ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.1159

GOOD CYBERSECURITY PRACTICES AGAINST CYBER ATTACKS ON IOT DEVICES OF RETAIL COMPANIES: LITERATURE REVIEW

Andre Emilio Marquina Sanchez[1], Axl Fabian Velez Baltazar[2], Gianina Carol Sotelo Broncano[3] and Jherber Fernando Ramos Pariachi[4]

[1,3]First and Third Author's Universidad Tecnológica del Perú, Lima - Perú, *U18102172@utp.edu.pe, c23332@utp.edu.pe*

[2,4]Second Author's Universidad Tecnológica del Perú, Lima - Perú, *U20207418@utp.edu.pe, c29531@utp.edu.pe*

***Abstract*– The growing use of IoT devices in companies has increased cyber threats, affecting data security and business operations. This study presents a systematic literature review to identify cybersecurity best practices aimed at mitigating these risks. Scientific articles published between 2019 and 2024 were analyzed in the Scopus database. The results highlight the importance of implementing detection software and audit tools, along with staff training. Additionally, the current limitations in the adoption of these practices by retail companies are discussed. This work contributes to the understanding of how to strengthen cybersecurity in IoT, guaranteeing a safer digital environment for the retail sector.**

***Keywords*-- Cybercriminals, IoT Devices, Mitigation, Good Practices, Retail Companies.**

BUENAS PRÁCTICAS DE CIBERSEGURIDAD ANTE CIBERATAQUES EN DISPOSITIVOS IOT DE EMPRESAS RETAIL: REVISIÓN DE LA LITERATURA

Andre Emilio Marquina Sanchez[1], Axl Fabian Velez Baltazar[2], Gianina Carol Sotelo Broncano[3] and Jherber Fernando Ramos Pariachi[4]
[1,3]First and Third Author's Universidad Tecnológica del Perú, Lima - Perú, *U18102172@utp.edu.pe, c23332@utp.edu.pe*
[2,4]Second Author's Universidad Tecnológica del Perú, Lima - Perú, *U20207418@utp.edu.pe, c29531@utp.edu.pe*

***Resumen*– El creciente uso de dispositivos IoT en las empresas ha incrementado las amenazas cibernéticas, afectando la seguridad de los datos y la operación de los negocios. Este estudio presenta una revisión sistemática de la literatura para identificar las mejores prácticas de ciberseguridad destinadas a mitigar estos riesgos. Se analizaron artículos científicos publicados entre 2019 y 2024, en la base de datos Scopus. Los resultados destacan la importancia de implementar software de detección y herramientas de auditoría, junto con la capacitación del personal. Además, se discuten las limitaciones actuales en la adopción de estas prácticas por las empresas retail. Este trabajo contribuye al entendimiento de cómo fortalecer la ciberseguridad en IoT, garantizando un entorno digital más seguro para el sector retail.**

***Palabras clave*-- Ciberdelincuentes, Dispositivos IoT, Mitigación, Buenas Prácticas, Empresas Retail.**

I. INTRODUCCIÓN

Cuidar nuestra información se vuelve más importante a diario, aunque muchas veces la expongamos sin darnos cuenta, de tal forma que puede vulnerarnos económica y socialmente; de igual forma, las empresas y organizaciones atraviesan este problema, siendo perjudicadas sus operaciones y la integridad de sus trabajadores; por esta razón nace la obligación de implementar técnicas para salvaguardar nuestros datos. La ciberseguridad es un conjunto de prácticas y herramientas diseñadas para ayudarnos a mitigar los ataques y accesos no autorizados en nuestros sistemas informáticos y dispositivos, protegiéndonos de malware, phishing, hacking y demás tipos de ciberataques. Debido a esta situación, la ciberseguridad ha ganado gran relevancia en los últimos años, convirtiéndose en una de las áreas de investigación más importantes dentro del campo de las TIC [1]. Por esta razón, es crucial conocer más sobre la ciberseguridad y poder aplicarla, no solo para cuidar nuestra información, sino también para no perjudicar los procesos en nuestras empresas u organizaciones.

Por otro lado, la tecnología avanza en distintos sectores, siendo cada vez más común encontrarnos con estas en una empresa, ya sea para automatizar sus procesos u otras operaciones; como también en una casa, que permite el encendido y apagado de luces, entre otras cosas. Es así como nace el termino internet de las cosas (IoT), el cual se refiere a la conexión que hay entre internet y los dispositivos físicos, teniendo una comunicación entre sí y con otros sistemas sin necesidad de influencia humana. El internet ha pasado a ser un elemento indispensable en la vida diaria de las personas. Aprovecharlo a través de sistemas automatizados que interactúan directamente con los usuarios tiene el propósito de optimizar el día a día, simplificando actividades, incrementando el bienestar y haciendo más sencillos diversos procesos en distintas áreas. Esto resulta factible, especialmente si consideramos la rápida evolución tecnológica que estamos experimentando [2]. Es así como el uso de esta nueva tecnología se ha vuelto importante en las empresas, ya que permite un mejor trabajo y una excelente satisfacción del cliente.

Si bien es cierto que el uso de esta nueva tecnología facilita varios procesos, como también mejora nuestra calidad de vida, es de suma importancia entender que nuestros datos recopilados por dispositivos IoT pueden ser vulnerados y estaríamos expuestos a cualquier ataque contra nuestra integridad; por esa razón es importante tener en cuenta conceptos sobre seguridad informática y aplicarlos en nuestro día a día. De igual forma es importante y necesario que las empresas implementen estrategias para mitigar estos ataques a sus dispositivos IoT, las cuales también deben cumplir con la normativa correspondiente. Además, debido al rápido crecimiento del Internet de las Cosas en el mercado de servicios lo ha vuelto un blanco atractivo para los ciberataques, debido a las diversas fallas de seguridad que presenta tanto en los protocolos que utiliza como en la manera en que se implementa [3].

Al conectarse distintos dispositivos en una red, los ciberdelincuentes encuentran puntos de entrada para robar la información que les parezca útil, y de no encontrarlas, seguirán explotándolas hasta encontrar la forma de acceder;

quiere decir, cada dispositivo conectado representa un peligro potencial, especialmente si no cuenta con mecanismos de protección adecuados. A nivel de seguridad, existe una gran diversidad de problemas que presenta la tecnología IoT en cuanto a la manipulación de su entorno operativo, ya sea a través de hardware o software [4]. Un análisis de los ciberataques arrojó que los ciberdelincuentes vulneraron los sistemas por estas causas: falta de actualización del software, contraseñas débiles o predeterminadas y comunicaciones no cifradas, permitiendo a los atacantes controlar los dispositivos y acceder a los datos.

Por ello, la rápida expansión del IoT y la creciente interconexión entre dispositivos han generado nuevas vulnerabilidades en la arquitectura de estos sistemas, haciéndolos susceptibles a diversos tipos de ciberataques. Entre las amenazas más críticas se encuentran los ataques de denegación de servicio (DoS) y los ataques de denegación de servicio distribuido (DDoS), que buscan sobrecargar los recursos de la red mediante un tráfico masivo generado por brechas en los dispositivos comprometidos, exponiendo así una de las principales debilidades de la tecnología IoT. Estos tipos de ataques han sido objeto de estudio en diversas investigaciones recientes, incluyendo un análisis sobre el uso de algoritmos de aprendizaje automático para detectar y mitigar los ataques DDoS en entornos IoT [5].

Además, la falta de estándares para los diversos dispositivos y la complejidad de su gestión resultan en un incremento en el riesgo de ciberataques. Asimismo, la ausencia de normativas uniformes lleva a que cada tipo de empresa implemente sus propios protocolos de seguridad, lo que resulta en inconsistencias y brechas en la protección de datos. En consecuencia, esta falta de uniformidad dificulta la garantía de seguridad en todos los dispositivos y redes. La necesidad de mantener actualizaciones continuas y de realizar un monitoreo eficaz hace que la gestión de estos dispositivos sea especialmente desafiante en entornos con una alta densidad de dispositivos interconectados. Por lo tanto, la protección de las redes IoT sigue siendo un desafío continuo y crítico para las empresas.

La integración de dispositivos IoT en el ámbito empresarial ha aumentado la exposición a ciberataques, debido a las vulnerabilidades propias de esta tecnología y a la falta de estándares de seguridad bien definidos. Ante esta realidad, es esencial realizar una Revisión Sistemática de la Literatura (RSL) que permita determinar las mejores prácticas en ciberseguridad para mitigar estos riesgos. Es indispensable consolidar el conocimiento sobre los desafíos de seguridad y privacidad en el IoT, para desarrollar estrategias efectivas que protejan tanto los datos como las operaciones empresariales. En consecuencia, esta RSL es crucial para proporcionar a las organizaciones directrices basadas en la evidencia que fortalezcan su seguridad frente a las amenazas cibernéticas [6].

A diferencia de las revisiones sistemáticas previas, que se han centrado en aspectos específicos de la ciberseguridad en IoT, como los ataques DDoS en determinados sectores, la presente RSL ofrece una perspectiva más integral y actualizada. Mientras que estudios anteriores se han limitado a analizar áreas concretas, esta revisión abarca una variedad de estrategias de mitigación y vulnerabilidades. Así, proporciona a las organizaciones una guía más completa y basada en evidencia, permitiéndoles implementar prácticas de seguridad más robustas y eficaces para fortalecer su defensa contra amenazas cibernéticas [7]. Asimismo, existe otra RSL que aborda el tema de los Sistemas de Detección de Intrusiones (IDS) y los Sistemas de Detección de Anomalías (ADS) que son esenciales en el tema de la ciberseguridad enfocándose en aspectos más específicos como son las tecnologías en el contexto IoT [8]. Por un lado, los IDS esencialmente utilizados y estudiados por la capacidad que tienen para monitorear el tráfico de red y las actividades del sistema en busca de comportamientos maliciosos o anormales esto permite proporcionar una respuesta de manera inmediata ya que se trata en tiempo real. Por otro lado, los ADS debido a su habilidad de aprendizaje automático y de uso de técnicas estadísticas, facilita la identificación de amenazas desconocidas o de actividades irregulares dentro de estas redes IoT.

En este estudio, el objetivo es entender e ilustrar la situación actual de las prácticas de ciberseguridad adecuadas aplicadas a dispositivos IoT de empresas retail. Así pues, la finalidad primordial de este estudio es reconocer y categorizar estrategias, herramientas y metodologías que ayuden a reducir amenazas cibernéticas particulares en este campo, incorporando enfoques técnicos y regulaciones, con el propósito de ofrecer una perspectiva completa y ordenada de las soluciones existentes en la literatura, sometiéndolas a un análisis crítico meticulosamente aplicado sobre el tema.

En consecuencia, este documento se estructura de la siguiente forma. La Metodología, en su sección 2, detalla el método empleado para el estudio de las buenas prácticas de ciberseguridad, incluyendo los criterios para elegir y valorar las estrategias implementadas en dispositivos IoT en empresas retail. La sección 3, Resultados, expone y estructura los descubrimientos realizados, resaltando las estrategias más eficaces para reducir las amenazas cibernéticas. En la sección 4, Discusión, se examina la importancia y utilidad de estas prácticas en el ámbito de empresas retail, valorando sus puntos fuertes, restricciones y potenciales áreas de mejora. Finalmente, en la sección 5, Conclusiones, se resumen los hallazgos más relevantes y se proponen proyectos de investigación futuros para potenciar la seguridad en los dispositivos de IoT.

II. METODOLOGÍA

En este estudio de investigación científica se llevó a cabo una revisión sistemática de la literatura sin metaanálisis, con el objetivo de analizar las buenas prácticas de ciberseguridad que permitirán mitigar amenazas cibernéticas en dispositivos IoT de las empresas retail.

Por esta razón, se utilizó como estrategia inicial los componentes PICOC para el proceso de búsqueda. Este método ayuda a describir cinco elementos esenciales de una pregunta de búsqueda, facilitando la identificación de los aspectos clave para un meta análisis y proporcionando palabras clave relevantes para la revisión de la literatura. Los componentes definidos para esta investigación son: (P) incremento de los ciberdelincuentes en los dispositivos IoT de empresas retail, (I) buenas prácticas de ciberseguridad, (C) estadísticas y métodos sobre los ataques cibernéticos, (O) mitigar los ataques cibernéticos a los dispositivos IoT de empresas retail, y (C) empresas retail. Además, se seleccionaron palabras clave asociadas a cada componente para desarrollar la ecuación de búsqueda, como se detalla en la tabla.

Para la selección de estudios en esta investigación, se han definido criterios de inclusión y exclusión que aseguran la relevancia y calidad de la información analizada. Se incluyen aquellos estudios que aborden los métodos utilizados por los ciberdelincuentes para vulnerar dispositivos IoT, las buenas prácticas de ciberseguridad para mitigar ataques, datos estadísticos sobre ciberataques y medidas de prevención, así como técnicas específicas para proteger dispositivos IoT. Además, se consideran estudios que analicen el uso de estos dispositivos en el sector retail.

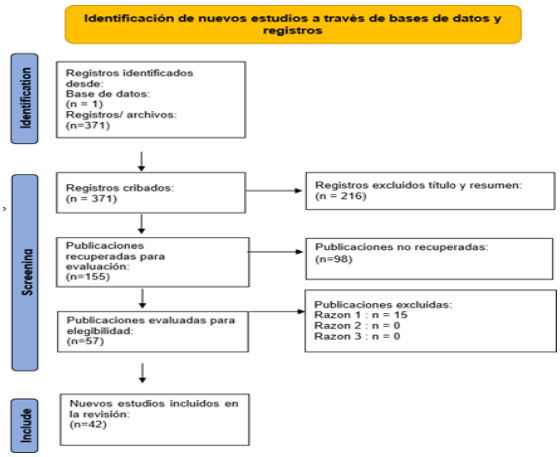
Por otro lado, se excluyen aquellos estudios que no presenten métodos empleados por ciberdelincuentes, publicaciones en idiomas distintos al japonés e inglés, investigaciones anteriores a 2019 y aquellas que no se enfoquen en dispositivos IoT utilizados en empresas del sector retail.

A continuación, se detallará los resultados del flujograma PRISMA. Al rodar la ecuación de búsqueda se obtuvo, en la base de datos Scopus se obtuvo 371 estudios.

Luego con los documentos encontrados en Scopus se procedió a exportarlo en un formato CVS, y se descargó en el programa Excel.

Después de realizar la descarga de los artículos de la base de datos de Scopus, estos estudios se descargaron en el Excel, para continuar con los cribados, donde se inició con el cribado por títulos y resumen, se empezó con 371 artículos, de las cuales se depuraron 216 artículos por los criterios de exclusión, quedando recuperadas para la evaluación 155 artículos, de los cuales publicaciones no recuperadas fueron 98, y publicaciones evaluadas para elegibilidad fueron 57. Para finalizar se excluyeron 15 artículos porque no cuentan con las competencias necesarios para el presente trabajo, según el número de estudios incluidos en la revisión son de 42 artículos. Según se muestra en la Figura 3.

Figura 1.



III RESULTADOS

Tras llevar a cabo un análisis de los artículos seleccionados para esta revisión sistemática, se organizó la presentación de los resultados en dos secciones. La primera se centra en los datos bibliométricos más relevantes de los estudios, mientras que la segunda aborda las características de los mismos, con el fin de responder a las preguntas PIOC del estudio. En lo que respecta a los resultados bibliométricos, el artículo titulado "Una revisión de las vulnerabilidades del firmware de IoT y técnicas de auditoría" de [9] se destaca por tener el mayor número de citas, alcanzando un total de 151, superando así a los demás estudios analizados. Este trabajo se enfoca en la identificación de vulnerabilidades en el firmware de dispositivos IoT y resalta la necesidad de aplicar técnicas de auditoría efectivas para asegurar la integridad y seguridad de estos sistemas. Además, se realizó un análisis exhaustivo de las técnicas disponibles, lo que llevó a la propuesta de estrategias para mitigar los riesgos asociados a las amenazas cibernéticas, garantizando así una mayor protección de los dispositivos conectados y de la información que manejan.

Por otro lado, el estudio con el mayor volumen con un total de 146 es "IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber-attacks" de [10]. Este artículo se centra en el desarrollo de un marco de seguridad que permite predecir el comportamiento de los dispositivos IoT y detectar dispositivos maliciosos que puedan comprometer la seguridad ante ciberataques. La combinación de estos enfoques refuerza la necesidad de investigar y mejorar las prácticas de seguridad en el ámbito del Internet de las Cosas.

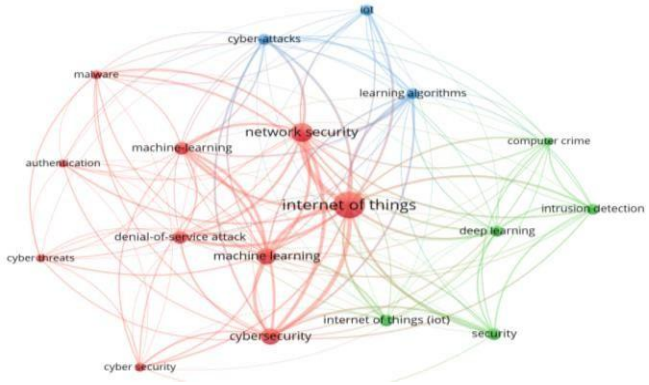
Tabla 1: Datos bibliométricos de los estudios analizados

N°	Autores	Volumen de la revista	N° de citas	Revista
[09]	Awajan, A.	12	24	Computers
[10]	Nazir, A.et al.	23	17	Sensors
[11]	Taimur Bakhshi et al.	6	151	Himanshu Agrawal y Neminath Hubballi
[12]	Daniel Okey et al.	7	81	Jiankun Hu
[13]	Ivan Cvitić et al.	9	44	JISEM
[14]	Rajasekhar Chaganti et al.	22	46	Abderrezak Rachedi
[15]	Yusuf Yamak et al.	26	37	IEEE Access
[16]	Doctor Sipon Miah et al.	15	43	IEEE Access
[17]	Randa Allafi et al.	14	28	IEEE Access
[18]	Denis Salopek et al.	105	47	Xiaojie Wang
[19]	Kim Hung Le et al.	8	67	Stavros Shiaeles, Bogdan Ghita y Nicholas Kolokotronis
[20]	Walid Dhifallah et al.	12	45	JISEM
[21]	Eric Gyamfi et al.	32	123	Claudia Campolo
[22]	Bebé Xu et al.	41	40	Dawid P Damasevicius y Hafiz Tayyab Rauf
[23]	Saeed Masoud Al-Shahrani et al.	27	26	JISEM
[24]	Walid Dhifallah et al.	10	1	IJATEE
[25]	Eric Gyamfi et al.	22	55	journal
[26]	Bebé Xu et al.	31	44	JISEM
[27]	Saeed Masoud Al-Shahrani et al.	74	3	Tech Science Press.
[28]	Bin Yuan et al.	21	0	IEEE Access
[29]	Weihong et al.	19	6	MDPI
[30]	Peng Xiao	13	1	Journal of Information Systems Engineering & Management (JISEM).
[31]	Luis Eduardo Suástegui et al.	2	0	JISEM
[32]	El rey Feng1 et al.	3	0	MDPI (Multidisciplinary Digital Publishing Institute).
[33]	Fatma S. Alrayes et al.	11	10	MDPI
[34]	Abdulmohsen Alharbi et al.	13	3	International Journal of Advanced Computer Science and Applications (IJACSA)
[35]	QIONG WU et al.	1	18	IEEE
[36]	Parque Jin Ho et al.	23	7	Journal of Internet Technology
[37]	Hisham	11	19	MDPI
[38]	Srikanth Reddy Vutukuru	19	27	J. Electrical Systems
[39]	Laraib Sana et al.	12	103	IEEE Access
[40]	Zhenhao Luo et al.	9	20	MDPI

[41]	Sung Moon Kwon-san et al.	123	22	Springer
[42]	Stanislav Abaymov	4	13	MDPI

Diagrama neuronal de palabras claves sobre el estudio realizado

Figura 2: Diagrama neuronal de palabras claves sobre el estudio realizado

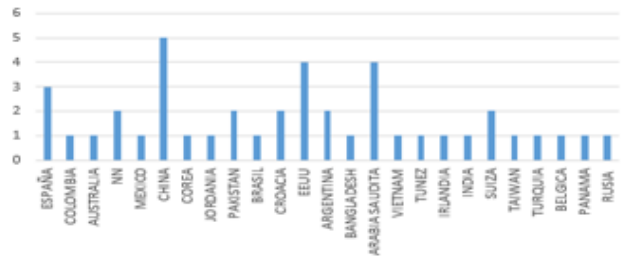


La Figura 3, con respecto a los años de publicación, la mayor parte de artículos analizados han sido publicados en el año 2023, como podemos observar en los estudios [21], [10], [38], [12], [6], [37], [15], [7], [18], [24], [30], [5], [20], [34], [13], [9], [28], [3], [40], [16], [11].

Figura 3: Años de publicaciones

La Figura 4 indica que, como parte del reconocimiento de los artículos, se halló la ubicación geográfica de cada uno de ellos. El país en donde se obtuvo la mayor cantidad de artículos es China con 5 artículos cono lo demuestran los estudios de [21], [16], [18], [42], [27].

Figura 4: País de Origen



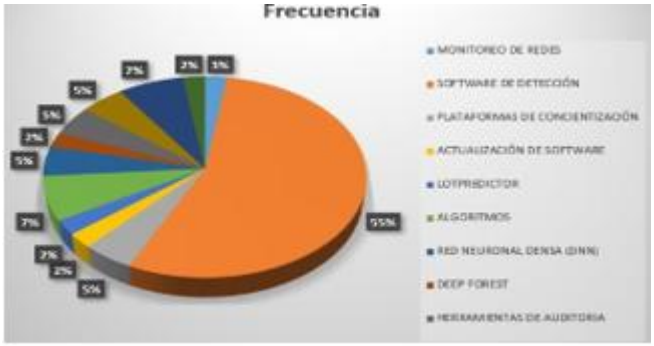
En cuanto a los resultados de los estudios evaluados se han segmentado en los siguientes elementos: Problema más frecuente que se encontró en los dispositivos IoT es la falta de seguridad que presentan los mismos, en la intervención se contempla a los softwares de detección como la herramienta más usada para la detección de los ataques, en resultados se observó una mayor precisión en la detección de amenazas y disminución de vulnerabilidades, y el contexto se identificó en microempresas, como también en macroempresas.

En la figura 5, en cuanto al problema, se han expuesto 20 de mayor relevancia, el mayor problema presentado fue la falta de seguridad que presentan los equipos IoT de las empresas retail con un 48%, como lo demuestran los estudios de: [9], [30], [7],[10], [38], [25] [6], [12], [21], [37], [42] [15], [19],[22],[1],[15][40], [27], [38], [16].

Figura 5: Problemas del diagnostico

Siguiendo el estudio de los datos de la intervención, la figura 6 ilustra las herramientas empleadas para el diagnóstico, la mayoría de las investigaciones han empleado software de detección, tal y como lo evidencian las investigaciones de [13], [30],[1], [28], [25], [16], [2], [15], [6], [11], [15], [19],[32],[7],[4], [40], [22], [33], [38],[27], [22], [23].

Figura 6: Herramientas el diagnostic



Asimismo, en la figura 7 y 8 se determinó las herramientas que permitieron la mejora y los resultados que se obtuvieron al implementarlos para una mejor seguridad en los dispositivos IoT, como lo evidencian las investigaciones de

[1] [28]. [42], [21],[10], [38], [30], [16], [12], [2], [15], [6],[25],[7], [31].

Figura 7: Herramientas de mejora

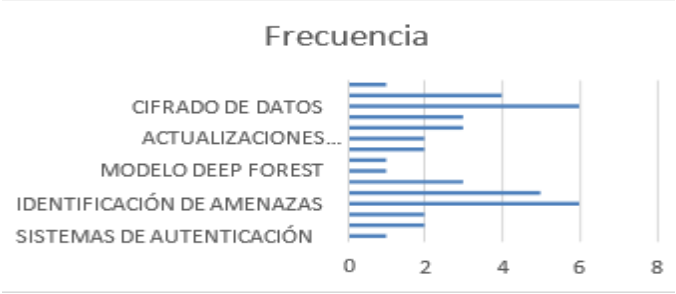


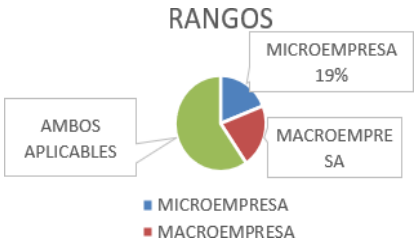
Figura 8: Resultados de los estudios realizados

Finalmente, en la figura 9, en relación al contexto, se detectaron los problemas de vulnerabilidades en los diversos rubros de las empresas. Esta muestra indica que, de los totales de artículos estudiados, el mayor número corresponde a la ciberseguridad en el campo de dispositivos IoT con 27 artículos estudiados: [30], [28], [30],[16],[12], [2], [15],[6], [9], [15], [16], [7], [33], [27], [15],[5], [1] [25], [36], [4], [22],[11] [37], [45], [30], [24],[42].

Figura 9: Estudios realizados en los sectores de seguridad informática

Asimismo, la figura 10 detalla el tipo de empresas por tamaño (microempresa, macroempresa o ambos aplicables) que están incluidas dentro del sector que hace uso de dispositivos IoT, sector al que pertenece 25 artículos seleccionados.

Figura 10: Tipo de empresa (por tamaño)



IV Discusión

En esta revisión sistemática, se encontró que la falta de seguridad en dispositivos IoT de empresas retail es una de las vulnerabilidades más comunes. Como señala [1], el rápido crecimiento del IoT no ha sido acompañado por el mismo nivel de atención en la seguridad de los dispositivos, lo cual expone a las empresas a una serie de ataques cibernéticos, siendo el ataque de denegación de servicio distribuido (DDoS) uno de los más frecuentes. En comparación con otros estudios, donde la seguridad en dispositivos IoT se consideraba suficiente con medidas básicas de protección, los hallazgos de esta revisión sugieren que estos métodos no son suficientes frente a la sofisticación de los ataques actuales. El uso de dispositivos IoT sin protocolos de seguridad robustos resulta en una mayor vulnerabilidad y un riesgo elevado de intrusiones maliciosas. Como señala [17], la creciente adopción de dispositivos IoT aumenta el riesgo de ataques cibernéticos, lo que requiere mejores estrategias de detección de intrusiones.

A diferencia de lo reportado en estudios previos sobre ciberseguridad en IoT, como lo señala [6], se destacan tecnologías como firewalls, sistemas de detección de intrusiones y mecanismos de autenticación como principales medidas para proteger los dispositivos IoT, en esta revisión se encontró que el empleo de algoritmos avanzados de detección y la implementación de softwares de seguridad especializados pueden mejorar significativamente la detección y respuesta ante ataques DDoS en dispositivos IoT. Estos métodos permiten identificar comportamientos anómalos de manera más rápida y efectiva, incrementando la capacidad de respuesta de las empresas ante amenazas en tiempo real y reduciendo así la probabilidad de que los ataques comprometan la infraestructura.

Si bien estas medidas técnicas son fundamentales, se identificó que la capacitación adecuada del personal es igualmente crucial para fortalecer la seguridad en IoT. Como señala [13], una formación adecuada al personal no técnico ayudaría a no caer ante intentos de ataques por parte de los ciberdelincuentes. En contraste con otros estudios, en los que se priorizaban las actualizaciones automáticas de software como principal método de prevención, esta revisión destaca la importancia de formar al personal en prácticas seguras, especialmente en la identificación temprana de amenazas y el

manejo adecuado de los dispositivos IoT. La combinación de herramientas tecnológicas y una fuerza laboral bien entrenada contribuye a un enfoque de seguridad integral, que disminuye la exposición de los dispositivos IoT a posibles ataques y vulneraciones.

V Conclusiones

A través de esta Revisión Sistemática de Literatura (RSL), se ha logrado alcanzar el propósito principal de evaluar las mejores prácticas de ciberseguridad para reducir los riesgos de ciberataques en dispositivos IoT dentro de empresas del sector retail. Los resultados obtenidos reflejan la preocupación creciente por la seguridad de estos dispositivos, debido a su vulnerabilidad por la falta de estándares de protección adecuados y a la variedad de ataques detectados, como los ataques de denegación de servicio (DDoS) y el control remoto de dispositivos mediante firmware comprometido.

Los hallazgos sugieren que las estrategias más efectivas incluyen la realización de auditorías regulares del firmware, el uso de sistemas para la detección de intrusiones (IDS) y de anomalías (ADS), además de la implementación de políticas de cifrado robustas para asegurar las comunicaciones entre los dispositivos. También, el análisis bibliométrico subraya investigaciones clave que proponen enfoques innovadores, como el marco de seguridad IoTPredictor, diseñado para anticipar comportamientos irregulares en dispositivos IoT y tomar medidas preventivas ante posibles ciberataques.

La principal contribución de esta revisión es ofrecer una visión integral sobre las prácticas de seguridad más recomendadas para el IoT en el contexto del retail, lo cual permite a las organizaciones mejorar su infraestructura y proteger de manera más efectiva los datos de sus clientes. Sin embargo, se detectaron limitaciones en cuanto a la falta de homogeneidad en la aplicación de estas prácticas, lo que representa un reto para desarrollar un marco de seguridad estandarizado para dispositivos IoT.

Además, el análisis de los 42 estudios considerados en esta RSL destaca que la Precisión en la Detección de Amenazas fue el resultado más notable, presente en un 36% de los trabajos revisados. Por otro lado, se observó una mejora significativa en la Disminución de Vulnerabilidades y la Implementación de Prácticas de Seguridad Más Robustas, reportadas en un 24% de los estudios cada una. Estos datos subrayan la efectividad de estas estrategias y refuerzan la necesidad de su adopción para fortalecer la seguridad de dispositivos IoT en el sector retail.

Para futuras investigaciones, se sugiere profundizar en el uso de métodos basados en inteligencia artificial y aprendizaje automático, con el fin de mejorar la identificación de amenazas y crear soluciones adaptativas que respondan a la evolución constante de los ataques cibernéticos. Igualmente, se considera esencial fomentar el desarrollo de normas internacionales que garanticen la seguridad de los dispositivos IoT, independientemente del contexto en que se implementen.

Aunque esta Revisión Sistemática de Literatura aporta hallazgos significativos, es necesario reconocer las limitaciones que enfrentamos durante su desarrollo. Aunque tuvimos acceso a bases de datos de artículos o revisiones sistemática de la literatura proveniente de Scopus, la naturaleza dinámica y en constante crecimiento del Internet de las Cosas (IoT) representó un desafío. Actualmente, no se cuenta con un marco consolidado que unifique las mejores prácticas de ciberseguridad en este campo, lo que dificulta la estructuración de enfoques consistentes. Asimismo, la amplitud y heterogeneidad del IoT, que incluye diversos sectores y dispositivos, hicieron que fuera complejo encontrar RSL completamente similares a esta. Estas características complicaron el proceso de selección y análisis de estudios, limitando la posibilidad de realizar generalizaciones más extensas. A pesar de estas dificultades, consideramos que nuestra revisión aporta valor al abordar un tema de alta relevancia que demanda mayor atención y esfuerzos de estandarización.

Referencias

[1] J. Mendivil-Caldentey B. Sanz-Urquijo and M. Gutiérrez Almazor. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura [Competencybased cybersecurity training and awareness: a systematic literature review]. Pixel-Bit. Revista de Medios y Educación, 63, 197-225. https://doi.org/10.12795/pixelbit.91640

[2] Y. Salinas Anaya, et al. (2022). El impacto del internet de todas las cosas (IoT) en la vida cotidiana. Ciencia Latina Revista Científica Multidisciplinar, 6(2), 1369-1378. https://doi.org/10.37811/cl_rcm.v6i2.1959

[3] J. Márquez Díaz (2022). Cybersecurity and Internet of Things. Outlook for this Decade. Computación y Sistemas, 26. https://doi.org/10.13053/cys-26-3-3925

[4] R. Kalaria, et al. (2024). IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks. Computers & Security, 146, 104037. https://doi.org/10.1016/j.cose.2024.104037

[5] M. Ebady Manaa, et al. (2024). DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments. Inteligencia Artificial, 27(74), 152–165. https://doi.org/10.4114/intartif.vol27iss74pp152-165

[6] C. D. Morales-Molina, et al. (2021). A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. Sensors, 21(9). https://doi.org/10.3390/s21093173

[7] R. Xu, et al. (2019). A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment. Symmetry, 11, 78. https://doi.org/10.3390/sym11010078

[8] Y.-S. Kim, Y.-E. Kim and H. Kim (2023). A Model Training Method for DDoS Detection Using CTGAN under 5GC Traffic. Computer Systems Science and Engineering, 47(1). https://doi.org/10.32604/csse.2023.039550

[9] A. Awajan (2023). A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. Computers, 12(2). https://doi.org/10.3390/computers12020034

[10] A. Nazir, et al. (2023). A Novel Feature-Selection Algorithm in IoT Networks for Intrusion Detection. Sensors, 23(19), 8153. https://doi.org/10.3390/s23198153

[11] T. Bakhshi, B. Ghita and I. Kuzminykh (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors, 24(2). https://doi.org/10.3390/s24020708
[12] O. D. Okey, et al. (2022). BoostedEnML: Efficient Technique for Detecting Cyberattacks in IoT Systems Using Boosted Ensemble Machine Learning. Sensors, 22(19). https://doi.org/10.3390/s22197409
[13] I. Cvitic, et al. (2022). Boosting- Based DDoS Detection in Internet of Things Systems. IEEE Internet of Things Journal, 9(3), 2109-2123. https://doi.org/10.1109/JIOT.2021.3090909
[14] R. Chaganti, et al. (2023). Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks. Information (Switzerland), 14(1). https://doi.org/10.3390/info14010041
[15] Y. Yamak, S. Tosun and M. Aydos (2024). DICEguard: Enhancing DICE security for IoT devices with periodic memory forensics. Journal of Supercomputing, 80(13), 19824-19844. https://doi.org/10.1007/s11227-024-06194-7
[16] M. S. Miah, et al. (2020). Enhanced sensing and sum-rate analysis in a cognitive radio-based internet of things. Sensors (Switzerland), 20(9). https://doi.org/10.3390/s20092525
[17] R. Allafi and I. R. Alzahrani (2024). Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model. IEEE Access, 12, 63282-63291. https://doi.org/10.1109/ACCESS.2024.3390093
[18] D. Salopek and M. Mikuc (2023). Enhancing Mitigation of Volumetric DDoS Attacks: A Hybrid FPGA/Software Filtering Datapath. Sensors, 23(17). https://doi.org/10.3390/s23177636
[19] K.-H. Le, et al. (2022). IMIDS: An Intelligent Intrusion Detection System against Cyber Threats in IoT. Electronics (Switzerland), 11(4). https://doi.org/10.3390/electronics11040524
[20] W. Dhifallah, et al. (2023). Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection. International Journal of Advanced Technology and Engineering Exploration, 10(106), 1167-1183. https://doi.org/10.19101/IJATEE.2023.10101465
[21] E. Gyamfi and A. Jurcut (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. Sensors, 22(10). https://doi.org/10.3390/s22103744
[22] B. Xu, et al. (2023). IoT Intrusion Detection System Based on Machine Learning. Electronics (Switzerland), 12(20). https://doi.org/10.3390/electronics12204289
[23] S. M. Alshahrani, et al. (2023). IoT- Cloud Assisted Botnet Detection Using Rat Swarm Optimizer with Deep Learning. Computers, Materials and Continua, 74(2), 3085-3100. https://doi.org/10.32604/cmc.2023.032972
[24] W. Dhifallah, et al. (2023). Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection. International Journal of Advanced Technology and Engineering Exploration, 10(106), 1167-1183. https://doi.org/10.19101/IJATEE.2023.10101465
[25] E. Gyamfi and A. Jurcut (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. Sensors, 22(10). https://doi.org/10.3390/s22103744
[26] B. Xu, et al. (2023). IoT Intrusion Detection System Based on Machine Learning. Electronics (Switzerland), 12(20). https://doi.org/10.3390/electronics12204289
[27] S. M. Alshahrani, et al. (2023). IoT- Cloud Assisted Botnet Detection Using Rat Swarm Optimizer with Deep Learning. Computers, Materials and Continua, 74(2), 3085-3100. https://doi.org/10.32604/cmc.2023.032972
[28] B. Yuan, et al. (2024). Leakage of Authorization-Data in IoT Device Sharing: New Attacks and Countermeasure. IEEE Transactions on Dependable and Secure Computing, 21(4), 3196-3210. https://doi.org/10.1109/TDSC.2023.3323713
[29] W. Han, et al. (2019). Low-Power Distributed Data Flow Anomaly-Monitoring Technology for Industrial Internet of Things. Sensors, 19(12), 2804. https://doi.org/10.3390/s19122804
[30] P. Xiao (2024). Malware Cyber Threat Intelligence System for Internet of Things (IoT) Using Machine Learning. Journal of Cyber Security and Mobility, 13(1), 53-90. https://doi.org/10.13052/jcsm2245-1439.1313
[31] L. E. S. Jaramillo (2019). Malware Threats Analysis and Mitigation Techniques for Compromised Systems. Journal of Information Systems Engineering and Management, 4(1). https://doi.org/10.29333/jisem/5742
[32] F. Wang, Y. Tang, & H. Fang (2023). Mitigating IoT Privacy-Revealing Features by Time Series Data Transformation. Journal of Cybersecurity and Privacy, 3(2), 209-226. https://doi.org/10.3390/jcp3020012
[33] S. F. Alrayes, M. Maray, A. Gaddah, A. Yafoz, R. Alsini, O. Alghushairy, H. Mohsen, & A. Motwakel (2022). Modeling of Botnet Detection Using Barnacles Mating Optimizer with Machine Learning Model for Internet of Things Environment. Electronics (Switzerland), 11(20). https://doi.org/10.3390/electronics11203411
[34] A. Alharbi, M. A. Hamid, & H. Lahza (2022). Predicting Malicious Software in IoT Environment Based on Machine Learning and Data Mining Techniques. International Journal of Advanced Computer Science and Applications, 13(8), 497-506. https://doi.org/10.14569/IJACSA.2022.0130857
[35] L. Sana, M. M. Nazir, J. Yang, L. Hussain, Y.-L. Chen, C. S. Ku, M. Alatiyyah, S. A. Alateyah, & L. Y. Por (2024). Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection With Vision Transformers. IEEE Access, 12, 82443-82468. https://doi.org/10.1109/ACCESS.2024.3404778
[36] J. H. Park, S. K. Singh, M. M. Salim, A. E. L. Azzaoui, & J. H. Park (2022). Ransomware-based Cyber Attacks: A Comprehensive Survey. Journal of Internet Technology, 23(7), 1557-1564. https://doi.org/10.53106/160792642022122307010
[37] H. Alasmary (2023). RDAF-IIoT: Reliable Device-Access Framework for the Industrial Internet of Things. Mathematics, 11(12). https://doi.org/10.3390/math11122710
[38] S. R. Vutukuru & S. C. Lade (2023). SecureIoT: Novel Machine Learning Algorithms for Detecting and Preventing Attacks on IoT Devices. Journal of Electrical Systems, 19(4), 315-335. https://doi.org/10.52783/jes.641
[39] L. Sana, M. M. Nazir, J. Yang, L. Hussain, Y.-L. Chen, C. S. Ku, M. Alatiyyah, S. A. Alateyah, & L. Y. Por (2024). Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection with Vision Transformers. IEEE Access, 12, 82443-82468. https://doi.org/10.1109/ACCESS.2024.3404778
[40] Z. Luo, B. Wang, Y. Tang, & W. Xie (2019). Semantic-based representation binary clone detection for cross-architectures in the internet of things. Applied Sciences (Switzerland), 9(16). https://doi.org/10.3390/app9163283
[41] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, & K. Yim. (2021). Towards 5G-based IoT security analysis against Vo5G eavesdropping. Computing, 103(3), 425-447. https://doi.org/10.1007/s00607-020-00855-0
[42] S. Abaimov (2024). Understanding and Classifying Permanent Denial-of- Service Attacks. Journal of Cybersecurity and Privacy, 4(2), 324-339. https://doi.org/10.3390/jcp4020016