Doi: *https://doi.org/10.26495/23m7xb95*
Fondo Editorial USS

Impacto de la IA en la gestión de seguridad de infraestructuras cloud en entornos TI: Una revisión sistemática

Impact of AI on cloud infrastructure security management in IT environments: A systematic review

Juan Diego Molina Nanfuñay[1], Leonardo Javier Guimaray Matute[1], Alberto Carlos Mendoza de los Santos[1]

[1]Universidad Nacional de Trujillo, Trujillo-La Libertad

Cómo citar
J. D. Molina Nanfuñay, L. J. Guimaray Matute, and A. C. Mendoza de los Santos, "Impacto de la IA en la gestión de seguridad de infraestructuras cloud en entornos TI: Una revisión sistemática," Ingeniería: ciencia, tecnología e innovación, vol. 13, 2026. https://doi.org/10.26495/23m7xb95

RESUMEN: El presente artículo **tuvo** como objetivo analizar el impacto de la inteligencia artificial en la gestión de la seguridad de infraestructuras cloud en entornos de TI, identificando sus principales aplicaciones, beneficios y desafíos. **Metodología:** Se realizó una revisión sistemática de la literatura, siguiendo la metodología PRISMA, a partir de artículos científicos y estudios relevantes publicados entre 2021 y 2025 en bases de datos académicas como Scopus y Google Scholar. **Resultados:** Los estudios seleccionados evidencian que la IA mejora la detección temprana de amenazas, automatiza procesos de seguridad críticos y optimiza la respuesta ante incidentes, contribuyendo al fortalecimiento de la gestión de servicios TI en la nube; sin embargo, también revelan riesgos asociados a la privacidad de los datos, la pérdida de control y la creciente dependencia tecnológica. **Conclusiones**: Se concluye que la IA constituye un recurso clave para incrementar la protección de las infraestructuras cloud, siempre que su implementación se realice de manera planificada, bajo marcos de buenas prácticas y con una supervisión humana constante que mitigue la aparición de vulnerabilidades no previstas.

Palabras clave: Ciberseguridad, gestión de riesgos, gestión de servicios TI, inteligencia artificial, seguridad en la nube.

Información del artículo
Recibido: 09/05/2025
Aceptado: 30/12/2025
Publicado: 13/02/2026

Autor correspondencia
Juan Diego Molina Nanfuñay
jmolina@unitru.edu.pe

ABSTRACT: This article **aimed** to analyze the impact of artificial intelligence on the security management of cloud infrastructures in IT environments, identifying its main applications, benefits, and challenges. **Methodology**: A systematic literature review was conducted using the PRISMA methodology, based on scientific papers and relevant studies published between 2021 and 2025 in academic databases such as Scopus and Google Scholar. **Results:** The selected studies show that AI enhances early threat detection, automates critical security processes, and optimizes incident response, thereby strengthening cloud-based IT service management; however, they also reveal risks related to data privacy, loss of control, and increasing technological dependency. **Conclusions:** It is concluded that AI is a key resource for improving the protection of cloud infrastructures, provided that its implementation is carefully planned, aligned with best-practice frameworks, and supported by continuous human oversight to mitigate unforeseen vulnerabilities.

.Keywords: Cybersecurity, risk management, IT service management, Artificial intelligence, cloud security.

1. INTRODUCCIÓN

El enfoque en la nube está ganando aceptación como un componente fundamental dentro del proceso de transformación digital de las organizaciones modernas, facilitando la adopción de tecnologías avanzadas que responden a las necesidades de un entorno empresarial que está transformándose y se mantiene en constante evolución [1]. Siguiendo este contexto, la nube ha cambiado su rol inicial de una simple alternativa tecnológica a un requisito indispensable para una exitosa adopción de las herramientas de IA, ya que actúa como la infraestructura base para su operatividad. La computación en la nube, la IA y la sinergia entre ambas han revolucionado la forma en la que se desenvuelven los sistemas de información, que han pasado de arquitecturas rígidas a entornos dinámicos y adaptables, diseñados para acelerar el entrenamiento de modelos, ofrecer inferencia en tiempo real y mantener sistemas de aprendizaje continuo.

Con la expansión del entorno en la nube, la seguridad de esta se ha convertido en una preocupación primordial para las organizaciones alrededor del mundo. La gran cantidad de información que es almacenada y tratada en entornos de la nube hace que la seguridad sea un tema que exige a las organizaciones una atención constante a fin de preservar la integridad de los datos [2]. Asimismo, la seguridad en la nube abarca diversas áreas, que incluyen el cifrado de datos para asegurar la confidencialidad, la seguridad de la red para prevenir el acceso de agentes no autorizados, el manejo de identidades para controlar quién puede acceder a qué recursos y, por último, el cumplimiento normativo para certificar que se están respetando los estándares y las regulaciones aplicables [3].

La IA se destaca también como una solución tecnológica que puede transformar lo que se conoce del manejo de la seguridad. Gracias al entrenamiento con datos a gran escala, la IA aprende y mejora de manera continua su capacidad para procesar información y realizar predicciones a partir de la retroalimentación y la comparación [4]. Este entrenamiento previo le otorga una ventaja frente al trabajador humano para detectar ataques de phishing avanzados, malware, ransomware, ataques DDoS y comportamientos anómalos de los usuarios que interactúan con el sistema [2].

Teniendo en cuenta lo previamente mencionado, la presente revisión sistemática de la literatura (RSL) se plantea como problema de investigación la siguiente interrogante general: ¿Qué beneficios trae la integración del uso de la IA en la gestión de la seguridad de infraestructuras cloud dentro de entornos de TI?
A partir de esta pregunta general, la RSL se orienta a responder las siguientes preguntas específicas:

- ¿Cuáles son las principales aplicaciones de la IA en la gestión de la seguridad de infraestructuras cloud dentro de entornos de TI?
- ¿Qué beneficios y desafíos surgen de la implementación de IA en la gestión de la seguridad en la nube?
- ¿Qué recomendaciones pueden proponerse para mejorar la integración de la IA en la gestión de la seguridad de las infraestructuras cloud?

Aunque en los últimos años se han publicado diversos trabajos sobre seguridad en la nube e inteligencia artificial, muchos de ellos se concentran en casos de uso, dominios o tecnologías puntuales, lo que genera una visión fragmentada del estado actual del conocimiento [2], [5]. En este sentido, una revisión sistemática de la literatura resulta necesaria para sintetizar la evidencia disponible, organizar los hallazgos dispersos, identificar vacíos de investigación y ofrecer una perspectiva estructurada que sirva de base para la toma de decisiones en la gestión de servicios TI sobre infraestructuras cloud apoyadas en IA.

El alcance de esta revisión se enfocó en los aspectos específicos del manejo de seguridad en infraestructuras cloud donde la IA tiene un impacto significativo, incluyendo el manejo de identidades y accesos, la reacción rápida ante incidentes de seguridad, el análisis eficiente de vulnerabilidades, la monitorización y registro de seguridad, así como el desempeño normativo y la gestión de riesgos.

Se sabe que la seguridad en las infraestructuras de la nube ha emergido como un campo de investigación relevante, en conjunto con estudios que abordan los desafíos de este entorno, que incluyen tanto las amenazas internas como externas, la protección de los datos personales y el cumplimiento de las diversas normativas regulatorias [2]. Investigaciones previas han explorado la progresiva aplicación de la IA en el entorno de la ciberseguridad, destacando su capacidad para integrar datos de múltiples servicios en la nube y proporcionar una visión holística de los riesgos y vulnerabilidades existentes [5]. Por otro lado, ITIL v4, un marco de buenas prácticas de TI, reconoce explícitamente el manejo de la seguridad informática como una práctica esencial dentro del modelo de gestión de servicios de TI, que debe ser considerada en todas las actividades de planificación e integrarse de manera transversal en cada una de las prácticas y servicios que ofrece la organización.

2. MÉTODOS Y METODOLOGÍA COMPUTACIONAL

En esta investigación se realizó una revisión sistemática de la literatura enfocada en el impacto de las tecnologías de inteligencia artificial para el manejo de la seguridad en infraestructuras cloud dentro de entornos de TI. El estudio adoptó un enfoque cualitativo de tipo documental, con diseño de revisión sistemática, sustentado en las directrices PRISMA. La población estuvo conformada por artículos científicos y ponencias indexados en las bases de datos Scopus y Google Scholar, publicados entre 2021 y 2025. A partir de esta población se obtuvo una muestra final de nueve estudios, seleccionados mediante criterios explícitos de inclusión y exclusión. Las categorías de análisis se agruparon en cuatro dimensiones: automatización de la detección y respuesta a incidentes, optimización de la protección en la nube, mejora de la gestión de riesgos y privacidad, y desafíos y oportunidades en la seguridad cloud.

2.1 Fundamentación de la metodología

Una revisión sistemática permite organizar de manera explícita y ordenada la evidencia disponible sobre un tema específico, lo que facilita la formulación de preguntas de investigación más precisas a partir de un proceso estructurado y transparente [6]. En este trabajo se siguieron las recomendaciones de la guía PRISMA, que orienta la identificación, selección, evaluación crítica y síntesis de los estudios, contribuyendo a mejorar la calidad metodológica de las revisiones sistemáticas [7].

2.2 Estrategia de búsqueda

La búsqueda de información se realizó en dos bases de datos académicas de amplia cobertura: Scopus y Google Scholar. Se consideraron publicaciones comprendidas entre los años 2021 y 2025, con el fin de recoger los aportes más recientes sobre el uso de la IA en la gestión de la seguridad en la nube. La búsqueda se ejecutó en los campos de título, resumen y palabras clave, priorizando estudios relacionados con ciberseguridad, servicios cloud, inteligencia artificial y gestión de servicios TI.

2.3 Términos de búsqueda

Para construir la estrategia de búsqueda se combinaron palabras clave en inglés relacionadas con inteligencia artificial, computación en la nube, aprendizaje automático, seguridad en la nube y tecnologías de la información. Estas palabras se articularon mediante operadores lógicos (AND) con el propósito de delimitar la intersección entre IA y seguridad en infraestructuras cloud.

2.4 Fórmulas de búsqueda por bases de datos

Scopus: (TITLE-ABS-KEY ("artificial intelligence" AND "cloud services") AND TITLE-ABS-KEY (network AND security) AND TITLE-ABS-KEY (machine AND learning) AND TITLE-ABS-KEY (cloud AND security))

Google Scholar: "artificial intelligence" AND "cloud services" AND "network security" AND "machine learning" AND "cloud security" AND "information technologies"

2.5 Parámetros de inclusión y exclusión

Parámetros de inclusión

Se incluyeron artículos publicados entre 2021 y 2025, relacionados con las áreas de informática, ingeniería, toma de decisiones y estudios empresariales. Los estudios debían abordar de manera explícita temas vinculados con inteligencia artificial, aprendizaje automático, computación en la nube, servicios cloud, seguridad en la nube, ciberseguridad, protección de datos o seguridad de la información. Asimismo, se consideraron únicamente artículos de revistas científicas y trabajos presentados en conferencias académicas.

Parámetros de exclusión

Se excluyeron los documentos duplicados y aquellos que no abordaban de forma directa la relación entre servicios en la nube, inteligencia artificial, aprendizaje automático y seguridad en la nube. También se descartaron fuentes no académicas (informes técnicos, entradas de blogs, material divulgativo), trabajos sin acceso completo y publicaciones fuera del rango temporal establecido (anteriores a 2021 o posteriores a 2025).

2.6 Proceso de selección de estudios

Inicialmente, se identificaron 303 artículos mediante la búsqueda en las dos bases de datos mencionadas. A continuación, se aplicaron los criterios de inclusión y exclusión de manera secuencial:

Identificación

En la fase de identificación se recuperaron 303 registros: 64 provenientes de Scopus y 239 de Google Scholar. Tras la eliminación de duplicados y la revisión inicial de títulos y resúmenes, se descartaron los trabajos que no cumplían con los criterios de inclusión, quedando 33 estudios para una evaluación más detallada.

Cribado

En la fase de cribado se procedió a la lectura crítica de resúmenes y palabras clave, lo que permitió seleccionar 25 artículos con mayor pertinencia temática. Posteriormente, en la etapa de elegibilidad se obtuvo el texto completo de estos 25 documentos y se aplicaron nuevamente los criterios de inclusión y exclusión. En esta fase se excluyeron 10 artículos por centrarse en contextos tecnológicos que no involucraban directamente

infraestructuras cloud, por tratar la IA sin vincularla a la seguridad o por no aportar información suficiente sobre la gestión de la seguridad en la nube.

Evaluación de texto

Se obtuvo acceso completo a 25 artículos, de los cuales 10 fueron excluidos por no cumplir con los criterios específicos de servicios y seguridad en la nube e inteligencia artificial.

Selección final

Como resultado de este proceso, se obtuvo una muestra final de 9 artículos que respondían de manera adecuada a las preguntas de investigación y al objetivo de la revisión sistemática. Este procedimiento se resume en el diagrama de flujo PRISMA presentado en la Figura 1, donde se detallan las fases de identificación, cribado, elegibilidad y selección final de los estudios, y a su vez un resumen de los registros identificados en la Tabla 1.

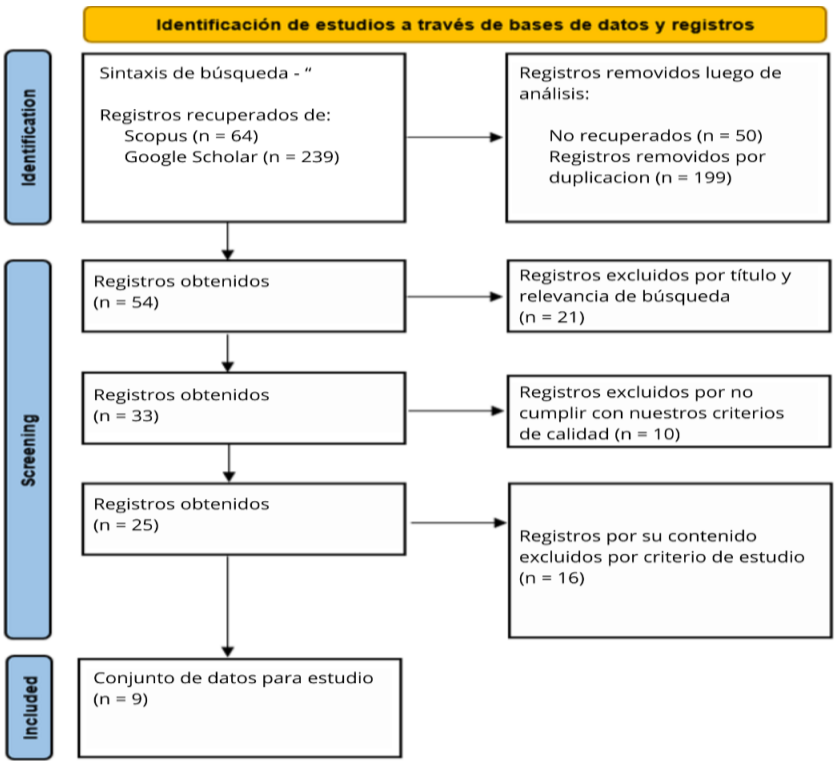

Figura 1. Diagrama de flujo PRISMA en cuatro niveles.
Fuente: elaboración propia.

Tabla 1. Número de registros identificados mediante búsquedas en bases de datos.
Fuente: elaboración propia.

Base de datos	Número de artículos
Scopus	64
Google Scholar	239
Total	303

Fuente: elaboración propia.

3. RESULTADOS

En esta sección se presentan los hallazgos obtenidos a partir de la revisión sistemática de la literatura, luego de aplicar los criterios de inclusión y exclusión descritos en el apartado

metodológico. De un total de 303 registros identificados en Scopus y Google Scholar, se seleccionó finalmente una muestra de 9 artículos que abordan la relación entre inteligencia artificial y gestión de la seguridad en infraestructuras cloud desde distintos contextos de aplicación (ciberseguridad general, servicios en la nube, salud, plataformas de comunicaciones y gestión de incidencias).

Como se observa en la Tabla 2, los estudios analizados se distribuyen entre los años 2021 y 2025 e incluyen propuestas centradas en detección de ataques, protección de servicios cloud, preservación de la privacidad de datos sensibles y eficiencia en la gestión de incidencias. A partir del análisis de contenido de estos trabajos, los hallazgos se organizaron en cuatro dimensiones que guardan relación directa con las preguntas de investigación planteadas: automatización de la detección y respuesta a incidentes, optimización de la protección en la nube, mejora en la gestión de riesgos y privacidad, y desafíos y oportunidades en la seguridad cloud.

Tabla 2. Artículos seleccionados. Fuente: elaboración propia.

N.°	Año	Autor(es)	Base de datos	Título
1	2023	Mehmood, M., Amin, R., Muslam, M. M. A., Xie, J., Aldabbas, H.	Scopus	Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning
2	2024	Dutta, J., Puthal, D.	Scopus	Advancing eHealth in Society 5.0: A Fuzzy Logic and Blockchain-Enhanced Framework for Integrating IoMT, Edge, and Cloud With AI
3	2024	Altowaijri, S. M., El Touati, Y.	Scopus	Securing Cloud Computing Services with an Intelligent Preventive Approach
4	2023	Azamuddin, W. M. H., Aman, A. H. M., Sallehuddin, H., Abualsaud, K., Mansor, N.	Scopus	The Emerging of Named Data Networking: Architecture, Application, and Technology
5	2021	Dinh, P. T., Park, M.	Scopus	R-EDoS: Robust Economic Denial of Sustainability Detection in an SDN-Based Cloud through Stochastic Recurrent Neural Network
6	2021	Mershad, K., Dahrouj, H., Sarieddeen, H., Shihada, B., Al-Naffouri, T., Alouini, M.-S.	Scopus	Cloud-Enabled High-Altitude Platform Systems: Challenges and Opportunities
7	2021	Seh, A. H., Al-Amri, J. F., Subahi, A. F., Agrawal, A., Kumar, R., Khan, R. A.	Scopus	Machine learning based framework for maintaining privacy of healthcare data
8	2022	Vegas-Capristan, N., Soto-Alarcón, A.	Google Scholar	La eficiencia de la gestión de incidencias en Cloud Services
9	2025	Eneque Suarez, V. G.	Google Scholar	Análisis comparativo de servicios y funcionalidades de AWS, Azure y Elastic Cloud en el entorno de Cloud Computing

En conjunto, los resultados muestran que la IA aporta capacidades avanzadas para la supervisión continua del entorno cloud, la identificación temprana de amenazas complejas y la reducción de tiempos de respuesta, pero también introduce nuevos puntos de vulnerabilidad derivados de su dependencia de grandes volúmenes de datos y de arquitecturas técnicas más complejas.

3.1 Automatización de la detección y respuesta a incidentes

En relación con la primera pregunta de investigación, vinculada con las principales aplicaciones de la IA en la gestión de la seguridad de infraestructuras cloud, los estudios coinciden en que su aporte más inmediato se encuentra en la automatización de la detección y respuesta a incidentes.

En [8] proponen un esquema de detección de escalamiento de privilegios en entornos cloud basado en algoritmos de aprendizaje supervisado (Random Forest, AdaBoost, LightGBM), capaz de procesar grandes volúmenes de registros y diferenciar más eficazmente entre actividades legítimas y maliciosas. Sus resultados muestran una mejora sustancial frente a enfoques tradicionales basados en reglas estáticas, tanto en la reducción de falsos positivos como en el tiempo de reacción ante eventos sospechosos.

De manera complementaria, [9]-[11] abordan los ataques de Economic Denial of Sustainability (EDoS) en nubes soportadas en SDN, proponiendo un modelo de red neuronal recurrente que analiza el tráfico y distingue entre incrementos legítimos y patrones maliciosos de consumo de recursos. Este enfoque evidencia cómo la IA puede anticiparse a ataques que buscan agotar la capacidad económica de los servicios cloud, más allá de la mera saturación técnica.

Los trabajos orientados a la gestión de incidencias en servicios cloud [12], [13] también destacan la utilidad de la IA para clasificar, priorizar y enrutar automáticamente los incidentes, reduciendo la carga operativa del personal de TI y permitiendo respuestas más alineadas con el impacto real sobre los servicios. En conjunto, estas evidencias muestran que la IA no solo acelera la identificación de amenazas, sino que contribuye a estructurar flujos de respuesta más coherentes con la criticidad de cada incidente.

Sin embargo, mientras la IA acelera la identificación de amenazas a velocidades inalcanzables para el ojo humano, también corre el riesgo de anclarse a patrones predefinidos que pueden pasar por alto lo inesperado. Por un lado, los modelos incrementan la precisión sobre escenarios ya conocidos; por otro, pueden volverse frágiles frente a ataques novedosos o a cambios drásticos en el comportamiento de los usuarios, lo que obliga a una actualización continua de los modelos y a la supervisión experta permanente.

3.2 Optimización de la protección en la nube

En cuanto a los beneficios de la IA para la protección y disponibilidad de servicios cloud, los estudios revisados evidencian que su integración permite fortalecer la resiliencia de infraestructuras distribuidas y complejas.

En [10] analizan plataformas de alta altitud (High-Altitude Platform Systems, HAPS) habilitadas por la nube, donde la IA se utiliza para anticipar fallos de comunicación, gestionar recursos de red y optimizar la continuidad del servicio en contextos remotos o de difícil acceso. El uso de algoritmos de aprendizaje permite ajustar dinámicamente la asignación de recursos y mitigar interrupciones antes de que se traduzcan en caídas visibles para el usuario final.

Desde otra perspectiva, [11] muestran que el aprendizaje profundo puede reforzar la sostenibilidad económica de servicios cloud al identificar patrones de uso anómalos que

comprometen la disponibilidad. Su propuesta no solo protege la infraestructura, sino que contribuye a preservar la calidad del servicio y a controlar los costos operativos vinculados a ataques persistentes.

Por su parte, [14], [15] plantean un marco para eHealth en Society 5.0 que integra IoMT, edge y nube con IA, enfatizando la necesidad de que los mecanismos de protección y continuidad del servicio acompañen el crecimiento del volumen de datos clínicos y del número de dispositivos conectados. En este escenario, la IA actúa como capa orquestadora que decide qué información se procesa en el borde, qué se envía a la nube y cómo se priorizan los recursos de seguridad para mantener la disponibilidad y la integridad del sistema.

La evidencia sugiere, en suma, que la IA fortalece la disponibilidad de los servicios cloud cuando las redes tradicionales sucumben a la presión de ataques volumétricos o a condiciones de operación extremas, aunque introduce complejidad en arquitecturas ya de por sí densas y demanda capacidades de cómputo adicionales que deben ser cuidadosamente planificadas.

3.3 Mejora en la gestión de riesgos y privacidad

Respecto a la dimensión de gestión de riesgos y privacidad, estrechamente ligada a la segunda pregunta de investigación sobre beneficios y desafíos de la IA, los estudios enfatizan una tensión permanente entre necesidad de datos y protección de la información sensible.

En [12] proponen un marco basado en aprendizaje automático para mantener la privacidad de datos sanitarios, en el que los modelos detectan accesos inusuales y comportamientos atípicos sobre historias clínicas electrónicas. La IA logra distinguir entre uso legítimo y potencial abuso con un nivel de precisión difícil de alcanzar mediante inspección manual, reforzando la protección de datos altamente sensibles. No obstante, esta mejora se sostiene en el acceso a grandes volúmenes de información clínica, lo que incrementa el impacto potencial de una brecha de seguridad si los controles fallan.

Los aportes de [13] muestran que la eficiencia de la gestión de incidencias en servicios cloud depende también de cómo se documentan, clasifican y retroalimentan los incidentes. La incorporación de analítica avanzada e IA en estos procesos permite identificar patrones recurrentes de riesgo y ajustar las políticas de seguridad y de continuidad del negocio, contribuyendo a una gestión más madura del riesgo operativo.

En conjunto, los hallazgos indican que la IA refuerza la protección de datos sensibles cuando las defensas convencionales flaquean, pero al hacerlo exige un caudal de información que amenaza la propia confidencialidad y obliga a replantear las estrategias de gobierno de datos, los acuerdos de nivel de servicio y los mecanismos de cumplimiento normativo.

3.4 Desafíos y oportunidades en la seguridad de la nube

Finalmente, en relación con la tercera pregunta de investigación, orientada a identificar recomendaciones y oportunidades para la integración de IA en la gestión de seguridad de infraestructuras cloud, los estudios revisados evidencian un escenario ambivalente: la IA se presenta simultáneamente como herramienta de protección y como fuente de nuevas vulnerabilidades.

[14] analizan el paradigma de Named Data Networking (NDN) y destacan su potencial para mejorar la privacidad y la distribución eficiente de contenidos mediante el almacenamiento en caché. Sin embargo, advierten que la fragmentación y replicación de datos puede multiplicar las superficies de ataque si no se acompaña de políticas rigurosas de autenticación, autorización y encriptación, especialmente cuando se combinan con algoritmos de IA para el encaminamiento y la optimización del tráfico.

[15], en el contexto de eHealth, enfatizan que la integración de IA, edge y nube abre oportunidades para fortalecer la seguridad —por ejemplo, detectando comportamientos anómalos en tiempo real—, pero al mismo tiempo eleva las exigencias de gobernanza, transparencia algorítmica y responsabilidad sobre el tratamiento de datos clínicos.

Finalmente, estudios comparativos de servicios y funcionalidades de proveedores cloud a gran escala evidencian que las plataformas líderes están incorporando cada vez más servicios de seguridad basados en IA, pero con diferencias significativas en las capacidades de monitoreo, automatización y gestión de identidades. Estas diferencias condicionan las posibilidades de las organizaciones para implementar estrategias de seguridad basadas en IA de forma consistente en entornos multicloud.

La promesa de la IA para blindar entornos cloud, por tanto, convive con la amenaza de nuevas vulnerabilidades derivadas de su uso intensivo, lo que refuerza la necesidad de marcos de referencia como ITIL v4 y de una supervisión humana constante que mantenga el equilibrio entre automatización, control y responsabilidad.

4. DISCUSIÓN

Los resultados de esta revisión sistemática muestran que la integración de la IA en la gestión de la seguridad de infraestructuras cloud no es un fenómeno aislado, sino una tendencia transversal que atraviesa diferentes dominios (servicios empresariales, salud, plataformas de comunicaciones, gestión de incidencias). La organización de los hallazgos en cuatro dimensiones permitió responder de manera articulada a las preguntas de investigación, evidenciando que las aplicaciones de IA se concentran en la automatización de la detección y respuesta a incidentes, la optimización de la protección y disponibilidad de servicios, el fortalecimiento de la gestión de riesgos y la apertura de nuevas oportunidades, pero también de desafíos, para la seguridad cloud.

En comparación con estudios previos, los hallazgos de [8] y [11] corroboran la idea, ya sugerida en la literatura técnica sobre ciberseguridad, de que los enfoques basados en reglas resultan insuficientes en entornos dinámicos de nube y deben ser complementados con modelos de aprendizaje automático capaces de adaptarse a patrones cambiantes de ataque. Sin embargo, esta revisión aporta un valor agregado al mostrar que soluciones originalmente diseñadas para problemas específicos (escalamiento de privilegios, EDoS) convergen en un mismo eje: la necesidad de sistemas de detección y respuesta capaces de operar en tiempo casi real y de integrarse con los procesos de gestión de servicios TI.

Asimismo, el trabajo de [10] sobre plataformas HAPS y el marco de eHealth propuesto por [15] amplían la discusión tradicional de la seguridad en la nube, normalmente centrada en centros de datos y servicios empresariales, hacia escenarios donde la continuidad del servicio implica impactos críticos sobre la comunicación y la salud de las personas. Al contrastar estos estudios con los enfoques orientados a la privacidad de datos sanitarios [12] y a la gestión de incidencias en servicios cloud [13], se observa que, más allá de las diferencias de contexto, existe un consenso en torno a la IA como soporte para decisiones rápidas en situaciones de alto riesgo, pero también un reconocimiento explícito del aumento de la complejidad técnica y del riesgo en caso de fallos.

Desde una perspectiva práctica, los resultados sugieren varias implicaciones para las organizaciones que gestionan infraestructuras cloud. En primer lugar, la adopción de soluciones de IA para la seguridad no debería limitarse a incorporar herramientas aisladas, sino integrarse en un modelo de gestión de servicios TI, como el propuesto por ITIL v4, que permita articular la detección automatizada, la respuesta a incidentes, la gestión de cambios y la mejora continua. En segundo lugar, se hace evidente la necesidad de robustecer la gobernanza de datos: la IA requiere grandes volúmenes de información para entrenar y mejorar sus modelos, pero esto debe equilibrarse con políticas claras de minimización de datos, segmentación de accesos y cumplimiento normativo.

En tercer lugar, los hallazgos refuerzan la importancia de mantener la supervisión humana sobre los procesos más críticos. Aunque los modelos de IA pueden superar al ojo humano en rapidez y capacidad de análisis, la toma de decisiones finales en incidentes de alto impacto —como accesos indebidos a datos clínicos [12] o pérdidas de disponibilidad en servicios esenciales [10], [11]— debe seguir recayendo en equipos especializados que evalúen el contexto, ponderen los riesgos y eviten respuestas automáticas desproporcionadas.

La revisión también pone de relieve varias limitaciones. En primer lugar, el número de estudios que cumplen con los criterios de inclusión es reducido (9 artículos), lo que impide generalizar los resultados a todas las realidades organizacionales y sectores. En segundo lugar, la revisión se restringió a dos bases de datos (Scopus y Google Scholar) y a un intervalo temporal acotado (2021–2025), por lo que es posible que existan investigaciones relevantes en otros repositorios o fuera de este rango temporal. En tercer lugar, la heterogeneidad de los diseños, contextos y métricas empleadas en los estudios seleccionados no permitió realizar un metaanálisis cuantitativo, por lo que los resultados se presentan en forma de síntesis narrativa.

Estas limitaciones abren líneas claras para investigaciones futuras: ampliar la búsqueda a otras bases de datos especializadas en seguridad y computación en la nube, incorporar literatura en otros idiomas, profundizar en estudios de caso que detallen la implementación concreta de soluciones de IA en organizaciones reales y avanzar hacia análisis comparativos que evalúen el desempeño de distintos enfoques de IA bajo condiciones similares.

En síntesis, el debate entre los estudios revisados muestra que la IA se consolida como un eje de transformación en la gestión de la seguridad de infraestructuras cloud, pero su aporte no es neutro ni automático. Los beneficios en términos de automatización, detección proactiva y resiliencia deben equilibrarse con una gestión cuidadosa de la privacidad, la gobernanza de datos y la dependencia tecnológica. En este escenario, la contribución de la presente revisión radica en ofrecer una visión estructurada de las aplicaciones, beneficios, desafíos y oportunidades de la IA en la seguridad en la nube, que sirva de insumo tanto para la toma de decisiones en la gestión de servicios TI como para el diseño de nuevas investigaciones en el campo.

5. CONCLUSIONES

La revisión sistemática realizada permitió analizar el impacto de la inteligencia artificial en la gestión de la seguridad de infraestructuras cloud en entornos de TI, a partir de nueve estudios que abordan este fenómeno desde distintos contextos de aplicación. En conjunto, la evidencia revisada muestra que la IA se ha convertido en un componente clave para fortalecer la seguridad en la nube, al aportar capacidades avanzadas de supervisión continua, detección temprana de amenazas y automatización de la respuesta ante incidentes, lo cual contribuye a mejorar la eficiencia operativa y la resiliencia de los servicios sobre infraestructuras cloud.

Los hallazgos permiten afirmar que las aplicaciones de IA más relevantes se concentran en la identificación proactiva de ataques complejos, la mitigación de incidentes que comprometen la disponibilidad y sostenibilidad económica de los servicios, así como en el refuerzo de la protección de datos sensibles en sectores críticos como la salud. La combinación de algoritmos de aprendizaje automático, redes neuronales y enfoques analíticos avanzados posibilita distinguir con mayor precisión entre comportamientos legítimos y maliciosos, reducir falsos positivos y priorizar la atención de los eventos de seguridad de acuerdo con su impacto sobre los servicios de TI. De este modo, la IA aporta un soporte significativo a la gestión de la seguridad en la nube desde una perspectiva integral de gestión de servicios.

Sin embargo, la integración de la IA también introduce desafíos importantes que no pueden ser ignorados. El uso intensivo de datos para entrenar y ajustar los modelos incrementa los riesgos vinculados con la privacidad y la confidencialidad de la información, al mismo tiempo que aumenta la complejidad técnica de las arquitecturas cloud y la dependencia de soluciones especializadas. De no gestionarse adecuadamente, estos factores pueden derivar en nuevas superficies de ataque, en una mayor exposición ante fallos de configuración o en decisiones automatizadas que no consideren suficientemente el contexto de negocio. En ese sentido, la IA no constituye una solución aislada, sino un elemento que debe articularse con políticas robustas de gobierno de datos, marcos de buenas prácticas como ITIL v4 y mecanismos claros de responsabilidad sobre el tratamiento de la información.

A partir de lo anterior, se concluye que la integración efectiva de la IA en la gestión de la seguridad de infraestructuras cloud exige un equilibrio entre automatización y control humano. Las organizaciones necesitan combinar herramientas inteligentes de monitoreo, detección y respuesta con equipos especializados capaces de supervisar los modelos, interpretar sus resultados, ajustar los umbrales de riesgo y tomar decisiones informadas en los incidentes de mayor impacto. Asimismo, resulta fundamental fortalecer la capacitación continua del personal de TI en temas de ciberseguridad, gobierno de datos y uso ético de la IA, así como evaluar con detenimiento las capacidades de los proveedores cloud cuando se operan entornos multicloud o híbridos.

Finalmente, aunque los resultados de nuestra revisión ofrecen una visión estructurada de las aplicaciones, beneficios, desafíos y oportunidades de la IA en la seguridad en la nube, también evidencian la necesidad de seguir investigando. Futuras investigaciones podrían ampliar el número de bases de datos consultadas, incorporar estudios de caso en organizaciones de distintos sectores, comparar el desempeño de diferentes enfoques de IA bajo condiciones similares y profundizar en aspectos como la explicabilidad de los modelos, la gestión del riesgo algorítmico y el impacto de la IA en la toma de decisiones dentro de la gestión de servicios TI. Estos esfuerzos permitirán consolidar y matizar las conclusiones aquí presentadas, contribuyendo a una adopción más madura y responsable de la IA en la protección de infraestructuras cloud.

6. ACERCA DEL ARTÍCULO

Financiamiento: El presente trabajo no contó con financiamiento externo y fue desarrollado íntegramente en el ámbito académico.

Agradecimientos: Los autores agradecen al curso Gestión *de Servicios de TIC,* Alberto Carlos Mendoza de los Santos de la Universidad Nacional de Trujillo por el marco académico que permitió el desarrollo del presente estudio, así como la orientación brindada por el docente responsable del curso.

Contribuciones de autoría:

Juan D. Molina: Investigación, conceptualización del estudio, redacción del borrador original, elaboración de tablas y revisión de la coherencia del manuscrito.

Leonardo J. Guimaray: Investigación, redacción del borrador original, visualización (creación de gráficos), ajuste de tablas y adecuación del formato final del documento.

Alberto C. Mendoza: Supervisión del proyecto, revisión crítica del manuscrito y validación de la versión final del contenido Todos los autores han leído y están de acuerdo con la versión publicada del manuscrito.

Conflictos de interés: Los autores declaran no tener conflictos de interés financieros, académicos ni personales que pudieran haber influido en el desarrollo o en los resultados del presente manuscrito.

REFERENCIAS

[1] L. F. Mero-Terán, and E. J. Macías-Arias, "Technological models of cloud computing in the digital transformation of higher education: A systematic literature review," *593 Digital Publisher CEIT*, vol. 10, no. 1, pp. 29–53, Jul. 2025. https://doi.org/10.33386/593DP.2025.1.2704

[2] imedia,"Cómo la IA puede mejorar la seguridad en Internet de las cosas," imediacomunicacion.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.imediacomunicacion.com/como-la-ia-puede-ayudar-a-mejorar-la-seguridad-en-internet-de-las-cosas-iot-2/

[3] S. Fernández, and L. Campo, "Inteligencia artificial al servicio de la seguridad en la nube," keepler.io. Accessed: Jul. 1, 2023. [Online]. Available: https://keepler.io/es/2021/06/02/inteligencia-artificial-al-servicio-de-la-seguridad-en-la-nube/

[4] NUTANIX, "¿Qué es la inteligencia artificial?," nutanix.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.nutanix.com/es/info/artificial-intelligence

[5] Microsoft "¿Qué es la inteligencia artificial para la ciberseguridad?," microsoft.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.microsoft.com/es-es/security/business/security-101/what-is-ai-for-cybersecurity

[6] M. Petticrew, and H. Roberts, *Systematic reviews in the social sciences: A practical guide*, Chichester, England: Wiley-Blackwell, 2005. https://onlinelibrary.wiley.com/doi/book/10.1002/9780470754887

[7] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, Jan. 2021. https://doi.org/10.1136/bmj.n71

[8] M. Mehmood, R. Amin, M. M. Ali Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," *IEEE Access*, vol. 11, pp. 46561–46576, May. 2023. https://doi.org/10.1109/ACCESS.2023.3273895

[9] S. M. Altowaijri, and Y. El Touati, "Securing cloud computing services with an intelligent preventive approach," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 3, pp. 13998–14005, Jun. 2024. https://doi.org/10.48084/ETASR.7268

[10] K. Mershad, H. Dahrouj, H. Sarieddeen, B. Shihada, T. Al-Naffouri, and M.-S. Alouini, "Cloud-enabled high-altitude platform systems: Challenges and opportunities," *Front. Comms. Net.*, vol. 2, p. 716265, Jul. 2021. https://doi.org/10.1109/ACCESS.2021.3061601

[11] P. T. Dinh, and M. Park, "R-EDoS: Robust economic denial of sustainability detection in an SDN-based cloud through stochastic recurrent neural network," *IEEE Access*, vol. 9, pp. 35057–35074, Feb. 2021. https://ieeexplore.ieee.org/document/9360795

[12] A. Hussain Seh, J. F. Al-Amri, A. F. Subahi, A. Agrawal, R. Kumar, and R. Ahmad Khan, "Machine learning based framework for maintaining privacy of healthcare data," *Intell. Autom. Soft Comput.*, vol. 29, no. 3, pp. 697–712, Jul. 2021. https://www.techscience.com/iasc/v29n3/43042

[13] N. Vegas-Capristan, and A. Soto-Alarcón, "Eficiencia de la gestión de incidencias en cloud services: una revisión sistemática," *Revista Campus,* vol. 27, no. 34, pp. 197–208, Nov. 2022. https://doi.org/10.24265/campus.2022.v27n34.03

[14] W. M. Hazwan Azamuddin, A. H. Mohd Aman, H. Sallehuddin, K. Abualsaud, and N. Mansor, "The emerging of named data networking: Architecture, application, and technology," *IEEE Access*, vol. 11, pp. 23620–23633, Feb. 2023. https://ieeexplore.ieee.org/document/10038676

[15] J. Dutta, and D. Puthal, "Advancing eHealth in Society 5.0: A Fuzzy Logic and Blockchain-Enhanced Framework for Integrating IoMT, Edge, and Cloud With AI," *IEEE Access*, vol. 12, pp. 195710-195730, Dec. 2024. https://ieeexplore.ieee.org/document/10810439