CIBERSEGURIDAD EN LOS DISPOSITIVOS IOT DE USO DOMÉSTICO: UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA

CYBERSECURITY IN HOME IOT DEVICES: A SYSTEMATIC REVIEW OF THE LITERATURA

Xavier Alexander Gálvez Cisneros [1*]

[1] Pontificia Universidad Católica del Ecuador. Ecuador. ORCID: https://orcid.org/0009-0009-0840-9672. Correo: xagalvez@pucesa.edu.ec

Dario Javier Robayo Jacome [2]

[2] Profesor Principal Auxiliar en la Escuela de Ingenierías de la Pontificia Universidad Católica del Ecuador. Ambato, Ecuador. ORCID: https://orcid.org/0000-0002-0661-6573. Correo: drobayo@pucesa.edu.ec

*** Autor para correspondencia: xagalvez@pucesa.edu.ec**

Resumen

Este estudio se enfocó en garantizar la seguridad de los dispositivos de Internet de las Cosas (IoT) en los hogares, dada la creciente adopción de tecnologías de automatización. Fue crucial evaluar su fiabilidad para proteger la privacidad y seguridad de los datos personales. El objetivo general fue realizar una revisión sistemática de la literatura sobre la situación actual de los dispositivos IoT de uso doméstico. Se empleó una metodología exploratoria, transversal y cualitativa, siguiendo el método PRISMA. Se buscaron artículos en bases de datos académicas como IEEE Xplore, Springer Link, ScienceDirect, SciELO y Google Scholar. Los criterios de inclusión se enfocaron en estudios de los últimos cinco años sobre tendencias, desafíos y vulnerabilidades en la seguridad de dispositivos IoT en hogares. La revisión identificó vulnerabilidades comunes como la falta de cifrado y contraseñas débiles, recomendando la implementación de cifrado, gestión de contraseñas y actualizaciones regulares. Los beneficios del IoT en hogares incluyen conveniencia y eficiencia energética, mientras que las limitaciones abarcan preocupaciones de privacidad y problemas de compatibilidad. Las técnicas de anonimización y pseudonimización son cruciales para proteger los datos personales. Además, se destacó la importancia de adoptar estándares comunes para mejorar la interoperabilidad y la seguridad en el ecosistema IoT doméstico.

Palabras clave: ciberseguridad; Dispositivos IoT; automatización del hogar; privacidad de datos; revisión sistemática.

Abstract

This study focused on ensuring the security of Internet of Things (IoT) devices in homes, given the growing adoption of automation technologies. Evaluating their reliability was crucial to protecting privacy and data security. The main objective was to conduct a systematic review of the current state of domestic IoT devices. An exploratory, cross-sectional, and qualitative methodology was employed, following the PRISMA method. Articles were searched in academic databases such as IEEE Xplore, Springer Link, ScienceDirect, SciELO, and Google Scholar. Inclusion criteria focused on studies from the last five years on trends, challenges, and vulnerabilities in the security of IoT devices in homes.The review identified common vulnerabilities such as lack of encryption and weak passwords, recommending the implementation of encryption, password management, and regular updates. The benefits of IoT in homes include convenience and energy efficiency, while limitations encompass privacy concerns and compatibility issues. Anonymization and pseudonymization techniques are crucial for protecting personal data. Additionally, the importance of adopting common standards to improve interoperability and security in the domestic IoT ecosystem was highlighted.

Keywords: *cybersecurity; IoT devices; home automation; data privacy; systematic review*

Fecha de recibido: 23/11/2024
Fecha de aceptado: 03/01/2025
Fecha de publicado: 06/01/2025

Introducción

La rápida adopción de dispositivos de IoT en el ámbito doméstico ha transformado la manera en que interactuamos con nuestro entorno. Desde asistentes virtuales y termostatos inteligentes hasta cámaras de seguridad y electrodomésticos conectados, estos dispositivos han incrementado la comodidad y eficiencia en los hogares. Sin embargo, esta creciente interconexión también ha generado preocupaciones significativas en torno a la ciberseguridad. La capacidad de estos dispositivos para recopilar, transmitir y almacenar datos personales los convierte en objetivos atractivos para los cibercriminales. Asimismo, A medida que las amenazas cibernéticas evolucionan, se vuelve imperativo asegurar que los dispositivos IoT utilizados en los hogares no solo funcionen correctamente, sino que además ofrezcan un nivel adecuado de protección contra accesos no autorizados y otras vulnerabilidades. En este contexto, el presente estudio tiene como objetivo realizar una revisión sistemática de la literatura reciente para evaluar las tendencias, desafíos y vulnerabilidades en la seguridad de los dispositivos IoT domésticos, proporcionando así una base sólida para futuras investigaciones y prácticas en ciberseguridad.

El IoT está experimentando un crecimiento continuo y una expansión en hogares de todo el mundo. Cada vez más, los hogares adoptan dispositivos IoT para mejorar la comodidad, la eficiencia y la seguridad en su vida diaria(Zermeño et al., 2021), (Soto et al., 2019). Estos dispositivos, como termostatos inteligentes, cámaras de seguridad y electrodomésticos conectados a la red, permiten a los usuarios controlar y monitorear sus hogares de forma remota a través de aplicaciones móviles y dispositivos inteligentes (Balanta et al., 2021). Sin embargo, este aumento en la adopción de dispositivos IoT plantea importantes desafíos, especialmente en lo que respecta a la protección de la información y la privacidad de los usuarios (Khan et al., 2018).

La falta de medidas de seguridad adecuadas puede exponer a estos dispositivos a amenazas cibernéticas, y la gran cantidad de información recopilada plantea preocupaciones sobre la privacidad y el uso indebido de los datos (Gutiérrez et al., 2022), (Revelo Vizcaino & Egas Acosta, 2023), (Girme & Patil, 2019), (Jain et al., 2019). Además, la falta de conciencia y capacitación en seguridad cibernética por parte de los usuarios puede aumentar el riesgo de vulnerabilidades (Morán et al., 2023), (ALshukri et al., 2019). La interconexión de múltiples dispositivos en un hogar también puede representar un riesgo, ya que un dispositivo comprometido podría amenazar toda la red doméstica.

Entre los ataques más conocidos a dispositivos IoT en hogares se encuentran el hackeo de cámaras de seguridad, que permite a intrusos acceder a imágenes grabadas o en vivo para obtener información de los residentes. También, se han registrado ataques de denegación de servicio (DDoS), dirigidos a saturar dispositivos conectados a la red, como routers y cámaras IP, dejando los hogares sin seguridad. Además, está el robo de información personal, donde los atacantes pueden filtrar datos comprometedores de los residentes para utilizarlos en extorsiones, chantajes o beneficio personal. Muchos usuarios adquieren dispositivos IoT sin recibir capacitación adecuada sobre cómo configurar correctamente sus productos, lo que facilita los problemas antes mencionados. Esto a menudo lleva a la necesidad de ayuda externa, lo que también favorece a los atacantes. Además, el costo de mantenimiento, ya sea a nivel de hardware o software, frena las mejoras en ciberseguridad debido a la necesidad de actualizar los parches de seguridad.

Por consiguiente, surge la necesidad imperante de investigar el nivel de desconocimiento que prevalece entre los usuarios domésticos en relación con el uso de dispositivos IoT y su configuración segura. ¿Cuáles son las principales vulnerabilidades y riesgos de seguridad con la implementación de dispositivos IoT en el uso doméstico?

En este estudio se plantean varias preguntas clave para abordar la problemática de la ciberseguridad en dispositivos IoT de uso doméstico que se presentan seguidamente:

- ¿Cuáles son las vulnerabilidades de seguridad más comunes en dispositivos IoT en el uso doméstico y cómo se pueden mitigar?
- ¿Cuáles son los beneficios y limitaciones de implementar IoT en hogares domésticos?
- ¿Cuál es el impacto de las técnicas de anonimización y pseudonimización en la protección de datos personales en el contexto de la ciberseguridad en dispositivos IoT en hogares?
- ¿Cómo afecta la falta de interoperabilidad entre diferentes dispositivos IoT la seguridad general del ecosistema doméstico y qué soluciones existen para mejorar esta interoperabilidad?

Materiales y métodos

El Internet de las Cosas (IoT, por sus siglas en inglés) se refiere a una red de dispositivos físicos que están conectados entre sí y a internet, permitiendo la recopilación, el intercambio y el análisis de datos en tiempo real. Asimismo, estos dispositivos pueden incluir desde electrodomésticos y automóviles hasta sensores industriales y sistemas de seguridad, equipados con software, sensores y otras tecnologías que les permiten interactuar y comunicarse con otros dispositivos y sistemas a través de internet (Hat, 2019).

Además, el IoT tiene como objetivo principal mejorar la eficiencia, la productividad y la calidad de vida mediante la automatización y el control remoto de tareas, así como la provisión de datos valiosos que pueden ser utilizados para tomar decisiones informadas. De esta manera, la interconexión de estos dispositivos facilita la creación de entornos inteligentes, como hogares, ciudades y fábricas, donde los sistemas pueden responder

automáticamente a diversas situaciones, optimizando recursos y mejorando la seguridad y el confort de los usuarios (Hat, 2019), (Escobar Carrillo et al.).

La seguridad del IoT se refiere a las estrategias, técnicas y herramientas empleadas para proteger los dispositivos conectados a internet o redes. Dado que el término IoT abarca una amplia gama de dispositivos tecnológicos, desde relojes inteligentes y termostatos hasta consolas de videojuegos, la seguridad del IoT es extensa y multifacética. Por lo tanto, con el constante avance de la tecnología, cada vez más dispositivos tienen la capacidad de interactuar con internet o con otros dispositivos, lo que aumenta su vulnerabilidad a ciberataques (Cardenas & Hahn, 2019).

En este sentido, la seguridad del IoT implica la implementación de métodos para proteger estos dispositivos y garantizar que no sean comprometidos. La conectividad inherente a los dispositivos IoT, que permite su interacción y comunicación, también los hace más susceptibles a amenazas cibernéticas. Por ello, la seguridad del IoT abarca una variedad de metodologías diseñadas para proteger estos dispositivos.

Problemas de Seguridad y Privacidad del IoT

El IoT se ha convertido en una parte integral de la vida cotidiana, conectando dispositivos entre sí y con sistemas centralizados a través de redes. Sin embargo, esta conectividad también expone estos dispositivos a riesgos significativos de seguridad que amenazan la integridad de los datos de usuarios y organizaciones, abriendo la puerta a actores malintencionados (Alharbi et al., 2020). A pesar de los esfuerzos de la industria por contrarrestar estas amenazas mediante herramientas de seguridad específicas para IoT, aún no existen mecanismos ni acuerdos estandarizados que permitan un control centralizado y eficiente del IoT (Radanliev et al., 2019).

Exposición Remota. Los dispositivos IoT, debido a su conectividad a Internet, presentan una amplia superficie de ataque. Esta accesibilidad, aunque valiosa, permite a los hackers interactuar con los dispositivos de forma remota. Por ello prácticas como el phishing son especialmente utilizadas en este contexto, ya que explotan los múltiples puntos de entrada de estos dispositivos para comprometer su seguridad (Albataineh & Alsmadi, 2019).

Falta de Previsión de la Industria. Jiménez (Jiménez, 2022), señala varios aspectos críticos en el crecimiento y los riesgos asociados con el Internet de las Cosas (IoT):

- Crecimiento del IoT: Se proyecta que para 2025, el número de dispositivos IoT conectados crecerá un 9%, alcanzando los 27,000 millones de conexiones.
- Riesgos de seguridad: A pesar de la adopción generalizada del IoT, el 43% de las organizaciones no protegen adecuadamente sus infraestructuras, incrementando los riesgos de ciberseguridad.
- Desafíos de implementación: Las empresas enfrentan diversos desafíos, como la diversidad de dispositivos IoT, altos costos y una escasez de personal especializado en seguridad IoT.

Contraseñas Débiles, Adivinables o Codificadas. Las contraseñas débiles y predeterminadas son una puerta abierta para los piratas informáticos que buscan implementar botnets y otros tipos de malware. Por lo tanto, la gestión de contraseñas en dispositivos IoT es crítica, especialmente porque estos dispositivos no suelen tener operadores humanos para efectuar cambios regulares de contraseña (Albataineh & Alsmadi, 2019).

Servicios de Red Inseguros**.** Una de las primeras áreas de ataque en dispositivos IoT es encontrar debilidades en el modelo de comunicación de la red y en los servicios de red ejecutados en el dispositivo. Por consiguiente, Los atacantes explotan estas vulnerabilidades para capturar credenciales de inicio de sesión y otros

identificadores, por lo que es imperativo asegurar estos puntos finales con las mejores prácticas de la industria (Albataineh & Alsmadi, 2019).

Interfaces Inseguras del Ecosistema

Para abordar las interfaces inseguras de la web, API de backend, la nube o móviles en el ecosistema IoT, es necesario implementar mecanismos robustos de autenticación y autorización. Esto incluye la protección del hardware, firmware y las comunicaciones de datos de extremo a extremo para asegurar que cada dispositivo tenga permiso para comunicarse con los servicios IoT (Min et al., 2022).

Falta de un Mecanismo de Actualización Seguro. Las actualizaciones de software y firmware no autorizadas son vectores importantes de amenaza para los dispositivos IoT. Las brechas pueden tener consecuencias físicas y legales significativas. Para mitigar estos riesgos, es esencial asegurar el acceso, verificar el origen y comprobar la integridad de las actualizaciones (Min et al., 2022).

Insuficiente Protección de la Privacidad. La protección de la privacidad en dispositivos IoT comienza con la seguridad desde el propio dispositivo, estableciendo confianza a través de la autenticación y el registro seguros. Esto garantiza que los datos confidenciales transmitidos a través de la red estén protegidos y que la integridad del dispositivo se mantenga (Min et al., 2022).

Transferencia y Almacenamiento de Datos Inseguros**.** La protección de los datos es crucial para la integridad de las aplicaciones de IoT. Los datos deben ser encriptados desde su creación hasta su consumo, requiriendo un alto nivel de versatilidad e inteligencia criptográfica más allá de lo que ofrece el cifrado tradicional. Esto asegura que tanto el origen como el contenido de los datos sean verificables y protegidos contra manipulaciones (Min et al., 2022).

La metodología de este estudio se estructuró en tres fases principales siguiendo el método PRISMA (Page et al., 2021): (i) investigación documental, (ii) lectura y registro, y (iii) producción del texto final.

Fase 1: Investigación Documental

La primera fase implicó el levantamiento de información en bases de datos académicas y motores de búsqueda especializados. Se realizó una recopilación exhaustiva de datos e información relevantes asociando documentos, unidades documentales, fuentes documentales y fichas de investigación. Las bases de datos consultadas incluyeron IEEE Xplore, Springer Link, ScienceDirect, y SciELO, y Google Scholar. El objetivo fue indagar sobre el estado actual de la ciberseguridad en dispositivos IoT de uso doméstico, permitiendo una recolección adecuada de datos para el análisis posterior.

Fase 2: Lectura y Registro

En este orden de ideas, en la segunda fase, se identificaron las temáticas y subtemáticas de los documentos seleccionados. Se elaboraron tablas y gráficos que permitieron deducir fundamentos de análisis sobre la seguridad en dispositivos IoT domésticos, así como destacar las tendencias, desafíos y vulnerabilidades más recientes en el campo. Esta fase facilitó una comprensión detallada de los avances y las áreas críticas en la ciberseguridad de IoT.

Fase 3: Producción del Texto Final

En este contexto, la fase final consistió en la redacción de los diferentes apartados que componen el presente artículo de revisión. Se organizó la información recolectada y analizada en una estructura coherente, abordando los objetivos y preguntas de investigación planteadas.

Selección de Términos de Búsqueda

La búsqueda de documentación se estableció a través de una cadena de búsqueda definida que fue utilizada en las bases de datos mencionadas: IEEE Xplore, Springer Link, ScienceDirect, y SciELO, y Google Scholar. La cadena de búsqueda se diseñó para abarcar de manera exhaustiva las áreas de interés específicas del estudio, incluyendo ciberseguridad, dispositivos IoT, automatización del hogar, privacidad de datos y revisión sistemática.

La cadena de búsqueda utilizada fue la siguiente:

- Cadena de Búsqueda en idioma inglés:

("cybersecurity" OR "data security" OR "network security") AND ("IoT devices" OR "Internet of Things" OR "smart home devices") AND ("home automation" OR "smart home") AND ("data privacy" OR "privacy protection" OR "data anonymization" OR "data pseudonymization") AND ("systematic review" OR "literature review")

- Cadena de Búsqueda en idioma español:

("ciberseguridad" OR "seguridad de datos" OR "seguridad de redes") AND ("dispositivos IoT" OR "Internet de las Cosas" OR "dispositivos inteligentes para el hogar") AND ("automatización del hogar" OR "hogar inteligente") AND ("privacidad de datos" OR "protección de privacidad" OR "anonimización de datos" OR "pseudonimización de datos") AND ("revisión sistemática" OR "revisión de literatura")

Seguiamente, estas cadenas de búsqueda se aplicarón para obtener una cobertura amplia y relevante de documentos académicos y estudios que aborden los temas cruciales del artículo. Las combinaciones de términos en inglés y español permitirán una búsqueda exhaustiva, asegurando que se capturen las publicaciones más pertinentes y actualizadas en el campo de estudio.

Finalmente, una vez aplicadas estas cadenas de búsqueda en las bases de datos seleccionadas, se procederá con la evaluación y filtrado de los resultados obtenidos según los criterios establecidos previamente.

Criterios de Selección de Documentos en Bases de Datos

Cabe destacar que, los términos clave se agruparon mediante un algoritmo de búsqueda basado en la configuración de las bases de datos. Las bibliotecas digitales consultadas incluyeron IEEE Xplore, Springer Link, ScienceDirect y SciELO. El único motor de búsqueda utilizado fue Google Scholar.

Asimismo, se consideraron las combinaciones de palabras en inglés y español, traduciendo términos relevantes según fuera necesario. Por ello, las combinaciones de términos permitieron obtener un conjunto amplio de documentos y se seleccionaron artículos bajo los siguientes criterios:

Criterios de inclusión:

- Período de publicación: Artículos publicados entre los años 2019 y 2024.
- Relevancia temática: Documentos pertenecientes a revistas, conferencias, publicaciones y/o libros en áreas como ingeniería de sistemas, electrónica, ciberseguridad y ciencias de la computación.
- Idioma: Artículos disponibles en inglés y español.
- Acceso completo: Documentos con acceso completo al texto para una revisión detallada.
- Calidad y rigor: Publicaciones revisadas por pares y con una sólida base metodológica y teórica.

Criterios de exclusión:

- Publicaciones previas a 2019: Documentos publicados antes del año 2019.
- Falta de relevancia: Artículos que no se centran en la ciberseguridad de dispositivos IoT, la implementación de IoT en hogares o la privacidad de datos en el contexto de IoT.

- Acceso restringido: Documentos con acceso restringido que no permiten una revisión completa del texto.
- Calidad inadecuada: Publicaciones sin revisión por pares o con metodologías deficientes.

En una búsqueda más restringida, se aplicaron criterios de inclusión y exclusión basados en las siguientes preguntas:

- Relevancia de la información: ¿El documento presenta información relevante sobre la seguridad en dispositivos IoT y/o datos fundamentales sobre ciberseguridad en el contexto doméstico?
- Distinción de tecnologías y herramientas: ¿El documento distingue tecnologías IoT, identifica herramientas de seguridad o evidencia prácticas recomendadas para mejorar la seguridad en el hogar?

Estas combinaciones de términos clave y criterios de selección permitieron obtener un conjunto amplio y relevante de documentos para el análisis y revisión del estado del arte en la seguridad de dispositivos IoT y su implementación en el entorno doméstico.

Seguidamente, se presenta de forma gráfica el proceso de revisión y selección de los artículos para el presente estudio realizado apegado al siguiente esquema de la
Figura **1**.

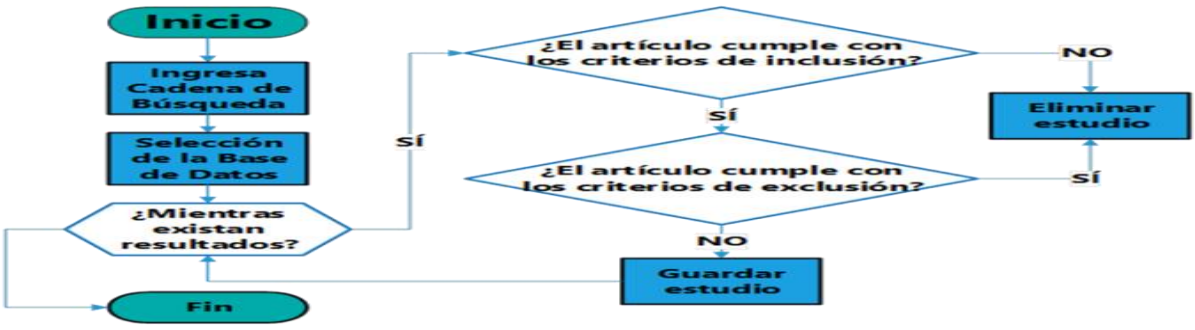


Figura 1. Proceso de selección de artículos.

Resultados y discusión

Resultados de Búsqueda

Para abordar las preguntas de investigación planteadas, se realizó una búsqueda exhaustiva en diversas bases de datos académicas utilizando términos clave relacionados con la ciberseguridad en dispositivos IoT, la interoperabilidad, la anonimización y pseudonimización, y la implementación de IoT en hogares domésticos. A partir de esta búsqueda inicial, se revisaron los títulos, palabras clave y resúmenes de los artículos encontrados para evaluar su relevancia con respecto al estudio.

Luego, se seleccionaron 20 documentos que se consideraron más pertinentes para el análisis detallado. Estos documentos proporcionan una base sólida de conocimiento sobre las vulnerabilidades de seguridad más comunes en dispositivos IoT, los beneficios y limitaciones de su implementación en entornos domésticos, y las técnicas para mejorar la interoperabilidad y proteger los datos personales. La Figuras 1 presentan un resumen detallado de los resultados de la búsqueda, incluyendo el título del artículo, el año de publicación y

la referencia, facilitando así una visión general de las fuentes seleccionadas y su contribución al marco de investigación.

Tabla 1. Formato extracción de documentos de estudios existentes.

Artículo	Título	Año
A1	Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations	2020
A2	Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review	2021
A3	Vulnerability in the security of the internet of things	2021
A4	Investigating the effect of security and privacy on IoT device purchase behaviour	2020
A5	A survey on IoT platforms: Communication, security, and privacy perspectives	2020
A6	The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws	2020
A7	Study of security issues and solutions in Internet of Things (IOT)	2020
A8	Future developments in standardisation of cyber risk in the Internet of Things (IoT)	2020
A9	IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process	2020
A10	Static analysis for discovering IoT vulnerabilities	2020
A11	Assessment of security threats on IoT based applications	2020
A12	Cyber Risk in Internet of Things World	2020
A13	IoT: What is, Concern, and How to Secure? A Systematic Literature Review	2022
A14	A survey on boosting IoT security and privacy through blockchain	2020
A15	A Systematic Literature Review of Privacy, Security, and Challenges on Applying IoT to Create Smart Home	2022
A16	Recent Privacy and Security Issues in Internet of Things Network Layer: A Systematic Review	2022
A17	A survey of the smart city data security and privacy-preserving approaches in the Internet of Things	2024
A18	A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment	2019
A19	A survey on Security and Privacy Challenges in Smarthome based IoT	2021
A20	Internet of Things (IoT) of Smart Homes: Privacy and Security	2024

Se presenta en la Figura 2 el año de la publicación de los artículos seleccionados para el presente estudio. Esta figura permite visualizar la distribución temporal de las investigaciones sobre la situación actual de los dispositivos IoT de uso doméstico. A continuación, se detalla la cantidad de artículos publicados por año.

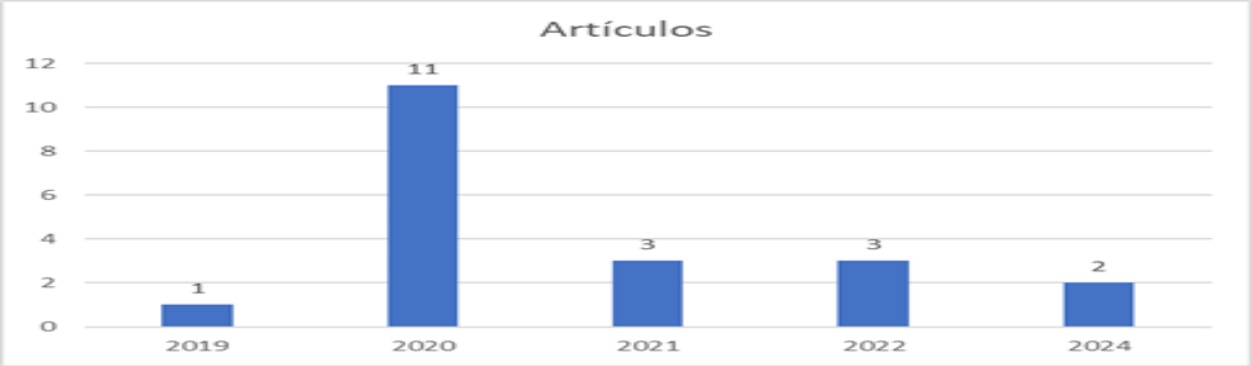
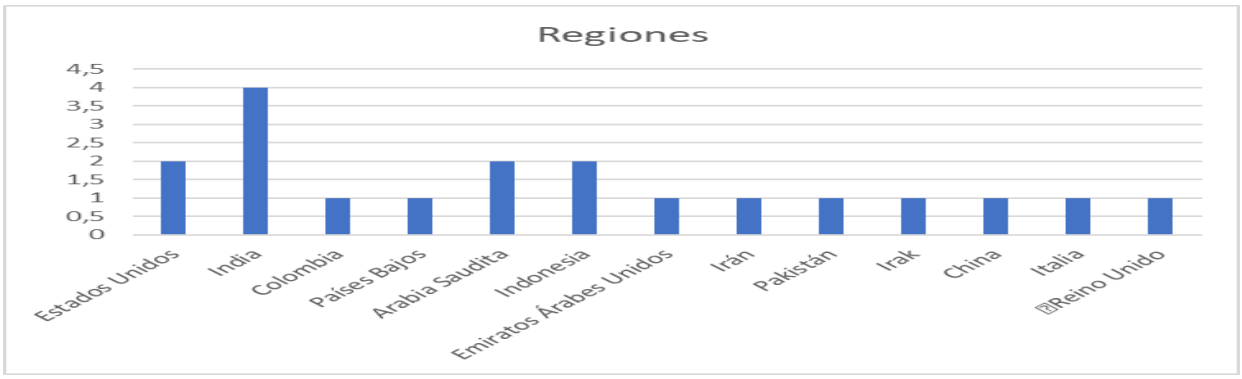


Figura 2. Año de Publicación de los Artículos.

Seguidamente, se muestra en la
Figura **3** la distribución geográfica de los artículos seleccionados para el presente estudio. Esta ilustra las regiones de origen de las investigaciones sobre la situación actual de los dispositivos IoT de uso doméstico. La diversidad geográfica de las publicaciones refleja el interés global y los diferentes enfoques que se están adoptando en torno a la seguridad y la interoperabilidad de los dispositivos IoT. Para ello, en la figura se detalla la cantidad de artículos publicados por región, destacando cómo distintas áreas del mundo están



contribuyendo al cuerpo de conocimiento en esta área.

Figura 3. Regiones de los Artículos consultados.

Esta distribución geográfica evidencia la diversidad y el alcance global de la investigación en el campo de la situación actual de los dispositivos IoT de uso doméstico. La predominancia de ciertos países puede estar relacionada con su capacidad tecnológica, el desarrollo del IoT en sus regiones, y el enfoque en la protección de datos personales. Esta variedad geográfica es esencial para entender cómo diferentes contextos y regulaciones pueden influir en las estrategias utilizadas.

Para evaluar la situación actual de los dispositivos IoT de uso doméstico, se ha analizado la presencia de términos relevantes en los artículos seleccionados. La Figura 4 presenta el porcentaje de artículos que incluyen y no incluyen ciertos términos clave en sus discusiones sobre ciberseguridad y protección de datos en el contexto de IoT doméstico.

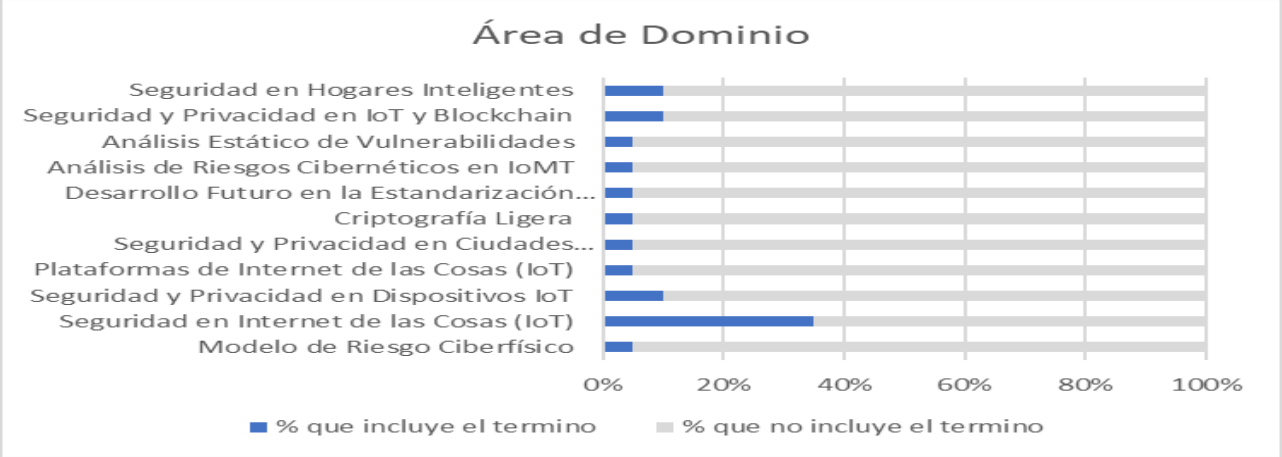


Figura 4. Área de domino.

La Figura 5 proporciona un análisis detallado de las temáticas abordadas en los artículos seleccionados, enfocándose en la situación actual de los dispositivos IoT de uso doméstico. Además, presenta el porcentaje de artículos que incluyen y no incluyen ciertos términos clave relacionados con la ciberseguridad y protección de datos en el contexto de IoT doméstico.

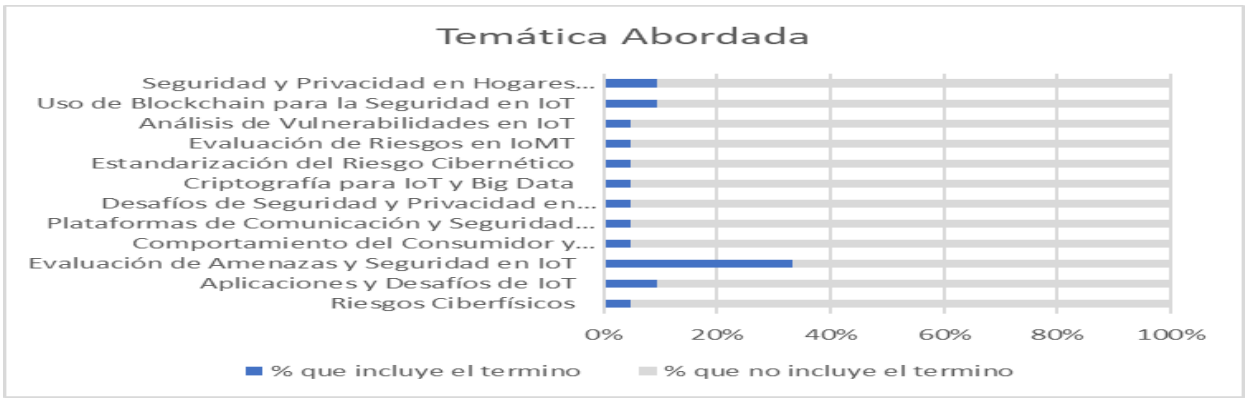


Figura 5. Temática abordada.

Presentación de Resultados sobre Pregunta Científica 1

La creciente adopción de dispositivos IoT en el ámbito doméstico ha traído consigo numerosos beneficios, como la automatización de tareas y una mayor conectividad. Sin embargo, ha introducido nuevas vulnerabilidades de seguridad que pueden ser explotadas por atacantes, poniendo en riesgo la privacidad y la integridad de los usuarios. Por lo tanto, identificar estas vulnerabilidades y desarrollar estrategias efectivas para mitigarlas es crucial para asegurar la seguridad de los hogares conectados.

La primera pregunta científica de la investigación se centra en:

¿Cuáles son las vulnerabilidades de seguridad más comunes en dispositivos IoT en el uso doméstico y cómo se pueden mitigar?

Para responder a esta pregunta, se realizó una revisión sistemática de la literatura utilizando la metodología PRISMA, analizando un total de 20 artículos académicos. A continuación, se presentan los resultados de esta revisión, organizados en dos tablas que detallan las vulnerabilidades comunes y las medidas de mitigación recomendadas. Esta presentación de resultados es seguida por una discusión que sintetiza los hallazgos de los autores y proporciona un marco comprensivo para abordar las vulnerabilidades de seguridad en dispositivos IoT de uso doméstico.

Tabla 2. Vulnerabilidades de Seguridad Comunes en Dispositivos IoT de Uso Doméstico.

Tipo de Vulnerabilidad	Detalles	Artículos
Contraseñas débiles	Contraseñas predeterminadas y fáciles de adivinar.	(Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021), (Magara & Zhou, 2024)
Falta de actualizaciones de software	Dispositivos que no reciben actualizaciones regulares.	(Ho-Sam-Sooi et al., 2021), (Radanliev et al., 2020)(Rekha et al., 2023), (Alfandi et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Comunicación no cifrada	Transmisión de datos sin cifrado.	(Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Vulnerabilidades en el firmware	Firmware inseguro o con vulnerabilidades conocidas.	(Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021)
Exceso de privilegios en dispositivos	Dispositivos que recopilan y envían datos sin restricciones.	(Babun et al., 2021)
Reconocimiento y detección de dispositivos	Atacantes que descubren debilidades en dispositivos IoT.	(Babun et al., 2021)
Falta de seguridad física	Dispositivos físicamente accesibles pueden ser comprometidos.	(Kandasamy et al., 2020)
Falta de control de acceso	Acceso no autorizado debido a una gestión deficiente de permisos.	(Rekha et al., 2023), (Alharbi et al., 2020), (Utomo et al., 2022) (Utomo et al., 2022)
Ataques de inyección de código	Vulnerabilidades que permiten inyección de código malicioso.	(Anand & Sharma, 2020), (Alharbi et al., 2020)
Privacidad comprometida	Violación de privacidad y fuga de información.	(Ferrara et al., 2021), (Alharbi et al., 2020), (Estella et al., 2022)
Autenticación débil	Métodos de autenticación fáciles de romper.	(Alharbi et al., 2020), (Estella et al., 2022), (Utomo et al., 2022)
Ataques a nivel de redes	Identifica vulnerabilidades como conexiones de red no confiables, heterogeneidad de redes y ataques de inundación	(Alam et al., 2022)

Tabla 3. Medidas de mitigación para las vulnerabilidades de seguridad en dispositivos IoT de uso doméstico.

Tipo de Medida de Mitigación	Detalles	Artículos
Contraseñas fuertes y únicas	Implementar contraseñas seguras y evitar las predeterminadas.	(Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Actualizaciones regulares de software	Asegurar actualizaciones periódicas y parches de seguridad.	(Ho-Sam-Sooi et al., 2021), (Rekha et al., 2023), (Rekha et al., 2023), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Cifrado de datos	Implementar protocolos de cifrado para proteger la transmisión de datos.	(Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Seguridad en el firmware	Implementar validación y mecanismos seguros de actualización del firmware.	(Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021)
Control de acceso mínimo	Implementar controles de acceso granular y estrictos.	(Babun et al., 2021), (Alharbi et al., 2020), (Utomo et al., 2022)
Parchado y escaneo de vulnerabilidades	Realizar escaneos periódicos de vulnerabilidades y aplicar parches.	(Babun et al., 2021)
Seguridad física	Implementar medidas de seguridad física para proteger los dispositivos.	(Kandasamy et al., 2020)
Autenticación fuerte	Implementar métodos de autenticación robustos como la autenticación de dos factores.	(Alharbi et al., 2020), (Estella et al., 2022), (Utomo et al., 2022)
Uso de algoritmos criptográficos ligeros	Implementar algoritmos de cifrado que sean adecuados para dispositivos IoT con recursos limitados.	(Estella et al., 2022), (Mehmood et al., 2019) (Mehmood et al., 2019)
Prevención de ataques	Implementar sistemas de prevención de intrusiones y manejo de ataques.	(Utomo et al., 2022)

Discusión de las Vulnerabilidades

La revisión de la literatura revela una serie de vulnerabilidades críticas en los dispositivos IoT de uso doméstico. (Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021), (Magara & Zhou, 2024) destacan el problema de las contraseñas débiles, señalando que el uso de contraseñas predeterminadas y fáciles de adivinar permite a los atacantes acceder fácilmente a los dispositivos. Además, (Ho-Sam-Sooi et al., 2021), (Rekha et al., 2023), (Rekha et al., 2023), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024) mencionan la falta de actualizaciones de software, lo que deja a los dispositivos expuestos a nuevas vulnerabilidades que surgen con el tiempo. Igualmente, se destaca que la comunicación no cifrada es otro problema crítico identificado por (Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) ,

(Magara & Zhou, 2024), ya que los datos transmitidos sin cifrado pueden ser interceptados, comprometiendo la privacidad y seguridad de la información.

Asimismo, (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Alfandi et al., 2021), (Ahmed & Zeebaree, 2021) discuten sobre el tema de las vulnerabilidades en el firmware, que pueden ser explotadas por atacantes si no se aplican parches de seguridad de manera regular. Por ello, (Babun et al., 2021) destaca la falta de control de acceso, donde los dispositivos recopilan y envían datos sin restricciones, y la detección de dispositivos, que permite a los atacantes identificar y explotar debilidades específicas de los dispositivos IoT.

Por otra parte, la seguridad física es otro aspecto crítico (Kandasamy et al., 2020), ya que los dispositivos físicamente accesibles pueden ser comprometidos. Por lo tanto, (Alharbi et al., 2020), (Utomo et al., 2022) enfatizan la importancia de un control de ingreso adecuado para prevenir accesos no autorizados. Además, (Anand & Sharma, 2020), (Alharbi et al., 2020) los ataques de inyección de código, donde los atacantes introducen código malicioso en el dispositivo aprovechando vulnerabilidades en el software puede permitir a los atacantes tomar el control del dispositivo, robar información sensible, o utilizar el dispositivo comprometido para lanzar otros ataques dentro de la red doméstica.

Finalmente, (Ferrara et al., 2021), (Alharbi et al., 2020), (Estella et al., 2022) abordan las violaciones de privacidad, donde la información personal de los usuarios puede ser expuesta debido a la falta de medidas de seguridad adecuadas. Estos problemas incluyen la recopilación y almacenamiento de datos sin el conocimiento del usuario, así como la posibilidad de que terceros accedan a datos sensibles sin autorización. Esto subraya la necesidad de implementar protocolos estrictos de protección de datos y políticas de privacidad claras para garantizar que la información de los usuarios esté segura y solo sea accesible para las partes autorizadas.

Discusión de las Medidas de Mitigación

Para mitigar estas vulnerabilidades, los autores proponen diversas medidas. (Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021), (Magara & Zhou, 2024) recomiendan el uso de contraseñas fuertes y únicas para cada dispositivo, evitando el uso de contraseñas predeterminadas. Además, es muy importancia realizar las actualizaciones regulares de software(Ho-Sam-Sooi et al., 2021), (Rekha et al., 2023), (Rekha et al., 2023), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024), ya que es necesario mantener los dispositivos actualizados para protegerlos contra nuevas amenazas.

Asimismo, (Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024) destacan la importancia del cifrado de datos como una medida esencial para proteger la transmisión de información, sugiriendo la implementación de mecanismos seguros de actualización y validación del firmware (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Alfandi et al., 2021) , (Ahmed & Zeebaree, 2021) . Por ello, estas medidas ayudan a prevenir la explotación de vulnerabilidades conocidas y aseguran que el software del dispositivo esté siempre protegido contra las últimas amenazas.

Adicionalmente, (Babun et al., 2021), (Alharbi et al., 2020), (Utomo et al., 2022) los autores consultados abogan por un control de acceso mínimo, limitando los permisos y accesos a lo estrictamente necesario. Además, (Babun et al., 2021) sugieren realizar escaneos periódicos de vulnerabilidades y aplicar parches para

proteger los dispositivos. (Kandasamy et al., 2020) enfatizan la necesidad de medidas de seguridad física para proteger los dispositivos contra accesos no autorizados.

Al mismo tiempo, para mejorar la autenticación, (Alharbi et al., 2020), (Estella et al., 2022), (Utomo et al., 2022) recomiendan la implementación de métodos robustos como la autenticación de dos factores. Igualmente, (Estella et al., 2022), (Mehmood et al., 2019) sugieren el uso de algoritmos criptográficos ligeros adecuados para dispositivos IoT con recursos limitados. Finalmente, (Utomo et al., 2022) destacan la importancia de sistemas de prevención de intrusiones y manejo de ataques para proteger los dispositivos IoT de uso doméstico.

Basado en los hallazgos encontrados en los artículos consultados, la

Tabla **4** resume las vulnerabilidades comunes y las medidas de mitigación recomendadas para dispositivos IoT de uso doméstico. Esta tabla proporciona una visión integral de las vulnerabilidades críticas identificadas, junto con las estrategias efectivas propuestas por los investigadores para mitigar estos riesgos. Organizada por tipo de vulnerabilidad y correspondiente medida de mitigación, esta herramienta facilita la comprensión y la implementación de prácticas de seguridad robustas en entornos domésticos conectados.

Tabla 4. Vulnerabilidades comunes y medidas de mitigación.

Vulnerabilidad	Medida de Mitigación
Contraseñas débiles	Uso de contraseñas fuertes y únicas
	Cambiar las contraseñas predeterminadas
Falta de actualizaciones	Implementar actualizaciones automáticas y regulares de software
	Garantizar que los dispositivos reciban parches de seguridad
Comunicación no cifrada	Usar protocolos de cifrado fuerte (como TLS) para todas las comunicaciones de datos
	Asegurar que los datos transmitidos y almacenados estén encriptados
Vulnerabilidades en firmware	Implementar mecanismos seguros de actualización de firmware
	Realizar auditorías de seguridad regulares del firmware
Falta de control de acceso	Implementar controles de acceso estrictos y autenticación de múltiples factores
	Asegurar que los dispositivos solo recopilen y envíen datos autorizados
Seguridad física deficiente	Fortalecer la seguridad física de los dispositivos IoT
	Proteger los dispositivos contra accesos físicos no autorizados
Violaciones de privacidad	Implementar fuertes medidas de protección de la privacidad
	Usar tecnologías como blockchain para mejorar la privacidad y seguridad
Ataques de inyección de código	Utilizar prácticas de programación seguras para prevenir la inyección de código malicioso
	Implementar validación y sanitización de datos de entrada

Presentación de Resultados sobre Pregunta Científica 2

La investigación sobre la ciberseguridad en los IoT en hogares ha revelado una amplia gama de beneficios potenciales y desafíos significativos. Por ello, este segmento del estudio se centra en la recopilación y análisis de datos provenientes de la revisión sistemática de la literatura, que examina críticamente los beneficios y limitaciones asociados con la integración de estos dispositivos.

La segunda pregunta científica de la investigación se centra en ¿Cuáles son los beneficios y limitaciones de implementar IoT en hogares domésticos?

Seguidamente, la

Tabla 5 presenta una síntesis detallada de los beneficios derivados de la implementación de IoT en hogares, basada en los hallazgos de diversos estudios revisados. Estos beneficios incluyen la automatización de tareas rutinarias, la mejora en la eficiencia energética mediante el control inteligente de dispositivos, y la comodidad proporcionada por la gestión remota de sistemas domésticos. Además, se destaca cómo los dispositivos IoT pueden contribuir significativamente a la seguridad del hogar mediante sistemas avanzados de vigilancia y alerta. Este análisis facilita una comprensión clara de cómo las tecnologías emergentes pueden transformar y optimizar el entorno doméstico, mejorando la calidad de vida de los usuarios al mismo tiempo que promueven prácticas sostenibles y eficientes.

Tabla 5. Beneficios de implementar IoT en hogares domésticos**.**

Beneficios	Autores Citados
Automatización de tareas	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Monitoreo remoto de dispositivos	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021)
Eficiencia energética	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Comodidad en la gestión del hogar	(Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Mejora en la seguridad del hogar	(Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Salud y bienestar	(Karale, 2021), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021)
Interoperabilidad entre dispositivos de diferentes fabricantes	(Babun et al., 2021), (Rekha et al., 2023)

Tabla 6. Limitaciones de implementar IoT en hogares domésticos.

Limitaciones	Autores Citados
Vulnerabilidades de seguridad	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Preocupaciones sobre privacidad de datos personales	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Costos iniciales y mantenimiento	(Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Dependencia de la conectividad a Internet	(Mishra & Pandya, 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021)
Problemas de interoperabilidad entre dispositivos de diferentes fabricantes	(Mishra & Pandya, 2021), (Babun et al., 2021), (Rekha et al., 2023), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021)
Riesgo de ciberataques	(Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021) [24], (Babun et al., 2021), (Rekha et al., 2023), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)

Discusión sobre los Beneficios y Limitaciones de Implementar IoT en Hogares Domésticos

La integración de IoT de uso domésticos presenta una serie de beneficios significativos, según lo revelado por diversos estudios. Entre los beneficios más destacados se encuentran la automatización de tareas cotidianas, facilitando la regulación de la temperatura, iluminación y seguridad del hogar de manera remota y eficiente (Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Asimismo, esta automatización no solo mejora la comodidad del usuario, sino que también contribuye a la eficiencia energética al optimizar el uso de recursos y reducir el consumo energético (Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Además, los sistemas de seguridad inteligentes, como cámaras y sensores conectados, proporcionan un monitoreo continuo del hogar, ofreciendo una mayor tranquilidad y protección contra intrusos (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). También se ha observado que IoT puede promover la salud y el bienestar mediante dispositivos que monitorean datos vitales y hábitos de vida (Karale, 2021), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021).

Por otro lado, la implementación de IoT de uso domésticos enfrenta varias limitaciones importantes que deben abordarse para maximizar sus beneficios. Entre las limitaciones más destacadas se encuentran las vulnerabilidades de seguridad, ampliamente mencionadas en los estudios revisados, que pueden exponer los dispositivos y datos personales a riesgos significativos de ciberataques (Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Estas vulnerabilidades subrayan la importancia de políticas de seguridad robustas y la adopción de estándares de encriptación efectivos para proteger la privacidad de los usuarios (Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024).

Además, la preocupación por la privacidad de los datos personales surge como otra limitación crucial, dado el potencial de recopilación y uso indebido de información sensible por parte de terceros (Cardenas et al., 2020), (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Adicionalmente, la dependencia de una conectividad a Internet estable y la interoperabilidad entre dispositivos de diferentes fabricantes también se identifican como desafíos significativos (Mishra & Pandya, 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , ya que la falta de estándares comunes puede dificultar la integración y funcionalidad fluida de los sistemas IoT en el hogar.

Al mismo tiempo, los costos iniciales y continuos de implementación y mantenimiento de dispositivos IoT son un factor a considerar, ya que pueden representar una barrera para la adopción masiva, especialmente para los consumidores con recursos limitados (Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Utomo et al., 2022), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Estos costos incluyen la compra de dispositivos y servicios relacionados, así como posibles tarifas de suscripción para garantizar actualizaciones y soporte continuo.

En síntesis, la implementación de IoT de uso doméstico ofrece beneficios significativos en términos de automatización, eficiencia energética, seguridad y comodidad. Sin embargo, estas ventajas deben equilibrarse con las considerables preocupaciones sobre seguridad, privacidad, interoperabilidad y costos asociados. Por ello, abordar estas limitaciones requiere un enfoque integral que combine políticas regulatorias efectivas, estándares de seguridad robustos y soluciones tecnológicas innovadoras para garantizar una experiencia IoT segura y satisfactoria para los usuarios finales.

Presentación de Resultados sobre Pregunta Científica 3

La pregunta científica 3 aborda el impacto de las técnicas de anonimización y pseudonimización en la protección de datos personales en el contexto de la ciberseguridad en dispositivos IoT en hogares. Con la proliferación de dispositivos IoT en el entorno doméstico, la protección de datos personales ha adquirido una importancia crítica. Por ello, las técnicas de anonimización y pseudonimización son estrategias clave para minimizar el riesgo de exposición de datos sensibles y cumplir con las regulaciones de privacidad. En esta sección, se presentan los resultados obtenidos de la revisión sistemática de la literatura, utilizando la metodología PRISMA, para evaluar la efectividad y las limitaciones de estas técnicas. Además, se discutirán las implicaciones de estos hallazgos en el contexto de la ciberseguridad doméstica, apoyados en estudios recientes de diversos autores.

La tercera pregunta científica de la investigación se centra en ¿Cuál es el impacto de las técnicas de anonimización y pseudonimización en la protección de datos personales en el contexto de la ciberseguridad en dispositivos IoT en hogares?

Tabla 7. Técnicas de anonimización y pseudonimización.

Técnica	Resumen	Artículos
Anonimización y pseudonimización	Analiza cómo la anonimización y pseudonimización ocultan la identidad y minimizan la exposición de datos en IoT domésticos. Utiliza un enfoque basado en simulaciones para evaluar la efectividad de estas técnicas.	(Cardenas et al., 2020)
Anonimización y pseudonimización	Describe la importancia de estas técnicas para proteger la privacidad en hogares con IoT, utilizando un estudio de caso para demostrar su implementación y resultados.	(Mishra & Pandya, 2021)
Anonimización y pseudonimización	Analiza el impacto positivo y las limitaciones de estas técnicas en la protección de datos personales en IoT, basado en un análisis de brechas de seguridad y estudios de casos reales.	(Magara & Zhou, 2024)
Anonimización y pseudonimización	Examina el impacto de estas técnicas en la protección de datos en dispositivos IoT, utilizando un análisis comparativo de estudios previos.	(Ho-Sam-Sooi et al., 2021)
Anonimización y pseudonimización	Enfatiza la necesidad de implementar correctamente estas técnicas para cumplir con normativas como el GDPR, basado en una revisión de literatura y análisis normativo.	(Karale, 2021)
Anonimización y pseudonimización	Examina cómo estas técnicas ayudan a preservar la privacidad y cumplir con regulaciones de protección de datos, utilizando un enfoque descriptivo y normativo.	(Kandasamy et al., 2020)
Anonimización y pseudonimización	Proporciona una visión sobre cómo estas técnicas pueden cifrar información y evitar divulgaciones, basado en estudios de caso y experimentos controlados.	(Ferrara et al., 2021)
Anonimización y pseudonimización	Discute los beneficios y limitaciones de estas técnicas, incluyendo su impacto en la privacidad y cumplimiento normativo, utilizando un enfoque teórico y práctico.	(Ahmed & Zeebaree, 2021)
Protección de datos y seguridad en IoT	Discute vulnerabilidades y ataques en IoT, y menciona brevemente el uso de anonimización y pseudonimización como parte de un enfoque más amplio para proteger datos personales.	(Cárdenas Quintero et al., 2020)

Tabla 8. Beneficios de implementar técnicas de anonimización y pseudonimización.

Beneficio	Descripción	Artículos
Ocultar la identidad de los usuarios	Estas técnicas permiten que los datos personales no puedan ser directamente asociados con un individuo específico, protegiendo así la privacidad del usuario.	(Cardenas et al., 2020), (Mishra &

		Pandya, 2021), (Ho-Sam-Sooi et al., 2021)
Minimizar el riesgo de exposición de datos	Al despersonalizar los datos, se reduce el riesgo de que la información sensible sea expuesta en caso de una brecha de seguridad.	(Cardenas et al., 2020), (Karale, 2021), (Ahmed & Zeebaree, 2021)
Cumplir con regulaciones de privacidad	Implementar estas técnicas ayuda a las organizaciones a cumplir con normativas de protección de datos, como el GDPR.	(Karale, 2021), (Kandasamy et al., 2020), (Magara & Zhou, 2024)
Mejorar la seguridad en dispositivos IoT	Estas técnicas contribuyen a fortalecer la seguridad en dispositivos IoT al reducir las vulnerabilidades asociadas con la identificación de datos personales.	(Cárdenas Quintero et al., 2020), (Ferrara et al., 2021)
Reducir la utilidad de los datos para atacantes	Al anonimizar o pseudonimizar los datos, se hacen menos útiles para los atacantes, ya que no pueden ser fácilmente vinculados a individuos específicos.	(Ho-Sam-Sooi et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Salvaguardar la privacidad del usuario	Protegen la privacidad del usuario al despersonalizar los datos, lo que es esencial para mantener la confianza en el uso de dispositivos IoT en hogares.	(Mishra & Pandya, 2021), (Kandasamy et al., 2020)
Limitar la reversibilidad	Aunque estas técnicas no son infalibles, su correcta implementación puede dificultar significativamente la reidentificación de los datos anonimizados o pseudonimizados.	(Ho-Sam-Sooi et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)

Tabla 9. Limitaciones de las técnicas de anonimización y pseudonimización.

Limitación	Descripción	Artículos
Falta de interoperabilidad	Las técnicas pueden no ser compatibles entre diferentes dispositivos IoT y soluciones de seguridad.	(Cardenas et al., 2020)
Reversibilidad	Si no se implementan correctamente, las técnicas de pseudonimización pueden ser revertidas.	(Ho-Sam-Sooi et al., 2021), (Magara & Zhou, 2024)
Reducción de la utilidad de los datos	La anonimización puede reducir la precisión y utilidad de los datos para ciertos análisis.	(Magara & Zhou, 2024)

Discusión de las Técnicas de Anonimización y Pseudonimización

La implementación de técnicas de anonimización y pseudonimización en dispositivos IoT de uso doméstico presenta varios beneficios significativos para la protección de datos personales. (Cardenas et al., 2020), (Mishra & Pandya, 2021) destacan que estas técnicas son fundamentales para ocultar la identidad de los usuarios y minimizar el riesgo de exposición de información sensible. Además, la correcta implementación

de estas técnicas contribuye a cumplir con regulaciones de privacidad como el GDPR, lo que es esencial para la protección de datos en el entorno de IoT (Karale, 2021), (Kandasamy et al., 2020), (Magara & Zhou, 2024). Asimismo, (Ho-Sam-Sooi et al., 2021), (Kandasamy et al., 2020) señalan que estas técnicas mejoran la seguridad en dispositivos IoT al reducir las vulnerabilidades asociadas con la identificación de datos personales. Sin embargo, es importante destacar que aunque estas técnicas pueden reducir significativamente los riesgos, no son infalibles. Por ello, la reversibilidad de las técnicas de pseudonimización, si no se implementan adecuadamente, puede comprometer la privacidad de los datos (Ho-Sam-Sooi et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024).

Por otra parte, la anonimización y pseudonimización de datos hacen que la información sea menos útil para los atacantes, ya que los datos anonimizados no pueden ser fácilmente vinculados a individuos específicos (Ho-Sam-Sooi et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024). Por lo tanto, este aspecto es crucial para salvaguardar la privacidad del usuario, especialmente en el contexto de dispositivos IoT en hogares, donde la confianza del usuario en la seguridad de sus datos personales es fundamental para la adopción y uso continuo de estas tecnologías (Mishra & Pandya, 2021), (Kandasamy et al., 2020).

Por lo anteriormente expuesto, los hallazgos indican que las técnicas de anonimización y pseudonimización son esenciales para proteger la privacidad de los datos personales en dispositivos IoT en hogares, proporcionando una capa adicional de seguridad que ayuda a proteger la privacidad y a reducir el riesgo de exposición de datos sensibles. Sin embargo, la correcta implementación de estas técnicas es vital para asegurar su efectividad y minimizar las posibles limitaciones asociadas.

Presentación de Resultados sobre Pregunta Científica 4

La falta de interoperabilidad entre diferentes dispositivos IoT en el ámbito doméstico presenta un desafío significativo para la seguridad del ecosistema. La interoperabilidad se refiere a la capacidad de los dispositivos para comunicarse y funcionar juntos de manera efectiva. Cuando los dispositivos IoT no pueden interoperar, se generan brechas de seguridad que pueden ser explotadas por atacantes, comprometiendo la integridad y privacidad de los datos del usuario.

La cuarta pregunta científica de la investigación se centra en ¿Cómo afecta la falta de interoperabilidad entre diferentes dispositivos IoT la seguridad general del ecosistema doméstico y qué soluciones existen para mejorar esta interoperabilidad?

Para responder a esta pregunta, se realizó una revisión sistemática de la literatura utilizando la metodología PRISMA, analizando un total de 20 artículos académicos. A continuación, se presentan los resultados de esta revisión, organizados en dos tablas que detallan los efectos de la falta de interoperabilidad en la seguridad y las soluciones propuestas para mejorar esta interoperabilidad. Esta presentación de resultados es seguida por una discusión que sintetiza los hallazgos de los autores y proporciona un marco comprensivo para abordar la falta de interoperabilidad en dispositivos IoT de uso doméstico.

Efectos de la Falta de Interoperabilidad en la Seguridad

La interoperabilidad entre dispositivos IoT es fundamental para garantizar un ecosistema doméstico seguro y eficiente. Sin embargo, la falta de interoperabilidad puede tener varios efectos negativos en la seguridad del ecosistema IoT en el hogar. Estos efectos incluyen la creación de vulnerabilidades y puntos débiles, dificultades en la comunicación y coordinación entre dispositivos, implementación inconsistente de medidas de seguridad, y una gestión compleja y fragmentada del ecosistema. A continuación se detallan en la Tabla **10** estos efectos organizados según la revisión de la literatura.

Tabla 10. Efectos de la falta de interoperabilidad en la seguridad.

Efecto de la Falta de Interoperabilidad	Artículos
Dificultad en la comunicación y coordinación entre dispositivos	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Cárdenas Quintero et al., 2020), (Babun et al., 2021), (Kandasamy et al., 2020)
Creación de vulnerabilidades y puntos débiles	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Cárdenas Quintero et al., 2020), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021)
Implementación de medidas de seguridad inconsistentes	(Babun et al., 2021), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Gestión y administración compleja	(Mishra & Pandya, 2021), (Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Fragmentación del ecosistema	(Rekha et al., 2023), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Limitación en la automatización del hogar	(Mishra & Pandya, 2021)
Obstaculización de estrategias de seguridad unificadas	(Kandasamy et al., 2020)
Incremento de la complejidad y posibles puntos de vulnerabilidad	(Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021)

Discusión sobre los Efectos de la Falta de Interoperabilidad en la Seguridad

La falta de interoperabilidad entre dispositivos IoT en el entorno doméstico representa un desafío significativo para la seguridad del ecosistema. Los estudios revisados destacan varios efectos adversos que esta falta de interoperabilidad puede causar. Primero, se observa que la dificultad en la comunicación y coordinación entre dispositivos es un problema recurrente. En consecuencia, esta dificultad puede llevar a una gestión ineficaz de los dispositivos IoT, incrementando el riesgo de vulnerabilidades explotables por atacantes (Cardenas et al., 2020), (Mishra & Pandya, 2021).

Además, la diversidad de dispositivos y protocolos no interoperables puede crear puntos débiles en el sistema de seguridad general del hogar. Por ello, esta heterogeneidad de dispositivos introduce inconsistencias en las políticas de seguridad, lo cual es un punto crítico de falla que los atacantes pueden explotar. Esto se ve exacerbado por la incapacidad de aplicar medidas de seguridad uniformes a través de diferentes dispositivos y plataformas (Cárdenas Quintero et al., 2020), (Babun et al., 2021).

Otro efecto significativo es la complejidad en la gestión y actualización de múltiples dispositivos de diferentes ecosistemas (Ho-Sam-Sooi et al., 2021), (Karale, 2021). Por consiguiente, esta gestión fragmentada de la seguridad y las actualizaciones puede llevar a configuraciones incorrectas o ineficaces, aumentando así la exposición a amenazas. Asimismo, dicha fragmentación del ecosistema IoT, complica la administración centralizada y puede resultar en la implementación de múltiples sistemas de seguridad con sus propias vulnerabilidades (Rekha et al., 2023), (Ahmed & Zeebaree, 2021) .

También, otro problema lo representa la falta de interoperabilidad que puede limitar la capacidad de comunicación efectiva entre dispositivos IoT, lo que es esencial para una respuesta rápida y coordinada a las

amenazas de seguridad. Por ello, la fragmentación en la seguridad puede llevar a la implementación de medidas inconsistentes, dejando brechas que los atacantes pueden explotar (Magara & Zhou, 2024). Además, que la ausencia de interfaces estándar para la interoperabilidad puede resultar en dificultades para la integración y comunicación de datos entre dispositivos, lo que afecta negativamente la capacidad de respuesta a incidentes de seguridad (Anand & Sharma, 2020), (Alharbi et al., 2020).

En síntesis, la falta de interoperabilidad entre dispositivos IoT en el hogar puede llevar a una serie de problemas de seguridad significativos. Estos incluyen dificultades en la comunicación y coordinación, creación de vulnerabilidades debido a la diversidad de dispositivos y protocolos, complejidad en la gestión y actualización de dispositivos, y la implementación inconsistente de medidas de seguridad.

Por esta razón, abordar estos problemas requiere una estrategia integral que incluya la adopción de estándares comunes, el desarrollo de protocolos interoperables y la colaboración entre fabricantes para garantizar una compatibilidad efectiva y segura entre dispositivos.

Soluciones para Mejorar la Interoperabilidad

Para mitigar los efectos negativos de la falta de interoperabilidad entre dispositivos IoT, se han propuesto varias soluciones en la literatura. Estas soluciones buscan establecer estándares comunes, desarrollar protocolos interoperables, fomentar la colaboración entre fabricantes y utilizar plataformas centralizadas y gateways universales.

Por consiguiente, la adopción de estas soluciones puede mejorar significativamente la seguridad y eficiencia del ecosistema IoT doméstico. A continuación, se presenta en la un resume de estas soluciones planteadas y agrupadas por las estrategias principales identificadas en los estudios revisados.

Tabla 11. Soluciones para mejorar la interoperabilidad.

Soluciones para Mejorar la Interoperabilidad	Artículos
Establecimiento de estándares de comunicación comunes	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Cárdenas Quintero et al., 2020), (Ho-Sam-Sooi et al., 2021), (Babun et al., 2021), (Karale, 2021), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Implementación de protocolos de seguridad interoperables	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Cárdenas Quintero et al., 2020),(Ho-Sam-Sooi et al., 2021), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021)
Fomentar la colaboración entre fabricantes	(Cardenas et al., 2020), (Mishra & Pandya, 2021), (Cárdenas Quintero et al., 2020), (Rekha et al., 2023), (Kandasamy et al., 2020), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Plataformas de gestión centralizada	(Ho-Sam-Sooi et al., 2021), (Karale, 2021), (Ferrara et al., 2021), (Ahmed & Zeebaree, 2021) , (Magara & Zhou, 2024)
Certificación y regulación	(Ho-Sam-Sooi et al., 2021)
Especificación MUD (Manufacturer Usage Description)	(Babun et al., 2021)
Gateways universales y soluciones de puente	(Mishra & Pandya, 2021), (Rekha et al., 2023)
APIs y middleware	(Rekha et al., 2023), (Utomo et al., 2022), (Magara & Zhou, 2024)

Soluciones para Mejorar la Interoperabilidad	Artículos
APIs y middleware	(Rekha et al., 2023), (Utomo et al., 2022), (Magara & Zhou, 2024)
Uso de arquitecturas de red bien diseñadas	(Utomo et al., 2022)
Sistemas basados en la nube	(Utomo et al., 2022)

Discusión sobre las Soluciones para Mejorar la Interoperabilidad

Las soluciones para mejorar la interoperabilidad entre dispositivos IoT en el entorno doméstico son variadas y se enfocan en abordar los múltiples desafíos identificados. Una de las soluciones más recurrentes en la literatura es la adopción de estándares de comunicación comunes. Por ello, se destaca la importancia de establecer estándares abiertos que permitan la comunicación y coordinación efectiva entre dispositivos de diferentes fabricantes. Estos estándares no solo facilitarían la integración de dispositivos, sino que también mejorarían la seguridad al permitir la implementación de medidas de seguridad uniformes (Cardenas et al., 2020), (Mishra & Pandya, 2021).

La implementación de protocolos de seguridad interoperables es otra solución destacada, donde se proponen la adopción de protocolos comunes que garanticen la compatibilidad y seguridad entre dispositivos IoT (Karale, 2021), (Ahmed & Zeebaree, 2021). Por consiguiente, permitiría una mejor gestión de la seguridad y reduciría las vulnerabilidades derivadas de la diversidad de protocolos. La especificación MUD (Manufacturer Usage Description), mencionada por Babun et al. (Babun et al., 2021), es un ejemplo de un protocolo que puede ayudar a reducir el impacto de ciberataques al limitar el acceso de dispositivos comprometidos a puertos específicos, mejorando así la interoperabilidad y la seguridad general del ecosistema.

La implementación de protocolos de seguridad interoperables es otra solución destacada, donde se proponen la adopción de protocolos comunes que garanticen la compatibilidad y seguridad entre dispositivos IoT (Karale, 2021), (Ahmed & Zeebaree, 2021). Esto permitiría una mejor gestión de la seguridad y reduciría las vulnerabilidades derivadas de la diversidad de protocolos.

Asimismo, la especificación *Manufacturer Usage Description* (MUD), mencionada por Babun et al. (Babun et al., 2021), es un ejemplo de un protocolo que puede ayudar a reducir el impacto de ciberataques al limitar el acceso de dispositivos comprometidos a puertos específicos, mejorando así la interoperabilidad y la seguridad general del ecosistema. MUD permite a los fabricantes definir y publicar las políticas de red necesarias para sus dispositivos, lo que facilita la implementación de configuraciones de red seguras y controladas.

Adicionalmente, la utilización de plataformas de gestión centralizada es otra estrategia clave, donde se destacan que estas plataformas permiten una administración eficiente y centralizada de dispositivos de diferentes fabricantes, lo que facilita la integración y la implementación de políticas de seguridad coherentes (Ho-Sam-Sooi et al., 2021), (Rekha et al., 2023). Además, estas plataformas pueden actuar como intermediarios, gestionando la comunicación y seguridad entre dispositivos heterogéneos, y proporcionando una solución unificada para la administración de la seguridad en el hogar.

Conjuntamente, la colaboración entre fabricantes es esencial para desarrollar soluciones interoperables. Por ello, es necesario enfatizar sobre la necesidad de fomentar alianzas industriales y la cooperación entre diferentes actores del mercado para crear estándares y protocolos que aseguren la compatibilidad entre dispositivos (Cardenas et al., 2020), (Magara & Zhou, 2024). Por consiguiente, esta colaboración puede llevar

a la creación de un ecosistema más seguro y cohesionado, donde los dispositivos puedan comunicarse y coordinarse de manera efectiva.

Adicionalmente Karale (Karale, 2021) destaca la importancia de adoptar estándares comunes en el contexto de la seguridad de IoT para mitigar los riesgos asociados con la falta de interoperabilidad. Estos estándares, desarrollados por organizaciones internacionales como ISO/IEC, ITU y IEEE, proporcionan marcos y directrices que facilitan la comunicación y la seguridad entre dispositivos de diferentes fabricantes. A continuación, se presenta una descripción de estas organizaciones y el propósito de los estándares propuestos en el contexto de la seguridad de IoT.

ISO/IEC: La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) colaboran para desarrollar estándares internacionales que promuevan la interoperabilidad y la seguridad en diversos sectores, incluido IoT. Los estándares ISO/IEC para IoT buscan establecer directrices y marcos que permitan una comunicación segura y eficiente entre dispositivos IoT (Karale, 2021).

Para abordar las vulnerabilidades y mejorar la seguridad en el ecosistema de IoT, es fundamental seguir estándares internacionales que aseguren la interoperabilidad y protección de los datos. Los estándares desarrollados por la ISO/IEC proporcionan un marco detallado para lograr estos objetivos, facilitando la integración de dispositivos IoT de diversos fabricantes y garantizando un entorno seguro y eficiente. A continuación, se presenta la Tabla 11 con los principales estándares ISO/IEC que contribuyen a la seguridad de IoT, tal como lo describe Karale (Karale, 2021).

Tabla 11. Estándares ISO/IEC para la Seguridad de IoT

Estándar ISO/IEC	Descripción
ISO/IEC 21823-1:2019	Ofrece un resumen de la interoperabilidad aplicable a los marcos de IoT, habilitando la interoperabilidad entre marcos independientes.
ISO/IEC 23093-1:2020	Describe la arquitectura de los marcos para IoT y determina las API y la representación de datos empaquetados.
ISO/IEC 21823-2:2020	Describe interfaces de interoperabilidad de transporte para el desarrollo de marcos de IoT con intercambio de datos.
ISO/IEC TR 30164:2020	Describe conceptos básicos, terminologías, casos de uso y avances de la computación de borde para IoT.
ISO/IEC TR 30166:2020	Trata marcos de la IIoT, análisis de riesgos y posibles estandarizaciones futuras.
ISO/IEC 27030	Se ocupa de la privacidad y la seguridad de IoT, proporcionando guías sobre principios, riesgos y controles.
ISO/IEC AWI 30147	Trata los procesos del ciclo de vida del sistema que se extienden a los marcos de IoT.
ISO/IEC AWI 30149	Aborda el marco de confianza de IoT, actualmente en desarrollo.

ITU: La Unión Internacional de Telecomunicaciones (ITU) es una agencia especializada de las Naciones Unidas que se ocupa de las tecnologías de la información y la comunicación. Los estándares ITU para IoT abordan aspectos como la interoperabilidad, la terminología y los requisitos de red para asegurar un ecosistema IoT cohesionado y seguro (Karale, 2021).

Para facilitar la comprensión y aplicación de estos estándares, se presenta a continuación la

Tabla **12**, que detalla los estándares ITU más relevantes para la seguridad de IoT. Estos estándares abordan una variedad de aspectos técnicos y operativos, proporcionando un marco robusto para mejorar la seguridad y la interoperabilidad en el ecosistema IoT (Karale, 2021).

Tabla 12. Estándares ITU para la Seguridad de IoT.

Estándar ITU	Descripción
Y.4000/Y.2060	Visión general de IoT.
Y.4050/Y.2069	Términos y definiciones de IoT.
Y.4100/Y.2066	Requisitos comunes de IoT.
Y.4103/F.748.0	Requisitos comunes de las aplicaciones de IoT.
Y.4552/Y.2078	Modelos de soporte de aplicaciones de IoT.
Y.4111/Y.2076	Requisitos y marco basados en la semántica de IoT.
Y.4113	Requisitos de la red para IoT.
Y.4453	Marco de software adaptable para dispositivos IoT.
Y.4101/Y.2067	Requisitos y capacidades comunes de una pasarela para aplicaciones IoT.
Y.4112/Y.2077	Requisitos de la capacidad plug and play (PnP) de IoT.
Y.4401/Y.2068	Marco funcional y capacidades de IoT.
Y.4806	Capacidades de seguridad de IoT.

IEEE: El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) es una organización profesional dedicada al avance de la tecnología. Los estándares IEEE para IoT se centran en la creación de marcos arquitectónicos y la armonización de dispositivos y sistemas para asegurar una integración fluida y segura en el ecosistema IoT (Karale, 2021).

Para proporcionar una visión clara y detallada de los estándares propuestos por el IEEE en el ámbito de la seguridad de IoT, se presenta la

Tabla **13**. Estos estándares abarcan diversos aspectos técnicos y metodológicos, incluyendo marcos arquitectónicos y la armonización de dispositivos, con el objetivo de garantizar una integración segura y eficiente de los sistemas IoT (Karale, 2021).

Tabla 13. Estándares IEEE para la Seguridad de IoT

Estándar IEEE	Descripción
P2413	Marco arquitectónico para IoT.
P1451-99	Armonización de los dispositivos y sistemas de IoT.
P1931.1	AF para la facilitación de operaciones en tiempo real en el sitio para IoT.
P2668	Índice de madurez de IoT: evaluación, calificación y clasificación.

Estos estándares propuestos por Karale (Karale, 2021) tienen como objetivo proporcionar una base sólida para la interoperabilidad y la seguridad en el ecosistema de IoT, abordando las vulnerabilidades y limitaciones actuales y facilitando la integración y gestión segura de dispositivos IoT en el entorno doméstico.

Finalmente, la adopción de gateways universales es una solución práctica para mejorar la interoperabilidad. Kandasamy et al. (Kandasamy et al., 2020), Utomo et al. (Utomo et al., 2022) y Rekha et al. (Rekha et al., 2023) sugieren el uso de gateways que puedan traducir y mediar entre diferentes protocolos y estándares de

dispositivos IoT. Estos gateways actúan como puentes, permitiendo la comunicación entre dispositivos que de otra manera no serían compatibles, y asegurando que se puedan implementar políticas de seguridad de manera uniforme a través de todo el ecosistema.

En síntesis, mejorar la interoperabilidad entre dispositivos IoT en el hogar requiere un enfoque multifacético que incluya la adopción de estándares abiertos, la implementación de protocolos de seguridad interoperables, el uso de plataformas de gestión centralizada, la colaboración entre fabricantes y el empleo de gateways universales. Estas soluciones no solo facilitarán la integración y comunicación entre dispositivos de diferentes fabricantes, sino que también mejorarán la seguridad general del ecosistema IoT doméstico.

Trabajos Futuros

La investigación sobre la interoperabilidad y la seguridad en entornos IoT en el hogar aún tiene muchos aspectos por explorar y mejorar. A continuación, se presentan algunas áreas clave para futuros trabajos:
Desarrollo de Estándares Globales. La falta de estándares globales es un obstáculo significativo para la interoperabilidad. Por ello, futuros trabajos podrían centrarse en el desarrollo y promoción de estándares internacionales que faciliten la comunicación y coordinación entre dispositivos IoT de diferentes fabricantes y regiones. La colaboración entre organismos de normalización, fabricantes y gobiernos será crucial para el éxito de estas iniciativas.
Mejoras en Protocolos de Seguridad. Aunque se han propuesto varios protocolos de seguridad interoperables, es necesario seguir investigando y desarrollando protocolos que no solo sean seguros, sino también eficientes y escalables. Por consiguiente, la especificación MUD es un paso en la dirección correcta, pero se requiere más trabajo para mejorar y adaptar estos protocolos a las necesidades cambiantes del mercado IoT.
Evaluación y Certificación de Dispositivos. Crear un marco de evaluación y certificación para dispositivos IoT que garantice que cumplen con los estándares de interoperabilidad y seguridad podría ser un área importante de investigación. Esto no solo aumentaría la confianza de los consumidores en estos dispositivos, sino que también facilitaría su integración en redes IoT existentes.
Desarrollo de Plataformas de Gestión Avanzada. Las plataformas de gestión centralizada actuales pueden beneficiarse de mejoras significativas. Por ende, las investigaciones futuras podrían enfocarse en desarrollar plataformas más inteligentes y autónomas que utilicen técnicas de aprendizaje automático y análisis de datos para gestionar la seguridad y la interoperabilidad de manera más efectiva.
Colaboración Interdisciplinaria. La naturaleza compleja de los desafíos de interoperabilidad y seguridad en IoT requiere un enfoque interdisciplinario. En consecuencia, trabajos futuros podrían centrarse en la colaboración entre expertos en seguridad, ingenieros de redes, científicos de datos y sociólogos para abordar estos problemas desde múltiples perspectivas y desarrollar soluciones holísticas.
Impacto de la Interoperabilidad en la Usabilidad. Es esencial investigar cómo las soluciones de interoperabilidad afectan la usabilidad y la experiencia del usuario. Así pues, estudios futuros podrían centrarse en evaluar cómo las medidas de seguridad interoperables influyen en la facilidad de uso y aceptación por parte de los consumidores, y cómo se pueden diseñar interfaces de usuario más intuitivas.
Resiliencia de las Redes IoT. Investigar cómo mejorar la resiliencia de las redes IoT ante fallos y ataques es otra área crucial. Por ello, futuros trabajos podrían enfocarse en desarrollar técnicas para detectar y mitigar

rápidamente los impactos de ciberataques y fallos de interoperabilidad, asegurando así una mayor estabilidad y seguridad de las redes IoT.

Regulación y Políticas. La investigación sobre el impacto de la regulación y las políticas en la interoperabilidad y la seguridad de IoT también es fundamental. Por lo tanto, futuros trabajos pueden explorar cómo las políticas gubernamentales y las regulaciones pueden incentivar la adopción de estándares y prácticas de seguridad interoperables, y cómo se pueden equilibrar estos requisitos con la innovación y el desarrollo del mercado.

Conclusiones

Este artículo ha explorado en profundidad varios aspectos críticos del IoT en el entorno doméstico, centrándose en la seguridad, los beneficios y limitaciones, la protección de datos personales, y la interoperabilidad. A continuación, se presentan las principales conclusiones del estudio, estructuradas en función de las preguntas de investigación abordadas:

Vulnerabilidades de Seguridad en Dispositivos IoT Domésticos y Mitigación

Las vulnerabilidades de seguridad en dispositivos IoT domésticos son numerosas y variadas, incluyendo problemas como la falta de cifrado, contraseñas predeterminadas débiles, y actualizaciones de firmware irregulares.

Para mitigar estas vulnerabilidades, se recomiendan varias estrategias:

- Implementación de cifrado en los datos trasmitidos, actualización de parches de seguridad constantes e implementación de contraseñas fuertes y únicas. Adicional es importante la doble autenticación (2FA) para el acceso de los dispositivos.

Beneficios y Limitaciones de Implementar IoT en Hogares Domésticos

La implementación de IoT en hogares ofrece numerosos beneficios, tales como la conveniencia, la eficiencia energética, y la automatización mejorada. Sin embargo, presenta varias limitaciones, incluyendo preocupaciones de privacidad, costos iniciales elevados, y problemas de compatibilidad entre dispositivos de diferentes fabricantes.

Impacto de las Técnicas de Anonimización y Pseudonimización en la Protección de Datos Personales

Las técnicas de anonimización y pseudonimización son cruciales para proteger los datos personales en el contexto de la ciberseguridad en dispositivos IoT en hogares. Por lo tanto, estas técnicas ayudan a minimizar el riesgo de identificación de individuos a partir de los datos recopilados por dispositivos IoT.

Efectos de la Falta de Interoperabilidad en la Seguridad y Soluciones para Mejorarla

La falta de interoperabilidad entre dispositivos IoT es un problema significativo que afecta la seguridad general del ecosistema doméstico. Por ello, los dispositivos que no pueden comunicarse entre sí de manera efectiva pueden dejar brechas de seguridad que los atacantes pueden explotar.

Efectos de la falta de interoperabilidad:

La falta de interoperabilidad en dispositivos IoT puede tener varios efectos negativos. Los dispositivos aislados son más vulnerables a ataques específicos, lo que aumenta los riesgos de seguridad. Además, la gestión y actualización de dispositivos de diferentes fabricantes se vuelve más complicada y poco consistente. Por último, los problemas de compatibilidad pueden limitar la funcionalidad de los dispositivos, reduciendo su eficiencia y utilidad.

En síntesis, la seguridad, interoperabilidad, y protección de datos en el IoT para hogares inteligentes son aspectos interrelacionados que deben ser abordados de manera conjunta. Por consiguiente, este estudio proporciona una base sólida para futuras investigaciones y desarrollos en el campo, destacando la importancia de un enfoque colaborativo y multidisciplinario para enfrentar estos desafíos complejos. La adopción de estándares comunes, el desarrollo de protocolos de seguridad avanzados, y la implementación de soluciones de gestión centralizada son pasos cruciales para asegurar un entorno IoT seguro y eficiente.

Finalmente, la adopción de estándares internacionales como los propuestos por ISO/IEC, ITU y IEEE es crucial para mejorar la interoperabilidad y la seguridad en el ecosistema IoT, ya que estos estándares proporcionan marcos y directrices que facilitan la comunicación y la integración entre dispositivos de diferentes fabricantes, reduciendo las vulnerabilidades y fortaleciendo la seguridad general del sistema. Por lo tanto, la implementación y el seguimiento de estos estándares son esenciales para enfrentar los desafíos actuales y futuros en el ámbito de la ciberseguridad en IoT, asegurando así un entorno doméstico más seguro y confiable.

Referencias

Ahmed, S. H., & Zeebaree, S. (2021). A survey on security and privacy challenges in smarthome based IoT. *International Journal of Contemporary Architecture*, *8*(2), 489-510.

Alam, M. Z., Reegu, F., Dar, A. A., & Bhat, W. A. (2022). Recent privacy and security issues in internet of things network layer: a systematic review. 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),

Albataineh, A., & Alsmadi, I. (2019). Iot and the risk of internet exposure: Risk assessment using shodan queries. 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM),

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, *24*(1), 37-55. https://link.springer.com/article/10.1007/s10586-020-03137-8

Alharbi, H. B., Baghanim, N. A., & Munshi, A. (2020). Cyber risk in internet of things world. 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS),

ALshukri, D., Sumesh, E., & Krishnan, P. (2019). Intelligent border security intrusion detection using IoT and embedded systems. 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC),

[Record #612 is using a reference type undefined in this output style.]

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks*, *192*, 108040. https://www.sciencedirect.com/science/article/am/pii/S1389128621001444

Balanta, L. A., Horta, M. D. L., & Duarte, S. I. H. (2021). Aplicaciones IOT para el hogar–desarrollo acuario IOT. *Publicaciones e Investigación*, *15*(4). https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/download/5591/5327

Cardenas, D. J. S., & Hahn, A. (2019). IoT threats to the smart grid: a framework for analyzing emerging risks. Proceedings of the Northwest Cybersecurity Symposium,

Cardenas, D. J. S., Hahn, A., & Liu, C.-C. (2020). Assessing cyber-physical risks of IoT-based energy devices in grid operations. *IEEE Access*, *8*, 61161-61173. https://ieeexplore.ieee.org/iel7/6287639/6514899/09046835.pdf

Cárdenas Quintero, D. M., Ropero Silva, E. L., Puerto, K., Sanchez Mojica, K. Y., Ramirez Mateus, J. J., & Castro Casadiego, S. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo Fesc*, *10*(19 (2020)), 162-179. https://repositorio.ufps.edu.co/handle/ufps/940

Escobar Carrillo, M. N., Giraldo García, J. P., & Ramírez Castiblanco, O. L. Implementación de un Sistema Iot-Cloud para el Ahorro de Agua y Energía en el Hogar.

Estella, T., Ghayatrie, N. A. I., Levina, A., & Prasetyo, A. (2022). IoT: What is, Concern, and How to Secure? A Systematic Literature Review. 2022 6th International Conference on Informatics and Computational Sciences (ICICoS),

Ferrara, P., Mandal, A. K., Cortesi, A., & Spoto, F. (2021). Static analysis for discovering IoT vulnerabilities. *International Journal on Software Tools for Technology Transfer*, *23*, 71-88. https://link.springer.com/content/pdf/10.1007/s10009-020-00592-x.pdf

Girme, G. S., & Patil, S. R. (2019). Internet of Things Based Intelligent Security using Android Application. 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT),

Gutiérrez, A. F., Gordillo, A. P., & Roa, L. A. (2022). Vulnerabilidad de la información en los dispositivos domésticos inteligentes del hogar. *Elementos*, *7*(1), 8. https://documat.unirioja.es/descarga/articulo/8821184.pdf

Hat, R. (2019). ¿ Qué es el Internet de las cosas (IoT). *Red Hat. Recuperado de www. redhat. com/es/topics/internet-of-things/what-is-iot*.

Ho-Sam-Sooi, N., Pieters, W., & Kroesen, M. (2021). Investigating the effect of security and privacy on IoT device purchase behaviour. *computers & security*, *102*, 102132. https://www.sciencedirect.com/science/article/pii/S0167404820304053

Jain, S., Jatain, A., & Bhaskar, S. (2019). Smart city management system using IoT with deep learning. 2019 International Conference on Communication and Electronics Systems (ICCES),

Jiménez, M. (2022). *Los dispositivos conectados se disparan, pero el 43% de las empresas no protege bien su infraestructura IoT*. https://cincodias.elpais.com/cincodias/2022/03/01/companias/1646134417_237983.html

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*, 1-18. https://link.springer.com/content/pdf/10.1186/s13635-020-00111-0.pdf

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420. https://www.sciencedirect.com/science/article/pii/S2542660521000640

Khan, J., ping Li, J., Ali, I., Parveen, S., ahmad Khan, G., Khalil, M., Khan, A., Haq, A. U., & Shahid, M. (2018). An authentication technique based on oauth 2.0 protocol for internet of things (IoT) network. 2018 15th International computer conference on wavelet active media technology and information processing (ICCWAMTIP),

Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of Smart Homes: Privacy and Security. *Journal of Electrical and Computer Engineering*, *2024*(1), 7716956. https://onlinelibrary.wiley.com/doi/pdf/10.1155/2024/7716956

Mehmood, M. S., Shahid, M. R., Jamil, A., Ashraf, R., Mahmood, T., & Mehmood, A. (2019). A comprehensive literature review of data encryption techniques in cloud computing and IoT environment. 2019 8th International Conference on Information and Communication Technologies (ICICT),

Min, N. M., Visoottiviseth, V., Teerakanok, S., & Yamai, N. (2022). OWASP IoT top 10 based attack dataset for machine learning. 2022 24th International Conference on Advanced Communication Technology (ICACT),

Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, *9*, 59353-59377. https://ieeexplore.ieee.org/iel7/6287639/6514899/09405669.pdf

Morán, J. A. S., Burgos, L. J. M., Ganchozo, J. G. P., & Arévalo, J. C. G. (2023). El internet de las cosas. Desafíos para la participación y el aprendizaje infantil. *RECIMUNDO*, *7*(1), 336-347. https://www.recimundo.com/index.php/es/article/download/1958/2439

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista española de cardiología*, *74*(9), 790-799. https://www.sciencedirect.com/science/article/pii/S0300893221002748

Radanliev, P., De Roure, D. C., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2019). Cyber Risk in IoT Systems.

Radanliev, P., De Roure, D. C., Nurse, J. R., Mantilla Montalvo, R., Cannady, S., Santos, O., Maddox, L. T., Burnap, P., & Maple, C. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Applied Sciences*, *2*, 1-16. https://link.springer.com/content/pdf/10.1007/s42452-019-1931-0.pdf

Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, *80*, 3554-3559. https://e-tarjome.com/storage/btn_uploaded/2022-03-03/1646289393_12401-English.pdf

Revelo Vizcaino, E., & Egas Acosta, C. (2023). Implementación de un sistema para evaluar la cobertura de la red sigfox en el interior de edificaciones. *Enfoque UTE*, *14*(1), 33-45. http://scielo.senescyt.gob.ec/pdf/enfoqueute/v14n1/1390-6542-enfoqueute-14-01-00033.pdf

Soto, J. P. T., Suárez, J. d. l. S. S., Rodríguez, A. B., & Cainaba, G. O. R. (2019). Internet de las cosas aplicado a la agricultura: estado actual. *Lámpsakos*(22), 86-105. https://dialnet.unirioja.es/descarga/articulo/7210369.pdf

Utomo, I. S., Pranoto, C. M., Moniaga, J. V., & Jabar, B. A. (2022). A systematic literature review of privacy, security, and challenges on applying IoT to create smart home. 2022 International Conference on Electrical and Information Technology (IEIT),

Zermeño, F. J. F., Franco, E. G. C., & Flores, F. J. (2021). Aplicaciones, enfoques y tendencias del Internet de las Cosas (IoT): revisión sistemática de la literatura. Memorias del Congreso Internacional de Investigación Academia Journals Hidalgo 2021 (Hidalgo, México, 20 al 22 de octubre,