLICACIÓN DE LA NORMA NTE INEN-ISO_IEC 40500 EN CONTENIDO DIGITAL DE INGENIERÍA SOCIAL. Repositorio PUCESA. Obtenido de https://bit.ly/3vSxzNF

Olic, A. (2015). Kanban: A Quick and Easy Guide to Kickstart Yor Project.

Otero, A. (2018). Enfoques de Investigación. Universidad del Atlántico. Obtenido de https://bit.ly/3Qrva3p

Oviedo Santillán, M. I., & López Parra, M. F. (2019). Vista de Una aproximación a lo cualitativo: identificando las creencias de la compartición de conocimiento en las comunidades de práctica | Estudios de la Gestión: Revista Internacional de Administración. UNIVERSIDAD ANDINA SIMÓN BOLÍVAR, Sede Ecuador. Obtenido de https://bit.ly/3UDqzxs

Paesini, M., Stucher V. (2017). Ingeniería Social, el arte de engañar. *lua.edu.ar.* Obtenido de https://bit.ly/3PSQ1wb

Policía Nacional del Ecuador (2015) Delitos informáticos o ciberdelitos. Obtenido de https://bit.ly/3WGO22o

Prado, J. (2021). Ingeniería social, un ejemplo práctico. *Revista ODIGOS*. Obtenido de https://bit.ly/4acMIbG

Rosero, L. (2021). El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático. Ups.edu.ec. Obtenido de https://bit.ly/3U7RIZ8

Sancho, C. (2023). Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro. *MQRinvestigar.* Obtenido de *https://bit.ly/4cQmrS7*

Universidad de California, Berkeley. (2024). Writing effective guides. Obtenido de https://bit.ly/4bXtcjN

Urrutia, J., Hernández, G. (2022). Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil. Ug.edu.ec. Obtenido de https://bit.ly/3PNb1EI

Web Content Accessibility Guidelines (WCAG) 2.1. (2021). Obtenido de https://bit.ly/3K3VP2x

ANEXOS

Anexo N°1. Entrevista a Mercedes Santana Analista

<table>
<tr><td colspan="2">  </td></tr>
<tr><td colspan="2">Entrevista realizada a Mercedes Santana psicóloga analista promotora laboral del SIL de Tungurahua.</td></tr>
<tr><td>Objetivo</td><td>Obtener información inicial del SIL de Tungurahua, saber cuál es el nivel de conocimiento de la analista promotora sobre ingeniería social y que medidas tiene para prevenir este problema.</td></tr>
<tr><td>Entrevistada</td><td>Psic. Mercedes Santana
Analista promotora laboral del SIL de Tungurahua.</td></tr>
<tr><td colspan="2">Consideraciones Generales
Solicitar información que se considere relevante para el inicio del desarrollo del proyecto.</td></tr>
<tr><td colspan="2">Desarrollo:

¿Cuál es el número de emprendedores que trabajan con usted, y con cuantas personas podría trabajar mi persona?
Actualmente cuento con 20 emprendedores en total que están dentro del SIL, y yo le puedo ayudar con el contacto de 10 personas, para su encuesta.

¿Han recibido alguna capacitación sobre ciberseguridad?
No he recibido.</td></tr>
</table>

¿Conoce de las estafas y suplantaciones de identidad que existen en redes sociales?

Si conozco.

Cada cuanto está acostumbrada a cambiar la contraseña de acceso personal a sus redes

No me gusta cambiar mis contraseñas, porque me olvido.

¿Cuánta información personal suya pueden encontrar en su perfil de trabajo?

El número de celular y la dirección de la oficina.

¿Sabe cómo reconocer cuando un correo electrónico es auténtico, o falsificado?

No se reconocer.

¿Conoce sobre algún problema de ciberseguridad con los emprendedores que trabajan con usted?

En emprendedores no, pero si en otras personas.

Ha tenido algún problema sobre que clonan sus perfiles o estafas

No, pero a otras personas si conozco.

Anexo N°2. Entrevista a Héctor Robayo

<table>
<tr><td colspan="2"> 
Pontificia Universidad Católica del Ecuador | Sede Ambato</td></tr>
<tr><td colspan="2">Entrevista realizada a Héctor Robayo magister en ciberseguridad, analista de TICS de la Gobernación de Tungurahua.</td></tr>
<tr><td>Objetivo</td><td>Obtener información sobre ciberseguridad, recopilada de un profesional en el tema.</td></tr>
<tr><td>Entrevistado</td><td>Mg. Héctor Vladimir, analista de TICS de la Gobernación de Tungurahua.</td></tr>
<tr><td colspan="2">Consideraciones Generales
Solicitar información de un profesional, para recopilar datos, más técnicos para el desarrollo del proyecto</td></tr>
<tr><td colspan="2">Desarrollo:
¿Cuáles considera que son las técnicas de ingeniería social más comúnmente utilizadas por los ciberdelincuentes en la actualidad?
Phising.

¿Qué tipos de ataques de ingeniería social son más frecuentes en entornos empresariales?
Phising.

¿Cuáles son los principales riesgos y consecuencias asociados con los ataques de ingeniería social para los grupos vulnerables?
Perdida de información - obtención de datos personales.</td></tr>
</table>

¿Qué medidas o estrategias considera más efectivas para prevenir los ataques de ingeniería social en grupos vulnerables?
Capacitación - firewall - antivirus _ políticas Alta.

¿Cómo puede adaptarse la capacitación en ciberseguridad para satisfacer las necesidades específicas de grupos vulnerables?
Capacitación permanente desde el ingreso y permanencia de los grupos vulnerables en la empresa.

¿Cuál es la importancia de establecer políticas y procedimientos internos para prevenir los ataques de ingeniería social en organizaciones?
Alta para evitar ataques y reducir riesgos

¿Conoce cuáles son los pasos para denunciar un ataque de ciberseguridad en Ecuador - Ambato?
No.

¿Qué papel juegan las redes sociales en la ejecución de ataques de ingeniería social y cómo pueden protegerse los usuarios?
Es un punto u objetivo en el cual los ciber atacantes lo ven como vulnerables.

¿Qué medidas de seguridad adicionales pueden implementarse en los entornos de trabajo remoto para proteger a los empleados contra los ataques de ingeniería social?
Capacitación antivirus políticas.

¿Cómo pueden las organizaciones evaluar su nivel de vulnerabilidad frente a los ataques de ingeniería social y qué acciones pueden tomar para mejorar su seguridad?
Mediante auditorias periódicos controles permanentes.

Anexo N°3. Entrevista a Liliana Mena

<table>
<tr><td colspan="2"> 
Pontificia Universidad Católica del Ecuador | Sede Ambato</td></tr>
<tr><td colspan="2">Entrevista realizada a Liliana Mena magister en ciberseguridad, coordinadora del programa de maestrías en ciberseguridad de la PUCESA.</td></tr>
<tr><td>Objetivo</td><td>Obtener información sobre ciberseguridad, recopilada de un profesional en el tema.</td></tr>
<tr><td>Entrevistada</td><td>Mg. Liliana Mena, coordinadora del programa de maestrías en ciberseguridad de la PUCESA.</td></tr>
<tr><td colspan="2">Consideraciones Generales
Solicitar información de un profesional, para recopilar datos, más técnicos para el desarrollo del proyecto</td></tr>
</table>

Desarrollo:

¿Cuáles considera que son las técnicas de ingeniería social más comúnmente utilizadas por los ciberdelincuentes en la actualidad?
Dentro de las técnicas creo que las más comunes son el *phishing* a través de mensajes, el *vishing* a través de llamadas telefónicas.

¿Qué tipos de ataques de ingeniería social son más frecuentes en entornos empresariales?
De igual forma el phishing más.
¿Cuáles son los principales riesgos y consecuencias asociados con los ataques de ingeniería social para los grupos vulnerables?
Cuando hablamos de grupos vulnerables, como me decía el tema usted, que tenían discapacidades, ya dependería, porque en el caso del *vishing* que son llamadas telefónicas, o de pronto también los mensajes que le indica que ha ganado un premio, o que ingrese en algún enlace. El robo de información personal, confidencial, también está de pronto el mal uso de esa información que pueden hacer otras personas, por ejemplo, si es de datos, una cuenta bancaria, pueden hacer un mal uso y robar el dinero.

¿Qué medidas o estrategias considera más efectivas para prevenir los ataques de ingeniería social en grupos vulnerables?
Yo creo que sería en parte la concientización a las personas acerca de los riesgos que se expone cuando están navegando en internet, o en la red, el no compartir información personal en redes sociales, en sitios públicos, porque también a partir de eso vendrían a ser debilidades, para apropiarse de la información. El uso también inapropiado de las contraseñas, a veces no resguardamos bien las contraseñas o ponemos contraseñas fáciles de adivinar.

¿Cómo puede adaptarse la capacitación en ciberseguridad para satisfacer las necesidades específicas de grupos vulnerables?
Yo pienso que tendría que hacerse un estudio de acuerdo con el tipo de discapacidad porque hay algunos que usan, por ejemplo, para navegar por

internet, tiene ciertos avisos, que sea visible con texto e imágenes, para que se pueda ir leyendo en el caso que usen otro tipo de lenguajes, deberían adaptarse de acuerdo con el tipo de discapacidad.

¿Cuál es la importancia de establecer políticas y procedimientos internos para prevenir los ataques de ingeniería social en organizaciones?

Es muy importante, porque, a partir de las políticas y de aplicar las normativas, entonces ya las instituciones van a tener enfoques desde donde actuar, por ejemplo, ya en la misma política, le diría como formular la contraseña, o aspectos de a qué información le da acceso, los roles que le dan.

¿Conoce cuáles son los pasos para denunciar un ataque de ciberseguridad en Ecuador - Ambato?

No, de lo que se escucha es que roban información, y que muchas personas hacen la denuncia y no dan el debido seguimiento, se reforzaría por parte del estado.

¿Qué papel juegan las redes sociales en la ejecución de ataques de ingeniería social y cómo pueden protegerse los usuarios?

Es un papel muy importante, porque la mayoría de las personas maneja redes sociales, pero no tienen los debidos cuidados, de ese aspecto se daría más información, mayor socialización de los peligros a los que están expuestos, dentro de las redes sociales. Nosotros mismos exponemos mucha información, tener más cuidado al momento de publicar, y ser más reservados, usar la autenticación en doble factor

.

¿Qué medidas de seguridad adicionales pueden implementarse en los entornos de trabajo remoto para proteger a los empleados contra los ataques de ingeniería social?

La red VPN, si les da un cierto grado de seguridad, claro que no podemos decir que al 100%, siempre hay un margen de error, la recomendación sería siempre trabajar, usando sitios seguros el https, siempre verificando que este navegando por sitios seguros.

¿Cómo pueden las organizaciones evaluar su nivel de vulnerabilidad frente a los ataques de ingeniería social y qué acciones pueden tomar para mejorar su seguridad?

Hay diferentes herramientas, las que se pueden usar, por ejemplo, una que se llama Set, hay también otra herramienta que es Tool Kit, claro que primero para esto hay que hacer el análisis de riesgos para poder saber cuáles son, previo a esto un inventario que compone la red, para ver el equipo que tiene mayor riesgo de sufrir algún tipo de ataque, en base al inventario de los equipos

Anexo N°4. Encuesta a emprendedores del SIL de Tungurahua.

<table>
<tr><td colspan="2">  </td></tr>
<tr><td colspan="2">Encuesta realizada a 12 emprendedores que se encuentran dentro del programa del SIL de Tungurahua</td></tr>
<tr><td>Objetivo</td><td>Obtener datos sobre el conocimiento de los emprendedores del SIL en cuanto a ciberseguridad.</td></tr>
<tr><td>Encuestados</td><td>Doce personas, pertenecientes al programa del SIL de Tungurahua.</td></tr>
<tr><td colspan="2">Consideraciones Generales
Analizar los resultados, para conocer el nivel de conocimiento de los emprendedores. La encuesta tiene preguntas abiertas y cerradas.</td></tr>
<tr><td colspan="2">Desarrollo:

¿Ha sido víctima de algún tipo de estafa en línea en el pasado?
Sí
No

¿Ha sido víctima o conoce a alguien que haya pasado por alguna de las siguientes situaciones?
Clonación de perfil en redes sociales
Correo electrónico fraudulento
Extorción por llamada telefónica
Robo de datos bancarios</td></tr>
</table>

Ninguna de las anteriores

¿Qué medidas tomas habitualmente para proteger tu información personal y financiera en línea? en caso de no tomar ninguna medida colocar (NINGUNA)

_____

¿Ha recibido capacitación sobre cómo prevenir ataques de ingeniería social?

Si

No

¿Está al tanto de los pasos a seguir en caso de ser víctima de algún tipo de estafa en la web?

Sí, estoy totalmente informado

Tengo una idea general

No, no estoy informado

En caso de ser víctima, ¿Sabe cómo denunciar este hecho a las autoridades?

Si

No

¿Utilizas medidas adicionales de seguridad, como la autenticación de dos pasos, en tus dispositivos electrónicos?

Si

No

¿Has recibido correos electrónicos o mensajes sospechosos solicitando información personal o financiera?

Sí, con frecuencia

Sí, ocasionalmente

No

¿Consideras importante que las instituciones educativas incluyan formación sobre seguridad en línea y prevención de estafas en sus programas?

Sí, es crucial
Sí, pero no es prioritario
No estoy seguro

¿Crees que sería obligatoria la capacitación sobre medidas de prevención contra cualquier tipo de ataque?

_____

Anexo N°5. Permiso para realizar ataque de ingeniería social

<table>
<tr><td colspan="2">  </td></tr>
<tr><td colspan="2">Solicitud para realizar una simulación de un ataque de ingeniería social a la Sra. Adriana Moscoso</td></tr>
<tr><td>Objetivo</td><td>Simular un ataque de ingeniería social, a una emprendedora, para ver el nivel de conocimiento de ciberseguridad y usar las herramientas previamente investigadas.</td></tr>
<tr><td>Víctima</td><td>Sra. Adriana Moscoso, propietaria de Rodamientos Bower 4</td></tr>
<tr><td colspan="2">Consideraciones Generales
Solicitar permiso a la propietaria de Rodamientos Bower 4, para poder realizar una simulación de ataque de ingeniería social.</td></tr>
<tr><td colspan="2">Desarrollo:</td></tr>
</table>

Sra. Adriana Moscoso
Propietaria
Rodamientos Bower 4

Estimada Sra. Moscoso:
Mi nombre es Fátima Manzano y soy estudiante de la carrera de Tecnologías de la Información en la Pontificia Universidad Católica del Ecuador, sede Ambato. Actualmente, me encuentro desarrollando mi tesis titulada "Herramientas de ingeniería social y estrategias para su prevención". Este trabajo tiene como objetivo investigar y analizar diversas técnicas de ingeniería social y proponer una guía con estrategias efectivas para prevenir estos ataques en organizaciones.

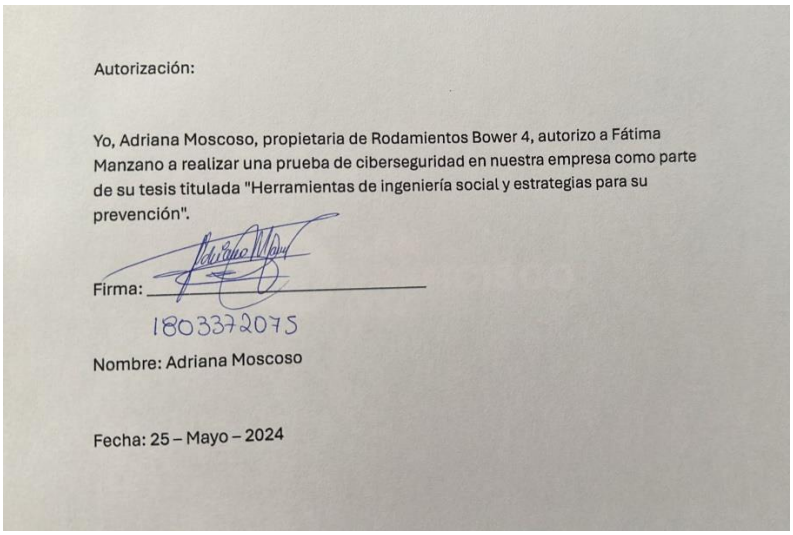
Con este propósito, estoy realizando un experimento que implica pruebas de ciberseguridad enfocadas en la ingeniería social. Me dirijo a usted para solicitar su autorización para llevar a cabo una prueba de ciberseguridad en su empresa, Rodamientos Bower 4. La prueba está diseñada para evaluar la efectividad de las medidas de seguridad actuales frente a posibles ataques de ingeniería social y no causará ninguna interrupción en las operaciones de su empresa ni comprometerá la integridad de los datos o sistemas.

La información obtenida durante esta prueba será tratada con la máxima confidencialidad y será utilizada exclusivamente para fines académicos. Al finalizar la tesis, se le proporcionará un informe detallado con los resultados de la prueba y una guía con estrategias recomendadas para fortalecer la seguridad contra ataques de ingeniería social en su empresa.

Agradezco de antemano su atención y espero contar con su valiosa cooperación para el desarrollo de esta investigación.

Atentamente,

Fátima Manzano



Autorización:

Yo, Adriana Moscoso, propietaria de Rodamientos Bower 4, autorizo a Fátima Manzano a realizar una prueba de ciberseguridad en nuestra empresa como parte de su tesis titulada "Herramientas de ingeniería social y estrategias para su prevención".

Firma: _____

1803372075

Nombre: Adriana Moscoso

Fecha: 25 – Mayo – 2024

Anexo N°6. Guía

<table>
<tr><td colspan="2"> 
Pontificia Universidad Católica del Ecuador | Sede Ambato</td></tr>
<tr><td colspan="2">Guía final llamada “Blindaje contra ataques de Ingeniería Social” la cual contiene definiciones, estrategias, ejemplos de ataques de ingeniería social, simulación de ataque y recomendaciones para protección.</td></tr>
<tr><td>Objetivo</td><td>Desarrollar una guía de ayuda para todas las personas, y que sea accesible para las personas con discapacidad, para protegerse contra ataques de ingeniería social.</td></tr>
<tr><td colspan="2">Consideraciones Generales
Dividir la información encontrada durante toda la investigación, para obtener una guía que sirva para prevenir los ataques de ingeniería social.</td></tr>
<tr><td colspan="2">Desarrollo:</td></tr>
</table>