ISBN: 978-628-96613-0-9. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LEIRD2024.1.1.307

Cybersecurity Strategies for Smart Homes: A Systematic Review of Threats and Mitigation Approaches in IoT Environments

Victor Gabriel, Vera-Mundaca, Bachelor[1], Jury Yesenia, Aquino-Trujillo, Dr. in Education[2],
[1,2]Universidad Tecnológica del Perú, Chiclayo, Perú, U19311676@utp.edu.pe, C22835@utp.edu.pe

Abstract*– The usage of IoT devices has grown exponentially in smart homes, thanks to the automation benefits they provide. However, this expansion has also increased security vulnerabilities, making these devices attractive targets for cybercriminals. This systematic review analyzes the main cybersecurity threats in domestic IoT environments and the emerging mitigation strategies. Forty-nine studies extracted from the Scopus database were examined, covering articles published between 2020 and April 2024. The results revealed that flooding attacks and authentication and session attacks are the most prevalent. To counter these threats, machine learning and blockchain techniques are highlighted, providing protection against authentication and manipulation. Machine learning methods implemented in intrusion detection systems achieve accuracies ranging from 97.7% to 99.68%. This analysis not only offers a detailed view of current vulnerabilities but also suggests that future research should develop techniques combining machine learning witch blockchain, allowing for greater resilience against diverse attacks.

***Keywords*—Cybersecurity, Smart Home, Cyber threats, IoT.**

Estrategias de Ciberseguridad para Hogares Inteligentes: Una Revisión Sistemática de Amenazas y Enfoques de Mitigación en Entornos IoT

Victor Gabriel, Vera-Mundaca, Bachiller[1], Jury Yesenia, Aquino-Trujillo, Dra. en educación[2],
[1,2]Universidad Tecnológica del Perú, Chiclayo, Perú, U19311676@utp.edu.pe, C22835@utp.edu.pe

Resumen*– El uso de dispositivos IoT ha crecido exponencialmente en los hogares inteligentes, gracias a los beneficios de automatización que estos proporcionan. Sin embargo, esta expansión también ha incrementado las vulnerabilidades de seguridad, convirtiendo a estos dispositivos en objetivos atractivos para ciberdelincuentes. Esta revisión sistemática analiza las principales amenazas a la ciberseguridad en entornos IoT domésticos y las estrategias de mitigación emergentes. Se examinaron 49 estudios extraídos de la base de datos Scopus, abarcando artículos publicados entre 2020 y abril de 2024. Los resultados revelaron que los ataques de inundación y los de autenticación y sesión son los más prevalentes. Para contrarrestar estas amenazas, se destacan técnicas de machine learning y blockchain, que proporcionan protección contra la autenticación y la manipulación. Los métodos de machine learning implementados en sistemas de detección de intrusos alcanzan precisiones entre 97.7% y 99.68%. Este análisis no solo ofrece una visión detallada de las vulnerabilidades actuales, sino que también sugiere que futuras investigaciones deberían desarrollar técnicas que combinen machine learning con blockchain, permitiendo una mayor resiliencia ante diversos ataques.

Palabras Clave—Ciberseguridad, hogar inteligente, Amenazas cibernéticas, IoT.

I. Introducción

Hoy en día, el uso de los dispositivos IoT ha crecido exponencialmente gracias a la automatización de funciones como la iluminación, seguridad, climatización, entre otros beneficios que nos brinda y como indica PwC en su informe [1], se espera que la cantidad de estos dispositivos instalados en los hogares aumente significativamente, pasando de 16,400 millones en 2022 a 25,100 millones en 2027. Esta expansión en el uso de los dispositivos IoT en los hogares se ve respaldada por el constante crecimiento de los hogares inteligentes puesto que según Statista [2] estos superaron los 300 millones en el 2023 y se proyecta que podrían duplicarse para 2028.

Sin embargo, este rápido crecimiento en la adquisición de estos dispositivos en entornos no seguros como los hogares, ha sido aprovechada por los ciberdelincuentes como lo demuestra el reporte de Bitdefender [3], en el cual se identificó que el dispositivo más vulnerable fue el Smart TV, contando con más del 52% de las vulnerabilidades de IoT identificadas por esta compañía de seguridad. Adicional a ello, en un reporte de SonicWall [4], se identificó que, en los primeros seis meses del 2023, se registraron 77.9 millones de ataques de malware dirigidos únicamente a dispositivos IoT, aumentando un 37% con respecto al año anterior.

En la literatura, se pueden apreciar investigaciones relacionadas a la seguridad de las casas inteligentes en la cual analizaron normas como el estándar 303 645 de ETSI, sin embargo, esta va orientada más hacia los fabricantes de estos dispositivos [5]. Otras han abordado ataques específicos como los ataques de firmware, XSS y fuerza bruta para descifrar contraseñas en estos dispositivos [6] y han propuesto soluciones al respecto. Además, mientras algunos estudios proponen soluciones como la gestión basada en políticas y un enfoque más orientado al usuario inexperto en conceptos técnicos [7], existen otros que clasifican los tipos de ataques hacia los dispositivos IoT en el hogar, destacando las amenazas, así como soluciones generales para proteger dichos sistemas [8].

En el marco de esta realidad, se justifica la necesidad de desarrollar una nueva revisión sistemática de la literatura (RSL) sobre las tendencias de amenazas y mitigación en los dispositivos IoT dentro de hogares inteligentes. Esta revisión es esencial para actualizar el conocimiento actual y sintetizar las investigaciones existentes en el área de estudio. El principal objetivo de esta revisión es identificar las estrategias de ciberseguridad actuales utilizadas para mejorar la protección frente a las amenazas cibernéticas en hogares inteligentes. Además, el estudio se centra en identificar las brechas existentes en la literatura y proponer futuras líneas de investigación que puedan abordar las deficiencias actuales en la mitigación de riesgos en dispositivos IoT.

Con respecto al resto de este estudio, la sección II aborda la metodología empleada, detallando las preguntas de investigación, los criterios de elegibilidad establecidos y la declaración PRISMA utilizada para asegurar la transparencia y el rigor del proceso de revisión. La sección III presenta los resultados, describiendo las amenazas cibernéticas más comunes, las principales estrategias de ciberseguridad identificadas y la efectividad de estas. Finalmente, la sección IV ofrece las conclusiones y sugerencias para futuras investigaciones, destacando las áreas que requieren más atención para mejorar la ciberseguridad en hogares inteligentes.

II. Metodología

La presente investigación se realizó mediante la elaboración de una RSL, la cual consiste en una secuencia de pasos estructurados y metódicos para realizar una revisión basada en evidencia, con el objetivo de abordar las preguntas

de investigación de manera objetiva [9]. Para guiar esta RSL, se propuso la siguiente pregunta de estudio: ¿Qué estrategias de ciberseguridad se están utilizando para mejorar la protección frente a las amenazas cibernéticas en hogares inteligentes? Esta pregunta se desagregó utilizando los componentes de la estrategia PICOC (Problema, Intervención, Comparación, Resultado, Contexto), la cual permite agilizar la revisión al afinar las preguntas de investigación para obtener un mejor rendimiento en la captura de publicaciones para la RSL [10], precisando las preguntas específicas y palabras clave necesarias para cada componente de PICOC, como se describe en la Tabla I.

TABLA I
APLICACIÓN DE PREGUNTAS PICOC

COMPONENTE	PREGUNTA	PALABRA CLAVE
Problema	¿Qué tipos de amenazas cibernéticas son más comunes en los entornos de hogares inteligentes?	Cyber threats, threats, vulnerability, attack, "computer crime", unauthorized access.
Intervención	¿Qué estrategias de ciberseguridad se están desarrollando para mejorar la seguridad de los hogares inteligentes?	Cybersecurity strategies, cybersecurity, mitigation, resilience, assessment, measures
Comparación	-	-
Resultados	¿Qué mejoras aportan estas estrategias para la protección de los hogares inteligentes?	Improve protection, enhance, improvement, secure, approach, solution
Contexto	El contexto, hogares inteligentes, se aborda en cada una de las anteriores preguntas.	Smart home, home automation, home network

Para ayudar a dar respuesta a las preguntas de investigación derivadas de PICOC, se hizo uso de la base de datos Scopus, una de las principales bases de datos bibliográficas revisadas por pares, que comprende más de 300 disciplinas y, hasta el año 2023, contaba con alrededor de 7 mil editoriales y más de 94 millones de registros [11]. En esta base de datos, se emplearon las palabras claves y sinónimos identificados mediante la estrategia PICOC, utilizando una cadena de búsqueda avanzada con operadores booleanos AND y OR. La búsqueda se limitó a títulos, resúmenes y palabras claves. La siguiente cadena canónica fue utilizada para la búsqueda:

TITLE-ABS-KEY ("cyber threats" OR threat OR vulnerability OR attack OR "computer crime" OR "unauthorized access") AND TITLE-ABS-KEY ("cybersecurity strategies" OR cybersecurity OR mitigation OR resilience OR assessment OR measures) AND TITLE-ABS-KEY (Improve OR protection OR enhance OR solution OR improvement OR secure OR approach) AND TITLE-ABS-KEY ("smart home" OR "home automation" OR "home network") AND PUBYEAR > 2019 AND PUBYEAR < 2025 AND (LIMIT-TO (OA,"all")) AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"ENGI"))

La cadena de recopilación fue diseñada para abarcar una amplia gama de estudios relevantes al tema de investigación. Esta estrategia permitió obtener un conjunto significativo de publicaciones pertinentes.

A continuación, se detallan los criterios de elegibilidad que se tomaron en cuenta para la presente investigación. Para asegurar la relevancia y calidad de los estudios seleccionados en esta RSL, mediante la Tabla II, se establecieron los siguientes criterios de inclusión.

TABLA II
CRITERIOS DE INCLUSIÓN

Nº	Criterio
CI1	Publicaciones que aborden temas relacionados con amenazas cibernéticas.
CI2	Publicaciones que discutan estrategias de ciberseguridad.
CI3	Publicaciones que versen sobre mejoras en la protección cibernética.
CI4	Publicaciones dentro del contexto de hogares inteligentes.

Asimismo, se definieron los siguientes criterios de exclusión, presentados en la Tabla 3.

TABLA III
CRITERIOS DE EXCLUSIÓN

Nº	Criterio
CE1	Publicaciones que no son de acceso abierto.
CE2	Publicaciones distintas de artículos originales.
CE3	Artículos científicos distintos al idioma inglés.
CE4	Artículos científicos anteriores al año 2020.
CE5	Artículos originales con área de estudio diferente a ciencias de la computación o ingeniería.
CE6	Artículos de revisión que aparecen como artículos originales.

El diagrama de flujo PRISMA, mostrado en la Fig. 1, describe el procedimiento para la selección de artículos. Después de aplicar la cadena de recopilación en la base de datos Scopus, dio como resultado 491 publicaciones donde, posteriormente, se utilizó la declaración PRISMA la cual es de gran ayuda en el desarrollo de una RSL para identificar y sintetizar los estudios encontrados a través de su diagrama de flujo [12]. Como primer filtro, se utilizaron los criterios de exclusión, dando como resultado la eliminación de 412 publicaciones, desglosadas de la siguiente manera: 334 publicaciones no eran de acceso abierto, 51 no eran artículos originales, una publicación estaba escrita en un idioma distinto al inglés, 20 no estaban comprendidos entre los años 2020 y 2024, y 6 no estaban relacionadas con las áreas de ciencias de computación o ingeniería. Este filtro inicial dejó 79 artículos potenciales para la revisión. Posteriormente, fue realizada una lectura exhaustiva de los artículos restantes, lo que resultó en la exclusión de 24 artículos que no se adecuaban a las reglas de inclusión y de 6 artículos de revisión que, a pesar de haber usado el filtro de solo ‘artículos’, se presentaban como artículos

originales. Finalmente, se identificaron 49 artículos que fueron incorporados al estudio de la RSL al cumplir con los criterios de inclusión establecidos. Cabe resaltar que los datos recopilados en esta revisión abarcan hasta abril 2024.

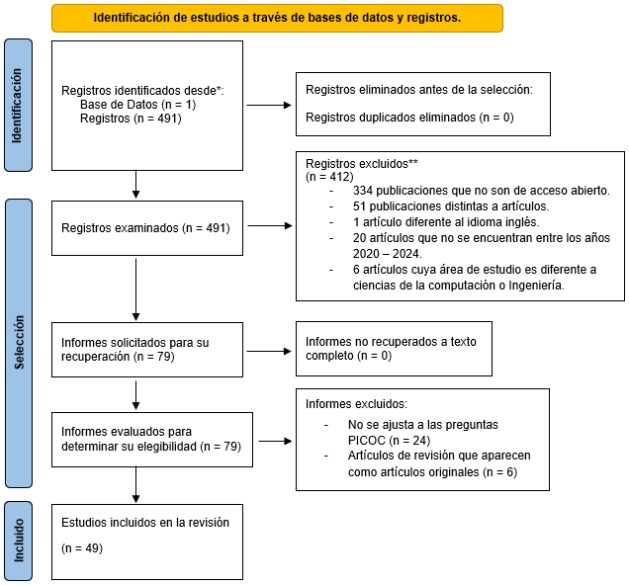

Fig. 1 Diagrama de Flujo PRISMA

III. Resultados y Discusión

Los 49 artículos previamente seleccionados fueron categorizados según su año de publicación y país con el objetivo de identificar patrones y tendencias en la literatura. La Fig. 2 muestra que, desde el 2020, los estudios sobre amenazas y estrategias de mitigación en hogares inteligentes fueron aumentando, alcanzando el pico más alto en el año 2023 con 17 publicaciones. Adicional a ello, se puede resaltar que durante solo el primer cuatrimestre del 2024 (enero – abril) se publicaron un total de 9 artículos, lo que evidencia un aumento significativo en la producción científica relacionada con la ciberseguridad en hogares inteligentes. Estos datos sugieren un creciente reconocimiento de la importancia de desarrollar y mejorar las estrategias de mitigación de ataques dirigidos a dispositivos IoT en los hogares inteligentes.

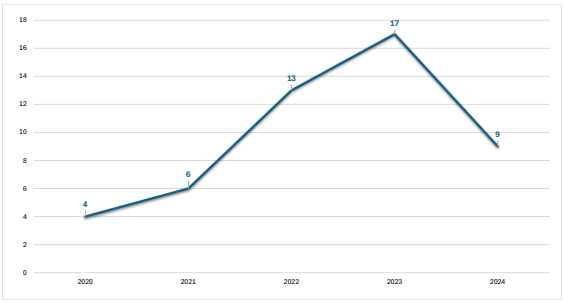

Fig. 2 Artículos científicos incluidos en la RSL según su año de publicación

Con respecto a los artículos científicos organizados por países, la Fig. 3 muestra los 5 países con mayor producción científica en el tema. Arabia Saudita destaca como el país con mayor número de publicaciones, representando el 28.6% del total de artículos. Le sigue Pakistán con el 22.4% y Estados Unidos con el 14.3%, evidenciando una significativa contribución a la investigación en este ámbito. India y China muestran una participación en la contribución científica, de un 12.2% y un 10.2% respectivamente. Estos datos estadísticos reflejan un interés global en la investigación sobre las amenazas presentes en los hogares inteligentes, así como en las estrategias de ciberseguridad para mitigarlas.

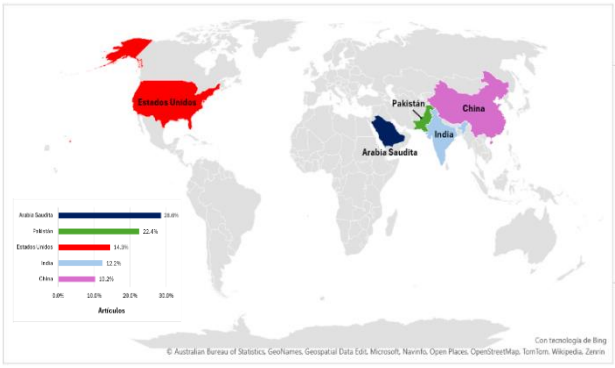

Fig. 3 Top 5 países con el mayor número de artículos incluidos en la RSL

Mediante el análisis bibliométrico realizado a los artículos seleccionados, se observó el nivel de co-ocurrencia de las palabras claves, tal como se muestra en la Fig. 4. Los nodos más grandes representan las palabras más recurrentes en la literatura, destacando "internet de las cosas", "seguridad de red", "automatización" y "ciberseguridad" como las más prominentes. Asimismo, el gráfico muestra la tendencia a lo largo del tiempo, representada mediante una escala de colores, en la cual los tonos más amarillos indican un aumento reciente en su mención, como en los casos de "block-chain", "ataque de denegación de servicios" y "machine-learning". Estos datos reflejan una evolución en el enfoque y las prioridades en la investigación, evidenciando una mayor atención a los nuevos tipos de ataques que surgen en el contexto de la seguridad de los hogares inteligentes, así como también a las tecnologías emergentes para mitigarlos.

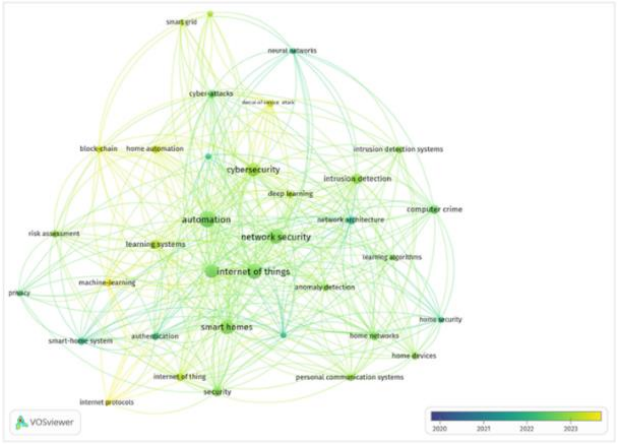

Fig. 4 Co-ocurrencia de palabras claves resultante del análisis bibliométrico

A. *Amenazas cibernéticas comunes en hogares inteligentes*

Abordando el primer componente de PICOC, mediante el análisis sistemático realizado, se logró identificar un total de 53 tipos de ataques específicos dirigidos hacia los hogares inteligentes. Entre estos, el ataque más mencionado en la literatura fue el de Denegación de Servicio Distribuido (DDoS), mencionado en 18 artículos. Este tipo de ataque se caracteriza por la utilización de redes de bots (botnets) compuestas por dispositivos IoT infectados, permitiendo su uso remoto para lanzar ataques hacia otras redes. Se destaca además su capacidad de paralizar los servicios mediante el envío masivo de solicitudes maliciosas, provocando la saturación de los recursos de red [5], [6], [8], [13]–[27].

Otros ataques significativos incluyen el "Man-in-the-Middle" y diversas formas de sniffing, que permiten a los atacantes interceptar y manipular la comunicación entre dos dispositivos sin que los usuarios lo detecten, poniendo en riesgo la confidencialidad de los datos como las contraseñas, información de los sensores, datos personales u otro tipo de información sensible presentes en los dispositivos IoT [18], [23], [25], [26], [28]–[35]. Estos demuestran la variedad y complejidad de las amenazas cibernéticas en estos entornos.

Los 53 ataques específicos fueron clasificados en 13 categorías principales de acuerdo al tipo de ataque al que pertenecen, lo que permitió proporcionar una estructura clara y detallada de las distintas formas de vulnerabilidad presentes en los hogares inteligentes. Las categorías identificadas abarcan desde ataques de inundación e intercepción, hasta ataques de exploración de red e ingeniería social. Esta categorización permitió sistematizar la gran cantidad de ataques en solo 13, permitiendo realizar un subsecuente análisis de tendencias e identificación de las estrategias de mitigación para cada una de estas.

La Tabla 4 presenta cada una de estas categorías y sus respectivos ataques específicos, junto con las referencias a los autores que hacen mención de dicho ataque en sus artículos originales.

TABLA IV
CLASIFICACIÓN DE LAS AMENAZAS CIBERNÉTICAS SEGÚN SU TIPO DE ATAQUE

Categoría de Ataque	Ataque específico	Referencias
A. de Inundación	DDoS	[5], [6], [8], [13]–[27]
	DoS	[28]–[32], [36]–[40]
	Inundación de protocolos (MAC, ICMP, SSDP, DNS, UDP, MQTT, etc.)	[24], [26], [29], [31], [40], [41]
	Inundación de paquete de conexión (SYN, ACK)	[16], [19], [25], [27]
A. de Intercepción	Man-in-the-Middle	[18], [23], [25], [26], [28]–[35]
	Eavesdropping	[14], [18], [32], [35], [38], [39], [42]
	Sniffing	[13], [25], [28], [39]
	Sinkhole attack	[26], [32]
A. de Privacidad y Robo de Información	Filtración de datos	[5], [6], [17], [20], [32], [36], [39], [43]
	Exfiltración de datos	[15], [30], [37], [40], [44]
	Violaciones de privacidad	[13], [14], [31], [45], [46]
	Robo de datos	[15], [17], [41]
	Keylogging	[15], [44]
A. de Suplantación	Suplantación ARP	[23], [29], [31], [46]
	Suplantación (DNS, DHCP, IP, GPS)	[16], [19], [32], [41]
	Otro tipo de suplantación (no especifica)	[30], [33], [35], [37], [40], [47]–[49]
A. de Autenticación y Sesión	Ataque de replay	[18], [25], [29], [30], [33]–[35], [48]–[50]
	Acceso no autorizado	[6], [14], [17], [20], [22], [40], [43], [45], [47], [51]
	control no autorizado	[29], [37], [43], [47], [52]
A. de Explotación de Vulnerabilidades	ataque de día cero	[13], [14], [20], [53]
	Ataque de canal lateral	[18], [28], [42], [46]
	Buffer overflow	[18], [25], [46]
	Otro tipo de explotación de vulnerabilidades (no especifica)	[8], [14], [38]
	Escalamiento de privilegios	[22], [37], [40]
A. de Inyección	Inyección de código	[28], [49], [54]
	Inyección de datos falsos (FDI)	[29], [38]
	Cross-site scripting (XSS)	[6], [18]
	Inyección SQL	[55]
A. de Malware	Ataque de malware	[18], [39], [52], [54]
	Paquetes atacados por malware	[53]
	Ataques de ransomware	[20]
	Ataque de gusanos	[21]
	Ataques adversarios	[50]
	Brickerbot	[27]
	Firmware malicioso	[42]
A. de Manipulación de Datos	Data tampering	[14], [17], [25], [30], [32], [37], [40], [48], [49]
	Envenenamiento de datos	[16], [32], [46]
	Data forgery	[14], [33]
	Inserción de objetos maliciosos	[42]
	Selective forwarding attacks	[26]
A. Criptográficos	Ataques criptográficos	[35]
	Ataque del 51% Blockchain	[14]
	Ataque de tablas pre-calculadas	[45]
	Ataques de firma	[22]
A. de Contraseñas	Ataque de fuerza bruta	[6], [23], [25], [27], [33], [41], [45], [56]
	Crackeo de contraseñas	[33], [55]
	Diccionario offline	[34]
A. de Exploración de Red	Ataque de reconocimiento	[15], [23], [31], [57]
	Escaneo de servicios	[44], [56]
	OS fingerprint	[15], [44]
	Captura de señal de radio	[46]
	Wormhole attacks	[26]
A. de Ingeniería Social	Phishing	[7], [34], [37], [38]

El gráfico presentado en la Fig. 5 resume la distribución de categorías de ataques cibernéticos en hogares inteligentes, identificados en la revisión. Se identificó que las tres categorías de ataque más mencionadas en la literatura son: ataque de inundación con 29 artículos, ataque de autenticación y sesión con 21 y ataques de privacidad y robo de información con 19. Asimismo, es importante destacar que, si bien las categorías de ataques mencionadas anteriormente son las más comunes, también se observó una menor cantidad de artículos relacionados con otras categorías de ataques, como los ataques criptográficos o los ataques de ingeniería social, ambos con únicamente 4 artículos. Esto sugiere que estos tipos de ataques no son tan frecuentes en el contexto de los hogares inteligentes o que la literatura existente sobre estos temas es limitada.

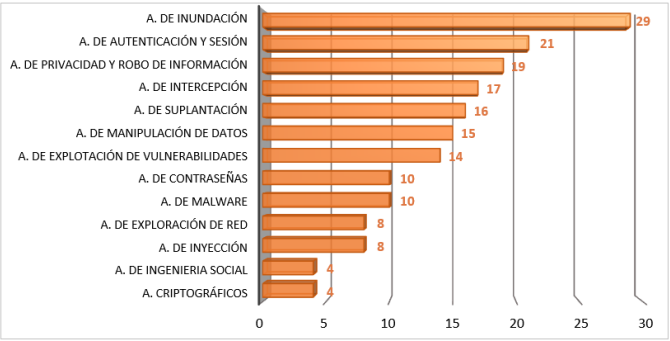

Fig. 5 Cantidad de artículos según su categoría de ataques cibernéticos

Estas categorías de ataque fueron clasificadas según el componente principal que afectan de la triada de seguridad de la información CID (Confidencialidad, Integridad y Disponibilidad) en el contexto de hogares inteligentes. Como lo muestra la Tabla 5, las 13 categorías de ataques identificadas previamente se han segmentado según el componente de la triada al que impactan. En cuanto a la confidencialidad, se incluyen siete categorías, destacando entre ellas los ataques de autenticación y sesión, así como los ataques de privacidad. Por otro lado, la integridad es afectada por cuatro categorías, donde resaltan los ataques de suplantación y explotación de vulnerabilidades. Finalmente, la disponibilidad es impactada por únicamente dos categorías: los ataques de inundación y malware.

TABLA V
CLASIFICACIÓN DE AMENAZAS QUE AFECTAN LA TRIADA DE SEGURIDAD DE LA INFORMACIÓN

CID	Categoría de Ataque	Referencia	Descripción
C	A. de Intercepción	[13], [14], [18], [23], [25], [26], [28]–[35], [38], [39], [42]	Intercepción de las comunicaciones entre componentes IoT, permitiendo la captura de información en tránsito.
	A. de Privacidad y Robo de Información	[5], [6], [13]–[15], [17], [20], [30]–[32], [36], [37], [39]–[41], [43]–[46]	Filtración de datos personales, como grabaciones de cámaras de seguridad, exponiendo la privacidad del usuario sin su consentimiento.
I	A. de Autenticación y Sesión	[6], [14], [17], [18], [20], [22], [25], [29], [30], [32]–[35], [37], [40], [40], [43], [45]–[52]	Acceso y control remoto de los dispositivos del hogar, permitiendo la manipulación, monitoreo, así como la realización de actividades maliciosas.
	A. criptográficos	[14], [22], [35], [45]	Ruptura del cifrado en las comunicaciones IoT, revelando información sensible como contraseñas de Wi-Fi o datos de sensores.
	A. de Exploración de Red	[15], [23], [26], [31], [44], [46], [56], [57]	Escaneo de dispositivos y servicios IoT, facilitando el acceso a información sensible, como patrones de uso y mapeo de la red interna.
	A. de Contraseñas	[6], [23], [25], [27], [33], [34], [41], [45], [55], [56]	Desciframiento de contraseñas de los dispositivos, permitiendo el acceso a datos privados, como configuraciones de sistemas de seguridad.
	A. de Ingeniería Social	[7], [34], [37], [38]	Obtención de información confidencial, tales como nombres de usuario, contraseñas o números de tarjetas, mediante técnicas de manipulación.
	A. de suplantación	[16], [19], [23], [24], [29]-[33], [35], [37], [40], [41], [47]-[49]	Fingen ser dispositivos legítimos, modificando datos como comandos de sistemas de control de acceso en el hogar.
	A. de Explotación de Vulnerabilidad	[8], [13], [14], [18], [20], [22], [25], [28], [37], [38], [40], [42], [46], [53]	Aprovechamiento de fallos de software en dispositivos IoT, permitiendo el escalamiento de privilegios.
	A. de Inyección	[6], [8], [28], [29], [38], [49], [54], [55]	Inserción de código malicioso en dispositivos IoT, manipulando datos como los presentados en webservices de los dispositivos.
	Manipulación y Falsificación de Datos	[14], [16], [17], [25], [26], [30], [32], [33], [37], [40], [42], [46], [48], [49]	Cambio o creación de datos falsos en dispositivos IoT, corrompiendo la veracidad de información como lecturas de sensores.
D	A. de Inundación	[5], [6], [8], [13]-[32], [36]-[41]	Sobrecarga de la red IoT con tráfico excesivo, bloqueando el acceso legítimo a servicios críticos como alarmas de seguridad.
	A. de Malware	[8], [20], [21], [27], [42], [46], [50], [52]-[54]	Introducción de software malicioso en dispositivos IoT, interrumpiendo o deshabilitando servicios esenciales como sistemas HVAC.

Nota: A pesar de la menor cantidad de categorías que afectan la disponibilidad, 35 artículos (71% del total) mencionan ataques que afectan a este componente, 33 (67%) la integridad y 41 (84%) la confidencialidad.

B. Estrategias de ciberseguridad para hogares inteligentes

Respecto al segundo componente de PICOC, se identificaron 45 estrategias de mitigación específicas que fueron planteadas o implementadas a lo largo de los artículos. Estas se clasificaron en 13 categorías según el tipo de estrategia

de ciberseguridad al que pertenecen, abarcando diversos enfoques, desde estándares, hasta técnicas más avanzadas como machine learning (ML), blockchain y criptografía, permitiendo obtener una estructura concisa y detallada de la información extraída de la literatura.

Ante esto, se identificó que las estrategias de ciberseguridad basadas en ML son las más sobresalientes, habiéndose identificado un total de 14 estrategias específicas que incorporan modelos de machine learning, mejorando la capacidad y precisión de sistemas de detección y prevención de intrusiones, así como también, modelos para la clasificación de estados de los dispositivos IoT [17], [21], [24], [25], [27], [28], [31], [32], [43], [44], [51]–[54], [56].

Además, se observó que la tecnología basada en blockchain fue la segunda categoría de mitigación más mencionada, con unas 6 distintas estrategias que buscan mitigar el impacto de ataques, entre estas, se mencionan sistemas de monitoreo, arquitecturas de puerta de enlace y protocolos de seguridad, entre otros métodos de blockchain [14], [19], [30], [38], [41], [43], [51].

Finalmente, como tercer punto a destacar, las técnicas criptográficas jugaron un papel esencial en la protección ante las amenazas cibernéticas, se observó el uso de marcos de autenticación biométrica, protocolos de criptografía de curva elíptica y la implementación de funciones hash unidireccionales, demostrando como la criptografía puede proteger la privacidad y asegurar las comunicaciones en redes IoT [35], [41], [45], [48], [49].

La Tabla 6 presenta en detalle, cada una de estas categorías y sus respectivas estrategias de mitigación, además de incluir una breve descripción de estas para brindar un mejor análisis.

TABLA VI
CATEGORIZACIÓN DE ESTRATEGIAS DE MITIGACIÓN CIBERNÉTICAS

Cat.	Estrategia de Mitigación	Referencia	Descripción
Estándares	Norma ETSI EN 303 645	[5], [13]	Orientada hacia los fabricantes de dispositivos IoT con una serie de requisitos para cumplir un nivel de resiliencia ante ataques.
	Estándar de Descripción de uso del fabricante (MUD)	[13]	Permite supervisar y liminar el comportamiento en la red al proporcionar los patrones de comunicación previstos de los dispositivos.
	Esquemas de certificación y etiquetado		Fomenta el desarrollo orientado a la seguridad en las organizaciones y aumenta la confianza de los consumidores en los dispositivos.
Blockchain	Métodos de blockchain	[43], [51]	Mecanismo descentralizado, seguro y confiable que asegure la autenticación e identificación de los dispositivos IoT
	Arquitectura de red de puerta de enlace basada en blockchain	[14]	Implementación de blockchain en la puerta de enlace para asegurar los hogares inteligentes contra ataques, asegurando la integridad de datos y proporcionando autenticación.
	Esquema de gestión de claves de autenticación basado en blockchain	[30]	Sistema de autenticación y gestión de claves que ayuda a crear un entorno seguro y a prueba de alteraciones para el intercambio en el flujo de datos.
	Framework para el intercambio de información sobre ciberamenazas (CTI) basada en blockchain	[19]	Framework para compartir información CTI permitiendo una red segura con medidas proactivas y reactivas ante ciberataques.
	Protocolo de seguridad basado en blockchain	[41]	Protocolo diseñado para la protección del protocolo DHCP, combina técnicas de encriptación como Diffie-Hellman y funciones hash unidireccionales, integrando además blockchain.
	Aplicación basada en blockchain	[38]	Uso de múltiples métodos de verificación y autenticación para asegurar que solo usuarios legítimos accedan a los dispositivos.
Autenticación y Gestión de Usuarios	Autenticación multifactor	[8], [36], [47]	Mecanismo de autenticación remota que utiliza métodos basados en hash y claves de sesión pre compartidas para reconocer la legitimidad de los usuarios.
	Mecanismo de autenticación remota	[33]	Protocolo basado en umbral de contraseña para la autenticación y acuerdo de claves en los entornos de hogares inteligentes.
	Protocolo de autenticación mutua basado en contraseña	[34]	Implementación de autenticación biométrica utilizando cifrado avanzado para asegurar dispositivos IoT y proteger la privacidad del usuario.
Técnicas Criptográficas	Framework de autenticación biométrica mediante métodos de encriptación	[45]	Protocolo que permite autenticar y realizar un acuerdo de claves entre los usuarios y los dispositivos en el hogar inteligente.
	Protocolo para autenticar y realizar el acuerdo de claves mediante criptografía de	[35]	Uso de función hash para asegurar la integridad de los datos durante su transmisión y almacenamiento.

	curva elíptica (ECC).		
	Verificación de hash	[41], [48], [49]	Sistemas de supervisión del tráfico de red en busca de actividades sospechosas o inusuales para detectar intrusiones.
Sistemas de Detección y Prevención de Intrusos	Sistema de detección de intrusos de red (NIDS)	[21], [22], [28]	Sistema que bloquea el tráfico malicioso en tiempo real, mediante el análisis de firmas, anomalías o patrones.
	Sistema de prevención de intrusiones (IPS)	[16], [18]	Sistemas que solo detectan y envían alertas ante actividades inusuales en la red y accesos no autorizados.
	Sistemas de detección de intrusos (IDS)	[18], [26], [27], [31], [56]	Sistema IoT que detecta y previene ataques de fuerza bruta, DoS y vulnerabilidades de scripting en redes de hogar inteligente
	Framework de detección y prevención de intrusiones (IDPS)	[6]	Sistema seguro con predicción de uso de energía mediante ML y gestión de perfiles de usuario mediante blockchain.
	IDS distribuido	[23]	Monitorea todo el tráfico de la red LAN permitiendo detectar anomalías y posibles ciberataques ante los sistemas de control y automatización en edificios (BACS).
Modelos de Machine Learning y Deep Learning	Sistemas de monitoreo basado en blockchain y técnicas de machine learning	[17]	Modelo para detectar malware en dispositivos IoT, combinando aprendizaje profundo y técnicas de ensamblado para mejorar la precisión y generalización.
	NIDS con inteligencia artificial basada en anomalías	[28]	IDS implementado en cada uno de los nodos IoT, permitiendo que cada dispositivo alimente la arquitectura ANN con el fin de detectar las amenazas que estos enfrentan.
	Framework de detección de malware con deep learning	[53]	IDS impulsado con ML en redes IoT con protocolo MQTT, permitiendo incrementar el rendimiento y la tasa de detección.
	IDS basado en host mediante redes neuronales artificiales	[27]	Modelo IDS con hiper parámetros optimizados para detectar ataques mediante clasificación binaria y clasificación por categorías y subcategorías.
	IDS con machine learning	[56]	Framework que permite modelar riesgos de privacidad compuesto por 3 modelos: de sistema, métricas de privacidad y amenazas.
	IDS basado en modelo de redes neuronales artificiales de varios niveles (MAMID)	[31]	Sistema con deep learning y CNN que clasifica los dispositivos en función de su estado encendido o apagado.
	Framework para modelar y analizar riesgos de privacidad.	[32]	Uso de ML para categorizar los dispositivos IoT en hogares inteligentes en función del comportamiento del tráfico de red, lo que permite identificar los dispositivos auténticos.
	Redes neuronales convolucionales (CNN)	[43], [51]	Detecta anomalías en las redes mediante algoritmos de aprendizaje profundo en un sistema en tiempo real, salvaguardando los dispositivos IoT conectados.
	Enfoque de ML para la clasificación de dispositivos IoT	[52]	Sistema seguro con predicción de uso de energía mediante ML y gestión de perfiles de usuario mediante blockchain.
	NIDS basado en algoritmos deep learning	[21]	Monitorea todo el tráfico de la red LAN permitiendo detectar anomalías y posibles ciberataques ante los sistemas de control y automatización en edificios (BACS).
	Framework de machine learning distribuido basado en el algoritmo H2O	[25]	Framework para mejorar la seguridad en el protocolo MQTT presente en redes IoT mediante la detección y mitigación en tiempo real ante comportamientos anómalos.
	Detector de ciberataques basado en firmas alimentado por una red neuronal de retardo temporal	[54]	Utilizo de red neuronal de retardo temporal para identificar ataques de alteración de carga eléctrica, lo que permite supervisar continuamente los perfiles de carga y aprender de las firmas de los ataques.
	Técnicas de detección de anomalías basadas en el aprendizaje automático	[44]	Modelo ML de detección de anomalías en hogares inteligentes, mediante el uso de clasificadores según el dataset de BoT IoT.
	Método de aprendizaje federado (FL)	[24]	Modelo que detecta anomalías en los dispositivos IoT, mejorando la precisión y reduciendo la tasa de falsos positivos.
Seguridad Basada en Arquitectura	Edge Computing	[5], [13], [17]	Permite almacenar los datos de forma descentralizada y local, posibilitando su análisis

			en el dispositivo del cliente.
	Arquitectura de software para la gestión de dispositivos IoT	[47]	Sistema que permite gestionar los dispositivos IoT de forma remota con la integración de autenticación múltiple para el inicio de sesión.
Evaluación y Gestión de Riesgos	Método de evaluación de riesgos	[46]	Método de evaluación de riesgos de privacidad que identifica y cuantifica escenarios de riesgo para mejorar la gestión de privacidad.
	Enfoque de modelado de amenazas STRIDE	[37], [40]	Enfoque que permite a los fabricantes identificar y mitigar ciberamenazas en los sistemas IoT que puedan causar phishing.
	Evaluación de riesgos DREAD	[40]	Evaluación de riesgos para calificar y priorizar amenazas en hogares inteligentes, considerando factores de daño, reproducibilidad, explotabilidad, usuarios afectados y descubribilidad.
Seguridad de conexión	Timestamp	[48], [49]	Asignación de marcas de tiempo a los datos enviados por los dispositivos IoT asegurando la secuencia e integridad temporal.
Técnicas de Señuelo	Defensa de objetivo móvil (MTD)	[57]	Implementación de técnicas de engaño proactivo y reactivas, incluyendo la utilización de señuelos que permiten desorientar a los atacantes.
Técnicas de Reducción de Ruido	Ruido gaussiano (Noise-adding)	[50]	Introducción de ruido leve en los audios de entrada de los sistemas de verificación de hablantes para reducir la tasa de éxito de ataques adversariales.
	Padding de paquetes	[39]	Técnica de añadir bytes falsos al final de cada paquete para uniformar su longitud, dificultando la identificación de patrones únicos en el tráfico.
Métodos de Evaluación y Optimización	Técnica de pruebas de penetración mediante el método de optimización por enjambre de partículas	[55]	Pruebas de penetración mediante agentes virtuales exploran vulnerabilidades potenciales en hogares inteligentes.
Gestión de Políticas	Gestión basada en políticas (PBM)	[7]	Los usuarios definen requisitos de seguridad en forma de políticas, las cuales son implementadas por procesos automáticos para configurar el sistema de manera transparente.

C. Mejoras aportadas por las estrategias de mitigación de amenazas

En la literatura se identificaron las mejoras aportadas por las estrategias de mitigación de amenazas en hogares inteligentes. Este análisis se centró en rescatar el impacto, efectividad o mejora como tal, que se obtengan de estas estrategias de ciberseguridad implementadas o propuestas.

Las mejoras aportadas por estas estrategias abarcan desde el aumento de la resiliencia ante ataques [16], [18], [19], [27], [30], [35], [41], [44], hasta la mejora en la eficiencia de la comunicación y la autenticación de dispositivos [14], [33], [38], [39], [43], [47], [51]. Estas mejoras son cruciales para fortalecer la seguridad de los hogares inteligentes, proteger la privacidad de los usuarios y asegurar la integridad de los datos.

Asimismo, las estrategias basadas en ML han mostrado una precisión notable, como el caso de Cvitić et al. [52], con su enfoque para la clasificación de dispositivos IoT, obteniendo una precisión de 99.79%. Otras contribuciones en el uso de esta tecnología, fueron aplicados para la detección de intrusos, tal lo presenta Dat-Thinh et al. [23] con su sistema de detección de intrusos (IDS) distribuido, consiguiendo una precisión del 99.68% y Sohail et al. [31] con 97.7% en su IDS combinado con redes neuronales de varios niveles, aportando así una reducción en el tiempo de procesamiento.

Por otro lado, las soluciones basadas en blockchain han demostrado ser efectivas contra la manipulación de datos, la mejora en la autenticación de los dispositivos y el aumento de confidencialidad durante el procesamiento de datos. Estas estrategias incluyen la implementación de arquitecturas de red de puerta de enlace, esquemas de gestión de claves y protocolos de seguridad, todos los cuales contribuyen a una infraestructura de ciberseguridad más robusta.

A continuación, la Tabla 7 detalla cada una de las estrategias de mitigación, la categoría de ataque que abordan y las mejoras específicas que aportan para la protección de los hogares inteligentes.

TABLA VII
ESTRATEGIAS DE MITIGACIÓN Y MEJORA APORTADA ANTE LAS CATEGORÍAS DE ATAQUE QUE ABORDAN

Estrategia de Mitigación	**Categoría de Ataque que aborda**	**Referencia**	**Mejora Aportada**
Norma ETSI EN 303 645	A. de Privacidad y Robo de Información	[5], [13]	Buenas prácticas para la fabricación y desarrollo de nuevos dispositivos IoT.
Estándar de Descripción de uso del fabricante (MUD)	Todas las categorías (según su implementación)	[13]	Gestión eficiente para la implementación de políticas basadas en comportamiento.
Esquemas de certificación y etiquetado	A. de Privacidad y Robo de Información A. de Ingeniería Social		Aumento en la transparencia hacia el consumidor de dispositivos IoT.
Métodos de blockchain	A. de Autenticación y Sesión A. Criptográficos A. de Manipulación	[43], [51]	Autenticación para el uso de los dispositivos Protección contra manipulación de datos

	y Falsificación de Datos		
Arquitectura de red de puerta de enlace basada en blockchain	A. de Inundación A. de Suplantación A. de Autenticación y Sesión	[14]	Mejora problemas de autenticación y confidencialidad. Evita el tráfico DDoS durante el procesamiento de datos.
Esquema de gestión de claves de autenticación basado en blockchain	A. Manipulación de Datos A. de suplantación A. de Privacidad y Robo de Información A. de Intercepción	[30]	Mayor resiliencia ante ataques de manipulación. Mejor eficiencia en la comunicación.
Framework para el intercambio de información sobre ciberamenazas (CTI) basada en blockchain	A. de Inundación A. Manipulación de Datos A. de suplantación	[19]	Resiliencia ante ataques. Mayor protección en el dispositivo final. Protección contra la manipulación de datos.
Protocolo de seguridad basado en blockchain	A. de suplantación A. de Autenticación y Sesión A. de Contraseñas	[41]	Mitigación ante amenazas comunes hacia DHCP. Aumento de resiliencia en un 21%
Aplicación basada en blockchain	A. de Intercepción A. Manipulación de Datos A. de Explotación de Vulnerabilidades	[38]	Descentralización de los dispositivos. Registro inmutable. Protección ante la manipulación de datos.
Autenticación multifactor	A. de Autenticación y Sesión A. de Contraseñas A. de Ingeniería Social	[8], [36], [47]	Protección contra el acceso no autorizado.
Mecanismo de autenticación remota	A. de Intercepción A. de Autenticación y Sesión A. de Contraseñas	[33]	Reducción de costos de computación en un 54.03% Reducción de costos de comunicación en un 25.28%
Protocolo de autenticación mutua basado en contraseña	A. de Autenticación y Sesión A. de Contraseñas A. de Ingeniería Social	[34]	Proporciona seguridad de extremo a extremo.
Framework de autenticación biométrica mediante métodos de encriptación	A. de Autenticación y Sesión A. criptográficos A. de Contraseñas A. de Intercepción	[45]	Protección contra el acceso no autorizado. Mejora la seguridad de los datos biométricos durante su transmisión y almacenamiento.
Protocolo para autenticar y realizar el acuerdo de claves mediante criptografía de curva elíptica (ECC).	A. criptográficos A. de Intercepción A. de Autenticación y Sesión A. de suplantación	[35]	Cifrado robusto mediante ECC. Resiliencia ante ataques de intercepción y monitoreo.
Verificación de hash	A. Manipulación de Datos A. de Inyección	[41], [48], [49]	Aseguramiento de la autenticidad de los datos.
Sistema de detección de intrusos de red (NIDS)	A. de Exploración de Red A. de Inundación A. de Intercepción A. de Explotación de Vulnerabilidades	[21], [22], [28]	Detección temprana ante ataques. Reducción de intrusiones.
Sistema de prevención de intrusiones (IPS)	A. de Intercepción A. de Inundación A. de Explotación de Vulnerabilidades	[16], [18]	Resiliencia ante ataques de intercepción e inundación.
Sistemas de detección de intrusos (IDS)	A. de Inundación A. de Exploración de Red A. de Malware	[18], [26], [27], [31], [56]	Identificación temprana de malware. Monitoreo del tráfico en tiempo real.
Framework de detección y prevención de intrusiones (IDPS)	A. de Intercepción A. de Autenticación y Sesión A. de Contraseñas A. de Inundación A. de Inyección	[6]	Precisión del 95% en la identificación de paquetes de ataques.
IDS distribuido	A. de Inundación A. de Intercepción A. de Exploración de Red A. de Contraseñas	[23]	Precisión de detección del 99.68% Adaptabilidad a dispositivos IoT con especificaciones diferentes.
Sistemas de monitoreo basado en blockchain y técnicas de machine learning	A. de Privacidad y Robo de Información A. de Inundación A. de suplantación	[17]	Mayor transparencia de datos. Reducción de ataques de suplantación. Detección de amenazas ante el incremento de energía.
NIDS con inteligencia artificial basada en anomalías	A. de Inundación A. de Intercepción A. de Explotación de Vulnerabilidades A. de Inyección	[28]	Aborda necesidades de seguridad únicas de BACS.
Framework de detección de malware con deep learning	A. de Explotación de Vulnerabilidades A. de Malware	[53]	Identificación temprana de malware. Precisión de detección del 98.5%.
IDS basado en host mediante redes neuronales artificiales	A. de Autenticación y Sesión A. de Contraseñas	[27]	Resiliencia ante ataques. Robustes en la arquitectura IoT de los hogares.
IDS con machine learning	A. de Exploración de Red A. de Contraseñas	[56]	Tiempo para la clasificación de ataques reducido en un 67.7% Identificación temprana de malware.
IDS basado en modelo de redes neuronales artificiales de varios niveles (MAMID)	A. de Intercepción A. de Privacidad y Robo de Información	[31]	Precisión de detección del 99.7% para categorías y 97.7% para subcategorías. Reducción de tiempo de procesamiento.
Framework para modelar y analizar riesgos de privacidad.	A. de Privacidad y Robo de Información A. de Intercepción A. de suplantación A. Manipulación de Datos	[32]	Identificación temprana de ataques. Gestión de riesgos automatizada.
Redes neuronales convolucionales (CNN)	A. de Privacidad y Robo de Información	[43], [51]	Mayor gestión del estado de los dispositivos.

			Clasificación de dispositivos.
Enfoque de ML para la clasificación de dispositivos IoT	A. de Autenticación y Sesión A. de Malware	[52]	Precisión de clasificación del 99.79%
NIDS basado en algoritmos deep learning	A. de Intercepción A. de Explotación de Vulnerabilidades A. de Malware A. de Inundación	[21]	Precisión del 99.14% de detección de anomalías. Defensa robusta contra violaciones de seguridad.
Framework de machine learning distribuido basado en el algoritmo H2O	A. de Intercepción A. de Explotación de Vulnerabilidades A. Manipulación de Datos A. de Inundación	[25]	Monitorización y detección de ataques en tiempo real.
Detector de ciberataques basado en firmas alimentado por una red neuronal de retardo temporal	A. de Inyección A. de Malware	[54]	Detección temprana de ataques. Precisión de detección del 98%.
Técnicas de detección de anomalías basadas en el aprendizaje automático	A. de Inundación A. de Privacidad y Robo de Información A. de Exploración de Red	[44]	Resiliencia ante ataques de inundación o ataques botnet.
Método de aprendizaje federado (FL)	A. de suplantación A. de Inundación	[24]	Precisión del 99.64% en la detección de ataques.
Edge Computing	A. de Privacidad y Robo de Información A. de Inundación	[5], [13], [17]	Mejora la gestión de amenazas externas y la protección de la privacidad.
Arquitectura de software para la gestión de dispositivos IoT	A. de suplantación	[47]	Gestión de los dispositivos del hogar. Aumento en la confidencialidad mediante alertas de inicio de sesión.
Método de evaluación de riesgos	A. de Privacidad y Robo de Información A. de Explotación de Vulnerabilidades A. de Malware	[46]	Reducción de riesgos de privacidad.
Enfoque de modelado de amenazas STRIDE	A. de Explotación de Vulnerabilidades A. de Privacidad y Robo de Información A. Manipulación de Datos A. de suplantación	[37], [40]	Identificación y mitigación temprana de amenazas (durante la fase de diseño).
Evaluación de riesgos DREAD	A. de Explotación de Vulnerabilidades A. de Exploración de Red	[40]	Evaluación precisa de riesgos. Identificación de amenazas.
Timestamp	A. de Autenticación y Sesión A. de suplantación	[48], [49]	Verificación de la autenticidad temporal. Prevención de ataques de replay.
Defensa de objetivo móvil (MTD)	A. de Intercepción A. de Exploración de Red	[57]	Reducción de ataques de reconocimiento. Robustes ante ataques de intrusión.
Ruido gaussiano (Noise-adding)	A. de Autenticación y Sesión A. de Malware A. Manipulación de Datos	[50]	Precisión en la Verificación de Hablantes. Reducción del éxito de ataques FakeBob del 95% al 0.5%.
Padding de paquetes	A. de Inundación A. de Intercepción A. de Privacidad y Robo de Información	[39]	Mitigación ante ataques dirigidos a los protocolos de comunicación Zigbee o Z-wave.
Técnica de pruebas de penetración mediante el método de optimización por enjambre de partículas	A. de Explotación de Vulnerabilidades A. de Contraseñas A. de Inyección	[55]	Detección de vulnerabilidades. Adaptabilidad ante diversas configuraciones de red o topologías.
Gestión basada en políticas (PBM)	A. de Ingeniería Social	[7]	Eficiente establecimiento de políticas de seguridad.

Gracias a la categorización de las estrategias de mitigación según la categoría de ataque que abordan, se identificó que 10 de estas estrategias contribuyen exclusivamente a la reducción de ataques contra la Confidencialidad, mientras que 3 se centran únicamente en la Integridad.

Por otro lado, si bien no se encontraron estrategias que aborden sólo la Disponibilidad, se identificaron un total de 21 estrategias que la integran junto con otros componentes de la triada. Destacando 11 estrategias de mitigación que abarcan los tres componentes CID, lo que demuestra la importancia de una protección integral.

La Fig. 6, presenta el diagrama de Venn que ilustra la cantidad de estrategias que abordan cada uno de los componentes de la triada de seguridad. Este diagrama permite identificar cómo las estrategias de mitigación se distribuyen entre la Confidencialidad, la Integridad y la Disponibilidad, proporcionando así una base sólida sobre lo encontrado en la literatura que servirá para guiar futuras investigaciones en la seguridad de hogares inteligentes.

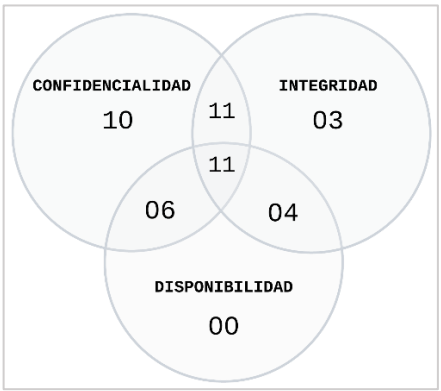

Fig. 6 Análisis de la cobertura de estrategias de mitigación en la Triada CID

IV. CONCLUSIONES

Esta investigación analizó y sintetizó 49 estudios, proporcionando una visión detallada de las vulnerabilidades y los tipos de ataques más comunes en hogares inteligentes. Los principales hallazgos indican que estas redes son particularmente susceptibles a ataques de inundación y de autenticación y sesión. En cuanto a las estrategias de mitigación, se destacaron las técnicas de machine learning, con algoritmos de detección de intrusos alcanzando precisiones de 99.68% y 97.7%, y algoritmos de clasificación de dispositivos con una precisión de 99.79%. Además, los enfoques basados en blockchain demostraron mejorar significativamente la efectividad frente a ataques de manipulación y autenticación en los dispositivos.

Como contribución significativa, esta investigación segmentó los ataques y las soluciones en función de la triada de seguridad de la información (CID). Este enfoque permitió una clasificación más clara y concisa de las amenazas y estrategias, siendo útil para la evaluación y mejora de la seguridad en hogares inteligentes. Esta segmentación ayuda a identificar los componentes más atacados y las soluciones que los abordan, proporcionando una herramienta valiosa para futuros investigadores y profesionales del sector.

Futuras investigaciones deberían expandir la búsqueda a otras fuentes de información, como Web of Science e IEEE Xplorer, así como incluir documentos de pago. Asimismo, se recomienda desarrollar técnicas que combinen machine learning con blockchain para abordar los tres componentes de la triada CID en conjunto, permitiendo una mayor resiliencia ante ataques diversos, asegurando la integridad de la información, la confidencialidad de los datos en tránsito y la disponibilidad crítica para sistemas IoT de seguridad o monitoreo.

REFERENCIAS

[1] PricewaterhouseCoopers, "El futuro del sector de telecomunicaciones, en juego", www.pwc.es. Consultado: el 18 de abril de 2024. [En línea]. Disponible en: https://www.pwc.es/es/telecomunicaciones/global-telecom-outlook-2023-2027.html

[2] R. Fernández, "Hogares inteligentes: número de smart homes en el mundo 2017-2028", es.statista.com. Consultado: el 18 de abril de 2024. [En línea]. Disponible en: https://es.statista.com/estadisticas/573159/evolucion-del-numero-de-hogares-inteligentes-a-nivel-mundial/

[3] BitDefender, "THE 2023 IOT SECURITY LANDSCAPE REPORT", BitDefender. Consultado: el 18 de abril de 2024. [En línea]. Disponible en: https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

[4] SonicWall, "Mid-Year Update: 2023 SonicWall Cyber Threat Report", www.sonicwall.com. Consultado: el 18 de abril de 2024. [En línea]. Disponible en: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2023-cyber-threat-report.pdf

[5] S. Piasecki, L. Urquhart, y 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.

[6] A. Bhardwaj, S. Bharany, A. Abulfaraj, A. Osman Ibrahim, y 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.

[7] D. Bringhenti, F. Valenza, y C. Basile, "Toward Cybersecurity Personalization in Smart Homes", IEEE Secur. Privacy, vol. 20, núm. 1, pp. 45–53, ene. 2022, doi: 10.1109/MSEC.2021.3117471.

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

[9] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, y G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research", MethodsX, vol. 9, p. 101895, 2022, doi: 10.1016/j.mex.2022.101895.

[10] J. Palaskar, "Framing the research question using PICO strategy", J Dent Allied Sci, vol. 6, núm. 2, p. 55, 2017, doi: 10.4103/jdas.jdas_46_17.

[11] Elsevier, "Scopus content", www.elsevier.com. Consultado: el 15 de mayo de 2024. [En línea]. Disponible en: https://www.elsevier.com/products/scopus/content

[12] M. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews", Syst Rev, vol. 10, núm. 1, p. 89, dic. 2021, doi: 10.1186/s13643-021-01626-4.

[13] J. Chen y L. Urquhart, "A 'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home", Information & Communications Technology Law, vol. 31, núm. 1, pp. 99–122, ene. 2022, doi: 10.1080/13600834.2021.1957193.

[14] Y. Lee, S. Rathore, J. H. Park, y J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery", Hum. Cent. Comput. Inf. Sci., vol. 10, núm. 1, p. 9, dic. 2020, doi: 10.1186/s13673-020-0214-5.

[15] I. Ullah y Q. H. Mahmoud, "A Two-Level Flow-Based Anomalous Activity Detection System for IoT Networks", Electronics, vol. 9, núm. 3, p. 530, mar. 2020, doi: 10.3390/electronics9030530.

[16] A. Sredhar, A. Khan, A. R. Gilal, A. Alsughayyir, A. Alshanqiti, y B. A. Talpur, "Assessing and Mitigating Network Vulnerabilities in Philips Hue and Nest Protect Smart Home Devices", IJACSA, vol. 15, núm. 2, 2024, doi: 10.14569/IJACSA.2024.0150202.

[17] F. Iqbal et al., "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction", Sensors, vol. 23, núm. 11, p. 5263, jun. 2023, doi: 10.3390/s23115263.

[18] P. Nespoli, D. Díaz-López, y F. Gómez Mármol, "Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices", Journal of Information Security and Applications, vol. 60, p. 102878, ago. 2021, doi: 10.1016/j.jisa.2021.102878.

[19] D. Mendez Mena y B. Yang, "Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things", IoT, vol. 2, núm. 1, pp. 1–16, dic. 2020, doi: 10.3390/iot2010001.

[20] H. Sallay, "Designing an Adaptive Effective Intrusion Detection System for Smart Home IoT", IJACSA, vol. 15, núm. 1, 2024, doi: 10.14569/IJACSA.2024.0150194.

[21] S. I. Imtiaz et al., "Efficient Approach for Anomaly Detection in Internet of Things Traffic Using Deep Learning", Wireless Communications and Mobile Computing, vol. 2022, pp. 1–15, sep. 2022, doi: 10.1155/2022/8266347.

[22] X. Li, H. Ghodosi, C. Chen, M. Sankupellay, y I. Lee, "Improving Network-Based Anomaly Detection in Smart Home Environment", Sensors, vol. 22, núm. 15, p. 5626, jul. 2022, doi: 10.3390/s22155626.

[23] N. Dat-Thinh, H. Xuan-Ninh, y L. Kim-Hung, "MidSiot: A Multistage Intrusion Detection System for Internet of Things", Wireless Communications and Mobile Computing, vol. 2022, pp. 1–15, feb. 2022, doi: 10.1155/2022/9173291.

[24] Y. Zhang, B. Suleiman, M. J. Alibasa, y F. Farid, "Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach", J Netw Syst Manage, vol. 32, núm. 1, p. 20, ene. 2024, doi: 10.1007/s10922-023-09782-9.

[25] N. S. Alotaibi, H. I. Sayed Ahmed, S. O. M. Kamel, y G. F. ElKabbany, "Secure Enhancement for MQTT Protocol Using Distributed Machine Learning Framework", Sensors, vol. 24, núm. 5, p. 1638, mar. 2024, doi: 10.3390/s24051638.

[26] Md. S. Islam, M. Tasnim, U. Kabir, y M. Jahan, "Securing smart home against sinkhole attack using weight-based IDS placement strategy", IET Wireless Sensor Systems, vol. 13, núm. 6, pp. 216–234, dic. 2023, doi: 10.1049/wss2.12069.

[27] M. Baz, "SEHIDS: Self Evolving Host-Based Intrusion Detection System for IoT Networks", Sensors, vol. 22, núm. 17, p. 6505, ago. 2022, doi: 10.3390/s22176505.

[28] V. Graveto, T. Cruz, y P. Simões, "A Network Intrusion Detection System for Building Automation and Control Systems", IEEE Access, vol. 11, pp. 7968–7983, 2023, doi: 10.1109/ACCESS.2023.3238874.
[29] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf, y D. Kundur, "A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids", IEEE Access, vol. 12, pp. 29414–29444, 2024, doi: 10.1109/ACCESS.2024.3364362.
[30] M. Wazid, A. K. Das, S. Shetty, y M. Jo, "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things", IEEE Access, vol. 8, pp. 88700–88716, 2020, doi: 10.1109/ACCESS.2020.2992467.
[31] S. Sohail, Z. Fan, X. Gu, y F. Sabrina, "Multi-tiered Artificial Neural Networks model for intrusion detection in smart homes", Intelligent Systems with Applications, vol. 16, p. 200152, nov. 2022, doi: 10.1016/j.iswa.2022.200152.
[32] J. Bugeja, A. Jacobsson, y P. Davidsson, "PRASH: A Framework for Privacy Risk Analysis of Smart Homes", Sensors, vol. 21, núm. 19, p. 6399, sep. 2021, doi: 10.3390/s21196399.
[33] Z. Ashraf, A. Sohail, A. Hameed, M. Farhan, F. A. Alotaibi, y M. M. Alnfiai, "Robust and Lightweight Remote User Authentication Mechanism for Next-Generation IoT-Based Smart Home", IEEE Access, vol. 11, pp. 137899–137910, 2023, doi: 10.1109/ACCESS.2023.3336763.
[34] A. Huszti, S. Kovács, y N. Oláh, "Scalable, password-based and threshold authentication for smart homes", Int. J. Inf. Secur., vol. 21, núm. 4, pp. 707–723, ago. 2022, doi: 10.1007/s10207-022-00578-7.
[35] S. Uppuluri y G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications", Wireless Netw, vol. 29, núm. 3, pp. 1333–1354, abr. 2023, doi: 10.1007/s11276-022-03197-1.
[36] N. Y.-R. Douha, M. Sasabe, Y. Taenaka, y Y. Kadobayashi, "An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks", Applied Sciences, vol. 13, núm. 7, p. 4645, abr. 2023, doi: 10.3390/app13074645.
[37] S. G. Abbas et al., "Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach", Sensors, vol. 21, núm. 14, p. 4816, jul. 2021, doi: 10.3390/s21144816.
[38] M. Waseem, M. Adnan Khan, A. Goudarzi, S. Fahad, I. Sajjad, y P. Siano, "Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges", Energies, vol. 16, núm. 2, p. 820, ene. 2023, doi: 10.3390/en16020820.
[39] O. Setayeshfar et al., "Privacy invasion via smart-home hub in personal area networks", Pervasive and Mobile Computing, vol. 85, p. 101675, sep. 2022, doi: 10.1016/j.pmcj.2022.101675.
[40] A. R. Mahlous, "Threat model and risk management for a smart home IoT system", IJCAI, vol. 47, núm. 1, abr. 2023, doi: 10.31449/inf.v47i1.4526.
[41] B. M. Yakubu, M. I. Khan, y P. Bhattarakosol, "IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes", JSAN, vol. 11, núm. 4, p. 80, nov. 2022, doi: 10.3390/jsan11040080.
[42] H. A. Abdulghani, A. Collen, y N. A. Nijdam, "Guidance Framework for Developing IoT-Enabled Systems' Cybersecurity", Sensors, vol. 23, núm. 8, p. 4174, abr. 2023, doi: 10.3390/s23084174.
[43] N. Alturki et al., "Efficient and Secure IoT Based Smart Home Automation Using Multi-Model Learning and Blockchain Technology", CMES, vol. 139, núm. 3, pp. 3387–3415, 2024, doi: 10.32604/cmes.2023.044700.
[44] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, y K. Saleem, "IoT Network Anomaly Detection in Smart Homes Using Machine Learning", IEEE Access, vol. 11, pp. 119462–119480, 2023, doi: 10.1109/ACCESS.2023.3325929.
[45] A. Altameem, P. P, S. T, R. C. Poonia, y A. K. J. Saudagar, "A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0", Systems, vol. 11, núm. 1, p. 28, ene. 2023, doi: 10.3390/systems11010028.
[46] Y. Wang, R. Zhang, X. Zhang, y Y. Zhang, "Privacy Risk Assessment of Smart Home System Based on a STPA–FMEA Method", Sensors, vol. 23, núm. 10, p. 4664, may 2023, doi: 10.3390/s23104664.
[47] R. F. Al-Mutawa y F. Albouraey, "A Smart Home System based on Internet of Things", IJACSA, vol. 11, núm. 2, 2020, doi: 10.14569/IJACSA.2020.0110234.
[48] T. Feng, B. Zhang, C. Liu, y L. Zheng, "Security assessment and improvement of building ethernet KNXnet/IP protocol", Discov Appl Sci, vol. 6, núm. 4, p. 162, mar. 2024, doi: 10.1007/s42452-024-05707-6.
[49] T. Feng y B. Zhang, "Security Evaluation and Improvement of the Extended Protocol EIBsec for KNX/EIB", Information, vol. 14, núm. 12, p. 653, dic. 2023, doi: 10.3390/info14120653.
[50] Z. Chen, L.-C. Chang, C. Chen, G. Wang, y Z. Bi, "Defending against FakeBob Adversarial Attacks in Speaker Verification Systems with Noise-Adding", Algorithms, vol. 15, núm. 8, p. 293, ago. 2022, doi: 10.3390/a15080293.
[51] M. Umer et al., "IoT based smart home automation using blockchain and deep learning models", PeerJ Computer Science, vol. 9, p. e1332, may 2023, doi: 10.7717/peerj-cs.1332.
[52] I. Cvitić, D. Peraković, M. Periša, y B. Gupta, "Ensemble machine learning approach for classification of IoT devices in smart home", Int. J. Mach. Learn. & Cyber., vol. 12, núm. 11, pp. 3179–3202, nov. 2021, doi: 10.1007/s13042-020-01241-0.
[53] S. H. Khan et al., "A new deep boosted CNN and ensemble learning based IoT malware detection", Computers & Security, vol. 133, p. 103385, oct. 2023, doi: 10.1016/j.cose.2023.103385.
[54] Youssef, F. Labeau, y M. Kassouf, "Detection of Load-Altering Cyberattacks Targeting Peak Shaving Using Residential Electric Water Heaters", Energies, vol. 15, núm. 20, p. 7807, oct. 2022, doi: 10.3390/en15207807.
[55] T. Schiller, B. Caulkins, A. S. Wu, y S. Mondesire, "Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing", Information, vol. 14, núm. 10, p. 536, sep. 2023, doi: 10.3390/info14100536.
[56] R. Alasmari y A. A. Alhogail, "Protecting Smart-Home IoT Devices From MQTT Attacks: An Empirical Study of ML-Based IDS", IEEE Access, vol. 12, pp. 25993–26004, 2024, doi: 10.1109/ACCESS.2024.3367113.
[57] S. Seo y D. Kim, "IoDM: A Study on a IoT-Based Organizational Deception Modeling with Adaptive General-Sum Game Competition", Electronics, vol. 11, núm. 10, p. 1623, may 2022, doi: 10.3390/electronics11101623.