Recibido 9 Nov. 2024 *ReCIBE, Año 14 No. 1, Mzo. 2025*

Aceptado 20 Feb. 2025

"Técnicas modernas de robo de identidad: Un panorama de herramientas de ataque y defensa, una revisión sistemática"

"Modern identity theft techniques: An overview of attack and defense tools, a systematic review"

Marisol Cruz[1]
t1023300521@unitru.edu.pe

[1] Universidad Nacional de Trujillo.

Resumen

El robo de identidad en la era digital representa un desafío que requiere de nuestra atención inmediata. El objetivo de este artículo es analizar las técnicas de ataque y defensa empleadas para cometer y prevenir estos delitos. Se uso la metodología PRISMA 2020 para realizar una revisión sistemática en bases de datos como Scopus y Science Direct, con estudios de los últimos cinco años.
Se obtuvo como resultados que el phishing se posiciona como una de las técnicas de ataque más recurrentes, junto con malware, ataques de man-in-the-middle y la Ingeniería Social. Para reducir estas amenazas, se identifican defensas como la autentificación multifactor, el uso de la inteligencia artificial para la identificación de fraudes y cifrado de información. Además, la investigación resalta la necesidad de actualizar el desarrollo de tecnologías de ciberseguridad debido a la constante adaptación de los ciberdelincuentes en ajustarse a las nuevas estrategias de seguridad.
Finalmente, es importante capacitar al usuario y entidades sobre las mejores prácticas de seguridad, lo que es vital para desarrollar estrategias más eficientes para proteger su identidad digital en un entorno digital en constante desarrollo.

Palabras clave: phishing, protección de datos, robo, identidad, digital

Abstract

Identity theft in the digital age represents a challenge that requires our immediate attention. The objective of this article is to analyze the attack and defense techniques used to commit and prevent these crimes. The PRISMA 2020 methodology was used to carry out a systematic review in databases such as Scopus and Science Direct, with studies from the last five years.
The results obtained are that phishing is positioned as one of the most recurrent attack techniques, along with malware, man-in-the-middle attacks and Social Engineering. To reduce these threats, defenses such as multifactor authentication, the use of artificial intelligence for fraud identification and information encryption are identified. In addition, the research highlights the need to update the development of cybersecurity technologies due to the constant adaptation of cybercriminals to adjust to new security strategies.
Finally, it is important to train users and entities on the best security practices, which is vital to develop more efficient strategies to protect their digital identity in a constantly developing digital environment.

Keywords: phishing, data protection, theft, identity, digital

1. Introducción

La identidad humana está formada por características que diferencian a cada individuo y evolucionan con el tiempo a través de sus interacciones. Este concepto se ha extendido al ámbito digital, donde la identidad digital se compone de los datos proporcionados por el usuario, sus acciones en el entorno virtual, y las inferencias realizadas por terceros con base en dichas acciones (Moreno et al., 2022).

Careja & Tapus (2023), afirman que la identidad digital está adquiriendo cada vez mayor relevancia, ya que abarca mucho más que la simple sustitución de documentos físicos por datos digitales. Este cambio plantea nuevos desafíos, especialmente en cuanto a la protección de la información personal.

El robo de identidad, definido como la apropiación o uso indebido de los datos y documentos de una persona para crear documentos falsos o establecer una identidad mínima que permita realizar actividades delictivas en nombre de la víctima, se ha convertido en una de las principales amenazas en el entorno digital (Guzmán et al., 2020). Hoy en día, esta problemática afecta tanto a individuos como a organizaciones a nivel mundial.

Zarate & Becerra (2011), sostienen que el avance de las sociedades modernas, junto con la evolución tecnológica, la globalización y la especialización en las TIC, ha proporcionado a los ciberdelincuentes un espacio intangible donde pueden violar prácticamente todos los derechos de una persona de manera casi imperceptible.

Para llevar a cabo estos delitos, los ciberdelincuentes utilizan diversas tácticas, como el phishing, malware, correos electrónicos fraudulentos y ataques de ingeniería social. Con la información obtenida, pueden abrir cuentas bancarias, solicitar tarjetas de crédito o incluso cometer otros delitos en nombre de la víctima, convirtiendo el ciberespacio en un entorno de alto riesgo (Murillo et al., 2023).

Simultáneamente, las defensas contra estos ataques han avanzado significativamente. Tanto las empresas como los usuarios están adoptando herramientas más sofisticadas, como la autenticación multifactorial, la inteligencia artificial para la detección de fraudes y la encriptación de datos, con el fin de mitigar los riesgos asociados al robo de identidad. Sin embargo, a pesar de estos avances, los ciberdelincuentes siguen adaptándose, lo que subraya la importancia de mantenerse a la vanguardia en términos de protección.

Este artículo tiene como objetivo ofrecer una revisión sistemática de las técnicas y herramientas más recientes utilizadas tanto para perpetrar como para prevenir el robo de identidad. A través del análisis de la literatura académica y técnica más actualizada, se explorarán las tendencias más destacadas en este campo, identificando las áreas de mayor riesgo y las soluciones emergentes. Asimismo, se examinarán las brechas en los mecanismos de defensa actuales, con el propósito de proporcionar una visión integral que contribuya al desarrollo de estrategias de ciberseguridad más efectivas en el futuro. Esto conduce a la pregunta de investigación: ¿Cuáles son las técnicas más efectivas utilizadas tanto por ciberdelincuentes para el robo de identidad y cuáles son las defensas identificadas para contrarrestar dichos ataques? Con esta pregunta, se busca determinar qué herramientas y estrategias resultan más eficientes para proteger la identidad digital en un entorno en constante evolución.

2. Metodología

2.1. Fundamentación de la metodología

En su estudio, (Barquero, 2022) menciona que es común que surjan interrogantes como por dónde iniciar, cómo elegir un tema adecuado y cuántos artículos incluir al abordar una revisión de la literatura. Es por ello que elegimos una metodología adecuada que nos dé solución a estas preguntas.

En este estudio se optó por llevar a cabo nuestra revisión sistemática utilizando la metodología PRISMA 2020, que nos va a permitir analizar los estudios científicos e identificar de manera rigurosa los que son más relevantes para nuestra revisión. Contiene un grupo de directrices que se enfocan en la búsqueda de estudios estrictamente científicos, con el fin de recopilar toda la evidencia experimental disponible y que cumpla con criterios de elegibilidad establecidos previamente, con el fin de abordar una hipótesis particular.

El estudio siguió la siguiente secuencia estructural: título, resumen, introducción, métodos, resultados, discusión y conclusiones. En primer lugar, el título dio a conocer nuestra investigación como una revisión sistemática. En la introducción se mencionó la problemática que estamos abordando y nuestra interrogante de investigación. En cuanto a los métodos, se detallaron los criterios de inclusión y exclusión, para seleccionar sólo aquellos estudios relevantes para nuestra investigación. Por otra parte, se especificaron las fuentes de información consultadas con sus respectivas tácticas de búsqueda, así como su procedimiento de selección.

Este enfoque permitió recolectar los datos más pertinentes para dar con la respuesta a la interrogante de investigación planteada. Además, sirvió como sustento para redactar de manera adecuada las partes de resultados, discusión y conclusiones.

2.2. Criterios de elegibilidad

La selección de los artículos se dio enfocado en los siguientes criterios con el fin de identificar fuentes de información relevante según el tema de investigación y sean útiles para formular preguntas de investigación.

Los criterios de inclusión se establecieron en:

- Estudios con un rango de 5 años de antigüedad.
- Estudios en idioma inglés o español.
- Estudios del tipo articulo enfocados en el tema central de investigación.

Se definieron por motivos de exclusión:

- Estudios que no se centren en herramientas enfocadas contra el robo de identidad o este centralizada en aspectos legales.
- Estudios de opinión, entrevistas o ensayos.
- Publicaciones no indexadas y no cuenten con revisiones sistemáticas.

2.3. Fuentes de información y estrategias de búsqueda

Las bases de datos que fueron seleccionadas como fuentes de información son Scopus y Science Direct revisada por última vez el 27 de septiembre del 2024.
Los términos utilizados para la búsqueda se aplicaron a los títulos, resúmenes y palabras clave relacionados con nuestro tema central de la investigación que fueron “identity AND theft”. Con el fin de obtener mejores resultados utilizamos operadores booleanos como “AND”, “OR” y “AND NOT”, lo que nos dio como resultados específicos en las fuentes de información seleccionadas detalladas en la Tabla 1.

Base de datos	**Términos de búsqueda**
Scopus	(TITLE-ABS-KEY ("identity theft") AND TITLE (attack OR vulnerability OR tools OR techniques) AND NOT TITLE-ABS-KEY (legal OR laws OR legislation) AND TITLE-ABS-KEY (defense OR security OR protection)) AND PUBYEAR > 2018 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (PUBSTAGE , "final"))
Science Direct	identity AND theft AND security AND digital AND cybersecurity AND personal data AND privacy AND vulnerability AND phishing

Tabla 1. Consultas de búsqueda

2.4. Proceso de selección

La selección de los artículos fue llevada a cabo manualmente por los autores utilizando hojas de cálculo en Excel. Esto facilitó el análisis de los estudios en base a los criterios de inclusión y exclusión definidos previamente. Se elaboraron hojas de cálculo específicas para analizar cada artículo en las tres etapas del flujo metodológico PRISMA: identificación, cribado e inclusión.

2.5. Extracción de datos y síntesis

La información se recolectó de las tablas de análisis de selección que tienen los campos de Titulo, DOI, Estado (Incluido o excluido). Además, también se agregaron tablas para los criterios de inclusión y exclusión para un análisis más profundo, donde presentan los campos de tipo de criterio, cumplimiento y fundamentación.

3. Resultados

Se identificaron un total de 87 artículos en las bases de datos consultadas, a partir de los cuales se recuperando 51 artículos para un análisis más detallado del contenido. Luego de verificar aspectos como la relevancia con nuestro tema y la existencia de herramientas o técnicas para el robo de identidad, se consiguió una muestra de 23 artículos para la revisión como se muestra en la Figura 1.

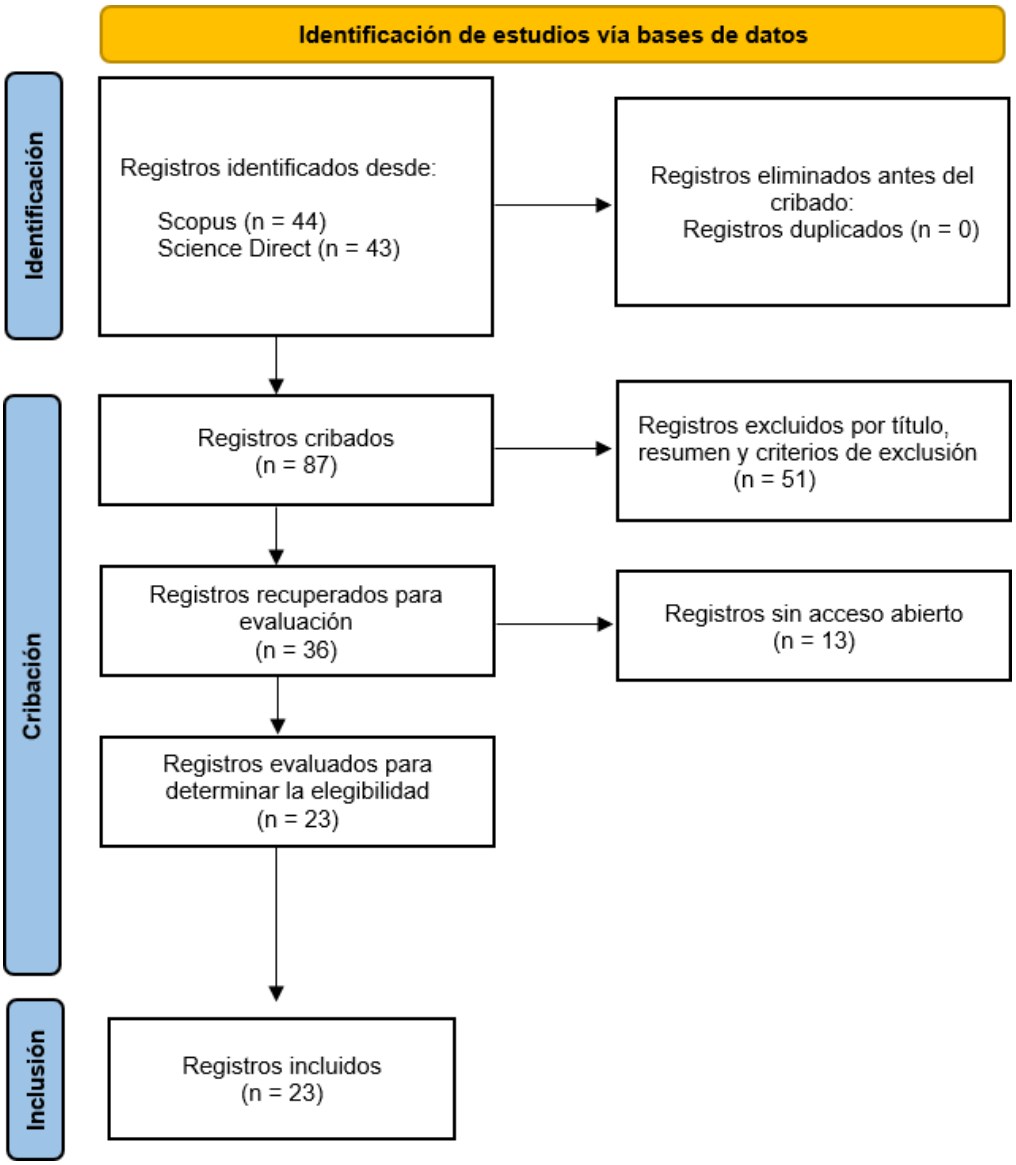

Figura 1. Diagrama de flujo de selección de estudios

Adicionalmente se elaboró un gráfico a través del software VOS VIEWER, como se puede apreciar en la Figura 2, el cual permite visualizar los términos más relevantes y sus relaciones entre publicaciones, siendo el más resaltante “identity theft”.

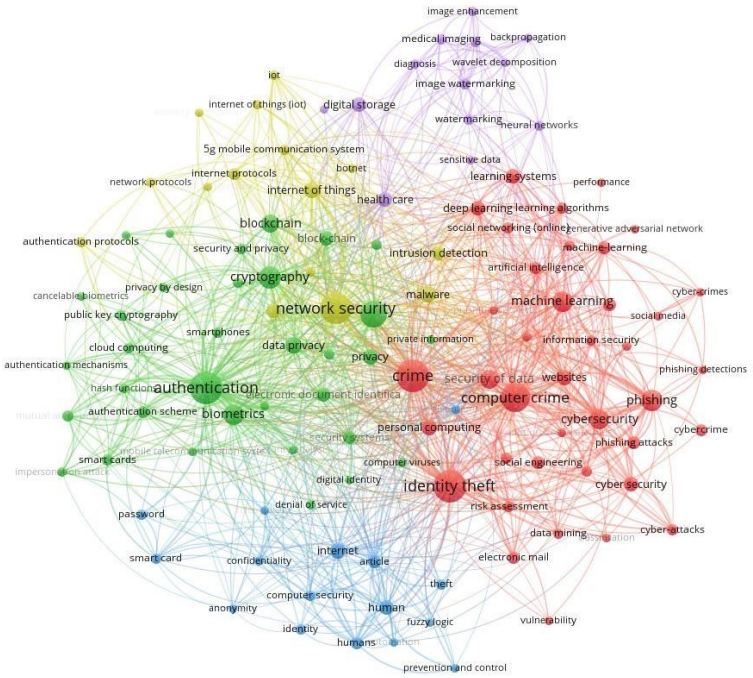

Figura 2. Mapa de co-ocurrencia de palabras clave

En la Tabla 2 se expone los hallazgos sobre las herramientas y técnicas más recientes para prevenir el robo de identidad.

Autores	**Títulos**	**Síntesis de la literatura**	**Herramientas o técnicas**
Ejaz et al. (2023)	"Life-long Phishing Attack Detection Using Continual Learning"	Se examina como los modelos tradicionales de ML pierden efectividad para detectar el phishing debido a que con el tiempo las técnicas de ataque evolucionan. Para detectar el ataque de phishing se propone usar el Aprendizaje Continuo (Cl) con un error de precisión del 2.45%	**Técnicas de ataque** - Se utilizan técnicas como el phishing y el robo de credenciales. **Técnicas de defensa:** - Se analiza técnicas como el aprendizaje continuo (CL) que detecta phishing, el embedding que analiza los contenidos HTML y la transferencia de aprendizaje (TL).
Venkatesan et al. (2023)	Hybrid Machine Learning Technique to Detect Active Botnet Attacks for Network Security and Privacy	Se discute sobre las botnets, un malware controlado a distancia que puede realizar ataques DoS, phishing y robo de identidad. La detección se realiza a través de firmas, pero resulta ineficaz, por lo cual se propone un algoritmo que utiliza el análisis de comportamiento y se emplea estrategias de reducción de tráfico para	**Técnica de ataque** - Se utiliza ataque de malware como las botnets. **Técnicas de defensa:** - Detección de los botnets: como método de defensa basado en el análisis del comportamiento.

		Una mayor precisión alcanzando una tasa de detección del 98.4%.	
Bera et al. (2023)	Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions	Se analiza las tácticas de ataque fraudulentas a pesar de los filtros anti-phishing como los ataques de Ingenieria social y robos de identidad.	**Técnicas de ataque** Se utiliza técnicas de ataque como el phishing, el spooging y la Ingeniería Social para la manipulación del usuario. **Técnicas de defensa:** Tenemos la educación al usuario sobre correos fraudulentos, filtros anti- phishing y análisis y monitoreo de correos.
Albalawi et al. (2023)	The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities	Se centra el desfiguramiento de sitios web y las vulnerabilidades que presentan sitios previamente comprometidos. Utiliza herramientas de escaneo como OWASP ZAP, Burp Suite y Nikto para identificar vulnerabilidades.	**Técnicas de ataque:** **-** Tenemos los ataques de desfiguramiento de sitios web, el ataque al DNS por envenenamiento de caché. **Técnicas de defensa:** Herramientas de Identificación de vulnerabilidades como OWASP ZAP, Burp Suite y Nikto y concientización a los desarrolladores sobre prácticas de seguridad.
Kothamas u et al. (2023)	An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures	Se centra en las tácticas de phishing, analizando diversas herramientas de phishing como Zphisher, CamPhish y PyPhisher, así como la simulación de estos ataques. Donde se discute las maneras de prevenirlo y mitigar riesgos.	**Técnicas de ataque:** - Tenemos al phishing y la Ingeniería social. **Técnicas de defensa:** -Tenemos la concientización a los desarrolladores sobre prácticas de seguridad, Filtros anti-phishing, simulación de ataques y verificación de identidad.
Abdulla et al. (2023)	Robust Password Encryption Technique with an Extra Security Layer	Presenta técnicas para el cifrado de contraseña con el uso de huellas dactilares y combinaciones aleatorias para hacerlas segura y únicas contra ataques. Esto protege las cuentas bancarias de los clientes y las transacciones en línea, reduciendo el robo de identidad por intercepción de contraseñas.	**Técnicas de ataque:** - Tenemos al phishing e intercepción de datos. **Técnicas de defensa:** -Tenemos la encriptación de contraseñas, autentificación multifactor, concientización a los usuarios y verificación biométrica.
Adane et al. (2023)	Email and Website-Based Phishing Attack:	Analiza como la falta de conocimientos y habilidades hace vulnerable al usuario	**Técnicas de ataque**- Tenemos al phishing e Ingeniería Social.

	Examining Online Users Security Behavior in Cyberspace Environment	que pueda sufrir de ataques de phishing. Se utiliza un modelo, que identifica factores claves que afectan la conducta de seguridad de los usuarios, conciencia como factores determinantes.	**Técnicas de defensa:** - Tenemos la autentificación multifactor, concientización a los usuarios y validación de URLs.
Rameem et al. (2022)	Detecting Covid-19 chaos driven phishing/maliciou s URL attacks by a fuzzy logic and data mining based intelligence system	Analiza como la pandemia COVID-19 trajo consigo un aumento en delitos cibernéticos como el phishing y el robo de identidad. Propone un sistema basado en lógica difusa y minería de datos para la detección de phishing, realzando su eficacia contra amenazas.	**Técnicas de ataque** - Tenemos los ataques de phishing y malware malicioso. **Técnicas de defensa:** -Esta la autentificación multifactor, sistemas de detección basado en inteligencia, seguridad de los dispositivos y concientización a los usuarios.
Nonvigno n et al. (2022)	A Copula-Based Attack Prediction Model for Vehicle- to-Grid Networks	Analiza vulnerabilidades de las redes V2G, resaltando ataques como hombre en el medio, denegación de servicios y robo de identidad. Presenta defensas como la detección de intrusiones basados en copulas a través del uso de herramientas como Mini2VG y Wireshark. Finalmente propone un enfoque de clasificación de datos para la detección de ataques y prevenir robos de identidad.	**Técnicas de ataque:** -Tenemos el ataque man in the middle, DoS y el rebound Attacks. **Defensas:** - Tenemos el cifrado de comunicaciones,la autentificación multifactor y el monitoreo de actividades y alertas.
Kampour akis et al. (2022)	Revisiting man-in- the-middle attacks against HTTPS	El ataque de man in the middle permite al atacante interceptar información cuando se da la comunicación. Esto le permite realizar cambios sin autorización del usuario y robo de identidad.	**Técnicas de ataque:** -Tenemos el ataque man in the middle, phishing, credential stuffing y el spoofing. **Defensas:** - Tenemos el cifrado de comunicaciones, la autentificación multifactor. el monitoreo de actividades y alerta y la concientización al usuario.
Minu et al. (2022)	An Edge Based Attack Detection Model (EBAD) for Increasing the Trustworthiness in IoT Enabled	Examina como los ataques de identidad amenazan la confiabilidad en las redes, proponiendo la defensa EBAD(Edge-based Accusation Analysis). Identifica nodos atacantes	**Técnicas de ataque:** -Tenemos el basado en robo de identidad, ataque Sybil donde crea múltiples identidades falsas, cooperación de chantaje (SA-CBA) donde utilizan

	Smart City Environment	Sybil y reduce comportamientos maliciosos.	identidades robadas para amenazar u extorsionar. **Técnicas de defensas:** -Como enfoque EBAD donde identifica nodos atacantes y el análisis de comportamiento.
Veena et al. (2022)	Cybercrime: Identification and Prediction Using Machine Learning Techniques	Analiza métodos de clasificación supervisada y no supervisada para la detección del robo de identidad y cibercrimen. Para la clasificación supervisada utiliza técnicas como SVM y KNN y para la no supervisada usa K-means y modelos gaussianas. Además, usa las redes neuronales para identificar el robo de identidad sintético.	**Técnicas de ataque:** -Tenemos el robo de identidad sintético y ataques de clasificación de datos. **Técnicas de defensas:** -Como las Máquinas de soporte vectorial, redes neuronales y modelos de mezcla gaussiana.
Sharma et al (2021)	FinPAD: State-of- the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives	Enfatiza la importancia de los sistemas biométricos, en especial las huellas dactilares, autentificación segura y el robo de identidad. Se discute sobre ataques PAs que evaden la seguridad a través de artefactos biométricos reales, de la misma manera se analiza la detección como técnicas de aprendizaje profundo como FinPAD.	**Técnicas de ataque:** Tenemos al ataque Pas que compromete la autentificación de sistemas basados en huellas dactilares y los instrumentos de ataque PAIs para engañar a estos sistemas biométricos. **Técnica de defensa:** Tenemos la detección FinPAD, sistemas y bases de datos anti-spoofing.
Saharan et al. (2021)	Scaling & fuzzing: Personal image privacy from automated attacks in mobile cloud computing	Propone un enfoque ingenioso para proteger la privacidad de los datos sensibles en la computación de la nube, mostrando la relación entre la filtración de datos y el robo de identidad. Se analiza técnicas de defensa como la ofuscación de datos y la transformada discreta de Fourier. Además, se incluyen métodos de segmentación de imágenes para reducir la vulnerabilidad de los datos sensibles.	**Técnicas de ataque:** Segmentación de imágenes, inferencias automatizadas para deducir el comportamiento del usuario. **Técnicas de defensa:** Tenemos el filtrado de imágenes con preservación de la privacidad, ofuscación de datos y modelo de seguridad semi-honesto.
Song et al. (2020)	Android data- clone attack via operating system customization	Presenta técnicas de ataque como datos-clone que explota Vulnerabilidades en aplicaciones clonadas por OEM que tiene acceso a las	**Técnicas de ataque:** Ataque de clonación de credenciales, personalización de sistema operativo y vulnerabilidades de OEM.

		credenciales sin tener permiso y acceso a la root. Además, se muestra otro tipo de ataque como el CloneDroid para eludir verificaciones de seguridad en nivel aplicación y sistemas operativos.	**Técnicas de defensa:** Autentificación multifactor, almacenamiento seguro de credenciales y actualización de regular aplicaciones.
Sobabe et al. (2020)	Biometric system vulnerabilities: A typology of metadata	Se analiza las vulnerabilidades en las técnicas biométricas susceptibles al robo de identidad, enfatizando la seguridad de los metadatos. Se divide los límites intrínsecos y ataques adversos y presenta un caso de implementación alcanzando un área bajo la curva (AUC) de 0.908.	**Técnicas de ataque:** Ataques intrínsecos y ataques adversos en sistemas biométricos, reconocimiento facial basado en el color de piel para engañar al sistema. **Técnicas de defensa:** Análisis de metadatos, sistemas biométricos multimodales y actualización y mantenimiento de sistemas.
Zahra et al. (2022)	Detecting Covid- 19 chaos driven phishing/maliciou s URL attacks by a fuzzy logic and data mining based intelligence system	Examina el aumento de ataques cibernéticos como el phishing y robo de identidad durante la pandemia de COVID-19. Se analizan el incremento de los ataques durante esa época, proponiendo estrategias de mitagación y un sistema de lógica difusa y minería de datos para detectar ataques de phishing.	**Técnicas de ataque:** Tenemos al phishing, el malware, ataques de ransoware y URLs maliciosas.
AlQadhee b et al. (2022)	Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior	Aborda los retos que enfrentan las organizaciones al adoptar nuevas tecnologías y seguridad. Propone un enfoque Zero Trust para dificultar el acceso de los atacantes y analiza el comportamiento de seguridad de los usuario.	**Técnicas de defensa:** Como la zero de trust, análisis del comportamiento del usuario y generación de políticas de seguridad.
Bojjagani et al. (2020)	PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification	Presenta un protocolo de autentificación para la protección de sistemas de pago móvil contra las amenazas de ataque como el phishing y hombre del medio. Utiliza la autentificación que envía una notificación al cliente, validado con la herramienta Scyther, con alta capacidad para prevenir ataques de phishing.	**Técnicas de defensa:** Protocolo de autentificación, prevención del phishing y verificación formal usando herramientas como Scyther.

Alhelaly et al. (2023)	When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection	Analiza la protección de la identidad móvil, utiliza un enfoque de métodos mixtos, hallazgos que muestran que la conciencia de protección entre las capacidades y expectativas influyen en las técnicas para la protección de la identidad.	**Técnicas de defensa:** Conciencia de protección, valores motivacionales, experiencia en protección.
Chien- Hua Tsai et al. (2024)	Blockchain- supported online banking scheme	Enfatiza la importancia de la banca en línea y propone un esquema de autentificación blockchain para mejorar la seguridad, confianza y rendimiento en las transacciones para la protección de los datos.	**Técnicas de defensa** Autentificación segura, contratos inteligentes y descentralización.
Afzal et al. (2024)	Context-aware embeddings for robust multiclass fraudulent URL detection in online social platforms	Se propone un enfoque basado en embeddings para la detección de URLs fraudulentas en plataformas sociales, para la clasificación de las mismas que son usadas en ataques de phishing.	**Técnicas de ataque:** **-**Detección de URLs fraudulentas asociadas con el ataque de phishing. **Técnica de defensa:** **-**Embeddings y clasificación multiclasificación
Ribaux & Souvignet (2020)	"Hello are you available?" Dealing with online frauds and the role of forensic science	Analiza un fraude en línea en la Universidad de Lausana, donde nos muestra como el atacante se hizo pasar por el director de Escuela para engañar a miembros a comprar tarjetas de regalos, donde nos muestra cada una de las fases del fraude en línea.	**Técnicas de ataque:** -Se uso el phishing, la compra de tarjeta de regalo para realzar estafas. **Técnica de defensa:** -Análisis forense digital, que investiga fraudes y rastrea huellas dejadas por los atacantes.

Tabla 2. Resultados de los artículos seleccionados

En la tabla 3, se muestran las principales técnicas de robo de identidad y herramientas de defensa mencionadas por los autores, lo que nos refleja las tendencias actuales en cuánto a la problemática que hemos desarrollado.
Se puede apreciar que la técnica mencionada con más frecuencia es el phishing, mientras que la herramienta de defensa más nombrada es la autenticación multifactor.

Materia de estudio	Técnicas o herramientas	Autores	Frecuencia
Técnica de robo de identidad	Phishing	(Ejaz et al; Bera; Kothama et al; Abdulla et al; Adane et al; Rameem et al; Kampour Akis et al; Syed et al; Olvier et al.)	6
	Malware	(Venkates et al; Rameem et al; Syed et al)	3
	Man in the middle	(Nonvigno et al; Kampour Akis et al.)	2
	Spoofing	(Bera et al; Kampour akis et al)	2
	Ingeniería Social	(Kothama et al; Adan et al)	2
	Robo de Credenciales	(Ejaz et al; Wenna et al)	2
	Segmentación de imágenes	(Saharan et al)	1
Herramienta de defensa	Autentificación multifactor	(Adane et al; Rameem et al; Abdulla et al; Nonvigno et al; Wenna et al; Sriramulu et al; Chien et al)	7
	Filtros anti – phishing	(Bera et al; Kothama et al)	2
	Validacion de URLS	(Adane et al; Sara et al)	2
	Zero Trust	(Arwa et al)	1
	Encriptación de contraseñas	(Abdulla et al)	1

Tabla 3. Técnicas de robo de identidad y herramientas de defensa encontradas.

4. Discusión

Las técnicas de robo de identidad han evolucionado en paralelo con el desarrollo de las nuevas tecnologías emergentes. Una de las técnicas más comunes y ampliamente estudiadas es el ataque conocido como phishing, el cual ha sido identificado como una amenaza constante en varios de los principales medios de comunicación. Diversos estudios resaltan la creciente vulnerabilidad en las redes sociales, donde una gran cantidad de usuarios se inician sesión diariamente, convirtiéndolas en uno de los entornos más susceptibles a este tipo de ataques (Kothamasu, et al., 2023). En los sitios web, en su mayoría, prevalece el uso de herramientas AntiPhishing en forma de complementos o extensiones para navegadores (Hernández, 2021). En el estudio de (Burnes, et al., 2020), se hace mención del robo de identidad a través de las tarjetas de crédito, pero además complementa con mostrar el tipo de personas más susceptibles a ser víctimas potenciales. Ante esto, podemos decir que, según nuestra investigación, el grupo de gente más apto para ser víctima de robo de identidad, serían jóvenes de clase media, porque deben tener acceso a dispositivos tecnológicos, sin embargo, su nivel de educación digital no es muy alto, puesto que pueden caer en trampas más fácilmente.
En la actualidad, se han desarrollado múltiples herramientas de defensa basadas en tecnologías emergentes. Podemos destacar el reconocimiento biométrico facial, una técnica utilizada ampliamente en sistemas de seguridad para la autenticación, pero que también es objeto de sofisticados ataques. Frente a esta amenaza, se han propuesto soluciones innovadoras que han sido probadas mediante experimentos utilizando bases de datos especializadas, como el uso de metadatos adicionales para reforzar la autenticidad de losrasgos faciales (Sobabe et al., 2020), que servirán como modelo para reforzar las herramientas de defensa en cuánto a la autenticación multifactorial.

Las investigaciones revisadas en este estudio apuntan a que el desarrollo de contramedidas efectivas está en marcha, impulsado por avances tecnológicos y experimentación científica.

5. Conclusiones

El análisis del estado actual de las técnicas de robo de identidad ha revelado un panorama complejo en constante crecimiento, donde los atacantes hacen uso de herramientas y estrategias cada vez más sofisticadas. Las principales modalidades de ataque identificadas, resaltando el phishing, el malware, y robo de credenciales, hacen ver la importancia de una perspectiva más proactiva y multidimensional en la defensa. El incremento del surgimiento de nuevas tecnologías digitales y la amplia interconectividad de dispositivos de uso cotidiano han dado lugar a nuevas superficies de ataque digital. La combinación de tecnologías avanzadas y un enfoque humano en la seguridad es esencial para mitigar los riesgos asociados con el robo de identidad.
Se concluye que las organizaciones deben adoptar una estrategia integral que incluya la educación del usuario, la implementación de tecnologías avanzadas, y un enfoque colaborativo para la defensa. La vigilancia continua y la adaptación a las nuevas amenazas son imperativas para proteger la identidad y la información sensible en un mundo digital en evolución.

6. Referencias bibliográficas

Abdulla, Q. Z., & Al-Hassani, M. D. (2023). Robust Password Encryption Technique with an Extra Security Layer. *Iraqi Journal Of Science*, 1477-1486. https://doi.org/10.24996/ijs.2023.64.3.36

Afzal, S., Asim, M., Beg, M. O., Baker, T., Awad, A. I., & Shamim, N. (2024). Context-aware embeddings for robust multiclass fraudulent URL detection in online social platforms. Computers & Electrical Engineering: An International Journal, 119(109494), 109494. https://doi.org/10.1016/j.compeleceng.2024.109494

Albalawi, N., Alamrani, N., Aloufi, R., Albalawi, M., Aljaedi, A., & Alharbi, A. R. (2023). The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities. Electronics, 12(12), 2664. https://doi.org/10.3390/electronics12122664

Alhelaly, Y., Dhillon, G., & Oliveira, T. (2023). When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection. Computers & Security, 134(103470), 103470. https://doi.org/10.1016/j.cose.2023.103470

AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. Array (New York, N.Y.), 14(100146), 100146. https://doi.org/10.1016/j.array.2022.100146

Barquero, W. G. (2022). ANALISIS DE PRISMA COMO METODOLOGÍA PARA REVISIÓN SISTEMÁTICA: UNA APROXIMACIÓN GENERAL. Saúde Em Redes, 8(sup1), 339–360. https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Bera, D., Ogbanufe, O., & Kim, D. J. (2023). Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. Decision Support Systems, 171, 113977. https://doi.org/10.1016/j.dss.2023.113977

Bojjagani, S., Brabin, D. R. D., & Rao, P. V. V. (2020). PhishPreventer: A secure authentication protocol for prevention of phishing attacks in mobile environment with formal verification. Procedia Computer Science, 171, 1110–1119. https://doi.org/10.1016/j.procs.2020.04.119

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, *17*(101058), 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Careja, A.-C., & Tapus, N. (2023). Digital identity using blockchain technology. Procedia Computer Science, 221, 1074–1082. https://doi.org/10.1016/j.procs.2023.08.090

Ejaz, A., Mian, A. N., & Manzoor, S. (2023). Life-long phishing attack detection using continual learning. Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-37552-9

Guzmán-Cedillo, L. A., Varela-Castro, W. H., & Briceño-Santacruz, M. de los A. (2020). Ciberseguridad 4.0: Factores que propician el delito de robo de identidad digital por medios informáticos. Repositorio De La Red Internacional De Investigadores En Competitividad, 13, 658–677. Recuperado a partir de https://www.riico.net/index.php/riico/article/view/1818

Hernández Dominguez, A., & Baluja García, W. (2021). Main mechanisms for dealing with phishing in data networks. Revista Cubana de Ciencias Informáticas, 15(4s1), 1-15. http://scielo.sld.cu/pdf/rcci/v15n4s1/2227-1899-rcci-15-04-s1-413.pdf

Kampourakis, V., Kambourakis, G., Chatzoglou, E., & Zaroliagis, C. (2022). Revisiting man- in-the-middle attacks against HTTPS. Network Security, 2022(3). https://doi.org/10.12968/s1353-4858(22)70028-1

Kothamasu, G. A., Venkata, S. K. A., Pemmasani, Y., & Mathi, S. (2023). An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures. International Journal Of Safety And Security Engineering, 13(2), 333-340. https://doi.org/10.18280/ijsse.130215

Marín, V. I. (2022). La revisión sistemática en la investigación en Tecnología Educativa: observaciones y consejos. RiiTE Revista interuniversitaria de investigación en Tecnología Educativa, 13, 62–79. https://doi.org/10.6018/riite.533231

Minu, R. I., Nagarajan, G., Munshi, A., Venkatachalam, K., Almukadi, W., & Abouhawwash, M. (2022). An Edge Based Attack Detection Model (EBAD) for Increasing the Trustworthiness in IoT Enabled Smart City Environment. IEEE Access, 10, 89499-89508. https://doi.org/10.1109/access.2022.3200703

Moreno Arvelo, P. M., Paucar Paucar, C. E., Cajas Parraga, C. M., (2022). Regulación global para evitar la suplantación de identidad digital. Revista Universidad y Sociedad, 14(6), 690-696.
Murillo González, G., Martínez Prats, G., & Vázquez Vidal, V. (2023). Desinformación tecnológica: factores y causas del robo de identidad del cibernauta en el mundo digital. Data and Metadata 2024, 2, 133. https://doi.org/10.56294/dm2023133

Nonvignon, T. Z., Boucif, A. B., & Mhamed, M. (2022). A Copula-Based Attack Prediction Model for Vehicle-to-Grid Networks. Applied Sciences, 12(8), 3830. https://doi.org/10.3390/app12083830

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. Egyptian Informatics Journal, 23(2), 197–214. https://doi.org/10.1016/j.eij.2021.12.003

Ribaux, O., & Souvignet, T. R. (2020). “Hello are you available?” Dealing with online frauds and the role of forensic science. Forensic Science International: Digital Investigation, 33(300978), 300978. https://doi.org/10.1016/j.fsidi.2020.300978

Saharan, S., Laxmi, V., Bezawada, B., & Gaur, M. S. (2021). Scaling & fuzzing: Personal image privacy from automated attacks in mobile cloud computing. Journal Of Information Security And Applications, 60, 102850. https://doi.org/10.1016/j.jisa.2021.102850

Sharma, D., & Selwal, A. (2021). FinPAD: State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives. Pattern Recognition Letters, 152, 225-252. https://doi.org/10.1016/j.patrec.2021.10.013

Sobabe, A., Djara, T., & Vianou, A. (2020). Biometric System Vulnerabilities: A Typology of Metadata. Advances In Science Technology And Engineering Systems Journal, 5(1), 191-200. https://doi.org/10.25046/aj050125

Song, W., Jiang, M., Yan, H., Xiang, Y., Chen, Y., Luo, Y., He, K., & Peng, G. (2020). Android Data-Clone Attack via Operating System Customization. IEEE Access, 8, 199733-199746. https://doi.org/10.1109/access.2020.3035089

Sohrabi, C., Franchi, T., Mathew, G., Kerwan, A., Nicola, M., Griffin, M., Agha, M., & Agha, R. (2021). PRISMA 2020 statement: What’s new and the importance of reporting guidelines. International Journal of Surgery (London, England), 88(105918), 105918. https://doi.org/10.1016/j.ijsu.2021.105918

Tsai, C.-H., Liou, D.-K., & Lee, H.-L. (2024). Blockchain-supported online banking scheme. Egyptian Informatics Journal, 27(100516), 100516. https://doi.org/10.1016/j.eij.2024.100516

Veena, K., Meena, K., Kuppusamy, R., Teekaraman, Y., Angadi, R. V., & Thelkar, A. R. (2022). Cybercrime: Identification and Prediction Using Machine Learning Techniques. Computational Intelligence And Neuroscience, 2022, 1-10. https://doi.org/10.1155/2022/8237421

Zahra, S. R., Chishti, M. A., Baba, A. I., & Wu, F. (2021). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. Egyptian Informatics Journal, 23(2), 197-214. https://doi.org/10.1016/j.eij.2021.12.003
Zarate, A. P., & del Carmen Becerra, M. A. M. (2011). Robo de Identidad y su Incidencia en el Cibercrimen. Org.Ar. https://50jaiio.sadio.org.ar/pdfs/sid/SID-08.pdf