# INSTITUTO SUPERIOR TECNOLÓGICO SAN ANTONIO

**Escuela de Ciberseguridad**

# CONCIENCIACIÓN EN CIBERSEGURIDAD MEDIANTE SIMULACIONES DE INGENIERÍA SOCIAL: UN ENFOQUE PRÁCTICO Y ÉTICO

**Pablo Sebastián Jarrin Cazco**

**Ciberseguridad**

Trabajo de fin de carrera presentado como requisito

para la obtención del título de

**Tecnólogo Superior en Ciberseguridad**

**Quito, 10 de julio de 2025**

# INSTITUTO SUPERIOR TECNOLÓGICO SAN ANTONIO

**Escuela de ciberseguridad**

## HOJA DE CALIFICACIÓN
## DE TRABAJO DE FIN DE CARRERA

# Concienciación en ciberseguridad mediante simulaciones de ingeniería social: un enfoque práctico y ético

**Pablo Sebastián Jarrin Cazco**

**SANTIAGO ROJAS BUKOVAC, Ing. Informático, Mg. en Sistemas Informáticos Educativos**

**Quito, 10 de julio de 2025**

# DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales del Instituto Superior Tecnológico San Antonio TESA, incluyendo la Política de propiedad Intelectual TESA, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a TESA para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Nombres y apellidos: Pablo Sebastián Jarrin Cazco

Código estudiante: 2086

Cédula de identidad: 1720622131

Lugar y fecha: Quito, 01 de mayo del 2025

# ACLARACIÓN PARA PUBLICACIÓN

**Nota:** El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, pese a estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en ttp://bit.ly/COPETheses.

# UNPUBLISHED DOCUMENT

**Note:** The following capstone project is available through Instituto Superior Tecnológico San Antonio TESA institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

# DEDICATORIA

A Dios, por su guía ininterrumpida en cada fase de mi existencia.

A mis padres, por su amor incondicional, sus sacrificios y el modelo de perseverancia que me han inculcado.

A mis hermanos gran motor de vida.

Al Instituto TESA y a cada profesor por cada aporte en mi día a día como estudiante.

# AGRADECIMIENTO

Le expreso mi más profundo agradecimiento al Instituto Superior Tecnológico San Antonio y a todos los docentes de la Escuela de Ciberseguridad, por su guía, compromiso con la excelencia académica y su respaldo a lo largo de mi formación como profesional.

A mi familia, por su paciencia, y su apoyo incondicional.

Finalmente, expreso mi gratitud a mis amigos y compañeros, quienes con sus palabras de ánimo y colaboración han contribuido a que este proceso sea culminado con éxito.

# RESUMEN

En este estudio se analiza la efectividad de las simulaciones de ingeniería social como recurso educativo para mejorar la sensibilización en ciberseguridad. Desde que se reconoce que el elemento humano es una de las debilidades principales en los espacios digitales, la investigación sugiere que las actividades prácticas favorecen un aprendizaje más profundo ante posibles riesgos. Se realizaron pruebas de suplantación de identidad a un grupo de participantes, además de encuestas, entrevistas y sesiones de grupo. Según los resultados, se observa disparidad entre la preparación previa de los encuestados y su habilidad real para reaccionar, así como un aumento en su nivel de comprensión tras finalizar su intervención. Además, se observaron distintos tipos de comportamiento, lo que indica la importancia de ajustar las tácticas de enseñanza.

El estudio demuestra que las simulaciones controladas resultan eficaces y pueden ser reproducidas en diversos entornos educativos y empresariales, convirtiéndose en un recurso ético y útil para promover la conciencia de seguridad digital.

**Palabras Clave**

Ingeniería social, seguridad cibernética, simulaciones, concienciación digital, phishing, smishing, vishing, enseñanza vivencial, factor humano y formación en ciberseguridad.

# ABSTRACT

This study analyzes the effectiveness of social engineering simulations as an educational resource to improve cybersecurity awareness. Since the human element is recognized as a major weakness in digital spaces, the research suggests that hands-on activities promote deeper learning in the face of potential risks. Impersonation tests were conducted on a group of participants, in addition to surveys, interviews and group sessions.

According to the results, a disparity was observed between the respondents' prior preparation and their actual ability to react, as well as an increase in their level of understanding after the end of their intervention. In addition, different types of behavior were observed, indicating the importance of adjusting teaching tactics.

The study demonstrates that controlled simulations are effective and can be replicated in various educational and business settings, becoming an ethical and useful resource for promoting digital security awareness.

Keywords.

Social engineering, cybersecurity, simulations, digital awareness, phishing, smishing, vishing, experiential learning, human factor and cybersecurity training.

CAPÍTULO I INTRODUCCIÓN ..... **¡Error! Marcador no definido.**

1.1. Planteamiento del Problema ..... **¡Error! Marcador no definido.**

1.2. Justificación ..... **¡Error! Marcador no definido.**

1.3. Alcance ..... **¡Error! Marcador no definido.**

1.4. Objetivos General y Específicos ..... **¡Error! Marcador no definido.**

CAPÍTULO II: MARCO TEÓRICO ..... 10

2.1. Fundamentos de la Ciberseguridad ..... **¡Error! Marcador no definido.**

2.2. Ingeniería Social ..... **¡Error! Marcador no definido.**

2.3. Concienciación en Seguridad Informática ... **¡Error! Marcador no definido.**

2.4. Simulación como Herramienta Pedagógica . **¡Error! Marcador no definido.**

2.5. Modelos o Teorías Relevantes ..... **¡Error! Marcador no definido.**

2.6. Antecedentes Investigativos Recientes ..... **¡Error! Marcador no definido.**

CAPÍTULO III MARCO METODOLÓGICO ..... 24

3.1. Tipo de investigación ..... **¡Error! Marcador no definido.**

3.2. Enfoque ..... **¡Error! Marcador no definido.**

3.3. Herramientas metodológicas ..... **¡Error! Marcador no definido.**

3.4. Técnicas ..... **¡Error! Marcador no definido.**

3.5. Estudios iniciales ..... **¡Error! Marcador no definido.**

3.6. Desarrollo ..... **¡Error! Marcador no definido.**

CAPÍTULO IV RESULTADOS Y DISCUSIÓN ..... 24

4.1. Presentación general de los datos ..... **¡Error! Marcador no definido.**

4.2. Análisis por tipo de técnica aplicada .....**¡Error! Marcador no definido.**

4.3. Análisis de perfiles de comportamiento.....**¡Error! Marcador no definido.**

4.3.1. Perfil reactivo.....35

4.3.2. Perfil evasivo .....35

4.3.3. Perfil reflexivo .....36

4.4. Comparación entre percepción previa y aprendizaje posterior.....37

4.5. Impacto emocional percibido y disposición al aprendizaje .....39

4.6. Discusión comparativa con literatura reciente.....42

4.7. Implicaciones para la formación en ciberseguridad.....**¡Error! Marcador no definido.**

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES.....47

5.1. Conclusiones.....**¡Error! Marcador no definido.**

5.2. Recomendaciones .....**¡Error! Marcador no definido.**

Referencias.....54

Bibliografía .....56

# CAPITULO I. INTRODUCCIÓN

## 1.1 Declaración del problema

La digitalización ha conectado rápidamente a personas, dispositivos y servicios y los ha interconectado. Pero tales avances han creado nuevos vectores de ataque que han sido explotados por actores inescrupulosos. En la actualidad las amenazas digitales no se limitan únicamente a fallas en los sistemas o programas, también puede involucrar el comportamiento o las acciones humanas ya que las personas pueden ser incentivadas o manipuladas para cometer acciones tontas o descuidadas. Por tal motivo es que la ingeniería social se ha convertido en una de las tácticas más preferidas por los cibercriminales ya que ellos buscan la manera de aprovechar el desconocimiento de las personas, sus debilidades psicológicas, o falta de información para lograr comprometer la seguridad de un sistema, red o datos.

La ingeniería social posee varias estrategias que pueden ser utilizados para engañar, persuadir o manipular a una persona para que exponga toda la información personal o privada que ellos requieran, bajo supuestos falsos permitiéndole al atacante acceder a información confidencial falsas o proporcione al atacante acceso a información confidencial. Entre estas técnicas o métodos que los atacantes utilizan es la confianza, urgencia, miedo, incluso ofreciendo beneficios para provocar reacción inmediata en las posibles víctimas. Algunos de los tipos de ataques más comunes son el phishing, smishing, vishing, baiting, y pretexting, entre otros, y cada vez todos estos se han ido perfeccionado, provocando que sean más difíciles de detectar (ENISA, 2023).

A través de los años también se han ido desarrollando soluciones tecnológicas con la finalidad de apoyar a los sistemas de ciberseguridad, entre estas una herramienta que está en apogeo es la inteligencia atificial que puede ser utilizada también para detectar amenazas,

generar una autenticación más fuerte, cifrado de extremo a extremo, etc., por lo que se puede decir que los humanos siguen siendo el punto más débil, debido a que puede ser influenciado fácilmente. Algunos estudios recientes muestran que debido a errores humanos se han producido hasta el 74% de las violaciones y por ende que la ingeniería social es uno de los ataques más utilizados (Verizon, 2023). Este hallazgo demuestra una disparidad preocupante entre las competencias técnicas disponibles y la disposición del usuario típico para combatir las explotaciones de ingeniería social.

Además, estudios de ámbito académico han indicado que los cursos de capacitación en ciberseguridad tradicional son relativamente contraproducentes a menos que estén acompañados de demostraciones de casos reales o simulaciones prácticas. La falta de experiencia práctica conduce a una falsa sensación de seguridad tanto para empleados como usuarios, y a un aumento en la vulnerabilidad al engaño. La capacitación simulada y repetitiva frecuentemente lleva a un aumento en la conciencia y practicar la respuesta a agresiones sociales generalmente es crucial (Moghimi & Varadharajan, 2022).

Un problema importante es que muchas organizaciones, especialmente en los países en desarrollo o sectores de bajo presupuesto, no tienen políticas claras para estar al tanto de la seguridad digital. A menudo, la capacitación en ciberseguridad no es el proceso de incorporación más importante, ni su efectividad medida en campañas informativas. Esto expone a los usuarios tanto en el ámbito profesional como personal y los hace susceptibles a diversas formas de cibercrimen como fraude, extorsión digital, robo de identidad, etc. (IBM, 2023).

El impacto de los ataques de ingeniería social es aún más severo en el escenario de fomentar el uso extensivo de herramientas tecnológicas sin proporcionar suficiente orientación para combatir sus riesgos. Los sitios de redes sociales, entre otros, se han convertido en una plataforma codiciada para el ciberdelito y quienes pueden descubrir

fácilmente las preferencias, hábitos diarios, lugares favoritos, y conexiones sociales y profesionales de sus víctimas. Este conocimiento es luego utilizado para crear mensajes infectados de tal manera que parecen ser enviados desde canales confiables, con el objetivo de aumentar la probabilidad de éxito del ciberataque (Oliveira et al., 2021).

Por lo tanto, el principal desafío en esta investigación no es la existencia de ataques de ingeniería social; es la incapacidad de los usuarios para identificar y reaccionar adecuadamente a los riesgos de seguridad en general. Esta deficiencia no solo pone en peligro los sistemas con los que trabajan, sino que también conduce a una cultura del error humano que desencadena ataques sofisticados.

En este contexto, el estudio indica la importancia de evaluar la integración de simulaciones de ingeniería social como un instrumento pedagógico para mejorar la percepción del riesgo, las habilidades de pensamiento crítico y la respuesta a escenarios puntuales. La hipótesis de la investigación se basa en la conjetura de que los ejercicios prácticos, realizados bajo un enfoque ético y controlado, apoyan la identificación de vulnerabilidades cognitivas y representan fundamentos axiomáticos para un aprendizaje relevante en el área de la ciberseguridad.

### 1.2 Justificación

En la sociedad actual, se han ido desarrollando distintos técnicas o métodos que vulneran la seguridad y privacidad de los usuarios de herramientas informáticas modernos, por lo que se ha visto la necesidad de incrementar o mejorar los niveles de seguridad computacional, que ahora es un requisito en todos los sectores de actividad. Actualmente se puede observar el gran progreso y avance de diversas tecnologías, en donde las organizaciones, o distintos usuarios se encuentran expuestos a varios tipos de amenazas, en donde no están comprometidos únicamente los sistemas, sino que están dictados por el comportamiento humano. Como resultado de lo anterior la ingeniería social se convierte en

un factor muy importante y de alto riesgo, el cual la tecnología no puede resolverlo por sí mismo, por esta razón es importante educar a los consumidores a tener más conciencia y ser más críticos a la hora de tomar decisiones al encontrarse en este tipo de situaciones.

En virtud de este contexto, se ve a este proyecto como un recurso que promueve y motiva la implementación de estrategias educativas que pueden considerarse más dinámicas o didácticas ya que pueden acercarse la realidad y el tipo de manipulación digitar que puede ser utilizada para acceder o violentar su seguridad cibernética. En el presente existen varias investigaciones las cuales mencionan que las estrategias tradicionales, que solo dependen de discursos o avisos visuales, no pueden impactar en el comportamiento de los usuarios de manera profunda o persistente. Mientras que el uso de recursos considerados como didácticos o interactivos que consiste en realizar simulaciones de amenazas reales, siempre y cuando se lo realice de manera adecuada y controlada con la finalidad de generar aprendizaejes de forma dinámica. Permitiendo que estas interacciones generen una mayor comprensión de los distintos riesgos y a su vez sea más fácil para las personas detectarlos y puedan protegerse y generar comportamientos de transmisión segura (Moghimi & Varadharajan, 2022).

Por consiguiente, la actual investigación, busca ofrecer una perspectiva diferente y de manera practica sobre un problema que genera riesgos y efectos negativos a nivel mundial. Cuando se analizó la eficiencia de la realización de dichas simulaciones de ingeniería social, se observó que se logró impactar y concientizar a los usuarios, ayudándolos a tener un pensamiento más crítico, por consiguiente, se puede recomendar que estas prácticas sean aprovechadas por el sector educativo, público y privado, y el Estado, y en campañas o políticas de capacitación, que es muy importante en países emergentes como el Ecuador donde no se puede observar que se implemente de forma adecuada la ciberseguridad en la educación de ciudadanos y trabajadores.

Lo que podría ayudar a mejorar las respuestas o reacciones de los usuarios que se encuentren en una situación de amenazas (hipotética) logrando analizar en tiempo real, la situación a las que se encuentren expuesto y así obtener más información que aporte con nuevos valores a la investigación de la ciberseguridad. Este análisis realizado en tiempo real podría ayudarnos a reconocer cuales son las falencias o debilidades de la conciencia sobre el riesgo al que están expuestos los usuarios en cuanto a revelación de sus datos, y a su vez se podría determinar cuáles son los patrones de comportamiento más comunes y que técnicas de prevención y concientización pueden ser utilizadas de una manera más especifica o personalizada. Un ejemplo, al revisar el correo electrónico debemos revisar detenidamente y observar los elementos de phishing que se encuentren presentes como un nombre real, logotipos reales o mensajes urgentes, podemos entrenar para la realidad y el tipo de atención que recibe (Oliveira et al., 2021).

**Criterios éticos**

El presente estudio ha sido desarrollado, siguiendo principios éticos respetando a cada uno de los participantes, guardando absoluta confidencialidad de los datos que fueron brindados por los mismos, obteniendo su consentimiento, informando que no serán expuestos a ningún tipo de riesgo o daño. Por lo que las simulaciones son realizadas únicamente con fines educativos y bajo una estricta vigilancia metodológica, evitando que se genere algún tipo de respuesta negativa o impacto psicológico en los participantes debido a la naturaleza de la información que es delicada. Esto es fundamental practicarlo durante los ejercicios para que estos puedan ser útiles y cumplir con el objetivo deseado y a su vez no provoquen desconfianza o daño alguno a los participantes.

Otro factor que tiene una gran relevancia en esta investigación es el alcance del mismo en cuanto a la educación, y que su enfoque puede expandirse o se puede buscar una mayor profundidad en el tema. Estos enfoques pueden adaptarse a otros entornos sociales que

actualmente carecen de protocolos de seguridad digital efectivos. El desarrollo de un protocolo (para simular conciencia y evaluar) puede servir como base para políticas institucionales de ciberseguridad en el futuro.

Cabe destacar la relevancia, utilidad, valor académico y social, así como su justificación preventiva, ética y pedagógica de estas investigaciones, en resumen. En un mundo donde las herramientas no son suficientes para derrotar a los ciberataques por sí solas, es obligatorio aumentar la conciencia y el pensamiento crítico de los usuarios, convirtiéndose en la línea de defensa contra la ingeniería social.

### 1.3 Alcance

La tesis pone énfasis en el área de conciencia sobre la seguridad informática en un contexto humano, restringida a la evaluación cualitativa de simulaciones de ingeniería social como instrumentos de conciencia contra las amenazas digitales. La investigación llega en un momento en que es necesario determinar y explicar las variables psicológicas, cognitivas y conductuales que ayudan a moderar cómo las personas reaccionan a los ataques basados en lo social. La evaluación involucraría solo métodos cualitativos, específicamente:

Punto final de comportamiento replicable inmediato: demostración por parte de los participantes ante estímulos simulados. Entrevistas semiestructuradas postratamiento centradas en la percepción del riesgo, el entendimiento de la amenaza y los resultados de aprendizaje. Discusiones en grupo focal, donde sea apropiado, para fomentar la reflexión mutua y recopilar resultados mejorados a través de experiencias anotadas. La investigación omite medidas automáticas y técnicas analíticas, porque el principal interés no es el valor de un sistema sino cómo los sujetos interpretan, sienten y actúan frente a situaciones de manipulación social.

No es un estudio exhaustivo en el sentido clásico, que pueda ayudar a los docentes a realizar amplias descripciones o decisiones, sino que es exploratorio y formativo, diseñado

para encontrar tendencias, sentido común y oportunidades de mejora para futuras capacitaciones. Cualquier aspecto técnico que no sea una actividad de inteligencia/reconocimiento como una auditoría de infraestructura de red, desarrollo de herramientas defensivas o análisis de vulnerabilidades queda fuera del alcance.

Como resultado final, se producirá un informe cualitativo integral que refleje los hallazgos obtenidos de las experiencias simuladas junto con conclusiones y propuestas de educación para la mejora de la cultura de seguridad digital desde una perspectiva humanista. Dicho recurso podría representar la base para el diseño de estrategias de capacitación transferidas a situaciones similares.

### 1.4. Objetivos generales y específicos

**Objetivo General:**

Evaluar la efectividad de los ataques de ingeniería social simulados en entornos controlados como una herramienta de aprendizaje para mejorar la conciencia de seguridad informática y la respuesta entre los usuarios.

**Objetivos específicos:**

1. Describir los métodos de ingeniería social más comúnmente utilizados en la era cibernética actual.
2. Crear y llevar a cabo simulaciones de ataques de ingeniería social dirigidas contra una población usuaria específica.
3. Analizar las respuestas elaboradas a partir de solicitudes de información sensible.
4. Recomendar enfoques y metodologías desde el dominio de la ciberseguridad.

# CAPÍTULO II: MARCO TEÓRICO

## 2.1 Fundamentos de la Ciberseguridad

La ciberseguridad abarca medidas, sistemas y procesos que protegen la confidencialidad, integridad y disponibilidad de la información digital. Su principal objetivo es rechazar intentos peligrosos de alterar la seguridad del ordenador o acceder a datos privados de varios usuarios.

Los tres pilares de la protección de la información son la privacidad, la integridad y la disponibilidad. Estos se conocen también como el triángulo CIA ((Universidad Politécnica de Cartagena, s. f.; Ruiz, 2024).

Proteger la privacidad de los datos es muy importante para que la información sensible no sea vista por personas no autorizadas. A su vez los datos invernadero son considerados como datos sagrados, por eso es importante que no se permita y se restrinja el acceso no autorizado o la manipulación de los datos que han sido almacenados. Pero también es clave que los sistemas y datos estén disponibles permanentemente para los usuarios brindándoles una mayor seguridad de que puedan acceder a los mismos siempre que les sea necesario.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) hace referencia a la diversidad de amenazas digitales y de acuerdo con su información evidencian que existen ataques de ransomware que son de alto grado que promueven un notable nivel de desinformación sofisticada, haciéndose evidente la necesidad de aplicar una red de seguridad cibernética robusta, adaptable y flexible (ENISA, 2023). En la actualidad los tipos de amenazas cibernéticas han ido incrementando notoriamente, por lo que varias organizaciones han visto la necesidad de adoptar nuevas prácticas en el manejo de su información y políticas o protocolos de seguridad mucho más estrictos. Lo que es crucial para que puedan proteger la

información confidencial dentro de las organizaciones y puedan accionar rápidamente en caso de que se encuentren expuestos ante algún tipo de riesgo cibernético, resguardando la seguridad de sus datos sensibles y críticos, asegurando su integridad, confidencialidad y disponibilidad.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) destaca que las amenazas digitales son variadas y, como ellos mismos dicen, van desde ataques de ransomware muy graves hasta desinformación compleja. Esto resalta la necesidad de tener una ciberseguridad que sea sólida, flexible y que se adapte a diferentes situaciones (ENISA, 2023).

### 2.2 Ingeniería Social

Es el uso de técnicas para manipular a las personas con el fin de obtener información o acceso a sistemas. A menudo se basa en la confianza y el engaño. Los atacantes pueden hacerse pasar por alguien de confianza o crear situaciones que hagan que las personas den información sensible sin darse cuenta. Es importante estar alerta y protegerse de estos tipos de engaños.

En cambio, la ingeniería social no requiere conocimientos técnicos avanzados; su enfoque está en el comportamiento psicológico de las personas a las que afecta.

Los criminales buscan conseguir información personal o entrar en tecnología personal engañando a la víctima, aprovechándose de su confianza o de su falta de conocimiento. A diferencia de otras violaciones que explotan fallos en la seguridad del software o hardware, la ingeniería social se centra en la persona, su comportamiento, la confianza y la presión (Proofpoint, 2023).

Las tres técnicas más comunes utilizadas para este tipo de lavado de cerebro son la persuasión, el engaño y el uso de un mensaje muy organizado para provocar una reacción inmediata.

como bancos o servicios web conocidos, como Google o Facebook. Estos son hechos para que el usuario entregue de forma voluntaria la contraseña, el número de tarjeta o cualquier información delicada si el remitente parece confiable. Los atacantes cuidan todos los detalles: logotipos, estilo, mensajes atractivos, para que el engaño no se pueda notar. En este caso, el usuario debe ser crítico y estar alerta ante cualquier pedido inesperado de datos personales.

Aunque es menos usado fácil, sobre todo porque cumplir con los requisitos de prueba suele ser más complicado, este tipo de ataque sigue siendo efectivo, especialmente cuando el hablante logra transmitir una impresión de urgencia o autoridad.El vishing se manifiesta a través de llamadas telefónicas. El estafador finge ser un empleado del gobierno e intenta presionar a la víctima para que dé información personal.

El individuo recibe un mensaje de texto a través de móvil (SMS) con una dirección URL o texto perturbador, con el objetivo de instigar la autolesión u otra actividad. La lucha contra tal fraude exige inicialmente un sentido crítico y un nivel mínimo de capacitación en relación con dichos riesgos.En el smishing, se sigue el mismo enfoque, pero se lleva a cabo mediante mensajes de texto. La persona recibe un mensaje de texto en su móvil (SMS) con una URL o un texto inquietante, para incitarlos a autolesionarse o a hacer otra actividad. Al publicar o responder, el usuario corre el riesgo de mostrar información que puede ser usada en su contra. Para combatir este fraude, primero se necesita un sentido crítico y un mínimo de entrenamiento sobre estos riesgos.

## 2.3 Conciencia sobre Ciberseguridad

La concienciación y sensibilidad sobre la seguridad de la información y la difusión del conocimiento sobre la seguridad de la información implica realizar actividades para enseñar a los usuarios sobre las amenazas que un usuario puede enfrentar en línea y de esta forma darle las habilidades necesarias para mantenerse alerta a los riesgos.

Capacitaciones recurrentes sobre ciberseguridad podría ser útil para reducir errores de los empleados de empresas. Cada vez existen distintas amenazas que son utilizadas en línea, por lo que es importante estar atento a estos cambios y realizar capacitaciones en ciberseguridad de manera continua con la finalidad de poder hacer frente a las tácticas de manipulación que pueden utilizar los atacantes en línea (Cabezas-Molina & Fiallos-Aguilar, 2024).

"Es importante que las organizaciones realicen programas constantes de concientización y capacitación para sus colaboradores, e incluso implementen ejercicios de Phishing o diferentes pruebas en las que estén expuestos a un riesgo que pueda ocurrir en la vida real, para que puedan generar conciencia y a su vez conocer maneras de protegerse y reconocer en caso de que estén expuestos a algún tipo de ataque cibernético". Todo esto con la finalidad de garantizar la seguridad de los empleados y a su vez estos sean capaces de mitigar los riesgos a los que se encuentran en línea (Rahartomo et al., 2025).

### 2.4 Modelado de Enseñanza

Se promueve un método que puede ser considerado más didáctico, y al ser practico a diferencia de los métodos tradicionales de enseñanza, puede ser relevante para mejorar las reacciones, habilidades de los usuarios mediante en análisis de la situación y brindándoles herramientas que les ayuden a enfrentar con mayor seguridad cuando se encuentren expuestos a este tipo de amenazas. (ENISA, 2023). Al nosotros poder recrear simulaciones de ciberataques, estamos dando la oportunidad a los demás usuarios de elementos digitales la oportunidad de aprender y entrenarse en ciberseguridad. Es importante recalcar que no se puede simular un ciberataque de manera muy realista debido a la naturaleza de la información y por respeto a los participantes, pero aun así se puede diseñar distintos entornos o situaciones semejantes a la vida real, exponiendo los riesgos del mundo digital, con la

finalidad de que se pueda aprender o practicar distintas habilidades como la identificación, respuesta, acción, en otras palabras se podría ayudar a fomentar una estrategia de acción simple en caso de riesgo.

Muchas veces los usuarios aprenden las de la experiencia, por lo que pueden entender mejor el riesgo y los efectos de un ataque siempre que se encuentren expuestos a una amenaza por lo importante que estas simulaciones sean realizadas en un entorno controlado, donde no estén expuestos a amenazas reales.

También es importante que exista diversos métodos de aprendizaje, un método que puede ser útil es hacer simulaciones a través de los juegos, es decir que mediante esta dinámica se pueda simular una situación que no es un juego, esto es importante realizarlo ya que mejora la atención, la participación, y los motiva más, llevando a obtener mejores resultados en su capacitación. Este método se ha utilizado con éxito en diferentes sistemas educativos y en la formación de empresas (Nespoli, Albaladejo-González, Ruipérez-Valiente y García-Alfaro, 2024).

### 2.5 Modelos o Teorías Relevantes

El marco de concienciación sobre ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) es una guía clara y organizada sobre cómo crear un programa de formación en concienciación sobre la seguridad de la información. Con el apoyo de las mejores prácticas y los marcos globalmente reconocidos, se ha vuelto un recurso esencial para aumentar la seguridad en las organizaciones.

La relevancia esta en que es importante que se tenga una formación continua en cuanto a ciberseguridad o prevención de sus riesgos y amenazas ya que esta última esta en cambio constante, siempre aparecen nuevas formas o métodos que atentan con nuestra seguridad cibernética. (Bazalar, 2023).

Icek Ajzen dice que la Teoría del Comportamiento Planificado sostiene que la persona se comportara de una forma determinada dependiendo de que actitud tenga para realizar ese comportamiento, también va a depender de las normas impuestas en su entorno o en la sociedad, o incluso del control que tenga sobre ese comportamiento. Dicha teoría es muy estudiada en la psicología y puede ser una herramienta que pueda ayudar a entender y facilitar la predicción del comportamiento que va a tener una persona ante diferentes situaciones.

### 2.6 Antecedentes Recientes en Investigación

Existen investigaciones recientes en donde se ha demostrado la eficiencia y la importancia de la simulación como un método o herramienta que facilita el aprendizaje y fortalece los conocimientos en ciberseguridad. Por ejemplo, según Oliveira, et al., (2021) mediante su investigación donde realizo distintas dinámicas de simulación de phishing, demostró que las personas que participaron en dichas actividades disminuyeron su susceptibilidad ante ataques reales. Gracias a este estudio es que se ve la importancia y la necesidad de que se promueva una educación continua en ciberseguridad o seguridad de la información, con el objetivo de limitar la exposición de los usuarios de internet o medios digitales a los distintos peligros que encontramos en línea.

En contraste otro estudio señala la trascendencia de que se pueda tener acceso a una capacitación continua y es de suma importancia que sea flexible con la intención de generar un mayor entendimiento y efectividad en cuanto a estos esfuerzos realizados para la concientización (Cabezas-Molina & Fiallos-Aguilar, 2024).

# CAPÍTULO III MARCO METODOLÓGICO

## 3.1 Tipo de investigacion

Esta tesis se basado en un estudio aplicado y exploratorio que busca evaluar el potencial valor de las simulaciones de ingeniería social como una herramienta de concienciación en ciberseguridad. Las investigaciones aplicadas transfieren el conocimiento teórico a contextos prácticos y su carácter exploratorio se justifica por la necesidad de entender los comportamientos en un entorno de ataque simulado y controlado, donde no tenemos precedentes de comportamientos predecibles (Hernández, 2021).

Además, se configura como una investigación de campo porque se realiza con 20 usuarios en un entorno realista donde se pueden ejecutar situaciones controladas para medir su reacción ante ataques de ingenieria social.

## 3.2 Enfoque

El estudio actual sigue un enfoque cualitativo, con el objetivo de tener una perspectiva mas a fondo en las actitudes, respuestas cognitivas y que percibieron los usuarios encuestados hacia las amenazas simuladas. De esta manera, esta metodología ayudara no sólo a visibilizar comportamientos, procesos de inetrpretacion y significados que los usuarios atribuyen a los eventos experimentales.

La elección de esta metodología cualitativa se justifica por la naturaleza del objeto de estudio: el comportamiento humano frente a amenazas digitales no puede medirse únicamente con números cuantitativos, sino que debe interpretarse en contexto. Aspectos importantes en la generación de estrategias educativas efectivas (Creswell, 2018).

## 3.3 Herramientas Metodológicas

También se utilizarán instrumentos enfocados en la interacción del usuario para recopilar datos en ambos entornos controlados.

Aquí simulamos solo ataques de phishing, ya que el correo electrónico se difunde desde el servidor al receptor y se utiliza para falsificar comunicaciones genuinas. Estos se personalizaron de manera que tuviera sentido, incluyendo el uso de logotipos de instituciones reales, nombres que las víctimas reconocerían y situaciones habituales que provocan un sentido de urgencia o pánico, como alertas de seguridad informática o mensajes bancarios. Este enfoque metódico reflejó la importancia dada al phishing como uno de los métodos de ataque más populares utilizados en todo el mundo y la posibilidad práctica y ética de implementarlo en un entorno de laboratorio. Otras técnicas de ingeniería social como el smishing o el vishing no formaron parte de la simulación, tanto por razones técnicas como por problemas de seguimiento.

Instrumentos que facilitan la recopilación de datos ricos y contextuales, que acceden a dimensiones que no se expresan comúnmente en evaluaciones cuantitativas, incluirán:

Guías de observación: herramientas para apoyar la codificación de comportamientos discretos mientras los usuarios interactúan con los escenarios simulados.

Guías de entrevistas semiestructuradas post-simulación: utilizadas tras la simulación para evaluar percepciones, sentimientos, decisiones y conciencia del riesgo.

Grupos focales: utilizados cuando es viable en el entorno del estudio, con el objetivo de fomentar la reflexión grupal y la triangulación de datos.

### 3.4 Técnicas

Los procedimientos primordiales empleados serán:Las entrevistas semiestructuradas que facilitan la adquisición de un entendimiento más profundo sobre las experiencias auténticas de los usuarios, su estado de conciencia, la conciencia del riesgo y su percepción del proceso de aprendizaje.

El análisis temático de discusión se empleará con el objetivo de organizar e interpretar las respuestas de los participantes, con el fin de identificar patrones

comunes, diferencias y emociones asociadas, así como el grado de conciencia inducido por estos.

Estos métodos constituyen una estrategia integrada de investigación cualitativa que adopta la perspectiva del usuario o encuestado, enfocándose en su realidad experiencial

### 3.5 Estudios Iniciales

Previo a la implementación de dichas simulaciones, llevamos a cabo una revisión sistemática de la literatura contemporánea (2021-2024) con el objetivo de identificar los métodos contemporáneos de ingeniería social, los elementos más convincentes y los errores frecuentemente cometidos por los usuarios en el contexto del sistema digital. Esta etapa facilitó la creación de escenarios con un elevado realismo y una significativa relevancia situacional.

De forma análoga, se implementó un cuestionario entre una muestra de usuarios con el objetivo de evaluar su conocimiento previo en relación con la ciberseguridad y las amenazas derivadas de la ingeniería social. Se identificó un nivel reducido de percepción de riesgo y un exceso de confianza en la identificación del fraude digital, factores que parecen justificar la necesidad de llevar a cabo la investigación contemporánea.

### 3.6 Desarrollo

El diseño del estudio se ejecutó en tres fases:

**Fase 1 - Diseño y desarrollo del experimento**: Se elaboró un diseño experimental que puede ser controlado mediante ataques de ingeniería social de tipo robo de identidad, que se caracteriza por su variabledad y complejidad. Los correos electrónicos de suplantación de identidad se elaboran mediante la combinación de elementos visuales y contextuales creíbles

(como logotipos institucionales auténticos, nombres familiares y estructuras de mensajes que evocan situaciones de urgencia habituales). Esta arquitectura se fundamentó en investigaciones anteriores como (Oliveira, et al., 2021), las cuales evidenciaron la eficacia de estos recursos para la manipulación de los usuarios.

**Fase 2 - Despliegue**: Despliegue: Se desplegaron un correo malicioso de manera controlada, ética y segura, y fueron pre-aprobadas. Se informó a los personas que estaban participando en un estudio sobre concienciación en ciberseguridad para un estudio académico y que la naturaleza del ataque simulado no se revelaría hasta después del estudio para garantizar respuestas válidas, ademas se indico que esta simulación no tendrá desarrollos intrusivos a cuentas no que sus datos podrian llegar a ser comprometidos.

**Fase 3: Recolección y análisis de datos**: Recolección y análisis de datos: En la ultima fase, después de completar la simulación, se realizaron entrevistas para analizar las reacciones de los participantes. Siguiendo el análisis sistemático, se identificaron patrones de comportamiento, percepciones de riesgo y emociones relacionadas con la experiencia a partir de los datos recopilados.

Cabe indicar que el estudio se realizó sobre la base de las reglas éticas fundamentales, que incluyen obtener el consentimiento informado, mantener la confidencialidad de los datos, el derecho a renunciar en cualquier momento y no causar daño a la integridad física y mental de los encuestados. Estas pautas están en sintonía con las directrices desarrolladas por la Asociación de Investigadores de Internet (AoIR), 2023 en este aspecto particular.

# CAPÍTULO IV RESULTADOS Y DISCUSIÓN

## 4.1. Descripción general de los datos

Este capítulo expone los hallazgos principales de un experimento controlado de phishing realizado en un contexto académico con la participación de 20 individuos en el mismo. Lo primordial de esta simulación es discernir la percepción de los usuarios, su interpretación y reacción frente a una labor de suplantación de identidad digital que replica las características más frecuentes y sofisticadas de las tácticas de phishing por correo electrónico.

Se insto a los participantes a estar atentos a posibles riesgos ciberneticos y ademas se les indico cómo podrían identificar y eludir amenazas previo a la simulación. Se implementó una escala de autoevaluación que va entre 1 - 10, en la cual 1 representa el nivel más bajo de seguridad percibida y 10 el nivel más alto de seguridad percibida. El propósito de la evaluación no era comparar medidas numéricas, sino servir como herramienta de introspección guiada para permitir una comparación con el nivel de conciencia expresado después del ejercicio.

Tras la simulación, se aplicó una segunda escala para medir la utilidad percibida del entrenamiento por parte de cada usuario. Así, se invitó a la reflexión sobre la relevancia de la parte práctica como método de aprendizaje y se comparó lo que se esperaba con lo que se percibía sobre la amenaza.

En cuanto a los resultados preliminares, se identificaron cinco hallazgos que permitieron identificar algunos elementos básicos. Por ejemplo, aproximadamente el 60% de los usuarios no reconocieron que el mensaje de ejemplo era un mensaje de phishing. De este grupo, además, el 35% tomó acciones inseguras al hacer clic en enlaces o proporcionar información sensible. Este comportamiento indica una diferencia interesante entre el nivel percibido de preparación y la respuesta real a un ataque digital.

Incluso los sujetos que informaron tener una alta confianza inicial en su juicio, a menudo se sorprendieron, ya sea por su prisa en emitir un juicio o por la dificultad para comprender la señal de confirmación que habían recibido. Este resultado converge con otras investigaciones que muestran que la sobreestimación de las competencias individuales actúa como un factor de riesgo en la manipulación digital (Oliveira, et al., 2021).

También hubo una actitud positiva hacia la utilidad del ejercicio. Casi todos los encuestados apreciaron la experiencia, señalando que:

Les dio una mejor comprensión de la complejidad de los ataques.

Les permitió notar indicadores que de otro modo podrían pasar por alto en el campo.

Estos hallazgos revelan el potencial educativo de las simulaciones como un entorno para el entrenamiento experiencial.

La Tabla 1 muestra las respuestas obtenidas de las diversas secciones evaluadas y proporciona una visión general de cómo el nivel inicial de confianza se correlaciona con la estrategia de respuesta al ataque, así como con la utilidad reconocida del ejercicio. Además, la comparación entre las dos variables se representa gráficamente en la Figura 1, que revela las implicaciones de aprendizaje que se estudiarán en secciones posteriores.

Tabla 1. Resultados simulados

| Part. | Pregunta 1 | Pregunta 2 | Pregunta 3 | Pregunta 4 | Pregunta 5 | Pregunta 6 | Pregunta 7 | Pregunta 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | No | 5 | No | Sí | Eliminé el mensaje | 2 | Tal vez | Sí, pero con incomodidad |
| 2 | Sí | 2 | Sí | Dudé, pero no actué | Hice clic en un enlace | 8 | Sí | Sí, pero con algo de incomodidad |
| 3 | Sí | 3 | No | Sí | Eliminé el mensaje | 9 | Tal vez | No, me sentí incómodo/a |
| 4 | No | 2 | No | No | No hice nada | 9 | Tal vez | Sí, sin malestar |
| 5 | Sí | 3 | Sí | Sí | No hice nada | 7 | Sí | Sí, sin malestar |
| 6 | No | 7 | Sí | No | Hice clic en un enlace | 7 | Tal vez | Sí, sin malestar |
| 7 | Sí | 5 | Sí | No | Proporcioné datos | 8 | Sí | Sí, sin malestar |
| 8 | No | 7 | Sí | Dudé, pero no actué | Hice clic en un enlace | 10 | No | Sí, sin malestar |
| 9 | No | 6 | Sí | No | Hice clic en un enlace | 4 | Sí | Sí, pero con algo de incomodidad |
| 10 | No | 4 | No | Dudé, pero no actué | No hice nada | 5 | Tal vez | Sí, sin malestar |
| 11 | No estoy seguro | 4 | No | Dudé, pero no actué | No hice nada | 10 | Tal vez | Sí, pero con algo de incomodidad |
| 12 | No estoy seguro | 10 | No | Sí | Proporcioné datos | 4 | Tal vez | No, me sentí incómodo/a |
| 13 | No estoy seguro | 9 | No | Sí | Hice clic en un enlace | 8 | Tal vez | No, me sentí incómodo/a |
| 14 | No estoy seguro | 4 | No | Sí | No hice nada | 10 | No | No, me sentí incómodo/a |
| 15 | Sí | 7 | Sí | Sí | Eliminé el mensaje | 7 | No | Sí, pero con algo de incomodidad |
| 16 | Sí | 9 | Sí | No | No hice nada | 5 | No | Sí, sin malestar |
| 17 | No | 2 | Sí | No | Hice clic en un enlace | 7 | Tal vez | Sí, pero con algo de incomodidad |
| 18 | No | 4 | No | Dudé, pero no actué | No hice nada | 9 | Tal vez | No, me sentí incómodo/a |
| 19 | No | 2 | Sí | Sí | Proporcioné datos | 2 | Sí | Sí, sin malestar |
| 20 | No estoy seguro | 7 | Sí | Sí | Proporcioné datos | 1 | Tal vez | Sí, pero con algo de incomodidad |

Fuente: Elaboración propia

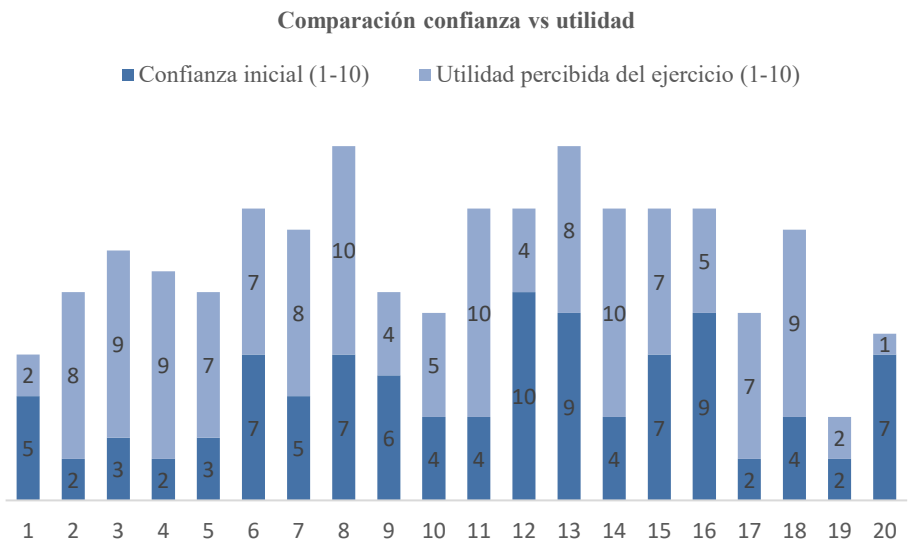


Figura 1. Comparación confianza vs utilidad

Los hallazgos aquí presentados resaltan el papel crucial que juegan los ejercicios prácticos en el área de ciberseguridad, particularmente al enfrentar riesgos relacionados con lo social, para los cuales se requiere más juicio basado en lo humano que herramientas técnicas. "La brecha entre lo que las personas pensaban que sabían y lo que hicieron cuando creyeron enfrentarse a un sitio web fraudulento es esencial para comenzar a estudiar comportamientos, diseñar planes de capacitación adecuados e inculcar una conciencia crítica respecto a la ciberseguridad."

### 4.2. Tipo de técnica empleada en el análisis

Dado que esta investigación indaga sobre el engaño desde la perspectiva de analizar la identidad falsa utilizada para engañar, la sección de resultados describe sistemáticamente las diferencias en significado, tareas y juicio con la interpretación inicial de los participantes, sus respuestas y evaluación de su experiencia durante la simulación de phishing por correo electrónico.

La simulación incluyó un enfoque muy detallado para imitar las propiedades de correos electrónicos potencialmente dañinos. Esto incluyó detalles visuales reales como logotipos y nombres reales de instituciones reales, y tácticas de urgencia y manipulación emocional, como suspensiones de cuenta o alertas bancarias. Se intentó simular un contexto realista y moral para facilitar la observación del comportamiento auténtico sin poner en peligro el bienestar psicológico de los participantes.

Se observó una clara diversidad en las respuestas conductuales y cognitivas al estímulo aplicado durante la tarea. Solo nueve de los 20 participantes reconocieron la presencia del caso de suplantación de identidad. Más de la mitad de los participantes no reconocieron señales claras de fraude a pesar de recibir la misma información que el grupo del 45% y diciendo que el mismo porcentaje se arriesgaría.

De la porción del grupo incapaz de identificar el intento, una gran parte todavía estaba interactuando activamente con el mensaje: aproximadamente el 30% del grupo hizo clic en el enlace del correo electrónico, proporcionó información en un formulario falso o respondió al correo electrónico como si fuera legítimo. La vulnerabilidad mostrada en este movimiento ilustra la perenidad de un movimiento popular, debido a su complejidad visual y narrativa.

Es interesante ver que un par de personas que dijeron estar confiadas antes (claramente no tenían nada que temer – altas puntuaciones) fueron las que ni siquiera notaron el peligro/jugaron con la sustancia dañina. Esto evidencia una brecha en cómo uno cree estar preparado frente a cómo puede responder a los ataques de ingeniería social.

También hubo diferentes estilos de pensamiento que los participantes informaron posteriormente como retroalimentación, es decir:

"Pensé que el mensaje era genuino, estaba tan bien escrito y no pensé en el remitente."

"Pensé que era genuino porque decía que venía de un banco."

Entre otras cosas. Dichas expresiones representan una percepción pobre de la amenaza de seguridad, caracterizada por un sesgo de producción y un sesgo de selección tales sesgos han sido descritos en trabajos anteriores sobre ingeniería social (Hadnagy, 2018).

Desde una perspectiva educativa, podemos inferir que el correo electrónico de ficción generó una serie de reacciones emocionales y racionales, que se basaron en elementos específicos de cada participante. Algunos mostraron una actitud reflexiva y escéptica hacia la veracidad del mensaje o de la fuente; el enfoque de otras personas ha sido más pasivo o impulsivo, es decir, simplemente ignoraron el mensaje sin ningún análisis cognitivo en el momento o actuaron de inmediato. Vamos a describir ahora estos distintos comportamientos con más detalle, clasificando los perfiles encontrados como sigue en la Sección 4.3.

En resumen, la evaluación de este mecanismo de ataque y defensa destaca el hecho de que el phishing sigue siendo un ataque efectivo en la práctica y en simulación. En tales casos, la posibilidad de aprovechar una amplia variedad de trampas cognitivas genéricas, como el exceso de confianza, la respuesta emocional impulsiva o la difusión de la responsabilidad, subraya la necesidad de incluir actividades prácticas y personalizadas dentro de los planes de concienciación relacionados con la seguridad. No es suficiente con simplemente contarle a la gente sobre el concepto de phishing; necesitan experiencias que les muestren cómo es el phishing, que los sorprendan y rompan su imagen mental de cómo será el phishing, y que les muestren cómo y por qué son susceptibles a él.

Como conclusión, gracias a la simulación pudimos analizar no solo cómo responden las personas a un ataque de phishing, sino también dónde se quedan atascados

en la toma de decisiones. Concentrarse en un solo método permite un diagnóstico más preciso de las medidas pedagógicas necesarias para contrarrestar su eficacia.

### 4.3. Análisis de Perfiles de Comportamiento

La necesidad de distinguir diferentes tipos de comportamiento en respuesta a pruebas de phishing se enfatiza en el presente trabajo. No se realiza sobre la base de una estructura establecida o predefinida, sino a través de una interpretación desarrollada mediante el análisis comparativo de las respuestas a dos preguntas básicas por parte de los participantes de la investigación.

¿Cómo supiste que el correo electrónico que recibiste era fraudulento?

¿Te involucraste con el contenido del mensaje?

A través de la combinación de estas dos variables, descubrimos tres formas de comportamiento en relación con los perfiles cognitivos: reactivo, evitativo y reflexivo. El proceso de categorización fue inductivo y de acuerdo con el análisis temático cualitativo, tal como lo formula Creswell (2018) y en consonancia con el carácter exploratorio del estudio. Al igual que en estudios similares sobre educación en ciberseguridad (Rahartomo et al., 2025) este modelo ha hecho posible la identificación de constructos de pensamiento y actos de comportamiento en situaciones simuladas de riesgo digital.

Los valores en las columnas de porcentaje para los perfiles se derivan del conteo del número de encuestados cuyas respuestas fueron indicativas de cada perfil (como se describe a continuación).

| Perfil | ¿Identificó el phishing? | ¿Interactuó con el mensaje? | Justificación |
|---|---|---|---|
| **Reflexivo** | Sí | No | Lo detectó como amenaza. |
| **Reactivo** | No o Dudó | Si | No detectó la amenaza. |
| **Evasivo** | No o Dudó | No hizo nada | No detectó la amenaza conscientemente. |

Tabla 2. Criterios para la categorización

### 4.3.1 Perfil reactivo

Estos individuos respondieron impulsivamente a ese mensaje sin invertir demasiado tiempo en analizar el mensaje. Lo más alarmante es que la mayoría de estas personas estaban dispuestas a involucrarse positivamente con tal intento, incluso cuando el mensaje contenía indicadores débiles de ser un impostor. Este rasgo fue reportado por el 30% de los participantes en esta tarea, lo cual es notable dado lo sensible de este comportamiento en el mundo real. La gran mayoría de las acciones se tomaron debido a mensajes que apuntaban a una necesidad urgente, una pérdida de acceso pendiente o el riesgo de una multa bancaria. Las respuestas están en línea con la urgencia y la autoridad como fundamentos psicológicos del phishing, según Hadnagy (2018).

Un ejemplo típico fue donde una persona había recibido un mensaje que decía que "su cuenta está a punto de ser bloqueada inmediatamente", y luego hizo clic en un enlace sin considerar quién lo había enviado ni mirando el contenido de la información. Más tarde dijeron que "no pensaron dos veces para tomar acciones rápidas debido a la obvia emergencia".

### 4.3.2 Perfil evasivo

Dentro de este grupo, los encuestados no tomaron en cuenta el mensaje que decidieron no responder debido a una sensación general de desconfianza o falta de interés hacia cuestiones digitales, en lugar de una decisión cuidadosamente hecha. Básicamente ignoraron el mensaje o no lo tomaron en serio sin verificar su veracidad. Este perfil representó el 25% de la muestra. Aunque no fueron engañados en la estafa, el bajo reconocimiento del riesgo por parte de los individuos podría llevar a una falsa sensación de seguridad o podría tener algún impacto en su educación futura.

En las entrevistas, algunos participantes dijeron cosas como: "No abrí el correo electrónico y lo eliminé porque no sé de dónde viene" o "Elijo no hacer clic en enlaces sospechosos". Mientras que este tipo de estrategia evitativa puede funcionar de inmediato, puede que no esté preparando contra un futuro en el que la desinformación se asemeje más estrechamente a la comunicación legítima.

### 4.3.3 Perfil reflexivo

El tercer estilo fue el estilo reflexivo, que se percibe como el más impermeable a la amenaza cibernética. Estos participantes mostraron habilidades críticas en el contexto del mensaje y/o una vez lo confrontaron (por ejemplo, verificar el origen de la dirección del remitente; buscar inconsistencias en el texto; dudar al hacer clic en enlaces). También obtuvieron los mejores resultados en evaluaciones de resultados de aprendizaje posteriormente. Esto es el 45% de todas las respuestas, igual que las personas que identificaron correctamente el phishing en la encuesta. La mayoría dijo que notaron "detalles sospechosos" o creyó que "algo no tenía sentido en el correo electrónico". Algunos incluso enviaron el mensaje a su soporte técnico o de seguridad, indicando un mayor nivel de madurez

digital. Estos hallazgos son consistentes con la idea de que la capacidad para analizar y ser crítico no es meramente una consecuencia del conocimiento tecnológico, y el resultado de una suma de capacitación previa, práctica digital y una intención de navegación segura.

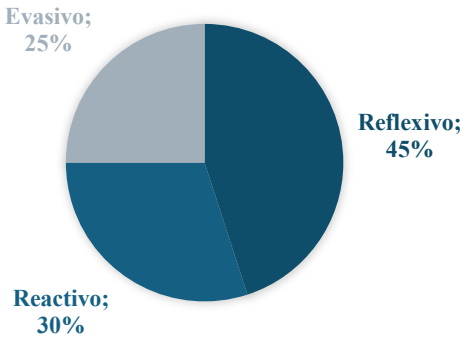


Figura 2. Distribución de perfiles de comportamiento

Los resultados muestran que una amenaza común puede llevar a diferentes reacciones de los usuarios y que la clasificación educativa basada en perfiles generales de comportamiento puede ser muy útil para diseñar estrategias de concienciación personalizadas. En lugar de una instrucción "talla única", se podrían personalizar los cursos según cómo piensa cada persona: para las personas que asisten a muchos grupos, práctica adicional y retroalimentación inmediata; para aquellos que evitan el conflicto, capacitación sobre la lectura de señales; para los que se detienen antes de actuar, capacitación para motivar a los compañeros.

### 4.3.4 Relación Entre Percepción Anterior y Conocimiento Posterior

Quizás el resultado más significativo de este estudio sea la destacada discrepancia entre la autoconfianza de los usuarios (reportada en las preguntas antes de la simulación) y el comportamiento de los usuarios cuando enfrentan el ataque de phishing. La diferencia que existe entre lo que los usuarios "saben" y lo

que hacen en un entorno simulado es crítica para comprender la dimensión humana en la ciberseguridad.

Antes de participar en la actividad, se solicitó a los participantes que calificaran su nivel de confianza en poder identificar correos electrónicos falsos en una escala del 1 al 10. La evaluación arrojo como resultado un nivel elevado ya que por cada 10 participantes 7 de ellos representan una percepción de confianza ante posibles correos maliciosos. Sin embargo, al realizar las revisiones durante la simulación, se puede observar que solo el 45% de participantes logró identificar correctamente el correo malicioso, mientras que el 35% continuó interactuando de forma insegura con el correo recibido.

Este descubrimiento también destaca una distinción significativa entre las percepciones subjetivas y la vivencia práctica auténtica, tal como se destacó en investigaciones previas (Moghimi & Varadharajan, 2022). No obstante, en entornos educativos, este contraste puede representar un obstáculo para la eficacia de los programas de enseñanza convencionales que se fundamentan únicamente en teoría, dado que los participantes pueden menospreciar sus carencias propiasceptivas si no se les confronta con situaciones prácticas.

La evolución de la primera confianza y la evaluación sobre cómo el ejercicio fue útil demuestra que hay un cambio en el proceso de aprendizaje percibido. "Unos pocos de los participantes que habían entrado a la sala declarándose "seguros de sí mismos" luego confesaron privadamente que no estaban tan seguros como antes. La encuesta posterior reveló que la mayoría de los participantes encontró el ejercicio altamente valioso (calificado entre 8 y 10), y se sorprendieron por la dificultad cognitiva del mensaje recibido (87%).

- *Un número de sujetos hizo explícita esta transición*
- "*Pensaba que era algo fácil de identificar, pero simplemente no lo era, sin saberlo".*
- *"Era la primera vez que veía algo como eso, y probablemente me mantuve un poquito más alerta".*
- *"Ahora sé por qué la gente cae, no es fácil", dijo.*

Los testimonios presentados, junto con los datos recopilados, sugieren que el proceso tanto fomenta la educación técnica como el desarrollo de la autoconciencia crítica, inherente en promover la protección personal en línea.

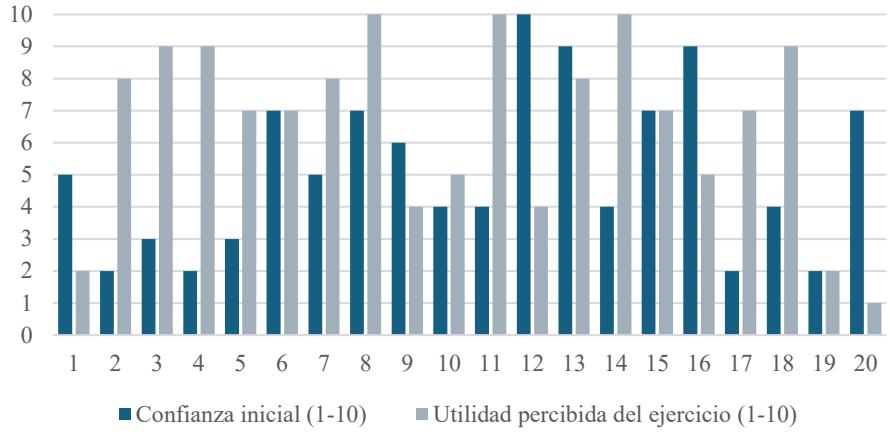


Figura 3. Relación entre confianza inicial y aprendizaje posterior

En general, esta comparación también resalta: No basta con simplemente conocer los peligros para reaccionar ante ellos de manera correcta. La capacitación exitosa en ciberseguridad requiere no solo instruir a los individuos sino también sacudir su confianza en que saben cuán preparados están. Solo de esta manera se genera un conocimiento que tiene un efecto real, que perdura, que de alguna manera disminuye el peligro para las personas. Impacto emocional percibido y disposición al aprendizaje

El impacto de la simulación de phishing se manifestó en respuestas observables del individuo, así como en múltiples efectos emocionales involucrados

que influyeron en la percepción de la actividad y la inclinación hacia futuros entrenamientos. Los factores afectivos son altamente relevantes en el área de la consciencia de ciberseguridad debido a la influencia de los sentimientos en la motivación para aprender, según SENA (2023).

Basado en las respuestas a la pregunta de los sentimientos durante la simulación, se encontraron los siguientes grupos:

- Sí, sin malestar: 9 usuarios.
- Sí, pero con algo de incomodidad: 7 usuarios.
- No, me sentí incómodo: 4 usuarios.

Esto significa que tanto la dificultad emocional leve como la notable fueron reportadas por el 55% de los alumnos como ocurriendo después, o durante, un episodio de actividad física. Este número es importante, ya que muestra que el procedimiento no fue emocionalmente neutral y que el conocimiento posterior al ejercicio también se ha vinculado con la emoción durante la exposición.

Entre los usuarios que mencionaron una emoción negativa, algunos también reportaron haber intentado la simulación o tener una fuerte creencia en no ser engañados, sugiriendo que el sentimiento de decepción o vergüenza estaba ligado a la experiencia de haber cometido un error en algo que creían tener bajo control. Como argumentan Moghimi y Varadharajan (2022), la idea de que permitir un error en un entorno seguro puede generar sentimientos negativos pero también contribuir a un aprendizaje más duradero se ve reforzada por esta observación.

Alternativamente, los individuos que no vieron esto como una mentira y no procesaron el mensaje, incluso en todas las condiciones, entretenían la posibilidad de la amenaza. Aunque no experimentaron daño, algunos de ellos no sintieron que

la actividad fuera beneficiosa, indicando la importancia de pasar por una emoción, sorpresa, o cometer un error para que la lección calara.

Además, se les preguntó a los encuestados si les gustaría participar en actividades similares y la respuesta fue la siguiente:

- "Sí": 7 personas
- "Tal vez": 11 personas
- "No": 2 personas

La actividad física se está repitiendo y la actitud sobre esta repetición es bastante buena en general, pero con cautela. La decisión mayoritaria sobre "quizás" puede ser una señal de cautela o requerir más claridad sobre los objetivos y beneficios de este entrenamiento específico.

En conclusión, el papel de lo emocional fue central para el aprendizaje en estas simulaciones sintéticas. Más que una barrera, el sutil malestar o preocupación ha sido un factor impulsor hacia una mayor consciencia. Sin embargo, también tiene un deber moral y pedagógico por cumplir. Es importante que estos esfuerzos se combinen con entornos de apoyo y evaluaciones que brinden espacio para una reflexión positiva sobre las experiencias.

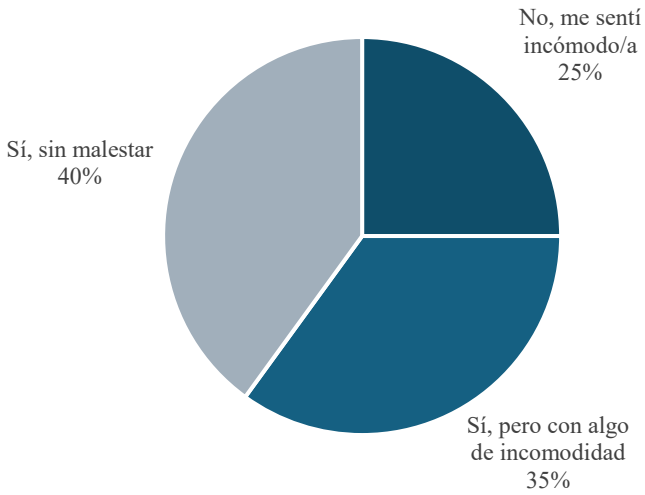


Figura 4. Impacto emocional percibido tras las simulaciones

### 4.4 Comparativa con literatura reciente

Los resultados obtenidos en este estudio tienen algunas similitudes, pero también algunas diferencias, con respecto a lo que reportan las publicaciones científicas más recientes e informes técnicos sobre ingeniería social y concienciación en ciberseguridad.

Esta discrepancia entre la autoconfianza y la capacidad para reaccionar efectivamente se enfatiza en un estudio, por ejemplo, como el de Moghimi & Varadharajan (2022). Encontraron que las personas sobreestiman su capacidad para reconocer estafas en Internet, más aún si no tienen experiencia práctica. Un tercio de las categorías sobre individuos en este estudio actual obtuvo puntuaciones entre 7 y 10 sobre el nivel de confianza para la primera página que visitaron y menos de la mitad (45%) pudo identificar correctamente un intento de suplantación, y alrededor de un 35% interactuó con enlaces peligrosos. El hallazgo corrobora la opinión expresada en ENISA (2023) donde se destaca la ingeniería social como un problema crítico de seguridad digital en Europa. Este método no se preocupa por el técnico, solo por lo que puede hacer.

Otro punto en común con los estudios más actuales es la influencia emocional como factor que impulsa el proceso de aprendizaje. Según el informe del SENA (2023), las emociones generadas por simulaciones realistas, como la vergüenza, la frustración o la alerta, funcionan como estímulos mentales que contribuyen a la retención del mensaje educativo. Durante la investigación actual, la mayoría de los encuestados expresaron sentir cierta incomodidad emocional en algún momento de la actividad, la cual no obstaculizó el proceso de aprendizaje, sino que en varios casos lo potenció. Esto subraya la importancia de crear tareas que no sean simplemente emocionalmente neutras, sino que representen un desafío ético y estén acompañadas de forma cuidadosa.

En cuanto a los perfiles detectados, los resultados obtenidos son concurrentes con las sugerencias de (Rahartomo et al., 2025) que sugieren segmentar las campañas de concienciación según el perfil de riesgo cognitivo: impulsivo (reactivo), desinteresado (evasivo) y analítico (reflexivo). De esta manera, se pueden entregar materiales educativos personalizados a cada individuo que sean más efectivos y realmente aumenten la conciencia sobre la autoprotección en línea.

Pero hay una parte adicional en el cálculo. Por ejemplo, algunos participantes creían que no habían obtenido mucho de la actividad física a pesar de sus mejores esfuerzos. Esto resalta la necesidad de momentos para la reflexión guiada que luego se puedan utilizar para enfrentar la decepción y convertirla en una experiencia de aprendizaje. La literatura es rica en cuanto a los efectos positivos de la gamificación y la simulación, pero relativamente limitada al revelar cómo las emociones, como la incomodidad, pueden impactar la percepción de la efectividad

de las actividades. El hallazgo muestra la importancia de cómo se realiza el ejercicio, así como el apoyo educativo brindado posteriormente.

En última instancia, la baja percepción de utilidad en algunos casos implica que parte del diseño de las simulaciones debería revisarse: ¿están las simulaciones diseñadas apropiadamente para coincidir con el nivel de competencia digital de los participantes? ¿Crees que estaban bien explicadas? ¿Estaba bien definido el propósito de los objetivos? Este estudio reconoce el valor de la simulación como herramienta; sin embargo, esto plantea varios factores relacionados con cómo se perciben, lo que añade a la discusión en curso sobre los mejores medios de educación en ciberseguridad.

### 4.5 Implicaciones para la educación en ciberseguridad

Los resultados de este estudio proporcionan implicaciones para los educadores y los profesionales de la industria en el diseño, realización y mejora del diseño y la gestión de programas de concienciación sobre la seguridad de la información en el ámbito educativo y la industria. Estas conclusiones se extraen no solo del análisis del comportamiento observado, sino también de las opiniones y sentimientos de los participantes después de participar en una simulación de phishing.

Y podemos confirmar que la autoconfianza resultante no representa una toma de decisiones adecuada sobre si estás o no preparado para los ataques de ingeniería social. En consecuencia, los planes de estudio necesitan herramientas de evaluación práctica para la comparación de decisiones personales con escenarios simulados. La discrepancia entre cuán confiados están inicialmente y lo mal que realmente lo hacen puede ser un primer paso hacia la autoconciencia y el cambio de actitudes negativas.

En segundo lugar, al identificar diversos perfiles de comportamiento (reactivo; evasivo; reflexivo), parece que los programas de entrenamiento no deberían definirse globalmente, sino que deberían tener en cuenta la especificidad, los límites y los estilos de aprendizaje de cada perfil de usuario. Por ejemplo, en el caso de los perfiles reactivos, una serie de ejercicios bien preparados que incluyan retroalimentación inmediata serían beneficiosos; los evasivos podrían ser desafiados con contenido que les invite a pensar críticamente y a analizar riesgos; y los perfiles reflexivos podrían crecer siendo autores de lo que aprendieron al hacerlo y liderando en entornos de trabajo en equipo.

La dimensión emocional en sí misma no es más que el ingrediente principal, no una adición dentro de la educación. Los sentimientos con valencia negativa (frustración, alerta, humildad [vergüenza y bochorno]) no tienen que ser contraproducentes, sino que pueden contribuir como elementos de una experiencia auténtica en el entrenamiento de habilidades disfrazadas si se facilita el dominio lúdico de la tarea. Esto también implica que se deben proporcionar espacios seguros para la reflexión después de las experiencias simuladas, ya sea en reuniones de discusión, entornos en línea o en bucles de retroalimentación que faciliten la integración de las experiencias en el comportamiento futuro.

La implementación de simulacros éticos y regulados puede implementarse como estrategias para la cultura de ciberseguridad. Son diferentes a las técnicas teóricas, las simulaciones prácticas generan emociones y evidencian las falencias impulsando las capacidades de pensamiento crítico para la captación de recursos. Cuando se incorporan en programas de educación continua, evaluaciones regulares y sugerencias para el uso de recursos particulares del entorno, sus impactos se potencian.

Además, las instituciones educativas y las empresas deben considerar el desarrollo de protocolos de simulación repetibles, así como de instrumentos para registrar, analizar y retroalimentar los comportamientos observados. Estas son herramientas vitales cuando se deciden cosas como dónde utilizar los recursos de capacitación y las políticas de seguridad interna. Y también cuidarse de la ética y la humanidad mientras se juegan siempre. Es importante asegurarse de que los participantes hayan dado su consentimiento en cada simulación, que se respete la confidencialidad; el "derecho a retirarse" en cualquier momento es respetado y no están sujetos a ninguna consecuencia disciplinaria. De esta manera, podremos construir un clima de aprendizaje de confianza, avance y cofabricación de una cultura de seguridad digital.

# CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

Se identificaron tres perfiles de comportamiento (reactivo, evasivo y reflexivo) que sugieren que no hay una única respuesta de los usuarios. Cada grupo exhibe características distintivas al enfrentar problemas en línea, lo que sugiere que las estrategias de enseñanza deben ser personalizadas y adaptadas.

1. La autopercepción de los usuarios (en relacion a su habilidad para identificar riesgos en la web) es notablemente diferente de su percepción real sobre la identificación de riesgos en línea. A pesar de que algunos de los sujetos inicialmente mostraron un alto nivel de confianza, solo el 45% de los sujetos seleccionaron la opción correcta. Entonces, la percepción personal no es una señal de preparación.

2. Las simulaciones de phishing pueden mostrar en los participantes debilidades emocionales y cognitivas. El 33.3% de los participantes en la encuesta que recibieron el correo sospechoso, ingresaron información y abrieron el enlace sin confirmar la veracidad de los contenidos. En el ejemplo estadístico se evidencia lo dañino que puede llegar a ser el phishing como origen de ataques y lo primordial que es adquirir conocimientos prácticos en posibes ataques pishing.

3. Se reconocieron tres tipos de conducta (reactiva, evasiva y reflexiva) que indican que no existe una sola reacción de los usuarios. Cada perfil de los tres identificados presentan particularidades al verse envueltos con posibles ataques de ingenieria social, por lo que se puede concluir que las tácticas de enseñanza deben ser efectivas y ajustadas para cada uno de los tres perfiles ya que no todos tenemos la misma capacidad de recepcion.

4. Es claro que algunos elementos como los emocionales son importantes en el proceso de aprendizaje. Durante el transcurso de la simulación, la mayor parte de los participantes sintieron un nivel de malestar, frustración o alerta. Estas emociones, en lugar de representar un reto, contribuyeron a identificar la fragilidad de las personas y la importancia de implementar acciones preventivas.

5. Se percibió de manera diferente la utilidad del ejercicio, con una calificación promedio de 6,4/10. Aunque la experiencia recibió algunos comentarios positivos, muchas personas estaban inseguras o indiferentes sobre la sabiduría que habían adquirido. Esto demuestra que la simulación por sí sola no es suficiente para facilitar el cambio de comportamiento y necesita complementarse con experiencias educativas y de reflexión adecuadas.

### 5.2. Recomendaciones

Dependiendo de los hallazgos y conclusiones de este estudio, se sugieren las siguientes recomendaciones para las próximas implementaciones:

1. Incluir simulaciones internas de ingeniería social en programas universitarios o de colegios de nivel superior, no como proyectos independientes, sino como parte integrada de la educación mediante teoría, práctica y reflexión.

2. Utilizar diagnósticos de perfil cognitivo-conductual antes y después de la formación para adaptar las intervenciones educativas a los estilos de aprendizaje de los usuarios y maximizar el impacto de la concienciación.

3. Desarrollar retroalimentación pedagógica y emocional durante la simulación que guíe al aprendiz hacia un aprendizaje positivo a partir del impacto emocional, sin culpa ni desaliento.

4. Implementar una cultura de autodefensa digital en las organizaciones que permita a las personas pensar de manera crítica, revisar seriamente los mensajes o medios digitales y reportar actividades sospechosas.

5. Ampliar estudios futuros a una gama más amplia de múltiples sectores (público, privado, educativo) para determinar la replicabilidad del modelo, converger parámetros de efectividad y proponer políticas públicas basadas en evidencia para la educación digital preventiva.

# ANEXOS

## Anexo A. Encuesta aplicada a participantes

Encuesta: Concienciación en Ciberseguridad ante Simulaciones de Ingeniería Social

1. ¿Consideras que tienes conocimientos para detectar correos electrónicos fraudulentos?

   ☐ Sí

   ☐ No

   ☐ No estoy seguro/a

2. ¿Qué nivel de confianza tenías antes del ejercicio para evitar caer en intentos de phishing? (Escala del 1 al 10).

   _____

3. ¿Has recibido formación previa en temas de fraudes digitales o ciberseguridad?

   ☐ Sí

   ☐ No

4. ¿Identificaste que el correo recibido era un intento de phishing?

   ☐ Sí

   ☐ No

   ☐ Dudé, pero no actué

5. ¿Interactuaste con el contenido del mensaje?

   ☐ Hice clic en un enlace

   ☐ Proporcioné datos

   ☐ No hice nada

   ☐ Eliminé el mensaje inmediatamente

6. ¿Qué nivel de utilidad le atribuyes al ejercicio para tu formación en ciberseguridad? (Escala del 1 al 10)

   _____

7. ¿Te gustaría participar en ejercicios similares en el futuro?

☐ Sí

☐ No

☐ Tal vez

8. ¿Cómo te sentiste durante la simulación?

☐ Sí, sin malestar

☐ Sí, pero con algo de incomodidad

☐ No, me sentí incómodo/a

## Anexo B. Tabla de resultados por participante

Resumen detallado de las respuestas individuales ante los ataques simulados: phishing

| ID Participante | ¿Tiene conocimientos para detectar phishing? | Confianza inicial (1-10) | Formación previa en fraudes digitales | ¿Identificó el correo como phishing? | ¿Interactuó con el mensaje? | Utilidad percibida del ejercicio (1-10) | ¿Participaría en ejercicios similares? | ¿Se sintió cómodo durante la simulación? |
|---|---|---|---|---|---|---|---|---|
| 1 | No | 5 | No | Sí | Eliminé el mensaje inmediatamente | 2 | Tal vez | Sí, pero con algo de incomodidad |
| 2 | Sí | 2 | Sí | Dudé, pero no actué | Hice clic en un enlace | 8 | Sí | Sí, pero con algo de incomodidad |
| 3 | Sí | 3 | No | Sí | Eliminé el mensaje inmediatamente | 9 | Tal vez | No, me sentí incómodo/a |
| 4 | No | 2 | No | No | No hice nada | 9 | Tal vez | Sí, sin malestar |
| 5 | Sí | 3 | Sí | Sí | No hice nada | 7 | Sí | Sí, sin malestar |
| 6 | No | 7 | Sí | No | Hice clic en un enlace | 7 | Tal vez | Sí, sin malestar |
| 7 | Sí | 5 | Sí | No | Proporcioné datos | 8 | Sí | Sí, sin malestar |
| 8 | No | 7 | Sí | Dudé, pero no actué | Hice clic en un enlace | 10 | No | Sí, sin malestar |
| 9 | No | 6 | Sí | No | Hice clic en un enlace | 4 | Sí | Sí, pero con algo de incomodidad |
| 10 | No | 4 | No | Dudé, pero no actué | No hice nada | 5 | Tal vez | Sí, sin malestar |
| 11 | No estoy seguro/a | 4 | No | Dudé, pero no actué | No hice nada | 10 | Tal vez | Sí, pero con algo de incomodidad |
| 12 | No estoy seguro/a | 10 | No | Sí | Proporcioné datos | 4 | Tal vez | No, me sentí incómodo/a |
| 13 | No estoy seguro/a | 9 | No | Sí | Hice clic en un enlace | 8 | Tal vez | No, me sentí incómodo/a |
| 14 | No estoy seguro/a | 4 | No | Sí | No hice nada | 10 | No | No, me sentí incómodo/a |
| 15 | Sí | 7 | Sí | Sí | Eliminé el mensaje inmediatamente | 7 | No | Sí, pero con algo de incomodidad |
| 16 | Sí | 9 | Sí | No | No hice nada | 5 | No | Sí, sin malestar |
| 17 | No | 2 | Sí | No | Hice clic en un enlace | 7 | Tal vez | Sí, pero con algo de incomodidad |
| 18 | No | 4 | No | Dudé, pero no actué | No hice nada | 9 | Tal vez | No, me sentí incómodo/a |
| 19 | No | 2 | Sí | Sí | Proporcioné datos | 2 | Sí | Sí, sin malestar |
| 20 | No estoy seguro/a | 7 | Sí | Sí | Proporcioné datos | 1 | Tal vez | Sí, pero con algo de incomodidad |

## Anexo C. Categorización de perfiles de comportamiento

En el análisis cualitativo que se hizo después de las simulaciones, se encontraron tres perfiles de comportamiento principales entre los participantes, que dependían de cómo reaccionaban a los ataques de ingeniería social.

### 1. Reactivo

Descripción: Personas que ingresaron al correo de forma inmediata por el estímulo generado ante el mensaje, sin verificar su autenticidad

Características: Influenciados por mensajes de urgencia o advertencias de bloqueos.

Riesgos: Probabildad alta de caer en correos engañozos.

### 2. Evasivo

Descripción: Personas que hicieron caso omiso al mensaje sin interactuar, pero no reconocieron el intento de ataque de manera conciente..

Riesgos: Ddesarrollar una falsa sensación de seguridad, no tiene una conciencia real.

### 3. Reflexivo

Descripción: Personas que antes de abrir el mensaje se cuestionaron la veracidad del mismo, tomaron una decision en base a un analisis sobre el contenido del mensaje.

Riesgos: Probabilidad baja de caer en correos engañozos, aun asi pueden tener riesgo de caer en correos maliciosos si son muy sofisticados.

## Referencias

Association of Internet Researchers (AoIR). (2023). *Ethical guidelines for internet research.* Obtenido de https://aoir.org/reports/ethics4.pdf

Bazalar. (2023). *Universidad Peruana de Ciencias Aplicadas.* Obtenido de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/669347/Bazalar_HG.pdf

Creswell. (2018). Qualitative inquiry and research design: Choosing among five approaches. SAGE Publications.

ENISA. (2023). *Cybersecurity Threat Landscape 2023. European Union Agency for Cybersecurity.* Obtenido de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Universidad Politécnica de Cartagena. (s. f.). Principios de la seguridad de la información. En A4C41A1D01. UPCT. Recuperado de https://opencontent.upct.es/f0fc64e3b2d34f3a872a841a9c37b249/ea25f7d23db041929a840cb2134aa6f0/

Gragg, D. (2023). *A Multi-Level Defense Against Social Engineering.* SANS Institute.

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking.* Wiley.

Hernández. (2021). Metodología de la investigación. En Hernández. McGraw-Hill.

IBM. (2023). *Cost of a Data Breach Report.* Obtenido de https://www.ibm.com/reports/data-breach

Mitnick, K. (2003). *The Art Of Deception.* John Wiley & Sons.

Moghimi, M., & Varadharajan, V. (2022). Obtenido de Human factor in phishing attacks: A study of the effectiveness of training and awareness programs: https://doi.org/10.1016/j.cose.2021.102584

Nespoli, P., Albaladejo-González, M., Ruipérez-Valiente, J., & Garcia-Alfaro, J. (2024). *SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification, and Learning Analytics to Train Cybersecurity Competencies.* Obtenido de https://arxiv.org/abs/2401.12594

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., & Ebadi, Y. (2021). Obtenido de Dissecting spear phishing emails for older adults: On characterizing and recognizing harmful emails. ACM Transactions on Computer-Human Interaction: https://doi.org/10.1145/3457600

Cabezas-Molina, E. M., & Fiallos-Aguilar, H. C. (2024). Simulación de ataques phishing y planes de concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional. INNOVA Research Journal, 9(4), 95–110. https://doi.org/10.33890/innova.v9.n4.2024.2678 Proofpoint. (2023). *¿Qué es la ingeniería social? Definición, tipos y más.* Obtenido de

SENA. (2023). *Aprendizaje significativo en ciberseguridad a través del simulador Hackend.* Obtenido de https://revistas.sena.edu.co/index.php/sennova/article/view/5374

Rahartomo, A., Ghaleb, A. T. A., & Ghafari, M. (2025). Phishing Awareness via Game-Based Learning. ArXiv. https://doi.org/10.48550/arXiv.2501.12077

Verizon. (2023). *Data Breach Investigations Report.* (DBIR).

**Bibliografía**

Association of Internet Researchers (AoIR). (2023). *Ethical guidelines for internet research.* Obtenido de https://aoir.org/reports/ethics4.pdf

Bazalar. (2023). *Universidad Peruana de Ciencias Aplicadas.* Obtenido de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/669347/Bazalar_HG.pdf

Creswell. (2018). Qualitative inquiry and research design: Choosing among five approaches. SAGE Publications.

ENISA. (2023). *Cybersecurity Threat Landscape 2023. European Union Agency for Cybersecurity.* Obtenido de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Universidad Politécnica de Cartagena. (s. f.). Principios de la seguridad de la información. En A4C41A1D01. UPCT. Recuperado de https://opencontent.upct.es/f0fc64e3b2d34f3a872a841a9c37b249/ea25f7d23db041929a840cb2134aa6f0/Gragg, D. (2023). *A Multi-Level Defense Against Social Engineering.* SANS Institute.

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking.* Wiley.

Hernández. (2021). Metodología de la investigación. En Hernández. McGraw-Hill.

IBM. (2023). *Cost of a Data Breach Report.* Obtenido de https://www.ibm.com/reports/data-breach

Mitnick, K. (2003). *The Art Of Deception.* John Wiley & Sons.

Moghimi, M., & Varadharajan, V. (2022). Obtenido de Human factor in phishing attacks: A study of the effectiveness of training and awareness programs: https://doi.org/10.1016/j.cose.2021.102584

Nespoli, P., Albaladejo-González, M., Ruipérez-Valiente, J., & Garcia-Alfaro, J. (2024). *SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification, and Learning Analytics to Train Cybersecurity Competencies.* Obtenido de https://arxiv.org/abs/2401.12594

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., & Ebadi, Y. (2021). Obtenido de Dissecting spear phishing emails for older adults: On characterizing and recognizing harmful emails. ACM Transactions on Computer-Human Interaction: https://doi.org/10.1145/3457600

Cabezas-Molina, E. M., & Fiallos-Aguilar, H. C. (2024). Simulación de ataques phishing y planes de concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional. INNOVA Research Journal, 9(4), 95–110. https://doi.org/10.33890/innova.v9.n4.2024.2678

SENA. (2023). *Aprendizaje significativo en ciberseguridad a través del simulador Hackend.* Obtenido de https://revistas.sena.edu.co/index.php/sennova/article/view/5374

Rahartomo, A., Ghaleb, A. T. A., & Ghafari, M. (2025). Phishing Awareness via Game-Based Learning. ArXiv. https://doi.org/10.48550/arXiv.2501.12077

Verizon. (2023). *Data Breach Investigations Report.* (DBIR).

TECNOLÓGICO SAN ANTONIO Tesa

# CERTIFICADO DE ORIGINALIDAD

## TESA

La Dirección de Carrera de Ciberseguridad, certifica que el trabajo de titulación denominado, "Concienciación en ciberseguridad mediante simulaciones de ingeniería social: un enfoque práctico y ético", presentado por Jarrin Cazco Pablo Sebastian, ha sido sometido a un análisis de similitud mediante la herramienta Turnitin.

El resultado obtenido refleja un 04 % de similitud, porcentaje que se encuentra dentro de los parámetros establecidos por el Instituto Superior Tecnológico San Antonio – TESA, cumpliendo con los criterios de originalidad y autenticidad académica exigidos por la institución.

Quito, 10 de julio de 2025

Santiago Xavier Rojas Bukovac

Decano Escuela Tecnología e Innovación

TECNOLÓGICO SAN ANTONIO Tesa
DIRECCIÓN CARRERA CIBERSEGURIDAD