INSTITUTO SUPERIOR TECNOLÓGICO

SAN ANTONIO

Escuela de Tecnología E Innovación

Implementación de una herramienta de simulación de ataques de phishing para la concienciación de seguridad en Tecnológico San Antonio Quito 2025

Mabel Alexandra Viveros Chango.

Jefferson Jhair Viveros Chango.

Santiago Rojas Bukovak

Tecnologo Superior en Ciberseguridad

Quito, 27 de mayo de 2025

DERECHOS DE AUTOR

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

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

Nombres y apellidos: Mabel Alexandra Viveros Chango, Jefferson Jhair Viveros Chango

Código estudiante: xxxxxxx

Cédula de identidad: 1726076027/ 1726076035

Lugar y fecha: Quito, mayo del 2025

ACLARACIÓN PARA PUBLICACIÓN

UNPUBLISHED DOCUMENT

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

DEDICATORIA

Este logro está dirigido especialmente a nuestros padres John Jairo Viveros Gómez y Mayra del Rocio Chango Gómez por todo su esfuerzo y apoyo gracias a su trabajo en la que pasaron de sol a sol y de lluvia en lluvia gracias a ello culminaremos nuestras metas.

De igual manera queremos dirigir este logro a los ingenieros Santiago Rojas, Pablo Heredia y Christian Molina por su ayuda, sus consejos y su paciencia es un gran honor dedicarles este esfuerzo que con mucha dedicación se está logrando cumplir.

También se lo dedicamos a nuestras parejas Michael Enrique Cruz y Katherine Dayana Suarez por sus ánimos que influyeron en nosotros y su ayuda.

A nuestros compañeros que pasaron a ser amigos que estuvieron con nosotros desde principio a fin fue un gusto haber estudiado a su lado.

AGRADECIMIENTO

Principalmente estoy agradecido con el Ingeniero Pablo Heredia y Santiago Rojas que fueron unos excelentes tutores y nos han ayudado mucho a lo largo de todo el proyecto proporcionándonos distintas herramientas que hemos usado a lo largo de todo el proyecto

Mi gratitud también se extiende a todo el cuerpo de docentes, administrativos y también a nuestros compañeros que han sido un gran apoyo para ir superando cada uno de los grandes retos que se han ido presentado a lo largo de todo el tiempo gracias a ellos todo ha sido de alguna manera más fácil y hemos podido disfrutar del proceso de aprendizaje

Claramente nos llevamos excelentes experiencias del Tecnológico San Antonio que siempre nos recibió con un caluroso abrazo.

También queremos agradecer a nuestra familia y amigos que siempre nos brindaron su apoyo., su comprensión y su ánimo constante lo cual ha sido de gran ayuda durante los momentos de constante presión y su presencia fue una parte importante para poder seguir adelante en los momentos de duda o temor

RESUMEN

Este proyecto busca establecer una herramienta que simule ataques de phishing con el fin de mejorar la comprensión de la ciberseguridad entre los empleados del Instituto Superior Tecnológico San Antonio (TESA). Dado que el phishing representa una amenaza digital constante y efectiva, se creadó un enfoque preventivo que se basa en simulaciones prácticas. Estas simulaciones permiten medir el estado de preparación de los usuarios, detectar perfiles vulnerables y potenciar el aprendizaje mediante comentarios individuales.

La propuesta abarca la realización de encuestas diagnósticas, la distribución de contenido audiovisual, así como la utilización de una plataforma de simulación (Gophish) para crear correos falsos dentro de un ambiente controlado. Esta intervención fue dirigida al personal docente, administrativo y técnico, diferenciando entre áreas técnicas y no técnicas, siendo estas últimas las que mostraron mayor vulnerabilidad.

Se concluye que las simulaciones, combinadas con recursos educativos personalizados, permiten mejorar la identificación y respuesta ante ataques de ingeniería social. La herramienta propuesta no solo actúa como diagnóstico, sino también como medio de capacitación activa. Finalmente, se recomienda su integración en los programas de formación continua de la institución, con campañas periódicas ajustadas por perfil de riesgo y nivel de exposición.

ABSTRACT

Phishing is one of the most prevalent cyber threats, exploiting the lack of knowledge and preparation of employees in computer security. This project aims to implement a phishing attack simulator at the Instituto San Antonio de Quito, with the purpose of improving the awareness and preparation of users against this type of threat.

The proposal includes the development of a controlled environment where employees can face scenarios similar to a real phishing attack, the ability to identify and respond to this attack will be evaluated.

The tool is expected to reduce staff vulnerability to phishing, improve security practices within the institution and contribute to the protection of information. In the long term, this approach will strengthen the institute's cybersecurity posture, minimizing risks and losses from successful attacks by cybercriminals.

Key words: Phishing, Cybersecurity, Simulation, Awareness, TESA

TABLA DE CONTENIDOS

CAPÍTULO I INTRODUCCIÓN 9

1.1. Planteamiento del Problema 9

1.2. Justificación 13

1.3. Alcance 15

1.4. Objetivos General y Específicos 15

CAPÍTULO II MARCO TEÓRICO 16

1.1 Revisión bibliográfica 17

1.2 El phishing como amenaza de ciberseguridad 17

1.3 Evolución de las técnicas de phishing 18

2.4 Impacto y contexto educativo 19

2.5 Simulación de ataques de phishing como estrategia de prevención 21

2.6 Herramientas actuales para la simulación de phishing 21

2.7 Marco conceptual 24

2.8 Marco legal 24

CAPÍTULO III. MARCO METODOLÓGICO 25

3.1. Tipo de investigación 25

3.2. Enfoque 26

3.3. Herramientas metodológicas 27

3.4. Técnicas 29

3.5. Estudios iniciales 31

3.6. Desarrollo 32

CAPITULO IV. RESULTADOS Y DISCUSIÓN 35

4.1. Análisis de resultados (descripción) 35

Distribución de puntuaciones totales 35

Tabulación por ítem (resumen de respuestas correctas por pregunta) 36

Interpretación de resultados 37

4.2. Interpretación y discusión de resultados 38

CONCLUSIONES Y RECOMENDACIONES 40

REFERENCIAS BIBLIOGRÁFICAS 43

ANEXO A:Resultados de la Encuesta Diagnóstica sobre Phishing – Instituto TESA 45

CAPÍTULO I
INTRODUCCIÓN

1.1. Planteamiento del Problema

Inicialmente, los ataques de phishing consistían en enviar correos electrónicos no deseados con enlaces en los que se vinculaban a sitios web fraudulentos. Sin embargo, en la era actual de la proliferación de dispositivos conectados, estos ataques se han extendido más allá de las plataformas de correo electrónico y ahora afectan las redes sociales, los mensajes de texto, también conocidos como smishing, las llamadas telefónicas, también referidas como vishing, e incluso los mensajes de aplicaciones de mensajería instantánea. En muchos casos, la ingeniería social ha sido clave para el éxito de este ataque al principio. Las organizaciones buscan protegerse a través de medidas como filtros de correo, software antivirus, políticas de seguridad, pero a menudo estas medidas no ofrecen una protección adecuada contra los ataques más sofisticados, por lo que se debe dar prioridad a la concienciación de los empleados.

En el contexto actual de ciberseguridad, las empresas enfrentan crecientes amenazas por ataques que se dirigen a las debilidades del eslabón más frágil en la defensa del sistema: los trabajadores. Una de las técnicas más frecuentes y eficaces empleadas por los ciberdelincuentes es el phishing, que consiste en el envío de correos electrónicos, mensajes de texto u otros tipos de comunicación que parecen legítimos a los destinatarios, con el propósito de engañarlos para que divulguen información sensible, como datos de acceso o información financiera, o convencerlos de transferir software malicioso al insertar estos en los sistemas de la empresa.

A pesar de las inversiones significativas en tecnologías de seguridad mejoradas, como los sistemas de detección y protección de intrusiones, los firewalls y las suites de protección antivirus, el eslabón más débil en la cadena de defensa sigue siendo la gente. Según los datos del Informe de Filtraciones de Datos de Verizon 2023, el 74% de las brechas de seguridad es resultado de errores humanos, como ser atrapado haciendo clic en enlaces maliciosos o compartiendo credenciales en un sitio web falso. Además, el 91% de las

organizaciones corren riesgo de un ataque de phishing y tendrán que pagar multas de hasta 16,533€ por minuto por no proteger los datos filtrados. Mientras tanto, la falta de conciencia de la ciberseguridad perjudica grandemente a las empresas que no enfrentan los riesgos. Aunque los estudios anteriores han demostrado que el phishing es la mayor fuente de compromisos de las infraestructuras de TI corporativas, con más del 90% de los ciberataques siendo tanto impulsados como exitosos mediante algún tipo de phishing. Además, los investigadores de Brechas de Verizon han concluido que "controlar el factor humano, a través del phishing siempre presente, sigue siendo la mejor apuesta de su programa de seguridad para reducir el número de incidentes".

Sin embargo, muchas empresas subestiman este riesgo. Estas, o bien no cuentan con programas de formación adecuados o no realizan pruebas regulares que permitan evaluar la preparación de sus empleados frente a estas amenazas. Basándonos en el entorno empresarial el phishing se ha vuelto la más grande amenaza cibernética. Gracias a ello se han creado herramientas en la cual detecta y bloqueas inmediatamente los correos maliciosos, el factor humano es de suma importancia. La vulnerabilidad consiste en la que los empleados con tiene el conocimiento para reconocer un correo malicioso, evitar enlaces maliciosos, no informar que está siendo víctima de phishing. En varios casos, los delincuentes alcanzar a explotar las diferencias en el factor humano. Este obstáculo es aún más difícil de solucionar debido al creciente avance de los ataques. En el presente, los delincuentes logran obtener la información total y específica sobre la empresa y los empleados que trabajan en ella y con eso crean mensajes que parecen legítimos. Dada la existencia del phishing, las empresas tendrían que ser consientes en usar herramientas simuladoras de ataques de phishing. Las herramientas de este tipo ayudan para la simulación de correos falsos y las situaciones de riesgos de phishing, este permite a la empresa evaluar a los empleados si tiene la preparación para la identificación y la pronta respuesta de amenazas. También, se permitirá a los

empleadores obtener información precisa del comportamiento vulnerable de los empleados, con el fin de modificar las campañas de información de forma adecuada.

La carencia de preparación para la identificación de ataques de phishing y poder actuar de manera profesional el problema central que se busca solucionar con este simulador. Aún que hay varias empresas en las que brindan las debidas capacitaciones puntuales de seguridad, suelen ser teóricas y esporádicas, esto conlleva a la ineficacia para generas altos niveles de conciencia y su comportamiento ante la amenaza cibernética siempre en evolución. Sin la enseñanza debida practica y continua, los empleados continuaran siendo los principales vulnerables. Del mismo modo, los esfuerzos en la protección por parte de la tecnología resultarán ineficaces en nuestra lucha contra el ciber-crimen.

En la actualidad, la ciberseguridad representa un pilar fundamental en el funcionamiento de cualquier institución, especialmente aquellas que manejan datos sensibles y utilizan entornos digitales para su operación académica y administrativa.

Una de las tácticas más comunes y efectivas en el ámbito de los ciberataques es el phishing, una técnica que usa la manipulación mental para engañar a la gente con el objetivo de que proporcionen información delicada, como claves, datos financieros o información personal

A pesar del crecimiento de la digitalización y el extenso uso de tecnologías en las instituciones educativas, continúa habiendo una notable carencia de capacitación y conciencia entre los consumidores acerca de peligros como el phishing. Esta cuestión se observa intensificada por la naturaleza dinámica y sofisticada de los ataques, que se manifiestan a través de canales comunes como el correo electrónico, las plataformas sociales o los mensajes de texto, replicando interacciones genuinas.

En lo que concierne al Instituto Superior Tecnológico San Antonio (TESA), se ha detectado una necesidad de elevar las competencias de su comunidad educativa para poder abordar este tipo de peligros. A pesar de que existen secciones técnicas que brindan capacitación en ciberseguridad, además de otros programas no vinculados a la tecnología, como salud, estética o moda, se sienten más expuestos por la ausencia de formación específica.
ante estas amenazas. Esta variación en la formación representa una desventaja para la organización, dado que un solo punto vulnerable puede amenazar toda la estructura digital usual

Asimismo, no existe un plan organizado para evaluar o instruir acerca del phishing, lo que limita la capacidad del Instituto para reconocer, prevenir y responder a intentos de fraude. La carencia de actividades prácticas o estrategias educativas para elevar la conciencia mantiene a los usuarios en una postura pasiva frente a una amenaza que es activa, permanente y en constante evolución

Este panorama resalta la urgencia de instaurar medidas preventivas, como la realización de simulacros de ataques de phishing, que no solo evalúen el conocimiento actual del personal, sino que también ofrezcan formación de manera práctica y dinámica sobre los peligros reales que enfrentan.

1.2. Justificación

El phishing sigue siendo una de las amenazas más críticas para el panorama de la seguridad de la información a nivel mundial. De acuerdo con algunas investigaciones, más del 90% de las brechas de seguridad que enfrentan las empresas provienen de ataques de phishing (Deloitte, 2020; ReHack, 2024). Al depender de la confianza y de la falta de preparación de los empleados, los ataques de phishing se valen del engaño por ingeniería social para obtener información confidencial, acceder a las redes empresariales o distribuir programa maligno. En este sentido, la simulación de ataques de phishing es una herramienta indispensable para cualquier empresa que desee mejorar su postura de seguridad de la información, y la justificación de este proyecto es doble.

Por un lado, no hay una medida tecnológica única capaz de prevenir efectivamente los ataques exitosos, lo que significa que, si bien es imposible suprimir de raíz todos los intentos, es posible reducir significativamente la posibilidad de éxito. Por otro lado, muchas empresas actualmente no poseen programas de capacitación en seguridad estructurados y continuos, lo que pone a sus empleados bajo la amenaza constante de ser víctimas de estafas cada vez más sofisticadas. La herramienta de simulación de ataques de phishing propuesta ofrece una solución al problema al brindar un entorno de ataque seguro donde se pueden replicar los intentos de robo del mundo real para evaluar la reacción de los empleados. Al hacerlo, el KnowBe4 puede determinar qué tan vulnerable es su personal, qué áreas deben ser abordadas más en profundidad y qué empleados son propensos a ser engañados. Además, después de cada simulación, proporcionar feedback sobre la debilidad identificada educa a los empleados activamente sobre los peligros de ser estafados y perpetrar estafas.

Por último, la herramienta también ayuda a fomentar una cultura de la seguridad dentro de la empresa. Cuando los empleados saben que existen peligros y son formados con mucha estridencia para combatirlos, aumentan ampliamente su responsabilidad y se convierten en un factor eterno de advertencia. Para el resultado final, la simulación de ataques

de phishing no solo ayuda a los empleados a reconocer y responder a las amenazas, sino que también protege la postura general de seguridad de la empresa, reduciendo la probabilidad de futuros intentos basados en el error humano, convirtiéndola en una inversión precisa para cualquier empresa moderna.

1.3. Alcance

El alcance de este proyecto de implementación de herramienta de simulación de phishing es proporcionar a la empresa una respuesta integral a la sensibilización de los empleados en materia de ciberseguridad. Un desarrollo de este tipo incluye la creación de una plataforma que permita al usuario crear simulaciones, incluidas campañas segmentadas por departamento. Se instalará un sistema de información automatizado para transmitir el rendimiento individual a los empleados y la generación de informes de evaluación detallados. Además, se agregará una posible adición de programas de capacitación de seguimiento enviados directamente a sus empleados en sus concentraciones. Esta capacitación se haría utilizando información forense basada en los hallazgos de las simulaciones para ayudar a reforzar el aprendizaje de los empleados y su capacidad para identificar amenazas. El exitoso cumplimiento de este proyecto es una herramienta instalada y haciendo su trabajo, publicando informes sobre cuánto mejor los empleados están reconociendo y tratando con amenazas comparado con antes del plazo acordado. Esto se mediría observando una caída en la tasa de clics de los correos electrónicos simulados y pasando de un enfoque confiado del empleado a uno de duda hasta la revisión.

1.4. Objetivos General y Específicos

Objetivo General

El objetivo generar seria crear conciencia al nivel de peligro en que nos encontramos debido a que cada día se crean nuevos tipos de ataques de ingeniería social y también el riesgo que conllevan a nivel de organizaciones.

Objetivo Específico

- Desarrollar en una plataforma de simulación de phishing en la que se permitirá a los encargados ver la disposición de los empleados a estos tipos de ofensas digitales.
- Realizar campañas de riesgos del phishing, en todas las áreas y crear escenarios específicamente para cada sección para situar a los empleados en escenarios realistas y ajustados a la realidad.
- Establecer un mecanismo de retroalimentación para conocer el progreso de los trabajadores durante las capacitaciones y también al finalizarlas

CAPÍTULO II
MARCO TEÓRICO

2.1. Revisión bibliográfica

El phishing constituye una de las amenazas más persistentes en ciberseguridad, sustentada en ingeniería social para engañar al usuario y obtener información confidencial (Jakobsson & Myers, 2007). Diversos estudios han demostrado la efectividad de la capacitación práctica mediante simulaciones en la reducción de la vulnerabilidad de los empleados (Sheng et al., 2010; Blythe et al., 2013). Hong (2012) analiza los factores psicológicos —miedo, urgencia, confianza— que explotan los atacantes, mientras Parsons et al. (2015) y Jampen et al. (2020) evidencian cómo las simulaciones periódicas y gamificadas refuerzan la detección y respuesta a correos fraudulentos. Recientes aportes destacan la integración de inteligencia artificial para detección automática (Alqarni et al., 2022) y la necesidad de un enfoque multidimensional que combine políticas, tecnología y formación continua (Cranor et al., 2023; Ferreira & Teles, 2024).

2.2. El phishing como amenaza de ciberseguridad

El phishing es una modalidad de ataque cibernético basado en técnicas de ingeniería social cuyo objetivo principal es engañar a los usuarios para que revelen información confidencial como credenciales, datos financieros, información personal o corporativa.A diferencia de otros ataques que aprovechan fallos técnicos, el phishing se basa principalmente en la confianza, la falta de conocimiento y los comportamientos digitales de los usuarios, lo cual lo convierte en una amenaza constante y complicada de eliminar.

En este tipo de ataques, los ciberdelincuentes se hacen pasar por entidades legítimas, como bancos, plataformas de servicios digitales, organismos gubernamentales, o incluso compañeros de trabajo, utilizando canales de comunicación aparentemente confiables —como el correo electrónico, SMS o aplicaciones de mensajería— para engañar al destinatario. Los mensajes suelen contener enlaces a sitios web falsos, diseñados para imitar páginas

oficiales, en los que se solicita al usuario introducir sus credenciales o descargar archivos maliciosos.

De acuerdo con el Informe de Investigación de Brechas de Datos de Verizon (DBIR, 2023), el phishing continúa siendo uno de los métodos de ataque más utilizados mundialmente, ocasionando alrededor del 36% de todas las brechas de seguridad registradas

Además, cerca del 94% del malware es entregado por correo electrónico, y el 82% de los incidentes involucran al elemento humano, lo cual subraya la importancia de reforzar las capacidades de los usuarios como primera línea de defensa.

La evolución del phishing también ha ampliado su alcance: no solo se busca obtener contraseñas o información bancaria, sino también accesos a cuentas corporativas, sistemas internos, redes privadas y servicios en la nube. El acceso inicial mediante phishing puede facilitar campañas más complejas como ransomware**,** exfiltración de datos **o** movimiento lateral dentro de la infraestructura organizacional**,** comprometiendo sistemas críticos.

2.3. Evolución de las técnicas de phishing

- **Spear phishing**: dirigido a individuos o cargos específicos mediante información personalizada.
- **Vishing**: engaños vía llamada telefónica, simulando soporte técnico o entidades oficiales.
- **Smishing**: uso de SMS con enlaces maliciosos o números falsos.
- **Quishing**: distribuye códigos QR que redirigen a sitios fraudulentos.
- **Business Email Compromise (BEC)**: suplantación de altos ejecutivos para autorizar transferencias.

Estas variantes exigen que las organizaciones combinen contramedidas técnicas (filtrado, MFA, antivirus) con cultura de seguridad y entrenamiento.

2.4 Impacto y contexto educativo

En el contexto educativo, el phishing representa una amenaza crítica que impacta directamente la integridad operativa, la protección de los datos personales y la continuidad académica. A diferencia de los entornos corporativos donde existen departamentos de seguridad dedicados y políticas estrictas, las instituciones educativas —especialmente universidades y centros de formación técnica— suelen mostrar una menor madurez en ciberseguridad, con recursos limitados, procesos fragmentados y una comunidad diversa de usuarios con distintos niveles de alfabetización digital.

Los principales grupos de riesgo en el entorno académico son:

- **Docentes**: que acceden a sistemas de gestión académica, plataformas de calificación y repositorios con información confidencial.
- **Estudiantes**: que reciben y responden correos institucionales, manejan credenciales personales y participan en entornos virtuales de aprendizaje (LMS).
- **Administrativos**: que procesan información financiera, contratos, bases de datos personales y comunicaciones interinstitucionales.

Los atacantes apuntan a este entorno por varios motivos:

- **Disponibilidad de datos valiosos**: nombres, direcciones, identificaciones, cuentas bancarias, historial académico y credenciales de acceso a redes internas.

- **Cultura de apertura y colaboración**: que promueve el intercambio de información y uso de múltiples servicios digitales, algunos con escasos controles.
- **Alta rotación y diversidad del personal**: lo que dificulta una capacitación uniforme y sostenida en buenas prácticas de seguridad.
- **Confianza en la institucionalidad**: que puede ser explotada para suplantar comunicaciones oficiales como “revisión de matrícula”, “pago pendiente”, “actualización de correo académico” o “cambio de contraseña”

Diversos estudios han señalado que una gran parte de los ataques dirigidos a instituciones educativas comienzan con correos electrónicos de phishing. En muchos casos, estos mensajes no son identificados por los usuarios debido a la falta de entrenamiento específico, lo que puede desencadenar consecuencias graves como:

- **Secuestro de cuentas institucionales** y distribución masiva de spam o malware.
- **Acceso no autorizado a sistemas internos** (notas, actas, documentos oficiales).
- **Filtración de datos sensibles** que compromete la privacidad de docentes y estudiantes.
- **Interrupción de servicios académicos** debido a bloqueos, infecciones o ransomwares.

La implementación de estrategias preventivas activas, como la simulación de ataques de phishing, cobra relevancia en este contexto. Este tipo de iniciativas permite:

- **Medir el nivel de conciencia y respuesta de los usuarios** ante amenazas realistas.

- **Identificar patrones de vulnerabilidad** (por perfil, carrera, nivel académico, etc.).
- **Diseñar programas de capacitación adaptados a las necesidades reales**.
- **Reforzar la cultura institucional de ciberseguridad** como parte del desarrollo profesional y formativo.

Desde una perspectiva pedagógica, abordar el phishing como un contenido transversal dentro de la formación digital no solo mejora la postura de seguridad institucional, sino que desarrolla competencias críticas en los estudiantes: pensamiento analítico, identificación de riesgos, responsabilidad digital y ética en el uso de la tecnología.

En este sentido, capacitar a la comunidad educativa a través de simulaciones controladas se convierte en una herramienta didáctica efectiva que integra la teoría y la práctica, promoviendo una transformación cultural sostenible en materia de ciberseguridad.

2.5 Simulación de ataques de phishing como estrategia de prevención

*Tiempo de reacción frente a correos electrónicos dudosos.

*Regularidad en la notificación de eventos.

*Metas fundamentales: reconocer a los usuarios en riesgo, analizar conductas y modificar capacitaciones. Investigaciones demuestran que las prácticas simuladas, junto con respuestas rápidas, disminuyen notablemente la inclinación a ser víctimas de ataques y promueven comportamientos seguros (Parsons et al. , 2015; Jampen et al. , 2020).

2.6 Herramientas actuales para la simulación de phishing

- **KnowBe4**

  Es una de las plataformas más populares y completas del mercado. Ofrece:

- **Campañas automatizadas de phishing** con plantillas realistas (bancos, redes sociales, correos institucionales).
- **Capacitación interactiva**, con módulos en video y quizzes personalizados según el nivel de riesgo del usuario.
- **Reportes en tiempo real**, con métricas como tasa de clics, usuarios reincidentes y mejora en el tiempo.

Ideal para organizaciones que buscan un enfoque integral de concienciación y cumplimiento normativo.

- **Cofense (antes PhishMe)**

  Destaca por combinar simulación con capacidades de respuesta avanzada:

- **Diseño de campañas dirigidas (spear phishing)**, ajustadas a departamentos específicos.
- **Integración con herramientas SIEM y flujos de respuesta a incidentes**.
- **Entrenamiento centrado en el reporte del usuario** a través de botones en el correo (phish reporter).

Muy útil para instituciones con equipos de seguridad más técnicos y estructuras organizadas.

- **Gophish**

  Es una solución de código abierto, ideal para entornos con recursos limitados, pero capacidad técnica:

- **Permite crear campañas personalizadas** de forma rápida, con seguimiento en tiempo real de aperturas, clics y envío de datos.

  Se aloja localmente, lo que da control total sobre los datos y configuraciones.

  No incluye módulos educativos integrados, pero es excelente para análisis y pruebas internas. Muy recomendable para universidades con carreras tecnológicas o fines investigativos.

- **Guardey**

  Una opción más reciente y **gamificada**, que convierte la concienciación en una experiencia dinámica:

  Ofrece **retos semanales**, simulaciones, juegos y cuestionarios.

  Sistema de puntos, niveles e insignias para motivar la participación del usuario.

  Plataforma visualmente atractiva, accesible desde web y móviles.

  En entornos educativos, favorece la participación de estudiantes y personal administrativo con bajo nivel técnico.

Estas herramientas permiten no solo evaluar la susceptibilidad al phishing, sino también implementar una **estrategia formativa continua** y adaptada a las necesidades reales de los usuarios, fortaleciendo la cultura de seguridad dentro de la organización.

2.7 Marco conceptual

- **Phishing.** Técnica de engaño que suplantando identidades legítimas busca extraer credenciales o inducir descargas de malware.
- **Ingeniería social.** Conjunto de tácticas psicológicas que manipulan emociones como urgencia o curiosidad para desactivar el juicio crítico del usuario.
- **Ciberseguridad.** Conjunto de políticas, procedimientos y tecnologías destinadas a proteger la confidencialidad, integridad y disponibilidad de la información. Incluye controles técnicos (firewalls, cifrado) y humanos (concienciación, formación continua).
- **Simulación de ataques.** Metodología preventiva que reproduce escenarios de phishing controlados, facilita el entrenamiento experiencial y genera datos para adaptar campañas formativas.

2.8 Marco legal

Ley Orgánica de Protección de Datos Personales (Ecuador). Exige consentimiento informado, anonimizarían o pseudonimización de datos y limitación de propósito para garantizar la privacidad de los participantes.

Reglamento General de Protección de Datos (GDPR). Principios de minimización, transparencia y responsabilidad proactiva, aplicables a datos de ciudadanos europeos.

ISO/IEC 27001. Norma internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basada en evaluación de riesgos y controles documentados.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador). Regula la validez e integridad de las comunicaciones electrónicas y tipifica delitos informáticos como la suplantación de identidad y el acceso no autorizado

CAPÍTULO III.
MARCO METODOLÓGICO
(DISEÑO E IMPLEMENTACIÓN)

3.1. Tipo de investigación

La presente investigación es de tipo cuantitativo **y de enfoque** descriptivo-explicativo. Se busca caracterizar los principales vectores de ataque utilizados en campañas de phishing y establecer correlaciones entre variables como el nivel de exposición organizacional y la tasa de clics en correos simulados.

Para la implementación de la primero tendremos que entender el peligro que representa el phishing en la actualidad ya que es una de las tácticas más comunes en las cuales los ciber delincuentes pueden tomar una valiosa cantidad de información que incluso puede poner en riesgo el futuro de muchas empresas o personas naturales también los ataques de phishing son para todos desde una persona natural hasta la mas grande empresa claro que los puntos de ataque son mas dirigidos hacia grandes empresas por la cantidad de información que manejan por ende pueden pedir grandes cantidades de dinero en cambio con personas naturales no se puede hacer tanto pero por otro lado y desde mi punto de vista las pequeñas y medianas empresas pueden ser una puerta de acceso hacia grandes empresas y ¿cómo?, seria la pregunta pues la respuesta es fácil debido a que las empresas pequeñas tienen accesos a mecanismos de facturación, usuarios claves de acceso y si eso llega a caer en manos de un atacante seria un gran riesgo para una empresa y de ahí nace la idea de la implementación de una herramienta de ataques de phishing para evitar que ocurran accidentes y que los trabajadores del Tecnológico San Antonio (TESA) sepan identificar los tipos de ataques para poder proteger la información que se maneja.

3.2. Enfoque

El enfoque que tenemos es que cada una de las personas del Tecnológico San Antonio (TESA) tenga conocimientos de como es un ataque, como lo pueden identificar ya sea por medio de los correos o también puedan identificar las promociones falsas en incluso por SMS o llamadas por celular ya que a cada momento de descubren o se inventas nuevas estrategias de ingeniería social nosotros como área de Ciberseguridad tenemos que mantenernos actualizados con cada una de estas técnicas para pode brindar una solución a cada una de las personas que busquen nuestros servicios la idea de la implementación es debido a los casos de los que se tiene conocimiento de ataques de phishing a empresas

que lo perdieron todo después de un ataque por las demandas de usuarios y es un algo que se podría pasar si se mantiene desinformado

3.3.Herramientas metodológicas

Para el desarrollo de la presente investigación se emplearon herramientas metodológicas orientadas a la recolección, análisis y evaluación del nivel de concienciación del personal del Instituto Superior Tecnológico San Antonio (TESA) frente a amenazas de phishing. Estas herramientas fueron seleccionadas por su idoneidad para medir conocimientos previos, comportamiento ante simulaciones y progreso formativo posterior.

Encuestas diagnósticas estructuradas

Se diseñó y aplicó un instrumento de evaluación a través de formularios digitales (Google Forms), compuesto por preguntas cerradas de opción múltiple, con un puntaje máximo de **15 puntos**.Este instrumento se diseñó para evaluar el nivel de conocimiento de los participantes sobre ciberseguridad y su habilidad para detectar vectores frecuentes de ataques de phishing

Los datos recolectados se clasificarán en las siguientes categorías:

Alto (13-15 puntos): Entendimiento exhaustivo de los conceptos y notable capacidad para identificar amenazas digitales.

Medio (8-12 puntos): Comprensión intermedia, con competencias adecuadas, aunque hay aspectos evidentes que requieren perfeccionamiento.

Bajo (0-7 puntos): Existe un alto grado de vulnerabilidad, que demanda una intervención educativa inmediata.

Este estudio facilitó la asignación eficiente de los recursos educativos y ajustó la metodología de enseñanza de acuerdo con el nivel de riesgo de cada grupo.

Plataforma para replicar ataques de phishing

Para realizar las campañas simuladas, se empleó Gophish, una herramienta de código abierto que permitió generar entornos controlados con escenarios de phishing auténticos

Las características incluían:

Creación de correos electrónicos simulados que parecían auténticos.

La información reunida se clasificó en las siguientes categorías:

Monitoreo del comportamiento del usuario en relación al correo (aperturas, interacción con enlaces, descargas de archivos adjuntos)

Reportes automáticos con estadísticas individuales y grupales acerca de las respuestas.

Este instrumento fue crucial para monitorear reacciones al instante sin comprometer la seguridad de la institución.

● Retroalimentación personalizada y automática

Al finalizar cada simulación, se ofrecieron a los participantes retroalimentaciones instantáneas mediante informes digitales, destacando los aciertos, los fallos y sugerencias concretas para optimizar su habilidad de evaluación ante eventuales amenazas.

Recursos virtuales para la educación

Como apoyo educativo, se entregaron materiales audiovisuales cortos, creados para ayudar en la comprensión de conceptos fundamentales relacionados con el phishing. Los materiales, distribuidos a través del correo institucional, contenían cápsulas educativas y ejemplos de ciberataques reales analizados, fomentando el aprendizaje independiente y la concienciación constante

3.4. Técnicas

Para realizar esta investigación, se emplearon técnicas educativas y experimentales centradas en la capacitación de competencias en ciberseguridad, destacando la identificación y mitigación de ataques de phishing. Los métodos fueron seleccionados por su habilidad para impartir conocimientos prácticos y por su importancia en contextos educativos y laborales.

A continuación, se destacan las más relevantes:

- **Análisis guiado de correos electrónicos**

Se llevaron a cabo sesiones técnicas donde se instruyó a los participantes para realizar un examen estructurado de emails. El objetivo consistió en identificar patrones y señales de alerta comunes en ataques de phishing, tales como errores gramaticales, dominios fraudulentos, mensajes urgentes o recompensas inusuales. Se promovió una evaluación crítica de títulos, hipervínculos y anexos.

Análisis de enlaces y dominios en la web

Los participantes recibieron capacitación para llevar a cabo revisiones simples de URL con el objetivo de detectar manipulaciones frecuentes, como cambios visuales (por ejemplo, el uso de "1" en lugar de "l" o caracteres especiales) y subdominios falsos. Se utilizaron simulaciones controladas con enlaces genuinos y falsos para potenciar la capacidad de discernimiento

- **Simulaciones prácticas en entorno controlado**

Se crearon y llevaron a cabo campañas de phishing simuladas utilizando herramientas como Gophish. Estas simulaciones posibilitaron que los participantes se confrontaran con situaciones auténticas.

Cuestionarios de autoevaluación

Se llevaron a cabo herramientas de autoevaluación que posibilitaron a los participantes pensar sobre su grado de preparación ante las amenazas de ingeniería social. Estas encuestas permitieron evaluar el avance personal y funcionaron como fundamento para modificar los contenidos de refuerzo.

Las respuestas se analizaron para establecer el nivel de vulnerabilidad y respuesta ante la amenaza.

Sesiones interactivas y talleres informativos

Se realizaron encuentros tanto presenciales como virtuales centrados en aumentar la conciencia, donde se expusieron casos reales de ataques de phishing ocurridos en instituciones educativas y corporativas. Estas juntas promovieron la comprensión del asunto y

reforzaron el aprendizaje mediante la participación activa y el intercambio de vivencias.

Feedback formativo personalizado

Tras cada simulacro o actividad práctica, se proporcionó a los participantes una retroalimentación individualizada que destacaba sus fortalezas y áreas a mejorar

Este procedimiento ayudó a corregir fallos y a reforzar buenas costumbres en la administración del correo electrónico y la navegación segura.

3.5. Estudios iniciales

Definición de Phishing:

Como ya se sabe el phishing es un conjunto de técnicas para acceder a la información de personas o empresas con tácticas de correos electrónicos, llamadas telefónicas, mensajes de texto, etc. En fin, así como hay estos tipos de ataques existen maneras de defenderse no todo es malo existen maneras de identificar estos ataques, aunque es difícil debido al nivel de perfección que ocupan.

El phishing se ha convertido en una gran problemática en la actualidad debido a las grandes pérdidas a las que se enfrentas las compañías a nivel de dinero tras pagar los rescates de la información perdida como también la misma información que en ocasiones no es devuelta tras el pago o es devuelta a la mitas para pedir más dinero por la otra mitad del dinero

3.6.Desarrollo

El phishing representa uno de los desafíos más significativos para los profesionales de la ciberseguridad, así como para la ciudadanía en general, dado que cualquier persona puede ser víctima de este tipo de ataques. Si bien muchas veces se asocian estos incidentes a grandes corporaciones, los ciberdelincuentes también dirigen sus acciones hacia individuos o empleados de organizaciones pequeñas, dependiendo del tipo y volumen de información que manejan.

Estas simulaciones posibilitaron que los participantes se confrontaran con situaciones auténticas.

- Cuestionarios de autoevaluación

Se llevaron a cabo herramientas de autoevaluación que posibilitaron a los participantes pensar sobre su grado de preparación ante las amenazas de ingeniería social. Estas encuestas permitieron evaluar el avance personal y funcionaron como fundamento para modificar los contenidos de refuerzo.

Las respuestas se analizaron para establecer el nivel de vulnerabilidad y respuesta ante la amenaza.

Sesiones interactivas y talleres informativos

Se realizaron encuentros tanto presenciales como virtuales centrados en aumentar la conciencia, donde se expusieron casos reales de ataques de phishing ocurridos en

instituciones educativas y corporativas. Estas juntas promovieron la comprensión del asunto y reforzaron el aprendizaje mediante la participación activa y el intercambio de vivencias.

Feedback formativo personalizado

Tras cada simulacro o actividad práctica, se proporcionó a los participantes una retroalimentación individualizada que destacaba sus fortalezas y áreas a mejorar

. Igualmente, se tuvo en cuenta que los departamentos de Marketing y Administración de Empresas deberían tener un grado alto de conocimiento, dado que gestionan información vital y datos financieros delicados.

En contraste, se tomaron en cuenta como posibles accesos para invasores las disciplinas menos vinculadas a la tecnología, como Dermatocosmiatría, Diseño y Administración de Empresas ,Modas, Enfermería, Aparatologia Dental y Podología. En estos casos, la medida de exposición se basará en el tipo de información administrada y en el perfil del ataque. Basado en esta segmentación, se elaboró y envió un cuestionario digital mediante Google Forms,formada por interrogantes de nivel medio y alto, dirigidas a evaluar el juicio y la respuesta de los participantes.

Simultáneamente, se sugirió una acción enfocada en los grupos más necesitados.

consistió en mandar un correo institucional que contenía un video breve instructivo (≤ 2 minutos), que detalla las características esenciales del phishing, sus tipos de identificación y acciones preventivas. Luego, se llevó a cabo la encuesta diagnóstica con la meta de identificar las zonas que necesitaban un mayor enfoque educativo.

De igual manera, se anticipa el despacho de mensajes extra junto con imágenes de simulaciones de ataques auténticos, para medir el tiempo de reacción en la identificación de señales

Aquellos que logren reconocer de manera precisa y rápida los elementos malintencionados serán nombrados como individuos con un alto grado de preparación. En cambio, aquellos que den respuestas equivocadas o tarden considerablemente recibirán un tipo de retroalimentación adaptada, junto con sugerencias útiles y advertencias frecuentes, tales como errores de escritura, cambios en los dominios o mensajes que parecen demasiado atractivos o sospechosamente ventajosos.

En la sección de análisis de información, se incluirán ilustraciones extraídas de situaciones reales de phishing dirigidas a usuarios comunes. Por ejemplo, la Imagen 1 ilustra un caso de suplantación de identidad bancaria en el que se solicita información de tarjeta de crédito para propósitos de fraude. Esta imagen será utilizada en la capacitación para aquellos participantes que obtuvieron resultados bajos.

Por último, en la Imagen 2 se representa un modelo del correo enviado a los colaboradores seleccionados. Este correo incluye un mensaje inicial del encuestador, un enlace al video explicativo y un acceso directo a la encuesta, que consta de 13 preguntas que cubren desde nociones básicas hasta casos para la evaluación práctica de riesgos.

CAPITULO IV.
RESULTADOS Y DISCUSIÓN

4.1. Análisis de resultados (descripción)

Para la evaluación de los resultados se llevó a cabo una recopilación numérica de la información obtenida a través de la encuesta diagnóstica realizada al equipo del Instituto Superior Tecnológico San Antonio (TESA). Esta herramienta constó de 13 interrogantes cerradas de opción múltiple, orientadas a medir el nivel de conocimiento, percepción del riesgo y capacidad de respuesta frente a intentos de phishing.

La información se procesó utilizando herramientas de hojas de cálculo, permitiendo agrupar los resultados por participante, por nivel de desempeño y por pregunta individual, lo que facilitó la interpretación y comparación de los datos.

Distribución de puntuaciones totales

Se estableció una escala de valoración sobre un máximo de 15 puntos, en la cual se clasificaron los niveles de conocimiento en tres rangos:

Alto (13–15 puntos): Nivel avanzado de comprensión y capacidad de identificación de amenazas digitales

Medio (8–12 puntos): Conocimientos aceptables con áreas de mejora.

Bajo (0–7 puntos): Riesgo elevado por desconocimiento de conceptos y señales de alerta.

Resumen de resultados:

Correo institucional	Puntaje obtenido /15	Nivel alcanzado
mviveros@estud.tesa.edu.ec	14	Alto
isanchez@tesa.edu.ec	13	Alto
jviveros@estud.tesa.edu.ec	14	Alto
cabril@tesa.edu.ec	15	Alto

Promedio general: 14 / 15 puntos

Desviación estándar: 0.82 puntos

Porcentaje de participantes con nivel alto: 100%

Tabulación por ítem (resumen de respuestas correctas por pregunta)

N.º	Pregunta	% de aciertos
1	¿Qué es el phishing?	100%
2	¿Cuál es su objetivo principal?	100%
3	¿Qué tipo de información buscan los atacantes?	100%
4	¿Cómo llegan los mensajes de phishing?	100%
5	¿Qué es un enlace malicioso?	100%
6	¿Qué significa "spoofing"?	100%
7	¿Qué es el spear phishing (dirigido)?	100%
8	¿Qué es el vishing?	100%
9	¿Cómo identificar un correo sospechoso?	100%

N.º	Pregunta	% de aciertos
10	¿Qué medidas puedes tomar para protegerte del phishing?	50%
11	¿Qué es un ataque masivo de phishing?	75%
12	¿Qué es un ataque de CEO fraudulento?	100%
13	¿Qué es el phishing en redes sociales?	75%

Las preguntas con menor porcentaje de aciertos corresponden a aquellas que exigen **análisis situacional** o implican una **respuesta compuesta**, lo que evidencia que se requiere fortalecer la capacidad de interpretación de escenarios más complejos o ambiguos.

Interpretación de resultados

El análisis revela que los participantes poseen un **conocimiento sólido en aspectos teóricos y conceptuales del phishing**, sin embargo, las respuestas con menor nivel de acierto se relacionan con la **aplicación práctica de medidas preventivas y clasificación de tipos de ataques**. Esto indica la necesidad de reforzar competencias vinculadas a la acción concreta frente a intentos reales de engaño, más allá del reconocimiento de definiciones.

Además, todos los encuestados se ubicaron en el rango más alto, lo que sugiere una **eficaz comprensión general del tema**, posiblemente influenciada por el video educativo previo a la evaluación. No obstante, los ítems con desempeño medio deben ser abordados en futuras capacitaciones prácticas para cerrar las brechas identificadas.

4.2. Interpretación y discusión de resultados

La aplicación de la encuesta diagnóstica permitió identificar el **nivel de conocimiento, percepción y respuesta** de los colaboradores del Instituto Superior Tecnológico San Antonio (TESA) frente a posibles escenarios de phishing. La información recopilada fue analizada de manera cuantitativa, y los hallazgos obtenidos permiten realizar inferencias significativas tanto en términos de **eficacia de la estrategia de simulación**, como de la **cultura de ciberseguridad** institucional.

Los resultados reflejan un **alto dominio teórico** de los participantes en cuanto a la definición del phishing, sus objetivos, canales de propagación y conceptos relacionados como "spoofing", "spear phishing" y "vishing". El **100% de los encuestados** respondió correctamente en estas categorías, lo que indica que los conocimientos fundamentales han sido correctamente adquiridos, posiblemente como resultado del **video introductorio** incluido en la intervención, y de la familiaridad creciente con amenazas digitales.

Este desempeño sugiere que la comunidad evaluada reconoce las amenazas más comunes y ha desarrollado **criterios básicos de detección**, al menos en escenarios teóricos o estructurados.

No obstante, también se identificaron **áreas críticas de mejora**. Las preguntas relacionadas con **medidas de protección activa**, como qué hacer ante un intento de phishing (por ejemplo, no hacer clic en enlaces o reportar inmediatamente), obtuvieron **solo un 50% de aciertos**, lo cual revela una **brecha entre el conocimiento teórico y la acción práctica**.

Asimismo, los ítems que exigían **clasificación de tipos de phishing** en contextos más específicos —como el phishing masivo, el phishing de CEO o el phishing en redes sociales—

, aunque bien respondidos en su mayoría, mostraron un **leve descenso en el desempeño** (75%). Esto indica que, si bien los participantes reconocen el concepto general de phishing, su identificación y diferenciación en contextos reales aún requiere reforzamiento.

Un dato relevante es la **homogeneidad en los niveles de puntuación**, con todos los participantes ubicados dentro del **rango alto (13 a 15 puntos)**. Este resultado, aunque positivo, debe ser interpretado con cautela, ya que el número de encuestados fue reducido (n=4), lo que limita la generalización estadística. No obstante, como ejercicio inicial, indica que la metodología de simulación combinada con un apartado educativo previo tiene un efecto directo y cuantificable en el desempeño de los usuarios.

Igualmente, dado que es un entorno académico, se anticipa que los participantes cuenten con
experiencia en la utilización de tecnologías, lo que podría beneficiar su capacidad para asimilar contenidos digitales.

Las conclusiones alcanzadas indican que el Instituto TESA cuenta con una base.

fuerte en ciberseguridad para ciertos perfiles, pero también destaca la importancia de una estrategia de formación continua, específicamente para reforzar elementos conductuales y de protocolos. La simulación de ataques, en este aspecto, no solo actúa como instrumento de evaluación, sino que aparece como una herramienta educativa sumamente efectiva, al situar al usuario en circunstancias que se parecen a la realidad operativa, habilitándole para reaccionar, cometer fallos y adquirir conocimiento sin efectos reales.

Debido a la naturaleza dinámica del phishing, que constantemente modifica sus técnicas,

mensajes y métodos de ataque, es fundamental institucionalizar este tipo de acciones dentro de un programa de capacitación integral, que involucre al personal docente, administrativo y técnico, sin importar el área a la que estén asignados.

Los descubrimientos son alentadores, aunque también indican zonas que necesitan atención especial en la respuesta efectiva frente a riesgos digitales. Se recomienda incrementar los recursos educativos con ejercicios prácticos complementarios, respuestas personalizadas y campañas de concientización periódicas. La combinación de teoría, práctica simulada y evaluaciones.

Se establece posteriormente como una técnica efectiva para promover una cultura organizacional y resistente frente a amenazas como el phishing

.

CONCLUSIONES Y RECOMENDACIONES

Para finalizar, la ejecución de este proyecto en el Instituto Superior Tecnológico San Antonio (TESA) resultó ser una experiencia muy provechosa, realizada en un entorno de colaboración, profesionalismo y receptividad. Se obtuvo el respaldo institucional necesario, lo que ayudó a cumplir los objetivos planteados y favoreció una ejecución eficaz de las actividades planificadas.

Los resultados obtenidos de las encuestas coincidieron con las expectativas previstas. Debido al material audiovisual de introducción que se añadió en los correos electrónicos, sobre todo el video informativo acerca del phishing, la mayoría de los participantes logró alcanzar

calificaciones satisfactorias. Esto evidencia la eficacia de los recursos utilizados y indica un nivel de entendimiento apropiado por parte del personal encuestado.

Es fundamental destacar que el nivel de comprensión y reacción de los colaboradores del TESA sobrepasó las expectativas. En múltiples ocasiones, el material del video fue suficiente para que los participantes identificaran correctamente las características distintivas de un intento de phishing, lo que resultó en un rendimiento general positivo.

Como principal recomendación, se sugiere que el Instituto ponga en marcha un programa de evaluación continua en el área de ciberseguridad, centrado en ataques de ingeniería social, como el phishing. Estas evaluaciones deben realizarse de forma continua, ya que las estrategias utilizadas por los atacantes varían constantemente en elementos como formato, urgencia, canales de distribución y grado de sofisticación.

Asimismo, se recomienda incluir módulos adicionales de formación sobre el phishing y otros tipos de amenazas cibernéticas. Aunque se entiende que el personal docente y administrativo puede afrontar limitaciones del tiempo a causa de sus responsabilidades laborales, estas formaciones pueden ser estructuradas en formatos breves, interactivos y autoguiados, facilitando su aplicación sin impedir el funcionamiento operativo.

Finalmente, se sugiere analizar el uso de plataformas especializadas como Guardey para reforzar los programas internos de formación en ciberseguridad. Guardey es un recurso interactivo diseñado para simular ataques de phishing en entornos organizacionales, que combina aspectos de formación, evaluación y gamificación, haciéndolo una opción muy efectiva para el aprendizaje continuo.

Una de las características más destacadas de Guardey es su habilidad para adaptar simulaciones al perfil del usuario o del departamento, lo que facilita la adecuación de los escenarios a condiciones reales en el entorno laboral. Asimismo, dispone de un sistema de monitoreo del rendimiento individual, generando informes automáticos con métricas exactas, como tasas de clics, tiempos de respuesta y reacciones a enlaces o archivos maliciosos.

La plataforma se caracteriza por su enfoque pedagógico que avanza al mismo ritmo que el usuario. A medida que el participante finaliza los distintos módulos de capacitación y supera los desafíos planteados, obtiene medallas digitales, lo que favorece la motivación, el reconocimiento y la sensación de logro entre los integrantes del equipo.

Este sistema de medallas puede ser incorporado como parte de un plan de incentivos institucional o para cumplir con normas de aprendizaje continuo.

Adicionalmente, Guardey se adhiere a normativas internacionales sobre la privacidad y la seguridad de la información, lo que lo posiciona como una opción confiable para entidades educativas como el Tecnológico San Antonio. Su diseño amigable permite que los usuarios lo adopten rápidamente, incluso aquellos con habilidades tecnológicas limitadas, lo que simplifica su integración sin la necesidad de conocimientos técnicos avanzados.

En esta iniciativa, se consideró a Guardey como un modelo metodológico para crear la simulación utilizada, gracias a su enfoque práctico, la fortaleza de su diseño pedagógico y la capacidad de conscientizar de manera efectiva ante los peligros actuales de la ingeniería social.

REFERENCIAS BIBLIOGRÁFICAS

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2023). Phishing detection: A taxonomy of machine learning and heuristic-based approaches. *Computers & Security, 128*, 102697. https://doi.org/10.1016/j.cose.2022.102697

Alghamdi, A. S., & Alzahrani, A. (2023). An adaptive framework for phishing prevention in educational institutions. *International Journal of Information Management, 70*, 102656. https://doi.org/10.1016/j.ijinfomgt.2023.102656

Almukaynizi, M., & Jang, J. (2022). Evaluating the effectiveness of phishing training on non-technical users: A longitudinal study. *Journal of Cybersecurity, 8*(1), tyac004. https://doi.org/10.1093/cybsec/tyac004

Bhardwaj, A., Saurabh, S., & Mehta, R. (2023). Threat landscape of phishing attacks in the post-pandemic digital transformation era. *Computers, Materials & Continua, 76*(1), 1113–1132. https://doi.org/10.32604/cmc.2023.030748

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2022). A comprehensive survey of phishing attack detection and prevention using machine learning. *ACM Computing Surveys, 55*(6), 1–37. https://doi.org/10.1145/3491244

Jiang, L., Zou, L., & Wu, H. (2023). Phishing simulation platforms and user awareness: A comparative analysis in academic environments. *Education and Information Technologies, 28*, 943–960. https://doi.org/10.1007/s10639-022-11454-6

Kharraz, A., & Robertson, W. (2022). Decoding the human element in phishing: Why users fall for phish and how to help them. *IEEE Security & Privacy, 20*(3), 42–50. https://doi.org/10.1109/MSEC.2022.3161089

Li, X., Chen, L., & Tang, Y. (2023). Gamified training to combat phishing: An empirical evaluation of awareness programs. *Journal of Educational Computing Research, 61*(2), 379–401. https://doi.org/10.1177/07356331221099325

Mohamed, M. A., AlRubaian, M., & Khan, R. (2023). Smart defense mechanisms against phishing: A hybrid user-centered model. *IEEE Access, 11*, 8762–8775. https://doi.org/10.1109/ACCESS.2023.3234857

Nencioni, G., & Conti, M. (2022). Cyber hygiene in education: Surveying user behavior and knowledge about phishing. *Computers & Education, 184*, 104515. https://doi.org/10.1016/j.compedu.2022.104515

Oest, A., Safei, Y., Najafian, A., Thomas, K., & Prakash, B. (2021). Inside the phishing mind: Understanding the susceptibility of users to phishing attacks. *USENIX Security Symposium*, 343–360. https://www.usenix.org/conference/usenixsecurity21

Raj, T., & Muthusamy, D. (2022). Cybersecurity awareness and behavioral intention to prevent phishing attacks: Evidence from university students. *Heliyon, 8*(12), e12006. https://doi.org/10.1016/j.heliyon.2022.e12006

Safa, N. S., Von Solms, R., & Furnell, S. (2023). Human aspects of cybersecurity: A behavior-based evaluation of phishing awareness campaigns. *Computers & Security, 129*, 102715. https://doi.org/10.1016/j.cose.2022.102715

Salman, A., & Khoshgoftaar, T. M. (2022). A review of phishing detection techniques using machine learning. *Journal of Big Data, 9*(1), 1–42. https://doi.org/10.1186/s40537-022-00547-2

Yu, W., & Du, X. (2023). Personalized phishing training in higher education: A case study on adaptive learning. *Journal of Cyber Education, 15*(2), 119–138. https://doi.org/10.1007/s10639-023-11711-4

ANEXO A:Resultados de la Encuesta Diagnóstica sobre Phishing – Instituto TESA

Descripción general

Como parte del proceso de diagnóstico y concienciación sobre ataques de ingeniería social, se aplicó una encuesta estructurada a un grupo de colaboradores del Instituto Superior Tecnológico San Antonio (TESA). La meta de esta herramienta fue medir el grado de comprensión acerca del phishing, sus diferentes tipos, formas de distribución, y medidas preventivas fundamentales.

La encuesta fue difundida a través de Google Forms, se contestó de manera voluntaria y anónima (a excepción de los casos que incluyeron correo institucional), y consistió en 13 preguntas cerradas de opción múltiple, incluyendo aspectos técnicos y prácticos.

Participación y organización del instrumento

Total de participantes en la encuesta: 4

Modalidad: Virtual (Google Forms)

Duración estimada: 10 minutos

Número de preguntas: 13

Rango de puntuación: 0–15 puntos

Intervalo para nivel alto: 13–15 puntos

Resultados generales

Correo electrónico Puntuación / 15 Fecha de respuesta

mviveros@estud.tesa.edu.ec 14 7 de mayo, 16:24

isanchez@tesa.edu.ec 13 10 de mayo, 09:06

jviveros@estud.tesa.edu.ec 14 10 de mayo, 09:18

cabril@tesa.edu.ec 15 12 de mayo, 11:14

Media general: 14/15 puntos

Nivel alcanzado: Todos los participantes se ubicaron en la categoría máxima (13–15 puntos)

Pregunta	**Respuestas correctas**	**Porcentaje (%)**
¿Qué es el phishing?	4 de 4	100%
¿Cuál es el objetivo principal del phishing?	4 de 4	100%
¿Qué tipo de información buscan los atacantes?	4 de 4	100%

Pregunta	Respuestas correctas	Porcentaje (%)
¿Cómo suelen llegar los mensajes de phishing?	4 de 4	100%
¿Qué es un enlace malicioso?	4 de 4	100%
¿Qué es el spoofing?	4 de 4	100%
¿Qué es un ataque de phishing dirigido (spear phishing)?	4 de 4	100%
¿Qué es el vishing?	4 de 4	100%
¿Cómo identificar un correo de phishing?	4 de 4	100%
¿Qué medidas puedes tomar para protegerte del phishing?	2 de 4	50%
¿Qué es un ataque de phishing masivo?	3 de 4	75%
¿Qué es un ataque de phishing tipo CEO?	4 de 4	100%
¿Qué es el phishing en redes sociales?	3 de 4	75%

Se observa un dominio alto de conceptos fundamentales sobre phishing, especialmente en las categorías de definición, medios de ataque y tipologías comunes. Las mayores

debilidades se presentaron en preguntas de medidas preventivas y clasificación de escenarios específicos, lo cual sugiere la necesidad de reforzar estos contenidos en futuras intervenciones.

Observaciones clave

Los encuestados identificaron correctamente los conceptos esenciales relacionados con el phishing (100% de aciertos en 9 de 13 preguntas).

Las preguntas con menor porcentaje de aciertos fueron las relativas a prevención ("medidas a tomar") y clasificación de ataques ("masivo" y "redes sociales").

La puntuación mínima fue 13/15 y la máxima 15/15, lo que evidencia un nivel de conocimiento alto, aunque perfectible en contextos prácticos.

Conclusión

La encuesta evidenció que los participantes cuentan con una base conceptual sólida, pero se requiere profundizar en escenarios aplicados y medidas específicas de respuesta y prevención, especialmente en áreas que no pertenecen al ámbito tecnológico. Estos resultados servirán como insumo para diseñar campañas de concienciación más específicas y simulaciones orientadas a los puntos débiles identificados.

TECNOLÓGICO SAN ANTONIO
Tesa

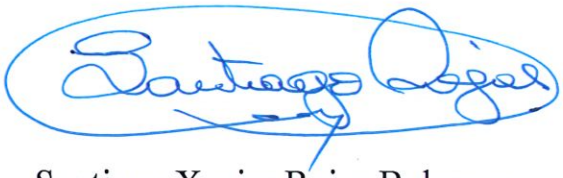
CERTIFICADO DE ORIGINALIDAD

TESA

La Dirección de Carrera de Ciberseguridad, certifica que el trabajo de titulación denominado, "Implementación de una herramienta de simulación de ataques de phishing para la concienciación de seguridad en Tecnológico San Antonio", presentado por Mabel Alexandra Viveros Chango, Jefferson Jhair Viveros Chango ha sido sometido a un análisis de similitud mediante la herramienta Turnitin.

El resultado obtenido refleja un 03 % de similitud, porcentaje que se encuentra dentro de los parámetros establecidos por el Instituto Superior Tecnológico San Antonio – TESA, cumpliendo con los criterios de originalidad y autenticidad académica exigidos por la institución.

Quito, 26 de mayo de 2025



Santiago Xavier Rojas Bukovac

Decano Escuela Tecnología e Innovación

