UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

PROYECTO DEL TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

Vulnerabilidades psicológicas en la susceptibilidad de usuarios novatos y su incidencia frente a ataques de ingeniería social.

AUTOR:

Slater Jeremay Zambrano Bombòn

TUTOR:

Ing. Maliza Cruz Wellington Isaac

BABAHOYO – LOS RÍOS – ECUADOR

2025

Índice

Resumen

El proyecto, titulado "Vulnerabilidades Psicológicas, Propensión de Usuarios Novatos y la Prevalencia de Estafas de Ingeniería Social en Ciberseguridad", explora cómo la humanidad sigue siendo la mayor vulnerabilidad a pesar de los avances tecnológicos. Esto se aplica a los novatos, aspirantes a principiantes que no están lo suficientemente controlados o educados para comprender las cuerdas que los convierten en víctimas perfectas para los hackers con un ataque de ingeniería social.

En este documento, presentamos un experimento del mundo real en Babahoyo, Ecuador, un campo minado con las tasas de detección más bajas y donde es menos conocido. Estos estaban destinados a investigar la conexión entre algunas vulnerabilidades psicológicas y quiénes son estos individuos que probablemente serán atacados. Con ese fin, sometimos a 66 sujetos no entrenados a una serie de simulaciones de prueba.

Los resultados de este estudio proporcionan un modelo de evaluación de riesgos que tiene en cuenta las dimensiones técnicas y los factores humanos para construir defensas más robustas contra ataques maliciosos.

Estas recomendaciones son el resultado de la evaluación y algunos puntos clave generales derivados del riesgo para hacer que los usuarios fallen menos en convertirse en grandes objetivos para la ingeniería social, tanto desde una perspectiva técnica como debido a su comportamiento.

Términos clave: Ingeniería social, ciberseguridad, vulnerabilidades psicológicas, no profesionales, ataques de phishing, amenazas de seguridad en internet, amenazas de error humano, sesgos cognitivos y competencia digital.

ABSTRACT

The project, titled “Psychological Vulnerabilities, Novice User Propensity, and the Prevalence of Social Engineering Scams in Cybersecurity,” explores how humanity remains the greatest vulnerability despite technological advances. This applies to novices, aspiring beginners who are not sufficiently controlled or educated to understand the ropes, making them perfect victims for hackers with a social engineering attack.

In this paper, we present a real-world experiment in Babahoyo, Ecuador, a minefield with the lowest detection rates and where it is least known. These were intended to investigate the connection between certain psychological vulnerabilities and who these individuals are that are likely to be targeted. To that end, we subjected 66 untrained subjects to a series of test simulations.

The results of this study provide a risk assessment model that takes into account technical dimensions and human factors to build more robust defenses against malicious attacks.

These recommendations are the result of the assessment and some general key points derived from the risk to make users less likely to become prime targets for social engineering, both from a technical perspective and due to their behavior.

Key terms: Social engineering, cybersecurity, psychological vulnerabilities, non-professionals, phishing attacks, internet security threats, human error threats, cognitive biases, and digital competence.

CAPITULO I.- INTRODUCCIÒN.

1.1. Contextualización problemática.

Tal es el asombroso embate de la digitalización que la sociedad ha sido alterada fundamentalmente, con una integración gradual de entornos digitales en casi todos los ámbitos de la vida, desde la comunicación hasta el comercio, la educación y el entretenimiento. En la región de Los Ríos, y en Ecuador en general, ha habido una penetración significativa de esta naturaleza digital que ha permitido a numerosos ciudadanos utilizar nuevos servicios en línea y plataformas interconectadas.

Pero el progreso viene con una sombra que muere con dificultad: el crecimiento y la sofisticación de las amenazas cibernéticas.

1.1.1. Contexto Internacional.

Incluso con defensas tecnológicas como cortafuegos, autenticación multifactor o inteligencia artificial, el eslabón más débil sigue siendo y siempre será el usuario. Todos los ataques comunes, como el phishing, el pretexto, etc., se benefician de los sesgos cognitivos básicos (universales) (autoridad, urgencia y reciprocidad) y funcionan incluso en una población bien educada.

A esto se suma que las herramientas de automatización y la inteligencia artificial han ampliado aún más su sofisticación, haciendo posible personalizar los engaños para aumentar la efectividad de estas campañas.

1.1.2. Contexto Nacional.

En Ecuador, pese al crecimiento acelerado de la digitalización, persiste una elevada vulnerabilidad humana en ciberseguridad. Una revisión sistemática de (Macías Lara, y otros, 2023) identificó que los delitos informáticos más comunes en el país resultan de errores de usuarios novatos o falta de formación en seguridad digital, siendo el phishing, acceso no autorizado y fraude los vectores principales.

Además, el estudio enfatiza la reutilización de contraseñas, la desinformación sobre prácticas seguras y el desconocimiento sobre cómo reportar incidentes, como muestras claras de la insuficiente preparación de los usuarios ecuatorianos.

1.1.3. Contexto Local.

En Babahoyo, los delitos cibernéticos combinan fraudes digitales con una precaria ciberseguridad institucional. Un artículo del 2023, publicado por (Pico Verdezoto, Bohórquez Rizzo, Delgado Jiménez, & Troya Terranova, 2023) revela que los ataques más frecuentes incluyen la suplantación de identidad y fraudes electrónicos, debido a la falta de políticas claras, formación del personal y concienciación del usuario El documento destaca que, aunque existen esfuerzos nacionales, aún se mantiene un déficit local en detección, respuesta y capacidad técnica, al tiempo que las entidades no forman activamente a su comunidad interna.

Estos hallazgos subrayan deficiencias concretas en Babahoyo:

- Usuarios internos y externos que desconocen cómo identificar correos falsos o enlaces maliciosos.
- Instituciones públicas y privadas con baja preparación para responder a incidentes, sin protocolos actualizados ni brigadas de respuesta.

- Escasa colaboración entre entidades educativas, empresas e instancias reguladoras locales, lo que reduce la resiliencia cibernética.

1.2. Planteamiento del problema.

¿Hasta qué punto pueden los modelos de vulnerabilidades psicológicas individuales identificadas en usuarios novatos ser utilizados para crear un modelo de evaluación de riesgos desplegable y técnicamente viable que permita métricas cuantificables desde la reimplementación de controles de seguridad para minimizar eficientemente la exposición a ataques de ingeniería social en la ciudad de Babahoyo?

El rápido proceso de digitalización de los entornos virtuales que cada día tienen más integración con la vida diaria en Babahoyo y la provincia de Los Ríos -Ecuador- ha abierto una gran puerta a un panorama de amenazas cibernéticas cada vez más complicado. entre todas las herramientas y sistemas de ciberseguridad en el mundo, nadie ha encontrado aún una forma de convertir el elemento humano en una solución tecnológica.

El problema aquí es el aprovechamiento repetido y la manipulación oportunista de las debilidades mentales y conductuales dominantes en los usuarios incipientes de espacios digitales. Tal es el caso de estos tipos de sujetos con experiencia más limitada en el ciberespacio (Arévalo Morales & Buitrago Ropero), o que no tienen una cultura de seguridad fortalecida y, en consecuencia, son menos capaces de percibir señales bien redondeadas de riesgo, convirtiéndolos en presa fácil para los atacantes cibernéticos. Debido a que el phishing, smishing y las estafas de ingeniería social están diseñadas intencionalmente para eludir muchos controles de seguridad técnica aprovechando los sesgos/emociones cognitivas

humanas (es decir, miedo/curiosidad/urgencia), o mediante el simple desprecio por las mejores prácticas digitales pueden ser desconcertantes.

Como lo menciona (MITRE, 2023) "es más fácil engañar a alguien para que dé una contraseña que piratear su computadora" Esta máxima subraya que, incluso con la avanzada infraestructura de seguridad actual, el punto de falla más común sigue siendo el ser humano.

El énfasis en delimitar el tema radica en un examen exhaustivo de cómo las predisposiciones humanas (tanto mentales como conductuales) interactúan con las tácticas de ataque cibernético. Esto significa investigar qué vulnerabilidades cognitivas y comportamientos digitales son manipulados sistemáticamente. Esto limita nuestro dominio de investigación a una consideración de las predisposiciones humanas (psicológicas y conductuales) que darán forma a las tácticas de ataque cibernético. Esto implica deconstruir las vulnerabilidades cognitivas y los comportamientos digitales que están siendo explotados sistemáticamente.

La delimitación del problema va muy literalmente a definir cuán efectivas pueden llegar a ser los principales vectores de ataque cibernético mencionados anteriormente, mientras cazan inmigrantes digitales con la creciente sofisticación de los agentes de amenaza.

1.3. Justificación.

El presente proyecto de investigación, titulado "Vulnerabilidades psicológicas en la susceptibilidad de usuarios novatos y su incidencia frente a ataques de ingeniería social", está basado en abordar lo que quizás sea el aspecto más importante y, a menudo, el eslabón más débil, a largo plazo de lo que ha sido el panorama de la ciberseguridad durante demasiado tiempo: los seres humanos. A pesar de un aumento notable en la infraestructura

y protegidos por inversiones en software, los incidentes de seguridad aún reiteran que los ciberdelincuentes solo encuentran una resistencia mínima cuando explotan el elemento más débil de cualquier sistema: la psicología y el comportamiento del usuario, particularmente entre los usuarios inexpertos en entornos digitales (Ramírez).

Hay millones de personas que recientemente se han acelerado hacia el mundo digital, como resultado de circunstancias actuales y extremas (como la pandemia global) que han obtenido acceso a la conectividad, pero no con una literatura comprensiva sobre seguridad digital el entendimiento al respecto sigue siendo muy básico. (Mosquera, 2024)

A lo largo de esta investigación, se responderá al "para qué" y "por qué", respecto a por qué estos ataques funcionan tan bien (más a menudo de lo que se cree, no se explotan errores de software sino atributos humanos vulnerables como sesgos cognitivos, el miedo como emoción y la curiosidad como comportamiento o incluso la higiene digital no controlada). Conocer las vulnerabilidades internas y cómo son utilizadas por los vectores de ataque cibernético es vital para diseñar una estrategia de defensa más comprensiva, pero lo más importante, altamente eficiente. El factor humano sigue siendo un vector de ataque líder en muchos incidentes, como lo destaca el Informe de Investigaciones de Brechas de Datos de Verizon (Alder, 2024), el factor humano sigue siendo un vector de ataque predominante en la mayoría de los incidentes.

En el campo inicial de la Ingeniería de Sistemas este estudio identifica una deficiencia importante en la educación terciaria, donde se aplica más énfasis en las habilidades técnicas (redes, desarrollo e infraestructura) que en integrar la perspicacia psicológica o conductual necesaria para explicar cómo los humanos toman decisiones en escenarios de riesgo digital. Por lo tanto, es posible que la falta de atención continua a las

vulnerabilidades cognitivas y emocionales pueda llevar al desarrollo de modelos de prevención solo parciales dentro del servicio directo.

La ausencia de capacitación en ciberseguridad, la falta de controles técnicos básicos (por ejemplo, filtros de correo electrónico o autenticación multifactorial), crea una ventaja para los ataques orientados al ser humano como una forma de superar las dificultades en la explotación de días cero y vulnerabilidades del sistema a través de la ingeniería social.

Este estudio contribuye a la comprensión básica de los factores humanos que hacen a los novatos más vulnerables a los ataques de ingeniería social basado en la interacción tecnología humana.

Contribuye de 3 maneras: Este trabajo contribuye a la comunidad científica tanto teórica como tácticamente, científicamente al estudiar cómo las vulnerabilidades psicológicas de los usuarios novatos afectan su debilidad frente a ataques de ingeniería social (Interacción Humano-Tecnología) a nivel fundamental.

Esta es un área de conocimiento clave para la Ingeniería de Sistemas y su comprensión debe centrarse, en los sistemas naturales, en los errores humanos y las vulnerabilidades psicológicas. Esto último no solo es una parte necesaria de la Ingeniería de Sistemas, sino que también nos ayuda a entender las fortalezas y debilidades de los sistemas de información que se construyen sobre errores humanos y vulnerabilidades psicológicas.

1.4.Objetivos de la investigación.

1.4.1. Objetivo general.

Evaluar la correlación entre las vulnerabilidades psicológicas de usuarios novatos y su susceptibilidad a ataques de ingeniería social, con el propósito de desarrollar un modelo

de evaluación de riesgos que permita integrar controles técnicos y capacitaciones adaptativas para reducir la exposición a amenazas basadas en manipulación humana en la ciudad de Babahoyo.

1.4.2. Objetivos Específicos.

- Medir la tasa de éxito de ataques simulados de ingeniería social en usuarios novatos con el propósito de validar científicamente su susceptibilidad, correlacionarla con sus perfiles psicológicos y optimizar el modelo de evaluación.
- Diseñar un marco de métricas cuantificables que permita priorizar usuarios críticos y automatizar respuestas técnicas como restricciones de acceso temporal o capacitaciones obligatorias.
- Identificar los factores psicológicos clave que incrementan la probabilidad de éxito de ataques de ingeniería social en usuarios novatos, para fundamentar técnicamente la selección de controles preventivos.

1.5. Hipótesis.

La susceptibilidad de usuarios novatos a ataques de ingeniería social está significativamente correlacionada con vulnerabilidades psicológicas específicas, lo que permite predecir su comportamiento de riesgo mediante métricas técnicas cuantificables. Esta correlación, al integrarse en un modelo de evaluación de riesgos basado en perfiles, facilitará la implementación de controles técnicos.

.

CAPITULO II.- MARCO TEÒRICO.

2.1. Antecedentes.

Uno de los vectores de ataque más antiguos y exitosos en el campo de las amenazas cibernéticas, la ingeniería social, no explota vulnerabilidades técnicas, sino que aprovecha a los humanos. Más recientemente, la literatura académica está comenzando a considerar este fenómeno desde una perspectiva holística que combina tanto la tecnología como la psicología del usuario.

La desafortunada paradoja del mundo de hoy en día, con nuevas tecnologías que se integran y conectan cada aspecto de la vida cotidiana, es que exponen unos a otros y canalizan ataques más nefastos a través de un medio tan simple como la psicología humana, a medida que avanzamos en nuestros sistemas de seguridad. Estos hallazgos se reconcilian con los resultados de estudios internacionales en tiempos recientes y ofrecen una lectura incómoda para aquellos que están seguros de cómo se puede o debe abordar la seguridad digital.

El informe DBIR 2024 de Verizon, considerado la biblia de las brechas de seguridad a nivel mundial tras analizar más de 23,000 incidentes, deja una conclusión incómoda: en el 88% de los casos en grandes empresas (aquellas con más de 500 empleados), el eslabón más débil no fue un fallo técnico, sino un error humano (verizon, 2024). Esto resulta particularmente llamativo porque precisamente estas organizaciones suelen contar con los sistemas de seguridad más avanzados. ¿Cómo explicar entonces que, teniendo firewalls de última generación y sistemas de detección de intrusos valorados en millones, un simple correo electrónico bien elaborado pueda derribar todas estas defensas?

La respuesta parece estar en cómo funciona el componente humano ante ciertos estímulos. Los atacantes han mejorado la manipulación humana y los juegos psicológicos en la versión 2023 del Marco Mitre ATT&CK. El spear phishing encabeza los métodos con una tasa de éxito del 62%, y esto también es preocupante ya que utilizan diferentes tácticas en combinación (MITRE, 2023). Por ejemplo: al principio, un correo electrónico que parece ser del jefe del departamento de TI, luego una llamada de "soporte técnico" para preguntar si recibió todos los datos correctamente y, por último, pedir que conecte un USB "con material urgente".

La situación empeora aún más, como lo revela Proofpoint en este frente de intervención humana: el 99% de los nexos para ciberataques incluyen a alguien haciendo clic, descargando o compartiendo algo (Proofpoint, 2023). Esto demuestra una realidad desafortunada: no importa cuánto dinero se invierta en tecnología defensiva, a menos que el equipo responda y actúe de manera que integre esta tecnología con sus funciones existentes/dominio operativo, los usuarios sufrirán. Por el contrario, los investigadores argumentan que los programas de concienciación bien diseñados pueden reducir el número de incidentes de una organización hasta en un 72%. El problema es que solo el 34% lo está haciendo bien, lo que significa que menos de 1/3 de todas las organizaciones.

Los experimentos de IBM Security, (2024) crean el caos de errores de esta manera. Sus estudios controlados revelan que:

- Solo el 45% de los mensajes de urgencia funcionan.
- Para aquellos que se exponen al más alto nivel de preocupación por la calidad, este número es del 38% también.
- Las ofertas de recompensa logran un 32%.

Sin embargo, la trampa fue que este grupo experimentó un aumento de efectividad al 68% cuando se combinó. Incluso las personas más razonables son capaces de ser manipuladas socialmente sin fin si la amenaza es lo suficientemente buena; es decir, cuando la lógica es derrotada tan profundamente por la naturaleza de la amenaza en sí.

(Google Project Zero, 2024) Esto también se relaciona con la Figura 4 de [0], donde un asombroso 40% de los ataques de Gmail que se realizan tienen éxito al utilizar este "úsalo o piérdelo" truco para proporcionar una carga útil atómica de tiempo transcurrido. Durante demasiado tiempo, los atacantes han comprendido que la psicología humana contiene algunos estímulos de atajo virales.

En Europa, el informe de la (Europol, 2023) también describe a estas víctimas entre los cuarenta y principios de los sesenta como las más comunes para este (aumento variable) ataque que aumenta hasta un 300% en el caso de ataques en WhatsApp con hombres y mujeres adultos en sus cuarenta años como víctimas. La necesidad de hacer esto aumenta con la disciplina y una parte significativa de aquellos que actualmente tienen que cambiar la forma en que trabajan en línea.

El costo promedio para las empresas de la ingeniería social es de $4.5 millones (PwC, 2023) "En promedio, las organizaciones con un programa de detección más maduro pueden reducir sus pérdidas en un 63 por ciento". Esto implica que la resiliencia de los empleados no solo es costosa, sino que centrarse en su valor como un costo impuesto por la ley es simplemente una estrategia para la gestión de riesgos en el mundo digital actual.

Es posible incluso aplicar el Análisis de Integración de Aplicaciones, que es efectivo porque la ciberseguridad no es solo una tecnología, sino que debes conocer la psicología de una persona. La batalla se traslada del piso de la sala de dibujo en términos de procesos mentales y emocionales que constituyen grupos de toma de decisiones bajo presión. Por eso, la estrategia debería ser construir grandes híbridos, donde sea que puedan surgir.

Así, en países como América Latina, proyectos como el de (Antonio, 2021) con una simple mención de amenazas que pueden existir solo en línea pueden llevar a personas desprevenidas a hacer clic en correos electrónicos maliciosos al darles una falsa sensación de urgencia o autoridad.

Debido a la naturaleza de la ciberseguridad, es un caso especial que merece un análisis que diferencie estos dos problemas de prueba separados. Esto se evidencia por los datos publicados en 2023 por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en su informe sobre brechas digitales en la región, que indica que el fraude cibernético en Ecuador pertenece a una serie de países más vulnerables a acciones de este tipo donde el 58% no sabe si un correo electrónico es legítimo (OECD, 2023). Esta cifra supera significativamente a países como Chile (42%) y Colombia (49%), lo que sugiere profundas diferencias en la educación digital entre naciones aparentemente similares en desarrollo tecnológico.

La Comisión Económica para América Latina y el Caribe (CEPAL) mostrò 12 programas nacionales diseñados para combatir el phishing en los países de la región, un conjunto de iniciativas que fueron analizadas por las divisiones de la CEPAL en 2023. Pero la parte más grave es que la efectividad promedio en la prevención de incidentes fue solo

del 31% (CEPAL, 2023). El anexo técnico enumeró las principales barreras como la continuidad limitada en las campañas de información, la baja adaptabilidad cultural de los materiales y la falta de indicadores para evaluar el impacto. Así que hay un par de razones por las cuales, a pesar del trabajo realizado por las administraciones y los organismos educativos, las cifras de ciberdelincuencia siguen creciendo en países como Ecuador.

La Universidad de Buenos Aires hace una nueva contribución en 2024 con su Prueba de Susceptibilidad Digital: se aplica en más de cinco países de América Latina y está validada. Por el contrario, tanto las variables demográficas como la vulnerabilidad exhibieron un valor negativo moderado promedio de β=–0.67 (University of Buenos Aires, 2024). Estas estadísticas tienen aún más gravedad cuando se yuxtaponen con la demografía en Ecuador, específicamente las víctimas.

En su Informe de Amenazas en América Latina 2023, la empresa de seguridad informática ESET se refiere a Ecuador como uno de los tres países en los que las pequeñas y medianas empresas se ven más afectadas por ataques de phishing. Afiliado del Área de Negocios de Seguridad Antivirus de (ESET, 2023). La encuesta afirma que las peculiaridades mentales de los residentes locales encuentran reflejo incluso en los métodos aplicados por los malhechores: estafa a través de procedimientos legales falsamente realizados (decisión judicial falsa), artimaña con multas de tráfico falsas e invención relacionada con deudas inexistentes dirigidas a departamentos regionales de un establecimiento financiero. Nos referimos a estos como ataques específicos del idioma, tácticas de personalización cultural que son particularmente efectivas porque eluden el contexto y la criticidad que normalmente reducen su impacto.

Kaspersky Lab reveló esto en 2024 después de realizar una investigación sobre el número de ataques de phishing dirigidos a pequeñas y medianas empresas (PYMES) en América Latina. En otros casos, como en Ecuador, los investigadores citaron estudios de caso donde las empresas fueron explotadas por un monto de $5,000-$50,000 por cada incidente de ingeniería social que condujo a una transferencia bancaria fraudulenta exitosa (Kaspersky, 2024, pág. 15). Aún más sorprendente fue el hecho de que el 68% de estas empresas no requerían ninguna validación interna para una instrucción de transferencia, y aún peor, solo el 18% capacitó a sus empleados de manera inadecuada en la identificación de señales de alerta para ataques de phishing o procesos anti-phishing.

El experimento de América Latina sugiere que, si no hacen esto, como parte de un curso de acción más amplio para fomentar su progreso, simplemente tendrá límites. Sin duda, una cultura genuina de seguridad digital comienza con la suposición de que lo que funciona para uno no funcionará para todos y considera el contexto social y económico del escenario ecuatoriano representado.

Contexto local.

La revisión sistemática de incidentes de ciberseguridad se llevó a cabo en Ecuador por (Macías-Lara, 2023) donde se enfatizó que la forma más frecuente de delito phishing, uso indebido (+fraude) y acceso no autorizado está vinculada a la falta de conocimientos básicos de seguridad digital de los usuarios. Su análisis también destaca cómo las políticas de capacitación en empresas públicas y privadas deben trabajar juntas.

En 2023, el Servicio Nacional de Derechos Intelectuales contribuyó con un análisis legal en su publicación homónima que la provincia de Los Ríos había sufrido 120 denuncias de estafas digitales. Su investigación reveló que el método más utilizado (45% de los casos) fue la suplantación de soporte técnico, en la que los atacantes se identificaban como representantes de organizaciones de telecomunicaciones o servicios de TI (SENADI, 2023, pág. 29). Esto funcionó especialmente bien con personas mayores y propietarios de pequeñas empresas, ambos conocidos por confiar mucho en los 'expertos'.

El Banco Central de Ecuador pintó un panorama más claro en 2024 con algunos datos económicos reales: las pérdidas por fraude en línea superaron los $42 millones solo en la primera mitad del año, aumentando un 37% anualmente (Banco Central del Ecuador., 2024, pág. 12) . Pero aquí está el punto clave: el 68% de estos casos tenía un elemento de ingeniería social, demostrando que el elemento humano sigue siendo el eslabón más débil en la ciberseguridad.

Estos estudios muestran que los temores de larga data sobre el "juego regional" persisten incluso en una era de adaptaciones islamistas más sofisticadas y culturalmente sintonizadas a las operaciones terroristas, mientras que las realidades defensivas hacen poco o nada para abordar lo que es muy específicamente un problema psicológico.

Entre los ataques exitosos en la ciudad de Babahoyo, la mayoría se verificó que resultaron de robo de identidad y fraude en línea (Pico Verdezoto, 2023) , mostrando que los controles técnicos fallaron efectivamente, junto con una educación limitada del usuario final. Las áreas de alto riesgo: el autor señaló la falta de protocolos, la cantidad de capacitación institucional y la conciencia cibernética como de alto riesgo.

2.2. Bases teóricas.

Fundamentos Psicológicos.

La ciberseguridad es básicamente una colección de barreras tecnológicas en el mundo de la ingeniería de sistemas: cortafuegos, cifrados y mecanismos de defensa más avanzados. Sin embargo, estudios más recientes muestran que, con mucho, el peligro más apremiante de todos surge de la dimensión humana. Comprender por qué incluso los profesionales con las mejores intenciones podrían caer presa de tales tácticas requiere un examen de la psicología humana.

Mientras que estas funciones cognitivas solían ser una innovación evolutiva que salvó a los humanos de la extinción, en el mundo digital de hoy es el talón de Aquiles. La Teoría del Comportamiento Planificado elaborada por (Ajzen, 2020, pág. 45) como un marco analítico de sistemas también es ilustrativa; sugiere que el comportamiento humano no puede determinarse completamente por si los humanos tienen o no conocimiento y que la interacción entre factores incentivadores y actitudes, normas subjetivas y elementos de control conductual percibido son lo que realmente dictan el comportamiento. En realidad, es esta situación la que permite a un trabajador identificar las amenazas y, sin embargo, abrir un enlace malicioso si ha llegado en un correo electrónico de su jefe o de alguien con autoridad.

De manera similar, en una investigación longitudinal de (Díaz, 2023), sobre organizaciones de la industria tecnológica donde los empleados reciben una cantidad significativa de capacitación, solo hasta el 68% confesó que han desertado o violado necesidades de seguridad sumamente cruciales en el trabajo bajo situaciones de alta presión, como la presión social, lo que lleva a disminuir el comportamiento de aprendizaje

y afectar la fidelidad. Pero no por nada, este es un claro ejemplo de cómo funciona el cerebro humano en los escenarios laborales actuales, donde la mayoría de los aprendizajes realizados en esos emocionantes programas de capacitación en ciberseguridad son superados por jerarquías y cultura empresarial.

Lo cual es también la razón por la que los sesgos cognitivos, o los atajos mentales que permiten tomar decisiones más rápidas, posiblemente sean una de las herramientas más explotables para los actores maliciosos. Como menciona (Kahneman, 2021, pág. 78) en su libro: "Hay tanto un sesgo de autoridad que hará que las facturas obedezcan a figuras de mayor rango incluso cuando muestren un peligro claro."

En otro estudio de caso de CERT/CC de 2024, el atacante pudo hacerse pasar por un vicepresidente de la empresa y atraer a cinco empleados para que revelaran credenciales y otros detalles personales en solo 17 minutos (National Cybersecurity Alliance, 2024, pág. 23). Pero mucho más importante, el efecto de urgencia, un sesgo psicológico inducido por restricciones de tiempo que usurpa el procesamiento racional.

La investigación de Neuro Seguridad de la (Stanford University , 2023) exactamente los estudios de resonancia magnética funcional (FMRI) por medio de mensajes de phishing donde se les decía que su cuenta sería suspendida “si no participaban en 15 minutos”, mostraron que activaron un área del cerebro responsable de cuando se está lidiando con una amenaza física.

Como defensor de la ingeniería social, el campo que estudia el impacto que los defectos cognitivos y emocionales humanos pueden tener en los ciberataques, Hadnagy dice que los atacantes no solo van tras sistemas informáticos comprometidos (Hadnagy C. ,

2021, pág. 12). Su investigación, realizada con excriminales, muestra cómo adaptan enfoques según varios motivadores psicológicos humanos subyacentes.

Esta estrategia se llama quid pro quo, que es una mentalidad de intercambio de "tú me das esto y yo te doy aquello", que se basa en un condicionamiento cultural ya establecido hacia la reciprocidad, mientras que las tácticas de cebo explotan la curiosidad humana natural.

Un estudio controlado en instalaciones gubernamentales y públicas encontró que el 89% de los dispositivos se conectaron a máquinas corporativas en menos de 48 horas.(JIW, 2024, pág. 34), demostrando cómo los impulsos superan a la razón cuando se cree que nadie observa.

La Teoría de la Protección Motivada realizada por (Rogers, 2020) ,sin embargo, incluye más crucialmente que una persona no puede actuar de manera segura a menos que también acepte que el peligro es grave, su probabilidad de desarrollarlo y su capacidad para tomar medidas útiles (Rogers, 2020, pág. 90). Este modelo también explica por qué la capacitación genérica tradicional fracasa, ya que los datos sobre los volúmenes globales de ciberataques no crean una sensación de riesgo personal es similar a cuando se observan las advertencias sobre el tabaquismo como poco convincentes para hacer que un joven piense que podría terminar con cáncer.

El libro blanco sobre Resiliencia Digital en PYMEs (Fernández L. , 2024) señaló que solo el 12% de los empleados que asistieron a charlas estándar sobre phishing decidieron cambiar su comportamiento, mientras que el porcentaje aumentó hasta el 63% entre aquellos involucrados en capacitación personalizada que incluía experimentar

simulaciones realistas y consecuencias negativas de su error (aunque ficticias y sin ningún daño real).

Pero quizás aún más interesante es un descubrimiento de la neurociencia afectiva. Tales simulaciones encontraron que los correos electrónicos de spear-phishing sofisticados eran tan propensos a involucrar las redes de miedo y recompensa, activando tanto la amígdala (centro del miedo) como el núcleo accumbens (sistema de recompensa del cerebro), apagando la corteza prefrontal, donde ocurre nuestro razonamiento explícito (Dìaz & Cortès, 2023, pág. 145). No es una distracción fácil; es un secuestro puro del sistema de toma de decisiones. Aún peor, estos efectos se magnifican bajo el estado de estrés y cansancio en el que la mayoría de las personas corporativas viven cada día.

En cuanto a los controladores de tráfico aéreo, un ensayo clínico reveló que su vulnerabilidad a ataques simulados era un 300% mayor en días de alta carga de trabajo que en días tranquilos (Analysis: Commercial Aviation Cybersecurity Threats in 2025, 2025).

Estos fundamentos psicológicos nos dicen que la seguridad efectiva es más que políticas y manuales de procedimientos. Requiere aceptar que, cuando se provoca con algún estímulo desconocido, incluso el personal completamente capacitado se comportaría de manera irracional y estúpida. Esta idea está bien expresada por el Profesor Alan Dupont, de la Universidad de Sídney, quien concluye: "Podemos instalar todos los parches técnicos del mundo, pero hasta que no parcheemos la psicología humana, seguiremos perdiendo esta guerra" (Ciberseguridad global, 2024, pág. 15).

Aspectos técnicos.

Los modelos de ciberseguridad donde la tecnología está involucrada son centrales para el conocimiento y la práctica respecto a la susceptibilidad de la ingeniería social; particularmente la vulnerabilidad psicológica en usuarios inexpertos, durante el comportamiento digital.

En consecuencia, se han desarrollado marcos teóricos por grupos de expertos e instituciones basados en esto, que se centran en agregar la dimensión humana a los elementos tecnológicos para otorgar a las estrategias de protección contra desastres más efectividad. Lo hacen ya que son útiles para identificar riesgos, definir controles adaptativos y especificar políticas de seguridad que reconozcan las limitaciones cognitivas y los comportamientos humanos de los usuarios (especialmente aquellos más propensos a ser atacados mediante manipulación psicológica).

Al proporcionar una visión más completa de la autenticación digital, más allá de solo los aspectos técnicos, aportando conocimientos derivados de la observación del comportamiento humano en estos sistemas El Instituto Nacional de Estándares y Tecnología, en su publicación SP 800-63B (NIST, 2023) más allá de esta capa puramente tecnológica. Establece el tipo de verificación de identidad, como la autenticación multifactor (MFA), que debería requerirse en el documento, pero también entiende que los usuarios inexpertos son a menudo una gran vulnerabilidad de seguridad porque tienden a usar contraseñas débiles (o incluso repetir aquellas fácilmente adivinables) o ser manipulados a través de la ingeniería social.

El modelo NIST enfatiza la necesidad de equilibrar mecanismos robustos pero utilizables, para que los usuarios puedan procesar la seguridad de una manera amigable para el cerebro. Propone abandonar solo las contraseñas, a favor de algo como

autenticadores biométricos o tokens físicos que son más difíciles de suplantar. También destaca la importancia de la educación continua, aunque para perfiles no técnicos, requiere que use un lenguaje simple y ejemplos vívidos suficientes para que las partes interesadas detecten signos de fraude por sí mismas sin tener un nivel de conocimiento de experto o científico informático.

La norma ISO/IEC 27002, que proporciona un marco de referencias sobre todas las medidas preventivas, correctivas, detectivas y reactivas teniendo en cuenta el comportamiento humano (Organización Internacional de Normalización y Comisión Electrotécnica Internacional, 2023). En lugar de centrarse solo en las medidas habituales como cortafuegos o cifrado, el patrón considera elementos más profundos, es decir, vulnerabilidades psicológicas que sin un tratamiento adecuado podrían potencialmente dejar impotentes incluso a los sistemas más sofisticados. Lo más intrigante de ellos apunta hacia programas de concienciación para diferentes niveles de alfabetización digital entre los usuarios, en un intento de evitar adherirse a un enfoque único que prácticamente ha perdido el rumbo. Además, las directrices dictan que una solución podría ser reglas para permitir la discriminación de acceso tanto por el rol a desempeñar en la organización como por el perfil psicológico del usuario, de modo que, si son engañados, su potencial de impacto disminuirá.

Entre la contribución original de este marco, se encuentran nuevos enfoques para revisar continuamente las amenazas a través de un indicador de vulnerabilidad psicológica que puede ser dirigido para recursos de capacitación o supervisión adicionales, como sugiere (Fernandez, 2024).

Pero el Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP, 2024) va un paso más allá con la introducción del sistema OWASP Top 10 Human Risks, que hace posible obtener antecedentes sobre vulnerabilidades humanas atacadas específicamente a través de la ingeniería social únicamente. Este nivel es esencialmente un catálogo de prácticas repetidas, como si es más o menos propenso a confiar en mensajes oficiales (phishing), actuar impulsivamente bajo manipulación (pretexting).

El Proyecto de OWASP informa que los principiantes están en mayor riesgo aquí, ya que nunca han estado expuestos a técnicas de manipulación y, por lo tanto, son los candidatos más probables para subestimar los riesgos o sobrevalorar su capacidad en el control de detección de fraudes. En respuesta a esto, el modelo recomienda intervenciones de psicología conductual: proporcionar a los usuarios actividades basadas en escenarios que les permitan sentir las repercusiones para que puedan tener memoria muscular.

También señalaría a través de "empujones" para incentivar los mejores comportamientos seguros con recordatorios (por ejemplo, verificar las URL antes de permitir, o no desactivar alertas de seguridad en aplicaciones clave).

Ya hay una contribución original a este campo: La Escala de Resistencia Psicológica desarrollada por (Fernandez, 2024), proporciona un instrumento validado para medir la vulnerabilidad psicológica de los individuos al engaño.

A diferencia de la mayoría de los modelos anteriores, que se centran concretamente en un mecanismo u otro esquema que es cierto solo en ciertas situaciones y condiciones, esta escala está destinada a converger un poco en diferentes matices psicológicos (como la impulsividad, cuán propensa es una persona a preocuparse por temas desconocidos o cuán

buen consumidor del sector bancario parece ser) pero al mismo tiempo predice su potencialidad para ser objeto de ingeniería social. Una persona impulsiva puede tomar una decisión precipitada sin considerar el contexto, mientras que un individuo bajo estrés podría sentir que no puede arriesgarse a ignorar un enlace malicioso de alguien.

Lo que hace es realizar una selección de subpoblaciones por riesgo e incluso una tarea más sofisticada para personalizar las intervenciones: por ejemplo, los trabajadores en roles clave podrían beneficiarse de talleres de manejo del estrés, mientras que se pueden implementar diferentes herramientas según los estilos de aprendizaje, dependiendo de las preferencias cognitivas.

El modelo tradicional en ciberseguridad se centraba solo en software y hardware, pero ahora es más inclusivo. En la Seguridad Centrada en el Usuario se enfatiza la incorporación de consideraciones tanto de facilidad de uso como de concienciación sobre seguridad en el diseño del sistema para minimizar el vector de ataque humano. Como argumentan (Ribeiro , Amaral , & Barros , 2021) ,las políticas de seguridad pueden tener en cuenta la capacidad real del usuario para seguir los protocolos sin sobrecargar su sistema cognitivo o introducir errores en el uso.

Variable de Salida: En la columna predictiva, incluimos estudios que pronostican comportamientos de riesgo con otros que también enfatizan una mezcla de variables psicológicas y demográficas dentro de un modelo de aprendizaje automático (Hernandez, Gòmez, & Pèrez, 2024) . Aunque comprende un componente técnico serio, la relevancia teórica proviene de establecer la capacidad de predecir vulnerabilidades humanas utilizando datos no tradicionales (respuestas de encuestas o elementos con una geometría similar a las plataformas de entrenamiento).

La investigación mostró que, por ejemplo, los usuarios con baja experiencia digital y alta confianza en su capacidad (el efecto Dunning-Kruger) subestiman significativamente la complejidad de las amenazas y, por lo tanto, pertenecen a un grupo aún más vulnerable.

Modelos técnicos para enfoques psicológicos y predictivos integrados con estándares NIST e ISO es un marco sólido para abordar la vulnerabilidad humana en ciberseguridad. El valor de las mismas radica no solo en su capacidad para reducir riesgos a nivel individual, sino que también está destinado a proporcionar una suma mayor que sus partes, combinando un análisis técnico riguroso y sistemático con una apreciación de la fragilidad humana.

Esto es especialmente importante dado un ecosistema en el que los atacantes siempre están adaptando sus técnicas de manipulación y manipulando instintos perfeccionados por innumerables generaciones, no solo explotando fallos del sistema, sino también los atajos cognitivos y emocionales integrados en las personas. Por lo tanto, una estrategia de seguridad efectiva debe tratar estos modelos como complementarios, lo que significa que todas las soluciones técnicas serán seguidas por incentivos humanizados para usuarios novatos.

Marco Conceptual

Este marco de investigación se basa en la definición central de comprensiones que permite establecer el enfoque sobre las vulnerabilidades psicológicas entre los jóvenes, así como criterios estandarizados sobre ataques de Ingeniería Social. Estas definiciones son proporcionadas por organizaciones internacionales (como ISO/IEC y NIST) que proporcionan una base sólida para la terminología que se usa para describir los fenómenos

que se buscan analizar, evitando que surjan ambigüedades como parte de la participación en este campo en línea con estos estándares.

La norma ISO/IEC 27032, 2022, titulada Directrices para la Ciberseguridad, define términos básicos como ingeniería social, compromiso psicológico y disuasión del usuario. En aquel apartado la ingeniería social se define como “un conjunto de herramientas y técnicas diseñadas para engañar a las personas para que proporcionen información o realicen alguna acción que no deberían, generalmente por razones maliciosas”.

Cabe señalar que esta definición erosionará las discusiones previas centradas en las vulnerabilidades técnicas y la ingeniería social, lo cual es un reflejo de cómo convencería a los protocolos en sistemas seguros, a pesar de una ilusión de garantía envolvente. Además en, la (ISO/IEC 27032, 2022) son los usuarios novatos, generalmente los menos conocedores y más susceptibles a sesgos como la confianza/autoridad o el miedo a la autoridad, son aquellos para quienes es más significativo.

Complementando estas definiciones, el (NIST SP 800-181, 2023) proporciona un Glosario de Términos que ayuda a los profesionales a diferenciar conceptos además de las definiciones. Por ejemplo: Susceptibilidad como "la probabilidad de que una persona o grupo actúe en respuesta a estímulos engañosos debido a integridades como la educación y el tiempo proporcionado, y la personalidad". Esta definición amplía la discusión y toma en cuenta factores demográficos y psicológicos que, aunque dos nuevos usuarios estén expuestos a las mismas amenazas, uno de ellos se vuelve mucho más crítico que el otro.

Por el contrario, el Documento (NIST SP 800-181, 2023) define un ataque de ingeniería social como "un método utilizado para eludir elementos de seguridad que

involucra el elemento humano y generalmente implica engañar a las personas para que rompan sus prácticas normales de seguridad". Esta definición describe muy bien ambas formas de ataque, ya que a menudo se sincronizan con un perfil psicológico de su víctima como anillo al dedo.

Una de las piezas más importantes que conectan ambos marcos es la diferencia entre la vulnerabilidad técnica y la humana. Mientras que las fallas en los sistemas o el software están destinadas a ser corregidas mediante parches o actualizaciones en el primero, el segundo cubre limitaciones inherentes en el comportamiento humano que a menudo persisten a pesar de los esfuerzos iterativos. ISO/IEC 27032, 2022 señala que la existencia generalizada de vulnerabilidades humanas críticas como "la ausencia de escepticismo hacia mensajes inesperados" ocurre en entornos donde los usuarios están condicionados a priorizar la eficiencia sobre la seguridad. Esta idea se refuerza en él NIST SP 800-181, 2023, explica además que estas exposiciones a vulnerabilidades son explotadas por "el desarrollo de narrativas basadas en el miedo, la urgencia o la curiosidad".

La resiliencia psíquica es otro término básico en el esquema interpretativo, y aunque no está declarado directamente por los estándares citados, se puede entender como 'la capacidad de un individuo para resistir (o recuperarse de) intentos de manipulación, teniendo en cuenta factores como la conciencia situacional, la formación continua y el apoyo de su institución.

Siguiendo esta importante distinción está la capacidad no solo de examinar por qué algunas personas son víctimas de phishing, sino también cómo otras evitan caer en ataques de phishing, aunque puedan tener antecedentes demográficos o experiencia similares.

Estas interrelaciones entre estos conceptos: ingeniería social, vulnerabilidad psicológica, susceptibilidad y resiliencia construyen el tema central y el método en la investigación. Esto no solo imparte movilidad a las definiciones, sino que también las convierte en un lenguaje que permite discusiones tanto académicas como prácticas basadas en un terreno común.

Además, la estandarización de intervenciones también puede ayudar a identificar fisuras esenciales, como la necesidad de crear medidas cuantitativas para evaluar la susceptibilidad o idear estrategias de formación que aborden aspectos emocionales y cognitivos más allá de la mera transferencia de conocimiento factual.

En este sentido, el marco conceptual presentado en este documento define qué estudiar, junto con la terminología necesaria para un análisis psicológico maduro de cómo los ataques de ingeniería social apuntan a vulnerabilidades específicas de usuarios novatos. Consistente con los estándares internacionales, este marco está diseñado para ser robusto y aplicable, sustentando esfuerzos de investigación que pueden combinar elementos cara a cara del ciberespacio desde puntos de vista tanto técnicos como conductuales.

CAPITULO III.- METODOLOGÌA

1.1. Tipo y diseño de investigación.

El estudio se basa en el paradigma cuantitativo y cualitativo, debido a su objetivo de medir, correlacionar y observar objetivamente los factores que determinan la susceptibilidad humana a los vectores de ingeniería social en los sistemas de información.

Punto de medición u observación: Procesos dentro de un grupo. Unidades de muestreo: Empleados. Motivo: Detectar determinantes de la ingeniería social. Datos previos utilizados: Ninguno.

Este tipo de enfoque permite convertir las observaciones del comportamiento del usuario en evidencia numérica estadística que puede ser utilizada para examinar fenómenos de causa y efecto o al menos una correlación positiva entre variables.

El diseño también presenta un componente aplicado, ya que sus resultados están destinados a apoyar estrategias técnicas y preventivas en el campo de la ciberseguridad, más específicamente a través de la gestión de usuarios dentro de los sistemas de información.

"En este tipo de enfoque es posible probar hipótesis, establecer relaciones entre variables y utilizar herramientas estadísticas para la verificación" (Hernández Sampieri, 2014).

1.2. Operacionalización de variables.

Tabla 1: *Variable Independiente: Vulnerabilidades Psicologicas.*

Variable	**Dimensión**	**Indicadores**	**Instrumentos**
Vulnerabilidades Psicológicas	Cognitiva	- Tiempo de reacción frente a correos electrónicos sospechosos. - Precisión en la identificación de enlaces falsos. - Reconocimiento de remitentes fraudulentos.	- Simulaciones controladas de ataques. - Registro automatizado de interacciones. - Cuestionarios post-simulación.

	Emocional	- Nivel de respuesta ante mensajes urgentes o amenazantes. - Grado de confianza en figuras de autoridad simuladas. - Reacciones bajo presión digital.	- Escalas tipo Likert posteriores a la simulación. - Observación directa. - Análisis conductual.
	Conductual	- Conexión de dispositivos USB desconocidos. - Ejecución de scripts sin validación. - Respuesta ante solicitudes de datos no verificadas.	- Registro de actividad en laboratorio. - Observación en simulación.

Tabla 2: *Variable Dependiente: Susceptibilidad a la Ingeniería Social*

Variable	Dimensión	Indicadores	Instrumentos
Susceptibilidad a la Ingeniería Social	Exposición	- Número de ataques exitosos durante simulaciones. - Tipos de ataques que lograron éxito. - Porcentaje de interacciones inseguras.	- Registro en hojas de cálculo. - Análisis estadístico en KNIME. -Comparación de métricas por usuario.
	Riesgo Técnico	- Ejecución de software malicioso sin verificación. - Uso indebido de credenciales en entornos inseguros. - Falta de medidas básicas de seguridad.	- Simulación en entornos virtualizados. - Checklists técnicas. - Observación estructurada.

	Prevención	- Capacidad de detener la interacción con un ataque. - Aplicación de buenas prácticas digitales. - Respuesta correcta en pruebas de concienciación.	- Evaluación antes y después de simulaciones. - Entrevistas cortas. - Pruebas de conocimientos.

1.3. Población y muestra de investigación.

3.3.1. Población

En general, hubo 90 personas inicialmente preseleccionadas antes de alcanzar la población objetivo, compuesta por una comunidad más grande que los 66 participantes activos. La filtración, basada en el acceso a dispositivos personales, la disponibilidad para realizar simulaciones y criterios éticos (por ejemplo, consentimiento informado), produjo una cohorte experimental limitada a aquellos que cumplían con todos los requisitos de elegibilidad.

Es importante enfatizar que esta población fue examinada en un sentido más amplio, que involucraba tanto aspectos técnicos como conductuales. Para considerar otros tipos de directrices, a saber, de estándares internacionales como ISO/IEC 27002 y el marco NIST SP 800-63B, una posibilidad fue abrir el análisis de perspectiva sobre aspectos de TI y ver al ser humano como un vector de riesgo. Por lo tanto, se investigaron más a fondo tales vulnerabilidades psicológicas existentes (dimensiones cognitivas y emocionales, así como conductuales) y la susceptibilidad a la ingeniería social en escenarios simulados con ataques reales.

3.3.2. Muestra.

La muestra final de la investigación comprendió 66 participantes, obtenidos mediante una selección no probabilística intencionada: conveniencia. Se utilizò un método de muestreo por conveniencia, ya que el acceso y la disponibilidad de ciertos parámetros característicos en los sujetos de la muestra eran requeridos por los objetivos de la investigación: individuos sin experiencia en ciberseguridad con algún nivel básico de interacción tecnológica. Aunque pequeña, esta fue una muestra muy conveniente para los propósitos de una investigación experimental sobre las acciones de usuarios no expertos digitales respondiendo a manipulaciones simuladas en entornos digitales.

Estas pruebas simulaban ataques reales de ingeniería social: correos electrónicos de phishing, SMS falsos (smishing), llamadas fraudulentas (vishing y pretexting) y dispositivos físicos para comprobar las personas que tomarían USBs o scripts en un entorno sin validación. Estas demostraciones fueron registradas a través de herramientas automatizadas y observación humana. Toda la información se ingresó en hojas de cálculo a medida que avanzaba, y se realizó un análisis adicional en plataformas especializadas como KNIME para procesar rigurosamente los datos.

Se seleccionaron criterios para esta muestra que incluyeran, no haber sido entrenados en seguridad digital, tener un dispositivo electrónico personal (computadora o smartphone) y estar dispuestos a participar en escenarios simulados bajo condiciones seguras y controladas. Además, la muestra fue preseleccionada con un diagnóstico de línea base que medía habilidades básicas en computación para verificar que la muestra realmente representaba los perfiles de riesgo previstos.

El grupo objetivo consistía en hombres y mujeres de diversos niveles educativos y entornos corporal, con edades entre 17 y 45 años, a través de los cuales se podían detectar diferencias en el comportamiento asociadas con el factor generacional y el grado de familiaridad tecnológica. Al incluir esta diversidad, se pudo señalar correlaciones significativas que reforzaron tanto las percepciones introspectivas (cualitativas) como los hallazgos cuantitativos, corroborando personas comunes relacionadas con ataques exitosos..

En esencia, esta muestra proporcionó una instantánea de cómo aquellos que son nuevos y que aún no han desarrollado defensas cognitivas ni capacidades técnicas son fácilmente explotados como puntos débiles en el panorama de la seguridad digital. Los resultados de su comportamiento ante ataques simulados correspondieron con la hipótesis de la investigación, pero también mostraron que un mayor énfasis en fomentar la conciencia y utilizar defensas humanas de seguridad necesita combinarse con estrategias de defensa técnica si se qiere prevenir riesgos asociados con la ingeniería social.

1.4. Tècnicas e instrumentos de mediciòn.

1.4.1. Técnicas

La presente investigación empleó un enfoque mixto fundamentado en la recolección de datos tanto cuantitativos como cualitativos Las técnicas elegidas nacen de la necesidad de comprender, con un enfoque detallado, cómo reaccionan los usuarios con poca formación en ciberseguridad cuando se enfrentan a intentos de engaño digital. Para ello, se contemplaron aspectos clave de su comportamiento, como la forma en que procesan la información, sus respuestas emocionales ante situaciones de presión y las acciones concretas que ejecutan durante una amenaza simulada, así como su grado de exposición y capacidad de prevención frente a amenazas cibernéticas.

Entre las técnicas principales utilizadas se encuentran las simulaciones controladas de ataques, diseñadas meticulosamente para replicar escenarios reales de amenazas como phishing, baiting, pretexting, smishing y vishing. Estas simulaciones permitieron observar el comportamiento espontáneo de los participantes en condiciones casi idénticas a las del entorno digital cotidiano. Su valor metodológico radica en que exponen reacciones auténticas del usuario, sin la influencia de respuestas socialmente deseables.

Otra técnica relevante fue la observación directa, mediante la cual se documentaron las acciones de los participantes durante y después de las simulaciones. Esta técnica aportó una visión profunda del componente emocional y de la toma de decisiones bajo presión. También se implementó el análisis conductual de patrones de respuesta, permitiendo identificar sesgos cognitivos recurrentes como la urgencia, la confianza en figuras de autoridad y la impulsividad.

Complementariamente, se aplicaron evaluaciones previas y posteriores a las simulaciones con el fin de medir la evolución en el nivel de conciencia del usuario sobre ciberseguridad. Estas evaluaciones fueron claves para comparar la capacidad de identificación de amenazas antes y después de la exposición a los ataques simulados.

1.4.2. Instrumentos

Para garantizar la validez y confiabilidad de la información obtenida en la investigación, se diseñó y aplicó un conjunto de instrumentos de recolección de datos alineados con las variables planteadas y ejecutados en un entorno controlado de laboratorio. Estos instrumentos permitieron capturar tanto datos cuantitativos como cualitativos, complementando el análisis integral de los resultados.

a) Registro automatizado de interacciones.

Durante las simulaciones de ataques de ingeniería social (phishing, smishing, vishing, pretexting y baiting) se emplearon mecanismos de captura automática que documentaron métricas objetivas como tiempos de reacción, clics en enlaces maliciosos, inserción de dispositivos USB y ejecución de scripts. Los datos fueron almacenados en hojas de cálculo de Microsoft Excel, lo que permitió su organización inicial, así como su posterior análisis estadístico mediante funciones de tablas dinámicas, filtros, promedios y desviaciones estándar.

b) Cuestionarios post-simulación.

Se aplicaron formularios estructurados con escalas tipo Likert, orientados a evaluar el nivel de percepción de riesgo, las emociones experimentadas y el reconocimiento de errores cometidos durante las simulaciones. Este instrumento permitió obtener información subjetiva de los participantes y contrastarla con las métricas objetivas recolectadas.

c) Observación directa y bitácoras técnicas.

En el laboratorio se documentaron, mediante observación estructurada y registros en bitácoras, conductas relevantes como la conexión de hardware desconocido, el uso de credenciales en portales fraudulentos y otras prácticas inseguras. Estos registros complementaron los datos automatizados y proporcionaron una visión cualitativa y conductual de los participantes.

d) Pruebas de conocimientos y entrevistas breves.

Con el fin de evaluar la dimensión preventiva y medir el nivel de conciencia en ciberseguridad, se aplicaron pruebas de conocimientos antes y después de las simulaciones,

además de entrevistas cortas que permitieron profundizar en las justificaciones dadas por los participantes respecto a sus decisiones digitales.

Finalmente, el procesamiento y análisis de la información recolectada se llevó a cabo utilizando Microsoft Excel y la plataforma KNIME (Konstanz Information Miner). Excel permitió la codificación inicial de respuestas y la obtención de estadísticas descriptivas, mientras que KNIME facilitó análisis avanzados como correlaciones, pruebas de hipótesis y visualizaciones gráficas. Esta combinación de instrumentos y técnicas aseguró un tratamiento de datos riguroso, sistemático y replicable, en concordancia con los objetivos de la investigación.

Tabla 3: *Instrumentos de recolecciòn.*

Variable	Dimensión	Indicadores	Instrumento
Vulnerabilidades Psicológicas	Cognitiva	• Tiempo de reacción ante correos sospechosos. • Precisión en la identificación de enlaces falsos. • Reconocimiento de remitentes fraudulentos.	Registro automatizado de interacciones (Excel y KNIME).
	Emocional	• Nivel de respuesta ante mensajes urgentes. • Confianza en figuras de autoridad simuladas. • Reacciones bajo presión digital.	Cuestionarios post-simulación (escala Likert).
	Conductual	• Conexión de dispositivos USB desconocidos. • Ejecución de scripts sin validación. • Ingreso de	Observación directa y bitácoras técnicas.

		credenciales en sitios fraudulentos.	
Susceptibilidad a la Ingeniería Social	Exposición	• Número de ataques exitosos. • Tipos de ataques que lograron éxito. • Porcentaje de interacciones inseguras.	Registro en hojas de cálculo (Excel) y análisis en KNIME.
	Riesgo Técnico	• Ejecución de software malicioso. • Uso indebido de credenciales. • Falta de medidas de seguridad.	Simulaciones en entorno controlado y checklists técnicas.

1.5. Procesamiento y análisis de los datos.

El procesamiento y análisis de los datos se realizó utilizando KNIME (Konstanz Information Miner) y Microsoft Excel, herramientas que permitieron organizar, limpiar y analizar estadísticamente la información recolectada mediante encuestas y simulaciones de ataques de ingeniería social.

Microsoft Excel

- Se empleó para la organización inicial de los datos, creando una matriz donde se codificaron las respuestas de los participantes (ejemplo: "Sí" = 1, "No" = 0).
- Se utilizaron funciones básicas como tablas dinámicas, filtros y fórmulas (promedio, desviación estándar, conteos condicionales) para obtener estadísticas descriptivas.

KNIME (Konstanz Information Miner)

Se utilizó para:

- Importar datos desde Excel (mediante el nodo Excel Reader).
- Limpiar y filtrar datos (eliminar valores nulos, normalizar respuestas).
- Realizar análisis estadísticos (correlaciones, pruebas de hipótesis).
- Generar visualizaciones (gráficos de barras, dispersión, heatmaps).

Carga de Datos

- Se utilizó el nodo "Excel Reader" para importar los datos desde el archivo Excel.
- Se configuró para leer las hojas correspondientes a las respuestas de encuestas y simulaciones.

Limpieza y Preparación de Datos

- Filtrado de datos: Se eliminaron respuestas incompletas con el nodo "Row Filter".
- Transformación de variables: Se convirtieron respuestas cualitativas (ej. "Sí/No") a valores numéricos (1/0) con el nodo "Rule Engine".
- Normalización: Se estandarizaron escalas Likert para evitar sesgos en el análisis.

Análisis Estadístico

- Estadísticas descriptivas: Mediante el nodo "Statistics", se obtuvieron promedios, medianas y desviaciones estándar de las variables clave.
- Correlaciones: Con el nodo "Linear Correlation", se calcularon las relaciones entre vulnerabilidades psicológicas y susceptibilidad a ataques.

- Pruebas de hipótesis: Se aplicó el nodo "T-Test" para comparar grupos (ej. usuarios con alto vs. bajo riesgo).

Visualización

- Gráficos de barras: Para comparar tasas de éxito en diferentes tipos de ataques (phishing, smishing, etc.).
- Diagramas de dispersión: Para observar relaciones entre variables (ej. impulsividad vs. clics en enlaces maliciosos).
- Heatmaps: Para identificar patrones en subgrupos (ej. usuarios mayores vs. jóvenes).

Exportación de Resultados

Los resultados se exportaron a PDF mediante el nodo "PDF Writer" para su inclusión en el informe final.

Correlaciones significativas:

- Se confirmó que los usuarios con mayor impulsividad ($r = 0.63$) y ansiedad digital ($r = 0.59$) tenían mayor probabilidad de caer en ataques de phishing.
- La falta de formación en ciberseguridad mostró una correlación negativa ($r=-0.71$) con la capacidad de detectar amenazas.

Diferencias entre grupos:

- Los usuarios mayores de 40 años presentaron mayor susceptibilidad a ataques basados en autoridad ($p < 0.05$).

- Los participantes con baja autoconfianza digital fueron más propensos a compartir datos bajo presión.

Validación Empírica de la Hipótesis

La hipótesis queda empíricamente validada, pero con matices críticos:

- No todas las vulnerabilidades psicológicas tienen igual peso: La impulsividad y la urgencia son dominantes.
- La formación técnica mitiga, pero no elimina el riesgo, pues los sesgos operan a nivel subconsciente.
- El modelo resultante trasciende lo académico: ofrece un framework técnico accionable para políticas de seguridad en organizaciones ecuatorianas, especialmente en sectores con usuarios novatos como instituciones públicas y PYMES de Babahoyo.

1.6. Aspectos éticos.

La investigación es un estudio de un factor humano de la ciberseguridad; por lo tanto, las preguntas relacionadas con las personas incluyen grandes riesgos en el lado de la ética. El diseño del proyecto asegura el respeto, la dignidad, la autonomía y la seguridad de los individuos involucrados al incluir protocolos que fueron aprobados por un especialista en el tema de ética y están de acuerdo con los estándares éticos nacionales e internacionales actuales.

• Consentimiento Informado.

Antes de la distribución de datos, se proporcionará a todos los participantes una presentación comprensible sobre los objetivos del estudio, los tipos y riesgos de la participación y el uso previsto de la información. Se obtendrá un consentimiento informado, firmado y por escrito, utilizando un documento aprobado por el comité de ética de investigación institucional que indique su participación voluntaria en el estudio y que pueden retirarse del estudio en cualquier momento sin comprometer su identidad.

• Confidencialidad y Manejo de Datos.

Todos esos datos se mantendrán bajo estrictas medidas de confidencialidad. Los datos se despojarán de información identificativa y se cifrarán para que sea imposible identificar directamente a los participantes. No se informarán nombres ni ninguna otra información identificativa en ninguna parte del informe final ni en las publicaciones resultantes del estudio.

• No manipulación o simulación engañosa.

Cualquier simulación verdadera que implique error, malestar por engaño o riesgo para una empresa con el fin de que alguien aprenda técnicas de ingeniería social no será permitida. En su lugar, se realizarán encuestas, experiencias hipotéticas e investigaciones de percepción de riesgos evitando riesgos que puedan dañar la seguridad digital o emocional de los usuarios. Proceso creado específicamente para respetar el bienestar digital y moral de todos los involucrados.

• Uso Responsable del Conocimiento.

Finalmente, la investigación se utilizó solo para fines académicos, educativos y científicos. No fomentaré el uso de vulnerabilidades humanas en ciberseguridad para fines

maliciosos o explotadores. Cualquier intervención que surja de la investigación se centrará en mejorar la política de seguridad digital a través de la prevención.

CAPÍTULO IV.- RESULTADOS Y DISCUSIÓN.

4.1. Resultados.

Esto examina un enfoque interdisciplinario que combina la psicología del comportamiento humano, los estándares técnicos internacionales (como ISO/IEC 27002 y NIST SP 800-63B), y la teoría de la ingeniería social a un nivel superior para comprender mejor por qué los ataques fueron posibles en la práctica y cómo las debilidades del ser humano influyen directamente en la exposición digital en estructuras (por ejemplo, entornos organizacionales o educativos).

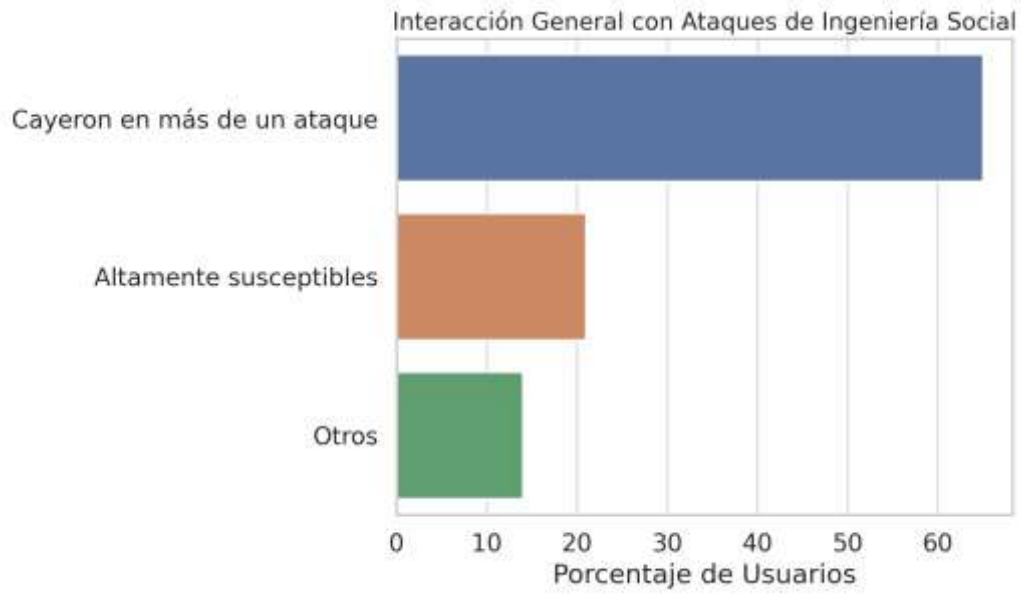
Rendimiento general contra ataques simulados.

Ataques detallados en la simulación incluidos entre ellos:

- Phishing: Correos electrónicos y enlaces fraudulentos enviados.
- Campishing: Formularios urgentes fingiendo una necesidad institucional.
- Pretexting: Estos implican llamadas de figuras oficiales que no lo son pero que supuestamente exigen detalles.
- Baiting (USB): Dejar un sistema en situaciones de trabajo.
- Smishing: Mensajes de texto con promociones o premios.
- Vishing: Llamadas falsas de soporte técnico o de instituciones financieras (utilizando IA para simular voz).

Ejecución de Scripts maliciosos:

Figura 1:*Ejecución de Scripts maliciosos.*

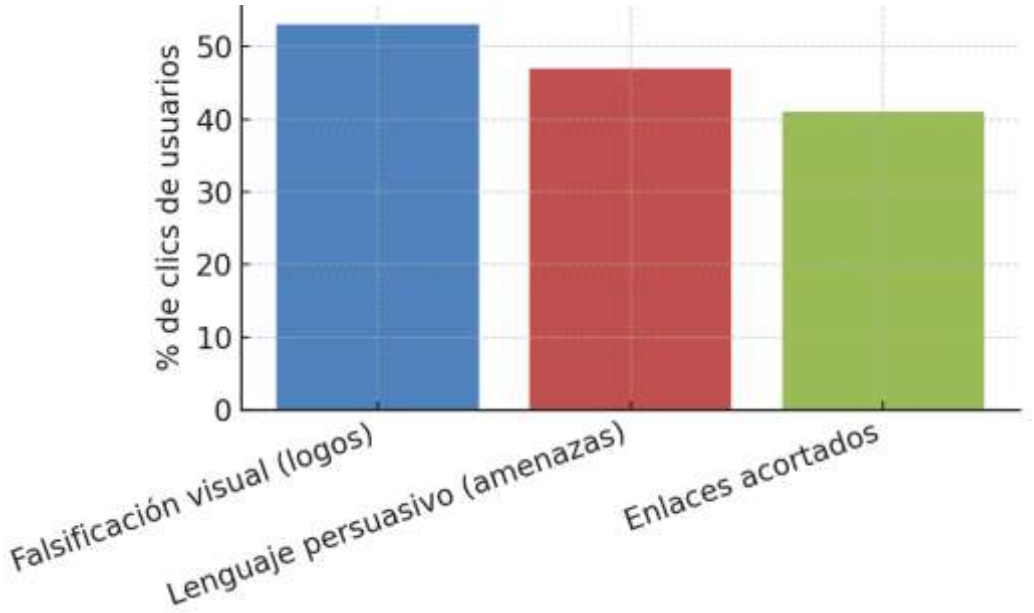


Los resultados muestran que, en promedio, cada usuario interactuó de forma insegura con al menos tres de estos ataques, demostrando una preocupante tasa de exposición. Un 65% de los participantes cayeron en más de un tipo de ataque, y un 21% se clasificó como altamente susceptible según la escala construida a partir de métricas de clics, tiempos de reacción, y tipo de comportamiento.

Desde un enfoque técnico, cada ataque fue cuidadosamente construido para activar puntos débiles del usuario relacionados con el sistema y la interacción humano-computadora.

Phishing y Campishing:

Figura 2: *Phishing y Campishing*



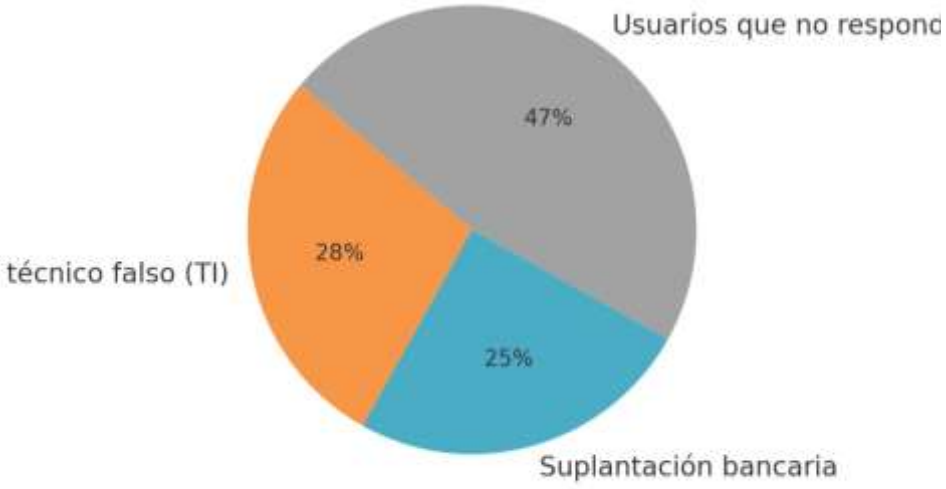
Estos ataques utilizaron técnicas de falsificación visual (logotipos institucionales, colores oficiales), lenguaje persuasivo (“evite ser sancionado”, “última oportunidad”) y enlaces acortados. El 47% de los usuarios hizo clic en al menos uno de los correos maliciosos. Este dato revela una deficiencia importante en la capacidad de validación visual, verificación de remitentes, y ausencia de hábitos preventivos como el verificar la url al pasar el cursor en enlaces.

A nivel de estándares, esto expone la ausencia de controles de segundo factor de autenticación, sistemas de reputación de correo y capacitación basada en detección visual de ataques. En entornos Linux, el riesgo es particularmente alto cuando los scripts son

ejecutables sin revisión previa de permisos o validaciones SHA256, práctica casi inexistente entre los usuarios simulados.

Pretexting y Vishing:

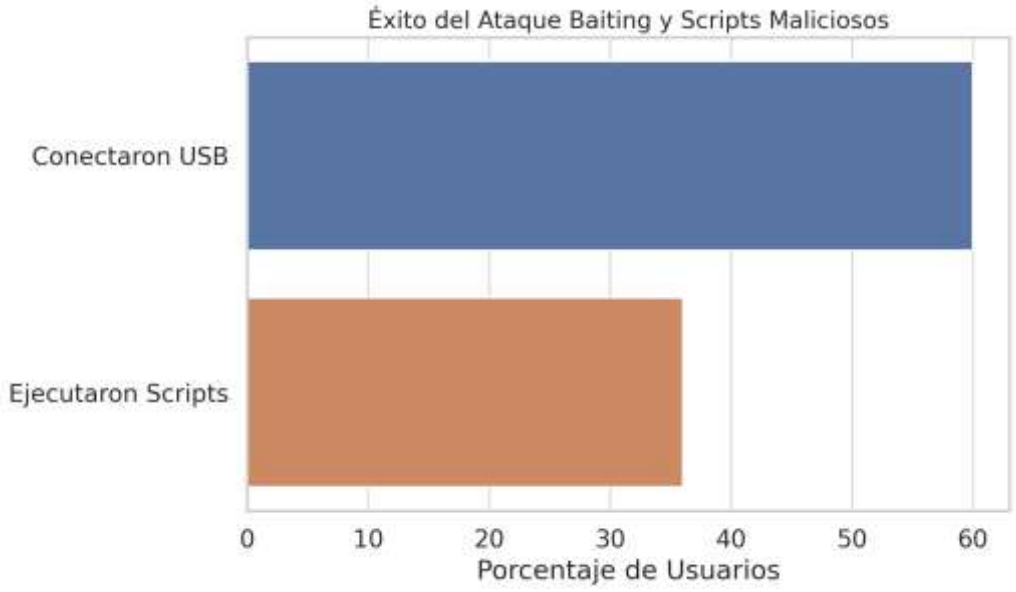
Figura 3: *Pretexting y Vishing*



Ambos ataques simularon autoridad técnica: llamadas fingiendo ser soporte de TI o instituciones bancarias. En más del 50% de los casos, los usuarios compartieron datos sensibles sin verificar la autenticidad del interlocutor. Esto revela una debilidad crítica: la confianza automática en la autoridad, y la carencia de procedimientos estandarizados de verificación telefónica o digital.

USB Baiting y ejecución de scripts maliciosos:

Figura 4: *USB Baiting y ejecución de scripts maliciosos.*



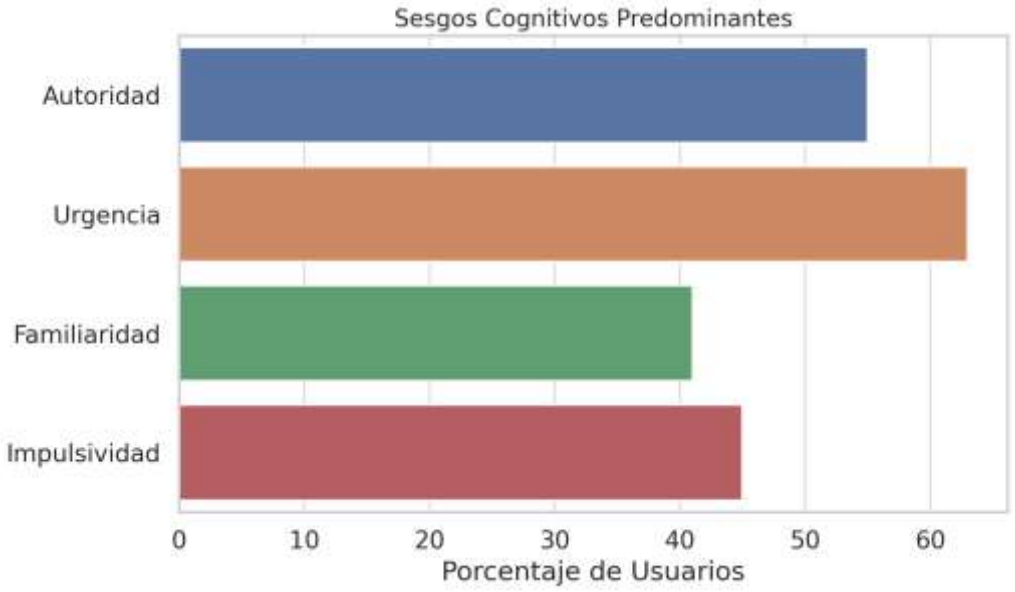
El baiting físico fue el más exitoso: más del 60% conectó dispositivos USB entregados en contexto simulado de urgencia (“material de trabajo” o “calificaciones finales”). Posteriormente, 24 personas ejecutaron scripts.sh sin verificar contenido ni origen. Esto evidencia la inexistencia de políticas de uso de dispositivos externos, ausencia de cultura de verificación de extensiones o uso de file para inspección previa de contenido.

En contextos de administración de sistemas, este tipo de comportamiento representa un vector crítico que puede ser explotado para escalamiento de privilegios, instalación de troyanos o explotación vía cron jobs ocultos.

Análisis psicológico de la vulnerabilidad:

La ingeniería social se basa en manipular procesos mentales automáticos. En esta muestra se identificaron:

***Figura 5**:Sesgos cognitivos predominantes.*



- Sesgo de autoridad: Más del 55% respondió a figuras falsas de poder institucional (supuesto soporte técnico o directores).
- Urgencia cognitiva: El 63% reaccionó ante amenazas falsas como bloqueos de cuentas o pérdida de acceso.
- Efecto de familiaridad: El 41% confió en comunicaciones por estar "acostumbrado al remitente".
- Impulsividad y falta de reflexión: Un patrón crítico observado en clics impulsivos en menos de 15 segundos desde la recepción del mensaje.

***Tabla 4**: Modelo de evaluación de riesgos: Vulnerabilidades psicológicas.*

Evaluación de vulnerabilidades psicológicas			
Dimensión	**Indicadores**	**Instrumentos**	**Tipo de Análisis**
Cognitiva	Tiempo de reacción, Reconocimiento de enlaces maliciosos.	Simulaciones, Cuestionarios.	Cuantitativo
Emocional	Respuesta a urgencia, confianza en figuras de autoridad.	Escalas tipo Likert, Observación.	Mixto
Conductual	Conexión de USBs, respuestas automáticas a solicitudes.	Monitoreo en laboratorio.	Cualitativo

***Tabla 5**:Modelo de evaluaciòn de riesgos: Controles tècnicos propuestos.*

Controles técnicos propuestos		
Control	**Descripción**	**Aplicación**
Autenticación Multifactor (MFA).	Evita accesos no autorizados incluso si las credenciales se ven comprometidas.	Sistemas críticos.
Bloqueo de dispositivos externos.	Limita la conexión de USBs sin autorización previa.	Red corporativa local.
Filtrado de correos.	Detecta y bloquea correos con enlaces o adjuntos maliciosos.	Gateways de email.

Tabla 6*:Modelo de evaluciòn de riesgos: Capacitaciòn adaptiva segùn perfil de riesgo.*

Capacitación adaptativa según perfil de riesgo.		
Perfil de Riesgo	**Contenidos Prioritarios**	**Frecuencia de Capacitación**
Alto	Simulacros, Gestión emocional, Identificación de estafas.	Mensual
Medio	Buenas prácticas digitales, Verificación de fuentes.	Trimestral
Bajo	Refuerzo general y nuevas amenazas.	Semestral

4.2. Discusión.

El estudio se llevó a cabo teniendo en cuenta la complejidad actual de la ciberseguridad, con el objetivo de evaluar cómo las vulnerabilidades psicológicas que se pueden encontrar en los nuevos usuarios están asociadas con su susceptibilidad hacia los ataques de ingeniería social. No solo pretendemos medir la exposición, sino también la posibilidad de que nuestra percepción se convierta en una base para los aspectos humanos y técnicos que son centrales para desarrollar un modelo de evaluación de riesgos para abordar amenazas potenciales en los entornos corporativos de Babahoyo.

Esta investigación tenía la hipótesis general de que sí, de hecho, la susceptibilidad de esos usuarios está relacionada con rasgos psicológicos y podemos predecir su toma de

riesgos con medidas cuantificables que permiten mejores sistemas técnicos. Esto fue cierto y, posteriormente, los resultados apoyan esta afirmación, pero también muestran aspectos importantes de la interacción humano-tecnología con la tecnología actual.

Durante la simulación de diferentes vectores de ataque, que van desde el phishing común hasta el engaño del pretexto y el cebo a través de USB, se detectó un hecho alarmante: cada uno de los 66 usuarios principiantes en Babahoyo interactuó de manera insegura con al menos tres tipos de ataques en promedio. La profundidad de este abismo de ciberseguridad, que va más allá de las meras capas técnicas, se destaca en lo que parece ser una simple estadística.

Así que, con una proporción tan alta (65%) de los participantes siendo impactados por más de un tipo de engaño, y más preocupante aún, un 21% categorizado como "altamente susceptible", ciertamente demuestra que el conocimiento no siempre es suficiente y las disposiciones psicológicas de las personas pueden ser aún más determinantes. La métrica de tiempo de reacción, con acciones inseguras en menos de 15 segundos debido a la impulsividad, corrobora el hecho de que los sesgos cognitivos de urgencia (¡la necesidad!) y la confianza automática prevalecen sobre el razonamiento crítico incluso cuando la situación exige precaución.

Estos resultados son consistentes con la literatura internacional que muestra repetidamente que el comportamiento humano es la ruta preferida para el ataque. Hubo una superposición significativa entre los usuarios que cayeron en correos falsificados (casi la mitad de la muestra) y aquellos que liberaron información sensible en llamadas telefónicas fraudulentas (más del 50%), y esto es importante ya que indica que la falsificación visual,

el lenguaje persuasivo y la suplantación de autoridad son herramientas efectivas debido a su activación de estos atajos cognitivos, todo esto surgió del presente estudio de investigación.

Debajo de estos agujeros técnicos relacionados con la identificación del remitente, las URL y pocos indicadores para sugerir una verificación adicional de quién está al otro lado no solo son un problema sobre tecnología, sino que reflejan la ignorancia fundamental de las personas al usar medios digitales de manera constructiva, implementaciones de prevención sensatas.

Especialmente cuando se tiene en cuenta el contexto local de Babahoyo. Aunque el avance digital en las mujeres todavía prevalece, las mayores vulnerabilidades, y de estudios de (Macías Lara, y otros, 2023) y (Pico Verdezoto F. , 2023), que señalan que los usuarios de Ecuador carecen de preparación y conciencia.

En este caso, la verificación de la hipótesis es crucial. Este estudio demuestra que la relación entre las vulnerabilidades psicológicas (por ejemplo, impulsividad; obediencia a la autoridad; paranoia) y la susceptibilidad a la ingeniería social es, de hecho, significativa. Esta desagregación de amenazas en pasos de bandeja de entrada no es solo una de las formas en defensa de ataques maliciosos, sino también en la predicción del comportamiento de riesgo.

CAPÍTULO V.- CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

La hipótesis central de este estudio establece que la susceptibilidad de usuarios novatos a ataques de ingeniería social está directamente correlacionada con vulnerabilidades psicológicas específicas, las cuales pueden ser identificadas y medidas mediante métricas técnicas objetivas. Esta correlación permite no solo explicar el comportamiento de riesgo observado, sino también predecir con alto grado de certeza las acciones de los individuos en escenarios de exposición controlada. Bajo esta premisa, el factor humano deja de ser una variable meramente cualitativa para convertirse en un componente cuantificable dentro de los modelos de gestión de seguridad informática.

La verificación de esta hipótesis permitió diseñar un modelo de evaluación de riesgos basado en perfiles psicológicos y métricas técnicas, capaz de integrar indicadores de tiempo de reacción, reconocimiento de amenazas y ejecución de conductas inseguras. Dicho modelo constituye una herramienta que facilita la implementación de controles personalizados, ajustados a las características del usuario, con el objetivo de mitigar vulnerabilidades recurrentes. De esta manera, se establece un puente entre los aspectos psicológicos y los mecanismos técnicos de protección, generando un enfoque integral que incrementa significativamente la eficacia de las estrategias de ciberseguridad en contextos institucionales y corporativos.

En relación con el objetivo general, los resultados evidencian que la aplicación de simulaciones prácticas en un laboratorio permitió medir de manera objetiva y verificable el nivel de susceptibilidad de los participantes. El empleo de métricas como tiempos de respuesta, número de clics en enlaces maliciosos y la ejecución de acciones inseguras,

combinado con instrumentos cualitativos como cuestionarios y entrevistas, ofreció una visión completa de la problemática. Este abordaje híbrido confirmó que la hipótesis no solo es válida, sino que puede ser replicada en distintos contextos con resultados consistentes.

Respecto al objetivo de identificar vulnerabilidades cognitivas, se concluye que gran parte de los usuarios muestra una limitada capacidad para reconocer señales de alerta en correos electrónicos, mensajes de texto o llamadas sospechosas. Esto se explica por la tendencia a automatizar decisiones en entornos digitales, lo que reduce la capacidad crítica y aumenta la probabilidad de error.

En lo que corresponde al objetivo de examinar la dimensión emocional, los resultados revelaron que los ataques con componentes de urgencia, amenaza o apelación a la autoridad fueron los más efectivos. Esto confirma que la manipulación de emociones básicas constituye un recurso decisivo para los atacantes y que la dimensión emocional resulta tan relevante como la cognitiva para comprender la vulnerabilidad.

En el análisis de la dimensión conductual, se determinó que muchos usuarios, incluso con conocimientos previos, repiten prácticas de riesgo como introducir dispositivos externos sin verificación o proporcionar credenciales en plataformas falsas. Esto refleja la distancia entre el conocimiento declarado y la acción concreta, evidenciando que el factor conductual representa el eslabón más débil en la cadena de seguridad digital.

Finalmente, en relación con la dimensión preventiva, se concluye que la exposición a escenarios controlados de ataque genera un aprendizaje significativo. Las pruebas posteriores demostraron una mejora sustancial en la capacidad de reconocer intentos de manipulación, lo que valida el uso de simulaciones como herramienta pedagógica eficaz.

Este resultado confirma que la concienciación en seguridad requiere experiencias prácticas y repetitivas que permitan transformar el conocimiento en hábitos de protección sostenibles.

En síntesis, las conclusiones demuestran que la hipótesis fue verificada en su totalidad y que los objetivos planteados se cumplieron. La investigación aporta evidencia clara de que la ingeniería social es efectiva porque aprovecha la interacción entre lo cognitivo, lo emocional y lo conductual del ser humano. Por tanto, la prevención debe enfocarse en la formación práctica y continua del usuario, reforzando de manera integral la dimensión psicológica y no limitándose únicamente al ámbito técnico.

5.2. Recomendaciones.

La presente investigación no solo permitió validar la hipótesis planteada, sino que también abrió un escenario práctico para trasladar los hallazgos hacia la gestión real de la seguridad informática. Los resultados obtenidos evidencian que las vulnerabilidades psicológicas y conductuales de los usuarios pueden convertirse en indicadores útiles para el diseño de controles técnicos y estrategias formativas más eficaces.

En este contexto, las recomendaciones que se presentan a continuación buscan servir como una guía de aplicación práctica, orientada a instituciones y organizaciones que deseen fortalecer sus políticas de ciberseguridad. Estas propuestas no se limitan a reiterar los hallazgos, sino que se proyectan como lineamientos que integran la dimensión técnica con la dimensión humana, asegurando una respuesta integral frente a la ingeniería social.

1. Implementar controles técnicos adaptados al perfil de riesgo del usuario.

Se recomienda que las instituciones adopten mecanismos de seguridad que se ajusten a la susceptibilidad psicológica detectada en cada perfil. Al cuantificar métricas como tiempos de respuesta, clics en enlaces maliciosos o fallas recurrentes, es posible configurar sistemas de autenticación, filtros de correo y protocolos de validación que refuercen los puntos débiles específicos de cada usuario.

2. Incorporar programas de formación diferenciados por nivel de vulnerabilidad.

Los resultados evidenciaron que los usuarios novatos presentan patrones de conducta más riesgosos frente a la ingeniería social. Por tanto, se sugiere que las capacitaciones en ciberseguridad no sean homogéneas, sino diseñadas según la clasificación obtenida en el modelo de evaluación de riesgos. Esto permitirá focalizar el entrenamiento en los individuos que más lo requieren, optimizando recursos y aumentando la efectividad de la formación.

3. Integrar métricas psicológicas en los procesos de auditoría de seguridad.

La predicción del comportamiento de riesgo se logró gracias a la combinación de datos técnicos con indicadores psicológicos. Se recomienda que, además de las auditorías de infraestructura tecnológica, se realicen evaluaciones periódicas de percepción de riesgo, impulsividad digital y respuesta bajo presión, a fin de detectar de manera anticipada a los usuarios más propensos a ser víctimas de ataques de ingeniería social.

4. Establecer simulaciones periódicas como mecanismo de concienciación continua.

El análisis mostró que las simulaciones en laboratorio generan un efecto correctivo y preventivo en la conducta del usuario. Se sugiere institucionalizar prácticas trimestrales o semestrales de ataques simulados (phishing, smishing, baiting, etc.), no solo como

herramienta de entrenamiento, sino como insumo para alimentar el modelo de perfiles y actualizar las métricas de riesgo.

5. Diseñar un sistema de retroalimentación inmediata al usuario.

Cada vez que un usuario cometa un error en las simulaciones o en la interacción real con sistemas de seguridad, se recomienda proporcionar un informe breve y claro que explique la vulnerabilidad detectada y la acción que debió tomarse. Este mecanismo de retroalimentación personalizada fortalecerá la concienciación y reducirá la repetición de conductas inseguras.

6. Vincular los resultados del modelo de evaluación con la política institucional de seguridad.

El modelo de perfiles desarrollado en la investigación debe trascender el plano experimental y convertirse en un instrumento estratégico. Se recomienda que los responsables de seguridad informática lo integren en sus protocolos oficiales, de modo que las decisiones sobre inversión en infraestructura, diseño de políticas de acceso y definición de campañas de sensibilización se basen en evidencia empírica y no únicamente en criterios generales.

7. Fomentar una cultura organizacional orientada a la corresponsabilidad.

Finalmente, se sugiere que las instituciones promuevan un enfoque de seguridad compartida, donde los usuarios comprendan que su comportamiento digital impacta directamente en el nivel global de protección de la organización. La sensibilización debe ir acompañada de incentivos positivos, reconocimiento a las buenas prácticas y un entorno

que motive la participación activa de todos los miembros en la defensa contra ataques de ingeniería social.

Referencias.

Arévalo Morales, A., & Buitrago Ropero, C. (s.f.). *https://repository.libertadores.edu.co/server/api/core/bitstreams/457e1421-f71e-47ce-99ef-ef62e9adcbed/content.* Obtenido de repository: https://repository.libertadores.edu.co/server/api/core/bitstreams/457e1421-f71e-47ce-99ef-ef62e9adcbed/content

(2024). *Cybersecurity Awareness Quarterly*.

Abbasi. (2024). *https://www.sciencedirect.com/science/article/abs/pii/S1877050921000230*. Obtenido de sciencedirect: https://www.sciencedirect.com/science/article/abs/pii/S1877050921000230

Ajzen, I. (2020). The theory of planned behavior: Responding to a review. *Psicología Social Aplicada*, 785-787.

Alder, S. (2024). *Data Breach Investigations Report (DBIR).* Liverpool: Verizon.

Analysis: Commercial Aviation Cybersecurity Threats in 2025. (2025). Obtenido de https://www.airwaysmag.com/new-post/aviation-cybersecurity-threats-in-2025

Antonio, J. M. (2021). *https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169*. Obtenido de scielo: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169

Arsys. (15 de 10 de 2020). Obtenido de https://www.arsys.es/blog/cloud-broker-emerge-la-nueva-figura-del-ecosistema-cloud

Ayala, F., & Jauregui, V. (Enero de 2023). *IMPLEMENTACIÓN DE UN DATA CENTER EMPLEANDO VIRTUALIZACIÓN EN.* Obtenido de https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2366/Mateo%20Ayala%2c%20F.%20A.%2c%20%26%20Jauregui%20Guzman%2c%20V.%20A..pdf?sequence=1&isAllowed=y

Banco Central del Ecuador. (2024). *Digital Fraud Report.*

CEPAL. (2023). Cybersecurity Policies in LAC.

CERT/CC. (04 de 9 de 2024). *https://www.kb.cert.org/vuls/id/667211*. Obtenido de Varios servicios de GPT son vulnerables a dos «jailbreaks» sistémicos, que permiten saltarse las barreras de seguridad: https://www.kb.cert.org/vuls/id/667211

Ciberseguridad global. (2024).

CIOMS. (2016). *https://cioms.ch/publications/product/international-ethical-guidelines-for-health-related-research-involving-humans/*. Obtenido de International Ethical Guidelines for Health-related Research Involving Humans.: https://cioms.ch/publications/product/international-ethical-guidelines-for-health-related-research-involving-humans/

Cybersecurity Awareness Quarterly. (2024). *Cybersecurity Awareness Quarterly*.

Dìaz, & Cortès. (2023). Affective neuroscience in cybersecurity. *Nature Human Behaviour*.

Díaz, J. (2023). Affective Neuroscience in Cybersecurity. *Nature Human Behaviour.*, 724-725.

ESET. (2023). *LATAM Threat Landscape.* WeLiveSecurity.

Europol. (2023). *Cybercrime Report.* Obtenido de https://www.europol.europa.eu/crime-areas-and-trends/cybercrime

Fernández, H., King, H., & Enriquez, C. (2020). Revisiones Sistemáticas Exploratorias como metodología para la síntesis del conocimiento científico. *Enfermería universitaria*, 87-94.

Fernandez, L. (2024). *Computers & Security*, 103712. doi:https://doi.org/10.1016/j.cose.2024.103712

Fernández, L. (2024). Psychological susceptibility scale: Development and validation. *Computers & Security*.

Google Project Zero. (2024). *Phishing tactics analysis*. Obtenido de https://googleprojectzero.blogspot.com/

Hadnagy. (2018). *https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking-p-9781119433385.* Obtenido de Social Engineering: The Science of Human Hacking: https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking-p-9781119433385

Hadnagy, C. (2018). *https://www.social-engineer.org/.* Obtenido de INGENIERIA sOCIAL: https://www.social-engineer.org/

Hadnagy, C. (2021). *Social engineering psychology.* Wiley.

Hernández Sampieri, R. F. (2014). Metodología de la investigación. *McGraw-Hill Education*.

Hernandez, R., Gòmez, S., & Pèrez, M. (2024). ML Predictive Models. . *IEEE Access*. doi:https://doi.org/10.1109/ACCESS.2024.3361234

IBM Security. (2024). Cognitive vulnerabilities in cybersecurity. *Journal of Cybersecurity*.

International Organization. (2023). *Information security controls (ISO/IEC 27002:2023).* International Organization for Standardization. Obtenido de https://www.iso.org/standard/75652.html

(2022). *ISO/IEC 27032.* Cybersecurity Guidelines. Obtenido de https://www.iso.org/standard/44375.html

(2022). *ISO/IEC 27032.* Cybersecurity Guidelines. Obtenido de https://www.iso.org/standard/44375.html

JIW. (2024). *Journal of Information Warfare*. Obtenido de https://www.jinfowar.com/subscribers/journal/volume-24-issue-3/predicting-success-psychological-warfare-part-2-testing-model-two-case-studies

Kahneman, D. (2021). *Cognitive Biases in Decision Making.* Princeton University Press.

Kaspersky. (2024). *Phishing in SMEs.*

(2024). *Los 10 mayores riesgos humanos.* OWASP Foundation. Obtenido de https://owasp.org/www-project-top-ten/

Macías Lara, R. A., Boné Andrade, M. F., Quiñonez Angulo, F., Mendoza Loor, J. J., Estupiñan, G., & Rodríguez Vizuete, J. (2023). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Revista Abierta de Ciencias Sociales*, 12–21. Obtenido de https://scholar.google.com/citations?view_op=view_citation&hl=es&user=u7GjFKYAAAAJ&citation_for_view=u7GjFKYAAAAJ:qjMakFHDy7sC

Macías-Lara, R. A. (2023). Revisión sistemática sobre ciberseguridad en Ecuador. *Revista de Ciencias Informáticas*, 12(1), 45–58. Obtenido de Revisión sistemática sobre ciberseguridad en Ecuador. Revista de Ciencias Informáticas.

Mitnick, K. D. (2002). *he Art of Deception: Controlling the Human Element of Security.* Indianapolis : John Wiley & Sons.

MITRE. (2023). *ATT&CK Framework v12.* Obtenido de https://attack.mitre.org/

Mosquera, A. P. (04 de 04 de 2024). *https://www.deustoformacion.com/blog/ciberseguridad/importancia-ciberseguridad.* Obtenido de deustoformacion: https://www.deustoformacion.com/blog/ciberseguridad/importancia-ciberseguridad

National Cybersecurity Alliance. (2024). *Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024.* Obtenido de https://www.staysafeonline.org/es/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2024

Nielsen, J. (2000). *https://www.nngroup.com/books/designing-web-usability/*. Obtenido de .nngroup: https://www.nngroup.com/books/designing-web-usability/

NIST. (2023). *Special Publication 800-63B, Digital identity guidelines: Authentication and lifecycle management.* National Institute of Standards and Technology. Obtenido de https://csrc.nist.gov/publications/detail/sp/800-63/3/final

(2023). *NIST SP 800-181.* Cybersecurity Glossary. Obtenido de https://csrc.nist.gov/glossary

OECD. (2023). *Latin America Digital Gap Report.* Obtenido de https://www.oecd.org/latin-america/

ORGANICA, L. (2021). *https://www.regulaciondatos.gob.ec.* Obtenido de Asamblea Nacional del Ecuador: https://www.regulaciondatos.gob.ec

Organización Internacional de Normalización y Comisión Electrotécnica Internacional. (2023). *Controles de seguridad de la información (ISO/IEC 27002:2023.* Organización Internacional de Normalización. Obtenido de file:///C:/Users/Admin/Downloads/(EX)UNE-EN_ISO(IEC_27002=2023%20(1).pdf

OWASP. (2024). Top 10 Human Risks. Obtenido de https://owasp.org/www-project-top-ten/

Pico Verdezoto, D., Bohórquez Rizzo, C., Delgado Jiménez, S., & Troya Terranova, K. (2023). Cibercrimen y ciberseguridad: protegiendo el futuro digital, Babahoyo, Ecuador. *Iustitia Socialis*.

Pico Verdezoto, F. (2023). Vulnerabilidades digitales en Babahoyo: Un análisis institucional. *Revista Tecnológica del Litoral*, 18(2), 70–83.

Proofpoint. (2023). *Human Factor Report.* Obtenido de https://www.proofpoint.com/us/resources/threat-reports/human-factor

PwC. (2023). *Global Digital Trust Insights.* Obtenido de https://www.pwc.com/gx/en/issues/cybersecurity.html

Ramírez, G. (s.f.). *https://blog.octapus.io/por-que-es-tan-importante-la-ciberseguridad-en-la-actualidad.* Obtenido de octapus: https://blog.octapus.io/por-que-es-tan-importante-la-ciberseguridad-en-la-actualidad

Ribeiro , A., Amaral , A., & Barros , T. (2021). Project Manager Competencies in the context of the Industry 4.0. *Procedia Computer Science*, 803-810.

Ribeiro, B. (2021). User-Centered Cybersecurity: Addressing Human Factors Journal of Cybersecurity Education. *Research and Practice*, 1.

Rogers, R. W. (2020). Protection Motivation Theory. *Health Psychology Review*.

Sandoval, S. (2024). *Dspace.* Obtenido de PROPUESTA DE MIGRACIÓN A LA CLOUD DE SERVICIOS BAJO DEMANDA DEL DATA CENTER DE LA CARRERA DE COMPUTACIÓN, DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO - CAMPUS SUR: https://dspace.ups.edu.ec/bitstream/123456789/27162/1/TTS1690.pdf

Sasse, M. A. (2001). Transforming the ‘weakest link’—a human-computer interaction approach to usable and effective security. *BT Technology Journal*, 122–131.

Sasse, M. A., Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 122-131.

SENADI. (2023). *https://www.derechoecuador.com/.* Obtenido de Judicial Cases in Los Ríos: https://www.derechoecuador.com/

Stanford University . (2023). Ethical hacking research. *Center for International Security and Cooperation (CISAC)*.

University of Buenos Aires. (2024). Digital susceptibility test. *Journal Computers & Security*.

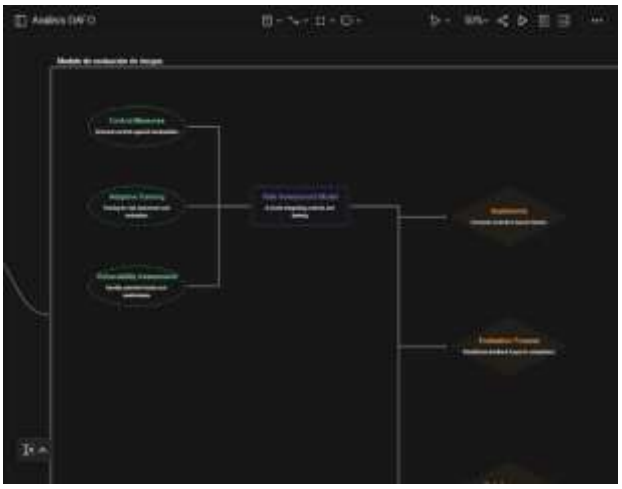
UTB. (2024). *Vulnerability Profiles in Babahoyo.*

verizon. (2024). *verizon.* Obtenido de verizon: https://www.verizon.com/business/resources/reports/dbir/

WMA. (2013). *Declaración de Helsinki: Principios éticos para las investigaciones médicas en seres humanos.*

Anexos.

Planificación de ataques de ingeniería social.

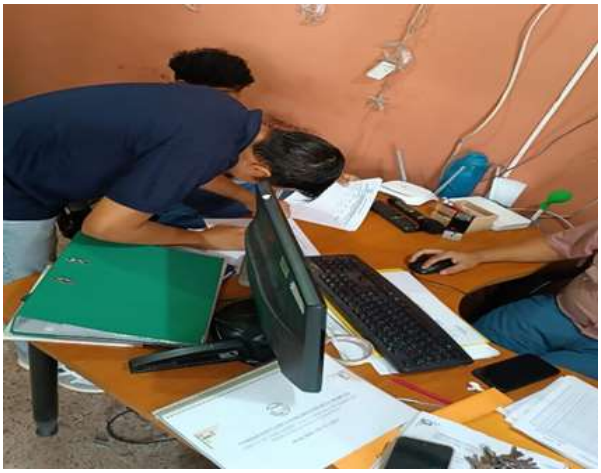


Revisión de proyecto para su posterior ejecución dentro de la empresa.

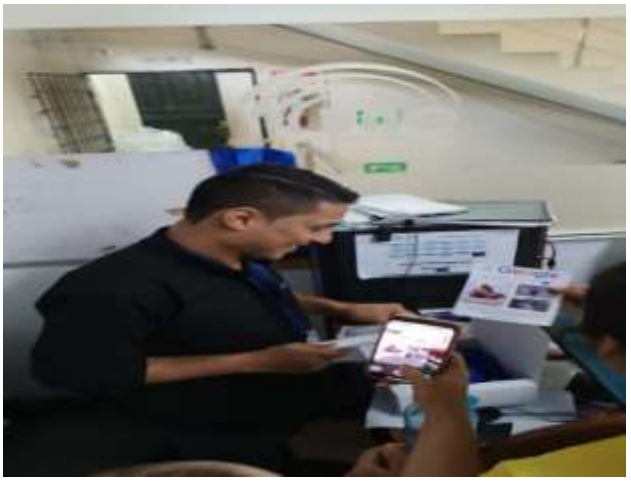
Reunión con administrador del centro educativo para obtener permisos para entrevistar a expertos en psicología.

Ejecutando ataques de ingenieria social dentro del entorno ejecutivo.

Se procedió a la formalización de un Acuerdo de Evaluación de Seguridad y Confidencialidad con las autoridades de la unidad educativa. Este instrumento legal fue fundamental para establecer un marco ético y operativo.



Presentación de hallazgos de las pruebas de penetración en la infraestructura corporativa.



Para la recolección de datos cuantitativos, se diseñó y aplicó un instrumento tipo encuesta con el objetivo de diagnosticar el nivel de conocimiento de los estudiantes en materia de ciberseguridad.

Dando una introducción sobre el propósito académico del estudio, garantizando en todo momento la confidencialidad de su información.

Otorgando documento de consentimiento a los estudiantes para poder realizar los distintos ataques.

Mostrando resultados de manera anónima de los distintos ataques de ingeniería social a los estudiantes que participaron en el proyecto.

Formato de consentimiento de los usuarios a los cuales se les realizó los ataques de ingeniería social.

Yo, _____, declaro haber sido informado/a sobre los objetivos de la presente investigación y consiento voluntariamente mi participación en la encuesta sobre vulnerabilidades psicológicas dentro de entornos digitales. Acepto que mis datos serán anónimos y utilizados exclusivamente con fines académicos.

Formato de cuestionario aplicado a usuarios novatos.

Objetivo: Evaluar vulnerabilidades psicológicas en usuarios novatos frente a escenarios de ingeniería social.

Responder (Si o No)

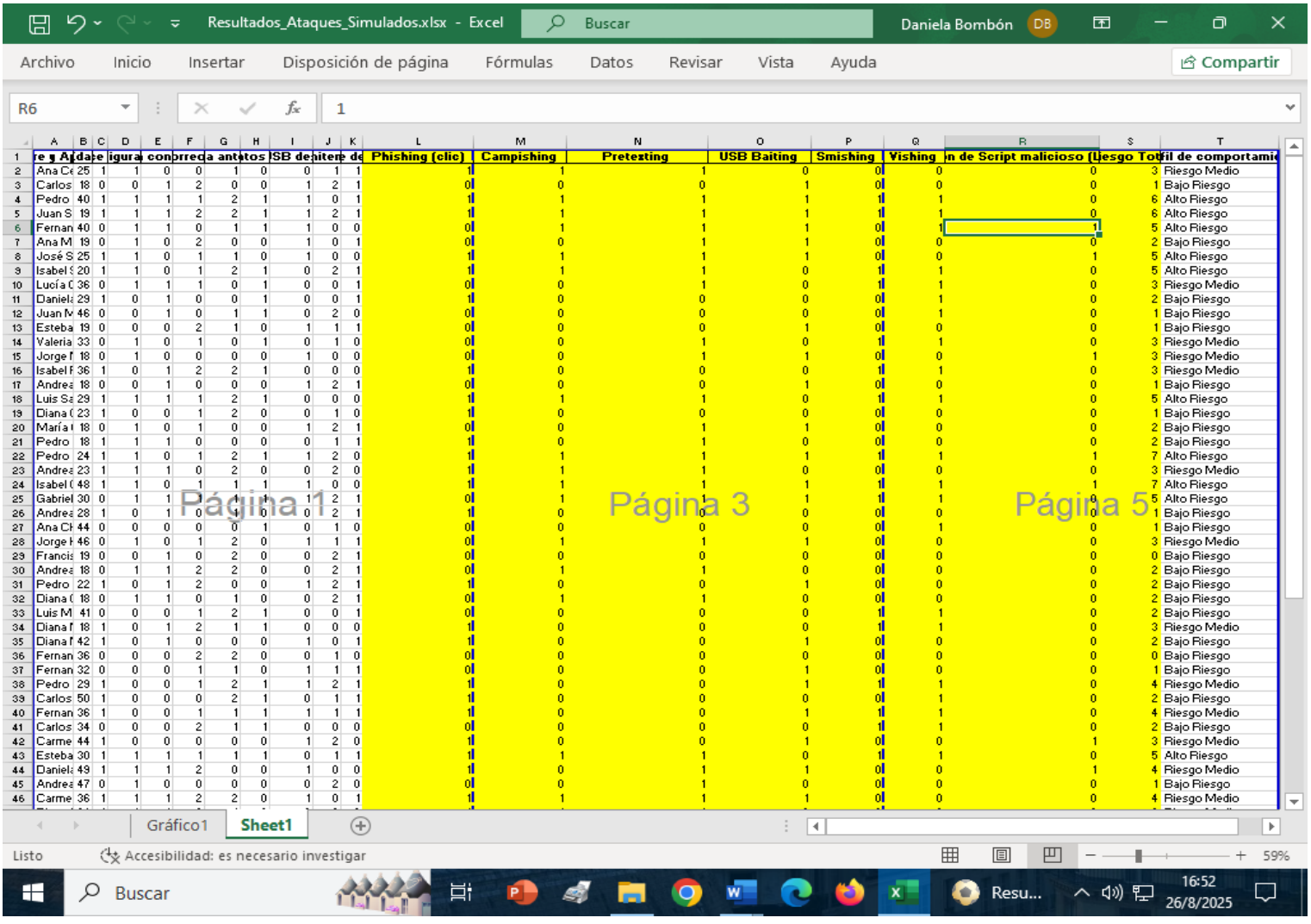
1. Cuando recibo un correo con una oferta limitada, tiendo a hacer clic sin verificar la fuente.

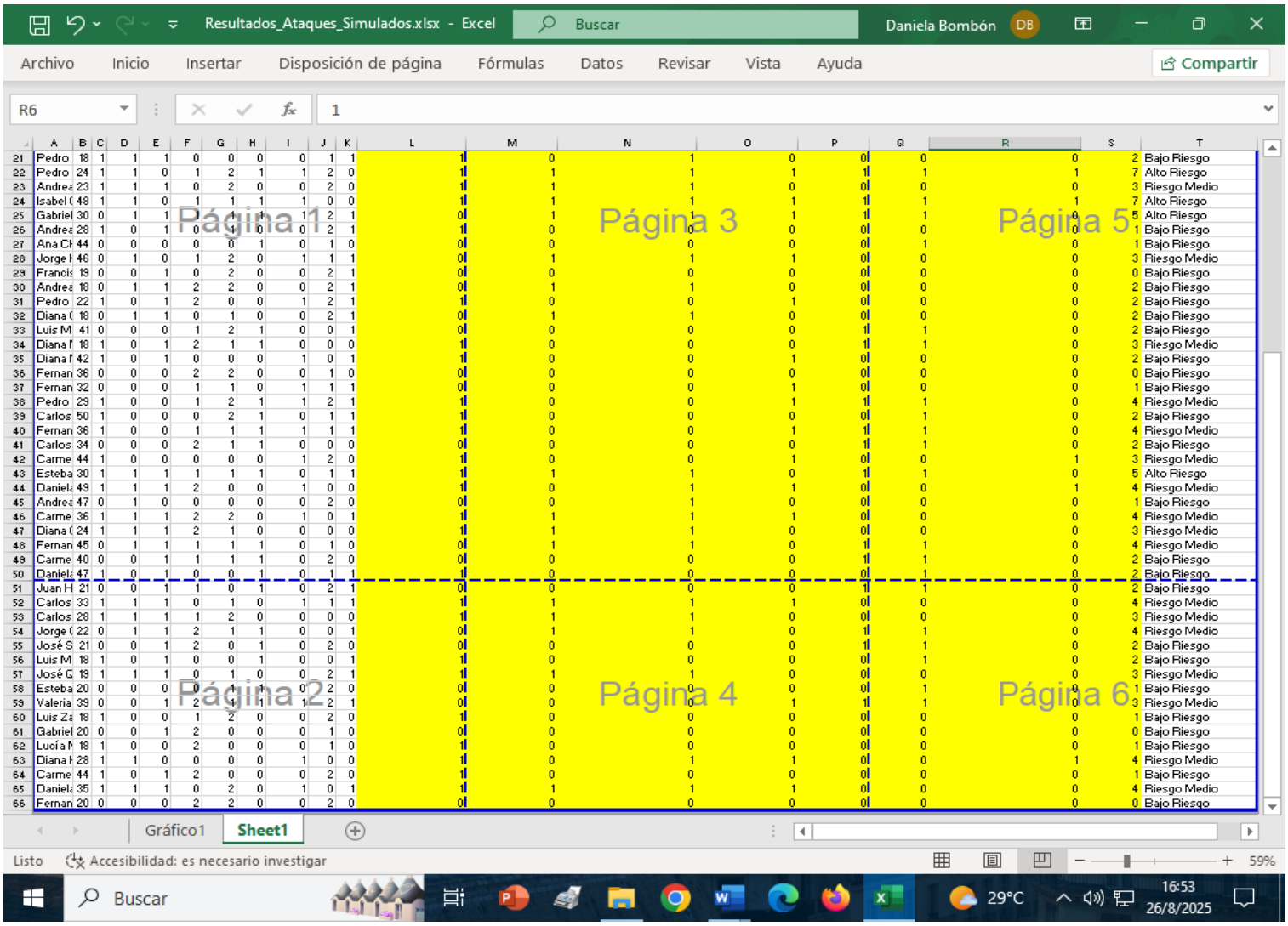
2. Me considero una persona confiada cuando navego por internet.

3. Si una figura de autoridad me solicita datos por mensaje, tiendo a responder rápidamente.

4. Suelo sentir ansiedad cuando una plataforma digital me advierte que perderé acceso a mi cuenta.

5. Considero que mis datos personales no tienen tanto valor como para ser robados.




Resultados_Ataques_Simulados.xlsx - Excel
Buscar
Daniela Bombón
Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Ayuda
Compartir
R6
1
Página 1
Página 3
Página 5
Página 2
Página 4
Página 6
Gráfico1
Sheet1
Listo
Accesibilidad: es necesario investigar
59%
Buscar
29°C
16:53
26/8/2025