REVISTA CUBANA
DE TRANSFORMACIÓN DIGITAL

RNPS 2487 • ISSN 2708-3411
Vol. 6 • 2025 • e285

ARTÍCULO ORIGINAL

Revisión sobre la gestión de la seguridad en Internet de las Cosas

Review of security management in Internet of Things

Angel Alejandro Guerra Vilches
angelagv@uci.cu • *https://orcid.org/0009-0009-4306-1261*

Leanny Laura Duardo Polo
leannyldp@uci.cu • *https://orcid.org/0009-0003-3129-0434*

Marcos Antonio Llanes Martínez
marcosalm@uci.cu • *https://orcid.org/0009-0002-3764-3264*

Mónica Peña Casanova
monica@uci.cu • *https://orcid.org/0000-0003-2500-451*

UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Recibido: 2025-10-28 • Aceptado: 2025-12-29

RESUMEN

La seguridad en entornos de Internet de las Cosas enfrenta desafíos críticos debido al crecimiento exponencial de dispositivos, la heterogeneidad tecnológica y la constante evolución de amenazas. El objetivo de este artículo es analizar mecanismos de protección, marcos de referencia y modelos de gestión aplicados a IoT mediante revisión sistemática de literatura. Se realizó una búsqueda en las bases de datos IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink y MDPI en el período del 2022 hasta el 2025, incluyendo en este trabajo 40 publicaciones luego de un proceso de cribado en cuatro fases según criterios de inclusión y exclusión predefinidos. El análisis cualitativo descriptivo-comparativo identificó subdominios prioritarios en gestión de la seguridad IoT: privacidad, autenticación y autorización, gestión de confianza, control de políticas, detección de intrusiones, cifrado, blockchain, arquitecturas de confianza cero y cumplimiento normativo. Los resultados muestran que los enfoques más efectivos integran múltiples capas de protección, combinando autenticación ligera basada en atributos, detección mediante aprendizaje automático y gobernanza descentralizada. A partir de estos resultados, se concluye que la integración de enfoques técnicos, metodológicos y normativos proporciona mayor resiliencia y trazabilidad, aunque persisten desafíos significativos de escalabilidad, interoperabilidad y estandarización. Además, se identifican vacíos importantes en la implementación práctica a gran escala y la evaluación en entornos reales de producción.

Palabras clave: arquitecturas de confianza cero, blockchain para IoT, control de acceso basado en atributos, detección de intrusiones en IoT, gestión de seguridad en IoT.

ABSTRACT

Security in Internet of Things environments faces critical challenges due to the exponential growth of devices, technological heterogeneity, and the constant evolution of threats. The objective of this article is to analyze protection mechanisms, reference frameworks, and management models applied to IoT through a systematic literature review. A search was conducted in the IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and MDPI databases for the period from 2022 to 2025, including 40 publications in this work after a four-phase screening process according to predefined inclusion and exclusion criteria. The qualitative descriptive-comparative analysis identified priority subdomains in IoT security management: privacy, authentication and authorization, trust management, policy control, intrusion detection, encryption, blockchain, Zero Trust architectures, and regulatory compliance. The findings reveal that the most effective approaches integrate multiple layers of protection, combining lightweight attribute-based authentication, machine learning-based detection, and decentralized governance. Concluding that the integration of technical, methodological, and regulatory approaches provides greater resilience and traceability, although significant challenges of scalability, interoperability, and standardization persist. Furthermore, important gaps are identified in large-scale practical implementation and evaluation in real production environments.

Keywords: Zero Trust architectures, blockchain for IoT, attribute-based access control, intrusion detection in IoT, IoT security management.

INTRODUCCIÓN

El Internet de las Cosas (IoT) ha evolucionado hasta convertirse en una de las infraestructuras tecnológicas más relevantes para la transformación digital de la sociedad contemporánea. Su capacidad para interconectar dispositivos, sensores, sistemas de control y aplicaciones distribuidas ha permitido optimizar procesos en sectores como la salud, el transporte, la industria manufacturera, la agricultura inteligente y las ciudades inteligentes. Sin embargo, esta expansión exponencial también ha expuesto a los entornos IoT a riesgos significativos derivados de su complejidad, heterogeneidad y masificación de dispositivos, los cuales amplían la superficie de ataque y desafían los modelos de seguridad tradicionales (Aiche, Tardif, & Erritali, 2024).

La gestión de la seguridad en IoT se ha convertido en un tema central de investigación, abordando desde mecanismos de privacidad y protección de datos hasta arquitecturas de confianza, control de acceso avanzado, detección de intrusiones y modelos de gobernanza basados en blockchain (Zhou et al., 2025). Estos avances buscan responder a la creciente necesidad de garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos que circulan en redes IoT, considerando además los requerimientos regulatorios y normativos que rigen en diferentes sectores (Santos et al., 2025).

En este contexto, la literatura académica ha identificado subdominios prioritarios para la gestión de la seguridad en IoT, entre los que destacan: gestión de la privacidad, control de acceso y autenticación, autorización y registro (AAA, por sus siglas en inglés de Authentication, Authorization, and Accounting), gestión de confianza, control de políticas mediante modelos de Lenguaje Extensible de Marcado para Control de Acceso (XACML) y Control de Acceso Basado en Atributos (ABAC), sistemas de detección de intrusiones (IDS) y gestión de amenazas, cifrado y administración de llaves criptográficas, blockchain para gobernanza descentralizada, arquitecturas seguras basadas en modelos de confianza cero, y alineación normativa. Cada uno de estos subdominios presenta desafíos particulares que deben ser comprendidos y atendidos mediante enfoques integrados de gestión (Dallel, Ayed, & Tahar, 2024; Rana et al., 2023).

Diversos estudios coinciden que la seguridad en IoT no puede abordarse únicamente mediante soluciones tecnológicas aisladas, sino que requiere modelos de gestión que articulen políticas, mecanismos de control y marcos de referencia aplicables en entornos heterogéneos. Esto supone integrar dimensiones técnicas, organizacionales y regulatorias, lo cual implica un reto tanto para investigadores como para profesionales encargados de desplegar y administrar sistemas IoT en escenarios reales (Jayaweera et al., 2025; Jang et al., 2025).

El presente artículo realiza una revisión sistemática de la literatura reciente sobre gestión de la seguridad en IoT, con énfasis en los subdominios mencionados y su articulación con los modelos de gestión de redes y servicios. El objetivo general es analizar el estado del arte en gestión de la seguridad en Internet de las Cosas mediante revisión de la literatura, identificando mecanismos de protección, marcos de referencia, modelos de gestión y sus principales desafíos para determinar tendencias emergentes y vacíos en la investigación actual. Para ello se definen los siguientes objetivos específicos:

1. Identificar los subdominios prioritarios en gestión de la seguridad IoT abordados en la literatura científica reciente, analizando las vulnerabilidades más críticas y los mecanismos de protección propuestos.

2. Analizar los marcos y modelos de gestión de seguridad aplicados a IoT, describiendo sus características principales y su aplicabilidad en entornos heterogéneos y distribuidos.

3. Determinar los principales desafíos técnicos, metodológicos y normativos que limitan la implementación efectiva de soluciones de seguridad en entornos IoT.

4. Identificar vacíos en la investigación actual y proponer líneas de investigación futuras orientadas hacia soluciones integrales, escalables y validadas en entornos reales.

METODOLOGÍA

El presente trabajo corresponde a una revisión sistemática de literatura orientada a analizar la gestión de la seguridad en IoT. El enfoque metodológico empleado es cualitativo y descriptivo-comparativo, ya que se pretende sintetizar los principales hallazgos de investigaciones recientes y contrastarlos con las tendencias identificadas.

La recolección de datos se realizó en las bases IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink y MDPI (Multidisciplinary Digital Publishing Institute). Se utilizaron cadenas de búsqueda combinando términos clave como “security management”, “IoT”, “network management”, “cybersecurity”, “threats and vulnerabilities”, “models”, “framework” entre otros. Estas combinaciones permitieron obtener un corpus inicial de 1342 publicaciones, el cual fue refinado en sucesivas fases de cribado.

Para garantizar la pertinencia de los artículos seleccionados, se establecieron los siguientes criterios:

Criterios de inclusión:

- Publicaciones entre 2022 y 2025.
- Estudios empíricos que abordaran específicamente la gestión de la seguridad en IoT.
- Artículos que aplicaran, de forma explícita o implícita, principios de modelos de gestión de redes en el ámbito de IoT.
- Trabajos publicados en revistas indexadas o en conferencias internacionales reconocidas.

Criterios de exclusión:

- Publicaciones duplicadas en diferentes bases de datos.
- Documentos de carácter no científico: informes técnicos sin revisión por pares, blogs, presentaciones comerciales.
- Estudios que solo abordaran IoT desde perspectivas sin relación con la gestión o seguridad.
- Trabajos puramente teóricos sin aplicación o validación práctica.
- Publicaciones de acceso cerrado que impidieron su evaluación completa.
- Otros criterios

Proceso de selección de estudios

El procedimiento de selección se desarrolló en las cuatro fases que se detallan en la Figura 1:

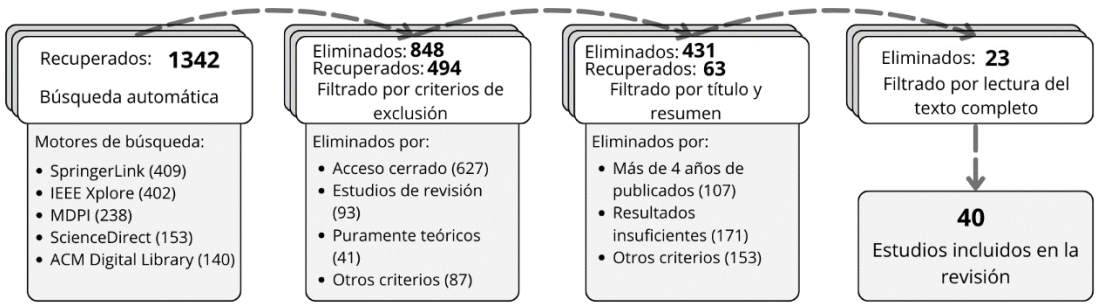

Figura 1. Procedimiento de selección de los estudios

El análisis se realizó mediante síntesis cualitativa temática, complementada con estadísticas descriptivas para identificar áreas de mayor atención científica. La Tabla 1 presenta la distribución de los 40 estudios incluidos según subdominio prioritario.

Tabla 1. Distribución de estudios por subdominio de seguridad en IoT

Subdominio	Cantidad	Porciento	Porciento acumulado
Autenticación y autorización (AAA)	9	22.5	22.5
Privacidad y protección de datos	7	17.5	40.0
Detección de intrusiones (IDS)	6	15.0	55.0
Cifrado y gestión de llaves	5	12.5	67.5
Gestión de confianza	4	10.0	77.5
Control de políticas (ABAC/XACML)	3	7.5	85.0
Blockchain para IoT	3	7.5	92.5
Zero Trust (confianza cero)	2	5.0	97.5
Cumplimiento normativo	1	2.5	100.0

Como se observa, los tres subdominios principales (AAA, privacidad, IDS) concentran el 55% de los estudios, mientras que Zero Trust (5.0%) y cumplimiento normativo (2.5%) presentan menor cobertura, sugiriendo oportunidades de investigación futura.

RESULTADOS Y DISCUSIÓN

Panorama general de la seguridad en IoT

El crecimiento del IoT ha sido exponencial en la última década, impulsado por la proliferación de dispositivos inteligentes en entornos domésticos, industriales, de transporte y salud. La literatura destaca que el número de dispositivos IoT conectados superó los 15.9 mil millones en 2023 y se proyecta que alcance más de 32.1 mil millones para 2030, lo que representa una expansión sin precedentes en la superficie de ataque. Este crecimiento genera una correlación directa entre la adopción masiva y la vulnerabilidad de los sistemas, dado que cada nuevo nodo conectado introduce un posible punto de entrada para amenazas cibernéticas (Choudhary, 2024).

Las vulnerabilidades más comunes se concentran en tres niveles: dispositivos, red y aplicaciones. A nivel de dispositivos, la limitada capacidad de procesamiento y memoria restringe la implementación de mecanismos criptográficos robustos, mientras que en la capa de red se evidencian problemas relacionados con protocolos inseguros como Message Queuing Telemetry Transport (MQTT) y el Protocolo de Aplicación Restringida (CoAP) en sus versiones no cifradas. Por su parte, en la capa de aplicación persisten deficiencias en la gestión de credenciales, almacenamiento de datos en texto plano y la ausencia de actualizaciones regulares de firmware, factores que incrementan el riesgo de ataques exitosos (Bojič Burgos & Pustišek, 2024; Dirin, Oliver, & Laine, 2023).

Un aspecto reiterado en diversos estudios es la persistencia de contraseñas débiles o predeterminadas en dispositivos IoT de bajo costo, lo que ha facilitado ataques masivos como el caso de la red de bots (botnet) Mirai en 2016, que aprovechó esta debilidad para lanzar ataques denegación de servicio distribuido (DDoS) a gran escala (Harada et al., 2022). Más recientemente, se han registrado variantes orientadas a entornos IoT industriales y de salud, como Masuta y Satori, que explotan vulnerabilidades de protocolos y configuraciones inseguras (Affinito et al., 2023).

Entre los ataques más recurrentes en IoT destacan los de DDoS, de suplantación de identidad (spoofing), intercepción de tráfico (sniffing), inyección de código y manipulación de firmware (Wang, 2025). En particular, los ataques DDoS se han visto potenciados por la capacidad de los atacantes de reclutar miles de dispositivos comprometidos en botnets, generando un impacto significativo en servicios críticos de infraestructura. Esto pone en

evidencia que la disponibilidad, uno de los pilares de la seguridad, es una de las dimensiones más comprometidas en IoT (Rouf et al., 2025; Rodríguez et al., 2022).

La literatura también resalta el riesgo asociado al manejo de datos sensibles en entornos IoT, particularmente en aplicaciones de salud y transporte. Las fugas de información personal pueden derivar en robo de identidad y riesgos para la privacidad del usuario. Estos hallazgos son consistentes con la necesidad de desarrollar marcos normativos que regulen el almacenamiento, transmisión y procesamiento de datos en entornos heterogéneos y altamente distribuidos (Orellana et al., 2024; Salehi et al., 2023).

En cuanto a tendencias emergentes, la interconexión creciente entre IoT, computación en el borde (edge computing) y 5G amplía aún más la superficie de ataque, dado que introduce nuevas dependencias tecnológicas y vectores de vulnerabilidad. Si bien estas tecnologías prometen mayor capacidad de procesamiento y latencia reducida, su integración sin mecanismos de seguridad adecuados puede intensificar los riesgos ya existentes en entornos IoT tradicionales (Lin, 2022; Michaelides et al., 2024).

En contraste, la rápida identificación de estas vulnerabilidades ha incentivado la investigación en modelos de gestión de seguridad específicos para IoT. Sin embargo, la mayoría de propuestas aún se encuentran en fases experimentales y carecen de validación a gran escala en entornos de producción (Shin et al., 2024). Esto limita la capacidad de las organizaciones para adoptar estrategias preventivas efectivas, evidenciando una brecha entre el desarrollo académico y la aplicación práctica.

Principales desafíos de seguridad En IoT

Los desafíos de seguridad en IoT son multifacéticos y se relacionan tanto con limitaciones técnicas de los dispositivos como con la diversidad de entornos de implementación. Uno de los problemas más recurrentes es la confidencialidad y privacidad, debido a que muchos nodos IoT operan con procesadores de baja capacidad y memoria reducida, lo que restringe la implementación de algoritmos criptográficos robustos (Babbar, Rani, & Shabaz, 2025; Lin et al., 2024). La adopción de métodos de cifrado ligero, mejora la eficiencia energética sin comprometer excesivamente la seguridad; sin embargo, aún se observan brechas significativas cuando los dispositivos deben interoperar con sistemas más complejos basados en el protocolo de Seguridad de la Capa de Transporte (TLS) o Seguridad de la Capa de Transporte de Datagramas (DTLS) (Höglund et al., 2024).

En lo que respecta a la integridad y disponibilidad, los ataques de DDoS en entornos IoT siguen siendo una de las principales amenazas, particularmente en arquitecturas de red distribuidas. Además, la fragmentación del tráfico y el uso de técnicas de spoofing continúan desafiando los mecanismos tradicionales de mitigación en redes IoT. En adición, la disponibilidad se ve comprometida por la limitada capacidad de los dispositivos para ejecutar procesos de recuperación ante incidentes, lo que genera puntos críticos en escenarios de ciudades inteligentes o aplicaciones industriales (Yang W. et al., 2025; Fotse et al., 2025).

La autenticación y el control de acceso representan otro desafío central. Diversos estudios muestran que las credenciales predeterminadas y la ausencia de gestión de identidades son responsables de la mayoría de intrusiones en dispositivos IoT (Alazab et al., 2024; Ali et al., 2022). Modelos como OAuth 2.0 o protocolos de autenticación ligeros se han propuesto como soluciones, pero su adopción ha sido parcial debido a la falta de estandarización y la dificultad de implementación en dispositivos heterogéneos (Alzahrani, 2025).

El problema de la escalabilidad y heterogeneidad es otro reto ampliamente discutido en la literatura. La proliferación de dispositivos con diferentes sistemas operativos, protocolos de comunicación y niveles de seguridad

dificulta la aplicación de políticas unificadas. Según Chaganti (2025), esta diversidad genera problemas para la interoperabilidad segura, especialmente en entornos donde conviven dispositivos legados con nuevas generaciones más seguras. Además, la gestión centralizada se ve limitada por la sobrecarga que implica monitorear y aplicar actualizaciones a millones de nodos distribuidos en entornos como transporte, salud y energía (Junior et al., 2025).

Un aspecto transversal es la limitación de recursos en la mayoría de dispositivos IoT. Las restricciones de energía, procesamiento y almacenamiento condicionan la adopción de mecanismos avanzados de seguridad. Por ejemplo, algoritmos de aprendizaje automático para detección de intrusiones requieren procesamiento en edge o fog computing, ya que la ejecución directa en sensores es inviable. Esto abre un debate sobre la dependencia de la nube y el impacto en la privacidad, dado que los datos deben transmitirse a infraestructuras externas para su análisis (Nguyen et al., 2025; Lin et al., 2024).

Por otra parte, la fragmentación normativa y regulatoria es otro desafío en la gestión de la seguridad en IoT. Mientras organismos como organismos como Grupo de Trabajo en Ingeniería de Internet (IETF), Instituto Europeo de Normas de Telecomunicaciones (ETSI) y Instituto Nacional de Estándares y Tecnología (NIST) han desarrollado guías para la seguridad en IoT, su implementación en sectores industriales y domésticos es todavía desigual. La ausencia de estándares globales vinculantes favorece la existencia de dispositivos inseguros en el mercado, lo que amplifica los riesgos (Brancati et al., 2025).

La combinación de estos desafíos genera una superficie de ataque en expansión y un ecosistema con vulnerabilidades difíciles de mitigar bajo los enfoques tradicionales de ciberseguridad. El avance hacia arquitecturas distribuidas de gestión, mecanismos de autenticación descentralizados y modelos de confianza cero (Zero Trust) representan posibles soluciones, aunque aún se encuentran en fases iniciales de investigación y estandarización.

Marcos y modelos para la gestión de la seguridad en IoT

La gestión de la seguridad en entornos IoT se ha abordado a partir de diferentes marcos conceptuales y normativos, algunos heredados de la gestión de redes tradicional y otros diseñados específicamente para ecosistemas distribuidos. El modelo FCAPS (Fault, Configuration, Accounting, Performance, Security), ampliamente utilizado en telecomunicaciones, sigue siendo un referente de partida, pues proporciona una estructura integral que permite mapear funciones de seguridad a las operaciones de administración de red. Sin embargo, FCAPS, en su forma original, resulta insuficiente para escenarios IoT caracterizados por alta heterogeneidad, movilidad y restricciones de recursos. En consecuencia, su implementación se ha adaptado reforzando el dominio de seguridad con mecanismos de confianza y control de acceso más dinámicos (Peoples et al., 2022; Mekrache et al., 2024).

Paralelamente, han cobrado relevancia los marcos basados en políticas, como los que implementan ABAC y su estandarización mediante XACML. Estos se valoran por su capacidad de aplicar controles granulares y contextuales, permitiendo administrar el acceso de forma más flexible en dispositivos de baja potencia. Si bien su adopción mejora la capacidad de respuesta frente a cambios contextuales, el sobrecoste computacional sigue siendo una limitación en nodos restringidos (Shin et al., 2024; Pathak et al., 2023).

Además de FCAPS y ABAC/XACML, otros modelos han emergido específicamente para abordar los desafíos de IoT. La Tabla 1 presenta una comparación de los principales marcos y modelos de gestión de seguridad aplicados a IoT, contrastando su origen, características, ventajas, limitaciones y nivel de adopción actual. Esta comparación permite apreciar que no existe un modelo único óptimo para todos los escenarios IoT, sino que la selección apropiada depende de factores como la criticidad de la aplicación, las restricciones de recursos, los requisitos regulatorios y las prioridades específicas de seguridad (confidencialidad, integridad, disponibilidad, trazabilidad).

Tabla 1. Comparación de marcos y modelos de gestión de seguridad en IoT

Marco/Modelo	Características principales	Ventajas en IoT	Limitaciones en IoT	Nivel de adopción	Referencias
FCAPS	Modelo integral: fallos, configuración, contabilidad, rendimiento y seguridad	Estructura probada, Mapeo claro de funciones, Facilita auditoría	Diseñado para redes homogéneas, Gestión centralizada poco escalable, Requiere adaptaciones para la heterogeneidad IoT	Medio (adoptado principalmente en IoT industrial con adaptaciones)	Peoples et al. (2022); Mekrache et al. (2024)
ABAC/ XACML	Control granular basado en atributos contextuales (usuario, dispositivo, entorno, tiempo)	Políticas dinámicas y flexibles, Adaptación a contextos cambiantes, Control fino de permisos	Alto coste computacional, Complejidad en la definición de políticas, Sobrecarga en dispositivos muy restringidos	Medio–Alto (aplicable en dispositivos con capacidad moderada)	Pathak et al. (2023); Shin et al. (2024)
Zero Trust	Verificación continua, ausencia de confianza implícita, microsegmentación y privilegio mínimo	Elimina la confianza implícita, Reduce la superficie de ataque, Efectivo frente a amenazas internas	Complejidad operativa elevada, Requiere infraestructura de identidad robusta, Incremento de latencia por verificaciones repetidas	Medio (aplicable en IoT crítico con recursos suficientes)	Son et al. (2024); Nguyen et al. (2025)
Blockchain	Registro inmutable y descentralizado con trazabilidad y contratos inteligentes	Inmutabilidad de registros, Gobernanza descentralizada, Alta resistencia a la manipulación	Latencia elevada (≈200–500 ms adicionales), Consumo energético alto (incremento del 30–40%), Escalabilidad limitada para operaciones en tiempo real	Bajo–Medio (adecuado para auditoría y trazabilidad, no para operaciones RT)	Zhou et al. (2025); Cao et al. (2024); Dallel et al. (2024)
AAA ligero	Autenticación, autorización y auditoría optimizadas para dispositivos con recursos limitados	Optimizado para baja capacidad, Reduce sobrecarga de autenticación, Mejora la trazabilidad	Menor robustez que protocolos completos, Requiere gestión centralizada, Vulnerable sin cifrado complementario	Alto (diseñado específicamente para entornos IoT)	Alzahrani (2025); Jang et al. (2025)
Aprendizaje federado para IDS	Detección de intrusiones colaborativa sin centralización de datos sensibles	Preserva la privacidad de los datos, Detección distribuida y resiliente, Reduce la transferencia de datos	Requiere capacidad de procesamiento en el Edge, Dependencia de la calidad de los datos	Medio (en expansión; dependiente de *edge computing*)	Yang et al. (2025); Fotse et al. (2025);

Marco/Modelo	Características principales	Ventajas en IoT	Limitaciones en IoT	Nivel de adopción	Referencias
			locales, Sincronización de modelos compleja		Jayaweera et al. (2025)

Como se evidencia en la Tabla 1, los marcos tradicionales como FCAPS requieren adaptaciones significativas para ser viables en IoT, mientras que enfoques más recientes como blockchain y aprendizaje federado ofrecen capacidades innovadoras pero enfrentan desafíos de madurez tecnológica y escalabilidad. La tendencia identificada en la literatura apunta hacia enfoques híbridos que combinan múltiples principios (por ejemplo, ABAC con blockchain, o Zero Trust con aprendizaje federado) para balancear las compensaciones inherentes entre seguridad, rendimiento y escalabilidad (Malik et al., 2023; Pathak et al., 2023; Son et al., 2024).

A su vez, se observa un esfuerzo por alinear los marcos de seguridad IoT con estándares regulatorios internacionales. El cumplimiento normativo no solo depende de la implementación técnica, sino de la capacidad de los marcos para traducir requerimientos legales en políticas operativas y medibles. Esto refuerza la idea de que un único modelo no es suficiente; más bien se requiere un enfoque híbrido que combine varios principios como FCAPS, Zero Trust, ABAC o blockchain, articulados bajo marcos regulatorios vigentes (Malik et al., 2023; Shin et al., 2024; Pathak et al., 2023; Son et al., 2024; Cao et al., 2024).

Convergencias, divergencias y soluciones propuestas

El análisis de los estudios incluidos revela consensos y enfoques diferenciados en gestión de seguridad IoT. En autenticación y control de acceso existe convergencia en identificar credenciales predeterminadas como vulnerabilidad crítica (Alazab et al., 2024; Ali et al., 2022; Alzahrani, 2025). Frente a esto, emergen dos líneas: protocolos ligeros específicos que optimizan consumo energético (Alzahrani, 2025; Jang et al., 2025) versus adaptación de estándares consolidados como EDHOC y OSCORE priorizando interoperabilidad (Höglund et al., 2024). Los protocolos ligeros ofrecen mejor rendimiento en dispositivos de muy baja capacidad pero requieren nuevas infraestructuras; los estándares garantizan compatibilidad inmediata aunque pueden resultar excesivos para sensores restrictivos.

En detección de intrusiones, los autores coinciden en la efectividad del aprendizaje automático pero difieren en arquitecturas: Yang et al. (2025) presentan técnicas híbridas validadas en redes RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) simuladas; Fotse et al. (2025) priorizan aprendizaje federado en tráfico real preservando privacidad; Rodríguez et al. (2022) proponen transferencia de aprendizaje reduciendo requerimientos de datos etiquetados. Estas diferencias reflejan prioridades distintas: precisión, privacidad y eficiencia. La limitación compartida es la dependencia de datos etiquetados representativos, limitando generalización a nuevos ataques.

Respecto a blockchain, existe consenso en ventajas (trazabilidad, inmutabilidad) y limitaciones (latencia, consumo energético) (Zhou et al., 2025; Cao et al., 2024; Dallel et al., 2024). Dallel et al. (2024) proponen arquitecturas híbridas registrando solo eventos críticos en blockchain, balanceando inmutabilidad con rendimiento, aunque requieren validación en despliegues masivos.

En Zero Trust, los estudios reconocen efectividad para reducir superficie de ataque (Son et al., 2024; Nguyen et al., 2025), pero difieren en implicaciones: Son reporta mejoras en resiliencia en 6G-IoT, mientras Nguyen advierte

sobre sobrecarga en aplicaciones de baja latencia. Como solución, Nguyen propone verificación adaptativa ajustando frecuencia según perfil de riesgo.

Un debate recurrente es la disyuntiva centralización/descentralización. Chaganti (2025) y Malik et al. (2023) favorecen arquitecturas distribuidas por resiliencia y privacidad; Brancati et al. (2025) señalan que entornos industriales regulados requieren auditoría centralizada para cumplir con certificaciones internacionales como IEC 62443 (estándar de ciberseguridad para sistemas de automatización y control industrial) o ISO/IEC 27001 (gestión de seguridad de la información). Ambos enfoques son válidos según dominio: sectores regulados requieren trazabilidad centralizada; ciudades inteligentes y agricultura se benefician de descentralización. Malik et al. (2023) proponen solución híbrida: gestión centralizada de políticas con ejecución descentralizada mediante contratos inteligentes.

En gestión de llaves criptográficas, los autores coinciden en la necesidad de algoritmos optimizados y en que distribución/revocación en redes masivas representa desafío significativo (Rana et al., 2023; Salehi et al., 2023; Lin et al., 2024). Rana propone sistemas jerárquicos específicos IoT; Salehi explora esquemas basados en identidad eliminando infraestructuras complejas de clave pública. Ambos enfoques buscan reducir complejidad operativa aunque presentan compromisos diferentes en sobrecarga y vulnerabilidades residuales.

La Tabla 2 sintetiza estas convergencias, divergencias y soluciones propuestas en los seis subdominios analizados, evidenciando que la gestión de seguridad IoT es un campo con debates metodológicos activos donde coexisten enfoques legítimos que priorizan diferentes dimensiones según contexto de aplicación.

Tabla 2. Síntesis de convergencias, divergencias y soluciones propuestas en gestión de seguridad IoT

Subdominio	Consenso identificado	Enfoques divergentes	Autores (posiciones)	Solución propuesta	Referencia
Autenticación y control de acceso	Las credenciales predeterminadas constituyen una vulnerabilidad crítica	Protocolos ligeros específicos para IoT vs. adaptación de estándares consolidados	Alzahrani, Jang (protocolos ligeros) vs. Höglund (estándares EDHOC/OSCORE)	Definición de perfiles de autenticación adaptativos según la capacidad del dispositivo	Höglund et al. (2024)
Detección de intrusiones	Eficacia general del aprendizaje automático para IDS en IoT	Precisión en entornos simulados vs. privacidad mediante aprendizaje federado vs. eficiencia con transferencia de aprendizaje	Yang (modelos híbridos) vs. Fotse (federado) vs. Rodríguez (transferencia)	Arquitecturas híbridas con detección local y refinamiento colaborativo	Rodríguez et al. (2022)
Blockchain	Aporta trazabilidad e inmutabilidad; penaliza latencia y consumo energético	No se identifican divergencias significativas (consenso sobre las limitaciones)	Zhou, Cao, Dallel (consenso)	Arquitecturas híbridas *off-chain* con registro en blockchain solo de eventos críticos	Dallel et al. (2024)
Zero Trust	Reduce eficazmente la superficie de ataque	Incremento de resiliencia vs. sobrecarga en	Son (efectividad en 6G-IoT) vs. Nguyen	Verificación adaptativa basada	Nguyen et al. (2025)

Subdominio	Consenso identificado	Enfoques divergentes	Autores (posiciones)	Solución propuesta	Referencia
		escenarios de baja latencia	(impacto en latencia)	en perfiles de riesgo contextual	
Gestión (centralización)	Centralización y distribución son válidas según el contexto	Gestión distribuida (resiliencia, privacidad) vs. centralización (cumplimiento normativo)	Chaganti, Malik (distribuida) vs. Brancati (centralizada)	Arquitectura híbrida: políticas centralizadas y ejecución descentralizada	Malik et al. (2023)
Gestión de llaves criptográficas	La distribución y revocación de llaves en redes masivas sigue siendo un desafío abierto	Sistemas jerárquicos vs. esquemas basados en identidad sin certificados	Rana (jerárquicos) vs. Salehi (sin certificados)	Selección del esquema según escenario; no existe una solución universal	Rana et al. (2023); Salehi et al. (2023)

Como se observa en la Tabla 2, algunos subdominios presentan consenso sobre problemas y limitaciones (blockchain), mientras que otros evidencian enfoques genuinamente divergentes (autenticación, detección, gestión). Las soluciones propuestas tienden hacia enfoques adaptativos e híbridos que balancean compensaciones inherentes.

Síntesis de tendencias integradas

La seguridad en entornos IoT evoluciona hacia modelos integrados que combinan criptografía ligera, aprendizaje federado, gestión automatizada de políticas y tecnologías distribuidas. El cifrado adaptado a dispositivos con recursos limitados mejora confidencialidad, aunque persiste vulnerabilidad ante ataques de correlación de metadatos y explotación de patrones, resaltando la necesidad de combinar medidas técnicas con políticas de protección de datos y anonimización.

Los protocolos AAA ligeros y basados en atributos han mostrado mejoras en gestión de identidades y control de acceso en entornos heterogéneos. La integración de auditoría y contabilidad fortalece trazabilidad de eventos críticos, aunque persisten limitaciones de escalabilidad y complejidad operativa, indicando que la adopción masiva requiere automatización avanzada y estandarización.

Los mecanismos de detección de anomalías basados en aprendizaje automático y arquitecturas híbridas evidencian aumento en precisión frente a ataques DDoS y manipulación de firmware. La integración de análisis en el borde y procesamiento colaborativo mejora detección temprana y respuesta a incidentes, aunque la dependencia de datos etiquetados de calidad puede generar falsos positivos en escenarios de alta heterogeneidad.

La gestión automatizada de llaves criptográficas contribuye a la resiliencia, superando desafíos de provisión manual y reduciendo errores humanos. Sin embargo, la escalabilidad en entornos masivos sigue siendo desafío donde heterogeneidad de dispositivos puede generar vulnerabilidades si no se diseñan protocolos tolerantes a errores.

Las tecnologías distribuidas y blockchain ofrecen trazabilidad, gobernanza y auditoría, mejorando confianza en entornos IoT. Las soluciones híbridas reducen latencia y consumo energético, aunque persisten limitaciones en revocación rápida de permisos e integración con sistemas de tiempo real.

Los principios de Zero Trust emergen como marco efectivo para verificación continua, segmentación de redes y ajuste dinámico de políticas, aumentando resiliencia ante amenazas internas y externas. La aportación central es la reducción de exposición a compromisos internos, aunque la complejidad operativa y necesidad de monitoreo constante en dispositivos de baja capacidad representan limitaciones.

La alineación con estándares internacionales continúa siendo desafío por fragmentación normativa y diversidad tecnológica. La integración de políticas automatizadas, auditoría y trazabilidad mejora cumplimiento de marcos como el Reglamento General de Protección de Datos (GDPR) u otros propuestos el NIST, el IETF o el ETSI, fortaleciendo gobernanza y consistencia, aunque la aplicación uniforme en redes IoT distribuidas y dinámicas sigue siendo difícil.

CONCLUSIONES

La presente revisión permitió constatar que la gestión de la seguridad en IoT constituye un desafío multidimensional que exige soluciones técnicas, organizacionales y normativas integradas. Entre los principales aportes del trabajo se encuentra la identificación de tendencias emergentes, como la aplicación de aprendizaje federado para detección de intrusiones, blockchain para gobernanza distribuida y Zero Trust para minimizar superficies de ataque, que en conjunto ofrecen un marco robusto para afrontar la complejidad de los entornos IoT. Asimismo, se evidenció que los modelos actuales de gestión tienden a enfocarse en capas o dominios específicos, sin lograr todavía una integración práctica y escalable en sistemas reales.

En términos de limitaciones, los estudios revisados muestran carencias en tres aspectos fundamentales: (i) la escalabilidad de las soluciones propuestas en entornos de gran magnitud y heterogeneidad, (ii) la interoperabilidad entre dispositivos y plataformas bajo estándares comunes, y (iii) la validación empírica en contextos de producción, más allá de simulaciones o prototipos controlados.

A partir de estas brechas, se definen las siguientes líneas de investigación futura:

- Escalabilidad y eficiencia energética: desarrollo de mecanismos de seguridad que sean sostenibles en dispositivos con recursos limitados, incluyendo algoritmos de cifrado y autenticación ligeros y optimizados para IoT.
- Interoperabilidad y estandarización: diseño de marcos de gestión de seguridad que aseguren compatibilidad entre plataformas heterogéneas y garanticen cumplimiento de normativas globales.
- Integración de tecnologías emergentes: evaluación práctica del potencial de blockchain, federated learning y Zero Trust como pilares complementarios de gobernanza y protección en IoT, priorizando casos de uso industriales y críticos.
- Automatización y orquestación inteligente: desarrollo de arquitecturas de gestión basadas en inteligencia artificial para la toma de decisiones autónoma en tiempo real, particularmente en la respuesta a incidentes.
- Modelos de gobernanza y cumplimiento normativo: creación de marcos regulatorios y políticas adaptativas que permitan balancear seguridad, privacidad y usabilidad, considerando regulaciones emergentes como GDPR, NIS2 y marcos sectoriales.

- Validación en entornos reales: realización de estudios longitudinales en escenarios de producción (transporte, salud, energía, ciudades inteligentes) que permitan medir la efectividad, costos y limitaciones de las soluciones propuestas.

Este artículo contribuye al campo al ofrecer una visión crítica y sistematizada de los avances y vacíos en la gestión de la seguridad IoT, orientando las futuras investigaciones hacia la integración práctica, la gobernanza distribuida y la sostenibilidad de las soluciones. De esta manera, se sientan bases sólidas tanto para la comunidad científica como para la industria en la construcción de ecosistemas IoT más confiables y resilientes.

REFERENCIAS

Peoples, C., Moore, A., Zoualfaghari, M., Kulkarni, P., & Abu-Tair, M. (2022). Chapter 24—Customizable service level agreement (SLA) generator platform using FCAPS management to enhance Quality of Experience (QoE) on Internet of Things (IoT). In J. R.Vacca (Ed.), Smart Cities Policies and Financing (pp. 335–351). Elsevier. https://doi.org/10.1016/B978-0-12-819130-9.00032-2

Mekrache,A., Ksentini,A., & Verikoukis,C. (2024). Machine Learning in FCAPS: Toward Enhanced Beyond 5G Network Management. IEEE Communications Surveys & Tutorials, 26(4), 2769–2797. https://doi.org/10.1109/COMST.2024.3395414

Aiche, A., Tardif, P.-M., & Erritali, M. (2024). Modeling Trust in IoT Systems for Drinking-Water Management. Future Internet, 16(8), 273. https://doi.org/10.3390/fi16080273

Santos, C. E. M., Correia Filho, P. T. de J., Canciglieri Junior, O., & Schaefer, J. L. (2025). The role of integrated information management systems in the relationship between product lifecycle management and Industry 4.0 technologies and market performance. Sustainability, 17(12), 5260. https://doi.org/10.3390/su17125260

Zhou, H., Gao, H., Ma, Z., & Lai, G. (2025). Blockchain-based trusted data management with privacy preservation for secure IoT systems. Sensors, 25(14), 4344. https://doi.org/10.3390/s25144344

Dallel, O., Ayed, S. B., & Tahar, J. B. H. (2024). Blockchain-based authorization mechanism for educational social Internet of Things. IEEE Access, 12, 42888–42907. https://doi.org/10.1109/ACCESS.2024.3379300

Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers. Sensors, 23(18), 7678. https://doi.org/10.3390/s23187678

Jayaweera, R., Agrawal, H., & Karie, N. M. (2025). Federated Security for Privacy Preservation of Healthcare Data in Edge-Cloud Environments. Sensors, 25(16), 5108. https://doi.org/10.3390/s25165108

Jang, H., Choi, J., Son, S., Kwon, D., & Park, Y. (2025). Provably Secure and Privacy-Preserving Authentication Scheme for IoT-Based Smart Farm Monitoring Environment. Electronics, 14(14), 2783. https://doi.org/10.3390/electronics14142783

Choudhary, A. (2024). Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discover Internet of Things, 4(1), 31. https://doi.org/10.1007/s43926-024-00084-3

Bojič Burgos, J., & Pustišek, M. (2024). Decentralized IoT Data Authentication with Signature Aggregation. Sensors, 24(3), 1037. https://doi.org/10.3390/s24031037

Dirin, A., Oliver, I., & Laine, T. H. (2023). A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems. Sensors, 23(17), 7532. https://doi.org/10.3390/s23177532

Harada, R., Tanaka, K., Suzuki, Y., & Nakamura, H. (2022). Quick suppression of DDoS attacks by frame priority control in IoT backhaul with construction of Mirai-based attacks. IEEE Access, 10, 22392–22399. https://doi.org/10.1109/ACCESS.2022.3153067

Affinito, A., Zinno, S., Stanco, G., Botta, A., & Ventre, G. (2023). The evolution of Mirai botnet scans over a six-year period. Journal of Information Security and Applications, 79, 103629. https://doi.org/10.1016/j.jisa.2023.103629

Wang, S. (2025). Network security protection model of electric power information system based on hierarchical weight pruning algorithm optimizing OD-CNN algorithm. Journal of Cyber Security and Mobility, 14(3), 673–700. https://doi.org/10.13052/jcsm2245-1439.1437

Rouf, M. A., Silvia, A. R., Roy, M. K., Das, S. K., & Chaity, S. K. (2025). Proposing a framework to prevent Distributed Denial of Service (DDoS) attacks on IoT devices. Proceedings of the 3rd International Conference on Computing Advancements (ICCA ’24), 1066–1073. Association for Computing Machinery. https://doi.org/10.1145/3723178.3723319

Rodríguez, E., Valls, P., Otero, B., Costa, J. J., Verdú, J., Pajuelo, M. A., & Canal, R. (2022). Transfer-Learning-Based Intrusion Detection Framework in IoT Networks. Sensors, 22(15), 5621. https://doi.org/10.3390/s22155621

Orellana, C., Cereceda-Balic, F., Solar, M., & Astudillo, H. (2024). Enabling Design of Secure IoT Systems with Trade-Off-Aware Architectural Tactics. Sensors, 24(22), 7314. https://doi.org/10.3390/s24227314

Salehi Shahraki, A., Lauer, H., Grobler, M., Sakzad, A., & Rudolph, C. (2023). Access Control, Key Management, and Trust for Emerging Wireless Body Area Networks. Sensors, 23(24), 9856. https://doi.org/10.3390/s23249856

Lin, T.-W. (2022). A Privacy-Preserved ID-Based Secure Communication Scheme in 5G-IoT Telemedicine Systems. Sensors, 22(18), 6838. https://doi.org/10.3390/s22186838

Michaelides, S., Mucke, J., & Henze, M. (2025). Assessing the Latency of Network Layer Security in 5G Networks. In 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 262–267). ACM. https://doi.org/10.1145/3734477.3734722

Nguyen, P., Nguyen, H.-H., Phung, P., Truong, H.-L., & Cheung, T. (2025). Advanced context-sensitive access management for edge-driven IoT data sharing as a service. ACM Transactions on Internet Technology, 25(2), Article 9, 1–31. https://doi.org/10.1145/3721430

Lin, H.-Y., Tsai, T.-T., Ting, P.-Y., & Chan, P.-C. (2024). CL-SML: Secure certificateless signature with message linkages for IoT-based fog computing environments. Proceedings of the 2023 5th International Conference on Big-Data Service and Intelligent Computation (BDSIC ’23) (pp. 9–15). Association for Computing Machinery. https://doi.org/10.1145/3633624.3633626

Shin, S., Park, M., Kim, T., & Yang, H. (2024). Architecture for Enhancing Communication Security with RBAC IoT Protocol-Based Microgrids. Sensors, 24(18), 6000. https://doi.org/10.3390/s24186000

Babbar, H., Rani, S., & Shabaz, M. (2025). Federated learning with enhanced cryptographic security for vehicular cyber-physical systems. Scientific Reports, 15, 28593. https://doi.org/10.1038/s41598-025-14341-0

Höglund, R., Tiloca, M., Selander, G., Mattsson, J. P., Vučinić, M., & Watteyne, T. (2024). Secure communication for the IoT: EDHOC and (group) OSCORE protocols. IEEE Access, 12, 49865–49877. https://doi.org/10.1109/ACCESS.2024.3384095

Yang, W., Wang, X., Zhang, Z., Chen, S., Hou, C., & Luo, S. (2025). Intrusion detection using hybrid Pearson correlation and GS-PSO optimized random forest technique for RPL-based IoT. IEEE Access, 13, 78320–78334. https://doi.org/10.1109/ACCESS.2025.3566368

Fotse, Y. S. N., Tchendji, V. K., & Velempini, M. (2025). Federated learning based DDoS attacks detection in large scale software-defined network. IEEE Transactions on Computers, 74(1), 101–115. https://doi.org/10.1109/TC.2024.3474180

Ali, W., Din, I. U., Almogren, A., & Kim, B. S. (2022). A Novel Privacy Preserving Scheme for Smart Grid-Based Home Area Networks. Sensors (Basel, Switzerland), 22(6), 2269. https://doi.org/10.3390/s22062269

Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., & Alturki, R. (2024). A Novel IDS with a Dynamic Access Control Algorithm to Detect and Defend Intrusion at IoT Nodes. Sensors (Basel, Switzerland), 24(7), 2188. https://doi.org/10.3390/s24072188

Yang, Z., Chen, X., He, Y., Liu, L., Che, Y., Wang, X., Xiao, K., & Xu, G. (2024). An attribute-based access control scheme using blockchain technology for IoT data protection. High-Confidence Computing, 4(3), 100199. https://doi.org/10.1016/j.hcc.2024.100199

Alzahrani, N. (2025). A verifiably secure and lightweight device-to-device (D2D) authentication protocol for the resource-constrained IoT networks. IEEE Access, 13, 92982–92996. https://doi.org/10.1109/ACCESS.2025.3568692

Chaganti, K. C. (2025). A scalable, lightweight AI-driven security framework for IoT ecosystems: Optimization and game theory approaches. IEEE Access, 13, 72235–72247. https://doi.org/10.1109/ACCESS.2025.3558623

Junior, N. F., Silva, A. A. A. d., Guelfi, A. E., Ueda, E. T., & Kofuji, S. T. (2025). FedSensor: Federated learning framework for secure sensor-based IoT at the extreme edge. IEEE Access, 13, 136945–136969. https://doi.org/10.1109/ACCESS.2025.3595490

Brancati, F., Mongelli, D., Mariotti, F., Ceccarelli, A., Bondavalli, A., & Buonanno, L. (2025). A cybersecurity risk assessment methodology for industrial automation control systems. International Journal of Information Security, 24(1), 76. https://doi.org/10.1007/s10207-025-00990-9

Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2023). TABI: Trust-based ABAC mechanism for Edge-IoT using blockchain technology. IEEE Access, 11, 36379–36398. https://doi.org/10.1109/ACCESS.2023.3265349

Son, S., Kwon, D., Lee, S., Kwon, H., & Park, Y. (2024). A zero-trust authentication scheme with access control for 6G-enabled IoT environments. IEEE Access, 12, 154066–154079. https://doi.org/10.1109/ACCESS.2024.3484522

Cao, Y., Li, J., Chao, K., Xiao, J., & Lei, G. (2024). Blockchain meets generative behavior steganography: A novel covert communication framework for secure IoT edge computing. Chinese Journal of Electronics, 33(4), 886–898. https://doi.org/10.23919/cje.2023.00.382

Yang, Y.-C., Lu, K.-F., Chen, Y.-X., & Tsay, R.-S. (2025). Ensuring GDPR compliance in IoT network with a glass box security guard system. IEEE Transactions on Privacy, 2, 27–40. https://doi.org/10.1109/TP.2025.3546854

Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B. R., Goyal, S. B., Martin, R. J., Srinivasan, K., & Mittal, A. (2023). Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. IEEE Access, 11, 70110–70131. https://doi.org/10.1109/ACCESS.2023.3293529