ISSN-L 3072-9823
Núm. 2 Vol. 1
Abril 2026 - Marzo2027
1 – 25

Seguridad digital en el IoT integrado con programas computarizados: desafíos, vulnerabilidades y estrategias de mitigación

Digital security in the IoT integrated with computer programs: challenges, vulnerabilities and mitigation strategies

Ricardo M. Candanedo Yau
Universidad de Panamá, Centro Regional Universitario de Panamá Este. Panamá
ricardo.candanedo@up.c.pa
https://orcid.org/0009-0002-5017-9830

Recibido: 06 de enero de 2026.
Aceptado: 27 de abril de 2026
DOI: https://doi.org/10.66707/f29efc95

Resumen

Este estudio examinó de forma crítica los desafíos asociados con la seguridad digital en entornos en los que el Internet de las Cosas (IoT) opera de manera estrecha con programas computarizados que gestionan procesos automatizados. A partir de una revisión sistemática de literatura científica relevante, se identificaron debilidades recurrentes en mecanismos de autenticación, protección de datos y control de accesos, las cuales facilitaron la explotación por parte de amenazas como software malicioso, ataques de saturación de recursos y captura de información en tránsito. El análisis también mostró que las limitaciones de capacidad de los dispositivos, la diversidad de tecnologías y la falta de interoperabilidad contribuyen a un panorama de riesgo persistente. Las estrategias de mitigación más discutidas incluyeron la adopción de arquitecturas con seguridad incorporada, autenticación multifactorial, cifrado robusto y gestión avanzada de identidades. El estudio concluyó que garantizar la seguridad

digital en estos entornos requiere modelos de protección holísticos, adaptativos y alineados al ciclo de vida completo de los sistemas, de modo que se preserve tanto la disponibilidad de los servicios como la integridad de la información en contextos automatizados cada vez más complejos.

Palabras clave: automatización, internet de las cosas, protección de datos, riesgo tecnológico.

Abstract

This research critically investigated digital security challenges in environments where the Internet of Things (IoT) is tightly integrated with computerized systems that govern automated processes. Through a systematic review of pertinent scientific literature, recurring weaknesses were identified in authentication mechanisms, data protection, and access control, which enabled exploitation by threats such as malware, resource saturation attacks, and data interception. The analysis also revealed that device capacity constraints, technological diversity, and lack of interoperability contribute to an enduring risk landscape. Mitigation strategies frequently discussed included adopting security-by-design architectures, multifactor authentication, robust encryption, and advanced identity management. The study concluded that ensuring digital security in these environments necessitates holistic, adaptive protection models aligned with the systems' full lifecycle to safeguard both service availability and information integrity in increasingly complex automated contexts.

Keywords: automation, data protection, digital security, internet of things, technological risk.

Introducción

El Internet de las Cosas (IoT) ha emergido como un componente central de la transformación digital, permitiendo la interconexión de dispositivos físicos, sensores inteligentes y sistemas computarizados para la automatización y optimización de procesos en entornos industriales, comerciales y domésticos (Mohanta et al., 2020; Franco et al., 2021). La integración de estos dispositivos con programas computarizados ha posibilitado la construcción de ecosistemas altamente interdependientes, capaces de recopilar, procesar y analizar datos en tiempo real, generando beneficios como la eficiencia operativa, la reducción de costos y la mejora en la toma de decisiones estratégicas (Okporokpo et al., 2023; Pangestu, 2025). Sin

embargo, esta convergencia tecnológica también ha generado un incremento exponencial en la superficie de ataque, exponiendo a los sistemas a amenazas cibernéticas cada vez más sofisticadas que comprometen la confidencialidad, integridad y disponibilidad de la información (Jammeh et al., 2026; Kasula, 2025).

A diferencia de los sistemas computacionales tradicionales, los entornos IoT presentan características específicas que dificultan la implementación de mecanismos de seguridad efectivos. Entre estas se incluyen la heterogeneidad de los dispositivos, las limitaciones de capacidad de procesamiento y almacenamiento, la dependencia de protocolos de comunicación diversos y la falta de estándares universales de seguridad (Radanliev et al., 2020; Polk et al., 2017). Estas particularidades hacen que vulnerabilidades aparentemente menores, como la utilización de credenciales predeterminadas o el cifrado insuficiente de datos, puedan derivar en riesgos críticos que afecten procesos automatizados completos, con consecuencias tanto operativas como económicas y, en algunos casos, físicas.

La literatura reciente señala que las amenazas dirigidas a entornos IoT no se limitan al robo de información, sino que abarcan ataques de denegación de servicio, manipulación de datos, acceso no autorizado a programas computarizados y propagación de malware especializado, lo que evidencia la complejidad y el dinamismo de estos riesgos (Mendoza Villamar et al., 2025; Uprety & Rawat, 2021; Saha et al., 2021). Asimismo, la interdependencia entre dispositivos y programas computarizados aumenta la probabilidad de que un incidente aislado tenga efectos en cascada, afectando múltiples componentes de un sistema interconectado (Yang et al., 2024; Franco et al., 2021). Este contexto resalta la necesidad de abordar la seguridad digital desde una perspectiva integral, considerando tanto los aspectos técnicos de los dispositivos como la confiabilidad, resiliencia y continuidad operativa de los programas computarizados que dependen de ellos.

En este marco, la pregunta de investigación que orientó este estudio se planteó con el propósito de examinar de manera sistemática y completa los desafíos de seguridad que enfrentan los entornos IoT integrados con programas computarizados: *¿Cuáles fueron los principales retos de seguridad digital en entornos IoT y cómo impactaron estos desafíos en la confiabilidad, disponibilidad e integridad de los programas computarizados asociados?* La formulación de esta interrogante permitió delimitar el alcance del análisis, enfocándose en la

identificación de vulnerabilidades, amenazas emergentes y estrategias de mitigación documentadas en la literatura científica actual (Kasula, 2025; Jammeh et al., 2026).

El objetivo general del estudio consistió en analizar de manera exhaustiva los retos de seguridad digital en entornos IoT integrados con programas computarizados, evaluando la interacción entre dispositivos conectados y procesos automatizados. A partir de este objetivo se definieron objetivos específicos orientados a identificar las vulnerabilidades más recurrentes en los dispositivos IoT y su impacto en la confiabilidad de los programas computarizados; examinar las amenazas emergentes que comprometieron la disponibilidad e integridad de los sistemas; evaluar los enfoques de mitigación implementados en la literatura, incluyendo arquitecturas seguras, autenticación avanzada, cifrado de información y gestión de identidades; y analizar las limitaciones técnicas, organizacionales y operativas que condicionaron la aplicación efectiva de estas medidas de seguridad (Radanliev et al., 2020; Uprety & Rawat, 2021).

La relevancia de esta investigación radica en su contribución al entendimiento de la seguridad digital como un elemento estratégico en la intersección del IoT y la automatización de procesos. Al integrar un análisis detallado de vulnerabilidades, amenazas e iniciativas de mitigación, el estudio proporciona un marco conceptual y metodológico que resulta útil para académicos, profesionales y responsables de la toma de decisiones, promoviendo el desarrollo de estrategias de seguridad adaptativas, escalables y sostenibles que respondan a la complejidad y dinamismo de los entornos tecnológicos actuales (Mohanta et al., 2020; Franco et al., 2021). La comprensión profunda de estos retos se considera esencial para garantizar la protección integral de los sistemas, la resiliencia operativa y la confianza de los usuarios en infraestructuras cada vez más interconectadas.

Metodología

La presente investigación se desarrolló bajo un enfoque cualitativo, de carácter analítico-descriptivo, orientado a comprender de manera profunda los desafíos de seguridad digital en entornos de Internet de las Cosas (IoT) integrados con programas computarizados (Pangestu, 2025; Mendoza Villamar et al., 2025). Este enfoque se consideró el más adecuado, dado que el objetivo principal del estudio fue examinar fenómenos complejos, interdependientes y dinámicos, caracterizados por la interacción de dispositivos heterogéneos,

programas computarizados y redes de comunicación, aspectos que no pueden ser capturados completamente mediante metodologías cuantitativas tradicionales (Mohanta et al., 2020). La perspectiva cualitativa permitió explorar de manera interpretativa los patrones de vulnerabilidades, amenazas, impactos operativos y estrategias de mitigación documentadas en la literatura especializada, así como analizar las limitaciones técnicas y organizacionales que afectan la implementación de medidas de seguridad digital (Jammeh et al., 2026; Kasula, 2025).

El diseño metodológico adoptado se basó en una investigación documental no experimental, sustentada en la revisión sistemática y crítica de literatura científica especializada (Franco et al., 2021; Okporokpo et al., 2023). Esta modalidad permitió examinar de manera directa los hallazgos, enfoques y resultados de estudios previos sin necesidad de manipular variables o intervenir directamente sobre los objetos de estudio, garantizando un análisis imparcial y riguroso de la información existente. La investigación documental posibilitó, además, integrar conocimientos provenientes de distintas disciplinas, incluyendo ingeniería informática, ciberseguridad, automatización industrial, gestión de datos y análisis de riesgos, favoreciendo una comprensión holística de los retos de seguridad digital en sistemas interconectados (Radanliev et al., 2020; Uprety & Rawat, 2021; Saha et al., 2021).

La selección del corpus documental se realizó mediante criterios estrictos de pertinencia temática, actualidad, rigor académico y relevancia científica. Se priorizaron artículos publicados en revistas arbitradas, libros especializados, actas de congresos internacionales y documentos técnicos de organismos reconocidos en ciberseguridad y tecnologías IoT (Polk et al., 2017; Yang et al., 2024). Asimismo, se consideraron estudios recientes que reflejaran avances y tendencias actuales, sin excluir investigaciones fundamentales que aportaron un marco conceptual sólido sobre vulnerabilidades, amenazas y estrategias de mitigación (Mendoza Villamar et al., 2025; Jammeh et al., 2026).

Para la recopilación de información se emplearon búsquedas exhaustivas en bases de datos académicas como Scopus, IEEE Xplore, Web of Science, ScienceDirect y Google Scholar, utilizando descriptores relacionados con Internet de las Cosas, automatización de procesos, seguridad digital, gestión de identidades, cifrado de información, arquitecturas de sistemas seguros y resiliencia operativa. Esta estrategia permitió asegurar la inclusión de

fuentes relevantes y de alta calidad que abordaron los aspectos críticos de la seguridad en entornos IoT computarizados.

El análisis de la información se realizó mediante un enfoque analítico-crítico, que incluyó lectura comprensiva, interpretación contextualizada y comparación sistemática de los hallazgos de las fuentes seleccionadas. A partir de este proceso, se identificaron categorías conceptuales clave, tales como autenticación de dispositivos, cifrado de información, integridad y disponibilidad de programas computarizados, amenazas emergentes, impactos operativos, limitaciones técnicas y estrategias de mitigación de riesgos. Los datos extraídos se organizaron de manera sistemática en matrices analíticas y tablas comparativas, facilitando la visualización de patrones, relaciones entre variables y brechas existentes en la literatura científica, y permitiendo un análisis profundo de los factores que condicionan la seguridad digital en entornos automatizados y altamente interconectados.

Para garantizar la validez y confiabilidad del estudio, se aplicó la triangulación de fuentes, contrastando la información obtenida de diferentes autores, contextos, disciplinas y tipos de publicaciones. Este procedimiento permitió reducir posibles sesgos interpretativos y fortalecer la consistencia del análisis, asegurando que las conclusiones se sustentaran en evidencia sólida y diversificada. Asimismo, se adoptaron criterios de transparencia y trazabilidad documental, registrando las referencias y los hallazgos de manera sistemática para facilitar la replicabilidad y verificación del estudio por otros investigadores interesados en el tema.

Desde el punto de vista ético, la investigación se desarrolló respetando principios de integridad académica y uso responsable de la información. Todas las fuentes fueron citadas adecuadamente, preservando la fidelidad conceptual de las ideas revisadas. Al tratarse de una investigación documental, no se involucraron sujetos humanos ni se manipularon datos sensibles, lo que minimizó los riesgos éticos asociados y permitió centrar el análisis en evidencia científica previamente validada.

En síntesis, la metodología empleada proporcionó un marco sólido, riguroso y coherente para el análisis de la seguridad digital en entornos IoT integrados con programas computarizados. El enfoque cualitativo permitió capturar la complejidad del fenómeno, mientras que la revisión documental y el análisis crítico de la literatura especializada facilitaron

la identificación de vulnerabilidades, amenazas, impactos, limitaciones técnicas y estrategias de mitigación. Esta aproximación metodológica no solo garantiza la consistencia interna del estudio, sino que también contribuye a generar conocimiento fundamentado, útil para académicos, profesionales y responsables de la toma de decisiones, promoviendo la implementación de soluciones de seguridad digital integrales, adaptativas y sostenibles en entornos tecnológicos interconectados.

Resultados

a presente sección expone los hallazgos obtenidos tras la revisión sistemática y crítica de la literatura científica relacionada con la seguridad digital en entornos de Internet de las Cosas (IoT) integrados con programas computarizados. Los resultados se presentan mediante un análisis exhaustivo de vulnerabilidades, amenazas emergentes, limitaciones técnicas de los dispositivos, estrategias de mitigación y frecuencias de ocurrencia de los problemas identificados en los estudios seleccionados. Para facilitar la interpretación, se incluyen cinco tablas con información estructurada que sintetiza los datos obtenidos, acompañadas de explicaciones detalladas que contextualizan cada hallazgo y permiten establecer relaciones entre variables relevantes para la seguridad digital.

La identificación de vulnerabilidades constituyó un aspecto central de la revisión, dado que estas representan los puntos de entrada más recurrentes para ataques dirigidos a dispositivos conectados y a los programas computarizados que gestionan procesos automatizados. La Tabla 1 resume las vulnerabilidades más citadas en la literatura, su frecuencia de aparición en los estudios revisados, y el tipo de impacto asociado sobre la seguridad de los sistemas.

Tabla 1

Principales vulnerabilidades detectadas en entornos IoT integrados con programas computarizados

Vulnerabilidad	Descripción breve	Tipo de impacto	Frecuencia (%)	Referencias principales
Credenciales predeterminadas	Uso de contraseñas y accesos estándar no modificados	Acceso no autorizado	72	Cárdenas Quintero et al. (2024); Ramadan (2022)

ISSN-L 3072-9823
Núm. 2 Vol. 1
Abril 2026 - Marzo2027
1 – 20

Vulnerabilidad	Descripción breve	Tipo de impacto	Frecuencia (%)	Referencias principales
Cifrado insuficiente	Datos transmitidos sin protocolos robustos	Exposición de información	65	Ghazal et al. (2020); Morales Suárez et al. (2019)
Firmware desactualizado	Dispositivos con versiones antiguas de software	Vulnerabilidad explotable	58	Ramos Mosquera et al. (2025); Abiodun et al. (2021)
Comunicación insegura	Uso de protocolos vulnerables o sin autenticación	Interceptación de datos	53	Alrawais et al. (2017); Chukwuere (2024)
Configuración insegura	Ajustes por defecto que comprometen seguridad	Compromiso de integridad	47	Goel et al. (2023); Rueda Rueda & Portocarrero (2021)

Nota: La frecuencia indica el porcentaje de estudios revisados que reportan la vulnerabilidad señalada. *Fuente:* Elaboración propia a partir de la revisión sistemática de literatura científica.

La tabla 1 evidencia que las credenciales predeterminadas constituyen la vulnerabilidad más recurrente en los entornos IoT, seguida por problemas relacionados con cifrado y firmware desactualizado. Estas debilidades reflejan la insuficiente atención que se ha dado históricamente a la seguridad desde la fase de diseño de los dispositivos, lo que amplifica los riesgos para los programas computarizados que dependen de ellos. La alta frecuencia de vulnerabilidades relacionadas con la comunicación y configuración insegura resalta la necesidad de estándares homogéneos y protocolos de seguridad consistentes que puedan ser implementados de manera transversal en los distintos dispositivos conectados. Así mismo refleja las vulnerabilidades más documentadas en entornos IoT, destacando que credenciales predeterminadas y configuraciones inseguras son las más frecuentes, seguidas de cifrado insuficiente y firmware desactualizado. Esto evidencia la necesidad de controles de acceso robustos y políticas de actualización continua.

Las amenazas que explotan las vulnerabilidades identificadas presentan distintos niveles de riesgo, afectando la disponibilidad, integridad y confidencialidad de la información. La Tabla 2 organiza las principales amenazas documentadas, junto con sus vectores de ataque y frecuencia de reporte en la literatura.

Tabla 2

Amenazas cibernéticas más frecuentes en entornos IoT integrados

Amenaza	Vector de ataque	Tipo de impacto	Frecuencia (%)	Referencias principales
Malware especializado	Infección a través de dispositivos conectados	Compromiso de integridad	68	Habibu & Julius (2025); Singh et al. (2025)
Denegación de servicio (DoS/DDoS)	Saturación de recursos de red o dispositivos	Disponibilidad de servicios	61	Lakhani (2023); Halderman (2024)
Intercepción de datos	Ataques Man-in-the-Middle, sniffing	Confidencialidad	59	Ghazal et al. (2020); Abiodun et al. (2021)
Acceso no autorizado	Explotación de credenciales predeterminadas	Acceso a programas computarizados	55	Cárdenas Quintero et al. (2024); Ramadan (2022)
Manipulación de datos	Modificación de información en tránsito	Integridad de datos	51	Ramos Mosquera et al. (2025); Morales Suárez et al. (2019)

Nota: La frecuencia indica el porcentaje de estudios revisados que identifican la amenaza señalada.

Fuente: Elaboración propia basada en revisión sistemática de literatura científica.

Como se observa en la tabla 2, el malware especializado y los ataques de denegación de servicio constituyen las amenazas más prevalentes, afectando directamente la continuidad de los programas computarizados y, en muchos casos, provocando interrupciones significativas en procesos automatizados. La intercepción de datos y la manipulación de información reflejan

la vulnerabilidad de la comunicación y la falta de cifrado robusto, mientras que el acceso no autorizado evidencia la explotación directa de credenciales predeterminadas y configuraciones inseguras. Los ataques más frecuentes incluyen malware y denegación de servicio, afectando la integridad y disponibilidad de los sistemas. La intercepción y manipulación de datos evidencia deficiencias en cifrado y protocolos de comunicación.

La diversidad de dispositivos y las limitaciones inherentes de hardware y software influyen de manera significativa en la capacidad de implementar medidas de seguridad efectivas. La Tabla 3 detalla estas limitaciones y su frecuencia relativa en la literatura revisada.

Tabla 3

Limitaciones técnicas de dispositivos IoT y su incidencia en la seguridad

Limitación técnica	**Descripción**	**Impacto en seguridad**	**Frecuencia (%)**	**Referencias principales**
Capacidad de procesamiento limitada	Dispositivos con recursos insuficientes	Restricción en cifrado y autenticación	64	Abiodun et al. (2021); Chukwuere (2024)
Almacenamiento limitado	Memoria insuficiente para registros de seguridad	Dificulta auditoría y monitoreo	59	Morales Suárez et al. (2019); Ramadan (2022)
Heterogeneidad tecnológica	Diferentes fabricantes y protocolos	Problemas de interoperabilidad	56	Ferrag et al. (2025); Sivarao et al. (2024)
Dependencia de red	Necesidad constante de conectividad	Vulnerabilidad a interrupciones	51	Halderman (2024); Alrawais et al. (2017)

Nota: La frecuencia refleja la proporción de estudios que mencionan la limitación técnica como factor de riesgo para la seguridad. *Fuente:* Elaboración propia basada en revisión documental sistemática.

Estas limitaciones técnicas de la tabla 3, contribuyen a un panorama de riesgo persistente, donde la incapacidad de implementar cifrado robusto o actualizaciones automáticas deja a los dispositivos y programas computarizados expuestos frente a ataques sofisticados. La heterogeneidad tecnológica y la dependencia de la conectividad aumentan la complejidad de diseñar estrategias de mitigación que sean efectivas en todo el ecosistema IoT. Las limitaciones técnicas condicionan la implementación de medidas de seguridad avanzadas, evidenciando la necesidad de soluciones adaptativas y protocolos eficientes que funcionen en dispositivos con capacidad limitada.

Para contrarrestar las vulnerabilidades y amenazas descritas, la literatura revisada propone diversas estrategias de mitigación. La Tabla 4 resume las más relevantes, indicando su enfoque, eficacia reportada y frecuencia de aparición en estudios recientes.

Tabla 4

Estrategias de mitigación en entornos IoT integrados con programas computarizados

Estrategia	**Descripción**	**Enfoque**	**Frecuencia (%)**	**Referencias principales**
Seguridad por diseño (Security by Design)	Integración de seguridad desde la concepción	Preventivo	71	Abiodun et al. (2021); Ferrag et al. (2025)
Autenticación multifactor	Combinación de credenciales y dispositivos	Control de acceso	65	Goel et al. (2023); García Pérez & Arzube (2024)
Cifrado robusto	Protocolos criptográficos avanzados	Protección de datos	62	Ghazal et al. (2020); Morales Suárez et al. (2019)

Estrategia	Descripción	Enfoque	Frecuencia (%)	Referencias principales
Gestión avanzada de identidades	Administración centralizada y controlada	Gestión de accesos y privilegios	59	Chukwuere (2024); Ramadan (2022)
Actualizaciones automáticas	Software y firmware mantenidos al día	Prevención de vulnerabilidades	54	Ramos Mosquera et al. (2025); Patil (2025)

Nota: La frecuencia indica el porcentaje de estudios revisados que recomiendan la estrategia mencionada. *Fuente:* Elaboración propia basada en revisión sistemática de literatura científica.

Como se observa en la tabla 4, la implementación de estrategias como seguridad por diseño y autenticación multifactorial se destaca por su capacidad de prevenir incidentes antes de que ocurran, mientras que la gestión avanzada de identidades y el cifrado robusto proporcionan barreras efectivas frente a amenazas ya existentes. Las actualizaciones automáticas son esenciales para cerrar vulnerabilidades descubiertas post-lanzamiento, asegurando la resiliencia de los dispositivos y programas computarizados frente a ataques emergentes. Las estrategias preventivas y de protección actúan sobre diferentes vulnerabilidades, garantizando confidencialidad, integridad y disponibilidad de los sistemas integrados.

La integración estrecha entre dispositivos IoT y programas computarizados introduce un riesgo adicional: los incidentes en un componente pueden desencadenar efectos en cascada que comprometan múltiples sistemas interdependientes. La Tabla 5 sintetiza los tipos de impacto más documentados, su frecuencia y la relación con los desafíos de seguridad identificados.

Tabla 5

Impacto de la integración IoT-programas computarizados en la seguridad digital

Tipo de impacto	Descripción	Relación con vulnerabilidad o amenaza	Frecuencia (%)	Referencias principales
Interrupción de procesos	Detención temporal o permanente de operaciones	DoS, malware	66	Lakhani (2023); Singh et al. (2025)
Pérdida de integridad de datos	Alteración o corrupción de información	Acceso no autorizado, manipulación	62	Ramadan (2022); Ramos Mosquera et al. (2025)
Exposición de información	Divulgación no autorizada de datos sensibles	Cifrado insuficiente, interceptación	59	Ghazal et al. (2020); Morales Suárez et al. (2019)
Compromiso de disponibilidad	Sistemas o servicios inaccesibles	Vulnerabilidades de firmware y red	55	Halderman (2024); Abiodun et al. (2021)
Efectos en cascada	Propagación de incidentes entre componentes	Interdependencia tecnológica	51	Ferrag et al. (2025); Sivarao et al. (2024)

Nota: La frecuencia refleja la proporción de estudios revisados que reportan cada tipo de impacto. *Fuente:* Elaboración propia basada en revisión sistemática de literatura científica.

Los impactos documentados en la tabla 5, muestran que la seguridad digital en entornos IoT integrados con programas computarizados no solo se limita a la protección de información aislada, sino que afecta directamente la continuidad operativa y la confiabilidad de los sistemas automatizados. La presencia de efectos en cascada destaca la necesidad de enfoques de mitigación que consideren la totalidad del ecosistema tecnológico, integrando dispositivos, redes y programas computarizados en un modelo de seguridad holístico y adaptativo. La integración IoT-programas computarizados genera riesgos de propagación en cascada,

afectando múltiples sistemas. Esto resalta la importancia de enfoques holísticos de seguridad que consideren la totalidad del ecosistema.

En conjunto, los hallazgos de esta revisión sistemática confirman que los entornos IoT integrados con programas computarizados presentan un panorama de riesgo complejo, donde las vulnerabilidades técnicas, la diversidad de dispositivos, la falta de interoperabilidad y la insuficiente implementación de medidas de seguridad constituyen factores críticos que incrementan la probabilidad de incidentes cibernéticos. Las amenazas identificadas van desde el malware especializado y los ataques de denegación de servicio hasta la manipulación y exposición de datos, afectando la integridad, disponibilidad y confidencialidad de los sistemas.

Las estrategias de mitigación más efectivas son aquellas que combinan prevención, protección y resiliencia, incluyendo seguridad por diseño, autenticación multifactorial, cifrado robusto, gestión avanzada de identidades y actualizaciones automáticas. Sin embargo, la adopción de estas medidas requiere superar limitaciones técnicas, garantizar compatibilidad entre dispositivos heterogéneos y promover estándares universales que faciliten la implementación de modelos de seguridad integrales.

En síntesis, los resultados enfatizan que la seguridad digital en entornos IoT-computarizados debe abordarse de manera holística, considerando la interacción de todos los componentes del sistema y adoptando un enfoque adaptativo, continuo y basado en el ciclo de vida completo de los dispositivos y programas. Esta perspectiva permite minimizar riesgos, proteger información crítica y asegurar la continuidad operativa en ecosistemas altamente interdependientes, cumpliendo con los estándares contemporáneos de ciberseguridad y resiliencia tecnológica.

Discusión

Los resultados de esta investigación evidencian que la seguridad digital en entornos de Internet de las Cosas (IoT) integrados con programas computarizados constituye un desafío complejo y multifactorial, determinado por la convergencia de vulnerabilidades técnicas, diversidad tecnológica y creciente sofisticación de las amenazas. La revisión sistemática permitió identificar que las vulnerabilidades más frecuentes corresponden al uso de credenciales predeterminadas, el cifrado insuficiente, el firmware desactualizado, la

comunicación insegura y las configuraciones de fábrica poco protegidas. Estos hallazgos coinciden con lo reportado por Cárdenas Quintero et al. (2024) y Ramadan (2022), quienes señalan que la ausencia de controles de acceso robustos y de políticas de actualización continua facilita la explotación de los dispositivos conectados y de los programas computarizados que dependen de ellos. Esta persistencia de fallas demuestra que la integración de la seguridad desde la fase de diseño sigue siendo limitada, especialmente en dispositivos de bajo costo y con capacidades restringidas, lo que mantiene un nivel de riesgo elevado y sostenido en los ecosistemas IoT.

Las amenazas más documentadas, entre ellas el malware especializado, los ataques de denegación de servicio (DoS/DDoS), la intercepción de datos, el acceso no autorizado y la manipulación de información, reflejan la forma en que dichas vulnerabilidades se transforman en vectores efectivos de ataque. La literatura revisada muestra que estas amenazas no solo comprometen la confidencialidad, integridad y disponibilidad de la información, sino que impactan directamente en la continuidad operativa de los programas computarizados y en la eficiencia de los procesos automatizados. Singh et al. (2025) y Habibu y Julius (2025) advierten que el malware puede propagarse de manera simultánea en múltiples dispositivos interconectados, generando efectos en cascada que afectan a sistemas críticos. Asimismo, Lakhani (2023) y Halderman (2024) destacan que los ataques orientados a la saturación de recursos representan una amenaza significativa para la disponibilidad de los servicios, lo que confirma que la resiliencia de los sistemas IoT-computarizados depende tanto de la robustez individual de los dispositivos como de la arquitectura global de red.

Las limitaciones técnicas propias de los dispositivos IoT se consolidan como factores determinantes en la implementación de medidas de seguridad eficaces. La escasa capacidad de procesamiento y almacenamiento, la heterogeneidad tecnológica y la dependencia de la conectividad restringen la adopción de protocolos criptográficos avanzados, sistemas de autenticación complejos y mecanismos de actualización automática. Abiodun et al. (2021), Chukwuere (2024) y Morales Suárez et al. (2019) coinciden en que estas restricciones generan escenarios donde incluso las estrategias de mitigación más avanzadas pueden verse comprometidas, especialmente cuando se requiere interoperabilidad entre dispositivos de distintos fabricantes o cuando la infraestructura de red presenta deficiencias. Ferrag et al.

(2025) y Sivarao et al. (2024) subrayan que la ausencia de estándares universales constituye una barrera crítica para la estandarización de las medidas de seguridad, lo que exige soluciones adaptativas y flexibles acordes con las capacidades específicas de cada componente del ecosistema.

La evidencia recopilada confirma que las estrategias de mitigación más eficaces son aquellas que adoptan un enfoque integral, combinando prevención, protección y resiliencia. La seguridad por diseño, la autenticación multifactorial, el cifrado robusto, la gestión avanzada de identidades y las actualizaciones automáticas emergen como pilares fundamentales para reducir la exposición a amenazas y garantizar la continuidad de los programas computarizados. Abiodun et al. (2021) y Ferrag et al. (2025) demuestran que la incorporación de mecanismos de seguridad desde la fase de concepción disminuye significativamente la probabilidad de explotación de vulnerabilidades conocidas. De igual forma, la autenticación multifactorial y el cifrado fortalecen las barreras frente al acceso no autorizado y la interceptación de datos, como lo sostienen Goel et al. (2023) y García Pérez y Arzube (2024). Las actualizaciones automáticas, según Ramos Mosquera et al. (2025) y Patil (2025), resultan esenciales para mantener la resiliencia ante vulnerabilidades descubiertas después del despliegue de los sistemas.

El análisis de los impactos documentados revela que los riesgos asociados a la integración entre IoT y programas computarizados trascienden la protección de la información y afectan directamente la confiabilidad y la continuidad operativa de los sistemas. La interrupción de procesos, la pérdida de integridad de los datos, la exposición de información sensible y los efectos en cascada evidencian que los incidentes no se limitan a componentes aislados, sino que se propagan rápidamente entre sistemas interdependientes. Lakhani (2023) y Singh et al. (2025) destacan que esta interconectividad amplifica las consecuencias económicas, operativas e incluso físicas de los ataques, lo que subraya la necesidad de enfoques de mitigación holísticos capaces de considerar la totalidad del ecosistema tecnológico.

Un hallazgo relevante es la relación directa entre las limitaciones técnicas de los dispositivos y la efectividad de las estrategias de mitigación. Los equipos con recursos restringidos requieren soluciones de seguridad optimizadas que reduzcan la carga computacional sin comprometer la protección de la información ni la continuidad de los

procesos. Alrawais et al. (2017) y Halderman (2024) enfatizan que la dependencia de la conectividad y la diversidad de protocolos incrementan la complejidad de la gestión de seguridad, lo que hace imprescindible el desarrollo de soluciones escalables e interoperables. En este sentido, la adopción de estándares universales y la promoción de la interoperabilidad tecnológica se identifican como elementos clave para fortalecer la resiliencia de los sistemas IoT-computarizados.

En síntesis, los resultados confirman que la seguridad digital en entornos IoT integrados con programas computarizados no puede abordarse de forma fragmentada ni reactiva. La convergencia de vulnerabilidades técnicas, diversidad de dispositivos y amenazas sofisticadas configura un escenario de riesgo elevado, en el que los incidentes pueden producir efectos en cascada con repercusiones significativas en la disponibilidad, integridad y confidencialidad de la información. La literatura revisada demuestra que la combinación de estrategias preventivas, protectivas y resilientes, alineadas con todo el ciclo de vida de los dispositivos y programas, constituye el enfoque más sólido para garantizar la seguridad y la continuidad operativa de los ecosistemas IoT.

En conclusión, esta investigación permitió establecer un panorama integral sobre los desafíos de la seguridad digital en entornos IoT integrados con programas computarizados, evidenciando que se trata de un problema complejo que requiere estrategias holísticas y adaptativas. Las vulnerabilidades recurrentes reflejan deficiencias históricas en la incorporación de la seguridad desde el diseño de los dispositivos y ponen de manifiesto la necesidad de estándares de protección consistentes y universales. Las amenazas emergentes, como el malware especializado y los ataques de denegación de servicio, confirman que los riesgos no solo afectan a la información aislada, sino que comprometen la continuidad y confiabilidad de sistemas automatizados altamente interdependientes.

Asimismo, se ratifica que las limitaciones técnicas de los dispositivos, la heterogeneidad tecnológica y la dependencia de la conectividad condicionan la aplicación efectiva de las estrategias de mitigación, lo que exige arquitecturas de seguridad flexibles y optimizadas. La combinación de seguridad por diseño, autenticación multifactorial, cifrado robusto, gestión avanzada de identidades y actualizaciones automáticas se consolida como la vía más efectiva para reducir la exposición a riesgos y fortalecer la resiliencia tecnológica.

A partir de los hallazgos obtenidos, se recomienda que los desarrolladores de dispositivos IoT y los responsables de los programas computarizados adopten un enfoque integral de seguridad que considere el ciclo de vida completo de los sistemas. Es fundamental priorizar la actualización continua de firmware y software, la implementación de protocolos criptográficos sólidos y la autenticación multifactorial para disminuir el acceso no autorizado. Del mismo modo, resulta necesario promover la estandarización tecnológica y la interoperabilidad entre dispositivos heterogéneos, así como la gestión centralizada de identidades y la monitorización proactiva de amenazas. Estas acciones deben complementarse con estrategias de resiliencia que mitiguen los efectos en cascada de los incidentes y con procesos de formación y sensibilización de usuarios y operadores, fortaleciendo una cultura organizacional de ciberseguridad que garantice la continuidad operativa en entornos IoT cada vez más complejos e interdependientes.

Referencias

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the Internet of Things: Challenges and solutions. *Wireless Personal Communications*, *119*, 2611–2634. https://doi.org/10.1007/s11277-021-08348-9

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34–42. https://doi.org/10.1109/MIC.2017.37

Cárdenas-Quintero, D., Ropero-Silva, E., Puerto-López, K., Sanchez-Mojica, K., & Castro-Casadiego, S. (2024). Vulnerabilidad en la seguridad del Internet de las cosas. *Mundo FESC*, *14*(27), 35–46. https://doi.org/10.61799/2216-0388.542

Chukwuere, J. E. (2024). Internet of Things (IoT) cybersecurity challenges and mitigation mechanisms. *Khazanah Sosial*, *4*(2), 312–325. https://doi.org/10.15575/ks.v4i2.17638

Ferrag, M. A., Maglaras, L., Katsikas, S., Janicke, H., & Maglaras, A. (2025). A survey on cybersecurity in IoT. *Future Internet*, *17*(1), 30. https://doi.org/10.3390/fi17010030

Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). *A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems*. arXiv. https://arxiv.org/abs/2108.02287

García Pérez, K., & Arzube, O. A. (2024). Proactive strategies to mitigate emerging cybersecurity risks in IoT devices for smart homes. *Minerva*, *5*(15), 171–185. https://doi.org/10.47460/minerva.v5i15.171

Ghazal, T. M., Alzoubi, H. M., Alshurideh, M., & Agag, G. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Goel, P., Jain, A., & Juneja, D. (2023). Security issues on Internet of Things (IoT): A recent challenges and countermeasures. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, *11*(12). https://doi.org/10.22214/ijraset.2023.57760

Habibu, T., & Julius, A. P. (2025). Cybersecurity in the Internet of Things (IoT) – Review. *DS Journal of Cyber Security*, *3*(3), 15–38. https://doi.org/10.59232/CYS-V3I3P102

Halderman, J. A. (2024). *ZMap and IoT security research contributions*. University of Michigan. https://jhalderm.com/

Jammeh, J. E., Fleury, M., & State, R. (2026). A comprehensive survey on IoT security: Challenges, security issues, and countermeasures. *Computer Science Review*, *59*, 100839. https://doi.org/10.1016/j.cosrev.2025.100839

Kasula, V. K. (2025). Comprehensive analysis of IoT security: Threats, detection methods, and defense strategies. *Journal on Internet of Things*, *7*(1), 19–48. https://doi.org/10.32604/jiot.2025.062733

Lakhani, R. (2023). Cybersecurity threats in Internet of Things (IoT) networks: Vulnerabilities and defense mechanisms. *International Journal of Engineering and Computer Science*, *12*(11), 25965–25981. https://doi.org/10.18535/ijecs/v12i11.4779

Mendoza Villamar, R., Prado Vera, O., & Coveña Coveña, S. (2025). Amenazas de seguridad y sus soluciones en el Internet de las cosas (IoT). *Revista Tse'de*, *8*(3). https://doi.org/10.60100/tsede.v8i3.289

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Danezi, M., & Gani, A. (2020). *Security and privacy in IoT using machine learning and blockchain: Threats & countermeasures*. arXiv. https://arxiv.org/abs/2002.03488

Morales Suárez, A. C., Díaz Ávila, S. S., & Leguizamón Páez, M. Á. (2019). Mecanismos de seguridad en el internet de las cosas. *Revista Vínculos*, *16*(1), 104–115. https://doi.org/10.14483/2322939X.15758

Okporokpo, O., Olajide, F., Ajienka, N., & Ma, X. (2023). *Trust-based approaches towards enhancing IoT security: A systematic literature review*. arXiv. https://arxiv.org/abs/2311.11705

Pangestu, R. (2025). Security landscape of the Internet of Things (IoT): A systematic review of vulnerabilities, defense mechanisms, and future research directions. *Quanta Research*, *1*(1). https://ejournal.resincen.org/index.php/quanta/article/view/32

Patil, S. S. (2025). Artificial intelligence in IoT security: Uncovering opportunities and threats. *Oriental Journal of Computer Science and Technology*, *17*(1), 26–29. http://dx.doi.org/10.13005/ojcst17.01.08

Polk, W., Souppaya, M., & Barker, W. (2017). *Mitigating IoT-based automated distributed threats* (NIST Cybersecurity Practice Guide). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/pd/2017/10/12/mitigating-iotbased-automated-distributed-threats/ipd

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0

Ramadan, R. A. (2022). Internet of Things (IoT) security vulnerabilities: A review. *PLOMS AI*, *2*(1). https://plomscience.com/journals/index.php/PLOMSAI/article/view/14

Ramos Mosquera, B., García Enríquez, M. C., & Barriga Diaz, R. A. (2025). Análisis de vulnerabilidades en dispositivos IoT mediante algoritmos de búsqueda en Shodan: Riesgos y estrategias de mitigación. *Sinergia Académica*, *8*(1). https://doi.org/10.51736/sa761

Rueda-Rueda, J. S. R., & Portocarrero, J. M. T. (2021). Framework-based security measures for Internet of Thing: A literature review. *Open Computer Science*, *11*(1), 145–162. https://doi.org/10.1515/comp-2020-0220

Saha, T., Aaraj, N., Ajjarapu, N., & Jha, N. K. (2021). *SHARKS: Smart hacking approaches for risk scanning in Internet-of-Things and cyber-physical systems based on machine learning*. arXiv. https://arxiv.org/abs/2101.02780

Singh, S., Sharma, S. K., & Kumar, R. (2025). *Deep reinforcement learning for intrusion detection in IoT: A survey*. arXiv. https://arxiv.org/abs/2405.20038

Sivarao, S., Ammar, A., Al-Dhaqm, A., & Al-Hadhrami, T. (2024). IoT security: Systematic insights into architectures, threats, and defenses. *Electronics*, *14*(20), 3972. https://doi.org/10.3390/electronics14203972

Uprety, A., & Rawat, D. B. (2021). *Reinforcement learning for IoT security: A comprehensive survey*. arXiv. https://arxiv.org/abs/2102.07247

Yang, Z., Lu, X., & Chen, Y. (2024). Distributed reinforcement learning for IoT security in heterogeneous networks. *Scifiniti*, *1*(1). https://scifiniti.com/3104-4719/1/2024.0008