Revisión del Estado del Arte sobre la Seguridad en Redes Wi-Fi Domésticas: Educación de Usuarios en Mejores Prácticas y Riesgos

Santiago Andres Moreno Sanchez, Estudiante de Ingeniería de Sistemas, Departamento de Boyacá, Universidad Santo Tomás – Seccional Tunja, Colombia, Santiago.moreno@usantoto.edu.co

Resumen - Con el crecimiento exponencial de dispositivos conectados, la seguridad en redes Wi-Fi domésticas se ha convertido en una preocupación clave. Muchas conexiones carecen de medidas adecuadas, lo que las hace vulnerables a ataques y accesos no autorizados. El presente estudio tiene como propósito analizar los riesgos y las estrategias recomendadas para mejorar la seguridad en redes Wi-Fi domésticas. A través de esta investigación, se busca proporcionar información útil a los usuarios, permitiéndoles fortalecer la protección de sus redes y reducir el riesgo de ser blanco de ataques cibernéticos. El análisis identificó vulnerabilidades, amenazas y prácticas clave. Las contraseñas débiles fueron la vulnerabilidad más frecuente con un 28.5%, la amenaza más frecuente fueron las vulnerabilidades de IoT con un 21.2% colectivamente. Finalmente en cuanto a prácticas recomendadas se encontró que la utilización de contraseñas fuertes y únicas fue la más efectiva, seguida por la activación del cifrado WPA y la actualización regular de firmware y software.

Palabras clave - Metodología PRISMA, Ciberseguridad, Amenazas, Vulnerabilidades, Prácticas, Wi-Fi, entorno doméstico.

Abstract - With the exponential growth of connected devices, security in home Wi-Fi networks has become a key concern. Many connections lack adequate measures, making them vulnerable to attacks and unauthorized access. The purpose of this study is to analyze the risks and recommended strategies to improve security in home Wi-Fi networks. Through this research, we seek to provide useful information to users, allowing them to strengthen the protection of their networks and reduce the risk of being targeted by cyber-attacks. The analysis identified key vulnerabilities, threats and practices. Weak passwords were the most frequent vulnerability with 28.5%, the most frequent threat was IoT vulnerabilities with 21.2% collectively. Finally, in terms of recommended practices, it was found that the use of strong and unique passwords was the most effective, followed by the activation of WPA encryption and the regular updating of firmware and software.

Keywords: PRISMA Methodology, Cybersecurity, Threats, Vulnerabilities, Practices, Wi-Fi, home environment.

I. INTRODUCCIÓN

Actualmente la información se ha convertido en uno de los activos más valiosos para individuos y empresas. La seguridad de las redes informáticas emerge como un aspecto necesario para garantizar la confidencialidad de los datos. De acuerdo con [1] cuando la pandemia de COVID-19 comenzó a extenderse globalmente, se aceleró la transformación digital; la personas se vieron obligadas a aislarse, pero las actividades en ámbito educativo o empresarial no podían detenerse. Así, surgieron nuevas estrategias que priorizaban el uso de la tecnología, dando mayor relevancia a conceptos como el teletrabajo y la educación a distancia. Bajo este contexto es fundamental analizar las vulnerabilidades en las redes informáticas debido a la creciente dependencia de la tecnología en todos los sectores. Con el aumento de actividades digitales, las amenazas cibernéticas se han intensificado, poniendo en riesgo la información personal de los usuarios.

Según [2], la ciberseguridad es aquella práctica que busca la protección de redes y sistemas de ataques digitales, los cuales tienen como propósito el acceso no autorizado a la información confidencial, con el objetivo de extorsionar a las víctimas. [3] señala que muchas empresas tienden a delegar la responsabilidad de los problemas de ciberseguridad únicamente a sus departamentos de tecnología y a la infraestructura de protección. Esta perspectiva conlleva una grave falta: se ignora la importancia de la concientización entre los empleados, quienes suelen ser el eslabón más vulnerable en la cadena de seguridad. Este enfoque reactivo, en el que las organizaciones solo se dan cuenta de la necesidad

Tabla 1. Preguntas de investigación

de mejorar sus medidas de seguridad tras sufrir un incidente, no solo puede resultar en pérdidas económicas, sino que también perjudica su reputación y puede acarrear complicaciones legales. El mismo autor subraya que muchas empresas no están dispuestas a invertir en programas de

ID	Pregunta de investigación	Motivación
PI1	¿Cuáles son las principales vulnerabilidades en las redes Wi-Fi domésticas identificadas en la literatura desde 2018 hasta 2025?	Identificar las principales brechas de seguridad en redes Wi-Fi domésticas más recientes
PI2	¿Qué factores contribuyen a la falta de concientización en ciberseguridad entre usuarios domésticos?	Analizar las causas más comunes que influyen en la falta de educación sobre ciberseguridad
PI3	¿Qué buenas prácticas se recomiendan para fortalecer la seguridad de la información a través de dispositivos interconectados en redes Wi-Fi y que sean accesibles para usuarios no especializados?	Recopilar buenas prácticas accesibles para fortalecer la seguridad de la información en redes Wi-Fi del hogar.

formación y concienciación hasta que se enfrentan a situaciones adversas, perpetuando así un ciclo de vulnerabilidad.

Lo mencionado no solo es evidente en las organizaciones, sino que también se manifiesta con usuarios domésticos, quienes a menudo subestiman la importancia de la ciberseguridad en su vida diaria. Esta creencia es apoyada por [4], donde se realizó un estudio de ciberseguridad a familias Colombianas determinando, por ejemplo, si cierto número de usuarios son conscientes de la seguridad de una página web. Los resultados indicaron que un gran porcentaje de los participantes carece de conocimientos sobre cómo identificar un sitio web seguro, con un 59.3% contestando con un sí y un 40.7% con un no. [5] menciona que, aunque existan medidas de protección como firewalls o sistemas de detección de intrusiones el factor humano siempre tendrá mayor relevancia para que la mayor parte de ataques se puedan realizar con éxito.

Al igual que muchas empresas, los usuarios domésticos tienden a no invertir en educación y formación hasta que se enfrentan a un incidente, como una violación de datos o un ataque de ransomware. Esta falta de preparación puede llevar no solo a pérdidas económicas, sino también a un daño irreversible en la privacidad y la seguridad de sus familias.

La seguridad de redes abarca un conjunto diverso de prácticas diseñadas para salvaguardar los sistemas de información contra ataques maliciosos y otros riesgos potenciales. Desde la autenticación de usuarios hasta la gestión de vulnerabilidades, cada aspecto de la seguridad de redes desempeña un papel importante en la protección de la infraestructura informática contra amenazas internas y externas. En el contexto de las redes Wi-Fi domésticas, muchas veces utilizadas sin una adecuada protección, los usuarios suelen desconocer las mejores prácticas para garantizar la seguridad de sus conexiones, exponiéndose a riesgos significativos como la pérdida de datos o la intrusión no autorizada.

Con base a lo mencionado, se realizó una revisión sistemática de la literatura utilizando la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) con el objetivo de analizar:

1. Las vulnerabilidades más frecuentes en redes Wi-Fi desde 2018 hasta 2025.
2. Las causas más comunes que influyen en la falta de educación sobre ciberseguridad entre usuarios domésticos.
3. Prácticas recomendadas accesibles para mejorar la seguridad de redes Wi-Fi de usuarios en el hogar.

Este proyecto tiene como principal objetivo analizar información sobre los riesgos y las prácticas recomendadas para la seguridad en redes Wi-Fi domésticas. A través de esta investigación, se busca brindar información relevante a los usuarios sobre cómo mejorar la protección de sus redes y evitar ser víctimas de atacantes cibernéticos, contribuyendo así a la disminución de vulnerabilidades y al aumento de la protección de su información personal, en un entorno cada vez más interconectado. Este artículo de divulgación se desenvuelve de la siguiente manera: en la segunda sección se describen los métodos para el desarrollo del estado del arte. En la sección tres se presentan los resultados de la investigación; en la cuarta sección se encontrara la discusión de la información recolectada y finalmente, una quinta sección presenta las conclusiones.

II. METODOLOGIA

Para el desarrollo de esta revisión se empleó la metodología PRISMA con el fin de buscar y recopilar la información. Esta investigación consistió en clasificar las amenazas, vulnerabilidades y prácticas de seguridad más comunes en redes Wi-Fi domésticas durante los años mencionados, así como en identificar las causas más frecuentes de los ataques dirigidos a las redes de los usuarios. Esta investigación se desarrolla en cuatro etapas: la primera consiste en definir las preguntas de investigación; la segunda establece las estrategias de búsqueda y las fuentes de información; la tercera se enfoca en la selección y clasificación de los estudios recopilados; y la cuarta se encarga del análisis y síntesis de los hallazgos.

A. Preguntas de investigación

La Tabla **1** presenta tres preguntas de investigación junto con una descripción de los motivos que justifican su selección.

Tabla 2. Terminos para elaboración de cadena de busqueda

B. Búsqueda literaria

1. Fuentes de datos

Palabras clave	Palabras similares
Cybersecurity	Information protection
Wi-Fi networks	Wireless networks, WLAN
Wi-Fi vulnerabilities	Wi-Fi weaknesses, Wi-fi flaws
User awareness	User education, user training
Security practices	Security guidelines, attacks mitigation

Esta investigación se llevó a cabo utilizando tres repositorios digitales: Scopus, IEEE y ScienceDirect. Durante la revisión, se recopiló información clave para la selección de estudios primarios, considerando el título y el resumen de cada documento, incluyendo artículos de revistas y ponencias de conferencias. Además, se establecieron los términos de búsqueda (ver Tabla **2Error! Reference source not found.**) junto con sinónimos y términos relacionados para ampliar la bibliografía analizada.

2. Estrategias de búsqueda

Con las palabras clave definidas se realizaron varios filtros de búsqueda (ver Tabla **4**). Estos filtros incluyen la delimitación por años de publicación y palabras clave específicas (tanto en inglés como en español) con el uso de conectores booleanos como AND, OR y NOT, este filtro fue modificado de acuerdo con la estructura sugerida en cada repositorio.

C. Selección de estudios primarios

En la búsqueda inicial de las 3 bases de datos se escogieron 1030 estudios entre el año 2009 a 2025. El gráfico ilustra el proceso de selección sistemática de estudios nuevos utilizando bases de datos y registros, siguiendo el esquema brindado por PRISMA [6]. La metodología comprende tres fases principales: 1) Se realizo la identificación de los estudios utilizando palabras clave asociadas con la temática (ver Tabla **2**), recopilando 1030 registros de tres bases de datos: Scopus (53), Science Direct (403) y IEEE (574). Se eliminaron 62 registros duplicados y 217 por otras razones, dejando un total de 751 estudios para revisión. 2) En el paso de cribado o prueba de Screening se realizó la selección de estudios entre el año 2018 a 2025. En el filtro también se incluyen artículos y conferencias publicadas en inglés, junto a la revisión de sus títulos, términos clave y resúmenes, lo que resultó en la exclusión de 681 registros. De los 751 documentos iniciales, se seleccionaron 70 informes para su revisión detallada, sin que fuera necesario descartar informes por falta de acceso. 3) Y finalmente en el paso de inclusión se evaluaron los 70 informes para determinar su relevancia y calidad. 12 fueron excluidos por centrarse en un ámbito empresarial y 37 más porque no se relacionaban con las preguntas de investigación. Finalmente, se incluyeron 23 estudios que cumplían con todos los criterios establecidos.

Para generar la gráfica (ver Figura **1**), se empleó el paquete de R junto con la aplicación Shiny para la creación de diagramas de flujo PRISMA 2020. Esta herramienta permitió estructurar visualmente el proceso de selección de estudios, facilitando su interpretación y análisis.

1. Criterios de inclusión

Se incluyen estudios publicados entre 2018 y 2025, así como artículos de investigación revisados por pares, tesis académicas y reportes de conferencias que aporten hallazgos significativos sobre la seguridad en redes Wi-Fi en entorno domésticos. Así mismo se incluyen investigaciones que contengan información sobre vulnerabilidades y prácticas recomendadas en la misma temática presentes en los idiomas inglés y español.

2. Criterios de exclusión

Se excluyen investigaciones que no aborden la temática en un contexto doméstico, como aquellas centradas en el ámbito empresarial. También se descartarán estudios que no cuenten con un respaldo suficiente de la información presentada, es decir, aquellos que tengan menos de 15 referencias.

D. Extracción de datos

Por medio de una plantilla se generó el proceso de extracción de la información más relevante de los estudios más relevantes. Para la construcción de esta se utilizaron las siguientes características: a) referencia, b) año de publicación, c) temática principal y d) contribuciones más importantes.

III. RESULTADOS

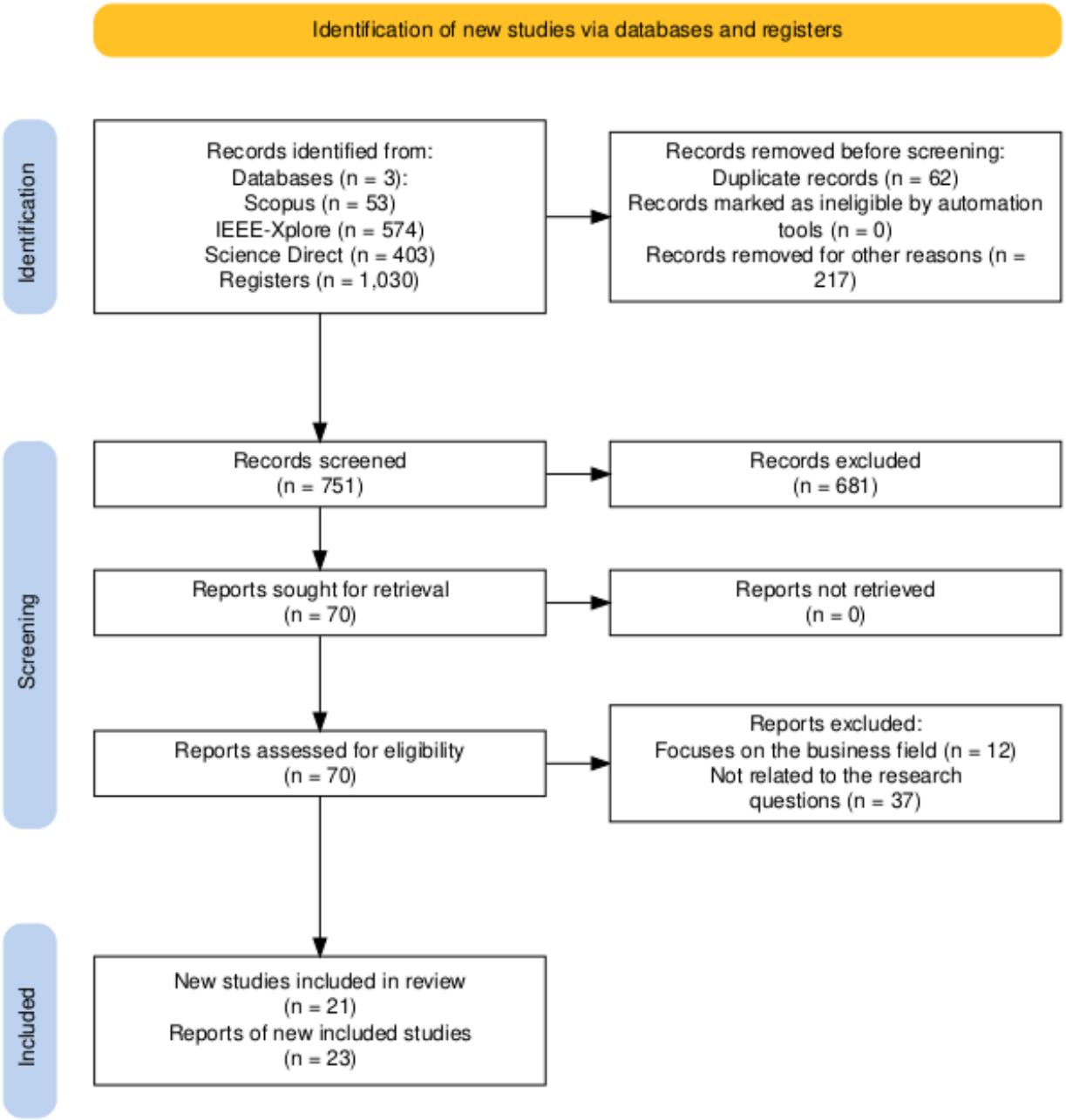
La seguridad de las redes Wi-Fi del hogar han cobrado mayor relevancia debido al incremento del uso de internet para actividades como el estudio, el trabajo remoto y el acceso a servicios digitales. Estos cambios han ampliado la dependencia de las redes en los hogares, lo que las convierte en un objetivo atractivo para los ciberdelincuentes. A su vez, el auge de los dispositivos IoT ha aumentado las superficies de ataque, lo que hace necesario reforzar las medidas de seguridad para proteger tanto los datos personales como las infraestructuras digitales del hogar. Desde 2015, la investigación en detección de anomalías para identificar ciberataques ha crecido, especialmente a partir de 2019, en parte por el aumento del teletrabajo durante la pandemia. La mayoría de los estudios se centran en enfoques de detección basados en red y estrategias centralizadas para validar modelos, identificando múltiples tipos de ataques, como DoS y DDoS. Sin embargo, las soluciones distribuidas son menos viables en entornos domésticos debido a la limitada capacidad de procesamiento de los dispositivos.

Tabla 3. Año, temática principal y principales contribuciones de (N=23) estudios primarios

ID	Refer.	Año	Tema	Principales contribuciones
1	[7]	2024	Actividades de ciberseguridad para educación y diseño curricular	Revisión de enfoques educativos y programas de ciberseguridad, presentación de estudios de caso globales sobre educación en ciberseguridad.
2	[8]	2025	Vulnerabilidades en dispositivos inteligentes del hogar	Identificación de cuatro vulnerabilidades desconocidas en dispositivos del ecosistema Tapo de TP-Link; divulgación responsable de las fallas.
3	[9]	2021	Ciberseguridad en hogares inteligentes y estándares	Crítica a los estándares de ciberseguridad de IoT, argumentando que se enfocan demasiado en arquitecturas en la nube y no consideran el enfoque emergente de Edge Computing.
4	[10]	2024	Integración de medidas de ciberseguridad basadas en IA y convencionales en la educación superior en línea	Este artículo aborda los desafíos y oportunidades de integrar medidas de ciberseguridad basadas en inteligencia artificial junto con enfoques tradicionales en la educación superior en línea. el estudio compara las técnicas de IA y convencionales para mitigar las amenazas cibernéticas.
5	[11]	2025	CyberFamily: un juego colaborativo para aumentar la conciencia de ciberseguridad en los niños	Este estudio presenta CyberFamily, un juego colaborativo diseñado para aumentar la conciencia de ciberseguridad entre los niños de 9 a 12 años a través de la colaboración padre-hijo.
6	[12]	2024	Revisión crítica de marcos de conciencia en ciberseguridad y modelos de capacitación	Este estudio analiza de manera cuantitativa varios enfoques de capacitación y concientización en ciberseguridad para evaluar su eficacia en la reducción de costos y la disminución de incidentes de seguridad en las empresas.
7	[13]	2018	Mejores prácticas de ciberseguridad entre los estudiantes polacos	Este estudio analiza el conocimiento y los patrones de comportamiento de los estudiantes polacos sobre ciberseguridad, con un enfoque en las mejores prácticas y la protección de contraseñas. Se reveló que las universidades no estaban promoviendo prácticas de comportamiento adecuadas ni ofreciendo formación profesional en ciberseguridad.
8	[14]	2023	Evaluación comparativa de los factores humanos en ciberseguridad: implicaciones para la gobernanza cibernética	Este estudio compara la conciencia sobre ciberseguridad en la población joven, educada y experta en tecnología de los Emiratos Árabes Unidos con la de los Estados Unidos. Los resultados muestran diferencias clave en la interpretación de la conciencia de ciberseguridad y factores humanos críticos entre las dos poblaciones.
9	[15]	2022	Conciencia sobre ciberseguridad en la educación en línea: análisis de un estudio de caso	Este estudio examina el nivel de conocimiento sobre ciberseguridad entre los estudiantes de la Universidad Kyrgyz-Turkish Manas, en relación con la educación a distancia. A pesar del aumento de ciberataques globales, los resultados revelan que los estudiantes tienen un conocimiento limitado sobre ciberseguridad y sus efectos.
10	[16]	2021	Ingeniería social en ciberseguridad: mecanismos de efecto, vulnerabilidades humanas y métodos de ataque	Este estudio propone un modelo conceptual para describir cómo funcionan los ataques de ingeniería social en ciberseguridad, identificando tres entidades clave: mecanismo de efecto, vulnerabilidades humanas y métodos de ataque.
11	[17]	2022	Impacto de la formación en seguridad informática.	Se evaluaron diversas estrategias de formación en seguridad informática y su impacto en el conocimiento, actitud y comportamiento de los empleados. Los resultados sugieren que todos los métodos aumentan el conocimiento de manera equivalente, pero tener más de un método de entrega mejora las actitudes de los usuarios.
12	[18]	2021	Efecto de la publicidad de brechas de datos en	El estudio investigó cómo la publicidad de brechas de datos afecta la concienciación sobre seguridad informática. Se descubrió que la

			la concienciación sobre seguridad informática.	publicidad de brechas de datos explica el 6.7% de la ISA, logrando el mayor coeficiente en comparación con otros factores conocidos.
13	[19]	2023	Ética en la ciberseguridad y futuros dilemas éticos.	El estudio explora los problemas éticos emergentes en la ciberseguridad, diferenciando entre señales fuertes (preocupaciones conocidas) y señales débiles (preocupaciones menos discutidas). En este se identifican dilemas éticos futuros en la ciberseguridad que podrían definir su evolución.
14	[20]	2021	Métodos de autenticación y prácticas de seguridad en línea.	Se identificaron tres métodos principales de autenticación: autenticación por contraseña, biométrica y multifactorial. Se concluyó que la autenticación multifactorial es la más segura y la más recomendada, sugiriendo la implementación futura de autenticación de tres factores y modelos multibiométricos para mejorar la seguridad de los usuarios en la computación en la nube.
15	[21]	2021	Ciberseguridad durante la pandemia de COVID-19	En este estudio se analiza la importancia de la educación y las políticas de seguridad en la protección contra ciber amenazas.
16	[22]	2025	Estrategias de defensa contra ataques DDoS usando aprendizaje profundo	El artículo analiza cómo los ataques DDoS, especialmente con la expansión de dispositivos IoT, son una amenaza creciente para los sistemas en red. Se categorizan estos ataques en tres tipos principales: volumétricos, basados en protocolos y en la capa de aplicación.
17	[23]	2023	Conciencia cibernética y políticas de seguridad entre trabajadores remotos	El estudio aborda los desafíos de la ciberseguridad en el contexto del trabajo remoto, destacando que, a pesar de las creencias comunes, el trabajo remoto está asociado positivamente con una mayor conciencia cibernética y con la adopción de medidas de seguridad.
18	[24]	2024	El factor humano en la ciberseguridad en entornos de trabajo remoto	El estudio presenta una herramienta diagnóstica para evaluar el comportamiento cibernético en entornos de trabajo remoto, identificando cuatro perfiles de riesgo: Cautelosos inconscientes, Buscadores de riesgos inconscientes, Cautelosos conscientes y Buscadores de riesgos conscientes. Se destaca la importancia del comportamiento humano en la ciberseguridad y la necesidad de adaptar las políticas a los distintos perfiles de riesgo.
19	[25]	2022	La pandemia de COVID-19 y la seguridad de las redes WLAN	El estudio analiza cómo la pandemia de COVID-19 afectó la seguridad de las redes WLAN en el suroeste de Finlandia. A pesar de un aumento del 50.2% en la implementación de WLAN durante la pandemia, no se observó una mejora significativa en la seguridad de estas redes. Aunque la mayoría de las redes estaban cifradas con el protocolo WPA2, el uso del protocolo más reciente, WPA3, no aumentó notablemente.
20	[26]	2022	Ataques Multi-Canal Man-in-the-Middle en redes Wi-Fi protegidas	El artículo revisa los ataques Multi-Canal Man-in-the-Middle que manipulan tramas inalámbricas cifradas entre dos puntos legítimos, destacando ataques como KRACK en 2017 y FragAttacks en 2021. Aunque estos ataques afectan principalmente dispositivos IoT, no existe una revisión holística de los mismos en la literatura.
21	[27]	2023	Intenciones de los usuarios hacia la seguridad en redes de hogares inteligentes IoT	El estudio examina los factores cognitivos y psicológicos que influyen en la intención de los usuarios de asegurar sus redes domésticas inteligentes. Aplicando la teoría del comportamiento planificado y la teoría de la elección racional, se propone un modelo que explica estas intenciones de seguridad.
22	[28]	2022	Seguridad en Internet de las Cosas y el impacto de tecnologías emergentes	El artículo examina los desafíos de seguridad y privacidad en los dispositivos IoT, que, debido a limitaciones de hardware, software y redes, enfrentan dificultades para implementar soluciones de seguridad convencionales.
23	[29]	2018	Amenazas ciber físicas en el hogar inteligente	El artículo propone una taxonomía para clasificar las amenazas cibernéticas en hogares inteligentes, teniendo en cuenta tanto los vectores de ataque como el impacto potencial en los sistemas y los residentes. Se identifican y clasifican 25 tipos de ataques, mostrando cómo configuraciones legítimas pero vulnerables pueden generar vectores de ataque secundarios.

Figura 1. Diagrama de flujo PRISMA para selección de estudios primarios



Repositorio	Cadena de búsqueda	Primer filtro	Segundo filtro	Tercer filtro
Scopus	TITLE-ABS-KEY (("Cybersecurity" OR "Information protection") AND ("Security practices" OR "Security guidelines" OR "Attacks mitigation") AND ("home" OR "domestic environment" OR "residential") AND NOT ("business" OR "enterprise")) AND PUBYEAR > 2017 AND PUBYEAR <2025	33	14	8
IEEE	("Cybersecurity" OR "Information protection") AND ("Wi-Fi networks" OR "Wireless networks" OR "WLAN") AND ("Wi-Fi vulnerabilities" OR "Wi-Fi weaknesses" OR "Wi-Fi flaws") AND ("home" OR "domestic environment" OR "residential") NOT ("enterprise" OR "corporate" OR "industrial")	432	39	6
Science direct	Cybersecurity AND (“User awareness” OR “User education”) NOT Business	286	17	9

Tabla 4. Filtros de búsqueda

1. Vulnerabilidades de redes Wi-Fi del hogar

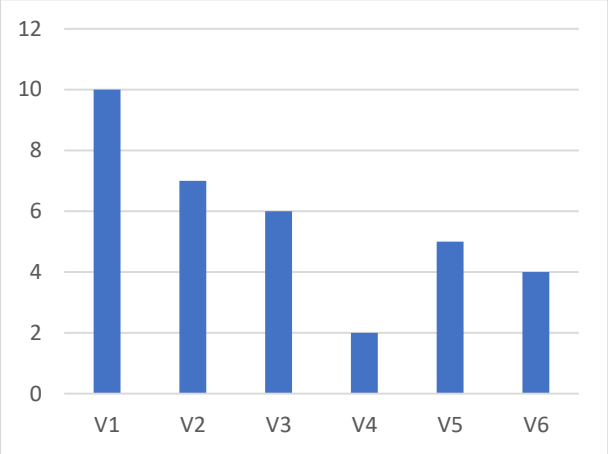
Una vulnerabilidad de red es una debilidad o fallo en la infraestructura de una red que puede ser explotado por atacantes para acceder a sistemas, robar datos o interrumpir el servicio. Estas vulnerabilidades pueden ser causadas por configuraciones incorrectas, software desactualizado o falta de medidas de seguridad. Bajo un entorno doméstico, las redes Wi-Fi suelen ser propensas a diversas vulnerabilidades debido a configuraciones inseguras y falta de medidas de protección adecuadas. En la Tabla **5** se destacan las vulnerabilidades más comunes en las investigaciones más recientes, mostrando patrones recurrentes en la seguridad de estas redes. En la Figura **2** se puede ver la frecuencia de cada una con base en el punto de investigación de cada estudio.

La vulnerabilidad más destacada por los investigadores se encuentra en las contraseñas débiles, predeterminadas o reutilizadas (V1), ya que facilitan el acceso no autorizado a la red. Al mismo tiempo, el cifrado débil (V2), que permite la interceptación de datos, y la falta de control de acceso (V3), que deja expuesta la red a usuarios no autorizados, representan un problema crítico en la seguridad de las redes domésticas.

Tabla 5. Vulnerabilidades de redes

ID	Nombre de vulnerabilidad	Referencia
V1	Contraseñas débiles, predeterminadas o reutilizadas	[7], [10], [11], [13], [15], [27], [30], [31], [32], [33]
V2	Cifrado Débil	[7], [8], [14], [26], [28], [31], [33]
V3	Falta de control de acceso	[8], [12], [19], [34], [35], [36]
V4	Uso de software y servicios no seguros.	[7], [25]
V5	Falta de parches y actualizaciones de seguridad en software	[24], [26], [28], [34], [37]
V6	Configuraciones predeterminadas en hardware de red	[9], [29], [38], [39]

Figura 2. Frecuencia de Vulnerabilidades de red



2. Amenazas de redes Wi-Fi del hogar

Una amenaza de red es cualquier acción malintencionada que busca explotar vulnerabilidades para comprometer la seguridad, disponibilidad o privacidad de una red. Estas pueden incluir ataques dirigidos, malware o intentos de interceptación de datos. En la Tabla **6**, se destacan las amenazas más comunes según investigaciones recientes, evidenciando la creciente preocupación por los ataques dirigidos a redes domésticas. En la Figura **3**, se representa la frecuencia con la que estas amenazas han sido reportadas en diferentes estudios.

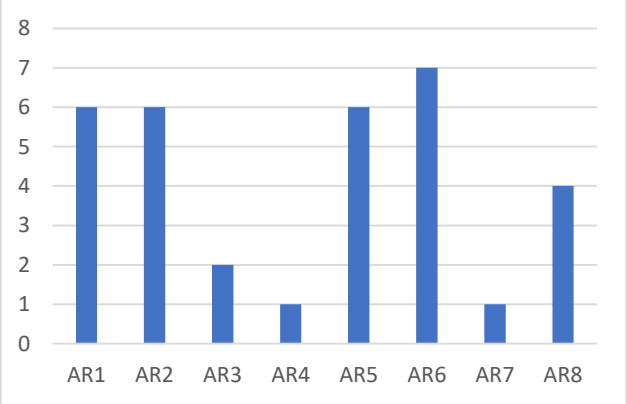
Entre las amenazas más destacadas, las vulnerabilidades de IoT (AR6) representan el mayor riesgo, ya que los dispositivos inteligentes suelen contar con medidas de seguridad insuficientes, facilitando su explotación por atacantes. El ataque Man-in-the-Middle (AR1), que permite interceptar y manipular la comunicación en la red, y la Denegación de Servicio (AR2), que satura la red para dejarla inoperable, también son problemas recurrentes. Además, tácticas como el Phishing (AR5), utilizadas para engañar a los usuarios y robar

credenciales, siguen siendo un vector de ataque relevante en el ámbito doméstico.

Tabla 6. Amenazas de red

ID	Nombre de amenaza	Referencias
AR1	Ataque Man-in-the-Middle	[7], [8], [28], [34] [33], [40]
AR2	Denegación de Servicio	[7], [8], [14], [26], [28], [31], [33]
AR3	Ransomware	[19], [41]
AR4	Sniffing de Red	[23]
AR5	Phishing	[10], [17], [21], [23], [42], [43]
AR6	Vulnerabilidades de IoT	[7], [31], [34], [40], [44], [45], [46]
AR7	Injección de codigo	[37]
AR8	Ataques DDoS	[8], [28], [31], [37]

Figura 3. Frecuencia de amenazas de red



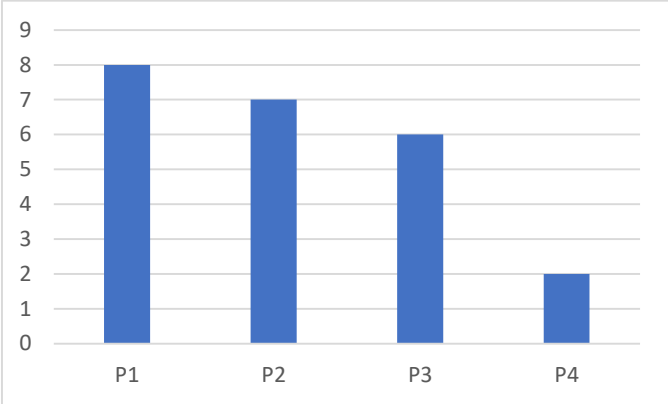
3. Prácticas recomendadas de ciberseguridad

Una práctica de ciberseguridad en redes es una medida preventiva o correctiva que reduce el riesgo de ataques cibernéticos y protege la integridad, confidencialidad y disponibilidad de la información. En la Tabla **7**, se presentan las prácticas de seguridad más recomendadas según investigaciones recientes, destacando estrategias efectivas para mitigar vulnerabilidades y amenazas en redes Wi-Fi. En la Figura **4**, se ilustra la frecuencia con la que estas prácticas han sido mencionadas en distintos estudios. Las más destacadas son el uso de contraseñas fuertes y únicas (P1), la activación del cifrado WPA3 en la red Wi-Fi (P2) y la actualización regular de firmware y software (P3). P1 previene accesos no autorizados, P2 refuerza la protección de los datos transmitidos y P3 corrige vulnerabilidades explotables reduciendo significativamente los riesgos de ataque en redes del hogar.

Tabla 7. Practicas de ciberseguridad

ID	Nombre de práctica	Referencia
P1	Uso de contraseñas fuertes y únicas	[7], [9], [11], [15], [18], [30], [31], [32]
P2	Activar el cifrado WPA3 en la red Wi-Fi	[14], [24], [25], [28], [33] [36], [46]
P3	Actualización regular de firmware y software	[8], [17], [23], [32], [34], [37]
P4	Desactivar la administración remota del router	[7], [39]

Figura 4. Frecuencia de prácticas de ciberseguridad



IV. DISCUSIÓN

PI1: ¿Cuáles son las principales vulnerabilidades en las redes Wi-Fi domésticas identificadas en la literatura desde 2018 hasta 2025?

Según el grafico de vulnerabilidades de red (ver Figura **2**) las vulnerabilidades más destacadas son las siguientes:

- Contraseñas débiles, predeterminadas o reutilizadas (V1): [47][15] mencionan que el uso de contraseñas poco seguras, como combinaciones cortas o fácilmente adivinables, representa una de las principales amenazas en redes Wi-Fi en general. Además, muchas personas no cambian la clave predeterminada del router, lo que permite a los atacantes utilizar bases de datos públicas con contraseñas conocidas para acceder a la red. La reutilización de contraseñas en diferentes servicios también incrementa el riesgo, ya que si una de ellas se filtra en una brecha de seguridad, puede ser utilizada para comprometer la red Wi-Fi y otros sistemas asociados.

- Cifrado Débil (V2): El cifrado débil es una de las principales vulnerabilidades en las redes de hogares inteligentes, ya que permite que los atacantes intercepten y manipulen la comunicación. [33] indica que muchas amenazas en IoT surgen debido a mecanismos de cifrado inseguros, lo que facilita ataques como la suplantación e intercepción de

datos. También menciona que el uso de cifrado fuerte en redes domésticas reduce significativamente la exposición a ataques como el eavesdropping y el hacking de routers, evitando que los dispositivos IoT sean vulnerables a accesos no autorizados.

- Falta de parches y actualizaciones de seguridad en software (V5): Según [48] actualizar el software regularmente es una estrategia clave para mitigar amenazas cibernéticas, ya que los desarrolladores lanzan parches para corregir vulnerabilidades explotables por hackers. Dado que los ciberdelincuentes evolucionan constantemente sus técnicas, no actualizar el software deja a los usuarios expuestos a ataques. Además, las actualizaciones no solo mejoran la seguridad, sino que también corrigen errores y optimizan el rendimiento del sistema, evitando fallos y pérdida de datos. El mismo autor recomienda activar actualizaciones automáticas para garantizar protección sin intervención manual.

PI2: ¿Qué factores contribuyen a la falta de concientización en ciberseguridad entre usuarios domésticos?

La falta de concientización en ciberseguridad entre los usuarios domésticos es un problema recurrente que expone las redes Wi-Fi a diversos riesgos. A menudo, los usuarios desconocen las mejores prácticas de seguridad, lo que facilita la explotación de vulnerabilidades por parte de ciberdelincuentes. Según [17] [49] factores como la falta de educación en seguridad digital, la percepción errónea sobre los riesgos y la complejidad técnica de las medidas de protección contribuyen a este problema:

- Falta de educación en seguridad digital: [17] afirma que muchas personas no han recibido formación sobre ciberseguridad y desconocen los riesgos asociados a una mala configuración de sus dispositivos. La ausencia de programas educativos sobre seguridad informática en escuelas y entornos laborales hace que los usuarios no adquieran conocimientos básicos sobre cómo proteger sus redes. Sin esta información, es común que no cambien contraseñas predeterminadas, no actualicen sus routers o no reconozcan intentos de ataque.

- Percepción errónea sobre los riesgos: Según [17] los usuarios subestiman la posibilidad de ser víctimas de un ciberataque, creyendo que los ciberdelincuentes solo se enfocan en grandes empresas o individuos con información valiosa. Esta falsa sensación de seguridad los lleva a ignorar medidas básicas de protección, como activar firewalls, usar contraseñas seguras o restringir el acceso a su red.

- Complejidad técnica de las medidas de seguridad: Algunas configuraciones avanzadas de seguridad pueden ser difíciles de entender para usuarios sin experiencia en redes y tecnología. [36] destaca que muchos usuarios tienen un bajo nivel de conciencia en ciberseguridad y no siguen las guías de seguridad al configurar sus dispositivos. Se identifican malas prácticas, como la autenticación forzada en dispositivos Apple y la falta de configuración adecuada en Android. Además, pocos usuarios emplean identidades anónimas o direcciones MAC aleatorias, exponiendo su información personal. Incluso en comunidades con formación técnica, hay desinterés en comprender los riesgos de seguridad.

PI3: ¿Qué buenas prácticas se recomiendan para fortalecer la seguridad de la información a través de dispositivos interconectados en redes Wi-Fi y que sean accesibles para usuarios no especializados?

Para fortalecer la seguridad de la información en redes Wi-Fi con dispositivos interconectados, es fundamental adoptar buenas prácticas accesibles para usuarios sin conocimientos técnicos avanzados. Estas medidas ayudan a reducir vulnerabilidades y proteger los datos personales de accesos no autorizados. Las prácticas más recomendadas se encuentran en la Tabla **7**, y se pueden analizar las más frecuentes en la Figura 5, entre las cuales destacan:

- Uso de contraseñas fuertes y únicas: Según [32], [50] configurar contraseñas complejas y diferentes para cada servicio es una de las maneras más efectivas de evitar accesos no autorizados. Se recomienda utilizar combinaciones de letras mayúsculas y minúsculas, números y símbolos, con una longitud mínima de 12 caracteres. Además, cambiar periódicamente la contraseña del Wi-Fi y evitar el uso de claves predeterminadas o fáciles de adivinar dificulta los ataques de fuerza bruta y diccionario

- Activar el cifrado WPA3 en la red Wi-Fi: [28] menciona que WPA3 es una medida de seguridad recomendada para proteger la conexión Wi-Fi en varios dispositivos IoT. Específicamente, señala que Google Nest utiliza WPA3 para unirse a la red Wi-Fi, asegurando la comunicación con TLS. También recomienda el uso de este protocolo para proteger la conexión de sensores de calidad del aire y asistentes de voz, asegurando la encriptación de datos. En general, destaca a WPA3 como una mejora en la seguridad de redes inalámbricas, reforzando la protección contra ataques.

V. CONCLUSIONES

El análisis de seguridad en redes Wi-Fi domésticas ha permitido identificar las principales vulnerabilidades, amenazas y prácticas recomendadas, proporcionando una visión clara sobre los riesgos más relevantes. Entre las vulnerabilidades más destacadas, la más frecuente fue "Contraseñas débiles, predeterminadas o reutilizadas", presente en el 28.5% de los casos, seguida por "Cifrado débil" con 22.8% y "Falta de control de acceso" con 17.1%. En cuanto a las amenazas, las vulnerabilidades de IoT fueron las más registradas, representando el 21.2% de los incidentes, seguidas por los ataques Man-in-the-Middle, Denegación de Servicio y Phishing, cada uno con un 18.1%. Respecto a las prácticas de seguridad más efectivas, la utilización de contraseñas fuertes y únicas fue la estrategia más recomendada, con un 34.7%, seguida por la actualización regular de firmware y software (30.4%) y la activación del cifrado WPA3 en la red Wi-Fi (26.09%). Estos hallazgos evidencian la importancia de reforzar la educación en seguridad digital y fomentar la adopción de buenas prácticas entre los usuarios domésticos. La implementación de estas

medidas puede reducir significativamente la exposición a ataques cibernéticos y mejorar la protección de la información en redes Wi-Fi del hogar.

REFERENCES

[1] J. G. Morales Rojas, "Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial," *Repositorio Institucional Universidad Piloto de Colombia*, 2022.

[2] U. Urquijo and A. Climaco, "Evaluación de ataque ransomware en equipos de cómputo del sector hogar con sistemas operativos windows 11 home," *Repositorio Institucional Universidad Cooperativa de Colombia.*, 2024, Accessed: Mar. 02, 2025. [Online]. Available: https://repository.ucc.edu.co/entities/publication/fdab6067-6859-4344-8a63-325d43d3c5bb

[3] C. E. Pardo Ferro, "Amenazas en la red : entrando al mundo de los ciberataques (Ingeniería Social, Phishing y Malwave)," *instname:Universidad Piloto de Colombia*, Apr. 2018, Accessed: Mar. 02, 2025. [Online]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/2647

[4] J. Fabian *et al.*, "Estrategias para la concienciación en seguridad de la Información en la Familia," 2022, *Fundación Universitaria Los Libertadores. Sede Bogotá.* Accessed: Mar. 02, 2025. [Online]. Available: http://hdl.handle.net/11371/5036

[5] D. Feito, J. Manuel Vázquez, N. Rubén, and P. Jove, "Análisis, diseño e implementación de una aplicación web de concienciación sobre ciberseguridad," 2023, Accessed: Mar. 02, 2025. [Online]. Available: https://ruc.udc.es/dspace/handle/2183/33011

[6] V. Mishra and M. P. Mishra, "PRISMA FOR REVIEW OF MANAGEMENT LITERATURE – METHOD, MERITS, AND LIMITATIONS – AN ACADEMIC REVIEW," *Review of Management Literature*, vol. 2, pp. 125–136, Nov. 2023, doi: 10.1108/S2754-586520230000002007/FULL/EPUB.

[7] M. Ismail *et al.*, "Cybersecurity activities for education and curriculum design: A survey," *Computers in Human Behavior Reports*, vol. 16, p. 100501, Dec. 2024, doi: 10.1016/J.CHBR.2024.100501.

[8] D. Bonaventura, S. Esposito, and G. Bella, "A case of smart devices that compromise home cybersecurity," *Comput Secur*, vol. 151, p. 104286, Apr. 2025, doi: 10.1016/J.COSE.2024.104286.

[9] S. Piasecki, L. Urquhart, and P. D. McAuley, "Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards," *Computer Law & Security Review*, vol. 42, p. 105542, Sep. 2021, doi: 10.1016/J.CLSR.2021.105542.

[10] M. M. A. Parambil *et al.*, "Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects," *Computers and Education: Artificial Intelligence*, vol. 7, p. 100327, Dec. 2024, doi: 10.1016/J.CAEAI.2024.100327.

[11] F. Quayyum and L. Jaccheri, "CyberFamily: A collaborative family game to increase children's cybersecurity awareness," *Entertain Comput*, vol. 52, p. 100826, Jan. 2025, doi: 10.1016/J.ENTCOM.2024.100826.

[12] H. Taherdoost, "A Critical Review on Cybersecurity Awareness Frameworks and Training Models," *Procedia Comput Sci*, vol. 235, pp. 1649–1663, Jan. 2024, doi: 10.1016/J.PROCS.2024.04.156.

[13] O. Szumski, "Cybersecurity best practices among Polish students," *Procedia Comput Sci*, vol. 126, pp. 1271–1280, Jan. 2018, doi: 10.1016/J.PROCS.2018.08.070.

[14] M. U. Shah, F. Iqbal, U. Rehman, and P. C. K. Hung, "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance," *IEEE Access*, vol. 11, pp. 87970–87984, 2023, doi: 10.1109/ACCESS.2023.3296580.

[15] M. E. Erendor and M. Yildirim, "Cybersecurity Awareness in Online Education: A Case Study Analysis," *IEEE Access*, vol. 10, pp. 52319–52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[16] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

[17] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

[18] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021, doi: 10.1109/ACCESS.2021.3107426.

[19] A. Pawlicka, M. Pawlicki, R. Kozik, and M. Choras, "What Will the Future of Cybersecurity Bring Us, and Will It Be Ethical? The Hunt for the Black Swans of Cybersecurity Ethics," *IEEE Access*, vol. 11, pp. 58796–58807, 2023, doi: 10.1109/ACCESS.2023.3283791.

[20] K. Kovalan *et al.*, "A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021, Accessed: Mar. 02, 2025. [Online]. Available: www.ijacsa.thesai.org

[21] L. Wang, C. A. Alexander, L. Wang, and C. A. Alexander, "Cyber security during the COVID-19 pandemic," *AIMS Electronics and Electrical Engineering 2021 2:146*, vol. 5, no. 2, pp. 146–157, Apr. 2021, doi: 10.3934/ELECTRENG.2021008.

[22] D. M. A. A. Afraji, J. Lloret, and L. Peñalver, "Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments," *Cyber Security and Applications*, vol. 3, p. 100085, Dec. 2025, doi: 10.1016/J.CSA.2025.100085.

[23] J. K. Nwankpa and P. M. Datta, "Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers," *Comput Secur*, vol. 130, p. 103266, Jul. 2023, doi: 10.1016/J.COSE.2023.103266.

[24] Z. Przymus, K. Małagocka, and K. Przybyszewski, "The human factor in cybersecurity: from risk profiles to resilience," *Procedia Comput Sci*, vol. 246, no. C, pp. 1437–1445, Jan. 2024, doi: 10.1016/J.PROCS.2024.09.587.

[25] S. Lindroos, A. Hakkala, and S. Virtanen, "The COVID-19 pandemic and remote working did not improve WLAN security," *Procedia Comput Sci*, vol. 201, no. C, pp. 158–165, Jan. 2022, doi: 10.1016/J.PROCS.2022.03.023.

[26] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review," *Expert Syst Appl*, vol. 210, p. 118401, Dec. 2022, doi: 10.1016/J.ESWA.2022.118401.

[27] S. J. Philip, T. (Jack) Luu, and T. Carte, "There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks," *Comput Human Behav*, vol. 139, p. 107551, Feb. 2023, doi: 10.1016/J.CHB.2022.107551.

[28] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/J.IOT.2022.100564.

[29] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things*, vol. 22, p. 100792, Jul. 2023, doi: 10.1016/J.IOT.2023.100792.

[30] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *Int J Child Comput Interact*, vol. 30, p. 100343, Dec. 2021, doi: 10.1016/J.IJCCI.2021.100343.

[31] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," *Comput Secur*, vol. 117, p. 102677, Jun. 2022, doi: 10.1016/J.COSE.2022.102677.

[32] S. Furnell and J. N. Shah, "Home working and cyber security – an outbreak of unpreparedness?," *Computer Fraud & Security*, vol. 2020, no. 8, pp. 6–12, Aug. 2020, doi: 10.1016/S1361-3723(20)30084-1.

[33] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281–292, 2023, doi: 10.1109/OJVT.2023.3234069.

[34] A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. Osman Ibrahim, and W. Nagmeldin, "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," *Egyptian Informatics Journal*, vol. 25, p. 100443, Mar. 2024, doi: 10.1016/J.EIJ.2024.100443.

[35] M. Boussard *et al.*, "Future Spaces: Reinventing the Home Network for Better Security and Automation in the IoT Era," *Sensors 2018,*

Vol. 18, Page 2986, vol. 18, no. 9, p. 2986, Sep. 2018, doi: 10.3390/S18092986.

[36] I. Palamà, A. Amici, G. Bellicini, F. Gringoli, F. Pedretti, and G. Bianchi, "Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments," *Comput Commun*, vol. 212, pp. 129–140, Dec. 2023, doi: 10.1016/J.COMCOM.2023.09.031.

[37] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," *Comput Secur*, vol. 109, p. 102382, Oct. 2021, doi: 10.1016/J.COSE.2021.102382.

[38] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1–2, pp. 81–98, Sep. 2018, doi: 10.1016/J.IOT.2018.08.009.

[39] S. M. Sajjad, M. Yousaf, H. Afzal, and M. R. Mufti, "EMUD: Enhanced manufacturer usage description for iot botnets prevention on home wifi routers," *IEEE Access*, vol. 8, pp. 164200–164213, 2020, doi: 10.1109/ACCESS.2020.3022272.

[40] K. Kaushik, A. Bhardwaj, and S. Dahiya, "Framework to analyze and exploit the smart home IoT firmware," *Measurement: Sensors*, vol. 37, p. 101406, Feb. 2025, doi: 10.1016/J.MEASEN.2024.101406.

[41] M. Bispham, S. Creese, W. H. Dutton, P. Esteve-Gonzalez, and M. Goldsmith, "Cybersecurity in Working from Home: An Exploratory Study," *SSRN Electronic Journal*, Aug. 2021, doi: 10.2139/SSRN.3897380.

[42] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," *Comput Secur*, vol. 148, p. 104110, Jan. 2025, doi: 10.1016/J.COSE.2024.104110.

[43] R. A. Alsharida, B. A. S. Al-rimy, M. Al-Emran, and A. Zainal, "A systematic review of multi perspectives on human cybersecurity behavior," *Technol Soc*, vol. 73, p. 102258, May 2023, doi: 10.1016/J.TECHSOC.2023.102258.

[44] A. Allen, A. Mylonas, S. Vidalis, and D. Gritzalis, "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks," *Comput Secur*, vol. 139, p. 103687, Apr. 2024, doi: 10.1016/J.COSE.2023.103687.

[45] P. Jokela, "A Quantitative Analysis of Vulnerabilities and Exploits in Home IoT Devices," *Jyväskylä: University of Jyväskylä*, 2023.

[46] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Your WAP Is at Risk: A Vulnerability Analysis on Wireless Access Point Web-Based Management Interfaces," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/1833062.

[47] D. Yu, L. Zhang, Y. Chen, Y. Ma, and J. Chen, "Large-Scale IoT Devices Firmware Identification Based on Weak Password," *IEEE Access*, vol. 8, pp. 7981–7992, 2020, doi: 10.1109/ACCESS.2020.2964646.

[48] I. Kumar, "View of Emerging Threats in Cybersecurity: A Review Article," *Bluemark Publishers*, 2023, Accessed: Mar. 02, 2025. [Online]. Available: http://bluemarkpublishers.com/index.php/IJANS/article/view/2/2

[49] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Jan. 2019, Accessed: Mar. 02, 2025. [Online]. Available: https://arxiv.org/abs/1901.02672v1

[50] T. I. Tanni, T. Taharat, M. Shakil Parvez, S. T. A. Rumee, and M. I. Zaber, "Is My Password Strong Enough?: A Study on User Perception in The Developing World," 2022, doi: 10.4108/eai.11-2-2022.173452.