Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Seguridad en dispositivos IOT : retos y soluciones en un mundo conectado.
Security in IOT devices: challenges and solutions in a connected world

Mgtr. Víctor Miguel Vera Estrada, Mgtr. Lina Dayana Aguirre Carrión, Mgtr. María Alexandra Pilco Llumitaxi, Tnlgo. Cristian Ramiro Valdivieso Tixe, Mgtr. Ángel Wilson Villarreal Cobeña.

CIENCIA E INNOVACIÓN EN DIVERSAS DISCIPLINAS CIENTÍFICAS.
Julio - Diciembre, V°5-N°2; 2024

- ✓ **Recibido:** 01/10/2024
- ✓ **Aceptado**:17/10/2024
- ✓ **Publicado:** 31/12/2024

PAIS
Ecuador – Quevedo
Ecuador – Quevedo
Ecuador – Quevedo
Ecuador – Quevedo
Ecuador – Quevedo

INSTITUCIÓN
- Unidad Educativa Quintiliano Sánchez Rendón
- Unidad Educativa Juan Montalvo
- Instituto Superior Tecnológico La Maná
- Instituto Superior Tecnológico La Maná
- Universidad Laica Eloy Alfaro de Manabí-Ext. EC.

CORREO:
vmiguelv@gmail.com
dayana1337@gmail.com
maryale.pilco@gmail.com
cristians2389@hotmail.com
angel.villarreal@uleam.edu.ec

ORCID:
https://orcid.org/0000-0002-5790-2385
https://orcid.org/0000-0002-2950-7863
https://orcid.org/0000-0003-3715-4508
https://orcid.org/0000-0002-9693-9033
https://orcid.org/0000-0003-0357-0538

FORMATO DE CITA APA.
Vera, V. Aguirre, L. Pilco, M, Valdivieso, C. Villareal, Ä. (2024). Seguridad en dispositivos IOT : retos y soluciones en un mundo conectado. Revista G-ner@ndo, V°5 (N°2,).1835– 1844.

Abstract

Este estudio aborda los principales retos de ciberseguridad que afectan al Internet de las Cosas (IOT), explorando las vulnerabilidades más comunes en los dispositivos conectados, como la autenticación débil, la falta de cifrado en las comunicaciones y la ausencia de actualizaciones automáticas de seguridad. A través de una revisión exhaustiva de literatura académica, análisis de incidentes de seguridad históricos, y el estudio de normativas emergentes, se examinan los riesgos que los dispositivos IOT presentan tanto para usuarios individuales como para infraestructuras críticas. Asimismo, se destacan las tecnologías emergentes, como la inteligencia artificial y blockchain, que ofrecen soluciones prometedoras para mitigar estos riesgos, aunque su implementación aún enfrenta barreras. El análisis comparativo revela que, a pesar de los avances regulatorios en mercados clave, como la Unión Europea y Estados Unidos, la fragmentación global de las normativas dificulta la creación de un entorno IOT seguro. Los resultados subrayan la necesidad urgente de una colaboración más estrecha entre fabricantes, reguladores y usuarios para mejorar la seguridad IOT y minimizar el riesgo de ciberataques.

Palabras clave: Ciberseguridad, Blockchain, Inteligencia Artificial, Botnets, Normativas.

Abstract

This study addresses the main cybersecurity challenges affecting the Internet of Things (IOT), exploring common vulnerabilities in connected devices such as weak authentication, lack of encryption in communications, and the absence of automatic security updates. Through a comprehensive review of academic literature, analysis of historical security incidents, and the study of emerging regulations, the risks posed by IOT devices to both individual users and critical infrastructures are examined. Furthermore, emerging technologies such as artificial intelligence and blockchain are highlighted as promising solutions to mitigate these risks, though their implementation still faces significant barriers. Comparative analysis reveals that despite regulatory advances in key markets like the European Union and the United States, global fragmentation of regulations hinders the creation of a secure IOT environment. The results emphasize the urgent need for closer collaboration between manufacturers, regulators, and users to improve IOT security and reduce the risk of cyberattacks.

Keywords: Cybersecurity, Blockchain, Artificial Intelligence, Botnets, Regulations

.

.

Introducción

A medida que el IOT revoluciona las actividades cotidianas y los procesos industriales, también introduce riesgos significativos relacionados con la seguridad. Los dispositivos IOT suelen tener capacidades de procesamiento y almacenamiento limitadas, lo que dificulta la implementación de medidas de seguridad robustas. La falta de estandarización en la seguridad de estos dispositivos aumenta su vulnerabilidad a ciberataques. Este artículo se propone explorar las principales amenazas y vulnerabilidades en el entorno IOT y ofrecer soluciones basadas en las mejores prácticas de ciberseguridad. (Red Hat, 2023).

El Internet de las Cosas (**IOT** , por sus siglas en inglés) ha experimentado un crecimiento acelerado en los últimos años, impactando diversas industrias como la manufactura, la salud, el transporte y el hogar. Esta tecnología conecta dispositivos inteligentes a internet, permitiendo la automatización y el intercambio de datos en tiempo real, lo que ha generado beneficios significativos en términos de eficiencia y productividad. En 2023, el número de dispositivos IOT conectados superó los 14 mil millones a nivel global, y se espera que esta cifra continúe en aumento en los próximos años (CEPAL, 2023). Sin embargo, este avance también ha dado lugar a nuevos retos de ciberseguridad que requieren ser abordados con urgencia.

Una de las principales preocupaciones en el ámbito del IOT es la falta de medidas de seguridad adecuadas en muchos de los dispositivos conectados. Dado que los dispositivos IOT suelen ser diseñados para ser pequeños, eficientes y de bajo costo, frecuentemente se omiten elementos claves de seguridad, lo que los hace vulnerables a ataques cibernéticos. Además, la heterogeneidad de los dispositivos IOT, provenientes de diferentes fabricantes y con distintos estándares de seguridad, dificulta la implementación de soluciones universales que puedan proteger la integridad de las redes donde operan Una revisión sistemática. Este escenario ha llevado a un aumento de los incidentes de seguridad relacionados con IOT en los últimos años.

Los ataques a dispositivos IOT no solo afectan a los usuarios individuales, sino que también representan una amenaza significativa para la infraestructura crítica. Los ciberataques dirigidos a dispositivos IOT que forman parte de sistemas de control industrial (ICS) y redes de servicios públicos pueden tener graves consecuencias, como la interrupción de servicios esenciales o incluso el sabotaje de instalaciones críticas (Hernández, Martínez, & Torres, 2023). Un ejemplo reciente de este tipo de ataque ocurrió en 2023, cuando una botnet IOT fue utilizada para lanzar un ataque de denegación de servicio (DDoS) contra una planta energética, lo que provocó cortes temporales en el suministro eléctrico de varias ciudades (López & Ramírez, 2023).

Otra preocupación relevante es la privacidad de los datos que manejan los dispositivos IOT. Estos dispositivos recopilan grandes cantidades de información personal y empresarial, lo que ha convertido la protección de estos datos en una prioridad tanto para los legisladores como para los expertos en ciberseguridad. En muchos casos, las comunicaciones entre dispositivos IOT y servidores no están cifradas adecuadamente, lo que permite que los atacantes intercepten o manipulen los datos transmitidos (Álvarez & Morales). Además, la falta de mecanismos robustos de autenticación facilita el acceso no autorizado a estos dispositivos, poniendo en riesgo tanto la privacidad de los usuarios como la seguridad de las organizaciones.

A pesar de los esfuerzos realizados para mejorar la seguridad en el IOT, los fabricantes enfrentan dificultades al intentar equilibrar la funcionalidad, el costo y la seguridad. Muchos dispositivos IOT no cuentan con sistemas de actualización automática, lo que significa que las vulnerabilidades descubiertas tras su comercialización pueden permanecer sin solución durante largos periodos de tiempo (Fernández & Gutiérrez, 2023). Esto expone a los dispositivos a ataques que podrían haberse evitado mediante una gestión proactiva de actualizaciones de seguridad, lo que subraya la importancia de que tanto empresas como usuarios se mantengan informados y adopten buenas prácticas de ciberseguridad.

Un desafío adicional es la falta de estandarización global en términos de seguridad IOT. Aunque algunos países han implementado regulaciones específicas, como la Ley de Mejora de la Ciberseguridad IOT en Estados Unidos, estos esfuerzos no se han adoptado de manera uniforme en todo el mundo (Ruiz, Romero, & Méndez, 2023). Esta situación crea un entorno fragmentado en el que los niveles de seguridad varían entre fabricantes y regiones, lo que dificulta la implementación de una protección integral contra las amenazas cibernéticas.

Ante estos retos, se han propuesto diversas soluciones que incluyen desde el desarrollo de mejores prácticas de seguridad hasta la adopción de tecnologías emergentes, como blockchain e inteligencia artificial, para la detección de anomalías y la prevención de ataques (Vázquez & Delgado, 2023). Estas tecnologías prometen mejorar significativamente la seguridad en las redes IOT mediante el fortalecimiento de los mecanismos de autenticación y control de acceso, así como la monitorización continua de las amenazas. Sin embargo, su adopción aún enfrenta barreras relacionadas con la escalabilidad y el costo.

Finalmente, es importante destacar que la seguridad en IOT no es solo responsabilidad de los fabricantes y legisladores, sino también de los usuarios finales. La falta de conciencia sobre las amenazas cibernéticas y las mejores prácticas de seguridad sigue contribuyendo a la vulnerabilidad de los dispositivos IOT. Campañas educativas dirigidas tanto a consumidores como a empresas son esenciales para garantizar que los dispositivos se configuren y utilicen de manera segura, minimizando los riesgos de ciberataques (Mendoza, Castillo, & Fernández, 2023). Esto incluye la adopción de medidas básicas como cambiar contraseñas predeterminadas y activar el cifrado de las comunicaciones.

Materiales Y Métodos

Para la realización de este estudio se empleó un enfoque cualitativo basado en una revisión documental exhaustiva de investigaciones académicas, informes sobre incidentes de seguridad y estudios de caso relacionados con ciberataques en dispositivos IOT. La metodología

utilizada permitió realizar un análisis profundo de las vulnerabilidades presentes en el ecosistema IOT, así como de las normativas vigentes y las soluciones de ciberseguridad propuestas por organizaciones especializadas en este ámbito. La estructura metodológica siguió cuatro etapas clave que garantizaron la validez y la relevancia de los datos recopilados para el estudio.

En la primera etapa, se llevó a cabo la selección de la literatura académica y los estudios de caso más relevantes. Para ello, se utilizó principalmente la base de datos Google Scholar. La búsqueda se centró en publicaciones recientes (a partir de 2020) que abordaran la seguridad en dispositivos IOT, identificando artículos revisados por pares, reportes técnicos de ciberseguridad y estudios de caso sobre incidentes específicos de ciberataques. La selección se realizó siguiendo criterios de relevancia, pertinencia y rigor metodológico de las publicaciones. Investigaciones como las de González y Ramírez (2023), así como los reportes de la Unión Internacional de Telecomunicaciones (UIT, 2023), fueron fundamentales para comprender la evolución de las amenazas y las medidas de seguridad en IOT.

La segunda etapa consistió en un análisis comparativo de las principales vulnerabilidades identificadas en dispositivos IOT. Para ello, se revisaron estudios previos que analizaron fallos en la autenticación, conectividad insegura, y la falta de actualizaciones de seguridad. Investigaciones como las de Pérez, Ramírez, & Sánchez, (2023) fueron utilizadas para examinar los patrones comunes de vulnerabilidades. El análisis incluyó tanto dispositivos de uso doméstico (como cámaras de seguridad y asistentes virtuales) como aquellos utilizados en infraestructuras críticas. Se recopiló información sobre la incidencia de cada tipo de vulnerabilidad y se comparó con estudios históricos para identificar tendencias recurrentes.

La tercera etapa implicó una revisión de incidentes históricos de ciberataques que involucraron dispositivos IOT. Se tomaron como referencia estudios de caso bien documentados, como el ataque de Mirai en 2016, y se incluyeron análisis de incidentes más recientes, como el ataque de la botnet Hajime en 2023. Estos casos permitieron ilustrar cómo las vulnerabilidades

en dispositivos IOT han sido explotadas para lanzar ataques de gran escala, afectando tanto a individuos como a infraestructuras empresariales (Fernández, López, & García, Evaluación de las vulnerabilidades en dispositivos IoT y su impacto en la ciberseguridad global, 2023). Este enfoque fue útil para comprender el impacto real de las vulnerabilidades IOT en entornos del mundo real.

La cuarta etapa de la metodología se centró en la identificación y el análisis de normativas y soluciones de seguridad emergentes. Se investigaron los principales marcos regulatorios, tanto a nivel nacional como internacional, con el objetivo de evaluar su eficacia y su aplicabilidad en diferentes contextos. Normativas como la Directiva NIS de la Unión Europea (2023) y la *IOT Cybersecurity Improvement Act* de Estados Unidos (2023) fueron analizadas para comprender cómo se están implementando las regulaciones en diferentes regiones del mundo. Además, se revisaron las soluciones propuestas por organizaciones de ciberseguridad, como el uso de blockchain e inteligencia artificial para la detección de amenazas, destacando su potencial para mejorar la seguridad en dispositivos IOT (López & García, 2023).

Análisis de Resultados

Vulnerabilidades más frecuentes en dispositivos IOT

El análisis de las investigaciones y estudios de caso revisados reveló que las vulnerabilidades más comunes en los dispositivos IOT están relacionadas con la conectividad a internet constante, la falta de autenticación multifactor y el uso de contraseñas predeterminadas que rara vez son modificadas por los usuarios. Estas debilidades incrementan significativamente el riesgo de ciberataques. De acuerdo con los datos recopilados por Fernández et al. (2023), aproximadamente el 45% de los dispositivos IOT analizados no contaban con mecanismos de actualización automática de seguridad. Esta falta de actualización regular y automática incrementa la exposición de los dispositivos a vulnerabilidades descubiertas después de su comercialización, un problema recurrente que dificulta la protección efectiva de los sistemas IOT.

Impacto de los ataques DDoS y botnets en redes IOT

El impacto de los ataques DDoS y las botnets en dispositivos IOT se destacó como una de las principales amenazas en el entorno de ciberseguridad actual. Casos emblemáticos como el ataque de la botnet Mirai en 2016 y el más reciente incidente de la botnet Hajime en 2023 demostraron la capacidad de estos ataques para interrumpir servicios críticos. Los dispositivos IOT , a menudo considerados inofensivos, como cámaras de vigilancia y enrutadores, fueron reclutados para formar parte de estas redes botnet, lo que resultó en ataques masivos de denegación de servicio (Rodríguez & Delgado, 2023). Según estimaciones de López y García (2023), los ataques DDoS generados a partir de redes botnet IOT pueden generar pérdidas económicas superiores a los 100 millones de dólares para las empresas afectadas, debido a la interrupción de servicios esenciales y a los costos asociados con la recuperación de los sistemas.

Eficacia de las normativas de seguridad emergentes

El análisis de las normativas de seguridad emergentes mostró que, si bien han tenido un impacto positivo en los mercados que las adoptan, la falta de estandarización global sigue siendo un obstáculo importante para la protección efectiva de los dispositivos IOT . Normativas como la Directiva NIS en Europa y la IOT Cybersecurity Improvement Act en Estados Unidos han establecido requisitos claros para los fabricantes de dispositivos IOT , pero su implementación no ha sido uniforme a nivel mundial. Esto crea brechas en la seguridad global, ya que muchos países aún no cuentan con regulaciones específicas para el IOT , lo que deja a los dispositivos expuestos a ciberataques en mercados menos regulados (González, 2023).

Conclusiones

El Internet de las Cosas (IOT) representa una revolución en la conectividad y automatización en múltiples sectores, pero también plantea importantes desafíos en términos de ciberseguridad. A lo largo de este estudio se han identificado las principales vulnerabilidades presentes en dispositivos IOT , incluyendo la autenticación débil, la falta de cifrado robusto y la carencia de actualizaciones automáticas. Estos factores hacen que los dispositivos IOT sean blancos fáciles para ciberataques, como los ataques de denegación de servicio (DDoS) y la creación de botnets. Además, la fragmentación normativa global y la falta de estandarización en las medidas de seguridad dificultan la creación de un entorno IOT verdaderamente seguro.

Aunque las normativas emergentes han tenido un impacto positivo en la mejora de la seguridad, aún queda mucho por hacer para lograr una protección efectiva a nivel mundial. Es esencial que los fabricantes adopten un enfoque de seguridad desde el diseño, integrando mejores prácticas y tecnologías avanzadas, como la inteligencia artificial y blockchain, para fortalecer los mecanismos de autenticación y control de acceso. Asimismo, los usuarios finales deben ser más conscientes de las amenazas cibernéticas y adoptar medidas básicas de seguridad, como la modificación de contraseñas predeterminadas y la actualización regular de sus dispositivos. En cuanto a futuras investigaciones, es necesario seguir explorando el potencial de la inteligencia artificial y el blockchain para mejorar la seguridad en IOT. En particular, se recomienda investigar cómo estas tecnologías pueden implementarse en dispositivos de bajo coste sin comprometer la eficiencia y accesibilidad de los mismos. Además, estudios que analicen la efectividad de campañas educativas dirigidas a consumidores y empresas podrían ofrecer soluciones valiosas para aumentar la conciencia sobre las amenazas y las mejores prácticas en ciberseguridad. La seguridad en IOT es un desafío complejo que requiere una colaboración continua entre reguladores, fabricantes y usuarios para lograr un entorno digital más seguro y confiable.

Referencias bibliográfica

Álvarez, P., & Morales, C. (s.f.). Seguridad de los datos en dispositivos IOT : Desafíos y soluciones. *Revista Iberoamericana de Ciberseguridad*, 215-230.

Cano, F. (2023). Cifrado en IOT : Retos y soluciones. *Revista Internacional de Ciberseguridad*, 45-58.

CEPAL, C. E. (2023). *CEPAL*. Obtenido de https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

Fernández, L., & Ruiz, P. (2023). Conectividad y seguridad en dispositivos IOT : Un análisis crítico. *Ciencia y Tecnología de la Información*, 12-25.

Fernández, R., & Gutiérrez, M. (2023). Mecanismos de actualización en dispositivos IOT : Implicaciones en la ciberseguridad. *Ciberseguridad y Sociedad*, 89-105.

Fernández, R., López, J., & García, P. (2023). Evaluación de las vulnerabilidades en dispositivos IOT y su impacto en la ciberseguridad global. *Revista Internacional de Seguridad Cibernética*, 78-91.

González, L. (2023). La Directiva NIS y su impacto en la seguridad IOT en Europa. *Revista de Derecho y Tecnología*, 101-114.

Hernández, A., Martínez, J., & Torres, R. (2023). Seguridad en el IOT industrial: Retos y estrategias de defensa. *Revista de Ingeniería y Tecnología*, 15-28.

López, A., & García, M. (2023). Implementación de inteligencia artificial en la ciberseguridad IOT : Una revisión crítica. *Journal of Cybersecurity Solutions*, 65-77.

López, P. (2023). Vulnerabilidades en dispositivos IOT : El estado actual de la ciberseguridad. *Análisis de Seguridad Digital*, 21-35.

López, P., & Ramírez, D. (2023). Ciberataques a infraestructuras críticas: El caso de las botnets IOT en 2023. *Análisis de Seguridad Cibernética*, 62-75.

Martínez, F., Pérez, H., & Vargas, E. (2023). Desafíos de ciberseguridad en dispositivos IOT . *Una revisión sistemática*, 101.

Méndez, F., & Castillo, J. (2023). El problema de la autenticación en dispositivos IOT : Soluciones y desafíos. *Revista de Ingeniería Informática*, 73-85.

Mendoza, L., Castillo, O., & Fernández, A. (2023). La importancia de la educación en ciberseguridad para usuarios de IOT . *Revista Latinoamericana de Ciberseguridad*, 42-58.

Pérez, H., Ramírez, C., & Sánchez, D. (2023). Seguridad en el Internet de las Cosas: Retos y avances en la protección de dispositivos. *Revista de Ingeniería y Tecnología*, 112-130.

Red Hat. (enero de 2023). *¿Qué es el Internet de las cosas (IOT)?* Obtenido de https://www.redhat.com/es/topics/internet-of-things/what-is-IOT

Rodríguez, E., & Delgado, S. (2023). Evolución de las botnets en IOT : De Mirai a Hajime. *Seguridad Cibernética y Redes*, 33-50.

Ruiz, J., Romero, V., & Méndez, F. (2023). Regulaciones globales para la seguridad en IOT : Un análisis comparativo. *Derecho y Tecnología*, 133-148.

Smith, T., & Johnson, K. (2023). IOT Security: Current Challenges and Future Directions. *Journal of Internet Security*, 150-170.

Torres, D., Martínez, F., & Ramírez, C. (2023). Botnets en el Internet de las Cosas: Principales amenazas y contramedidas. *Tecnología e Innovación*, 61-75.

UIT. (2023). *Informe sobre el estado global de la ciberseguridad en IOT .* Unión Internacional de Telecomunicaciones.

Vázquez, I., & Delgado, J. (2023). Soluciones basadas en blockchain e inteligencia artificial para la seguridad en redes IOT . *Innovación y Tecnología*, 321-340.