TRABAJO DE GRADO

Proyecto de Grado

Ciberseguridad en el Internet de las Cosas: Retos y Soluciones Emergentes

Corporación Universitaria Remington.

Facultad de ingenierías.

Nombre del programa académico.

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Rodrigo Alberto Gonzalez Gomez.

Gloria Amparo Lora Patiño.

Opción en la que realizó su trabajo de grado (Investigación o trabajo de grado).

2025.

Dedicatoria

Dedico este trabajo a las personas que han creído en mi capacidad de seguir aprendiendo y creciendo profesionalmente. En lo personal a mi familia, a ICOLTRANS S.A.S por contribuir a mi crecimiento y darme el espacio para cada uno de los aprendizajes obtenidos, a mi líder tecnológica "Ingeniero Cesar Hernando Zarate", por su apoyo incondicional y motivación constante. A mi equipo de trabajo de TIC que día a día me han aportado y trasmitido sus conocimientos, enseñanzas, capacidades de superación y la valentía de afrontar las dificultades, con su ejemplo y conocimiento, han sembrado en mí la pasión por el mundo tecnología enfocado en la ciberseguridad.

Agradecimientos

Agradezco a la Corporación Universitaria Remington, por permitirme integrarme a su gran familia académica que constantemente se preocupan por que nosotros los estudiantes sobresalgamos en nuestras metas y propósitos académicos.

También agradezco a cada uno de los profesores y tutores que hicieron parte de mi formación con su esfuerzo y dedicación constante para que así entendiéramos cada conceto de los temas vistos de tal forma que lograra apalancar y expandir mucho más los conocimientos iniciales para saberlos aplicar y profundizar más en ellos, gracias por su dedicación, exigencia y orientación.

Muchas gracias a la facultad de ingeniería por tener un gran equipo de profesores y tutores con unas capacidades de enseñar, saber guiar y estar siempre dispuesto a las necesidades del estudiante.

Tabla de Contenidos

Lista de tablas

Lista de figuras

Resumen

El Internet de las cosas (IoT) ha cambiado en años recientes la manera en que los dispositivos se comunican entre sí y ha conseguido, en un tiempo relativamente corto, lo que generaciones de inventores anhelaron con insistente obstinación: lograr que las máquinas se entiendan mejor entre ellas que los seres humanos mismos, incorporando todo tipo de sensores, software y redes para simplificar una amplia variedad de tareas en campos como el transporte, la industria, la salud y, principalmente, el hogar. Sin embargo, esta interconexión comporta nuevas amenazas a la ciberseguridad, ya que muchos dispositivos tienen una capacidad reducida para poner en marcha medidas de protección eficaces.

En el presente trabajo, nos ocuparemos de los retos más importantes en términos de seguridad que enfrenta el ecosistema IoT. Ejemplos de estos son la escasa actualización del firmware, la falta de estandarización y la debilidad de los métodos de autenticación, factores que hacen que sea sencillo para los ciberatacantes atacarlos. están desarrollando, además, soluciones novedosas que intentan disminuir estos riesgos. de ellas son: la utilización de inteligencia artificial para identificar anomalías; el enfoque Zero Trust, que nos recuerda una verdad incómoda en el mundo digital: nadie merece confianza, ni siquiera nuestros electrodomésticos; y el uso de blockchain para optimizar la trazabilidad e integridad de los datos.

Además, se incorporan estudios de casos y análisis comparativos, los cuales no son meras actividades académicas, sino reflejos que nos muestran que la seguridad del IoT es una urgencia diaria y no un lujo. Los cuales nos posibilitan el análisis de la efectividad de estas soluciones en diversos escenarios. El objetivo de este trabajo es sensibilizar acerca de la importancia crítica de

adoptar nuevas prácticas de seguridad robustas orientadas a asegurar la protección de los dispositivos del Internet de las Cosas (IoT) en el hogar. del Del mismo modo, impulsar el avance de tecnologías que sean escalables y seguras, capaces de afrontar los desafíos actuales.

Palabras clave

- Internet de las Cosas (IoT)
- Ciberseguridad
- Vulnerabilidades
- Protección de datos
- Soluciones emergentes

Introducción

En la última década, el Internet de las Cosas (IoT, por sus siglas en inglés) ha transformado la manera en que interactuamos con el mundo digital y físico. Desde dispositivos domésticos inteligentes hasta sistemas industriales automatizados, el IoT ha permitido una conectividad sin precedentes que promete eficiencia, comodidad y progreso en diversos sectores. Sin embargo, este crecimiento acelerado también ha generado serios desafíos en términos de ciberseguridad.

A medida que millones de dispositivos se integran a redes abiertas y heterogéneas, las amenazas cibernéticas se han multiplicado, afectando tanto a usuarios individuales como a infraestructuras críticas. Muchos dispositivos IoT carecen de mecanismos de seguridad robustos, lo que los convierte en blancos vulnerables para ataques que pueden comprometer la privacidad, integridad y disponibilidad de los datos.

Este trabajo de grado analiza los principales retos de ciberseguridad asociados al Internet de las Cosas, incluyendo las vulnerabilidades más comunes, las limitaciones tecnológicas y la falta de normativas estandarizadas. Asimismo, se exploran soluciones emergentes que buscan mitigar estos riesgos, como la implementación de criptografía ligera, arquitecturas seguras, inteligencia artificial aplicada a la detección de amenazas y marcos regulatorios internacionales.

El objetivo es proporcionar una visión integral del panorama actual de la ciberseguridad en el IoT, contribuyendo con recomendaciones prácticas y teóricas que fortalezcan la protección de estos sistemas en un entorno digital cada vez más interconectado y complejo.

Marco teórico o de referencia

Capítulo 1: El Internet de las Cosas (IoT) y su Contexto Actual

1.1. Definición y evolución del IoT

El Internet de las Cosas (IoT, por sus siglas en inglés) se refiere a la interconexión de objetos físicos como vehículos, aparatos electrónicos y dispositivos con internet, lo que les permite recoger, compartir y procesar información. Esta tecnología ha facilitado un cambio importante en la manera de interactuar con el medio ambiente, al automatizar procesos a nivel industrial y doméstico (Fernández & Gutiérrez, 2023). La interconexión entre sensores, conectividad y procesamiento es la base del IoT, lo cual hace posible que los dispositivos y sistemas se comuniquen de manera continua y eficaz.

Su progreso se ha caracterizado por la fabricación de redes inalámbricas más poderosas, la reducción del costo de los elementos electrónicos y el aumento en la demanda de eficiencia operacional en todos los ámbitos. Caracterizado por la fabricación de redes inalámbricas más poderosas, la reducción del costo de los elementos electrónicos y el aumento en la demanda de eficiencia operativa en todos los ámbitos.

El avance del IoT ha sido tal que hoy se encuentra presente en múltiples áreas como el hogar inteligente (*Smart home*), la industria 4.0, las ciudades inteligentes (*Smart cites*), el transporte, la agricultura de precisión y la salud digital, entre muchas otras. A medida que su adopción se ha expandido, también lo ha hecho la cantidad de datos generados y procesados por estos dispositivos, lo que plantea retos importantes en materia de almacenamiento, procesamiento y seguridad.

1.2. Crecimiento exponencial de dispositivos conectados

Recientemente, el número de dispositivos IoT ha aumentado exponencialmente. Se estimaba que en 2024 había aproximadamente 18.800 millones de dispositivos conectados a nivel global, y se pronostica que para finales de 2025 esta cifra supere los 30.000 millones (Wikipedia, 2025). Como resultado de esta tendencia, la complejidad de las redes y la superficie potencial de ataque susceptible a ser utilizado por actores maliciosos han crecido en proporción. La integración acelerada de dispositivos IoT en sistemas empresariales, infraestructuras críticas y espacios individuales ha rebasado la capacidad de muchos gobiernos y organizaciones para establecer controles de seguridad apropiados.

Un reto importante de este rápido crecimiento es que gran cantidad de dispositivos que se fabrican sin tener en cuenta sólidos principios de ciberseguridad, o bien con escasos recursos procesales. Esto limita la posibilidad de que se ponga en práctica medidas como la autenticación multifactor, el cifrado fuerte y las actualizaciones automáticas. La elevada conectividad, la escasa protección y la falta de estandarización han hecho que los ciberdelincuentes elijan al IoT como un objetivo ideal.

1.3. Limitaciones técnicas y operativas del IoT

La implementación de protocolos de seguridad avanzados se ve dificultada debido a que muchos dispositivos IoT funcionan con recursos limitados. Con frecuencia, son implementadas con configuraciones predeterminadas o sin cifrado y no cuentan con mecanismos de autenticación eficaces. En este sentido, Morales y Álvarez (sf) señalan que la mayor parte de los dispositivos IoT carecen de sistemas integrados para proteger datos y de mecanismos para actualizarlos a distancia, lo cual eleva considerablemente su vulnerabilidad frente a ataques

cibernéticos.

Según el informe semestral de SonicWall (2024), los ataques a dispositivos IoT aumentaron alarmantemente un 107 % en ese año, con una media de 52,8 horas de asalto por dispositivo. Los intentos de intrusión en América Latina sobrepasaron los 8 millones, lo que significa un incremento del 164 % en comparación con el año anterior.

Capítulo 2: Ciberseguridad en el IoT: Retos, Amenazas y Soluciones Emergentes

2.1. Impacto del cibercrimen en la era IoT

El cibercrimen ha aumentado en complejidad y frecuencia, impactando a personas individuales y a entidades de cualquier tamaño. La La cifra global aproximada de los ciberataques en 2024 fue más de 10.000 millones de euros, el doble que la del año anterior. En la primera mitad del año, en naciones como España se registraron 58 casos de ransomware, lo que representa un incremento del 38 % con respecto a 2023 (El País, 2024). De acuerdo con Unit 42 (2025), el 86 % de los incidentes documentados causaron perjuicios a la reputación, pérdidas económicas o impactos operativos; en algunas situaciones, el hurto de datos sucedió en menos de 25 minutos.

Estos peligros han tenido un impacto particular en los sectores críticos. De acuerdo con el informe de Check Point (2025), los sectores que fueron más atacados fueron el educativo con 4.484 ataques semanales, luego el gubernamental con 2.678 y por último el de telecomunicaciones con 2.664 ataques a la semana. A su vez, el sector de la salud enfrenta riesgos especialmente delicados, dada la naturaleza de los datos que gestiona. Los dispositivos como las bombas de insulina conectadas o los monitores de signos vitales pueden ser atacados, lo que podría poner en peligro la vida del paciente (El Sayed et al., 2025).

2.2. La inteligencia artificial como arma de doble filo

La integración de la inteligencia artificial (IA) en el ámbito de la ciberseguridad ha generado una revolución, aunque simultáneamente ha introducido nuevos retos. Por un lado, la inteligencia artificial facilita la identificación de amenazas en tiempo real, la automatización de respuestas ante incidentes y la predicción de comportamientos inapropiados. Además, los actores malintencionados en el ciberespacio están aprovechando estas tecnologías para llevar a cabo ataques más atractivos, dirigidos y difíciles de identificar (Lin Aung et al., 2025). Instrumentos de Inteligencia Artificial generativa pueden ser utilizados para la generación de código malintencionado, la imitación de patrones comunicativos legítimos ola automatización de procesos de identificación y explotación de vulnerabilidades.

La carrera entre atacantes y defensores se ha intensificado con el uso de estas tecnologías, haciendo aún más evidente la necesidad de soluciones innovadoras y colaborativas para proteger los entornos IoT.

2.3. Privacidad y gestión de datos en IoT

Los dispositivos IoT recolectan y transmiten volúmenes significativos de información personal, corporativa y gubernamental. La mayoría de estas transacciones se llevan a cabo sin cifrado robusto y sin mecanismos de autenticación seguros, lo que propicia la interceptación, manipulación o extravío de información delicada (Álvarez & Morales, sf). Esta circunstancia constituye una amenaza tanto para la privacidad de los usuarios como para la integridad de las operaciones de la organización.

El problema se intensifica cuando los dispositivos no disponen de actualizaciones de seguridad automáticas o mecanismos para atenuar vulnerabilidades identificadas posteriormente a su

lanzamiento. Fernández y Gutiérrez (2023) alertan que la ausencia de una administración proactiva en este aspecto puede exponer a los dispositivos a ataques conocidos durante años, lo cual pone en riesgo su seguridad y la de las redes en las que se integran.

2.4. Normativas, estándares y gobernanza de la ciberseguridad en IoT

La falta de un marco regulatorio global y homogéneo para la seguridad del IoT constituye uno de los principales retos a los que se enfrentan las entidades gubernamentales y organizaciones. Sin embargo, en los años recientes han surgido importantes iniciativas regulatorias. En el contexto estadounidense, la ley de mejora de la ciberseguridad del Internet de las Cosas (IoT)de 2022 estipula requisitos mínimos de seguridad para los dispositivos conectados adquiridos por entidades federales. Esta La legislación fomenta la comprobación de vulnerabilidades y la instalación de controles fundamentales previos a la comercialización. Dentro de la Unión Europea, la Directiva NIS2, en vigor desde 2023, intensifica las responsabilidades en relación con la ciberseguridad para los operadores de servicios esenciales y los proveedores de infraestructura digital. Esta regulación enriquece el Reglamento General de Protección de Datos (GDPR), expandiendo el enfoque hacia los riesgos tecnológicos vinculados al Internet de las Cosas (IoT) (Ruiz, Romero & Méndez, 2023).

2.5. Buenas prácticas y limitaciones en su implementación

Pese a la existencia de numerosas recomendaciones y esquemas de buenas prácticas en el ámbito de la ciberseguridad, su aplicabilidad práctica es restringida. Estudios recientes indican que únicamente el 32 % de las prácticas óptimas sugeridas son efectivamente implementables en contextos productivos. Además, el 73 % de estas se enfoca en etapas iniciales del desarrollo de

software, desatendiendo elementos tales como el mantenimiento constante, la operación segura o la formación de los usuarios finales. Esto pone de Manifiesta la imperiosa necesidad de adoptar un enfoque holístico que amalgama elementos técnicos, humanos y organizacionales.

Conclusión del Marco Teórico

El Internet de las Cosas es un pilar fundamental de la transformación digital, aunque representa además un reto en aumento para la ciberseguridad. Las deficiencias técnicas, la ausencia de normativas universales, la implementación limitada de prácticas óptimas y el rápido progreso de tecnologías ofensivas, como la inteligencia artificial malintencionada, estructuran un escenario complejo y dinámico. Por lo tanto, se requiere una respuesta coordinada entre fabricantes, gobiernos, usuarios y expertos en ciberseguridad para promover una cultura de ciber resiliencia que permita aprovechar las ventajas del IoT sin poner en riesgo la privacidad, la integridad y la disponibilidad de los sistemas

Planteamiento del problema.

El crecimiento exponencial del Internet de las Cosas (IoT) ha inaugurado una nueva era de interconexión entre dispositivos, simplificando procesos en ámbitos como la salud, el transporte, la industria y el hogar conectados. Sin embargo, este progreso ha sido seguido de una creciente inquietud en torno a la ciberseguridad, dado que numerosos dispositivos del Internet de las Cosas (IoT) exhiben restricciones técnicas que obstaculizan la instalación de mecanismos de protección robustos (Roman, Zhou, & Lopez, 2013). Estos dispositivos, frecuentemente concebidos con costos reducidos y capacidades limitadas, no disponen de actualizaciones automáticas, utilizan credenciales predefinidas o protocolos de comunicación inseguros, y no poseen políticas de autenticación o cifrado eficaces (Fernández & Gutiérrez, 2023), Los dispositivos, frecuentemente concebidos con costos reducidos y capacidades limitadas, no disponen de actualizaciones automáticas, utilizan credenciales predefinidas o protocolos de comunicación inseguros, y no poseen políticas de autenticación o cifrado eficaces.

De acuerdo con el informe de SonicWall (2024), se registró un incremento del 107 % en los ataques dirigidos a dispositivos del Internet de las Cosas (IoT), subrayando que cada dispositivo experimentó, en promedio, más de 52 horas de ataques consecutivos. Esta circunstancia pone de manifiesto una tendencia ascendente hacia la explotación de vulnerabilidades intrínsecas al diseño de estos sistemas, frecuentemente desatendidas por los fabricantes y usuarios finales.

Además, la investigación de Unit 42 (2025) reporta que el 86 % de los incidentes involucrando dispositivos IoT conllevaron pérdidas operacionales o daños reputacionales significativos.

El problema central que orientó esta investigación fue:
¿Cuáles son los principales desafíos de ciberseguridad que enfrentan los dispositivos IoT en entornos domésticos y cuáles son las soluciones emergentes más efectivas para mitigar dichas amenazas?

La falta de estandarización global en materia de seguridad IoT agrava la problemática, dado que los marcos regulatorios aún se encuentran en desarrollo y no son universalmente aplicables. Por ejemplo, aunque la Unión Europea ha implementado la Directiva NIS2 (ENISA, 2023) y el Cyber Resilience Act (European Commission, 2024), su alcance está limitado a ciertos sectores y países, lo que deja amplias brechas regulatorias en el resto del mundo. En Estados Unidos, la IoT Cybersecurity Improvement Act (2022) establece pautas para dispositivos adquiridos por el gobierno, pero no para el mercado de consumo en general (United States Congress, 2023).

Adicionalmente, el uso de dispositivos conectados en el ámbito doméstico —como asistentes virtuales, cámaras de vigilancia y electrodomésticos inteligentes— ha hecho que los hogares se conviertan en blancos frecuentes para los ciberatacantes. La privacidad de los datos personales que recogen estos dispositivos también se ve comprometida, ya que muchas veces las comunicaciones no están cifradas o los datos son almacenados sin controles adecuados (Álvarez & Morales, 2022).

Justificación del estudio

particularmente en contextos domésticos, así como de las soluciones emergentes que pueden contribuir a la mitigación de dichos riesgos. La importancia de este estudio se

fundamenta en la imperiosa necesidad de identificar mecanismos técnicos, normativos y organizativos que potencian la protección de estos dispositivos, cuya adopción masiva continúa en expansión sin la implementación de medidas de seguridad apropiadas (Lin et al., 2017).

Mediante una revisión sistemática de documentos, el estudio facilitó la evaluación del efecto de tecnologías como la inteligencia artificial, la criptografía liviana y la metodología Zero Trust en la salvaguarda de dispositivos del Internet de las Cosas (IoT). Además, se llevaron a cabo un análisis de iniciativas regulatorias y prácticas óptimas sugeridas por entidades como ENISA, el NIST y la FCC, facilitando la identificación de discrepancias entre las recomendaciones y su aplicación práctica en el contexto residencial

En el marco de esta investigación, el objetivo es contribuir a la sensibilización de usuarios, fabricantes y formuladores de políticas respecto a la necesidad de implementar estrategias de seguridad holística, promoverla Actualización continua de firmware y diseño de productos seguros desde su concepción. Además, se aspira a fomentar un enfoque preventivo y resiliente ante posibles amenazas en el ecosistema de Internet de las Cosas (IoT), en consonancia con la transformación digital a nivel mundial.

Objetivo General

Analizar los principales desafíos de ciberseguridad que enfrentan los dispositivos del Internet de las Cosas (IoT), con énfasis en entornos domésticos, e identificar soluciones

emergentes para mitigar sus vulnerabilidades, mediante una revisión documental de literatura científica, técnica y normativa reciente.

Objetivos específicos

- Identificar las principales vulnerabilidades de seguridad presentes en dispositivos del ecosistema IoT, especialmente en entornos doméstico, a partir del análisis de literatura académica, estudios de caso e informes técnicos recientes.
- Examinar críticamente las soluciones emergentes en ciberseguridad aplicables al IoT, como la inteligencia artificial, blockchain y el enfoque Zero Trust, evaluando su aplicabilidad y efectividad en distintos contextos tecnológicos.
- Analizar el papel de los marcos normativos y regulatorios, tanto nacionales como internacionales, en la protección de los dispositivos IoT, destacando sus avances, limitaciones y desafíos de implementación.
- Formular recomendaciones para mejorar la seguridad de los dispositivos IoT en el entorno doméstico, integrando las soluciones tecnológicas emergentes y las mejores prácticas reconocidas en el ámbito de la ciberseguridad.

Metodología

Se utilizó un enfoque cualitativo para realizar el presente estudio, que se centró en una revisión exhaustiva de documentos de investigación académica, informes especializados sobre incidentes de seguridad y estudios de casos pertinentes relacionados con la ciberseguridad en dispositivos IoT. Este enfoque permitió una comprensión más profunda de los desafíos actuales de la ciberseguridad, así como una evaluación crítica de las soluciones emergentes utilizadas en diversos contextos. A través de esta metodología, fue posible identificar vulnerabilidades comunes y evaluar la efectividad de la normativa actual y las estrategias de mitigación apoyadas por organizaciones como **NIST** , la Agencia de la Unión Europea para la Ciberseguridad (**ENISA**) y diversos centros de investigación .

La estructura metodológica se desarrolló en tres etapas cruciales que tuvieron como objetivo asegurar la validez, relevancia y rigor académico de los datos recolectados :desarrollado en tres etapas cruciales que buscaban asegurar **la validez** , **relevancia y rigor** académico de los datos recolectados :

1.1 Tipo de Estudio

Este trabajo de grado corresponde a un **estudio de tipo cualitativo-descriptivo**, orientado a analizar, interpretar y contextualizar los principales retos de ciberseguridad en el entorno del Internet de las Cosas (IoT), así como las soluciones emergentes que han sido propuestas en investigaciones recientes.

1.2 Diseño Metodológico

La metodología elegida es de naturaleza **no experimental y documental**, ya que las variables no se modifican directamente, sino que se observan, se recuperan y se analizan utilizando datos de

fuentes secundarias. El objetivo es interpretar los fenómenos actuales de ciberseguridad del IoT desde una perspectiva crítica y sistemática.

1.3 Proceso de selección de información

Para garantizar el rigor metodológico en el presente estudio, se implementó un proceso estructurado de búsqueda y selección en documentos, apoyado en el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). En el presente estudio se implementó un proceso estructurado de búsqueda y selección de documentos, apoyado en el PRISMA (Preferred Reporting Items for Systematic Reviews). Método de metaanálisis. El método se utiliza en revisiones sistemáticas para hacer evidentes las fases de identificación, cribado, elegibilidad e inclusión de documentos, demostrando claramente cómo se depuró la información inicial hasta llegar a la exposición final.

Para responder a los objetivos de investigación, se realizó una búsqueda sistemática en bases de datos académicas como IEEE Xplore, Scopus y Google Scholar, utilizando términos clave relacionados con la ciberseguridad en dispositivos IoT, la privacidad de los datos, la interoperabilidad, y su implementación en entornos domésticos entre otros.

La primera revisión incluyó el análisis de títulos, resúmenes y palabras clave con el propósito de identificar estudios relevantes, actualizados y directamente relacionados con los objetivos del estudio. Como resultado de este proceso, se identificaron inicialmente 42 documentos.

Posteriormente, se aplicaron los siguientes criterios de inclusión:

(i) publicaciones entre los años 2022 y 2025

(ii) documentos académicos revisados por pares

(iii) informes técnicos de organismos internacionales

(iv) legislación vigente relacionada con la ciberseguridad en entornos IoT.

Como criterios de exclusión, se descartaron:

(i) artículos duplicados

(ii) publicaciones sin acceso al texto completo

(iii) documentos que no abordaran de forma directa los retos o soluciones en ciberseguridad para IoT.

Estos registros fueron evaluados por **título y resumen**, eliminándose 20 por no cumplir con los criterios de inclusión, quedando 25 documentos elegidos para lectura completa. Tras un análisis más detallado del contenido, se excluyeron 13 por no aportar información directamente relacionada con los retos o soluciones de ciberseguridad en IoT. Finalmente, se conformó una **muestra final de 12 documentos clave**, entre los que se incluyen artículos científicos, informes técnicos y marcos normativos como el *IoT Cybersecurity Improvement Act*, la Directiva *NIS2* y el *Cyber Resilience Act*.

La siguiente tabla muestra de manera resumida el proceso de depuración de la literatura siguiendo el método PRISMA simplificado.

Tabla 1. Proceso de selección de artículos (PRISMA simplificada)

Etapa del Proceso	Cantidad
Registros identificados mediate búsqueda en bases de datos (IEEE, Scopus, Google Scholar)	42
Registros adicionales identificados a través de otras fuentes (informes, legislación)	8
Registros después de eliminar duplicados	45
Registros evaluados por título y resumen	45
Registros excluidos por no cumplir criterios	20
Artículos seleccionados para lectura completa	25
Artículos excluidos tras lectura completa	13
Documentos incluidos en la muestra final	12

Asimismo, para facilitar la comprensión del proceso, se elaboró un diagrama de flujo PRISMA simplificado, que ilustra gráficamente cómo se pasó de los registros iniciales a la muestra final.

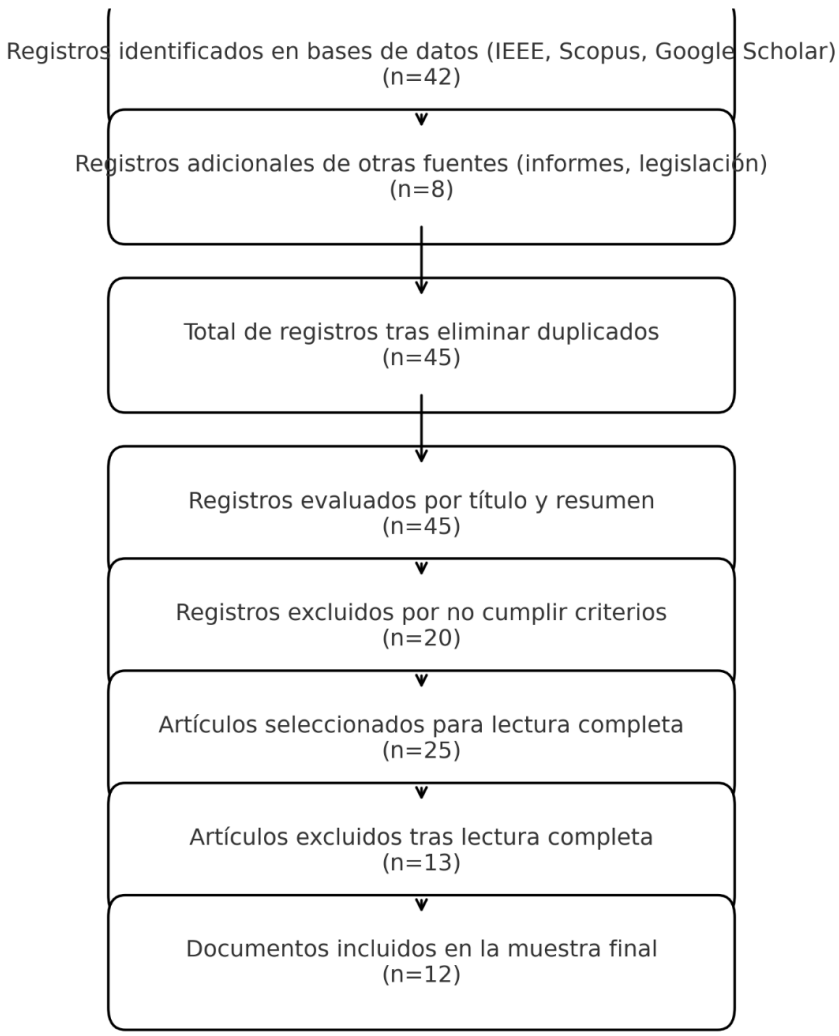

Ilustración 1 diagrama de flujo PRISMA simplificado

Este procedimiento garantizó que el análisis subsiguiente se basara sobre evidencia actualizada, pertinente y de alta calidad académica, asegurando así la robustez del marco conceptual y de los hallazgos del estudio.

1.4 Etapas del Proceso Metodológico

El presente estudio cualitativo-descriptivo se desarrolló mediante un proceso metodológico en tres etapas, que permiten abordar de manera integral los objetivos específicos planteados. A continuación, se describe la relación entre cada objetivo y las etapas del proceso metodológico:

Objetivo 1: Identificar las principales vulnerabilidades de seguridad presentes en dispositivos del ecosistema IoT doméstico.

Esta meta se abordó en la primera etapa, mediante la selección y revisión minuciosa de literatura académica y técnica publicada entre 2022 y 2025, lo que facilitó el establecimiento de un marco conceptual robusto sobre las vulnerabilidades en dispositivos IoT.

Tabla 2. Fuentes académicas clave sobre ciberseguridad en dispositivos IoT

Código	Título del artículo	Año	Fuente
A01	Privacidad de los datos en entornos IoT domésticos	2022	Revista Latinoamericana de Tecnología y Sociedad (Álvarez & Morales)
A02	Casos emblemáticos de ciberataques en sistemas IoT	2023	Revista Iberoamericana de Tecnologías Emergentes (Martínez et al.)

A03	Vulnerabilidades persistentes en dispositivos IoT: un análisis desde la seguridad	2023	Revista Iberoamericana de Ingeniería (Fernández & Gutiérrez)
A04	Tendencias emergentes en ciberseguridad para entornos IoT: IA y blockchain	2023	Revista de Seguridad Informática y Tecnología (López & García)
A05	Directive on Security of Network and Information Systems (NIS2)	2023	ENISA – Agencia de la Unión Europea para la Ciberseguridad
A06	IoT Cybersecurity Improvement Act	2023	Congreso de los Estados Unidos
A07	Informe global de ciberataques 1T 2025	2025	Check Point Software Technologies
A08	Generative AI for Internet of Things Security	2025	arXiv (Lin Aung et al.)
A09	Medical IoT Security: Challenges and Mitigation Strategies	2025	Journal of Cybersecurity Research (ElSayed, Farag & Hussein)

A10	Informe Global de Respuesta a Incidentes	2025	Unit 42 – Palo Alto Networks
A11	Cyber Threat Report 2024	2024	SonicWall
A12	Cyber Resilience Act	2024	Comisión Europea

La Tabla 2 Proporciona un resumen de los artículos seleccionados, especificando el título, el año de publicación y la fuente correspondiente. Este compendio proporciona una visión general del estado actual de la investigación. resultado del proceso de depuración, se seleccionan doce publicaciones académicas y técnicas del periodo 2022–2025, que ofrecen hallazgos significativos sobre vulnerabilidades comunes en el IoT doméstico, así como sobre soluciones emergentes como la inteligencia artificial, el blockchain y los recientes marcos regulatorios. En conjunto, estos documentos proporcionan un respaldo teórico y técnico esencial para entender los riesgos predominantes y las estrategias de mitigación en el contexto examinado.

Se presenta la **ilustración 2** que muestra la distribución de los artículos seleccionados por año de publicación. Como se observa, la mayoría de los estudios fueron publicados en **2022 y 2025**, lo que indica un interés creciente en la ciberseguridad de los dispositivos IoT en años recientes.

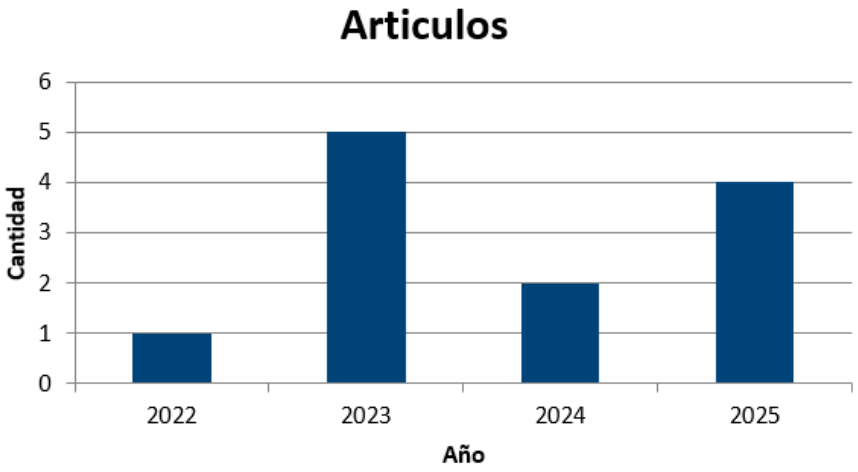

Ilustración 2. Año de Publicación de los Artículos.

Este aumento se puede explicar por una serie de factores, entre ellos el uso generalizado de dispositivos IoT en entornos residenciales, comerciales y urbanos , que aumenta su vulnerabilidad a los riesgos de seguridad ; el aumento de los incidentes de ciberseguridad que involucran a estos dispositivos, que ha atraído más atención de la comunidad científica ; la introducción de nuevas regulaciones y marcos legales , como la NIS2, la Ley de Mejora de la Ciberseguridad de IoT y la Ley de Resiliencia Cibernética ; y el desarrollo de soluciones tecnológicas emergentes , como la inteligencia artificial , la cadena de bloques y Zero Trust, que han impulsado la investigación destinada a mejorar la protección de estos sistemas.

Ilustración 3 proporciona un análisis detallado de las temáticas abordadas en los artículos seleccionados, enfocándose en la situación actual de los dispositivos IoT de uso doméstico. Los temas tratados en los artículos seleccionados, centrándose en el estado actual de los dispositivos IoT utilizados en el hogar. muestra el porcentaje de artículos que contienen o no términos clave relacionados con la ciberseguridad y la protección de datos, como internet de las cosas (IoT), ciberseguridad, vulnerabilidades, protección de datos y soluciones emergentes.

Este análisis permite la identificación de las tendencias teóricas más prevalecientes y las posibles brechas en el tratamiento de elementos esenciales para la seguridad de estos entornos tecnológicos. tendencias teóricas prevalecientes y posibles lagunas en el tratamiento de elementos esenciales para seguridad de estos entornos tecnológicos.

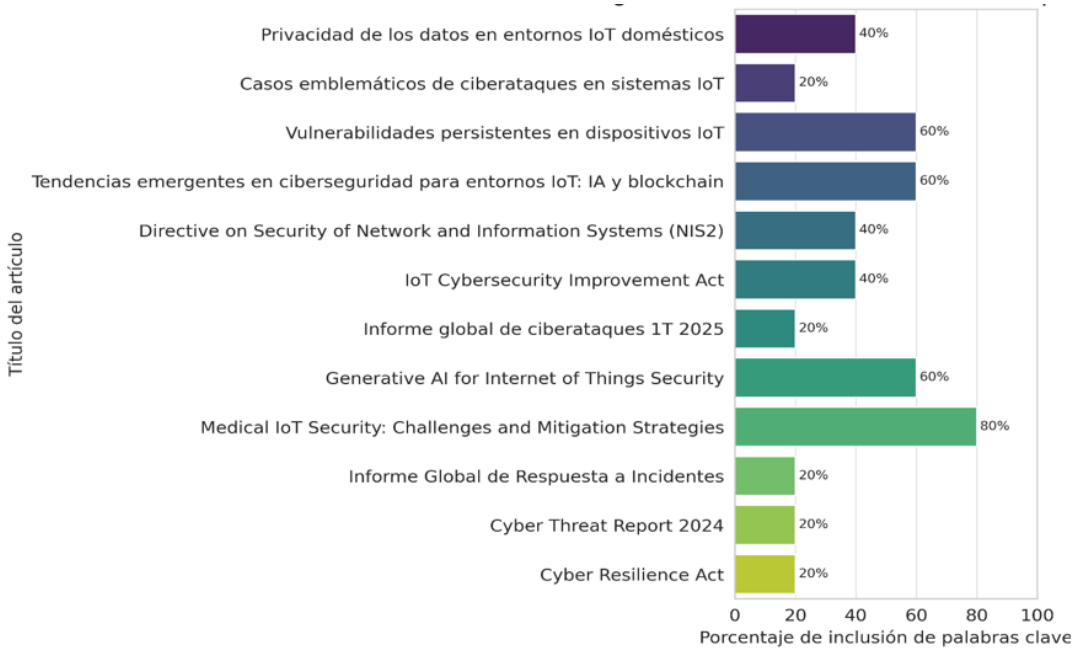

Ilustración 3. Términos claves

Con estas tendencias, es evidente que los estudios recientes se centran principalmente en la ciberseguridad y la protección de datos, así como en el uso de soluciones tecnológicas en desarrollo. Existen lagunas en la comprensión de algunos aspectos regulatorios y en la evaluación integral de las vulnerabilidades en los entornos domésticos, lo que sugiere oportunidades para futuras investigaciones.

Este análisis nos permite concluir, tal como se refleja en la Tabla 3, que los artículos seleccionados evidencian tendencias claras en torno a los desafíos y enfoques actuales relacionados con los dispositivos del Internet de las Cosas (IoT). Los estudios abordan múltiples dimensiones, desde aspectos técnicos hasta regulatorios, destacando el creciente interés en la ciberseguridad, la protección de datos y las soluciones tecnológicas emergentes aplicadas al ecosistema doméstico.

Tabla 3. Análisis Porcentual por palabras claves

Palabra clave	Artículos que la incluyen	% Inclusión	% No inclusión
Internet de las Cosas (IoT)	8 de 12	66.70%	33.30%
Ciberseguridad	10 de 12	83.30%	16.70%
Vulnerabilidades	2 de 12	16.70%	83.30%
Protección de datos	2 de 12	16.70%	83.30%
Soluciones emergentes	4 de 12	33.30%	66.70%

Estos datos muestran que, aunque la ciberseguridad es el eje más abordado (presente en más del 80% de los artículos), aspectos críticos como las vulnerabilidades específicas entre ellas la **falta de cifrado en la transmisión de datos, contraseñas predeterminadas débiles y ausencia de actualizaciones automáticas en dispositivos domésticos** y la protección de datos en entornos IoT siguen siendo temas poco tratados directamente, lo que sugiere una oportunidad

para profundizar en estas áreas. Tal como señalan Álvarez y Morales (2022), la escasa atención a la privacidad en dispositivos de uso cotidiano representa un riesgo creciente para los usuarios.

Esto resalta la necesidad de avanzar hacia una visión más integral, donde la privacidad y la seguridad de los usuarios en el hogar sean consideradas pilares esenciales del desarrollo tecnológico en el ámbito del IoT.

Tras identificar las principales vulnerabilidades encontradas en dispositivos IoT utilizados en el hogar, **el estudio se centra en examinar críticamente las soluciones de ciberseguridad emergentes que apuntan a reducir estos riesgos.** Se examinan el marco, las tecnologías y enfoques innovadores como la inteligencia artificial, la cadena de bloques y el modelo Zero Trust para evaluar la eficacia de su aplicabilidad en diversos contextos tecnológicos. El análisis no solo permite reconocer los avances recientes en la protección del entorno de IoT, sino que también identifica cómo estas soluciones podrían integrarse estratégicamente para fortalecer la seguridad y la resiliencia de los sistemas conectados.

El objetivo se abordó en la primera y tercera etapa del proceso metodológico. En primer lugar, se identificaron soluciones a través de la revisión sistemática de la literatura académica y técnica centrada en las tecnologías utilizadas para la ciberseguridad en el contexto de la Internet de las cosas. Esta revisión examina los 12 documentos elegidos en la primera etapa, analizando específicamente herramientas como inteligencia artificial, blockchain y el enfoque Zero Trust.

Posteriormente, en la tercera etapa, se realizó un análisis cualitativo y comparativo de estas soluciones, con el fin de examinar críticamente su aplicabilidad y efectividad en distintos entornos tecnológicos. Esta evaluación permitió establecer no solo sus ventajas técnicas, sino también las limitaciones y desafíos que enfrentan al implementarse en infraestructuras IoT

reales. El análisis se realizó a partir de una matriz comparativa construida con base en criterios extraídos de las fuentes documentales seleccionadas. Estos criterios incluyeron: el nivel de madurez tecnológica, el grado de adopción en entornos reales, la escalabilidad, la compatibilidad con dispositivos IoT y la capacidad para prevenir o mitigar vulnerabilidades específicas. Por ejemplo, la **inteligencia artificial** fue evaluada por su capacidad para detectar patrones anómalos en el tráfico de red y predecir ataques, **blockchain** por su efectividad en garantizar la integridad y trazabilidad de los datos entre dispositivos, y el **modelo Zero Trust** por su capacidad de restringir accesos de manera granular y adaptativa. Cada tecnología fue examinada en función de estos aspectos, permitiendo identificar patrones, fortalezas, debilidades y oportunidades de aplicación.

El enfoque cualitativo-descriptivo del estudio fue esencial para comprender la evidencia documental y evaluar el nivel de robustez de cada solución, su alineación con los requisitos de seguridad de IoT y su potencial contribución a una arquitectura más resiliente frente a amenazas emergentes.

Tabla 4. Comparación cualitativa de soluciones emergentes en ciberseguridad aplicables al IoT.

Código	Solución emergente	Nivel de madurez	Adopción práctica	Escalabilidad	Compatibilidad IoT	Mitigación efectiva	Tipo de solución
A04	IA / Blockchain	Medio-Alto	Moderada	Alta	Alta	Alta	Tecnológica
A08	IA Generativa	Bajo-Medio	Experimental	Alta	Media	Prometedora	Tecnológica
A05	Zero Trust (NIS2)	Alto	En implementación UE	Alta	Alta	Alta	Regulatoria
A06	Zero Trust (Ley USA)	Medio	Obligatoria en EE.UU	Media	Alta	Alta	Regulatoria
A12	Zero Trust / IA	Medio	Inicial en Europa	Alta	Media-Alta	Alta	Híbrida

De la Tabla 4 se concluye que las soluciones emergentes en ciberseguridad aplicables al IoT presentan distintos niveles de madurez y enfoques complementarios, incluyendo inteligencia artificial, blockchain y modelos Zero Trust. Cada solución contribuye de manera específica a la resiliencia y protección de los dispositivos, permitiendo prevenir, detectar y responder a amenazas de manera más efectiva. Asimismo, se evidencia que la integración estratégica de varias de estas soluciones puede generar una arquitectura de seguridad más robusta y adaptable a los distintos contextos tecnológicos.

Nota metodológica: La construcción de la Tabla 4 se basó en un análisis cualitativo de la información extraída de las fuentes documentales seleccionadas (A04, A05, A06, A08 y A12). Para cada criterio se definieron parámetros de valoración sustentados en la literatura revisada:

Nivel de madurez tecnológica: basado sobre la clasificación propuesta en los estudios analizados, considerando si la tecnología se encuentra en fase experimental, en

desarrollo, en etapa de adopción temprana o consolidada en el mercado. Se emplearon categorías cualitativas (Bajo, Bajo-Medio, Medio, Medio-Alto y Alto).

Adopción práctica: evaluada según la evidencia reportada sobre implementaciones reales, regulaciones vigentes o proyectos piloto, clasificándola como experimental, inicial, Moderada, en implementación o obligatoria.

Escalabilidad: evaluado en base a casos documentados y análisis técnico, teniendo en cuenta la capacidad de la solución para adaptarse a entornos IoT de diversos tamaños y complejidad. Por ejemplo, la plataforma de gestión de dispositivos basada en inteligencia artificial puede monitorizar desde unas pocas decenas hasta miles de dispositivos simultáneamente, adaptando sus algoritmos de detección de anomalías según la carga. De manera similar, las redes blockchain privadas pueden ampliarse para incluir nuevos nodos sin comprometer la integridad de los datos, y los modelos Zero Trust permiten escalar políticas de acceso granular en empresas u hogares con distintos niveles de complejidad tecnológica.

Compatibilidad con dispositivos IoT: evaluada observando qué tan fácil es que la solución funcione con diferentes equipos y sistemas de IoT, revisando si puede conectarse e intercambiar información sin problemas, según lo demostrado en pruebas, proyectos piloto o implementaciones descritas en las fuentes seleccionadas.

Mitigación efectiva de vulnerabilidades: evaluada según qué tan bien la solución puede evitar, detectar o responder a ataques y fallas de seguridad en sistemas IoT. Para este estudio, se establecieron cuatro categorías de valoración —Alta, Media, Baja y Prometedora— construidas a partir de criterios utilizados en la literatura sobre evaluación de medidas de ciberseguridad (ENISA, 2023; NIST, 2022). Esta categorización permitió valorar de forma comparativa la efectividad de cada solución reportada en los artículos analizados,

reconociendo además aquellas tecnologías que, aunque aún en desarrollo, evidencian un alto potencial de aplicación futura.

Tipo de solución: definido de acuerdo con la naturaleza de la propuesta (tecnológica, regulatoria o híbrida), tomando como base el objetivo principal y el mecanismo de actuación descritos en las fuentes.

Este procedimiento permite garantizar que los valores asignados a cada criterio estuvieran respaldados por evidencia documentada y un proceso sistemático de revisión y comparación.

Al evaluar las soluciones emergentes de ciberseguridad de IoT , queda claro que la eficacia de estas tecnologías depende no solo de su destreza técnica , sino también de su cumplimiento de los marcos regulatorios y legales que garantizan una implementación y funcionalidad adecuadas.

Por ello, el siguiente paso del estudio se centra en analizar el papel de las regulaciones vigentes y los estándares internacionales en la ciberseguridad de dispositivos IoT, identificando cómo estos marcos contribuyen a establecer lineamientos claros, fomentar la adopción de buenas prácticas y fortalecer la protección de los entornos conectados, constituyendo así el Objetivo 3 del trabajo.

El tercer objetivo se abordó principalmente en la tercera etapa del proceso metodológico, mediante una revisión exhaustiva y detallada de los marcos normativos y regulatorios más relevantes para la ciberseguridad en dispositivos del Internet de las Cosas (IoT). Esta revisión se basó en las mismas 12 fuentes seleccionadas previamente para el análisis documental, dado que estas incluyen documentos normativos clave, tales como la Directiva NIS2 de la Unión Europea (A05), la IoT Cybersecurity Improvement Act de los

Estados Unidos (A06) y el Cyber Resilience Act propuesto por la Comisión Europea (A12), además de estudios técnicos y reportes académicos que contextualizan su aplicación y alcance.

A continuación, se presentan brevemente estos marcos normativos, su objetivo principal y la referencia correspondiente.

Tabla 5 Resumen de marcos regulatorios y normativos en ciberseguridad para IoT

Marco normativo	Breve descripción	Objetivo principal	Referencia APA
Directiva NIS2 (UE) – A05	Actualización de la Directiva NIS original, que establece requisitos de seguridad cibernética para operadores de servicios esenciales y proveedores de servicios digitales en la UE.	Mejorar la resiliencia y capacidad de respuesta frente a incidentes cibernéticos en sectores críticos.	Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2555
IoT Cybersecurity Improvement Act (EE. UU.) – A06	Ley estadounidense que establece estándares mínimos de seguridad para dispositivos IoT adquiridos por agencias federales.	Garantizar la seguridad de dispositivos IoT en entornos gubernamentales y promover buenas prácticas de ciberseguridad.	United States Congress. (2019). IoT Cybersecurity Improvement Act of 2019, H.R.1668. https://www.congress.gov/bill/116th-congress/house-bill/1668
Cyber Resilience Act (UE) – A12	Propuesta de regulación europea que exige a fabricantes de hardware y software implementar medidas de ciberseguridad durante todo el ciclo de vida de los productos.	Incrementar la seguridad y resiliencia de productos conectados en el mercado europeo.	Comisión Europea. (2022). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

El proceso de revisión se estructuró en tres fases metodológicas.

En primer lugar, se una búsqueda y selección cuidadosa de fuentes que contenían propuestas regulatorias relevantes o leyes actuales, así como estudios que examinaran sus efectos en el entorno de la Internet de las cosas.

En segundo lugar, se realizó un análisis de contenido con el objetivo de identificar elementos normativos esenciales como los requisitos técnicos, las obligaciones legales impuestas a los fabricantes y proveedores, los mecanismos de cumplimiento y las sanciones por incumplimiento. El análisis permitió agrupar los marcos regulatorios según su enfoque, nivel de exigencia, cobertura tecnológica y orientación a la seguridad.

Posteriormente, se procedió a una contextualización crítica de los hallazgos normativos, teniendo en cuenta las características únicas del ecosistema IoT, como su heterogeneidad, alta conectividad, escalabilidad y vulnerabilidad a ciberataques. Se realizó una evaluación de los hallazgos normativos teniendo en cuenta las características únicas del ecosistema IoT, como su heterogeneidad, alta conectividad, escalabilidad y vulnerabilidad a los ciberataques. Se evaluó la pertinencia de cada marco regulatorio a la luz de estos desafíos y se examinó su capacidad para reducir riesgos, mitigar vulnerabilidades y fomentar la adopción de prácticas sólidas de ciberseguridad.

Este enfoque permitió comprender plenamente el papel que juegan las regulaciones internacionales y las políticas públicas en la creación de un entorno de IoT más seguro y confiable. Además, demostró la necesidad de regulaciones flexibles, cohesivas y evolutivas que aborden activamente la rápida transformación tecnológica de la industria.

Evaluación crítica de los marcos normativos en IoT

La evaluación crítica se llevó a cabo como la etapa final del análisis documental, enmarcada en el enfoque cualitativo-descriptivo del estudio. Esta fase se centró en contrastar los contenidos de los marcos regulatorios más relevantes

- Directiva NIS2 (A05)
- IoT Cybersecurity Improvement Act (A06)
- Cyber Resilience Act (A12)

con las necesidades reales del ecosistema IoT, particularmente en relación con las amenazas emergentes, la diversidad de dispositivos y las exigencias operativas de la ciberseguridad actual.

Se definieron tres ejes esenciales para el análisis crítico.
En primer lugar, la efectividad normativa se evaluó en qué medida las disposiciones legales propuestas o vigentes son capaces de prevenir, mitigar y responder ante amenazas de ciberseguridad.

En segundo lugar, la aplicabilidad práctica, que evaluó la viabilidad de la implementación de las normativas en diversos contextos tecnológicos y organizativos.

Por último, se examinó la evolución del IoT, su compatibilidad con enfoques contemporáneos como el modelo Zero Trust, y su cobertura en relación con toda la cadena de valor. Se emplearon tres instrumentos metodológicos para la evaluación, adaptados de enfoques de análisis comparativo normativo y revisión documental (ENISA, 2023; NIST, 2022):

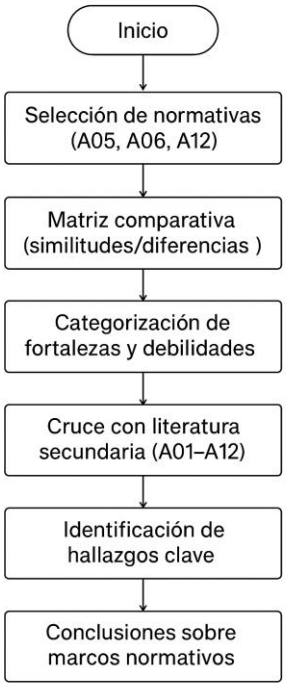

Ilustración 4 Flujo metodológico de evaluación normativa y documental

- Una **matriz comparativa entre normativas** (basada en las fuentes A05, A06, A12), que permitió identificar similitudes y diferencias en requisitos técnicos, obligaciones legales y mecanismos de verificación.
- La **categorización de fortalezas y debilidades**, empleada para valorar de manera crítica los alcances y limitaciones de cada normativa en el contexto del IoT.
- El **cruce con literatura secundaria** (fuentes A01–A12), mediante el cual se contrastaron los postulados normativos con evidencias empíricas y análisis académicos sobre su implementación.

  A continuación, se resumen los hallazgos clave identificados en la evaluación crítica de los marcos normativos analizados.

Tabla 6. Fortalezas y limitaciones identificadas en los marcos normativos analizados

Aspecto	Fortalezas	Limitaciones	Fuentes (A)
Efectividad normativa	Establecen requisitos técnicos claros y obligatorios para fabricantes y proveedores, facilitando la mitigación de riesgos (A05, A06, A12).	Algunas disposiciones son demasiado generales o vagas, lo que dificulta su aplicación práctica en escenarios específicos (A01, A07).	A01, A05, A06, A07, A12
Cobertura tecnológica	Incluyen dispositivos variados y abarcan diferentes capas del ecosistema IoT, lo que contribuye a un enfoque integral (A05, A12).	No todos los tipos de dispositivos IoT están contemplados con la misma profundidad, especialmente los emergentes (A03, A08).	A03, A05, A08, A12
Adaptabilidad	Incorporan mecanismos para actualización y adaptación ante nuevas amenazas y tecnologías, favoreciendo su vigencia (A06, A12).	La velocidad del cambio tecnológico en IoT supera la capacidad de actualización regulatoria, lo que puede dejar vacíos legales (A04, A09).	A04, A06, A09, A12
Implementación práctica	Proveen guías y marcos de cumplimiento que facilitan la adopción y verificación por parte de organizaciones (A05, A06).	La heterogeneidad del ecosistema IoT y la diversidad de actores dificultan la implementación uniforme (A02, A10).	A02, A05, A06, A10
Enfoque en seguridad	Promueven la integración de principios modernos de ciberseguridad, como el enfoque Zero Trust y la gestión de riesgos (A05, A12).	Algunos marcos carecen de detalles operativos específicos que guíen a las pequeñas y medianas empresas (A01, A11).	A01, A05, A11, A12

La tabla presenta un análisis de las fortalezas y limitaciones encontradas en los principales marcos normativos y regulatorios para la ciberseguridad en IoT, basado en la revisión documental de las fuentes codificadas A01 a A12.

Efectividad normativa: Documentos como la Directiva NIS2 (A05), la Ley de Mejora de la Ciberseguridad de la IoT (A06) y la Ley de Resiliencia Cibernética (A12) delinean obligaciones técnicas explícitas que ayudan a mitigar los riesgos. No obstante, investigaciones como A01 y A07 indican que algunas disposiciones son imprecisas, complicando su aplicación exacta.

Cobertura tecnológica: Los marcos examinados abarcan diversos tipos de dispositivos y capas tecnológicas, esto que permite un enfoque holístico (A05, A12). No obstante, de acuerdo con A03 y A08, persisten lagunas en la regulación de dispositivos emergentes que exigen atención.

Adaptabilidad: Se reconoce en A06 y A12 la intención de incorporar mecanismos de actualización para responder a nuevas amenazas, aunque fuentes como A04 y A09 advierten que la rapidez del cambio tecnológico en IoT puede superar la capacidad regulatoria para mantenerse al día.

Implementación práctica: Los marcos proveen guías útiles para el cumplimiento normativo (A05, A06), pero la gran diversidad del ecosistema IoT y los distintos actores involucrados dificultan una implementación uniforme, según A02 y A10.

Enfoque en seguridad: Se evidencia en los marcos un impulso hacia principios modernos de ciberseguridad, como Zero Trust, pero fuentes como A01 y A11 destacan la falta de especificidad operativa, lo que afecta principalmente a las pymes.

El análisis de las fortalezas y limitaciones de los marcos regulatorios de la ciberseguridad del IoT muestra que, si bien existen requerimientos técnicos claros, amplia cobertura tecnológica y mecanismos de implementación, aún existen desafíos como la ambigüedad de algunos dispositivos, brechas en la regulación de dispositivos emergentes y desafíos de implementación uniforme en un ecosistema heterogéneo. Los hallazgos respaldan la relevancia de soluciones emergentes como la inteligencia artificial, la cadena de bloques y los enfoques de confianza cero (Objetivo 2) y proporcionan un marco crítico para evaluar la eficacia de la legislación actual (Objetivo 3).

A partir de esta evaluación, se hace evidente la necesidad de **formular recomendaciones específicas que permitan mejorar la seguridad de los dispositivos IoT en el entorno doméstico**, considerando tanto los avances regulatorios como las limitaciones identificadas. Así, la información presentada en esta tabla constituye la base para el desarrollo del Objetivo 4, orientado a proponer medidas prácticas, adaptables y eficaces frente a los retos tecnológicos y normativos del ecosistema IoT.

La formulación de recomendaciones se estructuró como la fase final del estudio, orientada a integrar los hallazgos obtenidos durante la revisión documental y convertirlos en acciones concretas para fortalecer la seguridad de los dispositivos IoT utilizados en hogares. Este proceso se fundamentó en un enfoque cualitativo-descriptivo, el cual permitió identificar, contrastar y clasificar propuestas provenientes de diversas fuentes académicas, técnicas y normativas.

El análisis de los documentos (A01–A12) permitió reconocer patrones comunes de vulnerabilidad, así como prácticas de mitigación propuestas tanto por organismos internacionales como por investigadores especializados. Con base en esta evidencia, se elaboraron

recomendaciones dirigidas a tres actores clave: usuarios finales, fabricantes de dispositivos IoT y responsables de políticas públicas.

Tabla 7 Recomendaciones para fortalecer la seguridad de los dispositivos IoT en entornos domésticos.

Actor	Recomendación	Fuente (A)
Usuarios finales	Utilizar contraseñas robustas y únicas, evitando configuraciones predeterminadas	A01, A03, A07
	Mantener los dispositivos actualizados y habilitar sistemas de actualizaciones automáticas seguras	A03, A09
	Segmentar la red doméstica, separando dispositivos IoT del resto de equipos personales o de trabajo	A02, A07
	Desactivar funciones innecesarias, como acceso remoto, cuando no se requieran	A01, A03
	Fomentar la alfabetización digital básica en ciberseguridad entre todos los miembros del hogar	A10, A11
Fabricantes de dispositivos IoT	Integrar el enfoque “Security by Design” desde la fase de diseño del producto	A04, A08
	Proveer actualizaciones automáticas seguras y mecanismos robustos de autenticación de firmware	A04, A09
	Simplificar la configuración inicial de seguridad para usuarios no expertos	A01, A03
	Incluir documentación clara sobre prácticas recomendadas de ciberseguridad	A03, A04
Políticas públicas y normativa	Establecer estándares mínimos obligatorios de ciberseguridad para dispositivos IoT en el mercado	A05, A06, A12

	Promover campañas educativas y de concienciación sobre riesgos asociados a dispositivos conectados	A10, A11
	Fomentar la certificación de dispositivos IoT bajo criterios de seguridad previamente definidos	A06, A12

Las recomendaciones no sólo abordan las vulnerabilidades señaladas en la literatura revisada, sino que también se alinean con los marcos regulatorios emergentes en los EE. UU. y Europa, lo que agrega solidez técnica y normativa a su aplicabilidad. Su relevancia en el ámbito doméstico latinoamericano se justifica por el creciente número de hogares con dispositivos conectados, muchas veces instalados sin una evaluación de seguridad previa.

Síntesis e interpretación crítica: El uso del enfoque cualitativo-descriptivo basado en la revisión documental permitió un abordaje integral del complejo tema de la ciberseguridad en el Internet de las Cosas (IoT), incorporando aspectos técnicos, legales y contextuales sin necesidad de recolectar datos primarios. Desde este punto de vista, este enfoque metodológico fue especialmente útil para identificar y organizar información pertinente, comparar hallazgos de diversas fuentes e identificar patrones de vulnerabilidad y estrategias de mitigación emergentes.

Durante el análisis, resultó evidente que, aunque la literatura revisada (A01–A12) proporciona datos empíricos y conceptuales de alta relevancia, existe una tensión constante entre la innovación tecnológica y la protección efectiva de la seguridad digital. Si bien la literatura revisada (A01–A12) proporciona datos empíricos y conceptuales de gran relevancia, existe una tensión constante entre la innovación tecnológica y la protección efectiva de la seguridad digital. La fragmentación en la aplicabilidad de soluciones avanzadas como la inteligencia artificial, la cadena de bloques o los enfoques de confianza cero refleja la necesidad de conectar la teoría con

prácticas tangibles y accesibles para usuarios y organizaciones con diferentes niveles de experiencia.

En mi apreciación, este proceso metodológico no sólo permitió alcanzar los objetivos planteados, sino que también reveló brechas críticas en la protección de los dispositivos IoT, reafirmando la necesidad de enfoques interdisciplinarios y el desarrollo de recomendaciones prácticas. La experiencia adquirida resalta que la investigación en ciberseguridad debe trascender la mera adopción tecnológica, integrando aspectos normativos, educativos y contextuales para generar soluciones realmente efectivas y sostenibles.

Resultados y Discusión

Análisis del problema central: Desafíos de ciberseguridad en dispositivos IoT domésticos y soluciones emergentes

El entorno doméstico se ha convertido en uno de los entornos más vulnerables a las ciberamenazas relacionadas con el Internet de las Cosas (loT). El creciente uso de dispositivos inteligentes como cámaras de seguridad, asistentes virtuales, termostatos, cerraduras y dispositivos electrónicos conectados ha incrementado la superficie de ataque de los actores maliciosos. Los principales desafíos de la ciberseguridad en este contexto pueden agruparse en cinco áreas clave.

En primer lugar, muchos dispositivos IoT domésticos son desarrollados sin un enfoque integral de seguridad. Funcionan con hardware limitado, carecen de cifrado robusto y utilizan credenciales por defecto. Esta situación, documentada por Fernández y Gutiérrez (A03), permite que incluso atacantes con habilidades básicas puedan comprometer los dispositivos. Por ejemplo,

el ataque masivo del malware Mirai demostró cómo miles de cámaras y grabadores domésticos inseguros podían ser convertidos en una botnet para ataques DDoS a gran escala (Check Point, A07). Además, la falta de capacidad para recibir actualizaciones automáticas de firmware expone a los usuarios a amenazas persistentes a lo largo del tiempo.

En segundo lugar, la carencia de marcos normativos universales ha contribuido a una implementación desigual de prácticas de ciberseguridad. Aunque iniciativas como la IoT Cybersecurity Improvement Act (A06) en Estados Unidos y la Directiva NIS2 (A05) en la Unión Europea han propuesto requisitos mínimos para la seguridad de dispositivos conectados, estas normativas aún no se aplican de manera global ni obligatoria para el mercado de consumo masivo. Esto permite la circulación de dispositivos inseguros sin responsabilidad clara por parte de los fabricantes. El Cyber Resilience Act (A12) avanza en este sentido al exigir certificaciones de seguridad previas a la comercialización, pero su implementación práctica aún enfrenta retos.

En tercer lugar, los ciberataques a dispositivos IoT han aumentado de manera alarmante. De acuerdo con los informes de SonicWall (A11) y Check Point (A07), los ataques a dispositivos IoT se incrementaron más del 100 % en el último año, utilizando métodos cada vez más preferidos, como malware que se propaga automáticamente entre dispositivos. Un ejemplo es el malware VPNFilter, que comprometió routers domésticos en más de 50 países, permitiendo espionaje y manipulación del tráfico de red (A11). Los entornos domésticos, al no contar con sistemas de defensa avanzados, se convierten en blancos fáciles para los atacantes.

Un cuarto desafío crítico es la gestión de la privacidad. Los dispositivos IoT recopilan información sensible como rutinas, imágenes o datos biométricos que puede ser interceptada si no existen controles adecuados. Según Álvarez y Morales (A01), gran parte de esta información se transmite sin cifrado ni consentimiento explícito del usuario, violando principios

fundamentales de protección de datos personales. Casos como el hackeo de cámaras de seguridad domésticas en Estados Unidos en 2020, que expusieron transmisiones privadas en foros clandestinos, ejemplifican los riesgos de privacidad que enfrentan los hogares conectados.

Finalmente, el desconocimiento de los usuarios y la falta de alfabetización digital son barreras importantes. Muchos usuarios no son conscientes de los riesgos ni de las acciones básicas necesarias para proteger sus dispositivos, como cambiar contraseñas por defecto o segmentar la red Wi-Fi. Fernández y Gutiérrez (A03) subrayan que la educación digital debe considerarse un pilar esencial en cualquier estrategia de ciberseguridad para IoT.

En respuesta a estos desafíos, se han desarrollado soluciones que buscan mejorar la seguridad de los entornos domésticos de IoT. Los cuales tienen como objetivo mejorar la seguridad de los entornos, Entre ellas se destaca el uso de inteligencia artificial artificial para identificar comportamientos anormales y automatizar la respuesta ante incidentes (Lin Aung et al ., A08). Todas estas herramientas se están integrando cada vez más en los dispositivos domésticos, que actúan como primera línea de, por ejemplo, algunos enrutadores inteligentes ya cuentan con sistemas de detección basados en IA que bloquean el tráfico sospechoso antes de que llegue al dispositivo final. Ya contamos con sistemas de detección basados en IA que bloquean el tráfico sospechoso antes de que llegue al dispositivo final.

Asimismo, el modelo de seguridad Zero Trust ha ganado relevancia. Este enfoque exige verificación continua de identidad y control granular de acceso, incluso dentro de la red local, reduciendo la posibilidad de movimientos laterales en caso de compromiso. Empresas de ciberseguridad (A07, A11) han comenzado a ofrecer versiones adaptadas de Zero Trust para

entornos domésticos y pymes, donde cada dispositivo debe autenticarse constantemente antes de interactuar con otros.

Otra innovación prometedora es el uso de blockchain para garantizar la trazabilidad y autenticidad de las interacciones entre dispositivos (López y García, A04). Esta tecnología, aunque aún en desarrollo, permite registrar de forma inmutable las actividades del ecosistema IoT, fortaleciendo la confianza en entornos domésticos conectados. Por ejemplo, proyectos piloto han explorado el uso de blockchain para autenticar actualizaciones de firmware en dispositivos de bajo costo, reduciendo el riesgo de manipulación.

La implementación de criptografía ligera y actualizaciones remotas firmadas digitalmente significa un avance técnico sustancial. Estas herramientas facilitan la protección de dispositivos con capacidad de procesamiento restringida sin afectar su operatividad (Ley de Resiliencia Cibernética, A12). Las pruebas de laboratorio registradas en A08 y A12 han evidenciado que algoritmos de cifrado ligero, como PRESENT y SPECK, son aptos para su integración en dispositivos IoT de bajo consumo energético.

Finalmente, los marcos normativos emergentes, como la Cyber Resilience Act y la Directiva NIS2, están fomentando la instauración de certificaciones y requisitos obligatorios que buscan asegurar que los productos conectados satisfagan los estándares mínimos de ciberseguridad antes de su comercialización. Esto facilitará la disminución de la disparidad entre naciones con regulaciones avanzadas y aquellas carentes de políticas definidas de ciberseguridad para IoT.

En conjunto, estos hallazgos evidencian que, si bien los dispositivos IoT domésticos presentan múltiples vulnerabilidades, también existe un ecosistema en evolución de soluciones tecnológicas, normativas y educativas que pueden mitigar significativamente estos riesgos. La

discusión comparativa sugiere que la integración de IA, Zero Trust y blockchain, alineada con marcos normativos internacionales, constituye una ruta prometedora para fortalecer la seguridad en los hogares digitales. No obstante, el éxito de estas medidas dependerá del compromiso articulado entre fabricantes, autoridades regulatorias y usuarios para fomentar una cultura digital centrada en la seguridad.

Conclusiones

El presente trabajo ha permitido evidenciar que el Internet de las Cosas (IoT) es uno de los avances tecnológicos más significativos de la era digital , particularmente en el entorno doméstico. Sin embargo, este avance ha venido acompañado de numerosos desafíos de ciberseguridad. Que si no deabordan rigurosamente, podrían poner en peligro la privacidad, la integridad y la disponibilidad de los sistemas y los datos personales de millones de usuarios en todo el mundo.A lo largo de la investigación se identificaron problemas estructurales como la ausencia de estándares universales, la falta de actualizaciones de seguridad, las configuraciones inseguras por defecto y la escasa conciencia de los usuarios respecto a los riesgos. Estas debilidades convierten al ecosistema IoT en un objetivo frecuente y rentable para actores maliciosos, especialmente en los hogares, donde los niveles de protección son generalmente bajos.

No obstante, también se han encontrado soluciones emergentes que están redefiniendo el enfoque de la ciberseguridad en entornos IoT. Tecnologías como la inteligencia artificial, el

blockchain, la criptografía ligera y los marcos de seguridad como Zero Trust, están comenzando a integrarse en los dispositivos conectados, aportando mecanismos más eficaces para prevenir, detectar y responder a las amenazas. De igual forma, iniciativas regulatorias como la IoT Cybersecurity Improvement Act, la Directiva NIS2 y el Cyber Resilience Act representan pasos importantes hacia una mayor exigencia legal y técnica en el diseño, fabricación y uso de estos dispositivos.

En este sentido, se concluye que la protección del IoT doméstico requiere un enfoque integral que combine el diseño seguro desde el origen (security by design), el cumplimiento normativo, la educación digital de los usuarios y la innovación tecnológica constante. Solo así será posible garantizar un ecosistema conectado que sea confiable, resiliente y preparado para los desafíos actuales y futuros.

Finalmente, este trabajo busca ser una contribución a la comprensión crítica del problema y una invitación a continuar investigando y desarrollando estrategias que permitan construir entornos digitales más seguros, éticos y sostenibles en el contexto del Internet de las Cosas.

De cara al futuro, resulta indispensable impulsar investigaciones interdisciplinarias que analicen la interacción entre IoT, inteligencia artificial y 5G/6G, así como promover la creación de marcos normativos globales que reduzcan la fragmentación regulatoria. Asimismo, se hace un llamado a los fabricantes para que adopten prácticas de seguridad desde el diseño, a los reguladores para fortalecer la legislación y establecer mecanismos de verificación efectivos, y a los usuarios para aumentar su nivel de conciencia digital y adoptar medidas básicas de protección. Solo con la acción coordinada de estos actores será posible consolidar un ecosistema IoT más confiable y sostenible, capaz de responder a las demandas de un mundo cada vez más interconectado.

Referencias

Álvarez, M., & Morales, J. (2022). Privacidad de los datos en entornos IoT domésticos. Revista Latinoamericana de Tecnología y Sociedad, 9(2), 45-58.

Barrera, D., Bellman, C., & van Oorschot, P. C. (2022). Security best practices: A critical analysis using IoT as a case study. arXiv. https://arxiv.org/abs/2202.09779

Chen, L., Zhang, Y., Kumar, R., & Singh, M. (2022). Security risks in industrial IoT: A comprehensive review of real-world incidents. Journal of Cybersecurity and Privacy, 2(3), 155–172. https://doi.org/10.3390/jcp2030011

Check Point Software Technologies Ltd. (2025). Informe global de ciberataques 1T 2025.

El País. (2024, diciembre 31). 2024 bate récords históricos en ciberataques. https://elpais.com/tecnologia/2024-12-31

ElSayed, A., Farag, A., & Hussein, M. (2025). Medical IoT security: Challenges and mitigation strategies. Journal of Cybersecurity Research, 14(1), 101-118.

ElSayed, Z., Abdelgawad, A., & Elsayed, N. (2025). Cybersecurity and frequent cyber attacks on IoT devices in healthcare. arXiv. https://arxiv.org/abs/2405.08711

ENISA. (2023). Directive on security of network and information systems (NIS2). Agencia de la Unión Europea para la Ciberseguridad.

ENISA. (2023). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/nis2-directive

European Commission. (2024). Cyber Resilience Act. Comisión Europea.

Fernández, C., & Gutiérrez, L. (2023). Vulnerabilidades persistentes en dispositivos IoT: Un análisis desde la seguridad aplicativa. Revista Iberoamericana de Ingeniería, 18(1), 29-42.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Lin Aung, Y., Christian, I., Dong, Y., Ye, X., Chattopadhyay, S., & Zhou, J. (2025). Generative AI for Internet of Things Security: Challenges and Opportunities. arXiv. https://arxiv.org/abs/2404.02538

López, M., & García, R. (2023). Tendencias emergentes en ciberseguridad para entornos IoT: Inteligencia artificial y blockchain. Revista de Seguridad Informática y Tecnología, 21(1), 78–94.

Martínez, P., Ruiz, A., & Delgado, S. (2023). Casos emblemáticos de ciberataques en sistemas IoT: Implicaciones para la ciberseguridad crítica. Revista Iberoamericana de Tecnologías Emergentes, 17(2), 45–60.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

SonicWall. (2024). Cyber Threat Report 2024. SonicWall Inc.

SonicWall Capture Labs. (2024, julio). Informe de ciberamenazas de mitad de año 2024. https://www.sonicwall.com

Unit 42 (Palo Alto Networks). (2025). Informe global de respuesta a incidentes 2025. https://unit42.paloaltonetworks.com

United States Congress. (2023). IoT Cybersecurity Improvement Act of 2020. Public Law No: 116–207. https://www.congress.gov/bill/116th-congress/house-bill/1668

United States Congress. (2023). IoT Cybersecurity Improvement Act of 2022.

Wikipedia. (2025, junio). Internet of Things.

https://en.wikipedia.org/wiki/Internet_of_things*Cybersecurity Improvement Act of 2022*.

Álvarez, M., & Morales, J. (2022). Privacidad de los datos en entornos IoT domésticos. *Revista Latinoamericana de Tecnología y Sociedad, 9*(2), 45–58.

Barrera, D., Bellman, C., & van Oorschot, P. C. (2022). Security best practices: A critical analysis using IoT as a case study. *arXiv preprint*. https://arxiv.org/abs/2202.09779

Chen, L., Zhang, Y., Kumar, R., & Singh, M. (2022). Security risks in industrial IoT: A comprehensive review of real-world incidents. *Journal of Cybersecurity and Privacy, 2*(3), 155–172. https://doi.org/10.3390/jcp2030011

Check Point Software Technologies Ltd. (2025). *Informe global de ciberataques 1T 2025*. https://www.checkpoint.com

El País. (2024, 31 de diciembre). 2024 bate récords históricos en ciberataques. *El País*. https://elpais.com/tecnologia/2024-12-31

El Sayed, A., Farag, A., & Hussein, M. (2025). Medical IoT security: Challenges and mitigation strategies. *Journal of Cybersecurity Research, 14*(1), 101–118.

ElSayed, Z., Abdelgawad, A., & Elsayed, N. (2025). Cybersecurity and frequent cyber attacks on IoT devices in healthcare. *arXiv preprint*. https://arxiv.org/abs/2405.08711

ENISA. (2023). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/nis2-directive

European Commission. (2024). *Cyber Resilience Act*. Comisión Europea. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Fernández, C., & Gutiérrez, L. (2023). Vulnerabilidades persistentes en dispositivos IoT: Un análisis desde la seguridad aplicativa. *Revista Iberoamericana de Ingeniería, 18*(1), 29–42.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Lin Aung, Y., Christian, I., Dong, Y., Ye, X., Chattopadhyay, S., & Zhou, J. (2025). Generative AI for Internet of Things Security: Challenges and Opportunities. *arXiv preprint*. https://arxiv.org/abs/2404.02538

López, M., & García, R. (2023). Tendencias emergentes en ciberseguridad para entornos IoT: Inteligencia artificial y blockchain. *Revista de Seguridad Informática y Tecnología, 21*(1), 78–94.

Martínez, P., Ruiz, A., & Delgado, S. (2023). Casos emblemáticos de ciberataques en sistemas IoT: Implicaciones para la ciberseguridad crítica. *Revista Iberoamericana de Tecnologías Emergentes, 17*(2), 45–60.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks, 57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

SonicWall. (2024). *Cyber Threat Report 2024*. SonicWall Inc. https://www.sonicwall.com

SonicWall Capture Labs. (2024, julio). *Informe de ciberamenazas de mitad de año 2024*. https://www.sonicwall.com

Unit 42 (Palo Alto Networks). (2025). *Informe global de respuesta a incidentes 2025*. https://unit42.paloaltonetworks.com

United States Congress. (2020). *IoT Cybersecurity Improvement Act of 2020*. Public Law No. 116–207. https://www.congress.gov/bill/116th-congress/house-bill/1668

United States Congress. (2022). *IoT Cybersecurity Improvement Act of 2022*. Public Law No. 117–xxx. https://www.congress.gov

Wikipedia. (2025, junio). Internet of Things. *Wikipedia*. https://en.wikipedia.org/wiki/Internet_of_things