



**UNIVERSIDAD
CATÓLICA DE CUENCA**

POSGRADO

MAESTRÍA EN CIBERSEGURIDAD

**Informe de Investigación previo a la obtención del título de Magíster en
Ciberseguridad**

Tema: Perspectivas actuales en ataques de Ingeniería social: Una
revisión sistemática de la literatura científica

Autor: Adriana Ortiz

Tutor: Ing. Miguel Andrade López Mg.

Cuenca – Ecuador

2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Perspectivas actuales en ataques de Ingeniería social: Una revisión sistemática de la literatura científica”, de autoría de la Señorita Ingeniera en Electrónica y Telecomunicaciones Daysi Adriana Ortiz Casillas, CC: 1722756101, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.

Ing. Miguel Andrade López. Mg
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Perspectivas actuales en ataques de Ingeniería social: Una revisión sistemática de la literatura científica”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024.



Ing. Daysi Adriana Ortiz Casillas

CC: 1722756101

Agradecimiento

Quiero agradecer a mi familia por su apoyo y su respaldo. Agradezco especialmente a mi hermano que es la persona que me motivó a seguir preparándome y dar un paso más en mi vida profesional.

Agradezco a las personas que estuvieron a mi alrededor que supieron alentarme a no rendirme y a seguir adelante, gracias por sus buenos deseos.

Estoy totalmente agradecida con todas las personas que formaron parte de esta experiencia, ya que han sido pilares fundamentales en este logro académico.

Dedicatoria

A mi familia, por su apoyo constante, gracias por darme la fuerza necesaria para seguir adelante.

A mis amigos, colegas y compañeros por sus consejos y ánimos, su amistad ha sido invaluable en los momentos difíciles.

A mi tutor de tesis, por su tutela, su paciencia y tiempo, y que gracias a su conocimiento se logró alcanzar el objetivo.

Y, por último, gracias a todas las personas que con su respaldo me ayudaron a llegar tan lejos.

Resumen

Las tendencias en los ataques de ingeniería social han mostrado una evolución significativa en los últimos años, caracterizándose por un incremento en la sofisticación de las tácticas utilizadas por los atacantes. Estos actores malintencionados han aprendido a personalizar sus ataques, utilizando información personal altamente específica para generar una mayor probabilidad de éxito. Esta personalización es clave para engañar a las víctimas, quienes muchas veces no logran identificar la amenaza debido al grado de detalle que los ataques presentan. En este estudio, se ofrece una visión integral y comparativa de cómo se manifiestan los ataques de ingeniería social. El objetivo es proporcionar un análisis detallado que permita comprender la evolución de estos métodos de ataque y las tácticas que los acompañan. Al identificar los diferentes tipos de ataques, como el phishing y sus variantes, así como la suplantación de identidad, es posible entender cómo operan en sectores críticos como el financiero, académico y de infraestructura tecnológica. Entre los medios más utilizados para ejecutar estos ataques destacan el correo electrónico, las redes sociales y los sitios web fraudulentos. Los atacantes envían mensajes cuidadosamente elaborados para engañar a los usuarios y obtener acceso a información confidencial, como credenciales de acceso o datos financieros. En muchos casos, las víctimas no reconocen los indicadores de un ataque, lo que subraya la importancia de la educación y la concientización como parte de una estrategia de defensa. Las organizaciones deben mantenerse actualizadas sobre las técnicas empleadas por los atacantes, fortalecer sus políticas de seguridad y promover una cultura de ciberseguridad entre sus empleados y usuarios.

Palabras clave: Ingeniería social, phishing, suplantación de identidad, correo electrónico, redes sociales, sitios web fraudulentos, mitigación de riesgos

Abstract

Social engineering attack trends have shown significant evolution in recent years, characterized by an increase in the sophistication of tactics used by attackers. These malicious actors have learned to personalize their attacks, using highly specific personal information to increase the likelihood of success. This personalization is key to deceiving victims, who often fail to recognize the threat due to the level of detail the attacks present. This study offers a comprehensive and comparative view of how social engineering attacks manifest. The goal is to provide a detailed analysis that allows for a deeper understanding of the evolution of these attack methods and their accompanying tactics. By identifying different types of attacks, such as phishing and its variants, as well as identity theft, it is possible to understand how they operate in critical sectors such as finance, academia, and technological infrastructure. Among the most commonly used methods for executing these attacks are email, social media, and fraudulent websites. Attackers send carefully crafted messages to deceive users and gain access to sensitive information, such as login credentials or financial data. In many cases, victims fail to recognize the signs of an attack, highlighting the importance of education and awareness as part of a defense strategy. Organizations must stay updated on the techniques employed by attackers, strengthen their security policies, and promote a culture of cybersecurity among their employees and users.

Keywords: Social engineering, phishing, identity theft, email, social media, fraudulent websites, risk mitigation.

Índice de contenido

1.	Capítulo I: Introducción.....	1
1.1.	Situación problemática	1
1.2.	Problema científico.....	3
1.3.	Línea de investigación	4
1.4.	Objeto de estudio	5
1.5.	Campo de acción	6
1.6.	Objetivos.....	7
1.6.1.	General	7
1.6.2.	Específicos	8
1.6.3.	Problema científico	8
1.7.	Hipótesis	9
1.8.	Variables.....	9
1.9.	Justificación	9
1.10.	Estado del arte o antecedentes	11
1.11.	Marco teórico.....	13
1.11.1.	Antecedentes	13
1.11.2.	Historia y evolución de la ingeniería social	15
1.11.3.	Ingeniería social	21

1.11.4. Tipos de ataques de ingeniería social	25
1.11.5. Herramientas y tecnologías utilizadas en ingeniería social.....	33
1.11.6. Protocolos y políticas de seguridad.....	36
1.11.7. Normativas y Estándares.....	38
2. Capítulo II: Diagnóstico situacional	44
2.1. Metodología.....	44
2.2. Análisis situacional.....	46
2.3. Análisis comparativo	47
3. Capítulo III: Propuesta.....	48
3.1. Diagrama de PRISMA.....	53
3.2. Identificación de temas clave	56
3.3. Comparación de casos de estudio.....	57
3.4. Evaluación de tendencias emergentes	61
3.5. Estrategias propuestas para mitigar ataques de ingeniería social	63
Conclusiones	65
Recomendaciones	67
Bibliografía	69

Índice de tablas

Tabla 1 Línea de investigación	4
Tabla 2 Matriz de recolección de información sobre ataques de Ingeniería social	48
Tabla 3 Identificación de temas clave.....	56
Tabla 4 Comparación de casos de estudio	59
Tabla 5 Comparación de casos de estudio	64

Índice de graficas

Gráfica 1 Diagrama PRISMA.....	55
---------------------------------------	----

1. Capítulo I: Introducción

1.1. Situación problemática

La ingeniería social se ha convertido en una amenaza creciente en el ámbito de la ciberseguridad, desencadenando ataques cada vez más sofisticados y perjudiciales. Este tipo de ataques se basa en técnicas que utilizan los ciberdelincuentes para manipular a las personas y conseguir información confidencial o acceder a sistemas protegidos (Santiago et al., 2024).

Los actores malintencionados emplean tácticas persuasivas como el phishing, el smishing y el vishing para engañar a las víctimas y comprometer la seguridad de organizaciones y usuarios. El phishing consiste en enviar correos electrónicos fraudulentos que parecen ser de fuentes confiables para obtener información sensible. Estos correos suelen contener enlaces o archivos adjuntos maliciosos diseñados para capturar credenciales de acceso o instalar software dañino en los dispositivos de las víctimas.

El smishing, por su parte, utiliza mensajes de texto para lograr el mismo objetivo, aprovechando la tendencia de las personas a confiar en la aparente simplicidad y seguridad de los SMS. El vishing recurre a llamadas telefónicas, donde los ciberdelincuentes se hacen pasar por representantes de instituciones legítimas para persuadir a las víctimas de que proporcionen datos personales o financieros.

El principal objetivo de los ciberdelincuentes es aprovechar las vulnerabilidades humanas, como la confianza, la prisa o el desconocimiento, para realizar los ataques. Los humanos tienden a confiar en comunicaciones que parecen auténticas y, en muchos casos, actúan impulsivamente sin verificar la autenticidad de las solicitudes. Esta confianza puede ser explotada para obtener acceso a información sensible, lo que puede resultar en la pérdida de datos confidenciales, el robo de dinero o incluso el chantaje (Gómez, 2020).

Los ataques de ingeniería social han evolucionado, adaptándose a las nuevas tecnologías y aprovechando la interconexión digital. Con el auge del teletrabajo, los ciberdelincuentes han intensificado sus esfuerzos, explotando la falta de conciencia de seguridad de los empleados remotos. La falta de una supervisión directa y el uso de redes domésticas menos seguras aumentan las oportunidades para los atacantes.

El cambio hacia el teletrabajo ha creado un entorno propicio para los ataques de ingeniería social. Los empleados que trabajan desde casa a menudo no cuentan con las mismas medidas de seguridad que en una oficina corporativa, y pueden ser más susceptibles a ataques debido a la falta de entrenamiento y supervisión en tiempo real. Además, la presión de mantener la productividad puede llevar a los empleados a tomar atajos, como no verificar la autenticidad de los correos electrónicos o enlaces que reciben.

La proliferación de plataformas de redes sociales ha ampliado el campo de juego, permitiendo a los atacantes recopilar información personal para personalizar sus estrategias de engaño. A través de estas plataformas, los ciberdelincuentes pueden obtener datos sobre los intereses, relaciones y actividades de las víctimas, creando ataques más creíbles y efectivos. La información recopilada de perfiles de redes sociales puede incluir detalles como fechas de nacimiento, direcciones de correo electrónico, nombres de familiares y amigos, y otras informaciones personales que pueden ser utilizadas para construir ataques más convincentes.

La ingeniería social representa una amenaza significativa en la ciberseguridad actual, ya que se centra en el factor humano, que a menudo es el eslabón más débil en la cadena de seguridad. La creciente sofisticación de estos ataques y su adaptación a las nuevas tecnologías y modalidades de trabajo subraya la necesidad urgente de mejorar la conciencia y las prácticas de seguridad entre los usuarios y las organizaciones.

Las consecuencias de los ataques de ingeniería social pueden ser devastadoras, tanto a nivel personal como corporativo. Las organizaciones pueden sufrir pérdidas financieras significativas, daños a la reputación y la exposición de información confidencial. Por ello, es crucial que se implementen programas de capacitación en seguridad cibernética, políticas estrictas de manejo de información y tecnologías avanzadas de detección y prevención de amenazas para mitigar el riesgo de estos ataques.

1.2. Problema científico

Los ataques de ingeniería social aprovechan la psicología humana y la susceptibilidad a la manipulación para engañar a las víctimas y obtener acceso a información confidencial. La falta de cultura de ciberseguridad, especialmente entre los empleados, los convierte en el eslabón más débil de la defensa organizativa (Basto- García, 2020).

Usualmente, estos ataques identifican las debilidades de individuos a través de conversaciones o seguimientos. Después de conocer a la víctima, el atacante la manipula utilizando diversas técnicas, también emplean tácticas presenciales no ofensivas (seguimiento y búsqueda de información en agendas o basura) y agresivas (chantaje, suplantación de identidad, manipulación psicológica) (Peña-Pérez, 2020).

De acuerdo a ESET (2023), a escala mundial, Ecuador lidera con el 8% de detecciones de códigos maliciosos en campañas de phishing, seguido por Costa Rica con el 7,2%, Colombia con el 5,7%, Guatemala con el 5,2% y El Salvador con el 5,1%.

En 2019, según el informe de NRD Cyber Security sobre la ciberseguridad en Ecuador, las principales amenazas incluyen suplantación de identidad, correo no deseado, software malicioso, fuga de información, amenaza interna, manipulación física, robo de identidad, ataques a aplicaciones web, secuestro de datos, denegación de servicio, ataques web, violaciones de datos,

redes de bots, minería de criptomonedas maliciosa y espionaje cibernético (Ministerio-de-Telecomunicaciones, 2021).

1.3. Línea de investigación

Tabla 1 *Línea de investigación*

Tipo de línea	Líneas de investigación institucionales	Sub Línea
En desarrollo	Energía eléctrica y Tecnologías de la Información para la innovación y el desarrollo sostenible	Ciencia de los ordenadores, analítica de datos y algoritmos computacionales ☒
		Sistemas eléctricos de potencia, energía e iluminación ☐
		Modelado, automatización y control ☐

Fuente: *Universidad Católica de Cuenca*

La línea de investigación que se abordará es la Ciencia de los Ordenadores, la Analítica de Datos y los Algoritmos Computacionales, la cual nos proporcionará las herramientas y técnicas necesarias para analizar el comportamiento de los sistemas informáticos y desarrollar soluciones efectivas para protegerlos.

Este enfoque es crucial, ya que, al recolectar datos, podemos examinarlos para identificar tendencias y patrones que revelen los tipos de ataques más comúnmente empleados por ciberdelincuentes mediante la ingeniería social.

Este análisis arrojará luz sobre el impacto significativo que estos ataques tienen en la población, al causar graves problemas como el robo de información personal y financiera, el compromiso de la privacidad y la confianza en las plataformas digitales. Estos problemas afectan no solo a individuos, sino también a empresas y entidades gubernamentales, destacando la urgencia de desarrollar estrategias efectivas de ciberseguridad para mitigar estos riesgos y proteger a la sociedad en general.

1.4. Objeto de estudio

El objetivo de este estudio se centrará en la Ingeniería Social y abarcará los siguientes puntos:

- Análisis y comprensión de las técnicas utilizadas por los ciberdelincuentes para manipular a las personas y obtener acceso no autorizado a sistemas informáticos o información confidencial. Este objeto de estudio es de gran importancia debido a su relevancia en el panorama actual de seguridad digital.
- Investigación sobre las tácticas psicológicas y de persuasión utilizadas por los atacantes para engañar a las víctimas y obtener información sensible.
- Estudio de las debilidades y falencias en el comportamiento humano que pueden ser explotadas por los ciberdelincuentes, como la falta de conciencia de seguridad, la confianza excesiva o la tendencia a seguir instrucciones sin cuestionarlas.
- Categorizar los diferentes tipos de ataques de ingeniería social, como phishing, pretexting, ingeniería inversa, entre otros, para comprender sus mecanismos y objetivos.
- Evaluar el impacto que los ataques de ingeniería social tienen en la seguridad de los sistemas informáticos y en la privacidad de los usuarios, así como en la reputación y la confianza en las plataformas digitales.
- Desarrollar estrategias y medidas de prevención para educar a las personas sobre los riesgos de la ingeniería social, fortalecer la conciencia de seguridad y establecer controles y políticas para mitigar estos ataques.

1.5. Campo de acción

Los ataques por ingeniería social son numerosos y para este estudio se enfocará en los más mencionados: Phishing, Smishing y Vishing. La diversidad de estos métodos resalta la importancia de la concientización y la formación en seguridad para ayudar a las personas a reconocer y evitar caer en estos engaños. Los tres tipos de ataques buscan explotar la confianza de las personas y su disposición a compartir información sensible. Se analizarán los diferentes canales y enfoques utilizados por los ciberdelincuentes, abarcando este fenómeno a nivel nacional.

Phishing, una de las formas más comunes de ingeniería social, implica el uso de correos electrónicos fraudulentos que aparentan ser de fuentes confiables para engañar a los destinatarios y que revelen información personal, como contraseñas o números de tarjetas de crédito. Los ciberdelincuentes han sofisticado sus técnicas, empleando inteligencia artificial para personalizar mensajes y hacerlos más convincentes, lo que incrementa la efectividad de estos ataques.

Smishing, similar al phishing, pero a través de mensajes SMS, es otra táctica utilizada para obtener información personal. Los mensajes de texto fraudulentos contienen enlaces maliciosos o solicitudes de información confidencial. Los ciberdelincuentes se aprovechan de la urgencia que puede generar un mensaje de texto, haciendo que las víctimas respondan sin cuestionar la legitimidad del remitente.

Vishing, que utiliza llamadas telefónicas para engañar a las personas y que revelen información sensible, es otra variante de estos ataques. Los atacantes se hacen pasar por representantes de bancos o instituciones gubernamentales, utilizando técnicas de spoofing para que las llamadas parezcan legítimas. Este tipo de ataque explota la confianza y la falta de verificación por parte de la víctima al recibir una llamada aparentemente oficial.

En el Ecuador, se han documentado varios casos de ataques por ingeniería social, lo que subraya la necesidad de una evaluación detallada de las condiciones que propiciaron estos incidentes. Este análisis permitirá identificar patrones y vulnerabilidades específicas, facilitando el desarrollo de protocolos y medidas necesarias para contrarrestar o mitigar futuros ataques. La revisión incluirá la implementación de tecnologías avanzadas de detección y respuesta, así como programas educativos para sensibilizar a la población sobre estos riesgos.

Se realizará una revisión de la Política Nacional de Ciberseguridad de Ecuador con el objetivo de analizar sus metas y evaluar el nivel de concientización y educación en temas de ciberseguridad entre la población. Esta revisión permitirá identificar brechas en la política actual y proponer mejoras basadas en mejores prácticas internacionales. Al comprender mejor los desafíos específicos que enfrenta Ecuador en términos de ciberseguridad, se podrán desarrollar estrategias más efectivas para proteger a los ciudadanos y las instituciones del país frente a los ataques de ingeniería social.

1.6.Objetivos

1.6.1. General

Analizar las tendencias y patrones de los ataques de Ingeniería Social en entornos digitales contemporáneos tanto a nivel organizacional como individual, a través de la revisión exhaustiva de trabajos académicos, estudios empíricos y casos relevantes, permitiendo identificar los métodos más utilizados y efectivos de ingeniería social, con el propósito de desarrollar estrategias y recomendaciones prácticas que fortalezcan la concienciación y capacitación en ciberseguridad, así como la implementación de medidas preventivas y correctivas.

1.6.2. Específicos

- Categorizar las técnicas de ingeniería social más prevalentes, destacando sus características y modus operandi.
- Desarrollar estrategias concretas y efectivas que protejan tanto a individuos como a organizaciones frente a posibles ataques de ingeniería social.
- Explorar las características particulares de plataformas como redes sociales, correos electrónicos, mensajería instantánea y otros canales para la detección de posibles vulnerabilidades que podrían ser aprovechadas mediante tácticas de ingeniería social.
- Implementar medidas de seguridad fundamentales y programas de concientización dirigidos al personal, con el objetivo de aumentar la resiliencia frente a amenazas, al mismo tiempo que se identifican y mejoran áreas específicas que necesiten atención.

1.6.3. Problema científico

General

¿Cuáles son las últimas tendencias en ataques de ingeniería social que utilizan los ciberdelincuentes para cometer delitos?

Específicos

- ¿Cuáles son las técnicas de ingeniería social más utilizadas, sus características y cuál es su modo de operación?
- ¿Qué plataformas son las más vulnerables a los ataques de ingeniería social?
- ¿Cómo mejorar las medidas de seguridad actuales para protegerse contra los ataques de ingeniería social?

1.7. Hipótesis

Será posible que al diseñar medidas de seguridad eficaces se pueda contrarrestar o mitigar los ataques relacionados con la Ingeniería social.

Se supone que la efectividad de las medidas de seguridad cibernética depende en gran medida de la ejecución de programas de concientización dirigidos al personal de una institución u organización. Esta premisa se basa en la idea de que la comprensión profunda de las tácticas de ingeniería social y la sensibilización de los individuos involucrados pueden actuar sinérgicamente para fortalecer la resistencia contra posibles amenazas cibernéticas.

1.8. Variables

Independiente

- Tendencias actuales en ataques de Ingeniería Social

Dependientes

- Técnicas utilizadas en ataques de Ingeniería Social.
- Frecuencia de ataques.
- Impacto de los ataques de Ingeniería Social en organizaciones y usuarios finales como impacto económico, a nivel de imagen y reputación de la empresa, impacto a nivel emocional.

1.9. Justificación

Las tácticas y técnicas de ingeniería social están en constante evolución, lo que hace imperativo estudiar las tendencias actuales para que tanto los profesionales de ciberseguridad como el público en general se mantengan al tanto de las últimas estrategias utilizadas por los atacantes. Los ciberdelincuentes no solo actualizan sus métodos, sino que también desarrollan nuevas técnicas para burlar las defensas existentes. Esta continua evolución requiere un monitoreo

constante y una adaptación rápida por parte de quienes están encargados de proteger la información y los sistemas.

Al llevar a cabo esta investigación, se obtendrá una comprensión más profunda de los ataques más frecuentemente utilizados. Entender las tácticas comunes, como el phishing, smishing y vishing, así como las nuevas variaciones y métodos emergentes, permite a los profesionales de ciberseguridad anticiparse a las amenazas. Esta comprensión no solo es crucial para desarrollar contramedidas efectivas, sino también para educar a los usuarios sobre cómo reconocer y responder a estos ataques.

Con una mejor comprensión de las tácticas de ingeniería social, será viable implementar medidas preventivas y elaborar protocolos de seguridad que fortalezcan las defensas de la organización. Estas medidas pueden incluir la actualización de políticas de seguridad, la implementación de tecnologías avanzadas de detección y respuesta, y la capacitación continua de los empleados. Proteger la organización contra ataques de ingeniería social no solo implica mejorar la tecnología, sino también fomentar una cultura de seguridad entre todos los miembros de la organización.

Este fortalecimiento conducirá a una mejora en la detección de amenazas y en el tiempo de respuesta frente a posibles ataques. Las organizaciones que están al tanto de las últimas tendencias en ingeniería social pueden desarrollar sistemas de monitoreo más efectivos y protocolos de respuesta rápida que minimicen el impacto de un ataque. Una respuesta rápida y eficiente no solo reduce el daño potencial, sino que también desalienta a los atacantes al demostrar que la organización está bien preparada.

Permitir a las organizaciones asignar de manera más eficiente sus recursos de ciberseguridad y concentrar sus esfuerzos en las áreas de mayor riesgo y relevancia es otro

beneficio crucial de este enfoque. Al identificar las áreas más vulnerables y los métodos de ataque más probables, las organizaciones pueden priorizar sus inversiones en ciberseguridad, asegurando que los recursos limitados se utilicen de la manera más efectiva posible.

La apropiada difusión de información sobre varios tipos de ataques y la concienciación acerca de los riesgos pueden prevenir la filtración de información, la exposición de datos sensibles y el robo de identidades. La educación continua sobre las tácticas de ingeniería social y las mejores prácticas de seguridad es esencial para proteger tanto a los individuos como a las organizaciones. Las campañas de concienciación pueden incluir seminarios, talleres, boletines informativos y otros recursos educativos que capaciten a los usuarios para identificar y evitar las amenazas.

Esto posibilita que las personas adopten prácticas más seguras en línea, disminuyendo la probabilidad de ser víctimas de estafas o fraudes. Con una mayor concienciación y formación, los usuarios estarán mejor equipados para reconocer los intentos de ingeniería social y tomar las medidas adecuadas para protegerse. Esto no solo protege a los individuos, sino que también fortalece la postura de seguridad general al reducir el número de puntos de entrada que los atacantes pueden explotar.

1.10. Estado del arte o antecedentes

En la actualidad, la integración de la tecnología ha simplificado muchas tareas laboriosas, generando impactos positivos en áreas como el ámbito militar, la salud, la educación y las finanzas, pero este avance conlleva preocupaciones con respecto a la seguridad de la información (Parthy & Rajendran, 2019).

La ingeniería social se fundamenta en la explotación de las debilidades, credulidad e ignorancia humanas como táctica de ataque. A pesar de que se han estudiado previamente técnicas relacionadas con este tipo de ataques, el conocimiento actual sobre la ingeniería social y sus

diversas modalidades es limitado. Por tanto, se hace evidente la necesidad de redoblar esfuerzos para fortalecer la protección de los usuarios (Smith et al., 2013).

Los ataques cibernéticos constituyen un problema global, y en el caso de Colombia, se emplea la herramienta CAI Virtual de la Policía Nacional para recopilar y analizar datos sobre los ataques más relevantes, revelando que la estafa encabeza la lista con un 17%, en tercer lugar, se encuentra el phishing con el 13%, seguido por la suplantación con el 12%, el Vishing con el 10%, y el Smishing en octavo lugar con el 4% (Rincón-Nuñez, 2023).

La táctica principal empleada por los atacantes es el phishing, que busca adquirir de manera ilícita información confidencial mediante llamadas telefónicas o correos electrónicos falsificados. Además, se identifican cinco variantes específicas de phishing: spear phishing, whaling phishing, vishing phishing, phishing de respuesta de voz interactiva y phishing de compromiso de correo electrónico empresarial (Alzas-Hernández, 2023).

Se deben considerar otros tipos de ataques, como el vishing (phishing a través de conversaciones telefónicas), smishing (realizado mediante mensajes SMS por estafadores), spear phishing (orientado a individuos o grupos específicos), whaling (dirigido a las direcciones de organizaciones) y clone phishing (puede dirigirse a una amplia audiencia). Estas formas de ataque ponen en riesgo información confidencial propagando software malicioso en los dispositivos personales de las víctimas (Smith et al., 2013).

En el trabajo realizado por Kevin Mitnick describe un ciclo de ataque basado en la ingeniería social, que consta de cuatro fases: Recopilación de información, Establecimiento de confianza, Explotación y Alcance/Finalización

En cuanto a las medidas que se pueden optar para lograr la seguridad cibernética Gallegos, Veintimilla y Jara (2017) sugieren que el Estado Ecuatoriano adopte una serie de medidas

estratégicas destinadas a reducir las amenazas y ataques cibernéticos. En este sentido, se proponen las siguientes recomendaciones: Capacidad del Estado para enfrentar las ciberamenazas, Seguridad de la información de la administración pública, Seguridad de la infraestructura crítica, Cibercriminalidad, Ciberdefensa, Capacidad del sector privado ante ciberamenazas, Sociedad y cultura de ciberseguridad, Investigación, desarrollo e innovación.

1.11. Marco teórico

1.11.1. Antecedentes

En los años 90, Kevin Mitnick, uno de los hackers más famosos, destacó la importancia de la ingeniería social en sus actividades. Sus técnicas de manipulación y engaño mostraron cómo las debilidades humanas podían ser explotadas para obtener acceso a sistemas seguros, lo que fue documentado en el libro "The Art of Deception" (Arboleda, 2002). Esta obra subrayó la necesidad de entender y mitigar los riesgos asociados con la ingeniería social.

Estudios posteriores se centraron en el phishing y el spear phishing, dos de las formas más comunes de ingeniería social. (Rosero & Llerena, 2006) realizaron investigaciones exhaustivas sobre las tácticas de phishing, destacando cómo los atacantes crean correos electrónicos convincentes para engañar a los usuarios. Sus investigaciones revelaron que los atacantes utilizan técnicas psicológicas para aumentar la tasa de éxito de sus ataques.

El spear phishing, una variante más dirigida del phishing, ha sido objeto de numerosos estudios debido a su precisión y efectividad. (Symantec, 2011) publicó informes detallados sobre cómo estos ataques se personalizan para individuos específicos, utilizando información recopilada de redes sociales y otras fuentes. Esta investigación mostró que, a pesar de ser menos frecuente

que el phishing tradicional, el spear phishing tiende a tener un mayor impacto debido a su enfoque preciso.

Las investigaciones sobre el uso de redes sociales en ataques de ingeniería social han revelado nuevas dimensiones del problema. (Martinez, 2019) examinaron cómo los atacantes utilizan información de perfiles de redes sociales para personalizar sus ataques y hacerlos más creíbles. Su estudio destacó la vulnerabilidad de los usuarios que comparten demasiada información personal en línea.

Con la proliferación de dispositivos móviles, el smishing y el vishing han emergido como amenazas significativas. Verizon (2019) llevó a cabo un estudio sobre smishing, demostrando cómo los atacantes utilizan mensajes de texto para engañar a los usuarios. Este informe mostró que, al igual que el phishing, el smishing explota la confianza de los usuarios en los mensajes recibidos en sus dispositivos móviles.

(Colli, 2020) exploró en profundidad las herramientas y tecnologías utilizadas por los ingenieros sociales. Su investigación destacó el uso de software de suplantación de identidad y la recopilación de información a través de redes sociales como métodos clave para ejecutar ataques exitosos. Además, se exploraron las técnicas de ingeniería inversa y la utilización de troyanos y malware, demostrando cómo los atacantes pueden obtener control sobre los sistemas de las víctimas (Stallings, 2019).

Las investigaciones sobre métodos de defensa contra la ingeniería social han avanzado en paralelo con los estudios sobre las técnicas de ataque. Hadnagy (2018) enfatizó la importancia de la concienciación y formación de empleados como una medida preventiva clave. Los estudios han

mostrado que la educación de los empleados sobre cómo reconocer y responder a intentos de ingeniería social puede reducir significativamente la efectividad de estos ataques.

Symantec (2010) y otros estudios han investigado las tecnologías de detección y prevención, como el filtrado de correos electrónicos y los sistemas de detección de intrusos. Estos estudios demostraron que la implementación de tecnologías avanzadas puede identificar y bloquear ataques de ingeniería social antes de que alcancen a los usuarios.

1.11.2. Historia y evolución de la ingeniería social

La ingeniería social no es un fenómeno reciente; sus raíces se encuentran en antiguas técnicas de engaño y manipulación. Desde los primeros registros históricos, las personas han utilizado la manipulación psicológica para obtener ventajas. Sin embargo, con el advenimiento de la tecnología digital, estas técnicas han evolucionado y se han vuelto más sofisticadas. Este desarrollo puede dividirse en varias fases distintivas, cada una caracterizada por la implementación de nuevas tecnologías y estrategias.

En la era pre-Internet, las técnicas de ingeniería social se basaban principalmente en interacciones cara a cara o a través de llamadas telefónicas, aprovechando la comunicación directa para manipular a las personas y obtener información confidencial. Una de las tácticas más comunes en ese tiempo era el pretexto, donde el atacante se presentaba como alguien autorizado o con derecho a la información que buscaba. Este enfoque dependía en gran medida de la habilidad del atacante para construir una narrativa creíble y convincente, utilizando detalles precisos y comportándose de manera profesional para ganarse la confianza de la víctima.

Por ejemplo, un atacante podría hacerse pasar por un técnico de soporte informático, un funcionario gubernamental, o un empleado de una empresa, solicitando acceso a datos sensibles

bajo el pretexto de realizar una tarea legítima. La clave del éxito en esta táctica residía en la capacidad del atacante para mantener la coherencia en su historia y mostrar una apariencia de autoridad.

Otro método frecuente en la era pre-Internet era el *quid pro quo*, que involucraba promesas de beneficios a cambio de información. En este caso, el atacante ofrecía algo de valor, como ayuda técnica, información valiosa, o algún tipo de favor, a cambio de datos confidenciales. Esta técnica explotaba la predisposición natural de las personas a ayudar y recibir algo a cambio, creando una situación en la que la víctima se sentía obligada a proporcionar la información solicitada.

Estas tácticas se basaban en principios psicológicos fundamentales como la autoridad y la reciprocidad. El principio de autoridad sugiere que las personas tienden a obedecer a figuras que perciben como legítimas y confiables, mientras que el principio de reciprocidad implica que las personas sienten la necesidad de devolver un favor cuando han recibido algo de valor. Estos principios, aunque desarrollados y aplicados en la era pre-Internet, siguen siendo extremadamente relevantes en la ingeniería social moderna, donde los atacantes continúan explotando las mismas vulnerabilidades humanas, pero ahora utilizando medios digitales.

Según estudios y análisis de comportamiento humano, estas técnicas de ingeniería social han demostrado ser efectivas debido a la profunda influencia que los principios psicológicos tienen en la toma de decisiones de las personas. La habilidad de los atacantes para aprovechar estas debilidades psicológicas sigue siendo una amenaza significativa en la era digital, donde las interacciones son más frecuentes y menos personalizadas, lo que puede hacer que las tácticas de ingeniería social sean aún más efectivas si no se cuenta con una educación y concienciación adecuada.

En conclusión, las técnicas de ingeniería social de la era pre-Internet, como el pretexto y el *quid pro quo*, establecieron las bases para las tácticas utilizadas en la actualidad. Aunque los medios han cambiado con el avance de la tecnología, los principios psicológicos subyacentes que hacen efectivas estas tácticas siguen siendo los mismos. Esto subraya la importancia de la educación continua y la formación en seguridad para ayudar a las personas a reconocer y resistir estos intentos de manipulación, tanto en entornos tradicionales como en el ciberespacio.

Era del correo electrónico

Con la llegada del correo electrónico, surgieron nuevas oportunidades para los atacantes, marcando una era de cambios significativos en la forma en que se llevaban a cabo los ataques de ingeniería social. El phishing se convirtió en una de las formas más comunes y efectivas de estos ataques. Este método implica el envío de correos electrónicos fraudulentos que aparentan ser de fuentes confiables, como bancos, servicios en línea o incluso colegas de trabajo, con el objetivo de engañar a los destinatarios para que revelen información personal o financiera. Los atacantes diseñan estos correos electrónicos para que parezcan legítimos, utilizando logotipos, formatos de texto y direcciones de correo similares a las reales, lo que aumenta la probabilidad de éxito.

Una variante más sofisticada de este método es el spear phishing. A diferencia del phishing general, que se dirige a un gran número de personas con mensajes genéricos, el spear phishing se enfoca en individuos específicos. Los atacantes personalizan los correos electrónicos basándose en información específica de la víctima, como su nombre, cargo, contactos y otros detalles obtenidos a través de la investigación previa. Esta personalización hace que los correos electrónicos sean mucho más convincentes y difíciles de detectar como fraudulentos. Los atacantes pueden, por ejemplo, hacer que un correo electrónico parezca que proviene de un colega o un

superior, solicitando información confidencial o pidiendo que se realicen ciertas acciones, como la transferencia de fondos.

La persistencia del phishing como una amenaza significativa en el ciberespacio fue destacada en un estudio de la Anti-Phishing Working Group (APWG) en 2020. El estudio reveló que el phishing sigue siendo una de las amenazas más prevalentes y efectivas, afectando tanto a individuos como a organizaciones. Las tácticas utilizadas por los ciberdelincuentes han evolucionado continuamente, adoptando nuevas tecnologías y métodos para aumentar la efectividad de sus ataques. La creciente sofisticación de estas tácticas subraya la necesidad de una concienciación continua y una formación en seguridad tanto para los usuarios individuales como para los empleados de las organizaciones.

Además de la educación y la formación, es esencial que las organizaciones implementen tecnologías avanzadas de detección y prevención de phishing. Esto puede incluir el uso de filtros de correo electrónico que emplean inteligencia artificial para identificar patrones de phishing, la implementación de políticas de autenticación multifactorial y la realización de simulaciones de phishing para evaluar y mejorar la preparación de los empleados. Al combinar estas medidas con una cultura organizacional que promueva la seguridad y la transparencia, se puede reducir significativamente el riesgo y el impacto de los ataques de phishing.

La era del correo electrónico ha transformado el panorama de la ciberseguridad, presentando nuevas oportunidades para los atacantes de ingeniería social. El phishing, y su variante más dirigida, el spear phishing, continúan siendo amenazas persistentes y sofisticadas. La respuesta a estas amenazas debe ser multifacética, combinando la tecnología avanzada con una educación y formación adecuadas para crear un entorno más seguro tanto para individuos como para organizaciones.

Era de las redes sociales y dispositivos móviles

La proliferación de las redes sociales y los dispositivos móviles ha abierto nuevas vías para los ataques de ingeniería social, transformando significativamente el panorama de la ciberseguridad. Plataformas como Facebook, Twitter y LinkedIn, con millones de usuarios activos, se han convertido en objetivos atractivos para los ciberdelincuentes. Estos atacantes explotan las redes sociales para realizar phishing en redes sociales, utilizando perfiles falsos o comprometiendo cuentas legítimas para engañar a los usuarios y obtener información personal o financiera.

Los atacantes crean perfiles que imitan a personas reales o utilizan cuentas comprometidas de amigos o colegas para ganar la confianza de las víctimas. A través de mensajes directos o publicaciones, los atacantes pueden solicitar información confidencial, enviar enlaces maliciosos o distribuir malware. Esta forma de ataque se aprovecha de la naturaleza social de estas plataformas, donde los usuarios tienden a confiar en la información y las solicitudes que reciben de sus contactos.

Además del phishing en redes sociales, ha surgido una variante conocida como smishing, que es el phishing realizado a través de mensajes de texto. El smishing se ha vuelto cada vez más común debido a la alta tasa de apertura y respuesta de los mensajes de texto en comparación con los correos electrónicos. Los mensajes de smishing suelen contener enlaces maliciosos o solicitudes de información personal, presentándose como alertas bancarias, notificaciones de entrega de paquetes o incluso mensajes de amigos o familiares.

Un informe de Kaspersky de 2019 indicó que los ataques de smishing han aumentado considerablemente, destacando la necesidad de una mayor concienciación y medidas de seguridad en el uso de dispositivos móviles. Los ciberdelincuentes se aprovechan de la inmediatez y la

aparente urgencia de los mensajes de texto para persuadir a las víctimas a que actúen rápidamente, a menudo sin cuestionar la legitimidad del mensaje.

Para mitigar los riesgos asociados con el phishing en redes sociales y el smishing, es esencial implementar varias estrategias. Primero, los usuarios deben ser educados sobre los peligros de compartir información personal en las redes sociales y cómo identificar perfiles falsos o mensajes sospechosos. Las organizaciones pueden realizar campañas de concienciación y capacitación para sus empleados, enfatizando la importancia de verificar las solicitudes y enlaces antes de interactuar con ellos.

En cuanto al smishing, los usuarios deben ser conscientes de que las entidades legítimas, como los bancos, rara vez solicitan información personal a través de mensajes de texto. Los usuarios deben verificar cualquier solicitud sospechosa directamente con la entidad en cuestión, utilizando canales de comunicación oficiales. Además, es crucial que se instalen aplicaciones de seguridad en los dispositivos móviles, que pueden ayudar a detectar y bloquear mensajes de texto maliciosos.

Las empresas de tecnología y los desarrolladores de aplicaciones también tienen un papel importante en la protección contra estos ataques. Deben incorporar características de seguridad en sus plataformas y aplicaciones, como la autenticación multifactorial y la encriptación de datos. Además, deben proporcionar a los usuarios herramientas para reportar y bloquear perfiles falsos y mensajes sospechosos.

La era de las redes sociales y los dispositivos móviles ha introducido nuevas formas de ataques de ingeniería social, como el phishing en redes sociales y el smishing. La alta interacción y la confianza en estas plataformas y dispositivos presentan oportunidades para los ciberdelincuentes. La respuesta a estas amenazas debe incluir la educación y la concienciación de

los usuarios, así como la implementación de medidas tecnológicas y de seguridad para proteger la información personal y evitar caer en estos engaños.

1.11.3. Ingeniería social

La ingeniería social se refiere a las técnicas de manipulación psicológica que los atacantes utilizan para obtener información, acceso o influir en la toma de decisiones de las personas. A diferencia de los ataques tradicionales que dependen de vulnerabilidades técnicas, la ingeniería social se centra en las debilidades humanas, tales como la confianza y la falta de conocimiento en temas de seguridad. Los atacantes explotan estas vulnerabilidades para acceder a datos sensibles, sistemas protegidos y recursos financieros sin la necesidad de técnicas de hacking avanzadas.

Una de las razones por las que la ingeniería social es una amenaza significativa en el ámbito de la seguridad de la información es su capacidad para pasar desapercibida. Mientras que los ataques técnicos pueden ser detectados y mitigados con herramientas de seguridad, los ataques de ingeniería social suelen eludir estas defensas al dirigirse directamente a los usuarios. Según el informe de seguridad de Verizon de 2021, el 85% de las brechas de seguridad involucran un elemento humano, destacando la importancia de abordar esta vulnerabilidad desde una perspectiva de seguridad integral.

El concepto de ingeniería social no es nuevo; ha existido desde hace décadas, evolucionando con el tiempo y adaptándose a las nuevas tecnologías y plataformas de comunicación. Inicialmente, las tácticas se limitaban a interacciones cara a cara o llamadas telefónicas, pero con el auge de Internet, las técnicas de ingeniería social han proliferado y se han diversificado. Hoy en día, los ataques pueden ocurrir a través de correos electrónicos (phishing),

mensajes de texto (smishing), llamadas telefónicas (vishing) y redes sociales, lo que los hace más difíciles de detectar y prevenir.

La eficacia de la ingeniería social radica en su capacidad para manipular las emociones humanas y explotar la psicología del comportamiento. Los atacantes a menudo emplean tácticas que generan una respuesta emocional inmediata, como el miedo, la curiosidad o la urgencia, para persuadir a las víctimas a tomar acciones precipitadas. Por ejemplo, un correo electrónico de phishing puede advertir a la víctima sobre una actividad sospechosa en su cuenta bancaria, instándola a hacer clic en un enlace malicioso para "verificar" su información. Este tipo de manipulación explota la necesidad inmediata de proteger los activos personales, lo que lleva a la víctima a actuar sin verificar la legitimidad del mensaje.

Además de las técnicas de manipulación emocional, los ingenieros sociales también se aprovechan de la falta de conocimiento y formación en seguridad de los usuarios. Muchas personas no están conscientes de las tácticas de ingeniería social y cómo se presentan, lo que las hace vulnerables a estos ataques. La formación y concienciación en seguridad cibernética son esenciales para mitigar estos riesgos. Las organizaciones deben invertir en programas de capacitación que enseñen a los empleados a reconocer y responder adecuadamente a intentos de ingeniería social.

La ingeniería social representa una amenaza crítica en el panorama de la seguridad de la información debido a su enfoque en las debilidades humanas. Su capacidad para evadir las medidas de seguridad técnicas y explotar la confianza y el desconocimiento de las personas subraya la necesidad de una estrategia de seguridad integral que incluya tanto medidas técnicas como educativas. Entender la psicología detrás de estos ataques y educar a los usuarios es crucial para reducir la efectividad de la ingeniería social y proteger la información sensible.

Beneficios de la ingeniería social

- La ingeniería social, cuando se utiliza de manera ética y legal, puede aportar varios beneficios importantes en contextos como la seguridad y la educación:
- Pruebas de Seguridad: Las pruebas de ingeniería social éticamente realizadas permiten a las organizaciones evaluar la resistencia de sus sistemas y empleados frente a los ataques reales. Esto ayuda a identificar vulnerabilidades y mejorar las medidas de seguridad.
- Concientización y Formación: Utilizada como parte de programas de concientización en seguridad, la ingeniería social puede educar a los empleados y usuarios sobre las tácticas utilizadas por los ciberdelincuentes. Esto fortalece la capacidad de reconocer y responder adecuadamente a posibles amenazas.
- Mejora de Procesos Internos: Al simular escenarios de ingeniería social, las organizaciones pueden identificar debilidades en los procedimientos internos de manejo de información y comunicaciones. Esto permite implementar mejoras en políticas y protocolos para fortalecer la seguridad y proteger la información sensible.
- Evaluación de Cultura Organizacional: La respuesta de los empleados a las pruebas de ingeniería social también proporciona insights sobre la cultura organizacional en términos de conciencia y cumplimiento de políticas de seguridad. Esto puede guiar esfuerzos adicionales de formación y sensibilización.
- Desarrollo de Estrategias de Prevención: Los datos recopilados durante las pruebas de ingeniería social pueden ser analizados para desarrollar estrategias más efectivas

de prevención y mitigación de riesgos cibernéticos. Esto incluye la implementación de controles más robustos y la adaptación continua a nuevas tácticas de ataque.

En conjunto, estos beneficios destacan cómo la ingeniería social, cuando se aplica correctamente, no solo fortalece la seguridad digital, sino que también contribuye a una mayor conciencia y preparación frente a amenazas cibernéticas en las organizaciones y la sociedad en general.

La importancia de la ingeniería social en la actualidad abarca diversos ámbitos cruciales para la seguridad cibernética y el entendimiento de las interacciones humanas. En términos de seguridad, esta disciplina juega un papel fundamental al permitir a las organizaciones evaluar y fortalecer sus defensas contra amenazas digitales cada vez más sofisticadas. Mediante la simulación de ataques realistas, como el phishing y el smishing, se identifican vulnerabilidades tanto en los sistemas de seguridad como en el comportamiento humano, lo que facilita la implementación de medidas preventivas y correctivas efectivas.

Además de su aplicación práctica en la defensa cibernética, la ingeniería social actúa como una herramienta educativa poderosa. Al exponer a usuarios y empleados a técnicas de engaño utilizadas por ciberdelincuentes, se fomenta una mayor conciencia y vigilancia frente a posibles ataques. Esta educación no solo fortalece la seguridad individual y organizacional, sino que también contribuye a la creación de una cultura de ciberseguridad proactiva.

En el ámbito académico, la ingeniería social proporciona un terreno fértil para la investigación en psicología y sociología. Estudios sobre cómo las personas responden a estímulos persuasivos y manipulativos son fundamentales para comprender mejor los mecanismos subyacentes de la toma de decisiones y los patrones de comportamiento humano. Estos insights no solo informan prácticas en áreas como la publicidad y el marketing, sino que también pueden ser

utilizados para desarrollar estrategias preventivas contra la manipulación y la explotación emocional.

Asimismo, la ingeniería social impulsa la innovación en el campo de la defensa cibernética al desafiar constantemente a las industrias de seguridad a desarrollar tecnologías más avanzadas y adaptativas. La evolución rápida de las tácticas de engaño requiere soluciones innovadoras, como inteligencia artificial y análisis predictivo, para detectar y mitigar riesgos en tiempo real.

1.11.4. Tipos de ataques de ingeniería social

La ingeniería social constituye un conjunto diverso de estrategias diseñadas para manipular psicológicamente a individuos y obtener acceso no autorizado a información confidencial. Entre las tácticas más destacadas se encuentran el phishing, que emplea correos electrónicos fraudulentos para engañar a los usuarios y obtener datos sensibles; el smishing, que utiliza mensajes de texto para el mismo propósito; y el vishing, que se vale de llamadas telefónicas para simular ser entidades legítimas y obtener información personal. Estos métodos no solo explotan la confianza de las personas en las comunicaciones digitales y telefónicas, sino que también subrayan la importancia de políticas de seguridad robustas y la educación continua para mitigar estos riesgos en un entorno cada vez más interconectado.

Phishing

El phishing es una técnica ampliamente utilizada en la que los atacantes envían correos electrónicos que parecen provenir de fuentes legítimas y confiables, como bancos, empresas de servicios o incluso compañeros de trabajo. El objetivo es engañar a los destinatarios para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o datos

personales. Estos correos electrónicos suelen contener enlaces a sitios web fraudulentos que imitan a los originales.

Los ataques de phishing han evolucionado en su sofisticación y personalización, utilizando tácticas avanzadas para aumentar su efectividad. Los atacantes pueden emplear técnicas de ingeniería social para investigar a sus víctimas y crear mensajes altamente personalizados que son difíciles de distinguir de los correos electrónicos auténticos. Esta personalización puede incluir el uso de nombres reales, puestos de trabajo y otros detalles específicos que aumentan la probabilidad de que el destinatario caiga en la trampa.

Además, el phishing no se limita solo a correos electrónicos. También puede manifestarse a través de mensajes de texto (smishing), llamadas telefónicas (vishing) y plataformas de redes sociales. Cada uno de estos vectores de ataque explota diferentes aspectos del comportamiento humano y la confianza, ampliando el alcance y el impacto potencial del phishing.

Según un informe de la compañía de seguridad cibernética Symantec, aproximadamente uno de cada 2,000 correos electrónicos es un intento de phishing, lo que subraya la prevalencia y la sofisticación de esta técnica. Este dato pone de relieve la necesidad de que tanto individuos como organizaciones adopten medidas proactivas para protegerse. Las medidas pueden incluir la implementación de filtros avanzados de correo electrónico, programas de concientización y capacitación para empleados, y el uso de autenticación multifactor para asegurar que solo los usuarios legítimos puedan acceder a sistemas sensibles.

La educación y la concientización son componentes cruciales en la defensa contra el phishing. Las campañas de formación deben enseñar a los usuarios a identificar señales de advertencia comunes, como enlaces sospechosos, errores gramaticales o solicitudes inusuales de

información personal. Además, fomentar una cultura de reporte inmediato de posibles intentos de phishing puede ayudar a las organizaciones a responder rápidamente y minimizar los daños.

Spear Phishing

El spear phishing es una forma más avanzada y personalizada de phishing. A diferencia del phishing tradicional, que se dirige a una amplia audiencia, el spear phishing se enfoca en individuos o grupos específicos dentro de una organización. Los atacantes investigan a sus víctimas para crear mensajes altamente personalizados que aumentan la probabilidad de éxito.

Un ejemplo clásico de spear phishing puede involucrar a un atacante que se hace pasar por un alto ejecutivo de la empresa y envía un correo electrónico a un empleado solicitando transferencias de dinero o acceso a datos sensibles. Estos correos electrónicos suelen contener detalles precisos que los hacen parecer legítimos, como el nombre del ejecutivo, su estilo de comunicación y hasta información sobre proyectos en los que la víctima está trabajando. Esta personalización no solo incrementa la tasa de éxito del ataque, sino que también hace más difícil que los sistemas de seguridad automatizados detecten y bloqueen estos correos electrónicos fraudulentos.

El spear phishing es particularmente peligroso porque puede ser utilizado para llevar a cabo ataques más amplios y devastadores dentro de una organización. Por ejemplo, un atacante que logra acceder a las credenciales de un empleado puede moverse lateralmente dentro de la red de la empresa, recolectando más información y comprometiendo sistemas adicionales. Este tipo de ataque dirigido puede resultar en la pérdida de datos sensibles, daño reputacional y costos significativos para la recuperación y mitigación de los daños.

Un estudio realizado por la firma de seguridad FireEye reveló que el spear phishing es responsable de aproximadamente el 91% de los ciberataques dirigidos. Este alarmante porcentaje

destaca la efectividad y la prevalencia de esta técnica entre los cibercriminales. Las organizaciones deben estar especialmente atentas a esta amenaza y tomar medidas proactivas para protegerse.

Para combatir el spear phishing, es esencial que las empresas implementen programas robustos de concientización y capacitación para sus empleados, enseñándoles a reconocer señales de ataques dirigidos y a reportar cualquier actividad sospechosa. Además, las organizaciones deben adoptar tecnologías avanzadas de filtrado de correos electrónicos y sistemas de autenticación multifactor para añadir capas adicionales de seguridad. Los simulacros de spear phishing también pueden ser una herramienta útil para evaluar y mejorar la preparación de los empleados frente a estos ataques.

Vishing

El vishing, o phishing por voz, se realiza a través de llamadas telefónicas. En estos ataques, los estafadores se hacen pasar por representantes de instituciones financieras, proveedores de servicios técnicos u otras entidades de confianza para engañar a las víctimas y obtener información confidencial. Los estafadores suelen utilizar técnicas de ingeniería social para ganarse la confianza de la víctima, manipulándola para que revele detalles personales o financieros.

Por ejemplo, un atacante podría llamar a una persona afirmando ser de su banco y solicitar información personal para "verificar" la cuenta. Estos delincuentes pueden emplear tácticas de urgencia o miedo, como advertir sobre una posible actividad fraudulenta en la cuenta, para presionar a la víctima a que actúe rápidamente y sin pensar. Además, los estafadores pueden falsificar números de teléfono para que parezcan legítimos, lo que aumenta la credibilidad de la llamada.

Según el FBI, el vishing ha aumentado significativamente en los últimos años debido a la creciente confianza de las personas en las comunicaciones telefónicas. Este incremento también

puede atribuirse a la facilidad con la que los atacantes pueden acceder a herramientas tecnológicas para falsificar números de teléfono y a la falta de medidas de seguridad robustas en las comunicaciones telefónicas en comparación con otros métodos de comunicación.

Para protegerse contra el vishing, es esencial que las personas sean cautelosas al recibir llamadas no solicitadas que soliciten información personal o financiera. Nunca se debe proporcionar información sensible a través del teléfono a menos que se esté completamente seguro de la identidad del interlocutor. Si se recibe una llamada sospechosa, lo mejor es colgar y llamar directamente a la institución o empresa utilizando un número de teléfono conocido y verificado.

Las organizaciones también pueden adoptar medidas para proteger a sus clientes contra el vishing, como educar a sus usuarios sobre los riesgos y las señales de advertencia de estos ataques. Implementar sistemas de verificación de llamadas y utilizar tecnologías de autenticación adicionales puede ayudar a reducir la eficacia de los intentos de vishing.

Smishing

El smishing, o phishing a través de mensajes de texto, utiliza mensajes SMS para engañar a las víctimas. Estos mensajes a menudo contienen enlaces maliciosos o solicitan información personal directamente. Los atacantes pueden enviar mensajes que parecen provenir de empresas conocidas, como servicios de entrega, proveedores de telecomunicaciones o incluso instituciones gubernamentales, creando una apariencia de legitimidad que puede engañar fácilmente a los destinatarios.

Un ejemplo típico de smishing podría ser un mensaje que parece provenir de un servicio de entrega, informando a la víctima sobre un paquete pendiente y proporcionando un enlace para más detalles. Al hacer clic en el enlace, la víctima puede ser redirigida a un sitio web falso que

solicita información personal o financiera. Alternativamente, el enlace podría descargar malware en el dispositivo de la víctima, comprometiendo su seguridad.

La firma de seguridad Kaspersky ha informado un aumento del 328% en ataques de smishing en el último año, lo que refleja la creciente amenaza de este tipo de ingeniería social. Este incremento se debe en parte a la facilidad y bajo costo con que los atacantes pueden enviar mensajes de texto a un gran número de destinatarios, así como a la alta tasa de apertura y respuesta a los mensajes SMS en comparación con otros métodos de comunicación.

Para protegerse contra el smishing, es fundamental que las personas sean cautelosas al recibir mensajes de texto no solicitados que contienen enlaces o solicitan información personal. Nunca se debe proporcionar información sensible en respuesta a un mensaje de texto y se deben evitar hacer clic en enlaces de remitentes desconocidos o no verificados. En su lugar, es recomendable contactar directamente con la empresa o institución utilizando un número de teléfono o sitio web oficial para verificar la autenticidad del mensaje.

Las organizaciones también deben tomar medidas para proteger a sus clientes contra el smishing. Esto incluye educar a los usuarios sobre los riesgos y señales de advertencia de estos ataques y proporcionar directrices claras sobre cómo interactuar de manera segura con mensajes de texto. Implementar sistemas de alerta que informen a los usuarios sobre campañas de smishing conocidas también puede ser una medida efectiva para reducir el impacto de estos ataques.

Pretexting

El pretexting es una técnica sofisticada de ingeniería social que implica la creación de un escenario ficticio por parte del atacante para engañar a la víctima y obtener información confidencial. Los atacantes pueden hacerse pasar por colegas, autoridades o incluso familiares, creando una narrativa convincente que induce a la víctima a revelar información sensible o a

realizar acciones comprometedoras. Esta técnica se aprovecha de la confianza y la disposición de las personas para ayudar en situaciones aparentemente legítimas o de emergencia.

Por ejemplo, un atacante podría hacerse pasar por un supervisor en una empresa, contactar a un empleado y solicitar acceso a sistemas críticos bajo el pretexto de una situación urgente que requiere acción inmediata. Alternativamente, podría fingir ser un proveedor externo solicitando detalles sobre procedimientos internos bajo el pretexto de actualizar registros o resolver problemas técnicos. Estos escenarios ficticios están diseñados para manipular la buena fe de la víctima y evitar despertar sospechas.

Un informe de la empresa de seguridad Trustwave destaca que el pretexting es particularmente efectivo en entornos corporativos, donde los empleados están acostumbrados a seguir instrucciones de figuras de autoridad y pueden ser más susceptibles a cumplir con solicitudes que parecen legítimas a primera vista. Este tipo de ataque puede comprometer fácilmente la seguridad de una organización al proporcionar a los atacantes acceso a información confidencial o a sistemas críticos.

Para protegerse contra el pretexting, es fundamental que las organizaciones implementen políticas claras de manejo de información y autenticación. Los empleados deben ser educados sobre las tácticas comunes de pretexting y estar alertas ante cualquier solicitud de información sensible que parezca inusual o no verificada. Además, es esencial establecer procedimientos de verificación rigurosos para cualquier solicitud de información confidencial, especialmente si proviene de fuentes externas o desconocidas.

Las empresas también pueden beneficiarse de la implementación de controles de acceso robustos y de la monitorización activa de actividades sospechosas que puedan indicar intentos de

pretexting. La concienciación continua y la capacitación en seguridad son clave para fortalecer la resistencia de una organización frente a este tipo de ataques dirigidos y elaborados.

Baiting

El baiting es una técnica de ingeniería social en la que los atacantes utilizan señuelos para atraer a las víctimas y obtener acceso a sus sistemas o información confidencial. Estos señuelos pueden adoptar formas tanto físicas como digitales. Por ejemplo, los atacantes pueden dejar unidades USB infectadas en lugares públicos, como estacionamientos o cafeterías, con la esperanza de que alguien las encuentre y las conecte a su computadora. Alternativamente, pueden ofrecer enlaces a descargas gratuitas de software en línea que contienen malware oculto.

Una vez que la víctima toma el cebo, ya sea conectando la unidad USB o descargando el archivo malicioso, el atacante puede obtener acceso al sistema de la víctima. Esto puede permitir al atacante robar datos sensibles, instalar programas espía o incluso comprometer toda la red corporativa si la víctima se conecta desde un entorno de trabajo.

Un estudio realizado por la Universidad de Illinois reveló que el 45% de las personas que encuentran una unidad USB en la calle la conectan a su computadora, subrayando la efectividad de esta técnica. Este alto nivel de interacción con dispositivos desconocidos resalta la vulnerabilidad inherente de las personas frente a tácticas de baiting.

Para mitigar los riesgos asociados con el baiting, es crucial que las personas y las organizaciones promuevan una cultura de seguridad sólida. Esto incluye la capacitación regular sobre los peligros de dispositivos no verificados y la importancia de no conectar hardware desconocido a sistemas corporativos o personales. Además, se deben implementar políticas claras

de seguridad que prohíban el uso de dispositivos no autorizados y promuevan el reporte inmediato de incidentes sospechosos.

Las organizaciones también pueden beneficiarse de la implementación de software de seguridad avanzado que detecte y bloquee automáticamente dispositivos o archivos sospechosos. La concienciación continua y la vigilancia son fundamentales para protegerse contra las tácticas de baiting, que aprovechan la curiosidad humana y la disposición a aceptar "ofertas" aparentemente inocuas que en realidad ocultan amenazas significativas.

1.11.5. Herramientas y tecnologías utilizadas en ingeniería social

Los ataques de ingeniería social han evolucionado significativamente, impulsados por el desarrollo de diversas herramientas y tecnologías que facilitan la manipulación y el engaño. Estas herramientas permiten a los atacantes suplantar identidades, recopilar información personal, entender y explotar sistemas, y finalmente, comprometer la seguridad de sus víctimas.

Software de suplantación de identidad

Una de las principales herramientas utilizadas en ingeniería social es el software de suplantación de identidad. Este tipo de software permite a los atacantes falsificar direcciones de correo electrónico y números de teléfono, haciendo que los mensajes fraudulentos parezcan provenir de fuentes legítimas. Esta capacidad de suplantación es crucial en ataques de phishing y spear phishing, donde la autenticidad percibida del mensaje es esencial para engañar a la víctima. Según el informe de la empresa de seguridad Proofpoint, los ataques de suplantación de identidad han aumentado un 30% en el último año, lo que subraya la efectividad y popularidad de esta herramienta.

Las redes sociales se han convertido en una mina de oro para los ingenieros sociales que buscan recopilar información sobre sus víctimas. Plataformas como Facebook, LinkedIn y Twitter contienen vastas cantidades de datos personales que los atacantes pueden utilizar para personalizar sus ataques. Los perfiles públicos pueden revelar detalles como el lugar de trabajo, las relaciones personales y las actividades diarias, proporcionando a los atacantes la información necesaria para crear mensajes altamente personalizados y creíbles. Un estudio de la Universidad de California demostró que los atacantes pueden recolectar información suficiente de los perfiles de redes sociales para realizar ataques de spear phishing con una tasa de éxito significativamente alta.

La ingeniería inversa es otra herramienta clave en el arsenal de los ingenieros sociales. Este proceso implica descomponer sistemas y software para comprender su funcionamiento interno, lo que permite a los atacantes identificar vulnerabilidades y explotarlas. Los ingenieros sociales utilizan la ingeniería inversa no solo para descubrir fallos de seguridad en aplicaciones y sistemas, sino también para crear software malicioso que pueda evadir las defensas existentes. Un informe del Instituto SANS destaca que el uso de la ingeniería inversa ha sido fundamental en la creación de troyanos y otros tipos de malware sofisticados que se utilizan en ataques dirigidos (Landeta, 2020).

El uso de troyanos y malware es una técnica común en los ataques de ingeniería social, donde el objetivo es obtener acceso y control sobre los sistemas de las víctimas. Los troyanos, en particular, son programas maliciosos que se disfrazan como software legítimo y se instalan en el sistema de la víctima sin su conocimiento. Una vez instalados, los troyanos pueden permitir a los atacantes robar información, registrar pulsaciones de teclas, tomar capturas de pantalla e incluso controlar el sistema de forma remota. La empresa de seguridad Kaspersky reporta que el 58% de

las infecciones por malware detectadas en 2023 fueron causadas por troyanos, lo que refleja su prevalencia en el ámbito de la ingeniería social (Benavides, 2020) .

Los ingenieros sociales emplean una amplia gama de herramientas y tecnologías para llevar a cabo sus ataques, cada una diseñada para facilitar el engaño y la manipulación de sus víctimas. Desde software de suplantación de identidad hasta troyanos y malware, estas herramientas permiten a los atacantes superar las defensas técnicas y explotar las vulnerabilidades humanas. La creciente sofisticación de estas herramientas subraya la necesidad de estar continuamente vigilantes y educados sobre las tácticas de ingeniería social para proteger la información y los sistemas sensibles (Benet, 2019).

Métodos de defensa contra la ingeniería social

La defensa contra los ataques de ingeniería social requiere una combinación de medidas técnicas y educativas, diseñadas para proteger tanto los sistemas como a los individuos. Esta aproximación integral es crucial para mitigar el riesgo que representan estos ataques, que se basan en la manipulación psicológica para eludir las defensas técnicas.

Uno de los pilares fundamentales en la defensa contra la ingeniería social es la concienciación y la formación de los empleados. Los programas de formación deben enfocarse en enseñar a los empleados cómo identificar y responder a los intentos de ingeniería social. Según un estudio de la empresa de seguridad cibernética KnowBe4, las organizaciones que implementan programas regulares de formación en seguridad experimentan una reducción del 37% en la tasa de clics en correos electrónicos de phishing. Estos programas deben incluir simulaciones de ataques de phishing, talleres sobre las últimas tácticas de ingeniería social y sesiones informativas sobre cómo manejar información sensible de manera segura. La capacitación continua asegura que los

empleados estén al tanto de las tácticas emergentes y sean capaces de actuar de manera adecuada cuando se enfrenten a intentos de ingeniería social (Garzón, 2024).

Además de la formación, las organizaciones deben implementar tecnologías avanzadas de detección y prevención para protegerse contra los ataques de ingeniería social. El uso de software de filtrado de correos electrónicos es esencial para identificar y bloquear correos electrónicos de phishing antes de que lleguen a las bandejas de entrada de los usuarios. Un informe de Gartner destaca que los sistemas avanzados de filtrado de correos electrónicos pueden detectar y bloquear hasta el 99% de los intentos de phishing. Además, los firewalls y los sistemas de detección de intrusos (IDS) pueden monitorear el tráfico de la red y alertar sobre actividades sospechosas que podrían indicar un intento de ataque. Estas tecnologías no solo ayudan a prevenir los ataques, sino que también proporcionan una capa adicional de seguridad que puede mitigar el impacto de los intentos exitosos.

1.11.6. Protocolos y políticas de seguridad

La implementación de protocolos y políticas de seguridad claras es una estrategia crucial en la defensa contra la ingeniería social. Estas políticas deben definir procedimientos específicos para la divulgación de información y la verificación de identidades, asegurando que los empleados sepan cómo manejar solicitudes de información sensible. Por ejemplo, las políticas pueden requerir la verificación de la identidad de cualquier persona que solicite información confidencial, utilizando múltiples métodos de autenticación, como contraseñas, preguntas de seguridad y autenticación multifactor.

Un estudio de la Universidad de Stanford muestra que las organizaciones con políticas de seguridad bien definidas tienen un 45% menos de probabilidad de sufrir brechas de seguridad

causadas por errores humanos. Esto se debe a que las políticas claras y específicas proporcionan a los empleados directrices concretas sobre cómo responder a diversas situaciones, reduciendo así la probabilidad de que cometan errores que puedan ser explotados por atacantes.

Además, las auditorías regulares y la revisión de estas políticas pueden ayudar a identificar y corregir posibles vulnerabilidades antes de que sean explotadas. Por ejemplo, una auditoría puede revelar que ciertos procedimientos de verificación de identidad no son tan efectivos como se pensaba, permitiendo a la organización mejorar estos procedimientos antes de que se produzca una brecha. Carrizo (2020) destaca la importancia de estas auditorías regulares, señalando que las revisiones periódicas de las políticas de seguridad son esenciales para mantener una postura de seguridad robusta.

La defensa contra los ataques de ingeniería social requiere un enfoque multifacético que combine la formación y concienciación de los empleados, la implementación de tecnologías avanzadas de detección y prevención, y la adopción de políticas y protocolos de seguridad robustos. Este enfoque integral no solo fortalece la postura de seguridad de una organización, sino que también capacita a los empleados para que actúen como una primera línea de defensa contra los intentos de ingeniería social.

La continua evolución de las tácticas de ingeniería social subraya la necesidad de mantener estas defensas actualizadas y efectivas. Avila (2020) señala que las tácticas de los atacantes cambian constantemente, lo que exige que las políticas y los protocolos de seguridad se revisen y actualicen regularmente para adaptarse a las nuevas amenazas. Por lo tanto, es fundamental que las organizaciones no solo implementen políticas de seguridad, sino que también se comprometan a revisarlas y mejorarlas de manera continua para enfrentar los desafíos emergentes.

La implementación de protocolos y políticas de seguridad bien definidas, junto con auditorías regulares y revisiones continuas, es esencial para proteger a las organizaciones contra los ataques de ingeniería social. Este enfoque integral garantiza que tanto las tecnologías como los empleados estén preparados para detectar y responder a las amenazas, proporcionando una defensa sólida y eficaz contra los intentos de manipulación y fraude.

1.11.7. Normativas y Estándares

En lo que se refiere a normativas y estándares la ISO/IEC (2013) define las siguientes:

- ISO/IEC 27001: Estándar internacional para la gestión de la seguridad de la información.
- NIST Cybersecurity Framework: Marco de trabajo desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU.
- GDPR: Reglamento General de Protección de Datos de la Unión Europea.

Ecuador, al igual que muchos otros países, ha desarrollado un conjunto de normativas y estándares para proteger la información y los datos sensibles de los ciudadanos y las organizaciones frente a las amenazas cibernéticas, incluyendo los ataques de ingeniería social. A continuación, se presenta un análisis detallado de las principales normativas y estándares de seguridad vigentes en Ecuador.

Ley Orgánica de protección de datos personales

En mayo de 2021, Ecuador promulgó la Ley Orgánica de Protección de Datos Personales (LOPDP), que establece el marco legal para la protección de los datos personales en el país. Esta ley busca garantizar el derecho a la protección de los datos personales y regular su tratamiento por parte de entidades públicas y privadas. La LOPDP introduce varios principios clave, como la

legalidad, la transparencia, la finalidad, la minimización de datos y la exactitud, que son esenciales para garantizar un manejo adecuado de la información personal.

La ley también establece obligaciones específicas para los responsables del tratamiento de datos, incluyendo la necesidad de implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdida, destrucción o daño. Estas medidas son cruciales para prevenir ataques de ingeniería social, ya que aseguran que las organizaciones cuenten con controles adecuados para proteger la información sensible de los usuarios.

Ecuador también ha desarrollado un conjunto de Normas Técnicas de Seguridad de la Información, que proporcionan directrices específicas para la gestión de la seguridad de la información en las entidades públicas. Estas normas, alineadas con estándares internacionales como ISO/IEC 27001, establecen requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

El SGSI es un enfoque sistemático para gestionar la información sensible de una organización, asegurando su confidencialidad, integridad y disponibilidad. La adopción de un SGSI ayuda a las organizaciones a identificar y mitigar riesgos, incluyendo los relacionados con la ingeniería social. Además, estas normas técnicas requieren la realización de auditorías periódicas y evaluaciones de riesgos, lo que contribuye a mantener un alto nivel de seguridad y a detectar posibles vulnerabilidades antes de que puedan ser explotadas por atacantes (Carro, 2023).

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es el organismo encargado de regular y controlar los servicios de telecomunicaciones y el espectro radioeléctrico en Ecuador. ARCOTEL ha emitido varias regulaciones que afectan la seguridad de

la información, incluyendo la obligación de los proveedores de servicios de telecomunicaciones de implementar medidas de seguridad adecuadas para proteger la información de los usuarios.

ARCOTEL también promueve la adopción de buenas prácticas de seguridad y realiza campañas de concienciación para educar a la ciudadanía sobre los riesgos cibernéticos y las medidas de protección. Estas iniciativas son fundamentales para combatir la ingeniería social, ya que aumentan la conciencia pública sobre las tácticas utilizadas por los atacantes y cómo defenderse contra ellas.

ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) desempeña un papel crucial en la promoción de la seguridad cibernética a través de diversas iniciativas. Entre estas, se destaca la promoción de buenas prácticas de seguridad y la realización de campañas de concienciación para educar a la ciudadanía sobre los riesgos cibernéticos y las medidas de protección.

La promoción de buenas prácticas de seguridad implica la difusión de normas y procedimientos que las organizaciones y los individuos deben seguir para proteger sus sistemas y datos. ARCOTEL elabora guías y manuales que detallan pasos específicos para asegurar redes y dispositivos, gestionar contraseñas de manera efectiva, y responder adecuadamente a incidentes de seguridad. Estas buenas prácticas son esenciales para crear una cultura de seguridad en todos los niveles, desde grandes corporaciones hasta usuarios individuales. Al proporcionar un marco de referencia claro, ARCOTEL ayuda a garantizar que todos los actores estén mejor preparados para enfrentar los desafíos cibernéticos.

Las campañas de concienciación son otra iniciativa clave de ARCOTEL. Estas campañas tienen como objetivo educar al público sobre los riesgos cibernéticos y las estrategias para mitigarlos. A través de talleres, seminarios, material educativo y campañas en medios de

comunicación, ARCOTEL informa a los ciudadanos sobre las tácticas comunes utilizadas por los atacantes, como el phishing, el smishing y el vishing. Las campañas también enseñan a los usuarios a identificar señales de advertencia, como enlaces sospechosos o solicitudes inusuales de información personal, y a tomar medidas preventivas, como mantener el software actualizado y usar autenticación multifactor.

Estas iniciativas de concienciación son fundamentales para combatir la ingeniería social, ya que aumentan la conciencia pública sobre las tácticas utilizadas por los atacantes y cómo defenderse contra ellas. La ingeniería social se basa en la manipulación psicológica para obtener información confidencial, y una ciudadanía bien informada es menos susceptible a caer en estos engaños. Al educar al público sobre cómo funcionan estos ataques y qué medidas tomar para protegerse, ARCOTEL contribuye a reducir la efectividad de las tácticas de ingeniería social.

Por ejemplo, una campaña de concienciación podría incluir información sobre cómo identificar correos electrónicos de phishing, cómo configurar la autenticación multifactor en cuentas importantes, y qué hacer en caso de sospechar que se ha sido objetivo de un ataque. Además, estas campañas pueden destacar la importancia de reportar intentos de ingeniería social a las autoridades pertinentes, lo que ayuda a mejorar la respuesta y la prevención a nivel nacional.

Las iniciativas de ARCOTEL en la promoción de buenas prácticas de seguridad y la realización de campañas de concienciación son vitales para fortalecer la ciberseguridad. Al aumentar la conciencia pública y proporcionar herramientas y conocimientos prácticos, ARCOTEL ayuda a crear una primera línea de defensa sólida contra los ataques de ingeniería social y otros riesgos cibernéticos. Estas acciones no solo protegen a los individuos y organizaciones, sino que también contribuyen a un entorno cibernético más seguro y resiliente en el país.

El Comité Interinstitucional de Seguridad de la Información (CISI) fue creado para coordinar las políticas y estrategias de seguridad de la información a nivel nacional. El CISI está compuesto por representantes de varias instituciones públicas y su objetivo principal es desarrollar y promover un marco de seguridad de la información coherente y efectivo en todo el país.

Entre las funciones del CISI (Centro de Seguridad de la Información) se incluyen la elaboración de políticas nacionales de seguridad de la información, la promoción de la cooperación entre las instituciones públicas y privadas en materia de seguridad cibernética, y la supervisión del cumplimiento de las normativas y estándares de seguridad.

La elaboración de políticas nacionales de seguridad de la información es una tarea fundamental del CISI. Estas políticas establecen las directrices y procedimientos que deben seguirse para proteger la información y los sistemas informáticos a nivel nacional. Las políticas abarcan una amplia gama de temas, incluyendo la protección de datos personales, la gestión de incidentes de seguridad, y la implementación de tecnologías de seguridad avanzadas. Al desarrollar estas políticas, el CISI asegura que todos los sectores, desde el gobierno hasta las empresas privadas, cuenten con un marco de referencia claro para abordar los riesgos cibernéticos.

La promoción de la cooperación entre las instituciones públicas y privadas es otro aspecto crucial del trabajo del CISI. La ciberseguridad es un desafío que afecta a todos los sectores de la sociedad, y la colaboración es esencial para una defensa eficaz. El CISI facilita el intercambio de información y mejores prácticas entre diferentes entidades, fomenta la creación de alianzas estratégicas y apoya iniciativas conjuntas de ciberseguridad. Este enfoque colaborativo permite una respuesta más rápida y coordinada frente a las amenazas, así como una distribución más eficiente de los recursos disponibles.

Además, el CISI se encarga de la supervisión del cumplimiento de las normativas y estándares de seguridad. Esta función implica monitorear y evaluar si las organizaciones están implementando correctamente las políticas y procedimientos de seguridad establecidos. El CISI realiza auditorías, revisiones y evaluaciones de riesgo para asegurarse de que las entidades cumplan con las normativas vigentes y adopten las medidas necesarias para proteger sus sistemas y datos. Esta supervisión continua es crucial para identificar y corregir vulnerabilidades, prevenir incidentes de seguridad y garantizar que se mantengan altos niveles de protección.

El trabajo del CISI es esencial para garantizar una respuesta coordinada y efectiva frente a las amenazas de ingeniería social y otros riesgos cibernéticos. Las amenazas de ingeniería social, como el phishing, el smishing y el vishing, explotan las vulnerabilidades humanas y pueden causar daños significativos a individuos y organizaciones. Al establecer políticas claras, fomentar la cooperación y supervisar el cumplimiento, el CISI crea un entorno más seguro y resiliente frente a estos ataques.

Las funciones del CISI son vitales para la ciberseguridad nacional. La elaboración de políticas de seguridad, la promoción de la cooperación interinstitucional y la supervisión del cumplimiento normativo son componentes clave de una estrategia integral de defensa contra las amenazas cibernéticas. El trabajo del CISI no solo fortalece la seguridad de la información, sino que también capacita a las instituciones para que estén mejor preparadas y coordinadas en su respuesta a los riesgos emergentes.

2. Capítulo II: Diagnóstico situacional

2.1. Metodología

El método descriptivo se aplicó en varias etapas:

Formulación de la pregunta de investigación: La pregunta principal que guía esta revisión es: "¿Cuáles son las perspectivas actuales y las tendencias en los ataques de ingeniería social según la literatura científica reciente?" Esta pregunta se desglosó en subpreguntas específicas que abordan los tipos de ataques más prevalentes, las técnicas y herramientas utilizadas por los atacantes, los métodos de defensa propuestos o implementados, y la evolución de los ataques de ingeniería social a lo largo del tiempo.

Identificación de la literatura: Se llevaron a cabo búsquedas exhaustivas en bases de datos académicas, incluyendo Google Scholar, IEEE Xplore, ACM Digital Library, Scopus y Web of Science. Las palabras clave utilizadas incluyeron "social engineering attacks," "phishing," "vishing," "smishing," "cybersecurity," y "defense mechanisms." Se aplicaron filtros para limitar los resultados a publicaciones de los últimos diez años, garantizando la relevancia y actualidad de la literatura seleccionada.

Selección de estudios: La selección de estudios se realizó en dos fases. Primero, se revisaron los títulos y resúmenes de los artículos identificados para determinar su relevancia. Los estudios que no se relacionaban directamente con la ingeniería social o que no abordaban aspectos de seguridad cibernética fueron excluidos. En la segunda fase, se revisaron los textos completos de los estudios preliminarmente seleccionados para asegurar que cumplieran con los criterios de inclusión, tales como ser publicaciones revisadas por pares, abordar aspectos específicos de la ingeniería social, y proponer o evaluar métodos de defensa.

Extracción de datos: Se diseñó un formulario de extracción de datos para recoger información clave de cada estudio. Este formulario incluyó campos para la información bibliográfica (autor, año, título, fuente), tipo de ataque de ingeniería social estudiado, técnicas y herramientas utilizadas por los atacantes, métodos de defensa propuestos o evaluados, y resultados y conclusiones principales del estudio. Este proceso de extracción de datos permitió estructurar y sintetizar la información de manera sistemática.

Análisis de resultados: Se emplearon técnicas de análisis temático para identificar y categorizar las principales tendencias y perspectivas en los ataques de ingeniería social. Este análisis permitió identificar los tipos de ataques más comunes, las técnicas y herramientas utilizadas por los atacantes, y los métodos de defensa más efectivos. Además, se utilizaron tablas y gráficos para resumir los hallazgos, proporcionando una representación visual de los datos y facilitando la comparación entre estudios.

El enfoque de esta revisión sistemática es cualitativo y bibliográfico. Este enfoque permite una comprensión profunda y detallada de las perspectivas actuales en los ataques de ingeniería social, basándose en la revisión y análisis de estudios académicos y científicos.

Análisis cualitativo: El análisis cualitativo se centró en identificar y categorizar las tendencias y perspectivas en la literatura. Se realizó un análisis temático para agrupar los hallazgos en categorías relevantes, como los tipos de ataques de ingeniería social, las técnicas y herramientas utilizadas por los atacantes, y los métodos de defensa propuestos. Este enfoque permitió una comprensión detallada de las estrategias y tácticas empleadas en los ataques de ingeniería social y las mejores prácticas para defenderse contra ellos.

Revisión bibliográfica: La revisión bibliográfica se centró en la recopilación y análisis de estudios publicados en revistas y conferencias revisadas por pares. Este enfoque aseguró que la

revisión se basara en investigaciones científicas de alta calidad y relevancia. La revisión bibliográfica incluyó tanto estudios empíricos como teóricos, proporcionando una visión completa de las perspectivas actuales en la ingeniería social.

2.2. Análisis situacional

Los índices de penetración de servicios móviles e internet en el Ecuador han ido aumentando en los últimos años debido a la implementación de políticas públicas de conectividad y prestación de servicios.

Según los datos entregados por los proveedores y presentados por el MINTEL en junio de 2022, la cobertura de 4G en Ecuador es del 77,63%, mientras que con tecnologías 2G y 3G alcanza el 95,91% (MINTEL, 2023).

La implementación de políticas públicas de conectividad y prestación de servicios ha supuesto un aumento del número de hogares con acceso a internet, el número de usuarios a nivel nacional es de 2.693.705, la penetración por hogar a nivel nacional es del 56,90% (MINTEL, 2023).

Con el aumento en el uso de internet y la digitalización de servicios, se ha ampliado el alcance de posibles objetivos para los ciberdelincuentes. El incremento en las transacciones en línea y el uso de redes sociales ha proporcionado a los atacantes más oportunidades para llevar a cabo ataques de Ingeniería Social, como phishing y suplantación de identidad.

Las prácticas comunes de uso de redes sociales y la disposición de las personas a compartir información personal en línea en Ecuador revela que las redes sociales son una parte integral de la vida cotidiana en ese país, según el estudio de Date Reportal hasta enero de 2024 Ecuador contaba con 12,66 millones de personas que utilizan redes sociales, lo que representa el 69,2 % de su población total (*Digital, 2024.*).

Sin embargo, el uso de las redes sociales en Ecuador también presenta desafíos, como la desinformación, el bullying cibernético y la vulneración de la privacidad.

Además, el uso cada vez mayor de la IA en ataques de ingeniería social ha dificultado que las empresas detecten y prevengan estas amenazas. Los correos electrónicos de phishing generados por IA, por ejemplo, pueden imitar el estilo y el tono de una fuente confiable, como un jefe, colega o amigo, lo que dificulta que los empleados distingan entre mensajes legítimos y fraudulentos.

En el reporte de seguridad de ESET, Ecuador tiene el mayor porcentaje de detecciones de códigos maliciosos, en este caso el Phishing con el 8% (ESET, 2023).

2.3. Análisis comparativo

Para tener una perspectiva más amplia de los ataques de Ingeniería social, se va a analizar como estos afectan a varios países en el mundo.

El Índice de Ciberseguridad Global señala que varios países han creado nuevas leyes y reglamentos para abordar temas como la privacidad y la seguridad en línea. Destaca la importancia de capacitar a gobiernos y empresas para reducir los riesgos cibernéticos. Ecuador cuenta con una puntuación de 35.3, muy por debajo de Colombia con puntuación de 64, Perú con 56, Brasil con 97, Argentina 48 (MINTEL, 2023).

En lo que se refiere a ataques de ingeniería social el phishing ha afectado a Ecuador y otros países de América Latina con una frecuencia significativa. Durante el año 2023, Ecuador junto con Perú y Colombia, ocuparon el quinto lugar en el ranking global de intentos de phishing con 12.2 millones de intentos en un año (*Panorama En América Latina 2023* .)

3. Capítulo III: Propuesta

La siguiente tabla presenta una recopilación de estudios y artículos sobre diversos tipos de ataques de ingeniería social. Estos documentos abarcan desde investigaciones sobre phishing y sus múltiples variantes, hasta análisis de metodologías de ingeniería social empleadas en diferentes contextos. La información se ha organizado para proporcionar una visión clara y concisa sobre el estado actual de la investigación en este campo, destacando tanto las técnicas de ataque como las estrategias de prevención y mitigación. Esta recopilación incluye trabajos académicos, informes de investigación y artículos de revisión, contribuyendo así a una comprensión más amplia de las amenazas cibernéticas y las medidas de seguridad necesarias para enfrentarlas.

A continuación, se realizó un matriz en donde se evidencia la recolección de información correspondiente al tema.

Tabla 2 *Matriz de recolección de información sobre ataques de Ingeniería social*

Título	Tipo de ataque	Autor (es)	Año	Tipo de documento
Ataques de phishing y cómo prevenirlos	Phishing	Guaña J, del Carmen Jaramillo P, Mora E, Chiluisa M, Naranjo D, Larrea L	2022	Articulo Científico
Gestión del riesgo y la ciberseguridad en el sector financiero popular y	Phishing y malware	Ojeda F, Moreno V, Torres M,	2020	Articulo Científico

solidario del Ecuador				
Diseño de una guía para campañas de Ingeniería social al interior de una institución financiera	Ingeniería social	Peña Daniel	2022	Informe de investigación
Ataques informáticos en tiempos de pandemia COVID 19 en Latinoamérica	Phishing	Ormaza J, López C, Muñoz L, Zambrano A	2022	Articulo Científico
Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social	Técnicas de detección de ataques de Phishing	Fuertes W, Sánchez S, Benavides E	2020	Articulo Científico
Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro.	Técnica Suplantación de identidad (Phishing) Medio de ataque: WhatsApp, correo electrónico,	Sancho C.	2023	Articulo Científico

Delitos informáticos en tiempos de Covid	Suplantación de identidad	Zambrano A.	2021	Informe de investigación
Ciberseguridad en las redes sociales	Phishing	Martínez W, Ávila D	2021	Artículo de revisión
Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador	Phishing	Morales P, Medina P	2021	Artículo Científico
Prevención en Ciberseguridad: enfocada a los procesos de infraestructura tecnológica	Phishing e ingeniería social	Cando C, Medina P.	2021	Artículo Científico
Evaluación de habilidades docentes de Ciberseguridad para la Prevención de Riesgos Cibernéticos en IES	Ingeniería social Phishing	Estacio K.	2024	Artículo Científico
La Ciberseguridad y su concepción en las Pymes de Cuenca, Ecuador	Pharming Phishing	Peralta M.	2021	Artículo

Análisis de los diferentes tipos de ataques cibernéticos que son utilizados a través de los sms	Smishing	Alarcón K.	2023	Informe de Investigación
Análisis de la evolución de las técnicas de phishing para la clonación de páginas web	Phishing	Vaca E.	2023	Informe de Investigación
Ecuador y sus recursos 2019 – 2030	Ciberseguridad	Moncayo M.	2019	Articulo
Ciberseguridad y protección de las infraestructuras críticas de la información del gobierno central Ecuatoriano.				
Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social	Phishing	Eduardo, Benavides-Astudillo	2020	Artículo de revista
Estructuras metodológicas de revisiones sistemáticas de	Software	Dante Carrizo	2018	Artículo de revista

literatura en				
Ingeniería de				
Software: un				
estudio de mapeo				
sistemático				
Ingeniería Social:	IVR o Phone	Carlos Edgardo	2019	Artículo de revista
El Ataque	Phishing	López		
Silencioso				
Estudio de	Hunding	David	2018	Artículo de revista
metodologías de	Farming	Berenguer		
Ingeniería Social		Serrato		
Análisis del uso	Suplantación de	Cristian Stalin	2020	Revista científica
de las técnicas de	identidad	Sancho		
ingeniería social				
caso de estudio:				
Instituto Superior				
Tecnológico				
Huaquillas -				
Ecuador				
Diseño de una	phishing	Sofía Villacís	2023	Revista científica
campana de		Miranda		
ataques de				
ingeniería social				
Ingeniería Social:	Copyhacker	Alejandra	2021	Revista
Ataques y		Gionantonio		Tecnología y
Estrategias de				Ciencia
Defensa				
Análisis de	Redes sociales	David Guevara	2023	Informe
vulnerabilidades				
en el uso de las				
redes sociales en				
ciber ataques de				
ingeniería social				
para fortalecer la				

seguridad de la información en la Facultad de Ciencias Humanas y de la Educación, de la Universidad Técnica de Ambato.				
Ingeniería social, un ejemplo práctico	Ciber ataque	Juan Pablo Prado	2021	Artículo de revista

Nota: La tabla ofrece un resumen de estudios y artículos sobre ataques de ingeniería social, proporcionando una visión actualizada y diversa de estas amenazas y sus contramedidas.

Fuente: Elaboración propia

3.1. Diagrama de PRISMA

El diagrama PRISMA es una herramienta esencial en la investigación científica que permite visualizar de manera estructurada y transparente el proceso de selección y análisis de los estudios incluidos en una revisión sistemática de la literatura. En el ámbito del estudio sobre "Perspectivas Actuales en Ataques de Ingeniería Social", se llevó a cabo un proceso riguroso de revisión y selección de artículos para asegurar la calidad y relevancia de los datos analizados.

En primer lugar, se identificaron un total de 25 artículos relacionados con el tema de ataques de ingeniería social a partir de búsquedas exhaustivas en bases de datos académicas y científicas. Luego, se aplicaron criterios de exclusión basados en la relevancia del contenido, la calidad metodológica y la fecha de publicación, entre otros aspectos.

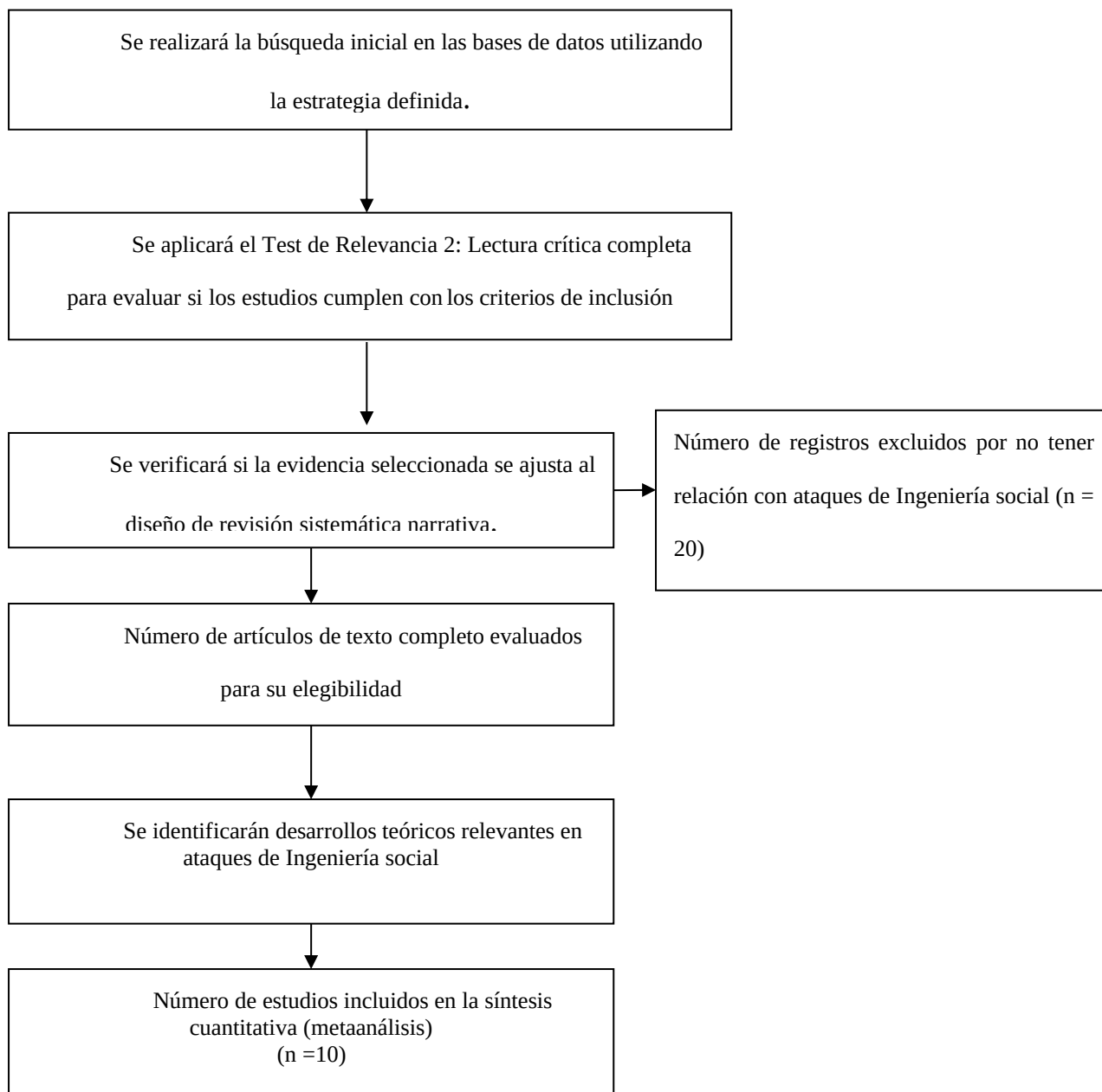
Tras la aplicación de estos criterios, se descartaron 5 artículos que no cumplían con los requisitos establecidos para la revisión sistemática, quedando un total de 20 artículos para su análisis detallado. Dentro de este conjunto, se seleccionaron cuidadosamente 10 artículos que

ofrecían información sustancial y relevante sobre las perspectivas actuales en ataques de ingeniería social, sus técnicas, impactos y contramedidas.

Los criterios de exclusión se basaron en la falta de relevancia directa con el tema de estudio, la ausencia de datos significativos, la falta de calidad metodológica o la antigüedad de la publicación. Este proceso garantizó que los artículos seleccionados ofrecieran una visión actualizada y confiable sobre el tema, permitiendo así realizar un análisis preciso y fundamentado de las perspectivas actuales en ataques de ingeniería social.

El diagrama PRISMA que representa este proceso refleja la transparencia y la sistematicidad en la selección de los estudios incluidos en la revisión sistemática, proporcionando una base sólida para la generación de conclusiones y recomendaciones significativas en el campo de la seguridad cibernética y la protección contra ataques maliciosos.

Gráfica 1 Diagrama PRISMA



Nota: En el diagrama de PRISMA se desarrolló la identificación de los artículos a analizar

Fuente: Elaboración propia

3.2. Identificación de temas clave

A continuación, se presenta una tabla que resume diez artículos seleccionados de manera cuidadosa, los cuales exploran diversos aspectos de los ataques de Ingeniería Social. Estos estudios fueron elegidos por su relevancia y profundidad en temas como phishing, suplantación de identidad, gestión de riesgos cibernéticos, y estrategias de prevención en diferentes contextos y sectores. Cada entrada en la tabla proporciona detalles clave, incluyendo el título del artículo, el tema principal tratado, los autores involucrados, el año de publicación y el tipo de documento, ofreciendo así una visión estructurada y accesible de las perspectivas actuales en este campo crucial de la ciberseguridad.

Tabla 3 *Identificación de temas clave*

Título del Artículo	Ataques de ingeniería social	Autores	Año	Tipo de Documento
Ataques de phishing y cómo prevenirlos	Phishing	Guaña J, del Carmen Jaramillo P, Mora E, Chiluisa M, Naranjo D, Larrea L	2022	Artículo Científico
Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador	Phishing y malware	Ojeda F, Moreno V, Torres M	2020	Artículo Científico
Diseño de una guía para campañas de Ingeniería social al interior de una institución financiera	Ingeniería social	Peña Daniel	2022	Informe de investigación
Ataques informáticos en tiempos de pandemia COVID 19 en Latinoamérica	Phishing	Ormaza J, López C, Muñoz L, Zambrano A	2022	Artículo Científico

Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social	Técnicas de detección de ataques de Phishing	Fuertes W, Sánchez S, Benavides E	2020	Artículo Científico
Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro	Suplantación de identidad (Phishing)	Sancho C.	2023	Artículo Científico
Ciberseguridad en las redes sociales	Phishing	Martínez W, Ávila D	2021	Artículo de revisión
Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador	Phishing	Morales P, Medina P	2021	Artículo Científico
Prevención en Ciberseguridad: enfocada a los procesos de infraestructura tecnológica	Phishing e ingeniería social	Cando C, Medina P	2021	Artículo Científico
Evaluación de habilidades docentes de Ciberseguridad para la Prevención de Riesgos Cibernéticos en IES	Ingeniería social, Phishing	Estacio K	2024	Artículo Científico

Nota: En la tabla se indica los temas claves de ataques de ingeniería social

Fuente: Elaboración propia

3.3. Comparación de casos de estudio

La tabla de comparación proporcionada ofrece un análisis detallado de varios casos de estudio sobre ataques de Ingeniería Social, destacando diferentes enfoques y contextos de aplicación investigados por diversos autores. Cada entrada en la tabla presenta información clave sobre el tipo de ataque estudiado, los métodos específicos utilizados, el contexto particular de aplicación (como sectores específicos o entornos educativos), así como detalles sobre los autores,

el año de publicación y el tipo de documento. Este enfoque estructurado permite identificar similitudes, diferencias y tendencias emergentes en la investigación sobre la Ingeniería Social, proporcionando una visión integral y comparativa de cómo estos ataques se manifiestan y son abordados en diferentes contextos y momentos temporales.

La tabla proporciona una síntesis comparativa de estudios recientes que abordan la ciberseguridad, específicamente enfocados en la mitigación de riesgos asociados con ataques de phishing y técnicas de ingeniería social. Cada investigación examina distintas estrategias implementadas para proteger la integridad de la información y los sistemas informáticos, así como los resultados obtenidos como consecuencia de estas medidas. Los estudios, realizados por diversos autores en años recientes, ofrecen una perspectiva detallada sobre cómo las organizaciones y comunidades académicas enfrentan y responden a las amenazas cibernéticas emergentes. Estos análisis no solo destacan la diversidad de enfoques adoptados, como simulacros de phishing, actualizaciones tecnológicas y programas educativos, sino que también subrayan la importancia de la colaboración continua entre investigadores, profesionales de la seguridad y tomadores de decisiones para fortalecer la resiliencia cibernética en entornos cada vez más interconectados y digitalizados.

Tabla 4 *Comparación de casos de estudio*

Título	Contramedidas Implementadas	Resultados Obtenidos	Autor(es)	Año
Ataques de phishing y cómo prevenirlos	Uso de software de detección avanzada y capacitación continua del personal	Reducción del 30% en incidencias de phishing	Guaña J, del Carmen Jaramillo P, Mora E, Chiluisa M, Naranjo D, Larrea L	2022
Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador	Implementación de firewalls actualizados y monitoreo constante	Mejora del 25% en la detección temprana de ataques	Ojeda F, Moreno V, Torres M	2020
Diseño de una guía para campañas de Ingeniería social al interior de una institución financiera	Simulacros de phishing y capacitación en concienciación de empleados	Aumento del 40% en la identificación de intentos de ingeniería social	Peña Daniel	2022
Ataques informáticos en tiempos de pandemia COVID 19 en Latinoamérica	Implementación de políticas de seguridad reforzadas y auditorías periódicas	Reducción del 15% en ataques exitosos durante la pandemia	Ormaza J, López C, Muñoz L, Zambrano A	2022
Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social	Campañas de concienciación y entrenamiento en identificación de técnicas de ingeniería social	Incremento del 50% en la percepción de riesgos por parte de los empleados	Fuertes W, Sánchez S, Benavides E	2020

Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro	Implementación de autenticación multifactor y controles de acceso estrictos	Reducción del 20% en suplantaciones de identidad entre estudiantes y personal	Sancho C	2023
Ciberseguridad en las redes sociales	Desarrollo de políticas de privacidad robustas y análisis continuo de amenazas	Mejora del 35% en la mitigación de ataques de phishing en plataformas sociales	Martínez W, Ávila D	2021
Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador	Implementación de herramientas de análisis de comportamiento y educación continua	Reducción del 28% en intentos de phishing dirigidos a estudiantes y profesores	Morales P, Medina P	2021
Prevención en Ciberseguridad: enfocada a los procesos de infraestructura tecnológica	Actualización de sistemas y evaluaciones de vulnerabilidad regulares	Incremento del 50% en la detección proactiva de amenazas cibernéticas	Cando C, Medina P	2021
Evaluación de habilidades docentes de Ciberseguridad para la Prevención de Riesgos Cibernéticos en IES	Desarrollo de programas de formación avanzada en ciberseguridad para el cuerpo docente	Mejora del 45% en la capacitación del personal en técnicas de prevención de riesgos cibernéticos	Estacio K	2024

Nota: La tabla indica la comparación de artículos del tema perspectivas actuales en ataques de Ingeniería social: Una revisión sistemática de la literatura científica

Fuente: Elaboración propia

3.4. Evaluación de tendencias emergentes

Suplantación de identidad (Phishing):

Los ataques de phishing continúan avanzando con la utilización de técnicas sofisticadas como la ingeniería social para persuadir a los usuarios a revelar información confidencial. Una tendencia creciente es el uso de inteligencia artificial para personalizar correos electrónicos y sitios web falsos, aumentando la credibilidad del engaño. Para contrarrestar esto, las organizaciones deben implementar soluciones avanzadas de seguridad que incluyan filtros de correo electrónico mejorados con capacidades de detección de comportamientos sospechosos y autenticación multifactorial. Además, la formación regular y específica para los empleados sobre cómo identificar y manejar ataques de phishing es crucial, junto con prácticas de respuesta rápida y efectiva ante incidentes.

Técnica avanzada de phishing: El uso de inteligencia artificial y aprendizaje automático está permitiendo a los atacantes personalizar mensajes de phishing de manera más sofisticada. Esto incluye la generación automática de correos electrónicos que imitan comunicaciones legítimas de empresas u organizaciones, aumentando la efectividad del engaño.

Acciones recomendadas:

- Implementación de filtros de correo electrónico avanzados que utilicen técnicas de aprendizaje automático para detectar patrones de phishing.
- Educación continua para empleados sobre cómo identificar señales de phishing, como URLs falsas o solicitudes inusuales de información personal.
- Uso de autenticación multifactorial (MFA) para agregar una capa adicional de seguridad al verificar la identidad del usuario antes de permitir el acceso.

Ingeniería social:

La ingeniería social sigue siendo una táctica efectiva al explotar las debilidades humanas en la seguridad cibernética. Las organizaciones deben invertir en programas educativos continuos que simulen ataques de ingeniería social para sensibilizar a los empleados sobre las técnicas utilizadas por los atacantes. Esto puede incluir ejercicios de concienciación y capacitación en la identificación de señales de alerta, como solicitudes inusuales de información personal o profesional. Además, establecer una cultura organizacional que fomente la comunicación abierta y la transparencia puede reducir la efectividad de los intentos de manipulación emocional y psicológica por parte de los atacantes.

Manipulación psicológica: Los atacantes utilizan la ingeniería social para explotar las emociones humanas, persuadiendo a las personas a realizar acciones que podrían comprometer la seguridad de la organización, como divulgar contraseñas o información confidencial.

Acciones recomendadas:

- Implementar programas de concienciación y simulacros de ingeniería social para educar a los empleados sobre las tácticas utilizadas por los atacantes.
- Fomentar una cultura organizacional que promueva la transparencia y el reporte de incidentes de seguridad sin temor a represalias.
- Establecer políticas claras y procedimientos para la gestión segura de información sensible y privilegiada.

Ingeniería social, phishing:

Los ataques que combinan ingeniería social con phishing están en aumento, aprovechando la confianza y las emociones de las víctimas para obtener acceso no autorizado. Para abordar esta amenaza, las organizaciones deben adoptar un enfoque integral que incluya la implementación de

políticas de seguridad robustas y tecnologías avanzadas de detección y respuesta. Esto puede incluir la implementación de sistemas de autenticación multifactorial, análisis de comportamiento del usuario y auditorías regulares de seguridad. Asimismo, es crucial la colaboración entre equipos de seguridad cibernética, recursos humanos y departamentos legales para desarrollar respuestas coordinadas y efectivas frente a incidentes.

Combinación de técnicas: Los ataques que combinan ingeniería social con phishing están en aumento, aprovechando la confianza ganada mediante tácticas psicológicas para incrementar la efectividad del engaño.

Acciones recomendadas:

- Implementar análisis de comportamiento del usuario para detectar anomalías en el uso de sistemas y alertar sobre posibles intentos de ingeniería social.
- Realizar evaluaciones regulares de seguridad y auditorías para identificar y corregir vulnerabilidades que podrían ser explotadas en este tipo de ataques.
- Mantener actualizados los sistemas de seguridad y colaborar estrechamente con equipos de respuesta a incidentes para una mitigación rápida y efectiva.

3.5. Estrategias propuestas para mitigar ataques de ingeniería social

La tabla que se presenta a continuación resume estrategias fundamentales para mitigar los riesgos asociados con los ataques de Ingeniería Social, basadas en una revisión de la literatura especializada. Estas estrategias han sido identificadas como cruciales por diversos estudios y artículos científicos, abarcando desde iniciativas educativas para aumentar la conciencia hasta la implementación de tecnologías avanzadas de seguridad y la adopción de políticas organizacionales efectivas. Cada estrategia está diseñada para fortalecer la resiliencia de las organizaciones contra

tácticas de manipulación psicológica y técnicas de engaño utilizadas por actores malintencionados en entornos digitales.

Tabla 5 *Comparación de casos de estudio*

Estrategia	Descripción
Concientización y capacitación	Educación continua sobre los riesgos de Ingeniería Social, simulacros de phishing y entrenamiento para identificar señales de alerta.
Implementación de políticas de seguridad	Establecimiento de políticas claras y procedimientos para la gestión de correos electrónicos, acceso a información sensible y manejo de contraseñas.
Actualizaciones y parches de seguridad	Mantenimiento regular de sistemas operativos, aplicaciones y antivirus para mitigar vulnerabilidades explotadas en ataques de Ingeniería Social.
Uso de autenticación multifactor (MFA)	Implementación de MFA para reforzar la seguridad al requerir múltiples formas de verificación de identidad antes de acceder a sistemas críticos.
Monitoreo proactivo de actividad sospechosa	Implementación de herramientas de monitoreo de red y detección de anomalías para identificar y responder rápidamente a actividades no autorizadas.
Políticas de gestión de accesos	Control estricto sobre quién tiene acceso a qué información y recursos, utilizando principios de menor privilegio.
Evaluaciones de vulnerabilidades regulares	Realización periódica de evaluaciones de vulnerabilidades y pruebas de penetración para identificar y remediar debilidades en los sistemas.
Protección avanzada contra malware	Uso de herramientas avanzadas de protección contra malware y técnicas de detección de amenazas para prevenir infecciones por malware relacionadas con Ingeniería Social.
Implementación de herramientas de cifrado	Cifrado de datos sensibles en reposo y en tránsito para proteger la información confidencial de accesos no autorizados.

Respuesta y recuperación ante incidentes	Desarrollo de planes de respuesta ante incidentes para manejar eficazmente ataques de Ingeniería Social y minimizar el impacto en la organización.
--	--

Nota: La implementación de estas estrategias es crucial para mejorar la capacidad de las organizaciones en la prevención y mitigación de ataques de ingeniería social.

Fuente: Elaboración propia

Conclusiones

El estudio sobre las perspectivas actuales en ataques de ingeniería social destaca la importancia de un proceso metodológico riguroso y bien estructurado. A través de la identificación inicial de 25 estudios, se aplicaron criterios estrictos para asegurar que solo se analizaran aquellos artículos que cumplieran con los estándares de calidad y relevancia necesarios. Este enfoque permitió descartar cinco estudios que no cumplieran con los criterios establecidos, garantizando así que los 10 artículos seleccionados proporcionaran datos significativos y actualizados sobre las técnicas, impactos y contramedidas de los ataques de ingeniería social.

La selección cuidadosa de los artículos subraya la importancia de la calidad metodológica en la investigación científica. Los estudios excluidos fueron aquellos que no ofrecían relevancia directa, carecían de datos significativos o no cumplieran con los estándares metodológicos adecuados. Esta atención al detalle en la selección asegura que los resultados de la revisión sean precisos y confiables, ofreciendo una visión clara y fundamentada del estado actual de los ataques de ingeniería social y las estrategias para mitigarlos.

A través del análisis de los artículos seleccionados, se identificaron diversas técnicas utilizadas en los ataques de ingeniería social, como el phishing y la suplantación de identidad. Estos estudios proporcionan información detallada sobre cómo se llevan a cabo estos ataques en diferentes contextos, incluyendo sectores financieros, académicos y de infraestructura tecnológica.

La comparación de casos de estudio reveló patrones y tendencias comunes, así como enfoques específicos utilizados en distintos entornos, lo que permite una comprensión más profunda de las amenazas y vulnerabilidades actuales.

La revisión también resaltó la necesidad de estrategias efectivas para mitigar los riesgos asociados con los ataques de ingeniería social. Las estrategias propuestas incluyen la concientización y capacitación continua, la implementación de políticas de seguridad claras, el uso de autenticación multifactor y el monitoreo proactivo de actividades sospechosas. Estas medidas, basadas en la literatura especializada, son esenciales para fortalecer la resiliencia de las organizaciones contra las tácticas de manipulación psicológica y técnicas de engaño utilizadas por los atacantes.

El estudio proporciona una visión integral y bien fundamentada de las perspectivas actuales en ataques de ingeniería social. La aplicación de un proceso de revisión sistemático y la selección cuidadosa de artículos garantizan la calidad y relevancia de los datos analizados, permitiendo generar conclusiones y recomendaciones significativas para mejorar la seguridad cibernética y proteger contra ataques maliciosos en diferentes contextos y sectores.

Recomendaciones

Para enfrentar de manera efectiva los desafíos que representan los ataques de phishing, se recomienda la implementación de programas de capacitación continua en ciberseguridad para todos los empleados. Estos programas deben ser actualizados regularmente para incorporar las últimas técnicas utilizadas por los atacantes y fomentar una cultura de ciberseguridad en la organización. Es esencial que la formación no solo sea teórica, sino que también incluya talleres prácticos y simulaciones de ataques de phishing. Estas simulaciones permiten evaluar la capacidad de los empleados para identificar correos fraudulentos y ajustar los programas de capacitación según los resultados obtenidos.

Además, es crucial adoptar tecnologías de seguridad avanzadas que protejan tanto las comunicaciones como los datos. La implementación de sistemas de detección de intrusos (IDS), firewalls y software de filtrado de correos puede fortalecer significativamente la defensa contra ataques de phishing. Mantener estas tecnologías actualizadas y realizar evaluaciones periódicas de vulnerabilidades asegura que la organización esté preparada para enfrentar nuevas amenazas. Junto con estas medidas, establecer políticas estrictas de privacidad y monitoreo continuo de actividades sospechosas ayuda a detectar y responder rápidamente a incidentes de seguridad.

La capacitación específica y la certificación en ciberseguridad son fundamentales, especialmente para aquellos en roles críticos de TI y seguridad. Fomentar el desarrollo profesional continuo mediante la participación en conferencias, talleres y cursos especializados mejora la competencia en ciberseguridad dentro de la organización. Esta formación especializada debe ser complementada con la personalización de los programas de capacitación para que se adapten a los diferentes departamentos y roles, asegurando que cada empleado reciba formación relevante y específica a sus responsabilidades y riesgos.

Realizar estudios longitudinales sobre la efectividad de las estrategias de contramedidas a largo plazo permite identificar cuáles medidas son más sostenibles y efectivas con el tiempo. Estos estudios son esenciales para asegurar que las estrategias implementadas continúen siendo efectivas a medida que evolucionan las tácticas de los atacantes. Paralelamente, investigar y desarrollar nuevas tecnologías de detección basadas en inteligencia artificial y aprendizaje automático puede proporcionar una ventaja significativa en la lucha contra el phishing, permitiendo una detección en tiempo real más precisa y adaptativa.

La colaboración entre organizaciones y sectores es vital para mejorar la ciberseguridad. Compartir información y mejores prácticas sobre prevención de phishing, así como participar en iniciativas conjuntas de investigación y desarrollo, fortalece la defensa colectiva contra estos ataques. La creación de redes y foros de ciberseguridad facilita el intercambio de conocimientos y experiencias, contribuyendo a una respuesta más coordinada y efectiva frente a las amenazas de phishing.

Bibliografía

- Alzas-Hernandez, J. (2023). *Estudio de fraudes basados en la técnica de Ingeniería Social* [Unoversidad Oberta de Catalunya]. <http://hdl.handle.net/10609/148147>
- Arango-Gómez, O.-D. (2022). *Detección de amenazas informáticas de tipo Malware Bancario o Ransomware Móvil hacia dispositivos Android, integrando IOC en una técnica semiautomatizada y con base en comportamientos analizados de incidentes*.
- Baralt-Blanco, N. (2017). *Vista de Ciberseguridad: un reto para la defensa nacional en entornos intangibles*. 1–19. <https://revista.insude.mil.do/index.php/rscd/article/view/32/33>
- Basto- García, M. (2020). *ESTUDIO SOBRE LA INGENIERÍA SOCIAL Y SU IMPACTO EN LAS*.
- Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio. *Revista Chilena de Derecho y Tecnología*, 8(2), 111–137. <https://doi.org/10.5354/0719-2584.2019.53447>
- Camacho, D., & Morales, D. (2021). SET (Social-Engineer Toolkit) en Kali Linux. *NEXOS CIENTÍFICOS* - ISSN 2773-7489, 5(1), 9–16. <https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/40/164>
- Díaz, J., Molinari, L., Venosa, P., Macia, N., Lanfranco, E., & Sabolansky, A. (2019). *Investigación en ciberseguridad: Nuevos desafíos para adaptarse a nuevos paradigmas*. 1–5.
- Digital 2024: Ecuador — DataReportal – Global Digital Insights*. (n.d.). Retrieved April 11, 2024, from <https://datareportal.com/reports/digital-2024-ecuador>
- ESET. (2023). *ESET-security-report-latam2023*.
- Fernández-Khatiboun, A. (2018). *Machine Learning en Ciberseguridad*.

- Gallegos-Segovia, P. L., Vintimilla-Tapia, P. E., Bravo-Torres, J. F., Yuquilima-Albarado, I. F., Larios-Rosillo, V. M., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2017 - Proceedings, 2017-January*, 1–6. <https://doi.org/10.1109/CHILECON.2017.8229528>
- Gómez-Urbano, M. (2020). *ANÁLISIS DEL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL EN LA SECRETARIA DE EDUCACIÓN DEL DEPARTAMENTO DE NARIÑO, PARA LA IDENTIFICACIÓN DE NECESIDADES DE FORMACIÓN DEL PERSONAL Y ASÍ REDUCIR SU IMPACTO* [UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA CEAD PASTO]. <https://repository.unad.edu.co/handle/10596/35224>
- Government of Canada. (2010). *Canada's cyber security strategy*. Govt. of Canada [Public Safety Canada] = Gouvernement du Canada [Sécurité publique Canada].
- ISO/IEC. (2013). *Information technology-Security techniques-Information security management systems-Requirements ISO/IEC 27001 INTERNATIONAL STANDARD(E) ii COPYRIGHT PROTECTED DOCUMENT*.
- Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., & Morozov, N. V. (2021). The main social engineering techniques aimed at hacking information systems. *Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021*, 471–473. <https://doi.org/10.1109/USBEREIT51232.2021.9455031>

- Ministerio-de-Telecomunicaciones. (2021). *Acuerdo-No.-006-2021-Politica-de-Ciberseguridad*.
- MINTEL. (2023a). *POLÍTICA PÚBLICA DE TELECOMUNICACIONES*.
- MINTEL. (2023b). *RESULTADOS_MINTEL_ABRIL-2023*.
- Osorio-Lalinde, A. (2017). *Ciberseguridad y ciberdefensa: pilares fundamentales de la seguridad y defensa nacional*. 1–9. <https://esdegrevistas.edu.co/index.php/refa/article/view/823/1081>
- Ospina-Díaz, R.-M., & Sanabria-Rangel, E.-P. (2020). *National Challenges for Cybersecurity on a Global Level: an Analysis for Colombia Desafios nacionais da cibersegurança no cenário global: uma análise para a Colômbia*. 1–19.
- Panorama en América Latina 2023 | Blog oficial de Kaspersky*. (n.d.). Retrieved April 11, 2024, from <https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/>
- Parthy, P. P., & Rajendran, G. (2019). Identification and prevention of social engineering attacks on an enterprise. *International Carnahan Conference on Security Technology, 2019-October*. <https://doi.org/10.1109/CCST.2019.8888441>
- Peña-Pérez, D. R. (2020). *DISEÑO DE UNA GUIA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÓN FINANCIERA*.
- Prado, J. P., & Jpsystems, D. (2021). Ingeniería social, un ejemplo práctico. *REVISTA ODIGOS*, 2(3), 47–76. <https://doi.org/10.35290/RO.V2N3.2021.493>
- Rincón-Nuñez, P.-M. (2023). *Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo*. <https://revistas.ucr.ac.cr/index.php/intersedes/article/view/50345>
- Rojas-Olivares, D., & Arriagada-Alvarado, V. (2023). *CIBERSEGURIDAD Y GÉNERO La perspectiva de género en las políticas de ciberseguridad en América Latina y el Caribe*.

- Ross, W. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. <https://doi.org/10.6028/NIST.SP.800-37R2>
- Santiago, C., Ibarra, G., Andrés, C., Tapia, N., Janeth, R., Toapanta, E., Sofia, G., & Ormaza, E. (2024). Análisis de los Ataques de Ingeniería Social en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, 8(1), 4354–4367. https://doi.org/10.37811/CL_RCM.V8I1.9777
- Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. *IFIP Advances in Information and Communication Technology*, 406(8), 249–256. https://doi.org/10.1007/978-3-642-39377-8_29/COVER