TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

AMENAZAS DE SEGURIDAD Y SUS SOLUCIONES EN EL INTERNET DE LAS COSAS (IoT)

SECURITY THREATS AND THEIR SOLUTIONS IN THE INTERNET OF THINGS (IoT)

AMEAÇAS À SEGURANÇA E SUAS SOLUÇÕES NA INTERNET DAS COISAS (IoT)

Ing. Rocío Mendoza Villamar
rocio.mendoza@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí, ext. El Carmen
Orcid: 0000-0002-1277-7162

Oscar Prado Vera
pradokevin486@gmail.com
Universidad Laica Eloy Alfaro de Manabí, ext. El Carmen
Orcid: 0009-0007-4210-1079

Sheily Coveña Coveña
sheycovenacovena@gmail.com
Universidad Laica Eloy Alfaro de Manabí, ext. El Carmen
Orcid: 0009-0003-5918-8466

REVISTA TSE´DE
Instituto Superior Tecnológico Tsa´chila
ISSN: 2600-5557

Resumen

El estudio se desarrolló ante la creciente vulnerabilidad del Internet de las Cosas (IoT), cuya expansión tecnológica ha incrementado los riesgos de ciberseguridad en dispositivos. El objetivo fue analizar las principales amenazas y proponer soluciones basadas en tecnologías emergentes para fortalecer la protección de la información. Se adoptó un enfoque mixto, basado en diseño no experimental y de tipo descriptivo, integrando el análisis cualitativo de los riesgos con la evaluación cuantitativa de amenazas identificadas en documentos académicos y técnicos. Los resultados mostraron que las vulnerabilidades más comunes están relacionadas con contraseñas débiles, software desactualizado y configuraciones inseguras, afectando la confidencialidad de los datos. También se determinó que la aplicación de cifrado, autenticación multifactor y tecnología blockchain reduce de manera significativa los riesgos detectados. En conclusión, la ciberseguridad en el IoT depende del avance tecnológico, la educación digital y la implementación de políticas públicas que promuevan un ecosistema seguro y sostenible.

Palabras clave: autenticación; ciberseguridad; dispositivos inteligentes; blockchain; vulnerabilidades

TSE'DE
Revista de Investigación Científica
ISSN 2600 - 5557

Abstract

This study was conducted in response to the growing vulnerability of the Internet of Things (IoT), whose technological expansion has increased cybersecurity risks in connected devices. The objective was to analyze the main threats and propose solutions based on emerging technologies to strengthen information protection. A mixed approach was adopted, based on a non-experimental and descriptive design, integrating qualitative analysis of risks with quantitative evaluation of threats identified in academic and technical documents. The results showed that the most common vulnerabilities are related to weak passwords, outdated software, and insecure configurations, which affect data confidentiality. It was also determined that the application of encryption, multi-factor authentication, and blockchain technology significantly reduces the risks detected. In conclusion, IoT cybersecurity depends on technological progress, digital education, and the implementation of public policies that promote a secure and sustainable ecosystem capable of supporting protection measures aligned with current needs and future technological challenges.
Keywords: authentication; blockchain; cybersecurity; intelligent devices; vulnerabilities

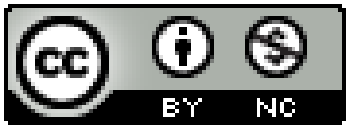
Resumo

Este estudo foi conduzido em resposta à crescente vulnerabilidade da Internet das Coisas (IoT), cuja expansão tecnológica aumentou os riscos de cibersegurança em dispositivos conectados. Seu objetivo foi analisar as principais ameaças e propor soluções baseadas em tecnologias emergentes que fortaleçam a proteção da informação. Adotou-se uma abordagem de métodos mistos, com um delineamento descritivo não experimental, integrando análise qualitativa de riscos com uma avaliação quantitativa da frequência de ameaças e soluções identificadas em documentos acadêmicos e técnicos relevantes. Os resultados mostraram que as vulnerabilidades mais comuns estão relacionadas a senhas fracas, softwares desatualizados e configurações inseguras, que afetam a confidencialidade e a disponibilidade dos dados. Além disso, constatou-se que a aplicação de criptografia, autenticação multifatorial e tecnologia blockchain reduz significativamente os riscos detectados. Em conclusão, a cibersegurança na IoT depende de avanços tecnológicos, alfabetização digital e da implementação de políticas públicas que promovam um ecossistema seguro, confiável e verdadeiramente sustentável.
Palavras-chave: autenticação; blockchain; cibersegurança; dispositivos inteligentes; vulnerabilidades

Periocidad Semestral
Vol. 8, núm. 3
revistatsede@tsachila.edu.ec

Recepción: 28-10-2025
Aprobación: 25-11-2025
Publicación: 25-12-2025

URL:
http://tsachila.edu.ec/ojs/index.php/TSEDE/issue/archive



Introducción

El internet de las cosas (IoT) se ha venido transformando de una manera radical teniendo una interacción entre los usuarios y dispositivos inteligentes, lo cual permite interconexión entre ellos, el internet ayuda a la mejora de la automatización de diferentes sectores. Sin embargo, Saavedra-Neira et al. (2023), se basan en que esta interconexión ha traído consigo una serie de vulnerabilidades que comprometen a la seguridad de la información los diversos dispositivos IoT, debido a sus limitaciones de hardware y diseño enfocado en la eficiencia, carecen de mecanismos robustos para su protección, lo que los hace susceptibles a ataques cibernéticos. Esta situación plantea un problema crítico en la gestión de la seguridad informática, especialmente en entornos donde la disponibilidad, integridad y confidencialidad de los datos son fundamentales dentro de las IoT.

Según Baccelli (2021), considera que las amenazas más comunes las cuales son las contraseñas por defecto o de caracteres débiles, desactualización del firmware, sus protocolos de comunicación y ataques de los servicios de negación, de esta manera los atacantes o botnets toman a su posesión los dispositivos para manipular de manera maliciosa la información, sus vulnerabilidades lleva consigo la afectación no solo en los usuarios, sino que también en las redes de dicha empresa. Por otra parte, Rivera et al. (2024), señalan lo siguiente para que sus amenazas se mitiguen, se cuenta con múltiples soluciones ya desarrolladas donde sus combinaciones tienen autenticidad, cifrado de extremo a extremo, la segmentación de redes y actualizaciones en el software.

Sin embargo, Flores et al. (2021), consideran que el IoT ha evolucionado hacia aplicaciones en múltiples disciplinas, donde no solo se basa en la eficiencia del hardware, sino también en el software que determina el comportamiento de los dispositivos, en dichas tecnologías como blockchain, inteligencia artificial y aprendizaje automático han sido integradas para mejorar la seguridad y el análisis de sus datos. De manera que, Joyanes Aguilar (2021), manifiesta que el IoT forma parte de un ecosistema hiperconectado que impulsa la transformación digital en sectores clave, y dicha integración con tecnologías disruptivas como Big Data y la computación en la nube donde se plantea nuevos retos en cuanto a la protección de la información y la gestión de riesgos, a pesar de estos avances, su implementación enfrenta desafíos como el manejo de grandes volúmenes de información y la necesidad de garantizar la seguridad y privacidad de los sistemas interconectados.

A pesar de los avances tecnológicos que ofrece el Internet de las Cosas (IoT), su desarrollo en entornos urbanos y críticos como el tránsito enfrenta desafíos importantes relacionados con la ciberseguridad, basada en la falta de familiaridad de los usuarios con estos sistemas, su limitada infraestructura tecnológica en ciertas comunidades y la percepción de que los procesos digitales son menos confiables que los tradicionales. Además, para que el IoT tenga una contribución efectivamente en la mediación de conflictos, principalmente en incidentes de tránsito, es de suma importancia que los sistemas estén respaldados por protocolos seguros, cifrado robusto de los datos. Según De Grado et al. (2025), destacan lo siguiente que la protección de los dispositivos conectados y la gestión segura de la información son pilares fundamentales para el desarrollo de ciudades inteligentes, donde las IoT puede

ser una herramienta clave tener prevención, análisis y resolución de conflictos. Por lo tanto, Pérez Martínez (2021), señala que el diseño de las ciudades inteligentes es considerado una evolución en los sistemas y la protección de privacidad para contar con una sostenibilidad clave. Asimismo, Villa Crespo (2023), enfatiza que la ciberseguridad en el IoT no solo depende de la tecnología, sino también de la capacitación impartidas hacia los usuarios y de las diferentes políticas públicas que regulen el uso de manera responsable.

En el entorno ecuatoriano, el desarrollo del IoT se ha visto enfrentado a diversos desafíos, lo cual están relacionados a la seguridad informática y su infraestructura tecnológica. Según Jumbo et al. (2023), manifiesta mediante un análisis de los dispositivos IoT en el Ecuador, donde revela que existe una alta demanda de exposición de una informática sensible, dentro de las cámaras web, servidores sin protecciones adecuadas, principalmente en las provincias de Pichincha y Guayas, lo que da por evidencia un nivel bajo de seguridad informática dentro del país. Como lo manifiestan Salazar y Silvestre (2025), destaca que los hogares ecuatorianos han adoptado las IoT de una manera favorable para la mejora en la conectividad, educación tecnológica, acceso a dispositivos inteligentes. En cuanto a las soluciones, se encuentra iniciativas mediante Smart Safety, que las impulsa empresas como lo es Sonda, las cuales integran tecnologías como lo es la inteligencia artificial, drones y sensores acústicos que son de ayuda para la seguridad en ciudades inteligentes.

Definición y evolución del IoT

Según Baccelli (2021), son el conjunto de tecnologías que conectan el mundo físico con lo digital. Esto permite la conexión entre dispositivos inteligentes por medio del

internet. La evolución de las IoT comenzó con las tecnologías domóticas en el año 1970. Posteriormente, en los años 90 se fortaleció el desarrollo de etiquetas RFID; estas permiten identificar objetos de forma única y así, de manera constante, siguieron evolucionando. Hasta el día de hoy lo siguen haciendo, y en la actualidad contamos con tecnologías muy avanzadas y las IoT integradas en diversos campos como la salud, la industria, etc.

Arquitectura general del IoT

Según Buitrón Ruiz (2022),las arquitecturas del IoT están estructuradas en capas, cada una con funciones específicas que permiten la recopilación, procesamiento y transmisión de datos, esta organización por niveles facilita la interoperabilidad entre dispositivos, aunque aún no existe una arquitectura estandarizada universalmente aceptada. El autor destaca que esta falta de estandarización complica la integración de sistemas heterogéneos, lo que representa uno de los principales desafíos actuales en el desarrollo de soluciones IoT.

Aplicaciones del IoT en sectores críticos

Según Joyanes Aguilar (2021), el Internet de las Cosas constituye un ecosistema tecnológico y social emergente que impulsa la transformación digital de organizaciones y empresas, mediante la red de objetos inteligentes interconectados permite recopilar, procesar y compartir datos, siendo clave en el desarrollo de la Industria 4.0 y en la evolución hacia una sociedad hiperconectada.

Seguridad Informática en el Contexto del IoT

El Internet de las cosas, también conocido como IoT, representa una gran transformación tecnológica que conecta lo físico y lo digital. Esto permite el intercambio de datos en tiempo real; sin embargo, este avance tecnológico también deja expuestos los dispositivos a muchos ataques. Laghari et al. (2024a) explican que los ataques en las IoT se encuentran clasificados en capas, afectando desde sensores hasta aplicaciones, y de la misma manera requieren soluciones por cada nivel. Por otra parte, Rahim y Chishti (2025) advierten que la abundancia de dispositivos heterogéneos dificulta la implementación de alguna medida de seguridad convencional. Esto hace que se incremente el riesgo de acceso no autorizado y manipulación de datos.

A pesar de los constantes avances tecnológicos, persisten desafíos importantes en la implementación de seguridad en las IoT. Además, Sebestyen et al (2022) destacan que, aunque existen regulaciones como el GDPR y el IoT Cybersecurity Improvement Act, aún existen brechas en la aplicación de estas normativas, especialmente en el entorno doméstico e industrial. Por eso se necesita una estrategia que combine tanto soluciones técnicas como buenas prácticas, para que así se garantice la protección de datos y la resiliencia de los sistemas IoT frente a amenazas, este reto se ve más notorio en sectores de salud o en ciudades inteligente donde una falla puede causar consecuencias graves.

Metodología

La presente investigación se desarrolló en un entorno documental, en el cantón El Carmen, Manabí, Ecuador, utilizando fuentes digitales e información de carácter académico. El enfoque que se adoptó es cualitativo, con un diseño no experimental y

su tipo es descriptivo. Esto se orientó al análisis de las amenazas de seguridad de las IoT. Según Senovia y Piña Ferrer (2023), la investigación cualitativa permite que se comprendan fenómenos; este enfoque se basa en la interpretación de los significados y a la vez también de las experiencias. Además, el diseño no experimental es adecuado cuando no hay manipulación de las variables.

Se aplicaron varios métodos: documental, analítico y comparativo, el método documental permitió la recopilación de la información sobre vulnerabilidades en IoT, el método analítico facilitó la identificación de patrones más comunes en ataques que fueron reportados, y, por último, el método comparativo permitió conocer las soluciones que se propusieron en distintos contextos, tanto tecnológicos como geográficos.

La población que se utilizó para el presente estudio fueron artículos científicos, informes técnicos y documentos relacionados a la ciberseguridad e IoT, dentro de la muestra se obtuvo mediante un muestreo de tipo no probabilístico por conveniencia, considerando solo los documentos que cumplían con los criterios necesarios para la investigación. Como lo indica Kwon, Jang y Kim (2025), este tipo de muestreo es frecuente en investigaciones de tipo exploratorias y descriptivas; su aplicación resulta válida siempre que se definan los criterios de inclusión y exclusión.

El análisis de la presente investigación se centró en dos puntos claves: las amenazas de seguridad que afectan a los dispositivos IoT y las soluciones técnicas para mitigar los riesgos, para la organización de la información se utilizó Mendeley; Además, se utilizó una matriz con el fin de clasificar las amenazas por su tipo y dispositivo afectado,

y la solución que se propuso, para el proceso de datos se utilizó Excel para tabular la frecuencia de aparición de amenazas y soluciones.

Resultados y Discusión

Como lo explicó Laghari (2024), en el desarrollo de esta investigación se identificaron las amenazas más comunes en los dispositivos IoT, muchas de las cuales comprometían la seguridad de la información y la operatividad de dichos sistemas, entre los problemas más frecuentes se encuentran las contraseñas por defecto, las cuales no son cambiadas y se mantienen activas, la falta de actualizaciones del firmware y la exposición de puertos abiertos sin la protección adecuada, más del 68 % de los dispositivos IoT en el mundo presentan al menos una vulnerabilidad crítica, y el 32% mantiene contraseñas por defecto o débiles, facilitando accesos no autorizados. Como lo manifestó, Jumbo (2023), en Ecuador se registró que el 54 % de las direcciones IP analizadas correspondían a cámaras web y el 27 % a routers domésticos sin cifrado, siendo Pichincha y Guayas las provincias con mayor concentración de dispositivos vulnerables, esta situación reflejó la necesidad urgente de fortalecer las medidas de seguridad y la configuración de los dispositivos IoT.

Como lo indicó, Harding et al. (2025), las soluciones identificadas en la literatura se agruparon en tres enfoques principales los cuales son: autenticación robusta, cifrado de extremo a extremo y segmentación de redes, destacó que la combinación de estas medidas permite redujo significativamente el riesgo de ataques, especialmente en entornos urbanos y domésticos. Como lo señaló Victor et al. (2023), la gestión segura de la información y la protección de dispositivos conectados son pilares fundamentales para un desarrollo sostenible en estos entornos.

Tabla 1

Tipos de vulnerabilidades en dispositivos IoT

Tipo de vulnerabilidad	Descripción	Impacto principal	Frecuencia estimada (%)
Accesos no autorizados	Uso indebido de credenciales o falta de autenticación multifactorial	Robo o alteración de datos sensibles	40%
Software desactualizado	Dispositivos sin parches de seguridad o firmware obsoleto	Explotación de vulnerabilidades conocidas	35%
Fallos humanos	Errores por falta de capacitación o desconocimiento de protocolos	Compromiso involuntario de la red IoT	15%
Configuración insegura	Ausencia de cifrado o contraseñas débiles	Interceptación de datos e intrusiones	10%

Fuente: Elaboración propia, basada en Laghari et al. (2024), Jumbo et al. (2023), Harding et al. (2025) y Victor et al. (2023).

Según Joyanes Aguilar (2021), la aplicación del Internet de las Cosas (IoT) en ciudades inteligentes permitió optimizar el uso de recursos urbanos mediante sensores conectados, redes de comunicación y plataformas de análisis en tiempo real, estas soluciones se implementaron en sistemas de transporte, alumbrado público, gestión de residuos y seguridad ciudadana, mejorando la eficiencia y sostenibilidad de los entornos urbanos, el IoT es el eje vertebrador de la transformación digital en la industria 4.0 y en los modelos de ciudad inteligente, donde tecnologías como 5G, inteligencia artificial y blockchain se integran para ofrecer servicios automatizados y personalizados.

Como lo indicaron, Philipe Moura y Stefano Nicoletti (2018), en el ámbito de la salud y los hogares, el IoT ha revolucionado la forma en que se monitorean y gestionaron los datos personales, en la salud, dispositivos portátiles como relojes inteligentes y sensores biomédicos permitieron la supervisión remota de pacientes, facilitando diagnósticos preventivos y atención personalizada. Dentro de los hogares, la domótica

basada en IoT permite controlar iluminación, climatización, seguridad y electrodomésticos desde aplicaciones móviles, estas soluciones requirieron arquitecturas robustas, protocolos seguros y una gobernanza ética para garantizar la privacidad y la interoperabilidad entre dispositivos.

Tabla 2

Soluciones técnicas IoT en contextos críticos

Contexto	Solución técnica IoT	Beneficio principal
Ciudad inteligente	Sensores urbanos, redes 5G, IA, blockhain	Eficiencia energética, seguridad, sostenibilidad
Salud	Wearables biomédicos, monitoreo remoto	Atención preventiva, reducción de hospitalización
Hogar	Domótica con apps móviles, asistentes virtuales	Comodidad, control remoto, ahorro de energía

Fuente: Elaboración propia basada en Joyanes Aguilar (2021) & Philipe et al. (2018)

Según Villa Crespo (2023), en el contexto ecuatoriano se observó una adopción creciente de tecnologías IoT en muchos hogares y espacios públicos, aunque persistieron desafíos relacionados con la infraestructura tecnológica y la capacitación de los usuarios, la ciberseguridad no depende únicamente de la tecnología, sino también de políticas públicas y educación digital, las cuales limitaron su implementación efectiva en sectores como el tránsito y la salud. Además, Victor (2023) señaló que la gestión segura de la información y la protección de dispositivos conectados fueron pilares fundamentales para el desarrollo sostenible de varios entornos.

Según Villa Crespo (2023), indicó que, a pesar de los avances tecnológicos siguen persistiendo amenazas que afectaron la seguridad de los dispositivos IoT, especialmente en entornos domésticos y urbanos estas amenazas se agruparon en

capas, desde el hardware hasta la aplicación y requirieron soluciones específicas para cada nivel, los problemas más frecuentes, como ya se mencionó anteriormente las contraseñas débiles y la falta de actualizaciones. Además, Kavitha et al. (2025) indicaron que los botnets diseñados para IoT evolucionaron y presentaron arquitecturas más sofisticadas, capaces de coordinar ataques de manera distribuida.

Tabla 3

Tipos de vulnerabilidades en dispositivos IoT

Amenaza emergente	Tecnología implicada	Solución técnica
Botnets distribuidos	IoT avanzado	Detección con machine learning
Malware en firmware	Firmware vulnerable	Actualización automática y monitoreo
Piratería de código fuente	Código fuente en dispositivos	Deep learning híbrido
Manipulación de tráfico	Redes IoT interconectadas	Blockchain y segmentación de red

Fuente: Villa Crespo (2023) & Victor et al. (2023) & Sharma & Dhiman (2025) & Kavitha et al. (2025)

Las soluciones tradicionales dentro de la seguridad informática, como el cifrado simétrico, la autenticación básica por usuario y contraseña, el uso de firewalls, fueron pilares fundamentales en la protección de sistemas digitales, estas técnicas presentaron limitaciones frente a los desafíos actuales del Internet de las Cosas (IoT), donde la escalabilidad y heterogeneidad de dispositivos tienen una exposición constante a redes públicas requieren enfoques más robustos. Según Maciej Serda et al. (2019), el cifrado clásico siguió siendo útil, pero debió complementarse con mecanismos más dinámicos y adaptativos para enfrentar amenazas modernas como el spoofing, el sniffing y los ataques de intermediario.

En resguardo, las soluciones emergentes como el uso de blockchain, inteligencia artificial (IA) y aprendizaje automático (machine learning) ofrecieron capacidades

avanzadas para la detección de anomalías, la trazabilidad de eventos y la gestión descentralizada de identidades, blockchain permitió registrar transacciones de forma inmutable, lo que mejora la integridad de los datos en redes IoT. Por su parte, la IA y el aprendizaje automático facilitaron la identificación de patrones de comportamiento malicioso en tiempo real, adaptándose a nuevas amenazas sin intervención humana. Como indicó Joyanes Aguilar (2021), estas tecnologías emergentes no solo fortalecieron la seguridad, sino que también optimizaron la eficiencia operativa en entornos críticos como ciudades inteligentes y sistemas de salud conectados.

Tabla 4

Comparación entre soluciones tradicionales y emergentes en IoT

Tipo de solución	Ejemplos principales	Ventajas clave
Tradicional	Cifrado simétrico, autenticación básica	Simplicidad, bajo costo
Emergente	Blockchain, IA, aprendizaje automático	Adaptabilidad, detección inteligente

Fuente: Elaboración propia basada en Maciej Serda et al. (2019) y Joyanes Aguilar (2021)

Como manifestó (Jumbo et al., 2023), en Ecuador un estudio realizado por investigadores de la Escuela Politécnica Nacional y el Instituto Superior Tecnológico Wissen identificó múltiples vulnerabilidades en dispositivos IoT expuestos públicamente, mediante un escaneo de direcciones IPv4, se detectaron cámaras web, servidores Apache y routers con credenciales accesibles sin cifrado, especialmente en las provincias de Pichincha y Guayas, esto evidencia un bajo nivel de seguridad informática en el país, donde muchos dispositivos están conectados sin medidas de protección adecuadas, exponiendo datos sensibles a posibles ataques.

Según (Celi Sandoya, 2023), a nivel regional un trabajo académico desarrollado en la Universidad Politécnica Salesiana de Guayaquil propuso soluciones de ciberseguridad para redes IoT en América Latina este estudio destacó la necesidad de implementar firewalls, segmentación de red, autenticación multifactor y monitoreo constante para mitigar ataques como el ransomware y el acceso no autorizado. Estas medidas fueron aplicadas con éxito en entornos industriales y urbanos, demostrando que una arquitectura de seguridad bien diseñada redujo significativamente los riesgos asociados al IoT.

Tabla 5

Ejemplos de vulnerabilidades y soluciones IoT en Ecuador y Latinoamérica

Región/País	Caso documentado	Solución propuesta
América Latina	Riesgo de ransomware y acceso no autorizado en redes IoT industriales.	Segmentación de red, autenticación multifactor, monitoreo
Ecuador	Exposición de cámaras web y routers sin cifrado en Pichincha y Guayas	Escaneo preventivo, cifrado de credenciales, firewall

Fuente: Elaboración propia basada en Jumbo et al. (2023) y Celi Sandoya (2023)

Conclusiones

El presente estudio permitió identificar las principales amenazas de seguridad que tiene la IoT, destacando varios puntos que se vieron con debilidad, que son contraseñas débiles, software desactualizado y configuraciones inseguras. Todos estos factores comprometen la seguridad de los sistemas, los mismos que pueden tener información personal de los usuarios. A través del análisis documental se evidenció que hay varias formas de proteger los sistemas IoT; una de esas opciones

es el cifrado de datos de extremo a extremo, la autenticación multifactor y también tecnologías blockchain. Todas estas soluciones contribuyen a mitigar todos los posibles riesgos en seguridad que presenten estos sistemas. Se concluye que la seguridad en las IoT no solo depende únicamente del desarrollo, sino también de los usuarios. La falta de educación digital es notoria y, a su vez, la falta de formulación de políticas públicas que regulen su uso responsable. Como recomendación, se sugiere analizar estudios empíricos los cuales evalúen la efectividad de estas soluciones en contextos reales y, a su vez, indagar sobre nuevas estrategias para la seguridad en las IoT, los resultados que se obtuvieron aportan una base sólida para el diseño de entornos IoT más seguros y sostenibles, especialmente en países como Ecuador, donde la implementación de estas tecnologías todavía enfrenta un gran desafío en la infraestructura y la conciencia de la ciudadanía.

Referencias Bibliográficas

Baccelli, E. (2021). *Libro Blancon°05In ternet de las cosas (IoT)*.

Buitrón Ruiz, D. F. (2022). *Arquitecturas y modelos de referencia para sistemas IoT: estado del arte de las arquitecturas para sistemas IoT.* https://bibdigital.epn.edu.ec/handle/15000/22368

Celi Sandoya, A. M. (2023). *Soluciones de ciberseguridad contra los ataques a redes IoT en América Latina, una Revisión Sistemática de la Literatura*. http://dspace.ups.edu.ec/handle/123456789/25904

De Grado, P., González, A., Pérez, G. y Lora, P. (2025). *Ciberseguridad en el Internet de las cosas: retos y soluciones emergentes*. Corporación Universitaria Remington. https://repositorio.uniremington.edu.co/handle/123456789/8282

Flores Zermeño, F., Cossio Franco, G. Flores, J. (2021). *Aplicaciones, Enfoques y Tendencias del Internet de las Cosas (IoT): Revisión Sistemática de la Literatura*. *13*(9), 568.

Harding, W., Hartmann, A., O'Brien, S., Sinzig, V., Break, G. and Sinzig, N. (2025a). *Securing a Connected Future*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-07309-9

Saavedra-Neira, J. (2023). *Vista de Aplicaciones y beneficios IOT como alternativa en el gobierno TI: Revisión sistemática de literatura*. https://revista.ucsa-ct.edu.py/ojs/index.php/ucsa/article/view/127/113

Joyanes Aguilar, L. (2021). *Internet de las cosas: un futuro hiperconectado: 5G, Inteligencia Artificial, Big data, Cloud, Blockchain, Ciberseguridad*. https://www.casadellibro.com/libro-internet-de-las-cosas-un-futuro-hiperconectado-5g-inteligencia-artificial-big-data-cloud-blockchain-y-ciberseguridad/9788426733214/12456139

Jumbo, E., Llumiquinga, J., Uyaguari, F., Superior, I., Wissen Cuenca -Ecuador, T. y Rivera, R. (2023). Un breve Análisis de Vulnerabilidades en dispositivos IOT en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(2), 5939–5953. https://doi.org/10.37811/CL_RCM.V7I2.5763

Kavitha, P., Malathi, S., Manoharan, H. and Anitha, J. (2025). Enhancing IoT cyber security with hybrid deep learning: a novel approach for malware detection

and source code piracy prevention using adaptive tensor flow and IPSO. *International Journal of System Assurance Engineering and Management*, *16*, 2280–2292. https://doi.org/10.1007/s13198-025-02794-5

Kwon, S., Jang, D. and Kim, K. (2025). Doubly Robust Estimation of the Finite Population Distribution Function Using Nonprobability Samples. *Mathematics*, *13*. https://doi.org/10.3390/math13193227

Laghari, A., Li, H., Khan, A., Shoulin, Y., Karim, S. and Khani, M. A. K. (2024). Internet of Things (IoT) applications security trends and challenges. En *Discover Internet of Things* (Vol. 4). Springer Nature. https://doi.org/10.1007/s43926-024-00090-5

Maciej Serda, Becker, F. G., Cleary, M., Team, R. M., Holtermann, H., The, D., Agenda, N., Science, P., Sk, S. K., Hinnebusch, R., Hinnebusch A, R., Rabinovich, I., Olmert, Y., Uld, D., Ri, W., Frxqwu, W., Zklfk, E., Edvhg, L. (2019). Internet de las cosas. Aplicaciones, tecnologías y seguridad. *Uniwersytet śląski*, *7*(1), 343–354. https://doi.org/10.2/JQUERY.MIN.JS

Pérez Martínez, F. (2021). *Ciudades inteligentes: Gobernanza, tecnología y sostenibilidad*. Tirant lo Blanch.

Moura, P. y Nicoletti, S. (2018). *Ciudades inteligentes e Internet de las Cosas: cómo fomentar su desarrollo en América Latina | InfoLibros.org*. https://infolibros.org/pdfview/23980-ciudades-inteligentes-e-internet-de-las-cosas-como-fomentar-su-desarrollo-en-america-latina-philipe-mourastefano-nicoletti/

Piña-Ferrer, L. S. (2023). El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria Koinonía*, *8*(15), 1–3. https://doi.org/10.35381/r.k.v8i15.2440

Rahim, R. and Chishti, M. A. (2025). *Security Framework for IoT Devices against Cyber-attacks*. 249–266. https://doi.org/https://doi.org/10.1007/s42979-025-04106-x

Rivera, J.y Lopera Sánchez, A. (2024). *Internet de las Cosas*.

Salazar, J. y Silvestre, Y. (2025). *INTERNET DE LAS COSAS*. http://www.techpedia.eu

Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2022). *Dynamic Clock Reconfiguration for the Constrained IoT and its Application to Energy-efficient Networking*. https://doi.org/https://doi.org/10.3390/computers14020061

Sharma, N., & Dhiman, P. (2025). *A survey on IoT security: challenges and their solutions using machine learning and blockchain technology*. https://doi.org/https://doi.org/10.1007/s10586-025-05208-

Victor, P., Lashkari, A. H., Lu, R., Sasi, T., Xiong, P., & Iqbal, S. (2023). IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. *Peer-to-Peer Networking and Applications*, *16*, 1380–1431. https://doi.org/10.1007/s12083-023-01478-w

Villa Crespo, I. (2023). *Ciberseguridad IoT y su aplicación en Ciudades Inteligentes*. www.ra-ma.com