RELIGACIÓN
REVISTA

Protección contra ataques de ingeniería social: análisis cualitativo de estrategias, tecnologías y patrones específicos

Protection against social engineering attacks: Qualitative analysis of strategies, technologies and specific patterns

Edison Andrés Fueres Quilumbango, Roberto Omar Andrade Paredes, Marco Vinicio Yamba Yugsi

Resumen:

La ingeniería social es una técnica que utiliza el cibercriminal, para aprovechar la falta de conocimiento sobre seguridad de la información por parte de los usuarios. En este sentido, la presente investigación explora las estrategias, tecnologías y patrones específicos para mitigar los ciberataques, con énfasis en la ingeniería social. Para lo cual, se utiliza una metodología cualitativa basada en entrevistas a docentes investigadores y expertos en ciberseguridad, seleccionados mediante un muestreo aleatorio simple. Los resultados muestran que la falta de capacitación en ciberseguridad convierte a los usuarios en blancos fáciles para los atacantes, a esto se suma la ausencia de estrategias adecuadas y tecnologías que mitiguen las amenazas. Entre las conclusiones, se destaca la urgencia de implementar políticas de seguridad, programas de concientización y herramientas tecnológicas como Firewalls, Antivirus, AntiSpam, autenticación multifactorial y sistemas de detección y prevención de intrusiones, con el objetivo de fortalecer la ciberseguridad en los entornos vulnerables.

Palabras clave: Ciberseguridad; ciberataque; ciberamenaza; ingeniería social; phishing.

Edison Andrés Fueres Quilumbango
Universidad Católica de Cuenca | Cuenca | Ecuador | edison.fueres.37@est.ucacue.edu.ec
https://orcid.org/0009-0006-8433-2898
Roberto Omar Andrade Paredes
Universidad Católica de Cuenca | Cuenca | Ecuador | roberto.andrade@ucacue.edu.ec
https://orcid.org/0000-0002-7120-281X
Marco Vinicio Yamba Yugsi
Universidad Católica de Cuenca | Cuenca | Ecuador | marco.yamba@ucacue.edu.ec
https://orcid.org/0000-0003-4095-1444

http://doi.org/10.46652/rgn.v10i44.1310
ISSN 2477-9083
Vol. 10 No. 44 enero-marzo, 2025, e2501310
Quito, Ecuador

Enviado: julio 31, 2024
Aceptado: septiembre 19, 2024
Publicado: octubre 12, 2024
Publicación Continua

CC BY NC ND

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

Social engineering is a technique used by cybercriminals to take advantage of the lack of knowledge about information security on the human side. In this sense, this research explores the strategies, technologies and specific patterns to mitigate cyberattacks, with emphasis on social engineering. For this purpose, a qualitative methodology is used based on interviews with teacher researchers and cybersecurity experts, selected through simple random sampling. The results show that the lack of training in cybersecurity makes users easy targets for attackers, in addition to the absence of appropriate strategies and technologies to mitigate threats. Among the conclusions, it must be highlighted the urgency of implementing security policies, awareness programs and technological tools such as Firewalls, Antivirus, AntiSpam, multifactor authentication and intrusion detection and prevention systems, this in order to strengthen cybersecurity in vulnerable environments.

Keywords: Cybersecurity; cyberattack; cyberthreat; social engineering; phishing.

Introducción

Actualmente, múltiples entidades públicas y privadas del Ecuador han sufrido distintos tipos de ataques informáticos a su información, esto se debe al desconocimiento en el ámbito de la ciberseguridad, pues no han logrado contrarrestar dichas ciberamenazas (Torres, 2022). Lo cual ha dado apertura al planteamiento de estrategias, patrones y tecnologías que puedan implementarse para la mitigación de ciberataques.

Las estadísticas revelan que el Ecuador se sitúa como el tercer país de América Latina más afectado por ataques cibernéticos (Kaspersky Team, 2024). Estos ciberataques han dejado a las entidades ecuatorianas de los sectores estratégicos como la banca, e-commerce, entre otros, en una posición vulnerable frente a las amenazas digitales (Naranjo Godoy, 2024).

Uno de los factores clave para la evolución continua de los ciberataques es el aumento del entorno de ataque con el que cuentan los ciberdelincuentes (Vega, 2023). Inicialmente lo único que se podía atacar era un computador, en dicho espacio era muy común que los virus se expandan por medio de dispositivos de almacenamiento. Pero cuando se extendió la comunicación mediante las redes informáticas y el internet, los virus entraban a través de puntos poco seguros, en ese proceso todo quedaba en las computadoras (Agudelo, 2023). Sin embargo, actualmente se pueden atacar casi todos los dispositivos tecnológicos que se encuentran conectados a internet, esto produce que las posibilidades de robo de información mediante ciberataques sean muy comunes (Sosa, 2023).

Entre los métodos de ciberataque mayormente utilizados en nuestro entorno está el de ingeniería social (Meza et al., 2024). El cual se basa en el uso de técnicas de manipulación para engañar a las personas y lograr que revelen información confidencial brindando acceso a datos valiosos (Garzón Ibarra et al., 2024). Esta estrategia es altamente efectiva para evadir la seguridad de las redes, sin importar la fortaleza de los cortafuegos, las claves criptográficas, los sistemas de detección de intrusos, los antivirus y otras herramientas de seguridad (ISACA, 2022).

Los ataques de ingeniería social buscan aprovechar las debilidades humanas aplicando técnicas de ciberataques tales como *Phishing, Baiting, Tailgating, Spear Phishing, Vishing, Smishing,* entre otros (IBM, 2024). Por lo cual, es necesario reconocer las vulnerabilidades ante estas amenazas,

establecer estrategias y tecnologías que permitan en lo posible mitigar este tipo de ciberamenazas (Adu-Manu, 2023).

La técnica de phishing es el ataque de ingeniería social más común (ISACA, 2022), la cual tiene como objetivo, obtener de manera fraudulenta información personal o confidencial de una empresa o persona (Garzón Ibarra et al., 2024). Los atacantes utilizan sitios web falsos, correos electrónicos, anuncios, programas antivirus, scareware, sitios web de PayPal, premios y ofertas gratuitas para engañar a las víctimas y obtener información confidencial (Alzas Hernandez, 2023).

Con el fin de contrarrestar este tipo de ciberamenazas, el gobierno del Ecuador ha levantado la estrategia nacional de ciberseguridad. Esta estrategia es una herramienta fundamental para combatir los ciberataques continuos (Sagayo-Heredia, 2022). A la vez, busca impulsar otros desarrollos digitales como el comercio electrónico, la protección de la información, transacciones financieras, entre otras (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Así también, el 10 de mayo del año 2021, la Asamblea Nacional del Ecuador basado en el artículo 66, numeral 19 de la Constitución de la República del Ecuador, establece el derecho a la protección de datos de carácter personal. Con la Ley de Protección de Datos Personales, se busca generalmente cuidar la titularidad de los datos de los usuarios (Dirección Nacional de Registros Públicos, 2021).

Estas políticas aportan en la protección de información de los usuarios finales, apoyados por las tecnologías que en las entidades del Ecuador se utilizan para la protección ante ciberataques. Pero queda la incógnita, si estas técnicas y métodos, son realmente suficientes para mitigar riesgos de las ciberamenazas en nuestro entorno. En tal razón, se plantea la investigación sobre estrategias, patrones específicos y tecnologías efectivas para la protección contra ataques de ingeniería social en función de las siguientes preguntas:

¿Cómo la implementación de estrategias de seguridad, patrones de comportamiento y tecnologías específicas en comparación con la ausencia de estas medidas contribuye a la protección contra ataques de ingeniería social? Y ¿Cuál ha sido el impacto económico y operativo de los ataques de ingeniería social en el Ecuador y qué estrategias, leyes regulatorias y tecnologías existen o deberían implementarse para prevenir y mitigar eficazmente estas ciberamenazas?

En este sentido, el presente estudio se desarrolla bajo un modelo cualitativo, el cual se basa en entrevistas dirigidas a docentes investigadores, directivos de instituciones ecuatorianas y expertos en ciberseguridad. Los cuales fueron seleccionados mediante un método de muestreo aleatorio simple para la participación en dicho procedimiento. Las preguntas de la entrevista buscan responder directamente la pregunta de investigación, aprovechando el amplio conocimiento y experiencia de los entrevistados.

Metodología

Para el presente estudio, se adoptó un enfoque cualitativo basado en entrevistas dirigidas a docentes investigadores, directivos de instituciones ecuatorianas y expertos en ciberseguridad. Las preguntas de la entrevista se diseñaron en consonancia con los objetivos de la investigación, con el propósito de identificar estrategias y tecnologías efectivas para protegerse contra ataques de ingeniería social en el contexto ecuatoriano.

Asimismo, se utilizó un método de muestreo aleatorio simple para seleccionar a quince participantes. Inicialmente, los participantes fueron contactados por teléfono para confirmar su idoneidad, asegurando que poseían un conocimiento profundo y experiencia en tecnologías de la información y ciberseguridad, lo cual se corroboró mediante sus publicaciones de investigación en bases de datos científicos. Posteriormente, se les extendió una invitación formal, explicando el propósito del estudio y la naturaleza voluntaria de su participación. Todos los participantes otorgaron su consentimiento informado antes de las entrevistas.

Las entrevistas se realizaron a través de plataformas tecnológicas como Zoom y Google Meet. Las preguntas fueron estructuradas para abordar directamente el tema de investigación, aprovechando el amplio conocimiento y experiencia de los entrevistados. Se abordaron aspectos como las técnicas prevalentes de ataques de ingeniería social, factores que contribuyen a las vulnerabilidades de las instituciones en Ecuador, comparaciones con patrones internacionales, protocolos para evaluar vulnerabilidades, marcos legales, impacto económico y operativo de los ataques, respuestas institucionales, políticas de seguridad, tecnologías utilizadas, y desafíos futuros en la protección contra estos ataques. En este sentido las preguntas consideradas para la entrevista fueron las siguientes:

- ¿Conoce usted cuáles son las técnicas de ataques de ingeniería social más prevalecientes en las instituciones públicas y privadas en Ecuador?
- ¿Desde su perspectiva, qué factores contribuyen a las vulnerabilidades de las instituciones en el Ecuador frente a los ataques de ingeniería social?
- ¿Existen patrones específicos en los ataques de ingeniería social dirigidos a instituciones en Ecuador comparados con otros países?
- ¿Qué protocolos se deben seguir para evaluar las vulnerabilidades de las instituciones del Ecuador ante ataques de ingeniería social?
- ¿Qué marco legal y regulatorio existe en Ecuador para proteger a las instituciones contra los ataques de ingeniería social?
- ¿Cuál ha sido el impacto económico y operativo de los ataques de ingeniería social en las instituciones ecuatorianas?

- ¿Cómo han respondido las instituciones afectadas por ataques de ingeniería social y qué medidas han tomado para recuperarse?
- ¿Qué políticas de seguridad y estrategias utilizan o deben implementarse en las instituciones del Ecuador para prevenir los ataques de ingeniería social?
- ¿Qué tecnologías efectivas utilizan o deben implementarse en las instituciones en Ecuador para protegerse contra los ataques de ingeniería social?
- ¿Qué nuevos desafíos anticipa el ámbito de la ingeniería social y que mejoras deberían plantearse para fortalecer la protección contra este tipo de ataques?

El análisis de los datos se realizó mediante un análisis temático, que permitió identificar patrones, tendencias y temas clave en las respuestas de los entrevistados. Este método facilitó la organización y categorización de la información en torno a las estrategias y tecnologías de protección más efectivas contra ataques de ingeniería social. Además, los datos recolectados fueron comparados y contrastados entre los participantes, lo que permitió contextualizar los hallazgos dentro del marco teórico y práctico de la ciberseguridad en Ecuador.

Por último, para asegurar la confidencialidad y privacidad de los participantes, se implementó un protocolo estricto de manejo de datos. La invitación formal a participar en las entrevistas destacaba que toda la información proporcionada sería utilizada únicamente con fines investigativos.

Resultados

El planteamiento de los resultados se basan en la participación de quince participantes entre docentes investigadores, directivos de instituciones ecuatorianas y expertos en ciberseguridad destacados por su conocimiento y experticia en el tema de estudio, los cuales participaron de las entrevistas proporcionando respuestas detalladas a la primera y segunda pregunta de investigación, que busca entender cuáles son las técnicas de ingeniería social más prevalentes y los factores que contribuyen a las vulnerabilidades en las instituciones de Ecuador, así como comparar estos patrones con los observados en otros países.

¿Cuáles son las técnicas de ingeniería social más prevalentes y los factores que contribuyen a las vulnerabilidades en las instituciones del Ecuador, y cómo se comparan estos patrones con otros países?

Para abordar esta pregunta, se plantearon una serie de preguntas que fueron respondidas por los expertos, quienes proporcionaron información basada en su experiencia y conocimiento. Los cuales identificaron las técnicas de ingeniería social más comunes y los factores que contribuyen a las vulnerabilidades en el contexto ecuatoriano. Además, discutieron los patrones y elementos específicos que se están utilizando en los ciberataques en Ecuador, comparándolos con prácticas observadas en otros países.

Técnicas de ataque

La Tabla 1 resume los cinco principales tipos de ataques de ingeniería social: *phishing, spear phishing, pretexting, vishing y baiting*. Para cada tipo de ataque, se incluye una breve descripción y el número de entrevistados que reportaron los ataques frecuentes más comunes.

Tabla 1. Principales Ataques de Ingeniería Social

Nro.	Tipo	Descripción	Entrevistados coincidentes
1	Phishing	Los atacantes envían correos electrónicos que parecen legítimos para engañar a los usuarios y que revelen información confidencial, como credenciales de inicio de sesión o datos financieros. Usan técnicas como la suplantación de dominio para hacer que el correo electrónico parezca auténtico.	12
2	Spear Phishing	A diferencia del *phishing* general, el *spear phishing* está dirigido a individuos específicos o a un grupo dentro de una organización, utilizando información personal para hacer el ataque más convincente.	2
3	Pretexting	Aquí, los atacantes crean una historia convincente o una identidad falsa para obtener información. Por ejemplo, pueden presentarse como un auditor que necesita acceso a datos específicos para realizar una supuesta revisión.	2
4	Vishing	Esta técnica utiliza llamadas telefónicas para engañar a las personas, a menudo haciéndose pasar por personal de soporte técnico o por alguien con autoridad para obtener información sensible o realizar transacciones fraudulentas.	3
5	Baiting	En esta técnica, los atacantes ofrecen algo que parece atractivo, como un software gratuito, que en realidad contiene malware. La víctima lo descarga y lo instala, lo que permite a los atacantes comprometer su sistema.	2

Fuente: elaboración propia basada en las respuestas de los participantes

Los resultados que los participantes reflejan en sus entrevistas indican que, la principal y predominante técnica de ataque ingeniería social en el Ecuador es el Phishing. Por otra parte, el investigador Sang Guun Yoo argumenta otra técnica de ataque de ingeniería social.

- **Whaling:** Es un método con objetivos más específicos que el Spear Phising normalmente con cargos muy importantes en las organizaciones.

En la Tabla 2 el docente investigador Pablo Andrés Landeta de la Universidad Técnica del Norte argumenta tres técnicas adicionales de ataques de ingeniería social: Smishing, Quid pro quo y Tailgating. Para cada tipo de ataque, se incluye una breve descripción de acuerdo con la metodología de ataque.

Tabla 2. Otros tipos de ataques de Ingeniería Social.

Nro.	Tipo	Descripción
1	Smishing	Esta técnica utiliza la ejecución de un ataque *phishing* a través de SMS.
2	Quid pro quo	Este tipo de ataque ofrece un servicio falso a cambio de información.
3	Tailgating	En esta técnica se busca seguir a alguien autorizado para acceder a áreas restringidas.

Fuente: elaboración propia basada en las respuestas de los participantes

Factores de vulnerabilidad

Los resultados que los entrevistados reflejan en sus argumentos que, el principal factor que contribuye a las vulnerabilidades frente a los ataques de ingeniería social es el Desconocimiento y la Falta de Capacitación (quince participantes).

Los profesionales Sang Guun Yoo y Gonzalo Gabriel Bonilla concuerdan que la obsoleta infraestructura tecnológica, los sistemas de seguridad desactualizados en las instituciones del Ecuador son factores que lastimosamente aumentan las vulnerabilidades ante los ciberataques en las entidades ecuatorianas. A esto, los docentes investigadores de la UTN, Pablo Andrés Landeta y Daysi Elizabeth Imbaquingo argumentan que, las limitantes presupuestarias de las instituciones ecuatorianas y la cultura organizacional de varias entidades consideran que la ciberseguridad no es una prioridad por lo cual no se promueve una cultura de seguridad, lo que aumenta el riesgo de ataques exitosos de ingeniería social.

El investigador Sang Guun Yoo finalmente argumenta que, el manejo público de información personal y profesional que se comparte en redes sociales y otros canales públicos proporciona a los atacantes material valioso para diseñar ataques de ingeniería social más personalizados y efectivos.

Patrones específicos

Los resultados de los entrevistados (doce participantes) indican que, existen patrones específicos en los ataques de ingeniería social en el país. El investigador Sang Guun Yoo menciona que, la existencia de los patrones de ataques de ingeniería social en el Ecuador está estrictamente especificada de acuerdo con el ámbito al cual están dirigidos esto es:

- Entidades Financieras: Los ataques a instituciones financieras son comunes, utilizando técnicas como el phishing para obtener credenciales bancarias o realizar transferencias fraudulentas.
- Empresas de Tecnología: Las empresas de tecnología son objetivo frecuente debido a la información sensible y los sistemas críticos que manejan. Los atacantes a menudo utilizan spear phishing para infiltrarse en las redes empresariales.

- Organizaciones Públicas: Los atacantes a menudo se hacen pasar por autoridades gubernamentales o entidades reguladoras para obtener acceso a datos o realizar manipulaciones.

Comparativa internacional

Los participantes Sang Guun Yoo y Roberto Omar Andrade argumentan que, comparado con otros países en el Ecuador los ataques tienden a aprovechar más las referencias locales y eventos nacionales para hacer los engaños más creíbles. Es decir que, los ciberataques de phishing se adaptan al tema de nuestra realidad y entorno ecuatoriano. En otros países, los ataques suelen ser distintos, más globales y menos personalizados lo cual se distingue con nuestro entorno.

Protocolos de evaluación

Aunque trece de los participantes en las entrevistas coincidieron que, los protocolos de evaluación ante ataques de ingeniería social son indistintos tales como la evaluación de concienciación del personal, simulaciones de ataques controlados, revisión de políticas y procedimientos, evaluación de seguridad física, desarrollo de plan de mitigación, entre otros. Los investigadores Sang Guun Yoo y Roberto Omar Andrade en sus entrevistas coinciden que, para evaluar las vulnerabilidades se deben seguir varios protocolos.

La Tabla 3 identifica los principales protocolos de evaluación que deben tomarse en cuenta para valorar las vulnerabilidades ante ataques de ingeniería social, los mismos que están definidos por su respectivo protocolo y descripción.

Tabla 3. Protocolos de evaluación

Nro	Protocolo	Descripción
1	Evaluación de Riesgos	- Análisis de Amenazas: Identificar y analizar posibles amenazas específicas a la organización, incluyendo técnicas de ingeniería social. - Evaluación de Impacto: Evaluar el impacto potencial de un ataque de ingeniería social en la organización, considerando tanto el impacto financiero como el daño a la reputación.
2	Pruebas de Penetración y Simulaciones	- Simulaciones de Ataques: Realizar simulaciones de *phishing, vishing* y otras técnicas de ingeniería social para evaluar la capacidad de respuesta del personal. - Pruebas de Penetración: Ejecutar pruebas de penetración enfocadas en técnicas de ingeniería social para identificar debilidades en la seguridad humana.
3	Revisión de Políticas y Procedimientos	- Auditoría de Políticas: Revisar y actualizar las políticas de seguridad para asegurarse de que incluyan procedimientos para manejar solicitudes sospechosas y verificar identidades. - Procedimientos de Respuesta: Evaluar y mejorar los procedimientos de respuesta a incidentes relacionados con ingeniería social.
4	Plan de Capacitación y Sensibilización	Formación Regular: Implementar programas de capacitación y concienciación continua sobre ciberseguridad para mantener al personal informado sobre nuevas amenazas.

Fuente: elaboración propia basada en las respuestas de los participantes

Para complementar la investigación, los entrevistados participaron respondiendo a la segunda pregunta de investigación que tiene como objetivo conocer:

¿Cuál ha sido el impacto económico y operativo de los ataques de ingeniería social en el Ecuador y qué estrategias, leyes regulatorias y tecnologías existen o deberían implementarse para prevenir y mitigar eficazmente estas ciberamenazas?

Para responder a esta incógnita de investigación se ha planteado varias preguntas que el personal entrevistado ha argumentado de acuerdo con su experticia y conocimiento las cuales han acertado sobre las estrategias, marco legal y tecnologías que en el entorno ecuatoriano están siendo implementadas o deben implementarse para mitigar este tipo de ciberataques.

Marco legal y regulatorio

Los quince entrevistados coincidieron que, en el Ecuador existe el marco legal y regulatorio para proteger a las instituciones contra los ataques de ingeniería social. Este marco legal se sustenta en diversas leyes y normativas que abordan la temática de la ciberseguridad y la protección de datos.

La Tabla 4 detalla el marco legal y regulatorio existente en el Ecuador para aportar a la protección ante ataques de ingeniería social. Para cada normativa, se incluye una breve descripción de la norma que establece cada ley regulatoria.

Tabla 4. Marco legal y regulatorio

Nro.	Marco Legal	Descripción
1	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.	Esta ley establece el marco jurídico para las transacciones electrónicas, el uso de firmas electrónicas y la validez legal de los mensajes de datos. Aunque su enfoque principal no es la ciberseguridad, establece bases importantes para la autenticación y la integridad de la información (Asamblea Nacional del Ecuador, 2021).
2	Código Orgánico Integral Penal (COIP)	Delitos Informáticos: El COIP tipifica una serie de delitos relacionados con la informática, incluyendo el acceso no autorizado a sistemas informáticos, la interceptación de datos, el sabotaje informático, y el fraude electrónico. Estas disposiciones son relevantes para sancionar actividades relacionadas con la ingeniería social (Asamblea Nacional del Ecuador, 2021).
3	Ley Orgánica de Protección de Datos Personales (LOPDP)	Esta ley, promulgada en 2021, establece los derechos de los ciudadanos sobre sus datos personales y las obligaciones de las entidades que manejan dicha información. Incluye disposiciones sobre el consentimiento, la transparencia, y la seguridad de los datos, que son fundamentales para prevenir ataques de ingeniería social (Asamblea Nacional del Ecuador, 2021).

Fuente: eelaboración propia basada en las respuestas de las participantes fundamentadas en el marco legal ecuatoriano

Impactos

Los entrevistados (quince participantes) argumentaron que el impacto económico y operativo de las instituciones en el Ecuador ante ataques de ingeniería social ha sido muy considerable.

La Tabla 5 es un resumen de los impactos que ha generado los ataques de ingeniería social en el entorno ecuatoriano de acuerdo con cada impacto desarrollado. Aquí se incluye una breve descripción de las repercusiones que han generado los impactos que producidos por este tipo de ciberataque.

Tabla 5. Impactos

Nro.	Impacto	Descripción
1	Impacto Económico	- Costos de Recuperación: Incluye gastos asociados con la remediación del ataque, como la reparación de sistemas, recuperación de datos y, en algunos casos, pagos de rescate. - Multas y Sanciones: Las organizaciones pueden enfrentar multas por incumplimiento de regulaciones de protección de datos si no toman medidas adecuadas para proteger la información.
2	Impacto Operativo	- Interrupción de Servicios: Los ataques pueden interrumpir operaciones normales, afectando la productividad y causando tiempos de inactividad. - Daño a la Reputación: La pérdida de confianza de clientes y socios puede tener un impacto a largo plazo en la reputación de la organización y en su capacidad para hacer negocios.
3	Impacto en la Moral del Personal	Confusión y Desconfianza: Los ataques pueden generar confusión y desconfianza dentro de la organización, afectando la moral y la efectividad del personal

Fuente: elaboración propia basada en las respuestas de los participantes

Estrategias de seguridad

Los docentes Marco Remigio Pusdá Chulde y Pablo Pablo Andrés Landeta y los expertos en ciberseguridad Javier Vaca Valencia y Edwin Guevara Castillo, argumentaron estrategias de seguridad específicas para la protección ante ataques de ingeniería social

La Tabla 6 es un resumen de las estrategias de seguridad que han aportado los participantes. Aquí se incluye una breve descripción de las estrategias que pueden ayudar a mitigar este tipo de ciberataque.

Tabla 6. Estrategias de seguridad

Nro.	Estrategia	Descripción
1	Capacitación y Concienciación	- Programas de Formación: Implementar programas de formación y concienciación continua sobre ciberseguridad y técnicas de ingeniería social que incluyan simulaciones de ataques reales para promover una cultura de seguridad en los usuarios. - Simulaciones de ataques realistas: Herramientas para realizar simulaciones de ciberataques que permitan evaluar y mejorar la capacidad de respuesta del personal.
2	Revisión de Procedimientos	- Políticas de Verificación: Establecer procedimientos estrictos para verificar la autenticidad de las solicitudes de información o acceso. - Actualización constante de Procedimientos: Revisar y actualizar las políticas de seguridad regularmente para reflejar las últimas amenazas y técnicas de ingeniería social. - Protocolos de Respuesta a Incidentes: Desarrollar y validar protocolos de respuesta a incidentes específicos monitoreando su efectividad ante las ciberamenazas constantes.
3	Colaboración y Comunicación	- Colaboración con Expertos: Trabajar con expertos en ciberseguridad y participar en redes de intercambio de información sobre amenazas. - Transparencia: Informar de manera transparente sobre incidentes de seguridad y las medidas tomadas para prevenir futuros ataques.

Fuente: elaboración propia basada en las respuestas de los participantes

Tecnologías efectivas

Los expertos en Ciberseguridad Sang Guun Yoo y Rolando Ortiz Valencia de acuerdo con su experticia aportaron con distintas tecnologías actuales implementadas o que deberían implementarse para una protección eficaz ante ataques de ingeniería social.

La Tabla 7 es un resumen de las tecnologías efectivas utilizables para mitigar el riesgo de ciberamenazas. Aquí se incluye una breve descripción del tipo de tecnologías que pueden utilizarse para mitigar este tipo de ciberataque.

Tabla 7. Tecnologías efectivas

Nro.	Tecnología	Descripción
1	Soluciones de Seguridad de Correo Electrónico	- Filtros de Spam y Phishing: Tecnologías que utilizan análisis heurístico y machine learning para identificar y bloquear correos electrónicos maliciosos. - Antivirus XDR y AntiSpam. - Firewalls avanzados.
2	Sistemas de Gestión de Identidades y Accesos (IAM)	- Autenticación Multifactorial (MFA): Implementación de MFA para asegurar el acceso a sistemas críticos. - Monitoreo de Acceso: Soluciones que apliquen el principio de mínimo privilegio y que supervisen regularmente los accesos para detectar actividades y vulnerabilidades sospechosas antes de ser explotadas. - Sistemas de Monitoreo Detección y Prevención de Intrusiones (IDS/IPS) para identificar y prevenir no autorizados. - Sistemas de Información y Gestión de Eventos de Seguridad (SIEM) para el fortalecimiento de la seguridad tecnológica.
3	Tecnologías de Detección de Amenazas	- Inteligencia Artificial y Machine Learning: Soluciones que utilizan IA para identificar patrones de comportamiento anómalos y detectar ataques de ingeniería social en tiempo real.

Fuente: elaboración propia basada en las respuestas de los participantes

Nuevos desafíos

Finalmente, los profesionales Roberto Omar Andrade Paredes y Sang Guun Yoo coinciden que, los nuevos desafíos para protección de ataques de ingeniería social se centran en hacer uso de estrategias y tendencias de tecnologías del futuro.

La Tabla 8 presenta un resumen de las nuevas tecnologías que involucra a la ingeniería social. Aquí se incluye un breve detalle de los desafíos que deben ser tomados en cuenta en este tipo de ciberataques.

Tabla 8. Desafíos futuros

Nro.	Desafíos	Descripción
1	Inteligencia Artificial en Ataques	Personalización de Ataques: La IA puede crear ataques altamente personalizados y difíciles de detectar. Esto incluye la generación de correos electrónicos y mensajes adaptados a las características individuales de las víctimas.
2	Deepfakes	Engaños Visuales: La tecnología de *deepfake* puede ser utilizada para crear videos falsos de figuras de autoridad que solicitan acciones urgentes o confidenciales, haciéndolos más persuasivos.
3	Aumento del Trabajo Remoto	Seguridad en Entornos Descentralizados: El trabajo remoto expone nuevas vulnerabilidades, especialmente si los empleados usan dispositivos personales o redes inseguras para acceder a la red corporativa por lo cual es necesario implementar políticas y tecnologías que aseguren que los dispositivos y acceso a redes institucionales estén protegidas.

Fuente: elaboración propia basada en las respuestas de los participantes

Discusión

Los resultados de investigaciones confirman que, el Phishing es la técnica de ingeniería social más utilizada en Ecuador. Esto se puede evidenciar con investigaciones que subrayan la vulnerabilidad ante ataques de esta naturaleza.

Por ejemplo, Sancho et al. (2023), documentaron un ataque de phishing dirigido a 83 estudiantes del Instituto Superior Tecnológico Huaquillas. En este caso, los atacantes utilizaron un correo electrónico de suplantación de identidad de un Centro de Idiomas con el asunto "Certificaciones A1-A2 en inglés". En este correo electrónico, se solicitaba llenar un formulario de Google con información confidencial. De los estudiantes, 12 fueron víctimas de dicha técnica, y de este grupo, 10 personas proporcionaron el número de teléfono, lo cual permitió enviar un mensaje malicioso a través de WhatsApp. Como resultado, lograron obtener las credenciales de 2 estudiantes, permitiendo acceder a los correos de los estudiantes afectados.

En otro estudio, Prado Díaz (2021), identificó ataques de ingeniería social, Phishing, Spoofing, Vishing realizados a la empresa Omnidata. En este caso, los ataques se dirigieron al personal de la institución mediante la suplantación de identidad del portal web empresarial, esto con el fin de obtener credenciales de acceso de los empleados y comprometer la confidencialidad de la información de la empresa.

En los dos casos de investigación, los autores resaltan la necesidad de implementar políticas de seguridad que permitan mitigar considerablemente los riesgos de ataques de ingeniería social. Las investigaciones coinciden con este estudio con la necesidad de implementar políticas de seguridad, campañas de concientización y capacitación al personal sobre el riesgo de estas ciberamenazas. Adicional a esto, de fortalecer el entorno tecnológico con herramientas avanzadas como Firewalls, Antivirus XDR, AntiSpam, MFA, y sistemas IDS/IPS, para mitigar los ciberataques.

Conclusión

En la investigación de protección contra ataques de ingeniería social políticas y estrategias se pudo concluir que:

La técnica de ataque de ingeniería social más preponderante es el Phishing esto aprovechado por las principales vulnerabilidades como el desconocimiento y falta de capacitación que hacen de las entidades del Ecuador un objetivo de ataque vulnerable para los ciberataques.

Aunque existe un marco legal y regulatorio que identifica leyes como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código integral, Código Orgánico Integral Penal (COIP) y Ley Orgánica de Protección de Datos Personales (LOPDP), las instituciones en Ecuador continúan siendo vulnerables a las ciberamenazas. Estas amenazas generan impactos significativos que afectan la moral, la economía y las operaciones de las organizaciones ecuatorianas.

Por lo cual la aplicación de estrategias de protección como la implementación de políticas de seguridad, capacitaciones de concientización, actualización continua de las ciberamenazas más recientes por parte del personal de Tics de cada entidad, al igual que buscar la cooperación de expertos en ciberseguridad ayudarán a mitigar los riesgos ante las ciberamenazas.

Así también, es necesario hacer uso de tecnologías avanzadas como Firewalls Avanzados, Antivirus XDR, AntiSpam, autenticación multifactorial (MFA) y Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) para mitigar eficazmente los riesgos ante ataques de ingeniería social.

Para futuras investigaciones los nuevos desafíos de protección contra ataques de ingeniería social se centran en hacer uso de las herramientas de inteligencia artificial que permitan la rápida detección de estas ciberamenazas y el pronto accionar por parte de las tecnologías utilizadas para la mitigación de estos riesgos cibernéticos.

Agradecimientos

La investigación de protección contra ataques de ingeniería social: análisis cualitativo de estrategias, tecnologías y patrones específicos, fue posible realizarla gracias a la participación de las entrevistas de varios docentes investigadores, directivos de instituciones del Ecuador y expertos en ciberseguridad, quienes con su conocimiento y experticia aportaron al desarrollo de la investigación.

La Tabla 9 proporciona un resumen detallado de los participantes en las entrevistas del estudio, destacando sus respectivos perfiles profesionales.

Tabla 9. Participantes de las entrevistas

Nro.	Participantes	Perfil profesional
1	Ph.D. Sang Guun Yoo	Experto en Ciberseguridad
2	Mgs. Roberto Omar Andrade Paredes	Experto en Ciberseguridad
3	Mgs. Pablo Andrés Landeta López	Docente Investigador Universidad Técnica del Norte
4	Mgs. Marco Remigio Pusdá Chulde	Docente Investigador Universidad Técnica del Norte
5	Ing. Alvaro Guerrero	Docente Investigador
6	Ing. Kevin Adrian Naranjo Flores	Profesional de Tics
7	Ing. Marco Benjamín Tocagón Tocagón	Gerente propietario Cobernet
8	Mgs. Patricia Lorena Chandi Andrango	Docente Investigador MINEDUC
9	Ing. Vicente Javier Vaca Valencia	Experto en Ciberseguridad
10	Ing. Gonzalo Gabriel Bonilla Bravo	Experto en Seguridad Informática
11	Ing. Sandra Ximena Chandi Andrango	Gerente de Sucursal Banco Produbanco
12	Ing. Jhoana Cristina Campaña Flores	Profesional de Tics
13	Ing. Edwin Guevara Castillo	Experto en Ciberseguridad
14	Mgs. Rolando Ortiz Valencia	Experto en Ciberseguridad
15	Mgs. Daisy Elizabeth Imbaquingo Esparza	Subdecana FICA Universidad Técnica del Norte

Fuente: elaboración propia basada en las respuestas de los participantes

Referencias

Adu-Manu, K. S. (2023). Phishing Attacks in Social Engineering: A Review. *Journal of Cyber Security, 4*(4), 243-245. https://doi.org/http://dx.doi.org/10.32604/jcs.2023.041095

Agudelo, A. (2013, 24 de noviembre). Los ciberataques con ingeniería social marcarán el 2024. Play Marketing América. https://lc.cx/Dvjooz

Alzas Hernandez, J. (2023). *Estudio de fraudes basados en la técnica de Ingeniería Social* [Tesis de licenciatura, Universitat Oberta de Catalunya]. http://hdl.handle.net/10609/148147

Asamblea Nacional del Ecuador. (2021, 26 de mayo). Quinto Suplemento del Registro Oficial No.459. https://lc.cx/Q6HTgv

Asamblea Nacional del Ecuador. (2021). *Defensoría Pública del Ecuador.* http://biblioteca.defensoria.gob.ec/handle/37000/3374

Asamblea Nacional del Ecuador. (2021). *Ministerio de Defensa Nacional del Ecuador.*

El Comercio. (2024, 16 de septiembre). Smishing, Vishing y Spooging, los delincuentes informáticos y sus formas de ataque. https://lc.cx/cw81Rw

Dirección Nacional de Registros Públicos. (2021, 26 de mayo). Registros Públicos. https://lc.cx/ulCP-b

Garzón Ibarra, C. S., Navas Tapia, C. A., Illicachi Tene, A. M., Espinoza Toapanta, R. J., & Estrella Ormaza, G. S. (2024). Análisis de los ataques de ingeniería social en Ecuador. *Ciencia Latina Internacional, 8*(1), 4364-4365. https://doi.org/https://doi.org/10.37811/cl_rcm.v8i1.9777

Harán, J. M. (2021, 14 de octubre). Banco Pichincha sufrió ataque informático que afectó parte de sus servicios. Comunidad de Seguridad de ESET. https://lc.cx/fZGuvi

IBM. (2024, 22 de julio). ¿Qué es la ingeniería social? IBM. https://lc.cx/wcymiT

ISACA. (2022, 23 de marzo). Download the State of Cybersecurity 2022 Report. *2022.* https://www.isaca.org/resources/reports/state-of-cybersecurity-2022

Kaspersky Team. (2024, 26 de agosto de 2024). Los ataques contra celulares crecen un 70%, lo que marca un récord en América Latina. Kaspersky Daily. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2024/27591/

Meza, J., Cedeño, E., Zambrano, M., Zambrano, W., & Zambrano, D. (2024). Social engineering: Methodologies to counter computer attacks on the web. Case: Barrio 26 de Septiembre, Portoviejo, Ecuador. *AIP Conference Proceedings, 2994*(1). https://doi.org/10.1063/5.0188636

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de ciberseguridad.* https://lc.cx/21yiff

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (5 de Agosto de 2022). *Mintel.* Mintel: https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

Naranjo Godoy, L. (2024, 16 de septiembre). Por primera vez Ecuador cuenta con su Estrategia Nacional de Ciberseguridad. https://lc.cx/09oVrG

Prado Díaz, J. P. (2021). Ingeniería social, un ejemplo práctico. *Revista Odigos, 2*(3), 71-72. https://doi.org/https://doi.org/10.35290/ro.v2n3.2021.493

Sancho, C., Alejandro, J., Herrera, J., Machuca, S., & Cuadros, P. (2023). Análisis del uso de las técnicas de ingeniería social caso de estudio: Instituto Superior Tecnológico Huaquillas–Ecuador. *Ciencia Latina Revista Científica Multidisciplinar, 7*(1), 11475-11476. https://doi.org/https://doi.org/10.37811/cl_rcm.v7i2.5696

Sosa, P. (2023, 05 de diciembre). *Los ciberataques con ingeniería social marcarán el 2024.* Sr Radio.

Torres, A. (2022, 07 de marzo). Exagente de la Senain investigado por hackeos a más de 50 entidades. Primicias. https://lc.cx/1P1FnC

Vega, J. (2023, 04 de diciembre). Los ciberataques con ingeniería social marcarán el 2024. PrensaEC. https://lc.cx/

Autores

Edison Andrés Fueres Quilumbango. Profesional con una sólida formación en sistemas informáticos y ciberseguridad, con experiencia en desarrollo de software, administración del sistema médico MIS-AS400 y soporte técnico a unidades médicas del IESS. Es estudiante de la Maestría en Ciberseguridad de la Universidad Católica de Cuenca y Licenciado en Ingeniería de Sistemas Computacionales de la Universidad Técnica del Norte.

Roberto Omar Andrade Paredes. Profesor e investigador de la Universidad Católica de Cuenca.

Marco Vinicio Yamba Yugsi. Candidato a Doctor en Ciencias Experimentales y Tecnología por la UVic | Universitat de Vic–Universitat Central de Catalunya. Máster en Diseño Multimedia por la Universidad del Azuay con amplia experiencia en educación superior: desde 2019 hasta la actualidad se desempeña como Coordinador Técnico en posgrado en la Universidad Católica de Cuenca. Anteriormente, del 2014 al 2017 como Tutor Externo en Proyectos de Tesis en el Instituto Universitario Cordillera. De 2009 a 2011 como docente en desarrollo web, multimedia y TIC en el Instituto Tecnológico Latino.

Declaración

Conflicto de interés
No tenemos ningún conflicto de interés que declarar.
Financiamiento
Sin ayuda financiera de partes externas a este artículo.
Nota
El artículo es original y no ha sido publicado previamente.