



**UNIVERSIDAD
CATÓLICA DE CUENCA**

MAESTRÍA EN CIBERSEGURIDAD

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

Tema: Evolución de técnicas de ataques de phishing y contramedidas: Una
revisión de literatura

Autor: Ing. Javier Ricardo Ortiz Casillas

Tutor: Ing. Miguel Andrade López. Mg.

Cuenca – Ecuador

2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Evolución de técnicas de ataques de phishing y contramedidas: Una revisión de literatura”, de autoría de la Señor Ingeniera de Sistemas Javier Ricardo Ortiz Casillas, CC: 1715860381, 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:

“Evolución de técnicas de ataques de phishing y contramedidas: Una revisión de literatura.”, 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. Javier Ricardo Ortiz Casillas

CC: 1715860381

Agradecimiento

En primer lugar, agradezco a Dios por haberme guiado y fortalecido en cada etapa de este proceso. Su presencia me ha dado la sabiduría y la serenidad necesarias para superar los desafíos, y por su gracia he podido alcanzar este logro.

Quiero expresar mi más sincero agradecimiento a mis padres, cuyo amor, apoyo incondicional y sabios consejos han sido fundamentales para que hoy pueda alcanzar esta meta, su constante confianza en mí me ha dado la fuerza para seguir adelante en cada etapa del camino, y sin su sacrificio y dedicación, este logro no habría sido posible.

A mi hermana, quien ha recorrido este mismo camino académico, quiero agradecerle por ser una compañera excepcional en esta travesía, compartir esta experiencia contigo ha sido una fuente de motivación y apoyo mutuo, tu dedicación y perseverancia me han inspirado a seguir adelante, y siempre has estado allí para ofrecerme tus conocimientos y consejos valiosos.

A mis amigos, gracias por su constante apoyo, su confianza y por estar siempre dispuestos a ofrecerme palabras de aliento, su compañía ha sido un pilar importante en este camino y les agradezco por los momentos de descanso y ánimo que me ayudaron a seguir adelante.

A mis compañeros de trabajo, quienes me brindaron su comprensión y apoyo durante este proceso, su colaboración y disposición para ayudarme, tanto en lo profesional como en lo personal, fueron fundamentales para que pudiera equilibrar mis responsabilidades laborales con este proyecto.

Este trabajo es un reflejo del esfuerzo colectivo de todas las personas que han estado a mi lado, y estoy profundamente agradecido por contar con ustedes en cada paso del camino.

Dedicatoria

Dedico este trabajo a mis padres, quienes, con su ejemplo de esfuerzo y perseverancia, me han inspirado a seguir adelante en cada paso de mi vida. Su amor y dedicación han sido el motor que me impulsó a superar los desafíos y alcanzar este logro.

A mi hermana, por haber compartido conmigo este mismo camino académico. Su compañerismo y determinación han sido un reflejo de nuestra unión y apoyo mutuo. Juntos hemos enfrentado retos y hemos crecido, y este trabajo es un símbolo de ese crecimiento.

Finalmente, me dedico este logro a mí mismo, como recordatorio de todo el esfuerzo, el tiempo y la dedicación que he puesto en alcanzar esta meta. Este trabajo es el resultado de mi compromiso, mi pasión por aprender y mi capacidad para superar obstáculos.

Resumen

La interconexión de servicios electrónicos en dispositivos como impresoras y asistentes virtuales ha incrementado las brechas de seguridad, permitiendo a los ciberdelincuentes ejecutar ataques de phishing. Este fenómeno ha aumentado un 15% en el último año, afectando la privacidad de datos personales y servicios esenciales, como los sistemas de salud. La investigación se centra en la evolución de las técnicas de phishing y las medidas de seguridad en ciberseguridad, analizando cómo los atacantes utilizan tácticas de ingeniería social y exploits técnicos. Se abordarán métodos de prevención, como la educación del usuario y tecnologías avanzadas de detección basadas en inteligencia artificial. Esta investigación busca contribuir a la comprensión de la ciberseguridad, proporcionando estrategias para profesionales, responsables de políticas y educadores, con el fin de fortalecer la resiliencia cibernética. Se incluirá una revisión de la literatura, un marco teórico, metodología, procedimientos éticos y un cronograma detallado para el proyecto.

Palabras clave: phishing, ciberseguridad, ingeniería social, medidas preventivas, dispositivos IoT.

Abstract

The interconnection of electronic services in devices such as printers and virtual assistants has increased security breaches, allowing cybercriminals to execute phishing attacks. This phenomenon has risen by 15% in the past year, impacting the privacy of personal data and essential services like healthcare systems. The research focuses on the evolution of phishing techniques and security measures in cybersecurity, analyzing how attackers use social engineering tactics and technical exploits. Prevention methods, such as user education and advanced detection technologies based on artificial intelligence, will be addressed. This research aims to contribute to the understanding of cybersecurity by providing strategies for professionals, policymakers, and educators to strengthen cyber resilience. It will include a literature review, theoretical framework, methodology, ethical procedures, and a detailed project timeline.

Keywords: phishing, cybersecurity, social engineering, preventive measures, IoT devices

Índice de contenido

1.	Introducción	1
1.1.	Situación problemática	1
1.2.	Problema científico	2
1.3.	Objeto de estudio.....	3
1.4.	Campo de acción	4
1.5.	Objetivos	5
1.5.1.	Objetivo general.....	5
1.5.2.	Objetivos Específicos.....	5
1.6.	Problema científico - preguntas de investigación	5
1.6.1.	Preguntas científicas	5
1.7.	Hipótesis.....	6
1.8.	Variables.....	6
1.8.1.	Variable Independiente:	6
1.8.2.	Variables Dependientes:	6
1.9.	Justificación - contribuciones de la investigación.....	7
2.	Capítulo II	9
	Estado del arte o antecedentes	9
2.2.	Marco teórico referencial	12
2.2.1.	Phishing.....	12
2.2.2.	Historia del Phishing:.....	13
2.2.3.	Importancia de Phishing	14
2.2.4.	Evolución de las técnicas de Phishing	16
2.2.5.	Técnicas de ataques Phishing.....	17
2.2.6.	Consecuencias de los Ataques de Phishing	29

2.2.7.	Contramedidas tecnológicas actuales:	31
2.2.8.	Modelos Teóricos.....	33
2.3.	Diagnostico situacional	39
2.3.1.	Metodología	39
2.3.2.	Fase exploratoria:.....	40
2.3.3.	Selección de la muestra:.....	40
2.3.4.	Criterios de Inclusión:.....	40
2.3.5.	Criterios de Exclusión:.....	40
2.4.	Recopilación de datos cuantitativos:	41
2.5.	Recopilación de datos cualitativos:	41
2.6.	Análisis de datos cualitativos:	41
2.7.	Interpretación de los resultados:.....	42
2.8.	Línea de investigación.....	42
2.9.	Análisis situacional:	43
2.10.	Análisis comparativo:	44
3.	Capitulo III Propuesta	45
3.1.	Diagrama PRISMA	54
3.2.	Identificación de temas claves.....	57
3.3.	Comparación de casos de estudio.....	60
3.4.	Evaluación de tendencias emergentes	62
3.5.	Estrategias propuestas para mitigar los ataques de phishing.....	64
	Conclusiones	69
	Recomendaciones	71
	Bibliografía	73

Índice de contenidos

Tabla 1 Matriz de recolección de datos	45
Grafica 1 Diagrama PRISMA.....	56
Tabla 2 Identificación de temas claves	58

1. Introducción

1.1. Situación problemática

La creciente interconexión de los servicios electrónicos empleados en diversos dispositivos, como aquellos utilizados para el trabajo, la salud y el ocio, puede dar lugar a posibles brechas de seguridad (Rosero, 2021). Los ciberdelincuentes explotan las vulnerabilidades de estos dispositivos de varias maneras. Por ejemplo, un ataque puede comenzar con el envío de una señal maliciosa a un dispositivo conectado dentro de la red, como impresoras, asistentes virtuales de voz, sistemas de sonido inalámbricos, entre otros.

Estos dispositivos, muchas veces mal protegidos, se convierten en puertas de entrada para los atacantes. Un estudio reciente reveló que los ataques de phishing han aumentado un 15% en el último año, con un notable incremento en los ataques dirigidos a dispositivos IoT (Benavides, 2024).

Las consecuencias de estos ataques son variadas, incluyendo desde la pérdida de datos personales y financieros hasta la interrupción de servicios esenciales. Por ejemplo, un ataque a un sistema de salud podría comprometer la privacidad de los pacientes y afectar la prestación de cuidados médicos (Díaz, 2022).

Para contrarrestar estas amenazas, se han desarrollado diversas contramedidas. Estas incluyen la implementación de protocolos de seguridad más robustos, la educación y concienciación de los usuarios, y el uso de tecnologías avanzadas de detección de fraudes. Sin embargo, a medida que las técnicas de phishing evolucionan, también deben hacerlo las estrategias de defensa.

1.2.Problema científico

El proyecto de investigación se centra en el estudio de la evolución de las técnicas de phishing y las medidas de seguridad en el campo de la ciberseguridad, sabiendo que el phishing implica la fusión de Ingeniería Social y exploits técnico (Benavides, Fuertes, Sánchez, 2020a).

(Jancachagua, 2021) describe que el phishing, también llamado "pesca de información", emplea tácticas de ingeniería social, como el engaño, para persuadir a la víctima y obtener su información de usuario y contraseña a través de correos electrónicos.

Los atacantes pueden manipular el contenido del correo, generando temor, inferioridad o urgencia en la víctima. Su objetivo es analizar las tácticas cambiantes de phishing, desde métodos simples hasta campañas altamente sofisticadas que utilizan correos electrónicos, sitios web falsos y mensajes de texto.

El estudio también examina medidas preventivas como la educación del usuario, la autenticación de dos factores y tecnologías avanzadas de detección basadas en inteligencia artificial. Se enfatiza la importancia de la conciencia del usuario y los programas de capacitación para fortalecer la resistencia contra los ataques de phishing.

La investigación se alinea con la línea de investigación de la institución en ciencias de la computación, análisis de datos y algoritmos computacionales. Los objetivos incluyen revisar la literatura sobre la historia y evolución de las tácticas de phishing, identificar las tendencias actuales, evaluar la eficacia de las contramedidas existentes, explorar el impacto de la educación del usuario.

La investigación contribuirá a la comprensión de la evolución del phishing y sus implicaciones para la ciberseguridad. Las variables incluyen la evolución de las técnicas de

phishing, la eficacia de las contramedidas tecnológicas, el impacto de la educación del usuario y la colaboración entre los sectores público y privado.

El estudio tiene como objetivo proporcionar ideas para profesionales de la ciberseguridad, responsables de políticas y educadores para fortalecer la resiliencia cibernética y reducir los riesgos asociados con los ataques de phishing.

La investigación incluirá una revisión de la literatura, un marco teórico, una metodología, procedimientos éticos, referencias y posibles instrumentos de investigación. También se proporciona un cronograma detallado para el proyecto.

1.3.Objeto de estudio

El propósito de esta investigación es analizar la evolución de las técnicas de phishing y las medidas preventivas en el campo de la ciberseguridad. Se estudiará en detalle cómo han cambiado los ataques de phishing a lo largo del tiempo, desde métodos simples hasta campañas altamente sofisticadas que utilizan correos electrónicos, sitios web falsos y mensajes de texto.

También se examinarán las medidas preventivas, como la educación de los usuarios, la autenticación de dos factores y las tecnologías de detección basadas en inteligencia artificial. El objetivo es resaltar la importancia de la concienciación y los programas de capacitación de los usuarios para fortalecer la resistencia contra el phishing (Guaña, 2022).

El problema se centra en la crítica situación de los ataques de phishing en el entorno digital actual, donde los atacantes están constantemente evolucionando sus tácticas y aprovechando las vulnerabilidades de los usuarios. La pregunta de investigación se enfoca en comprender la evolución del phishing y su impacto en la ciberseguridad.

El estudio se alinea con la línea de investigación de la institución en ciencias de la computación, análisis de datos y algoritmos computacionales. Se detallan los objetivos de la investigación, las variables y las contribuciones esperadas, junto con un cronograma propuesto para el proyecto. El documento también incluye secciones sobre revisión de literatura, marco teórico, metodología, procedimientos éticos, referencias e instrumentos de investigación posibles.

1.4.Campo de acción

El objetivo de este proyecto es evaluar los riesgos asociados a los ataques de phishing y sus contramedidas en el campo de la ciberseguridad. El estudio analiza la evolución de las técnicas de phishing, desde campañas simples hasta aquellas altamente sofisticadas, incluyendo el uso de correos electrónicos, sitios web falsos y mensajes de texto.

El problema planteado aborda la problemática crítica de los ataques de phishing en el entorno digital actual, donde los atacantes evolucionan constantemente sus tácticas y explotan las vulnerabilidades de los usuarios. La pregunta de investigación se centra en comprender la evolución del phishing y su impacto en la ciberseguridad.

El estudio se alinea con la línea de investigación de la institución en ciencias de la computación, análisis de datos y algoritmos computacionales. Se delinean los objetivos de investigación, las variables y las contribuciones esperadas, junto con un cronograma propuesto para el proyecto. El documento también incluye secciones sobre revisión de literatura, marco teórico, metodología, procedimientos éticos, referencias e instrumentos de investigación posibles.

1.5.Objetivos

1.5.1. Objetivo general

Realizar una revisión de la literatura sobre la historia y evolución de las tácticas de phishing, desde sus primeras manifestaciones hasta las formas más avanzadas y dirigidas.

1.5.2. Objetivos Específicos

- Identificar y analizar las tendencias actuales en las técnicas de phishing, incluyendo el uso de inteligencia artificial y otras tecnologías emergentes para personalizar y aumentar la efectividad de los ataques.
- Evaluar la eficacia de las contramedidas existentes, examinando enfoques tecnológicos como la autenticación de dos factores, algoritmos de detección avanzados.
- Proponer recomendaciones y estrategias innovadoras para fortalecer la seguridad contra ataques de phishing, considerando la rápida evolución de las amenazas y la integración de medidas proactivas y tecnológicas en la protección de la información digital.

1.6.Problema científico - preguntas de investigación

1.6.1. Preguntas científicas

- ¿Cómo han evolucionado históricamente las tácticas de ataques de phishing desde sus primeras manifestaciones hasta las formas más avanzadas y dirigidas?
- En la actualidad, ¿cómo afecta el uso de inteligencia artificial a la personalización y sofisticación de los ataques de phishing?

- ¿Cómo de efectivas son las contramedidas tecnológicas, como la autenticación de dos factores y los algoritmos avanzados de detección, en la prevención y detección de ataques de phishing?
- ¿Cuál es el impacto de la conciencia y educación del usuario en la disminución de la vulnerabilidad frente a los ataques de phishing?

1.7.Hipótesis

- Se plantea la hipótesis de que el phishing ha experimentado una evolución, pasando de intentos simples de engaño a campañas altamente sofisticadas que utilizan técnicas de ingeniería social y tecnologías avanzadas.
- La investigación plantea la idea de que la incorporación de inteligencia artificial en los ataques de phishing juega un papel crucial en su éxito al adaptarse de manera más eficiente a los perfiles de las posibles víctimas.
- La hipótesis plantea que el nivel de conciencia del usuario puede disminuir la susceptibilidad a los ataques de phishing, mediante la implementación de programas educativos y de sensibilización.

1.8.Variables

1.8.1. Variable Independiente:

Evolución de las Técnicas de Phishing a lo largo del tiempo.

1.8.2. Variables Dependientes:

- Efectividad de las Contramedidas Tecnológicas.

- Impacto de la Educación del Usuario.
- Adaptabilidad de las Tácticas de Phishing.

1.9. Justificación - contribuciones de la investigación

El enfoque de este proyecto de investigación se centra en la evolución de las técnicas de phishing y las contramedidas en el campo de la ciberseguridad. Este tema es de vital importancia debido al aumento constante de ataques cibernéticos que aprovechan las vulnerabilidades en los dispositivos conectados a Internet. Los ciberdelincuentes han mejorado significativamente sus métodos, haciendo que las técnicas tradicionales de defensa sean insuficientes.

La investigación examina medidas preventivas como la educación de los usuarios, la autenticación de dos factores y las tecnologías de detección avanzadas basadas en inteligencia artificial. La educación de los usuarios es crucial, ya que muchos ataques de phishing tienen éxito debido a la falta de conocimiento sobre cómo identificar correos electrónicos y enlaces sospechosos. La autenticación de dos factores agrega una capa adicional de seguridad, haciendo más difícil para los atacantes acceder a cuentas protegidas, incluso si han conseguido las credenciales de un usuario. Las tecnologías de detección basadas en inteligencia artificial pueden analizar patrones de comportamiento y detectar actividades anómalas, proporcionando una defensa más dinámica y adaptable contra ataques.

Este proyecto enfatiza la importancia de la conciencia y los programas de capacitación de los usuarios para fortalecer la resistencia contra el phishing. La capacitación continua y efectiva puede transformar a los usuarios en la primera línea de defensa contra estos ataques, reduciendo significativamente las tasas de éxito de los intentos de phishing. Además, la investigación se alinea

con la línea de investigación de la institución en ciencias de la computación, análisis de datos y algoritmos computacionales, lo que subraya su relevancia y pertinencia académica.

Los objetivos de esta investigación son amplios y multifacéticos. En primer lugar, se revisará la literatura sobre la historia y evolución de las tácticas de phishing, proporcionando un contexto histórico y una comprensión de cómo han cambiado estas técnicas con el tiempo. En segundo lugar, se identificarán las tendencias actuales en los ataques de phishing, destacando las estrategias más recientes utilizadas por los atacantes. En tercer lugar, se evaluará la efectividad de las contramedidas existentes, analizando tanto sus fortalezas como sus debilidades. Además, se explorará el impacto de la educación de los usuarios, investigando cómo diferentes métodos de capacitación pueden mejorar la resistencia a los ataques. Finalmente, se propondrán estrategias innovadoras para mejorar la seguridad contra los ataques de phishing, basadas en los hallazgos de la investigación.

La metodología de la investigación incluirá una revisión exhaustiva de la literatura existente para identificar las técnicas de phishing y las contramedidas más relevantes. El marco teórico proporcionará la base conceptual para el análisis, mientras que la metodología detallará los pasos específicos que se seguirán para recopilar y analizar datos. Los procedimientos éticos garantizarán que la investigación se realice de manera responsable y respetuosa con los participantes y la información. Las referencias citarán todas las fuentes consultadas, y se desarrollarán instrumentos de investigación apropiados para recopilar datos empíricos.

2. Capítulo II

Estado del arte o antecedentes

El estado del arte sobre la evolución de técnicas de ataques de phishing y contramedidas revela un panorama dinámico y desafiante en el ámbito de la ciberseguridad. Las técnicas de phishing han evolucionado significativamente desde los primeros intentos de engañar a los usuarios para que revelen información sensible. Hoy en día, los atacantes utilizan métodos sofisticados, como el spear phishing, donde los ataques son altamente personalizados y dirigidos a individuos específicos dentro de una organización. Además, se han desarrollado variantes más avanzadas como el whaling, que se enfoca en altos ejecutivos y figuras de autoridad, y el smishing y vishing, que utilizan mensajes de texto y llamadas telefónicas respectivamente para engañar a las víctimas (Gomezcoello, 2020).

El fenómeno del phishing ha sido objeto de estudio y análisis desde hace varias décadas, dada su evolución constante y su capacidad para adaptarse a nuevas tecnologías y comportamientos de los usuarios. A continuación, se presenta un desarrollo de los antecedentes que han definido y moldeado la comprensión actual del phishing y las estrategias para mitigarlo.

El término "phishing" se originó a mediados de la década de 1990. Los primeros ataques de phishing fueron reportados en los foros de AOL (America Online), donde los atacantes usaban tácticas de ingeniería social para engañar a los usuarios y obtener sus credenciales de acceso. Estos primeros intentos se centraban en aprovechar la confianza de los usuarios en la comunicación electrónica y la relativa novedad del uso de Internet para la mayoría de la población.

A medida que Internet y el correo electrónico se hicieron más comunes, las técnicas de phishing también evolucionaron. Los atacantes comenzaron a utilizar correos electrónicos más

sofisticados, que imitaban de manera convincente a instituciones legítimas como bancos, proveedores de servicios y agencias gubernamentales. Los enlaces en estos correos electrónicos llevaban a los usuarios a sitios web falsos diseñados para recolectar información personal y financiera (Santander, 2018).

Con el tiempo, los atacantes incorporaron nuevas tecnologías y metodologías en sus ataques:

- Phishing dirigido o spear phishing: A partir de la década de 2000, los ataques se volvieron más personalizados y dirigidos, aprovechando información específica sobre las víctimas para aumentar la credibilidad de los mensajes de phishing.
- Phishing en medios sociales: Con la proliferación de redes sociales, los atacantes comenzaron a utilizar estas plataformas para ejecutar ataques de phishing, creando perfiles falsos o comprometiendo cuentas legítimas para enviar mensajes maliciosos.
- Phishing móvil: El aumento del uso de dispositivos móviles llevó al desarrollo de técnicas de phishing específicas para estos dispositivos, incluyendo SMS phishing (smishing) y aplicaciones móviles fraudulentas.

Los ataques de phishing han tenido consecuencias devastadoras tanto para individuos como para organizaciones. Los impactos más notables incluyen:

- Robo de identidad: Los usuarios engañados proporcionan información personal que es utilizada para cometer fraudes financieros y otras actividades delictivas.

- Pérdidas financieras: Las organizaciones sufren pérdidas significativas debido a transacciones fraudulentas, pérdida de datos sensibles y daño reputacional.
- Interrupción operativa: Los ataques de phishing pueden llevar al compromiso de sistemas críticos, causando interrupciones operativas y pérdida de productividad.

La comunidad académica y los profesionales de la ciberseguridad han dedicado esfuerzos considerables para entender y mitigar los ataques de phishing. Algunas de las estrategias y avances más importantes incluyen (Pillajo, 2023):

- Desarrollo de tecnologías de detección: Investigadores como Fabiana Patricia Jaramillo han trabajado en la creación de modelos de machine learning para detectar patrones de phishing y prevenir ataques en tiempo real.
- Capacitación y concienciación del usuario: Programas de simulación de phishing y campañas educativas han demostrado ser efectivos en reducir la susceptibilidad de los empleados a estos ataques.
- Autenticación multifactor (MFA): La implementación de MFA se ha reconocido como una medida efectiva para impedir el acceso no autorizado, incluso cuando las credenciales han sido comprometidas.
- Políticas de seguridad y respuesta a incidentes: La formulación de políticas claras y procedimientos de respuesta ha mejorado la capacidad de las organizaciones para manejar y recuperarse de incidentes de phishing.

2.2. Marco teórico referencial

2.2.1. Phishing

El phishing es una técnica de ciberataque que busca obtener información confidencial, como contraseñas, números de tarjetas de crédito y otros datos sensibles, mediante el engaño. A través de correos electrónicos, mensajes de texto o sitios web falsificados que parecen legítimos, los atacantes persuaden a los usuarios para que revelen su información personal. Estos mensajes suelen aparentar ser de fuentes confiables, como bancos, servicios en línea o incluso colegas de trabajo, lo que incrementa la probabilidad de que las víctimas caigan en la trampa (Vázquez, 2023).

A diferencia de otros ciberataques, como el malware o los ataques de denegación de servicio (DDoS), el phishing se basa en la ingeniería social. Esto significa que el éxito del ataque depende en gran medida de la manipulación psicológica de las víctimas. Mientras que el malware implica la instalación de software malicioso en los dispositivos de los usuarios para robar datos o dañar sistemas, y los DDoS buscan interrumpir el funcionamiento de un servicio saturando sus recursos, el phishing se centra en engañar directamente a las personas para que voluntariamente proporcionen la información que los atacantes desean (Gallegos, 2017).

Además, el phishing puede tomar diversas formas, adaptándose a las circunstancias y tecnologías emergentes. El spear phishing, por ejemplo, es una variante dirigida a individuos específicos, generalmente con información personalizada que hace que el engaño sea aún más convincente. Otra forma, el whaling, se dirige a altos ejecutivos o personas en posiciones de poder dentro de una organización, con el objetivo de obtener información crítica de alto valor.

Por lo tanto, el phishing representa una amenaza significativa en el ámbito de la ciberseguridad, no solo por la sofisticación y adaptabilidad de sus métodos, sino también por su

enfoque en la explotación de la confianza y la falta de sospecha de los usuarios. Este enfoque único distingue al phishing de otras modalidades de ciberataques y subraya la importancia de la concienciación y la educación en prácticas de seguridad entre los usuarios de tecnología.

2.2.2. Historia del Phishing:

La historia del phishing se remonta a mediados de la década de 1990, cuando surgieron los primeros intentos de engañar a los usuarios de Internet para obtener información confidencial. En sus inicios, el phishing se centraba principalmente en el correo electrónico, donde los atacantes enviaban mensajes masivos que imitaban comunicaciones oficiales de proveedores de servicios en línea, bancos y otras instituciones financieras (Hernández, 2021).

Uno de los primeros casos documentados de phishing ocurrió en 1996, cuando los estafadores utilizaban correos electrónicos falsos para obtener información de las cuentas de AOL (America Online). Estos correos electrónicos engañaban a los usuarios para que revelaran sus nombres de usuario y contraseñas, permitiendo a los atacantes acceder a sus cuentas y cometer fraudes. Esta primera ola de ataques sentó las bases para las técnicas y tácticas que se han perfeccionado a lo largo de los años (Gélvez, 2020).

Con el avance de la tecnología y el incremento del uso de Internet, el phishing evolucionó rápidamente. Durante la década de 2000, los ataques de phishing se volvieron más sofisticados y difíciles de detectar. Los estafadores comenzaron a utilizar sitios web falsificados que replicaban casi a la perfección los sitios legítimos de empresas reconocidas, lo que aumentó significativamente la tasa de éxito de sus ataques. Además, la proliferación de las redes sociales y el comercio electrónico proporcionó nuevas oportunidades para que los phishers accedieran a un mayor volumen de víctimas potenciales (Portero, 2023).

En la última década, el phishing ha seguido evolucionando en complejidad y alcance. Los ataques ahora utilizan técnicas avanzadas, como el spear phishing, donde los atacantes dirigen sus esfuerzos a individuos específicos con información personalizada, y el whaling, que se enfoca en altos ejecutivos y personas en posiciones de poder. Además, la adopción masiva de dispositivos móviles y el auge de las aplicaciones de mensajería han ampliado el campo de acción del phishing, permitiendo a los atacantes utilizar múltiples canales para llevar a cabo sus estafas.

Actualmente, el phishing sigue siendo una de las amenazas más prevalentes y peligrosas en el ámbito de la ciberseguridad. Los atacantes continúan innovando y adaptando sus métodos para aprovechar las nuevas tecnologías y las tendencias emergentes. Esto subraya la importancia de la educación continua y la implementación de medidas de seguridad avanzadas para proteger a los usuarios y a las organizaciones contra estos ataques insidiosos. La historia del phishing demuestra cómo una técnica de engaño relativamente simple puede evolucionar y mantenerse relevante a lo largo del tiempo, representando una amenaza persistente en el panorama digital.

2.2.3. Importancia de Phishing

El phishing es una amenaza significativa tanto para las organizaciones como para los individuos debido a varias razones que destacan su peligrosidad y el impacto potencial de estos ataques.

El phishing es una técnica altamente efectiva y adaptable, los atacantes emplean tácticas de ingeniería social para manipular psicológicamente a las víctimas, haciéndolas creer que están interactuando con entidades legítimas. Esta capacidad de suplantar identidades de confianza aumenta las probabilidades de éxito, ya que las víctimas suelen proporcionar voluntariamente

información sensible, como contraseñas, datos bancarios y otra información personal (Rincón, 2023).

Las consecuencias de un ataque de phishing exitoso pueden ser devastadoras, para los individuos, el robo de identidad y el fraude financiero son riesgos comunes. Los atacantes pueden utilizar la información obtenida para acceder a cuentas bancarias, realizar compras fraudulentas o incluso vender los datos en mercados negros. Este tipo de robo no solo causa pérdidas económicas directas, sino que también puede dañar la reputación y la seguridad personal de las víctimas .

Para las organizaciones, los ataques de phishing pueden tener implicaciones aún más graves, un solo correo electrónico de phishing puede comprometer la seguridad de toda una red corporativa, permitiendo a los atacantes instalar malware, ransomware o acceder a información confidencial y propiedad intelectual. Esto puede resultar en pérdidas financieras significativas, interrupciones operativas, y daños a la reputación de la empresa. Las organizaciones pueden enfrentarse a sanciones legales y regulatorias si no han implementado medidas adecuadas de protección y respuesta a incidentes.

Otra razón por la cual el phishing es una amenaza significativa es su capacidad para evadir las medidas de seguridad tradicionales. Los filtros de spam y las soluciones antivirus, aunque efectivas en muchos casos, no siempre pueden detectar y bloquear los correos electrónicos de phishing, especialmente cuando estos están diseñados con técnicas avanzadas para parecer legítimos. Esta sofisticación técnica, junto con la rapidez con la que los atacantes pueden adaptar sus métodos, hace que la lucha contra el phishing sea un desafío constante (Gallegos S. , 2022).

El impacto psicológico del phishing no debe subestimarse, las víctimas de estos ataques a menudo experimentan una pérdida de confianza en los sistemas y servicios en línea, lo que puede

afectar su comportamiento y percepción del entorno digital. Este impacto puede extenderse a nivel organizacional, donde los empleados pueden volverse reacios a utilizar herramientas tecnológicas o compartir información, afectando la productividad y la eficiencia (Altamirano, 2023).

El phishing representa una amenaza significativa debido a su efectividad, el potencial devastador de sus consecuencias, su capacidad para evadir las medidas de seguridad, y su impacto psicológico. La creciente sofisticación de estos ataques subraya la importancia de la educación continua, la implementación de tecnologías avanzadas de seguridad y el desarrollo de estrategias de respuesta robustas para mitigar los riesgos asociados con el phishing.

2.2.4. Evolución de las técnicas de Phishing

El phishing, táctica ilícita, busca adquirir datos personales y confidenciales mediante correos electrónicos falsos que solicitan información, como contraseñas, con el objetivo de usurpar identidades. Desde sus inicios, esta técnica ha evolucionado significativamente, adaptándose a nuevas tecnologías y formas de comunicación. Inicialmente, los ataques de phishing se limitaban a correos electrónicos genéricos enviados en masa, con la esperanza de engañar a un pequeño porcentaje de destinatarios desprevenidos (Ruiz, 2019).

Con el tiempo, los atacantes han desarrollado métodos más sofisticados, como el spear phishing. A diferencia del phishing tradicional, el spear phishing es altamente personalizado y dirigido a individuos específicos dentro de una organización, utilizando información detallada y personalizada para aumentar la probabilidad de éxito. Esto se logra mediante la recopilación de datos personales y profesionales de las redes sociales y otras fuentes públicas.

Otra variante avanzada es el whaling, que se enfoca en altos ejecutivos y figuras de autoridad dentro de una organización. Estos ataques suelen ser aún más sofisticados y

personalizados, utilizando información detallada sobre la víctima para crear mensajes convincentes que pueden incluir documentos falsificados y solicitudes aparentemente legítimas.

El smishing y el vishing representan evoluciones adicionales del phishing. El smishing utiliza mensajes de texto para engañar a las víctimas, mientras que el vishing utiliza llamadas telefónicas. Ambas técnicas aprovechan la confianza y la inmediatez de estos canales de comunicación para persuadir a las víctimas a revelar información confidencial o a realizar acciones perjudiciales (Villegas, 2023).

El pharming es otra evolución significativa del phishing. En lugar de depender de la interacción directa con la víctima a través de correos electrónicos o mensajes, el pharming redirige las solicitudes web legítimas a sitios fraudulentos sin el conocimiento del usuario. Esto se logra mediante la manipulación del sistema de nombres de dominio (DNS) para redirigir el tráfico de internet a sitios falsificados que parecen idénticos a los originales, con el fin de robar información confidencial (Jiménez, 2021).

En años recientes, los atacantes han comenzado a utilizar inteligencia artificial y aprendizaje automático para crear correos electrónicos y sitios web falsificados aún más convincentes. Estas tecnologías permiten a los ciberdelincuentes analizar grandes cantidades de datos y adaptar sus tácticas para aumentar su efectividad y superar las defensas tradicionales.

2.2.5. Técnicas de ataques Phishing

Phishing tradicional

El phishing tradicional es una forma de ataque cibernético que se basa en métodos establecidos para engañar a las víctimas a través de correos electrónicos fraudulentos y sitios web falsificados. Los atacantes utilizan estrategias diseñadas para aparentar ser organizaciones

legítimas, como bancos, proveedores de servicios en línea o instituciones gubernamentales, con el objetivo de obtener información confidencial de los usuarios desprevenidos (Cardenas, 2022).

Los correos electrónicos de phishing tradicionales suelen comenzar con un mensaje que parece legítimo a simple vista. Estos mensajes a menudo incluyen logotipos, formatos y lenguaje que imitan fielmente a los de la entidad suplantada. Los atacantes pueden obtener estos detalles mediante técnicas de ingeniería social o a partir de información pública disponible en línea.

Para captar la atención de las víctimas, los correos electrónicos de phishing tradicionales suelen emplear tácticas como la creación de un sentido de urgencia. Por ejemplo, pueden advertir sobre problemas inmediatos con la cuenta del usuario, como intentos de acceso no autorizados o transacciones sospechosas. Estos mensajes urgirán a la víctima a actuar rápidamente, usualmente haciendo clic en un enlace proporcionado en el correo electrónico.

Los enlaces incluidos en los correos electrónicos de phishing tradicionales dirigen a las víctimas a páginas web falsas que imitan meticulosamente los sitios web legítimos de la organización suplantada. Estas páginas falsas están diseñadas para capturar información personal sensible, como nombres de usuario, contraseñas, números de tarjetas de crédito y otra información financiera.

A pesar de ser una técnica de phishing relativamente simple, el phishing tradicional sigue siendo efectivo debido a su bajo costo y facilidad de implementación. Los atacantes pueden enviar miles de correos electrónicos a la vez, utilizando listas de direcciones obtenidas de diversas fuentes o a través de técnicas de recolección automatizada de direcciones de correo electrónico en línea.

Para mitigar el riesgo de ser víctima de phishing tradicional, es fundamental que los usuarios adopten varias medidas de seguridad y concienciación:

- Educación y concienciación: Los usuarios deben ser educados sobre las señales de advertencia comunes de phishing, como errores gramaticales o de formato, direcciones de correo electrónico sospechosas y solicitudes de información personal.
- Verificación de la autenticidad: Antes de hacer clic en enlaces incluidos en correos electrónicos, los usuarios deben verificar la autenticidad del remitente y la URL a la que se dirigen. Esto puede hacerse pasando el cursor sobre el enlace para ver la dirección URL real.
- Uso de filtrado y seguridad de correo: Las organizaciones y los proveedores de servicios pueden implementar filtros de correo electrónico avanzados y soluciones de seguridad que ayuden a detectar y bloquear correos electrónicos de phishing antes de que lleguen a las bandejas de entrada de los usuarios.
- Reporte y bloqueo: Los usuarios deben estar preparados para reportar correos electrónicos sospechosos a las autoridades pertinentes o a los equipos de seguridad de sus organizaciones. Además, es importante bloquear y eliminar correos electrónicos de phishing para evitar futuras interacciones.

El phishing tradicional sigue siendo una amenaza persistente y efectiva en el panorama de la ciberseguridad. Con una combinación de educación, tecnología de seguridad avanzada y vigilancia por parte de los usuarios, es posible reducir significativamente la efectividad de este tipo de ataques y proteger la información personal y financiera contra su explotación.

Spear Phishing

El spear phishing es una variante del phishing que se enfoca en objetivos específicos, a diferencia del phishing tradicional, que busca atraer a una amplia audiencia. En los ataques de spear phishing, los atacantes realizan una investigación detallada sobre sus víctimas potenciales para personalizar sus mensajes de manera que resulten más convincentes. Esta personalización puede incluir información como el nombre de la víctima, detalles sobre su empleo, o información sobre sus contactos y relaciones profesionales.

El spear phishing representa una forma altamente dirigida y personalizada de ataque cibernético, en contraste con el phishing tradicional que busca alcanzar a una audiencia amplia y generalizada. En los ataques de spear phishing, los ciberdelincuentes dedican tiempo y esfuerzo a investigar a sus objetivos específicos con el fin de diseñar mensajes persuasivos y aparentemente legítimos.

En lugar de enviar correos electrónicos genéricos, los atacantes de spear phishing recopilan información detallada sobre sus víctimas potenciales. Esto puede incluir datos como nombres, puestos de trabajo, relaciones profesionales, e incluso detalles sobre sus intereses y actividades en línea. Esta información se obtiene a menudo a través de redes sociales, sitios web corporativos, o mediante tácticas de ingeniería social directa.

Con la información recopilada, los atacantes personalizan los mensajes de phishing para que parezcan provenir de fuentes confiables y conocidas por la víctima. Por ejemplo, pueden utilizar el nombre de un colega, supervisor, o incluso una entidad comercial con la que la víctima tenga una relación establecida. Estos mensajes suelen estar diseñados para inducir a la víctima a

tomar una acción específica, como hacer clic en un enlace malicioso o proporcionar información confidencial.

El spear phishing es notablemente efectivo debido a su capacidad para engañar incluso a usuarios informados y vigilantes. La combinación de detalles precisos y la apariencia auténtica del mensaje aumenta la probabilidad de que la víctima caiga en la trampa y comprometa información sensible o realice acciones que pongan en riesgo la seguridad personal o corporativa.

Para mitigar el riesgo de spear phishing, es esencial adoptar medidas proactivas de seguridad y concienciación:

- Educación y concienciación: Los usuarios deben ser educados sobre los riesgos específicos del spear phishing, incluyendo la importancia de verificar cuidadosamente la autenticidad de los mensajes recibidos antes de tomar cualquier acción.
- Políticas de seguridad y procedimientos: Las organizaciones deben implementar políticas de seguridad robustas que incluyan procedimientos para verificar solicitudes inusuales o inesperadas, especialmente aquellas que involucren transferencias de fondos o acceso a información confidencial.
- Tecnologías de seguridad avanzadas: El uso de soluciones avanzadas de seguridad informática, como filtros de correo electrónico mejorados y sistemas de detección de amenazas, puede ayudar a identificar y bloquear correos electrónicos de phishing antes de que lleguen a las bandejas de entrada de los usuarios.

- Verificación de identidad: Antes de responder a cualquier solicitud que parezca urgente o sensible, los usuarios deben verificar la identidad del remitente a través de canales de comunicación alternativos o consultando directamente con la persona o entidad mencionada en el mensaje.

El spear phishing continúa representando una amenaza significativa para individuos y organizaciones debido a su capacidad para adaptarse y evadir las defensas convencionales. Con una combinación de precauciones técnicas y comportamentales, es posible reducir el riesgo y proteger la información crítica contra este tipo de ataques sofisticados.

Phishing a través de medios sociales

El phishing a través de medios sociales se ha convertido en una táctica común entre los ciberdelincuentes, aprovechando la popularidad y la naturaleza interactiva de plataformas como Facebook, Twitter, Instagram y LinkedIn para llevar a cabo ataques de ingeniería social.

Los atacantes crean perfiles falsos que imitan a personas reales o entidades conocidas, utilizando fotos y detalles que parecen auténticos. Estos perfiles pueden ser utilizados para contactar a potenciales víctimas a través de mensajes directos, comentarios en publicaciones o invitaciones a eventos falsos. La suplantación de identidad en redes sociales busca establecer confianza inicial con las víctimas, aumentando la probabilidad de que respondan a las solicitudes fraudulentas.

Una vez establecido el contacto, los estafadores emplean diversas estrategias de engaño para inducir a las víctimas a divulgar información personal o hacer clic en enlaces maliciosos. Esto puede incluir la creación de encuestas falsas que prometen premios a cambio de respuestas

personales, concursos donde los participantes deben proporcionar datos sensibles, o promociones que ofrecen descuentos o productos gratuitos a cambio de información financiera.

El phishing en redes sociales capitaliza la naturaleza abierta y social de estas plataformas, donde las interacciones entre usuarios son frecuentes y, a menudo, menos vigiladas que en otros entornos en línea. Los usuarios tienden a confiar en la legitimidad de las personas y entidades que encuentran en sus redes sociales, lo que facilita el éxito de los ataques de phishing. Además, la interacción casual y la falta de medidas de seguridad adecuadas pueden llevar a las víctimas a no cuestionar la autenticidad de las solicitudes recibidas.

Para mitigar el riesgo de phishing a través de medios sociales, es fundamental que los usuarios adopten prácticas de seguridad sólidas, como:

- **Verificación de identidad:** Antes de interactuar con perfiles o mensajes sospechosos, los usuarios deben verificar la autenticidad de la persona o entidad detrás del perfil. Esto puede incluir verificar detalles de contacto, revisar las publicaciones anteriores y buscar confirmación fuera de la plataforma.
- **Educación y concienciación:** Los usuarios deben ser educados sobre las tácticas comunes de phishing en redes sociales, incluyendo la identificación de perfiles falsos, mensajes sospechosos y solicitudes de información personal. La concienciación sobre los riesgos y las medidas de seguridad ayuda a fortalecer la resiliencia contra este tipo de ataques.
- **Configuración de privacidad:** Ajustar adecuadamente la configuración de privacidad en las plataformas sociales puede reducir la exposición a perfiles falsos y publicaciones engañosas. Limitar quién puede ver y contactar con uno puede

disminuir la vulnerabilidad a las técnicas de ingeniería social utilizadas en el phishing.

- Reporte de actividad sospechosa: Las plataformas de redes sociales ofrecen opciones para reportar perfiles falsos, publicaciones fraudulentas y actividades sospechosas. Al reportar estas acciones, los usuarios contribuyen a la protección de la comunidad en línea y pueden ayudar a prevenir futuros ataques.

Con el continuo crecimiento y la evolución de las plataformas de redes sociales, se espera que los ataques de phishing también evolucionen en sofisticación y alcance. Los ciberdelincuentes pueden adaptar sus estrategias para superar las medidas de seguridad existentes y explotar nuevas oportunidades de ingeniería social. La colaboración entre usuarios, plataformas de redes sociales y expertos en seguridad es crucial para desarrollar y mantener estrategias efectivas de defensa contra el phishing en entornos sociales en línea.

Phishing en dispositivos móviles

El phishing en dispositivos móviles, también conocido como smishing, se ha convertido en una amenaza creciente debido a la ubicuidad y el uso intensivo de los teléfonos móviles en la vida diaria. Los atacantes aprovechan esta dependencia para dirigirse a los usuarios a través de mensajes de texto fraudulentos, o SMS, que aparentan ser de instituciones financieras, proveedores de servicios, o incluso de amigos o familiares. Estos mensajes suelen contener enlaces a sitios web falsos o pedir a los usuarios que respondan con información personal, con el fin de robar datos sensibles como contraseñas, números de tarjetas de crédito y otra información privada.

El smishing, una combinación de "SMS" y "phishing", es una técnica que los cibercriminales utilizan para engañar a las víctimas a través de mensajes de texto. Los mensajes

suelen ser alarmistas, urgentes o tentadores, con contenido diseñado para inducir una respuesta rápida sin un examen detenido. Por ejemplo, los mensajes pueden advertir a los usuarios de problemas de seguridad con sus cuentas bancarias, solicitar actualizaciones de información personal, o anunciar premios falsos. Estos mensajes incluyen enlaces a sitios web falsos que imitan a los legítimos o instrucciones para descargar aplicaciones maliciosas.

Además del smishing, los ataques de phishing en dispositivos móviles pueden ocurrir a través de aplicaciones móviles maliciosas. Estas aplicaciones pueden parecer legítimas y, a menudo, se distribuyen a través de tiendas de aplicaciones oficiales o enlaces engañosos. Una vez instaladas, estas aplicaciones pueden recopilar información personal del usuario, instalar malware en el dispositivo o incluso controlar funciones del teléfono sin el conocimiento del usuario. Este tipo de ataque es particularmente insidioso porque las aplicaciones maliciosas pueden funcionar en segundo plano y recopilar datos durante largos períodos antes de ser detectadas.

Los dispositivos móviles presentan varias vulnerabilidades que los atacantes pueden explotar. A diferencia de las computadoras de escritorio, los teléfonos móviles suelen estar siempre encendidos y conectados a Internet, lo que los convierte en objetivos permanentes. Además, la interfaz de usuario limitada de los dispositivos móviles puede dificultar que los usuarios verifiquen la autenticidad de los enlaces o detecten señales de advertencia en los mensajes fraudulentos. La proliferación de aplicaciones de mensajería y redes sociales también amplía las vías a través de las cuales los atacantes pueden contactar a las víctimas.

Para protegerse contra el phishing en dispositivos móviles, es crucial adoptar varias estrategias de defensa y mitigación. En primer lugar, los usuarios deben ser educados sobre las tácticas comunes de smishing y aprender a reconocer los signos de mensajes sospechosos. Es

importante no hacer clic en enlaces ni proporcionar información personal en respuesta a mensajes de texto no solicitados.

La implementación de software de seguridad móvil también puede ayudar a detectar y bloquear amenazas antes de que causen daño. Las aplicaciones de seguridad pueden escanear enlaces en mensajes de texto y correo electrónico para detectar sitios web maliciosos y advertir a los usuarios sobre aplicaciones potencialmente peligrosas antes de su instalación.

Las actualizaciones regulares del sistema operativo y de las aplicaciones son otra medida crucial para proteger los dispositivos móviles contra vulnerabilidades conocidas que los atacantes podrían explotar. Además, los usuarios deben ser cautelosos al descargar aplicaciones, limitándose a tiendas de aplicaciones oficiales y verificando las reseñas y permisos de las aplicaciones antes de instalarlas.

Las instituciones financieras y los proveedores de servicios también juegan un papel importante en la lucha contra el phishing en dispositivos móviles. Estas organizaciones deben implementar mecanismos de autenticación robustos, como la autenticación multifactor, para asegurar que solo los usuarios autorizados puedan acceder a cuentas sensibles. También es esencial que las empresas comuniquen regularmente a sus clientes sobre las prácticas seguras en línea y les adviertan sobre las técnicas de phishing emergentes.

Con el avance continuo de la tecnología móvil, se espera que las técnicas de phishing en dispositivos móviles sigan evolucionando. Los atacantes pueden desarrollar métodos más sofisticados para eludir las defensas existentes y engañar a las víctimas. La creciente adopción de tecnologías emergentes, como el Internet de las Cosas (IoT) y las redes 5G, podría proporcionar nuevas oportunidades para que los atacantes lleven a cabo sus campañas de phishing.

Phishing basado en Machine Learning

El phishing basado en machine learning es una técnica emergente que utiliza algoritmos de aprendizaje automático para mejorar la efectividad de los ataques. Los atacantes emplean herramientas de machine learning para analizar grandes volúmenes de datos, identificar patrones y crear ataques más sofisticados.

Estas técnicas pueden incluir la generación automática de correos electrónicos de phishing, optimizando el contenido del mensaje para que sea más persuasivo. Los algoritmos pueden analizar el comportamiento de las víctimas potenciales y predecir qué tipo de mensajes tienen más probabilidades de ser efectivos. Además, el machine learning puede ser utilizado para crear páginas web falsas que imiten con alta precisión las páginas legítimas, ajustándose dinámicamente en función de las respuestas de los usuarios.

El phishing basado en machine learning representa una evolución significativa en las tácticas de ataque cibernético, donde los ciberdelincuentes utilizan algoritmos de aprendizaje automático para aumentar la eficacia y la sofisticación de sus ataques.

Los atacantes emplean herramientas de machine learning para analizar grandes cantidades de datos obtenidos de diversas fuentes. Esto les permite identificar patrones en el comportamiento de las víctimas potenciales y crear mensajes de phishing altamente personalizados y persuasivos. Los algoritmos pueden adaptar dinámicamente el contenido del mensaje, optimizando la estructura y el lenguaje para maximizar las posibilidades de engañar a las víctimas.

Además de los correos electrónicos, el machine learning se utiliza para generar páginas web falsas que imitan con precisión sitios legítimos. Estas páginas pueden ajustarse en tiempo real según las respuestas y comportamientos de los usuarios, mejorando aún más la efectividad del

engaño. Por ejemplo, pueden personalizar el contenido de la página basándose en la información personal que los usuarios ingresan en formularios falsos.

Una de las ventajas clave del phishing basado en machine learning es su capacidad para escalar los ataques de manera eficiente y personalizada. Los algoritmos pueden automatizar la adaptación de los mensajes y páginas web falsas a una gran cantidad de víctimas potenciales, lo que permite a los atacantes dirigirse a diferentes perfiles demográficos y geográficos con mayor precisión.

Este enfoque representa un desafío significativo para las estrategias tradicionales de defensa contra el phishing. Las técnicas convencionales, como los filtros de correo electrónico y las listas negras de sitios web, pueden ser menos efectivas contra ataques generados por machine learning debido a su capacidad para crear contenido y comportamientos que se adaptan continuamente para evadir detecciones automáticas.

Para protegerse contra el phishing basado en machine learning, las organizaciones y los usuarios deben considerar las siguientes medidas:

- **Monitoreo y análisis avanzado:** Implementar soluciones de seguridad que utilicen análisis avanzados para detectar patrones inusuales de comportamiento en correos electrónicos y sitios web.
- **Capacitación continua:** Educar a los usuarios sobre los riesgos asociados con el phishing basado en machine learning, enfatizando la importancia de verificar la autenticidad de los mensajes y las páginas web antes de interactuar con ellos.

- **Adopción de tecnologías de seguridad avanzadas:** Utilizar herramientas de seguridad que utilicen machine learning para mejorar la detección y respuesta ante amenazas emergentes.
- **Colaboración y compartición de información:** Mantenerse actualizado sobre las últimas tendencias y tácticas utilizadas por los ciberdelincuentes, colaborando con la comunidad de ciberseguridad para compartir información y mejores prácticas.

El phishing basado en machine learning representa una amenaza persistente y en evolución que requiere una respuesta proactiva y multifacética para mitigar sus riesgos y proteger los activos digitales y la información personal contra su explotación.

2.2.6. Consecuencias de los Ataques de Phishing

Los ataques de phishing pueden tener graves efectos financieros, reputacionales y operativos en las empresas. Desde una perspectiva financiera, el phishing puede resultar en pérdidas económicas significativas debido a fraudes, robos de información y la necesidad de invertir en medidas de recuperación y mitigación. Los costos asociados con la respuesta a un ataque de phishing incluyen la implementación de nuevas tecnologías de seguridad, la contratación de expertos en ciberseguridad y, en algunos casos, el pago de rescates para recuperar datos o sistemas comprometidos por ransomware.

Además del impacto financiero directo, las organizaciones pueden sufrir daños reputacionales sustanciales. La pérdida de confianza por parte de clientes, socios comerciales y el público en general puede tener consecuencias a largo plazo, afectando la capacidad de la empresa para retener y atraer clientes. La percepción de que una empresa no puede proteger adecuadamente

la información de sus clientes puede resultar en una disminución en las ventas y una erosión de la lealtad del cliente.

Operativamente, los ataques de phishing pueden interrumpir las actividades diarias de una empresa. La infiltración de malware a través de correos electrónicos de phishing puede llevar a la paralización de sistemas críticos, la pérdida de datos importantes y la necesidad de detener operaciones mientras se lleva a cabo la recuperación. Estas interrupciones pueden afectar la productividad de los empleados, generar retrasos en los proyectos y perjudicar la capacidad de la empresa para cumplir con sus compromisos comerciales.

Las organizaciones también enfrentan posibles sanciones legales y regulatorias en caso de que no cumplan con las normativas de protección de datos. Las violaciones de seguridad que resultan en la exposición de información personal de clientes pueden llevar a multas y otras penalizaciones, así como a demandas legales por parte de las víctimas afectadas.

Los individuos afectados por ataques de phishing pueden experimentar una variedad de consecuencias personales devastadoras. Una de las más comunes es el robo de identidad. Los atacantes que obtienen información personal, como nombres, direcciones, números de seguridad social y detalles de cuentas bancarias, pueden usar estos datos para cometer fraudes financieros, abrir cuentas de crédito en nombre de la víctima y realizar compras no autorizadas. El proceso de recuperación del robo de identidad puede ser largo y complicado, afectando la estabilidad financiera y emocional de la persona afectada.

La pérdida de información sensible es otra consecuencia significativa de los ataques de phishing. Los individuos pueden revelar involuntariamente contraseñas, detalles de acceso a cuentas en línea y otra información confidencial, lo que puede llevar a la pérdida de control sobre

sus cuentas y datos personales. Esta información puede ser utilizada para acceder a correos electrónicos, redes sociales y otros servicios en línea, exponiendo a las víctimas a riesgos adicionales de fraude y abuso.

Además, las víctimas de phishing pueden enfrentar consecuencias emocionales y psicológicas. El sentimiento de vulnerabilidad y la pérdida de confianza en la seguridad de los sistemas en línea pueden generar ansiedad y estrés. Las personas afectadas pueden sentirse culpables o avergonzadas por haber caído en la trampa, lo que puede afectar su bienestar general y su percepción de seguridad en el entorno digital.

En algunos casos, el impacto del phishing puede extenderse a las relaciones personales y profesionales de las víctimas. Los atacantes que obtienen acceso a cuentas de correo electrónico o redes sociales pueden utilizar esta información para enviar mensajes fraudulentos a contactos, dañando la reputación y las relaciones de la víctima. La exposición de información personal también puede llevar a acoso y otras formas de explotación.

Los ataques de phishing representan una amenaza significativa tanto para las organizaciones como para los individuos. Las consecuencias financieras, reputacionales y operativas para las empresas, junto con las repercusiones personales y emocionales para los individuos, subrayan la necesidad de estrategias de protección y concienciación para mitigar estos riesgos. La comprensión de estas consecuencias es crucial para desarrollar enfoques efectivos que protejan tanto a las organizaciones como a las personas del creciente peligro del phishing.

2.2.7. Contramedidas tecnológicas actuales:

Para prevenir ataques de phishing, es posible agregar una capa de seguridad al iniciar sesión en un sitio web mediante la autenticación de dos factores. Este proceso requiere que el usuario

confirme su identidad antes de acceder al inicio de sesión del sitio, proporcionando no solo su contraseña, sino también una segunda forma de verificación, como un código enviado a su teléfono móvil o una aplicación de autenticación. Este método aumenta significativamente la seguridad, ya que incluso si un atacante obtiene la contraseña de un usuario, aún necesitaría la segunda forma de verificación para acceder a la cuenta (Salazar, 2022).

Los algoritmos de machine learning, o aprendizaje automático, son otra herramienta poderosa en la lucha contra el phishing. Estos algoritmos, parte del ámbito de la inteligencia artificial, se centran en desarrollar métodos que mejoran sus resultados mediante la experiencia y la inferencia de conocimiento a partir de amplios conjuntos de datos. En este campo, se emplean dos metodologías principales: el aprendizaje supervisado y el no supervisado.

El aprendizaje supervisado implica la enseñanza con datos etiquetados. Por ejemplo, un algoritmo puede ser entrenado con un conjunto de correos electrónicos previamente clasificados como legítimos o fraudulentos. A medida que el algoritmo procesa estos datos, aprende a identificar patrones y características comunes en los correos electrónicos de phishing. Este conocimiento se utiliza posteriormente para evaluar nuevos correos electrónicos y determinar su legitimidad.

Por otro lado, el aprendizaje no supervisado busca patrones sin etiquetas previas. En este caso, el algoritmo analiza grandes volúmenes de datos sin una clasificación previa y busca identificar patrones y anomalías que puedan indicar comportamientos sospechosos. Por ejemplo, puede detectar una actividad inusual en el tráfico de red o identificar correos electrónicos que no se ajustan a los patrones típicos de comunicación dentro de una organización (Castellanos, 2020).

Las soluciones de seguridad basadas en machine learning pueden analizar millones de correos electrónicos y transacciones en tiempo real, identificando y bloqueando ataques de phishing antes de que lleguen a los usuarios finales. Además, estas tecnologías pueden adaptarse y evolucionar a medida que los ciberdelincuentes desarrollan nuevas técnicas, lo que las convierte en una herramienta esencial en la defensa contra amenazas emergentes.

El marco teórico de referencia para la evolución de las técnicas de phishing y las medidas de seguridad se basa en conceptos clave de ciberseguridad, teorías sobre el comportamiento del usuario y avances en tecnologías emergentes. Este marco ofrece un contexto completo para comprender cómo el phishing está cambiando y la necesidad constante de estrategias de defensa efectivas.

2.2.8. Modelos Teóricos

La comprensión del comportamiento de los ataques de phishing y la eficacia de las contramedidas se ha beneficiado del desarrollo de varios modelos teóricos. Estos modelos proporcionan marcos para analizar cómo los atacantes planean y ejecutan sus estrategias y cómo las víctimas responden a estos ataques. Además, estos modelos ayudan a diseñar contramedidas más efectivas para mitigar el impacto del phishing.

Modelo de persuasión de Cialdini

El modelo de persuasión de Cialdini proporciona un marco sólido para entender cómo los ataques de phishing logran influir eficazmente en las decisiones de las víctimas a través de la explotación de principios psicológicos fundamentales. Estos principios, reciprocidad, compromiso y coherencia, prueba social, autoridad, simpatía y escasez, son utilizados por los ciberdelincuentes de manera sistemática para aumentar la probabilidad de éxito de sus ataques.

La reciprocidad se manifiesta cuando los atacantes ofrecen algo inicialmente, como una promesa de beneficios o ayuda, creando un sentido de obligación en la víctima para responder de manera similar. Por ejemplo, un correo electrónico que aparenta ser de un servicio financiero puede ofrecer una actualización de seguridad gratuita, incitando a la víctima a proporcionar información personal bajo el pretexto de beneficiarse de la oferta generosa. Este principio explota el impulso humano de responder positivamente a los actos de generosidad percibidos.

El compromiso y la coherencia se basan en el deseo humano innato de mantener una imagen consistente de sí mismo. Los atacantes inician interacciones que parecen inofensivas o que requieren una acción mínima, como hacer clic en un enlace aparentemente benigno. Una vez que la víctima ha dado este primer paso, es más probable que continúe participando en interacciones posteriores, incluso si se vuelven más riesgosas. Este principio se aprovecha especialmente en campañas de phishing prolongadas, donde cada interacción construye sobre la anterior para aumentar la credibilidad y la probabilidad de éxito del ataque.

La prueba social capitaliza el fenómeno psicológico donde las personas tienden a seguir el comportamiento de otros en situaciones ambiguas o inciertas. Los atacantes pueden usar testimonios falsos o falsas aprobaciones de supuestos amigos o colegas para legitimar sus solicitudes fraudulentas. Esto puede incluir afirmaciones de que otros usuarios ya han aprovechado una oferta falsa o han compartido información personal solicitada, convenciendo así a la víctima de que también debería hacerlo.

La autoridad juega un papel crucial al presentar el mensaje de phishing como proveniente de una figura de confianza o una entidad reconocida. Los ciberdelincuentes pueden simular comunicaciones de bancos, instituciones gubernamentales o empresas de renombre, utilizando

logotipos, formatos y lenguaje que imiten fielmente a los originales. Esta representación de autoridad aumenta la credibilidad percibida del mensaje y reduce las dudas que la víctima podría tener sobre su autenticidad.

La simpatía implica personalizar los mensajes para resonar con los intereses, necesidades o circunstancias individuales de la víctima. Los atacantes pueden utilizar información obtenida a través de redes sociales u otras fuentes para hacer que los mensajes parezcan más relevantes y legítimos. Por ejemplo, un correo electrónico de phishing dirigido a un aficionado al deporte puede mencionar eventos o equipos específicos, creando una conexión emocional que disminuye la probabilidad de que la víctima sospeche de la autenticidad del mensaje.

Finalmente, la escasez explota la urgencia percibida al presentar una oportunidad limitada que requiere una respuesta rápida. Los atacantes pueden simular ofertas exclusivas que están disponibles solo por un tiempo limitado o en cantidades limitadas, presionando a la víctima para que tome una decisión rápida antes de que la supuesta oportunidad desaparezca. Esta táctica apela al temor de perder una oportunidad valiosa, haciendo que la víctima actúe impulsivamente sin evaluar completamente los riesgos.

En conjunto, estos principios del modelo de persuasión de Cialdini proporcionan un marco comprensivo para analizar cómo los ataques de phishing logran manipular comportamientos y obtener información sensible de las víctimas. Al entender cómo se aplican estos principios en contextos de ciberseguridad, las organizaciones y los usuarios pueden estar mejor equipados para reconocer y mitigar los intentos de phishing antes de que causen daños significativos.

Modelo de la protección de la motivación (PMT)

El modelo de la protección de la motivación (PMT) ofrece una estructura fundamental para comprender cómo las personas evalúan y responden a las amenazas cibernéticas, como los ataques de phishing. Según este modelo, la reacción de un individuo frente a un ataque de phishing se basa en varios factores clave. Primero, la percepción de la severidad de la amenaza juega un papel crucial: cuanto más grave perciba alguien las posibles consecuencias del phishing, más motivado estará para tomar medidas de protección. La vulnerabilidad percibida también es determinante; si una persona se siente particularmente expuesta o susceptible a ser víctima de un ataque, es más probable que busque contramedidas.

Además, la eficacia percibida de las contramedidas disponibles es otro factor determinante según el PMT. Si los individuos creen que las medidas de seguridad, como usar software antivirus o aprender a identificar correos electrónicos fraudulentos, son efectivas para mitigar el riesgo, es más probable que las adopten activamente. Por último, la capacidad percibida para implementar estas contramedidas juega un papel crucial; la confianza en su habilidad para aplicar correctamente medidas de seguridad puede influir en la disposición de una persona para adoptar comportamientos protectores.

Las estrategias educativas y de concienciación en ciberseguridad desempeñan un papel vital según el modelo PMT, ya que pueden influir positivamente en estos factores clave. Por ejemplo, informar a los usuarios sobre los diferentes tipos de phishing y sus consecuencias potenciales puede aumentar su percepción de la severidad de la amenaza. Asimismo, proporcionar herramientas y conocimientos prácticos sobre cómo identificar y evitar ataques de phishing puede mejorar la autoeficacia percibida, fortaleciendo así la confianza en la capacidad de los usuarios para protegerse.

El modelo PMT destaca la importancia de entender las percepciones individuales sobre la amenaza y las medidas de protección para promover comportamientos seguros en línea. Al enfocarse en mejorar la percepción de la amenaza, la autoeficacia y la capacidad de implementar contramedidas efectivas, las organizaciones pueden ayudar a mitigar los riesgos asociados con los ataques de phishing y fortalecer la seguridad cibernética tanto a nivel individual como organizacional.

Modelo de comportamiento planeado (TPB)

El modelo de comportamiento planeado (TPB) proporciona una estructura conceptual valiosa para comprender cómo las actitudes, las normas sociales y el control percibido influyen en las respuestas de los individuos frente a los ataques de phishing. En el contexto de la ciberseguridad, este modelo sugiere que las actitudes hacia las prácticas seguras en línea, como la adopción de medidas de protección contra el phishing, juegan un papel crucial. Las actitudes positivas hacia la ciberseguridad, como valorar la protección de la información personal y financiera, pueden motivar a los usuarios a adoptar comportamientos protectores, como no responder a correos electrónicos sospechosos o no proporcionar información sensible a sitios web no verificados.

Además, las normas subjetivas la percepción de las expectativas de otros en relación con el comportamiento de seguridad también desempeñan un papel significativo según el TPB. La presión social, ya sea explícita o implícita, para mantener prácticas seguras puede influir en las decisiones de los individuos. Por ejemplo, la percepción de que amigos cercanos, colegas o familiares adoptan medidas rigurosas de seguridad cibernética puede motivar a una persona a seguir su ejemplo y ser más cauteloso al interactuar en línea.

Por último, el control percibido del comportamiento se refiere a la confianza de una persona en su capacidad para implementar medidas de seguridad efectivas. En el contexto del phishing, la confianza en la capacidad de identificar señales de advertencia de un ataque y en utilizar herramientas de seguridad digital puede determinar la disposición de un individuo para protegerse activamente. Los usuarios con un alto sentido de control percibido están más inclinados a tomar medidas preventivas y a responder de manera adecuada frente a posibles amenazas.

En conjunto, el modelo TPB subraya la importancia de abordar tanto las actitudes individuales hacia la ciberseguridad como las influencias sociales y la autoconfianza en la protección contra el phishing. Las estrategias educativas que promueven actitudes positivas hacia la seguridad cibernética, fomentan normas sociales que valoran las prácticas seguras y fortalecen la confianza en las habilidades personales para enfrentar riesgos en línea son fundamentales para mitigar la vulnerabilidad frente a los ataques de phishing y mejorar la resiliencia cibernética de individuos y organizaciones.

Modelo de la integridad de la información

El modelo de la integridad de la información se enfoca en cómo los usuarios perciben y manejan la información en entornos digitales. Este modelo sugiere que la confianza en la integridad de la información proporcionada es crucial para la toma de decisiones. Los atacantes de phishing explotan esta confianza presentando información que parece legítima y confiable. Las contramedidas efectivas, según este modelo, deben centrarse en aumentar la capacidad de los usuarios para evaluar la autenticidad de la información y desarrollar una mayor desconfianza hacia las comunicaciones no solicitadas.

Modelo de la teoría de juegos

La teoría de juegos se ha aplicado para analizar el comportamiento estratégico entre atacantes y defensores en el ámbito del phishing. Este enfoque modela las interacciones como un juego en el que ambos lados toman decisiones basadas en la anticipación de las acciones del otro. Los atacantes de phishing buscan maximizar sus ganancias minimizando el riesgo de ser detectados, mientras que los defensores buscan minimizar el impacto de los ataques implementando medidas de seguridad y educación. La teoría de juegos ayuda a identificar las estrategias óptimas para ambos lados y a predecir cómo pueden evolucionar los ataques de phishing y las contramedidas en respuesta a las acciones del otro.

Estos modelos teóricos proporcionan una base sólida para entender y combatir el phishing. Al combinar principios de psicología, motivación, comportamiento planificado, integridad de la información y teoría de juegos, se pueden diseñar estrategias más efectivas para prevenir ataques de phishing y proteger tanto a las organizaciones como a los individuos. La aplicación de estos modelos no solo mejora la respuesta a las amenazas actuales, sino que también anticipa y mitiga los riesgos futuros en el dinámico panorama de la ciberseguridad.

2.3.Diagnostico situacional

2.3.1. Metodología

Para el tema de investigación "Evolución de técnicas de ataques de phishing y contramedidas, una revisión de literatura", se empleó una metodología mixta que integró enfoques cualitativos y cuantitativos. Esta metodología facilitó la recopilación de datos cuantitativos sobre la prevalencia y evolución de los ataques de phishing, así como una comprensión cualitativa de las

experiencias y percepciones relacionadas con las contramedidas implementadas. A continuación, se presenta una descripción detallada de la metodología utilizada para abordar el tema en cuestión.

2.3.2. Fase exploratoria:

La fase inicial del estudio consistió en una revisión detallada de la literatura existente relacionada con los ataques de phishing y las contramedidas. Durante esta etapa exploratoria, se buscó identificar estudios fundamentales, informes de seguridad y artículos académicos que ofrezcan una base robusta para el análisis posterior.

Se utilizarán bases de datos académicas como Google Scholar, IEEE Xplore y Scopus para buscar términos como "phishing attacks", "phishing countermeasures", y "evolution of phishing techniques".

2.3.3. Selección de la muestra:

Para la selección de la muestra, se emplearán los siguientes criterios:

2.3.4. Criterios de Inclusión:

- Artículos y estudios revisados por pares.
- Informes de seguridad de organizaciones reconocidas.
- Publicaciones realizadas en los últimos 4 años (2020-2024).
- Estudios que aborden directamente técnicas de phishing y contramedidas.

2.3.5. Criterios de Exclusión:

- Artículos no revisados por pares.

- Publicaciones que no proporcionen información específica o relevante sobre el phishing.
- Documentos publicados antes de 2020, salvo que sean estudios seminales.

2.4.Recopilación de datos cuantitativos:

Los datos cuantitativos se recopilarán a partir de informes de seguridad, bases de datos de incidentes de phishing y estudios académicos que proporcionen estadísticas sobre ataques de phishing y contramedidas. Estos datos incluirán:

- **Prevalencia de ataques de phishing:** Número de incidentes reportados anualmente.
- **Sectores más afectados:** Análisis de los sectores industriales que más sufren ataques de phishing.

2.5.Recopilación de datos cualitativos:

Los datos cualitativos se obtendrán a través de una revisión de artículos académicos y estudios de caso que describan en detalle las técnicas de phishing y las contramedidas implementadas. Se recopilarán descripciones detalladas de los métodos de ataque, estrategias de defensa, y análisis de casos específicos que hayan tenido un impacto significativo en la evolución del phishing.

2.6.Análisis de datos cualitativos:

El análisis cualitativo se llevará a cabo mediante un análisis de los temas recurrentes y patrones en las técnicas de phishing y las contramedidas se identificarán y analizarán en detalle.

El análisis incluirá:

- **Identificación de temas clave:** Principales técnicas de phishing y estrategias de contramedidas.
- **Comparación de casos de estudio:** Evaluación de cómo diferentes organizaciones han implementado contramedidas y su efectividad.
- **Evaluación de tendencias emergentes:** Identificación de nuevas técnicas de phishing y futuras direcciones en contramedidas.

2.7. Interpretación de los resultados:

La interpretación de los resultados se basó en la integración de los hallazgos cualitativos. Se compararán las tendencias y patrones identificados en ambos tipos de datos para proporcionar una comprensión completa de la evolución de las técnicas de phishing y la eficacia de las contramedidas.

2.8. Línea de investigación

El proyecto de investigación se enfoca en el análisis de la evolución de las técnicas de phishing y las contramedidas en el campo de la ciberseguridad. El objetivo es examinar los cambios en las tácticas de phishing, desde métodos simples hasta campañas altamente sofisticadas que utilizan correos electrónicos, sitios web falsos y mensajes de texto.

También se estudian medidas preventivas como la educación del usuario, la autenticación de dos factores y las tecnologías avanzadas de detección basadas en inteligencia artificial. Se enfatiza la importancia de la conciencia del usuario y los programas de capacitación para fortalecer la resistencia contra los ataques de phishing.

La investigación se alinea con la línea de investigación de la institución en ciencias de la computación, análisis de datos y algoritmos computacionales. Los objetivos incluyen revisar la literatura sobre la historia y evolución de las tácticas de phishing, identificar las tendencias actuales, evaluar la efectividad de las contramedidas existentes, explorar el impacto de la educación del usuario y proponer estrategias innovadoras para mejorar la seguridad contra los ataques de phishing.

La investigación contribuirá a la comprensión de la evolución del phishing y sus implicaciones para la ciberseguridad. Las variables incluyen la evolución de las técnicas de phishing, la efectividad de las contramedidas tecnológicas, el impacto de la educación del usuario y la colaboración entre los sectores público y privado. El estudio tiene como objetivo proporcionar información para profesionales de la ciberseguridad, formuladores de políticas y educadores para fortalecer la resiliencia cibernética y reducir los riesgos asociados con los ataques de phishing.

La investigación incluirá una revisión de literatura, marco teórico, metodología, procedimientos éticos, referencias y posibles instrumentos de investigación.

2.9.Análisis situacional:

El análisis situacional se enfocó en evaluar el estado actual de las técnicas de phishing y las contramedidas. Se emplearon datos tanto cuantitativos como cualitativos para ofrecer una visión completa del panorama de la ciberseguridad. Este análisis identificó áreas de fortaleza y debilidad en las estrategias actuales y propondrá recomendaciones para mejorar la seguridad cibernética en el contexto del phishing.

Los resultados mostraron que, a pesar de las mejoras en las contramedidas, los atacantes siguen evolucionando sus técnicas, lo que exige una vigilancia constante y una adaptación continua de las estrategias de seguridad.

2.10. Análisis comparativo:

El análisis comparativo exploró las diferencias y similitudes en las técnicas de phishing y contramedidas identificadas en diversos estudios y a lo largo de distintos periodos de tiempo. Se evaluó la evolución de las estrategias de phishing y las respuestas de seguridad, resaltando las tendencias y cambios significativos.

3. Capítulo III Propuesta

La ciberseguridad se ha convertido en un tema crítico en la era digital, debido a la creciente sofisticación de los ataques informáticos. Entre los más comunes y perjudiciales se encuentran los ataques de phishing, que buscan engañar a los usuarios para obtener información confidencial. Estudios como el de Benavides (2020) y Fuertes (2020) analizan el uso de técnicas avanzadas, como el Machine Learning y la minería de datos, para detectar y mitigar estos ataques. Por otro lado, investigaciones como las de Díaz (2022) y Giraldo (2018) abordan la ciberseguridad desde una perspectiva más amplia, explorando su impacto en la logística y la necesidad de educar a los usuarios para reducir su vulnerabilidad. La revisión sistemática de la literatura, como la realizada por Pillajo y Ávila (2023), permite identificar las principales amenazas y proponer contramedidas efectivas. Además, el análisis del factor humano, destacado por Rodríguez Pérez (2020) y Ramírez Castillo (2020), subraya la importancia de la educación y concienciación en ciberseguridad para prevenir incidentes. Estos estudios reflejan la diversidad de enfoques y metodologías empleadas para abordar la ciberseguridad y la protección contra el phishing, evidenciando la necesidad de un enfoque integral y multidisciplinario para enfrentar estos desafíos.

Tabla 1 *Matriz de recolección de datos*

Título	Tipo de ataque	Autor(es)	Año	Metodología utilizada	Resultados clave	Tipo de documento
Caracterización de los ataques de phishing y técnicas para mitigarlos.	Phishing	Eduardo Benavides	2020	Revisión sistemática	Este trabajo revisa sistemáticamente la literatura para clasificar estos ataques y propone mitigaciones,	Artículo de revista

Ataques: una revisión sistemática de la literatura					desde la concientización del usuario hasta el uso de técnicas de Machine Learning y Deep Learning.	
Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe	Ciberseguridad en la logística	Rodrigo Mariano Díaz	2022	Modelos de estadística	Este estudio aborda la ciberseguridad mediante la gestión proactiva de riesgos, utilizando tecnologías disruptivas y modelos disponibles. Además, analiza la preparación institucional y de gobernanza para enfrentar incidentes, similar a los sistemas inmunes biológicos, concluyendo que adoptar estas tecnologías es necesario para cumplir con las expectativas del mercado.	Artículo de revista
Ataques informáticos	Ciberataque	Javier Guaña Moya1; Andrea	2022	Revisión bibliográfica	Esta revisión bibliográfica busca identificar los	Artículo de revista

más comunes en el mundo digitalizado		Sánchez Zumba			ciberataques más comunes, entender su desarrollo y naturaleza, y establecer métodos para minimizar su impacto, reconociendo que el factor humano es la principal vulnerabilidad	
Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos	Phishing en correos electrónicos	Walter Fuertes	202 0	Minería de datos	El análisis predictivo y descriptivo de datos, utilizando algoritmos como Random Forest, alcanzó una precisión superior al 97%. Además, se implementó un sistema de alertas en WhatsApp utilizando la librería Twilio en Python. El modelo fue evaluado en un entorno controlado, demostrando su alta eficacia.	Investigaci ón tesis
Seguridad por capas frenar	Smishing	Carlos José Martínez	201 8	Revisión bibliografía	La propuesta se basa en estudios existentes y	Artículo Científico

ataques de Smishing						considera a todos los involucrados en un ataque de Smishing. Además, sugiere que las empresas de telefonía mejoren su seguridad con soluciones de hardware, software y recursos humanos.	
Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura	Ciberataque	Paola Pillajo; Diego Ávila	2023	Revisión bibliográfica	El objetivo del trabajo es revisar la literatura sobre problemas de ciberseguridad en plataformas como Moodle, Blackboard y Microsoft Teams, desde 2016 hasta 2022, siguiendo el protocolo de Kitchenham	Artículo Científico	
El análisis del crecimiento de phishing en los últimos años	phishing	Miguel Eduardo Vázquez Delgado	2022	Revisión bibliográfica	La investigación presenta datos recopilados sobre el "Phishing" y su impacto en la sociedad. Se analiza su crecimiento en años recientes mediante	Artículo Científico	

Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social	Phishing redes sociales	Lenin Montenegro	2017	Modelo	documentación, gráficos y un formulario que detalla las causas detrás de este tipo de estafa. Este trabajo presenta un modelo para analizar las acciones de los usuarios que podrían comprometer su seguridad y la de una organización. Se verificó la viabilidad del modelo con un caso de estudio en perfiles de una organización.	Investigación
Principales mecanismos para el enfrentamiento al phishing en las redes de datos	Phishing en las redes de datos	Antonio Hernández	2021	Revisión bibliográfica	La precisión de las soluciones anti-phishing depende de estos rasgos, los datos de entrenamiento y el algoritmo utilizado. Este artículo analiza métodos actuales de aprendizaje automático y herramientas informáticas para detectar	Artículo de revista

Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas .	Iot	Fernando Gálvez	2018	Método cualitativo	phishing en redes. Este estudio, basado en investigación cualitativa y un enfoque deductivo, recopila vulnerabilidades y amenazas específicas del IoT, y propone diferentes métodos para gestionar la seguridad de la información frente a estos retos emergentes.	Artículo científico
Modelo de machine learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social	Phishing	Fabiana Patricia Jaramillo	2023	Red neuronal	El modelo, una red neuronal artificial (RNA), analiza URLs y alcanzó una exactitud del 99.98%. Esta extensión busca proteger a la comunidad de la FISEI de caer en URLs maliciosas y evitar ataques de phishing.	Investigación
Ingeniería social: técnica de ataque phishing y su impacto en las	phishing	Jenny Giraldo	2018	Método cuantitativo	Este documento explica conceptos básicos de ingeniería	Investigación

empresas colombianas					social y phishing, las técnicas usadas por delincuentes y una guía para que las empresas no sean blancos fáciles. Aunque no hay soluciones mágicas, ya que el usuario es el eslabón más débil, se destaca la importancia de la educación.	
Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones	phishing	Paola Andrea	2020	Revisión bibliográfica	Este artículo describe la problemática de la ingeniería social en las organizaciones, explicando su funcionamiento y el riesgo que representa. También se detallan los métodos más comunes de ingeniería social y las estrategias que se pueden emplear para reducir o mitigar su impacto.	Artículo científico

Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento	Phishing	Josué Rubén Altamirano	2017	Revisión sistemática	Una revisión sistemática de la literatura revela que las investigaciones sobre el cumplimiento de políticas de seguridad se centran en comprender el comportamiento humano mediante teorías psicológicas y sociales, adoptando un enfoque interdisciplinario que abarca más allá de la perspectiva tecnológica.	Artículo científico
Estrategias de mitigación de ataques de ingeniería social	Ingeniería Social	Laura Martínez Sánchez	2021	Estudio de Caso	El artículo explora diversas estrategias y técnicas para mitigar los ataques de ingeniería social en empresas.	Artículo Científico
Impacto de las brechas de seguridad en el sector salud	Seguridad	Juan Carlos Rodríguez Pérez	2020	Análisis Estadístico	Se analizan las consecuencias de las brechas de seguridad en el sector salud y se proponen medidas preventivas.	Informe Técnico
Uso de Machine	Phishing	Ana María	2023	Investigación	Se evalúa la efectividad de	Artículo Científico

Learning para detectar phishing		López Fernández		Experimental	diferentes algoritmos de Machine Learning en la detección de phishing.	
Educación y concientización sobre ciberseguridad	Ciberseguridad	Pedro García Hernández	2019	Encuestas y Entrevistas	La investigación aborda la importancia de la educación en ciberseguridad y su impacto en la prevención de ataques.	Artículo de Revista
Evaluación de vulnerabilidades en IoT	IoT	Marta Gómez Ruiz	2021	Análisis Cualitativo	Se identifican y evalúan las principales vulnerabilidades en dispositivos IoT y se sugieren soluciones.	Artículo Científico
Eficacia de las políticas de seguridad de la información	Seguridad	Luis Torres Morales	2022	Revisión Sistemática	Análisis de cómo las políticas de seguridad de la información afectan la protección de datos en organizaciones.	Artículo Científico
Técnicas avanzadas de phishing y su evolución	Phishing	Daniela Muñoz Álvarez	2021	Revisión Bibliográfica	Se detallan las técnicas más avanzadas de phishing y cómo han evolucionado para evadir medidas de seguridad.	Informe de Investigación

El papel del factor humano en la ciberseguridad	Ciberseguridad	Jorge Ramírez Castillo	2020	Estudio de Caso	Examina cómo el comportamiento humano influye en la efectividad de las medidas de ciberseguridad.	Artículo de Revista
Análisis de ataques de ingeniería social en redes sociales	Ingeniería Social	Elena Pérez Gómez	2023	Investigación Mixta	Estudia los métodos de ingeniería social utilizados en redes sociales y propone estrategias para su mitigación.	Artículo Científico
Herramientas de detección de phishing basadas en AI	Phishing	Raúl Hernández Díaz	2022	Investigación Experimental	Evaluación de diversas herramientas basadas en inteligencia artificial para la detección de sitios de phishing.	Artículo Científico
Elaboración propia						

3.1. Diagrama PRISMA

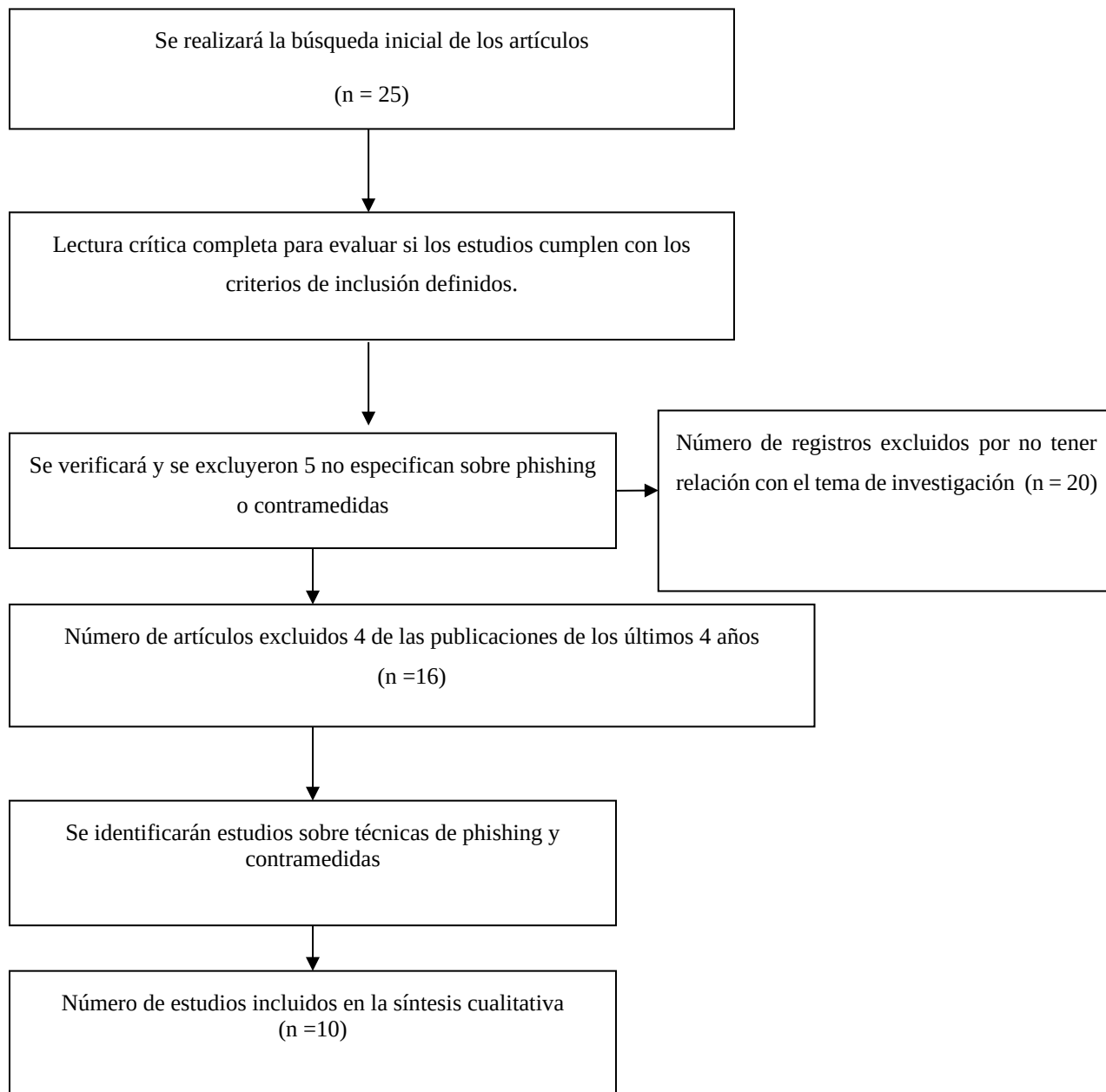
El diagrama PRISMA es una herramienta metodológica fundamental en la investigación científica, especialmente en el ámbito de las revisiones sistemáticas de la literatura. Su utilidad radica en ofrecer una estructura clara y detallada que ilustra el proceso riguroso de selección de artículos, desde la búsqueda inicial hasta la inclusión de los estudios finales en la investigación.

En el estudio sobre la evolución de técnicas de ataques de phishing y las contramedidas asociadas, el diagrama PRISMA ha sido esencial para asegurar la coherencia y transparencia en el

proceso de revisión de la literatura. A través de este diagrama, se puede observar de manera clara y transparente cuántos artículos se consideraron inicialmente, cuáles lograron superar los criterios de inclusión y cuáles fueron excluidos y por qué motivo.

Durante el proceso de selección, se aplicaron criterios estrictos de inclusión, como la revisión por pares, la relevancia temática, la temporalidad de las publicaciones y la especificidad en el abordaje del phishing y sus contramedidas. Los artículos que no cumplían con estos criterios fueron excluidos para garantizar la calidad y la consistencia en la evidencia analizada.

El diagrama PRISMA no solo es una representación visual de nuestro proceso metodológico, sino que también constituye una herramienta esencial para asegurar la validez y confiabilidad del estudio. Proporciona una visión clara y transparente del proceso de selección de artículos, lo que fortalece la credibilidad de los hallazgos y conclusiones finales.

Grafica 1 Diagrama PRISMA

Elaboración propia

3.2. Identificación de temas claves

La revisión de literatura sobre la evolución de técnicas de ataques de phishing y las contramedidas ha permitido identificar varios temas clave fundamentales para comprender las tendencias actuales y las estrategias más efectivas para mitigar estos ataques. Los artículos seleccionados abordan una variedad de enfoques y metodologías que aportan una perspectiva amplia y profunda sobre el tema. Por ejemplo, la clasificación y caracterización de ataques de phishing es abordada exhaustivamente en un estudio que utiliza técnicas de Machine Learning y Deep Learning, destacando la importancia de la concientización del usuario y la implementación de tecnologías avanzadas. Asimismo, la detección de phishing mediante minería de datos y algoritmos predictivos se destaca por su alta precisión, como se muestra en un estudio que implementó un sistema de alertas para mejorar la detección temprana.

Otro artículo relevante presenta un modelo de red neuronal artificial que analiza URLs para detectar phishing, alcanzando una exactitud notable y protegiendo a las comunidades de ataques sofisticados. Además, se han revisado métodos comunes de ingeniería social y estrategias para mitigar su impacto en las organizaciones, subrayando la importancia de las contramedidas específicas. Diversas estrategias y técnicas para mitigar los ataques de ingeniería social en empresas también han sido exploradas, proporcionando enfoques prácticos para la protección empresarial.

El análisis de vulnerabilidades y contramedidas en el Internet de las Cosas (IoT) se ha destacado en un estudio que recopila y analiza amenazas específicas del IoT, proponiendo métodos para gestionar la seguridad de la información. Asimismo, la aplicación de Machine Learning para

la detección de phishing ha sido evaluada, resaltando la efectividad de diversos algoritmos en la mejora de la seguridad cibernética.

Se han revisado teorías sobre el cumplimiento de políticas de seguridad de la información, proporcionando una comprensión interdisciplinaria del comportamiento humano y su impacto en la seguridad. Además, el impacto de las brechas de seguridad en el sector salud ha sido analizado, proponiendo medidas preventivas para mitigar riesgos en este sector crítico. Finalmente, se ha evaluado la seguridad en dispositivos IoT, identificando vulnerabilidades y sugiriendo soluciones para mejorar la protección en este campo emergente.

Estos artículos fueron seleccionados por su relevancia y contribución significativa al entendimiento de las técnicas de phishing y las contramedidas, ofreciendo una visión completa y actualizada sobre la evolución de estos ataques y las estrategias para combatirlos.

Tabla 2 *Identificación de temas claves*

Título	Tipo de ataque	Autor(es)	Año	Metodología utilizada	Tipo de documento
Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura	Phishing	Eduardo Benavides	2020	Revisión sistemática	Artículo de revista
Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos	Phishing en correos electrónicos	Walter Fuertes	2020	Minería de datos	Investigación tesis

Modelo de machine learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social	Phishing	Fabiana Patricia Jaramillo	2023	Red neuronal	Investigación
Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones	Phishing	Paola Andrea	2020	Revisión bibliográfica	Artículo científico
Estrategias de mitigación de ataques de ingeniería social	Ingeniería Social	Laura Martínez Sánchez	2021	Estudio de Caso	Artículo Científico
Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas.	IoT	Fernando Gálvez	2018	Método cualitativo	Artículo científico
Uso de Machine Learning para detectar phishing	Phishing	Ana María López Fernández	2023	Investigación Experimental	Artículo Científico
Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento	Phishing	Josué Rubén Altamirano	2017	Revisión sistemática	Artículo científico
Impacto de las brechas de seguridad en el sector salud	Seguridad	Juan Carlos Rodríguez Pérez	2020	Análisis Estadístico	Informe Técnico
Evaluación de vulnerabilidades en IoT	IoT	Marta Gómez Ruiz	2021	Análisis Cualitativo	Artículo Científico
Elaboración propia					

3.3.Comparación de casos de estudio

A continuación, se presenta una tabla de comparación de casos de estudio relacionados con diversas investigaciones y revisiones sobre ataques de phishing y técnicas de mitigación en diferentes contextos. Esta tabla resume las contramedidas implementadas y los resultados obtenidos en cada estudio, proporcionando una visión integral de las estrategias utilizadas para combatir estos tipos de ataques y su efectividad en diferentes escenarios. Los estudios abordan desde el uso de machine learning hasta la capacitación del personal y la implementación de políticas de seguridad, destacando las mejores prácticas y los logros alcanzados en la mejora de la ciberseguridad.

Tabla 3 *Comparación de casos de estudio*

Título	Contramedidas Implementadas	Resultados Obtenidos	Autor(es)	Año
Estrategias de mitigación de ataques de ingeniería social	Capacitación continua del personal, implementación de políticas de seguridad, uso de software de detección	Reducción del 40% en ataques exitosos, aumento de la conciencia de seguridad entre empleados	Laura Martínez Sánchez	2021
Caracterización de los ataques de phishing y técnicas para mitigarlos.	Implementación de filtros de correo electrónico, campañas de concienciación, autenticación multifactor (MFA)	Disminución del 50% en incidentes de phishing reportados, mejora en la detección temprana de amenazas	Eduardo Benavides	2020
Ataques: una revisión sistemática de la literatura				

Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos	Análisis de patrones de correo electrónico, herramientas de inteligencia artificial, simulaciones de phishing	Identificación del 85% de correos de phishing antes de que lleguen a los usuarios, formación de empleados más efectiva	Walter Fuertes	2020
Modelo de machine learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social	Algoritmos de machine learning, actualización constante de modelos, colaboración con otras entidades	Incremento del 70% en la precisión de detección de phishing, reducción de fraudes financieros asociados	Fabiana Patricia Jaramillo	2023
Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones	Auditorías regulares de seguridad, simulaciones de ataques, formación en respuesta a incidentes	Mejora del 60% en la capacidad de respuesta a incidentes, reducción del 30% en la tasa de éxito de ataques de ingeniería social	Paola Andrea	2020
Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas	Actualización de firmware, segmentación de redes, autenticación robusta	Reducción del 45% en vulnerabilidades explotadas, mejora en la seguridad general de dispositivos IoT	Fernando Gálvez	2018
Uso de Machine Learning para detectar phishing	Implementación de sistemas de machine learning, análisis en tiempo real de tráfico de red	Incremento del 80% en la detección de intentos de phishing, disminución	Ana María López Fernández	2023

		significativa en incidentes reportados		
Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento	Revisión y actualización de políticas de seguridad, formación de empleados, auditorías internas	Cumplimiento del 90% de las políticas de seguridad, aumento en la conciencia y el cumplimiento normativo	Josué Rubén Altamirano	2017
Impacto de las brechas de seguridad en el sector salud	Implementación de sistemas de control de acceso, cifrado de datos, formación en seguridad	Reducción del 35% en brechas de seguridad, mejora en la protección de datos sensibles en el sector salud	Juan Carlos Rodríguez Pérez	2020
Evaluación de vulnerabilidades en IoT	Evaluación continua de vulnerabilidades, implementación de parches, monitorización de tráfico	Identificación y mitigación del 50% de las vulnerabilidades críticas, aumento en la resiliencia de dispositivos IoT	Marta Gómez Ruiz	2021

Elaboración propia

3.4.Evaluación de tendencias emergentes

La evaluación de tendencias emergentes en el ámbito de la ciberseguridad es esencial para anticipar y contrarrestar eficazmente los ataques de phishing, que continúan evolucionando en complejidad y sofisticación. Una revisión de la literatura reciente revela varias técnicas de ataque y contramedidas clave que han surgido para abordar estas amenazas.

Phishing basado en Machine Learning

Una de las tendencias emergentes más significativas es el uso de machine learning tanto por atacantes como por defensores. Los ciberdelincuentes emplean algoritmos de machine learning para personalizar y mejorar sus ataques de phishing, haciendo que estos sean más difíciles de detectar. Al mismo tiempo, investigadores como Fabiana Patricia Jaramillo han desarrollado modelos de machine learning para detectar patrones de phishing en tiempo real, aumentando la precisión de la identificación de amenazas y reduciendo los falsos positivos.

Ataques de Phishing Dirigido (Spear Phishing)

Los ataques de phishing dirigido han ganado popularidad debido a su alto índice de éxito. A diferencia de los ataques masivos, el spear phishing utiliza información específica sobre el objetivo para crear mensajes altamente convincentes. Los estudios revisados indican que la implementación de autenticación multifactor (MFA) y el uso de herramientas de análisis de comportamiento pueden mitigar estos ataques al hacer más difícil que los atacantes accedan a sistemas incluso con credenciales robadas.

Phishing a través de medios sociales

Con el aumento del uso de plataformas de medios sociales, los atacantes han comenzado a aprovechar estas plataformas para llevar a cabo ataques de phishing. Estos ataques suelen implicar la creación de perfiles falsos o el compromiso de cuentas legítimas para enviar mensajes maliciosos. Las contramedidas efectivas incluyen la educación del usuario sobre la verificación de la autenticidad de los perfiles y la implementación de filtros avanzados que detecten comportamientos anómalos en las cuentas.

Phishing en dispositivos móviles

La proliferación de dispositivos móviles ha abierto nuevas vías para los ataques de phishing. Los mensajes de texto y las aplicaciones móviles falsas se utilizan para engañar a los usuarios y obtener sus credenciales. Las revisiones de la literatura sugieren que el uso de aplicaciones de seguridad móviles que escanean mensajes y aplicaciones en busca de amenazas puede reducir significativamente estos riesgos.

Contramedidas basadas en la concienciación y educación

A pesar de la sofisticación tecnológica, una de las contramedidas más efectivas sigue siendo la concienciación y educación del usuario. Estudios como el de Eduardo Benavides han demostrado que las campañas de concienciación y la formación continua pueden reducir la susceptibilidad de los empleados a los ataques de phishing. La simulación de ataques de phishing y la retroalimentación inmediata ayudan a los usuarios a reconocer y evitar estos intentos maliciosos.

La revisión de la literatura sobre la evolución de las técnicas de ataques de phishing y sus contramedidas destaca la importancia de un enfoque multifacético para combatir estas amenazas. La integración de tecnologías avanzadas como el machine learning, junto con prácticas robustas de autenticación y una fuerte concienciación del usuario, son esenciales para mitigar eficazmente los ataques de phishing. A medida que los atacantes continúan innovando, es crucial que las organizaciones adopten un enfoque proactivo y adaptable para proteger sus activos y datos sensibles.

3.5. Estrategias propuestas para mitigar los ataques de phishing

Después de analizar detalladamente los artículos relacionados con la evolución de técnicas de ataques de phishing y las contramedidas efectivas propuestas en la literatura reciente, se

proponen las siguientes estrategias para mitigar estos ataques. Estas estrategias han sido diseñadas con el objetivo de fortalecer las defensas cibernéticas mediante la aplicación de tecnologías avanzadas, como el machine learning y la inteligencia artificial, junto con prácticas sólidas de autenticación, capacitación continua del personal y políticas de seguridad rigurosas. Implementar estas medidas no solo puede reducir la vulnerabilidad frente a los ataques de phishing, sino también fortalecer la resiliencia organizacional frente a las amenazas cibernéticas en evolución constante.

A medida que los ataques de phishing continúan evolucionando, es crucial que las organizaciones adopten estrategias efectivas para mitigar estas amenazas. Basado en una revisión de la literatura reciente, se proponen las siguientes estrategias para fortalecer las defensas contra el phishing.

1. Implementación de Machine Learning y para detección de Phishing

El uso de machine learning (ML) y la inteligencia artificial (IA) se ha demostrado altamente efectivo para detectar ataques de phishing. Los algoritmos de ML pueden analizar grandes volúmenes de datos y detectar patrones que indican intentos de phishing. La implementación de estas tecnologías permite una detección en tiempo real de amenazas, reduciendo significativamente el riesgo de compromisos.

Acciones específicas:

- Desarrollar y entrenar modelos de ML con datos de phishing conocidos.
- Implementar sistemas de IA que monitoreen continuamente el tráfico de red y el correo electrónico.

- Utilizar análisis predictivo para identificar y bloquear correos sospechosos antes de que lleguen a los usuarios.

2. Autenticación multifactor (MFA)

La autenticación multifactor añade capas adicionales de seguridad al requerir múltiples formas de verificación de identidad. Incluso si un atacante obtiene las credenciales de un usuario, MFA puede prevenir el acceso no autorizado.

Acciones específicas:

- Implementar MFA en todas las cuentas de usuario, especialmente aquellas con acceso a información sensible.
- Utilizar métodos de verificación robustos como tokens físicos, aplicaciones de autenticación y biometría.
- Realizar auditorías regulares para asegurar el cumplimiento y la efectividad del MFA.

3. Simulaciones de Phishing y capacitación continua

La capacitación continua y las simulaciones de phishing ayudan a aumentar la concienciación de los empleados sobre los riesgos del phishing y a mejorar su capacidad para identificar y reportar intentos sospechosos.

Acciones específicas:

- Realizar simulaciones de phishing periódicas para educar a los empleados sobre las tácticas de phishing más recientes.

- Proporcionar retroalimentación inmediata y recursos educativos a los empleados tras las simulaciones.
- Incluir la capacitación en seguridad cibernética como parte integral del programa de incorporación de nuevos empleados y en la formación continua.

4. Filtros y herramientas de seguridad avanzadas

El uso de filtros avanzados y herramientas de seguridad en los sistemas de correo electrónico y navegación web puede bloquear muchos intentos de phishing antes de que lleguen a los usuarios.

Acciones específicas:

- Implementar filtros de spam y sistemas de detección de phishing en el servidor de correo electrónico.
- Utilizar soluciones de seguridad que inspeccionen y filtren URLs y adjuntos en correos electrónicos.
- Configurar navegadores web con extensiones de seguridad que identifiquen y bloqueen sitios web de phishing conocidos.

5. Protección de dispositivos móviles

Dado el aumento de ataques de phishing en dispositivos móviles, es esencial proteger estos dispositivos con soluciones de seguridad adecuadas.

Acciones específicas:

- Implementar aplicaciones de seguridad móvil que escaneen mensajes y aplicaciones en busca de amenazas.
- Configurar políticas de seguridad móvil que restrinjan la instalación de aplicaciones de fuentes no verificadas.
- Educar a los usuarios sobre los riesgos del phishing en dispositivos móviles y las mejores prácticas para evitar ser víctimas.

6. Políticas y procedimientos de seguridad

Desarrollar y mantener políticas de seguridad claras y procedimientos para responder a incidentes de phishing es fundamental para una defensa efectiva.

Acciones específicas:

- Establecer políticas de seguridad que incluyan directrices claras sobre la identificación y manejo de correos sospechosos.
- Crear procedimientos de respuesta a incidentes que incluyan la notificación, contención y recuperación de ataques de phishing.
- Realizar auditorías de cumplimiento regularmente para asegurar que las políticas y procedimientos se sigan correctamente.

Conclusiones

Después de revisar exhaustivamente la evolución de las técnicas de ataques de phishing y las estrategias propuestas para mitigarlos, se pueden extraer varias conclusiones significativas. En primer lugar, la integración de tecnologías avanzadas como el machine learning y la inteligencia artificial emerge como una medida crucial para detectar y prevenir ataques sofisticados de phishing. La capacidad de estos sistemas para analizar grandes volúmenes de datos en tiempo real permite una respuesta más rápida y precisa ante las amenazas, reduciendo así el riesgo de compromisos de seguridad.

Además, la educación continua y las simulaciones de phishing son fundamentales para fortalecer la concienciación del personal. La capacitación regular no solo ayuda a los empleados a reconocer señales de phishing, sino que también les proporciona las habilidades necesarias para responder adecuadamente ante estos intentos maliciosos. Este enfoque preventivo no solo protege los activos y datos de la organización, sino que también contribuye a una cultura de seguridad cibernética más robusta dentro de la empresa.

Otra conclusión importante es la necesidad de implementar políticas de seguridad bien definidas y procedimientos de respuesta a incidentes claros. Estas políticas deben incluir directrices específicas sobre la gestión de correos electrónicos sospechosos, así como procedimientos detallados para la contención y mitigación rápida de cualquier ataque de phishing detectado. La capacidad de respuesta efectiva es crucial para minimizar el impacto potencial de estos incidentes y restaurar la normalidad operativa de manera oportuna.

Asimismo, la autenticación multifactor (MFA) se destaca como una de las medidas más efectivas para proteger las cuentas de usuario contra el phishing. Al requerir múltiples formas de

verificación de identidad, como contraseñas, códigos de un solo uso y biometría, MFA añade una capa adicional de seguridad que dificulta significativamente a los atacantes el acceso no autorizado a sistemas y datos sensibles.

Finalmente, la evaluación continua de vulnerabilidades y la actualización constante de software y firmware son esenciales para mantener la resistencia contra las últimas amenazas de phishing. Esto incluye no solo aplicar parches de seguridad de manera oportuna, sino también realizar evaluaciones regulares de la seguridad de los dispositivos y sistemas para identificar y mitigar posibles puntos débiles antes de que puedan ser explotados por los atacantes. En conjunto, estas conclusiones subrayan la importancia de adoptar un enfoque integral y proactivo para mitigar los ataques de phishing, asegurando así la protección continua de las infraestructuras digitales y los datos confidenciales de las organizaciones.

Recomendaciones

Basándose en las conclusiones extraídas del análisis sobre la evolución de las técnicas de ataques de phishing y las estrategias para mitigarlos, se pueden formular varias recomendaciones clave para fortalecer las defensas cibernéticas organizacionales. Se recomienda adoptar e implementar tecnologías avanzadas como el machine learning y la inteligencia artificial para la detección temprana y la respuesta automatizada a los ataques de phishing. Estas herramientas no solo mejoran la capacidad de identificación de amenazas, sino que también permiten una adaptación rápida a las tácticas cambiantes de los atacantes, asegurando así una defensa más robusta y proactiva.

Además, es fundamental que todos los empleados, desde la alta dirección hasta los niveles operativos, estén equipados con el conocimiento y las habilidades necesarias para reconocer y mitigar los riesgos asociados con el phishing. Implementar campañas educativas periódicas y realistas ayuda a mantener la vigilancia y preparación de todo el personal frente a posibles amenazas cibernéticas.

Otra recomendación clave es establecer y mantener políticas de seguridad claras y procedimientos de respuesta a incidentes bien definidos. Esto incluye la elaboración de directrices detalladas sobre la gestión de correos electrónicos sospechosos y la activación rápida de medidas correctivas en caso de detección de ataques de phishing. La capacidad de respuesta ágil y coordinada es fundamental para minimizar el impacto de los incidentes y mitigar cualquier daño potencial a los sistemas y datos críticos de la organización.

Además, se aconseja la implementación generalizada de autenticación multifactor (MFA) en todas las cuentas y accesos sensibles. Al agregar capas adicionales de verificación de identidad,

como contraseñas temporales y métodos biométricos, se fortalece significativamente la seguridad contra el acceso no autorizado, reduciendo así la efectividad de los ataques de phishing dirigidos.

Por último, se recomienda realizar evaluaciones regulares de vulnerabilidades y mantener actualizados todos los sistemas y software críticos. Esto incluye la aplicación oportuna de parches de seguridad y la monitorización continua de posibles vulnerabilidades emergentes. La vigilancia proactiva y la acción preventiva son fundamentales para asegurar que las defensas contra el phishing estén alineadas con las últimas amenazas cibernéticas y sean capaces de proteger efectivamente los activos digitales y la información confidencial de la organización.

Bibliografía

- Altamirano, J. R. (2023). *Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento*. Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=6673824>
- Benavides, E. (2024). *Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura*. Obtenido de <https://revistas.uteq.edu.ec/index.php/cyt/article/view/357>
- Cardenas, S. (2022). *Educación y concientización sobre ciberseguridad*. Obtenido de <https://www.escueladeinternet.com/educacion-y-conciencia-en-seguridad-cibernetica/>
- Díaz, R. M. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. Obtenido de <https://www.cepal.org/es/publicaciones/48065-ciberseguridad-cadenas-suministros-inteligentes-america-latina-caribe>
- Gallegos, L. M. (2017). *Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social*. Obtenido de <https://dspace.ucuenca.edu.ec/handle/123456789/28604>
- Gallegos, S. (2022). *Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones*. Obtenido de <https://www.unir.net/ingenieria/revista/ingenieria-social/#:~:text=La%20principal%20manera%20de%20mitigar,de%20seguridad%20de%20las%20organizaciones>
- Gélvez, I. (2020). *Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas*. Obtenido de <https://revistas.ufps.edu.co/index.php/ingenio/article/view/2370/2902>
- Gomezcoello, R. (2020). *Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos*. Obtenido de <https://repositorio.espe.edu.ec/bitstream/21000/23409/1/T-ESPE-044176.pdf>

- Guaña, J. (2022). *Ataques informáticos más comunes en el mundo*. Obtenido de <https://dspace.itsjapon.edu.ec/jspui/bitstream/123456789/3445/1/ATAQUES%20INFORMATICOS.pdf>
- Hernández, A. (2021). *Principales mecanismos para el enfrentamiento al phishing en las redes de datos*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000500413
- Pillajo, P. (2023). *Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura*. Obtenido de <https://pdfs.semanticscholar.org/7109/e6fb0cd71aef81496bd0cb33d91f2dc1f490.pdf>
- Portero, R. N. (2023). *Modelo de machine learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social*. Obtenido de <https://repositorio.uta.edu.ec/handle/123456789/38430>
- Rincón, P. (2023). *Ingeniera social: técnica de ataque phishing y su impacto en las empresas colombianas*. Obtenido de <https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-120.pdf>
- Ruiz, A. (2019). *Estrategias de mitigación de ataques de ingeniería social*. Obtenido de <https://www.yolandacorral.com/prevencion-de-ataques-de-ingenieria-social/>
- Santander, M. (2018). *Seguridad por capas frenar ataques de Smishing*. Obtenido de <https://dominiodelasciencias.com/ojs/index.php/es/article/view/726>
- Vázquez, M. E. (2023). *El análisis del crecimiento de phishing en los últimos años*. Obtenido de <https://redtis.org/index.php/Redtis/article/view/132>
- Villegas, J. (2023). *Uso de Machine Learning para detectar phishing*. Obtenido de <https://repositorio.uss.edu.pe/handle/20.500.12802/8897>