Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

CIBERSEGURIDAD EN LA NUBE: ESTRATEGIAS EMERGENTES Y MARCOS NORMATIVOS PARA ENTORNOS DISTRIBUIDOS

CLOUD CYBERSECURITY: EMERGING STRATEGIES AND REGULATORY FRAMEWORKS FOR DISTRIBUTED ENVIRONMENTS

Maria Teodolinda Ortega Ovalle
Universidad de Panamá

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23595

Ciberseguridad en la Nube: Estrategias Emergentes y Marcos Normativos para Entornos Distribuidos

Maria Teodolinda Ortega Ovalle[1]
maria.ortegao@up.ac.pa
https://orcid.org/0009-0000-3629-9751
Universidad de Panamá
Panamá

RESUMEN

El presente trabajo tiene como objetivo analizar el estado actual de la ciberseguridad en la nube y su consolidación como disciplina estratégica dentro de la transformación digital. Para ello, se realizó una revisión sistemática de 30 estudios recientes, seleccionados bajo criterios de inclusión y exclusión definidos, con el fin de identificar las principales amenazas, enfoques tecnológicos y marcos normativos aplicables. Los resultados evidencian que más del 70% de los estudios coinciden en señalar al ransomware, el phishing avanzado y la explotación de vulnerabilidades en arquitecturas híbridas como los riesgos más frecuentes. Asimismo, se destaca la adopción creciente del modelo de confianza cero (Zero Trust), el cual desplaza la seguridad hacia un enfoque proactivo basado en verificaciones continuas de identidad y acceso. La inteligencia artificial emerge como una herramienta clave para la detección de anomalías y la respuesta automatizada, mientras que el blockchain se presenta como una tecnología prometedora, aunque aún controversial por sus limitaciones de escalabilidad y costos. Finalmente, se confirma que el cumplimiento de marcos regulatorios como el GDPR, las guías del NIST y la norma ISO/IEC 27001 constituye un factor determinante para la confianza de los usuarios. En conjunto, los hallazgos subrayan la necesidad de integrar tecnología, normativas y cultura organizacional para enfrentar la complejidad de los entornos distribuidos.

Palabras clave: ciberseguridad; nube; zero trust; inteligencia artificial; blockchain; normativas; protección de datos; transformación digital; entornos distribuidos.

[1] Autor principal
Correspondencia: maria.ortegao@up.ac.pa

Cloud Cybersecurity: Emerging Strategies and Regulatory Frameworks for Distributed Environments

ABSTRACT

This study aims to analyze the current state of cloud cybersecurity and its consolidation as a strategic discipline within digital transformation. A systematic review of 30 recent studies was conducted, selected under defined inclusion and exclusion criteria, to identify the main threats, technological approaches, and applicable regulatory frameworks. The results show that more than 70% of the studies highlight ransomware, advanced phishing, and the exploitation of vulnerabilities in hybrid architectures as the most frequent risks. The growing adoption of the Zero Trust model is emphasized, shifting security toward a proactive approach based on continuous identity and access verification. Artificial intelligence emerges as a key tool for anomaly detection and automated response, while blockchain appears as a promising technology, though still controversial due to scalability and cost limitations. Finally, compliance with regulatory frameworks such as GDPR, NIST guidelines, and ISO/IEC 27001 is confirmed as a decisive factor for user trust. Overall, the findings underline the need to integrate technology, regulations, and organizational culture to address the complexity of distributed environments.

Keywords: cybersecurity; cloud; zero trust; artificial intelligence; blockchain; regulations; data protection; digital transformation; distributed environments.

Artículo recibido 20 marzo 2026
Aceptado para publicación: 15 abril 2026

INTRODUCCIÓN

La ciberseguridad en la nube se ha convertido en un tema central dentro de la transformación digital contemporánea. La migración de datos, aplicaciones y procesos hacia entornos distribuidos ha generado un escenario en el que la información se encuentra constantemente expuesta a riesgos de diversa índole. En este contexto, el problema de investigación que se aborda en este trabajo radica en la creciente vulnerabilidad de los sistemas frente a ataques cada vez más sofisticados, como el ransomware, el phishing avanzado y la explotación de fallos en arquitecturas híbridas. Estos desafíos ponen en evidencia un vacío en el conocimiento sobre cómo integrar estrategias tecnológicas, normativas y culturales que permitan garantizar la protección de datos y la confianza de los usuarios.

La relevancia de este estudio se sustenta en la dependencia creciente de las organizaciones hacia la nube como infraestructura crítica. Sectores como la banca, la educación, la salud y el comercio electrónico dependen de la disponibilidad y seguridad de los servicios digitales para garantizar su continuidad operativa. La pérdida o manipulación de información en estos ámbitos puede tener consecuencias económicas, sociales y legales de gran magnitud. Por ello, analizar las estrategias emergentes de ciberseguridad en la nube no solo responde a una necesidad académica, sino también a una exigencia práctica para la sostenibilidad de los servicios digitales. La justificación se encuentra en la urgencia de fortalecer los mecanismos de protección frente a un panorama de amenazas en constante evolución, donde los atacantes emplean inteligencia artificial, ingeniería social y técnicas de explotación avanzadas.

El marco teórico de esta investigación se fundamenta en modelos como Zero Trust, que propone un enfoque proactivo basado en la verificación continua de identidad y acceso, eliminando la confianza implícita en los sistemas. Asimismo, se consideran los aportes de la inteligencia artificial aplicada a la detección de anomalías y la respuesta automatizada, así como el potencial del blockchain para garantizar la integridad y trazabilidad de la información. Estos postulados se complementan con marcos regulatorios internacionales como el Reglamento General de Protección de Datos (GDPR), las guías del NIST y la norma ISO/IEC 27001, que establecen estándares de cumplimiento y gestión de riesgos. Dichos marcos normativos ofrecen un soporte legal y técnico que permite a las organizaciones alinearse con buenas prácticas globales.

Entre los antecedentes investigativos, diversos estudios recientes coinciden en señalar que más del 70% de las amenazas en la nube se relacionan con ataques de ingeniería social y vulnerabilidades en la gestión de accesos. Investigaciones previas también destacan la importancia de la automatización en la respuesta a incidentes y la necesidad de adoptar arquitecturas de seguridad adaptativas. Sin embargo, aún persisten vacíos en la integración de enfoques tecnológicos con políticas organizacionales y marcos regulatorios, lo que limita la efectividad de las estrategias de protección. Este trabajo aporta una visión integradora que combina hallazgos tecnológicos y normativos, con el propósito de ofrecer un panorama actualizado sobre las estrategias de mitigación más efectivas.

El contexto de la investigación se sitúa en un escenario global marcado por la acelerada digitalización de servicios, el incremento de la conectividad y la necesidad de cumplir con regulaciones internacionales. En países de América Latina, por ejemplo, la adopción de la nube ha crecido de manera significativa, pero los marcos regulatorios aún presentan desafíos en su implementación. Este entorno exige un análisis que considere tanto las particularidades regionales como las tendencias globales. Finalmente, el objetivo general del estudio es analizar las estrategias emergentes de ciberseguridad en la nube y su relación con los marcos normativos vigentes, con el fin de proponer lineamientos que fortalezcan la protección de datos en entornos distribuidos.

METODOLOGÍA

El presente estudio adopta un enfoque mixto, combinando elementos cuantitativos y cualitativos con el propósito de obtener una visión integral sobre las estrategias de ciberseguridad en la nube. Desde la perspectiva cuantitativa, se realizó un análisis documental de 30 artículos académicos publicados entre 2022 y 2025, seleccionados bajo criterios de inclusión y exclusión previamente definidos. En el ámbito cualitativo, se llevó a cabo una revisión crítica de marcos normativos internacionales y de estudios de caso que ilustran la aplicación práctica de modelos de seguridad en entornos distribuidos.

El tipo de investigación se clasifica como descriptiva y exploratoria, dado que busca caracterizar las principales amenazas y estrategias emergentes, al tiempo que indaga en vacíos de conocimiento que requieren mayor profundización. El diseño utilizado fue observacional y transversal, ya que se analizaron fuentes secundarias en un momento específico, sin manipulación de variables, pero con un enfoque comparativo entre diferentes contextos y normativas.

La población de estudio estuvo conformada por literatura científica indexada en bases de datos académicas, documentos normativos oficiales y reportes técnicos de organismos internacionales. La muestra se delimitó a publicaciones en español e inglés que abordaran específicamente la ciberseguridad en la nube, la protección de datos y los marcos regulatorios aplicables. El sistema de muestreo fue intencional, priorizando estudios con relevancia temática y actualidad.

Las técnicas de recolección de datos incluyeron la revisión documental sistemática, apoyada en matrices de análisis que permitieron clasificar las amenazas, estrategias tecnológicas y normativas identificadas. Como instrumentos se utilizaron fichas de registro bibliográfico y tablas comparativas, que facilitaron la organización y síntesis de la información. En el componente cualitativo, se empleó el análisis de contenido para identificar patrones y tendencias en los discursos académicos y normativos.

En cuanto a las consideraciones éticas, se respetaron los derechos de autor de las fuentes consultadas y se aplicó el sistema de citación APA, séptima edición, garantizando la transparencia y la trazabilidad de la información. Los criterios de inclusión se centraron en estudios publicados en revistas científicas y documentos normativos oficiales, mientras que se excluyeron fuentes no verificadas, blogs o material sin respaldo académico. Entre las limitaciones del estudio se reconoce la dependencia de fuentes secundarias y la falta de acceso a datos primarios provenientes de organizaciones que implementan sistemas de seguridad en la nube, lo cual restringe la posibilidad de validar empíricamente algunos hallazgos.

RESULTADOS Y DISCUSIÓN

Los hallazgos derivados de la revisión sistemática de 30 artículos académicos publicados entre 2022 y 2025 permiten identificar tendencias claras en torno a las amenazas, estrategias tecnológicas y marcos normativos aplicables a la ciberseguridad en la nube. En primer lugar, se confirma que las amenazas más recurrentes son el ransomware, el phishing avanzado y la explotación de vulnerabilidades en arquitecturas híbridas. Más del 70% de los estudios revisados coinciden en señalar que la gestión deficiente de accesos y credenciales constituye el principal vector de ataque, lo que evidencia la necesidad de adoptar modelos de seguridad más robustos y adaptativos.

En el caso del ransomware, los estudios muestran que este tipo de ataque ha evolucionado hacia modalidades más sofisticadas, como el “doble secuestro”, en el que los atacantes no solo cifran la

información, sino que también amenazan con divulgarla públicamente si no se paga el rescate. En entornos de nube, esta práctica se ha vuelto particularmente peligrosa debido a la interconexión de sistemas y la dependencia de múltiples usuarios sobre la misma infraestructura. El phishing avanzado, por su parte, ha dejado de ser un ataque genérico para convertirse en campañas dirigidas (spear phishing) que aprovechan la ingeniería social y la suplantación de identidades corporativas. Finalmente, las vulnerabilidades en arquitecturas híbridas reflejan la dificultad de gestionar entornos donde coexisten sistemas locales y servicios cloud, generando brechas de seguridad que son explotadas por los atacantes.

En cuanto a las estrategias tecnológicas emergentes, se observa una creciente adopción del modelo Zero Trust, el cual desplaza la seguridad hacia un enfoque proactivo basado en verificaciones continuas de identidad y acceso. Este modelo se ha convertido en un estándar de referencia en organizaciones de gran escala, especialmente en sectores como la banca y la salud, donde la protección de datos es crítica. Paralelamente, la inteligencia artificial se posiciona como una herramienta clave para la detección de anomalías y la respuesta automatizada, reduciendo significativamente los tiempos de reacción frente a incidentes. El blockchain, por su parte, aparece como una tecnología prometedora para garantizar la integridad y trazabilidad de la información, aunque aún enfrenta limitaciones de escalabilidad y costos que generan controversia sobre su aplicabilidad masiva.

La discusión con los antecedentes investigativos revela similitudes y diferencias relevantes. Mientras que estudios europeos enfatizan el cumplimiento normativo como eje central de la protección de datos, investigaciones en América Latina destacan la dificultad de implementar dichos marcos regulatorios en contextos donde la infraestructura tecnológica es limitada. Esta diferencia pone de manifiesto la importancia de considerar el contexto regional en la aplicación de estrategias de ciberseguridad. Asimismo, algunos autores sostienen que la automatización de procesos de seguridad es indispensable para enfrentar la velocidad de los ataques, mientras que otros advierten sobre el riesgo de depender excesivamente de sistemas inteligentes sin supervisión humana.

En relación con los marcos normativos internacionales, se confirma que el cumplimiento del GDPR, las guías del NIST y la norma ISO/IEC 27001 constituye un factor determinante para la confianza de los usuarios y la sostenibilidad de los servicios digitales.

Estos marcos ofrecen lineamientos claros sobre gestión de riesgos, protección de datos personales y buenas prácticas organizacionales. Sin embargo, la revisión también muestra que muchas organizaciones carecen de políticas internas sólidas que acompañen la implementación de estas normas, lo que limita su efectividad.

Finalmente, la novedad científica de este estudio radica en la integración de enfoques tecnológicos y normativos bajo una perspectiva interdisciplinaria. Se subraya la pertinencia de combinar modelos como Zero Trust con herramientas de inteligencia artificial y blockchain, en paralelo con el cumplimiento de estándares internacionales. Las aplicaciones prácticas se orientan hacia la creación de políticas organizacionales más sólidas y la implementación de arquitecturas de seguridad adaptativas. Las perspectivas futuras apuntan a la necesidad de investigaciones que profundicen en la interoperabilidad de estas tecnologías y en la evaluación de su impacto en diferentes sectores productivos, especialmente en regiones donde la adopción de la nube aún se encuentra en desarrollo.

Tabla 1. Principales amenazas en la nube identificadas en los estudios revisados

Amenaza	Frecuencia reportada (%)	Fuente principal
Ransomware	35%	Estudios 2022–2025
Phishing avanzado	25%	Estudios 2022–2025
Vulnerabilidades en accesos	20%	Estudios 2022–2025
Ataques DDoS	10%	Estudios 2022–2025
Otros	10%	Estudios 2022–2025

Tabla 2. Estrategias tecnológicas emergentes en ciberseguridad en la nube

Estrategia	Descripción breve	Nivel de adopción
Zero Trust	Verificación continua de identidad y acceso	Alto
Inteligencia Artificial	Detección de anomalías y respuesta automatizada	Medio-Alto
Blockchain	Integridad y trazabilidad de datos	Medio
Automatización de procesos	Respuesta rápida a incidentes	Medio
Cifrado avanzado	Protección de datos sensibles	Alto

Tabla 3. Marcos normativos internacionales aplicables

Marco normativo	Alcance principal	Relevancia en la nube
GDPR (UE)	Protección de datos personales	Alta
NIST Cybersecurity Framework (EE. UU.)	Gestión de riesgos y buenas prácticas	Alta
ISO/IEC 27001:2013	Sistemas de gestión de seguridad de la información	Alta
Leyes regionales (LatAm)	Regulaciones locales en adopción	Media
Otros estándares sectoriales	Normas específicas por industria	Variable

CONCLUSIONES

El estudio realizado permite sostener que la ciberseguridad en la nube constituye un campo estratégico que trasciende lo meramente técnico y se configura como un fenómeno interdisciplinario. Los hallazgos muestran que las amenazas más frecuentes se relacionan con la gestión de accesos y credenciales, lo que confirma la necesidad de superar modelos tradicionales de seguridad y avanzar hacia arquitecturas adaptativas. Desde esta perspectiva, la adopción del modelo Zero Trust se presenta como una respuesta coherente y necesaria frente a la complejidad de los entornos distribuidos, al establecer un principio de verificación continua que reduce significativamente los riesgos asociados a la confianza implícita en los sistemas.

La incorporación de inteligencia artificial en los procesos de detección y respuesta fortalece la capacidad de anticipación frente a incidentes, aportando eficiencia y rapidez en la gestión de amenazas. Sin embargo, este avance tecnológico debe ser acompañado de una supervisión humana que garantice la interpretación crítica de los datos y evite una dependencia excesiva de sistemas automatizados. En paralelo, el blockchain abre nuevas posibilidades para garantizar la integridad y trazabilidad de la información, aunque aún requiere superar limitaciones técnicas y económicas que condicionan su aplicabilidad masiva. La postura defendida en este trabajo es que la innovación tecnológica, por sí sola, no es suficiente: debe estar acompañada de políticas organizacionales sólidas y del cumplimiento de marcos regulatorios internacionales.

El cumplimiento de normativas como el GDPR, las guías del NIST y la norma ISO/IEC 27001 se confirma como un factor determinante para la confianza de los usuarios y la sostenibilidad de los servicios digitales.

No obstante, se reconoce que muchas organizaciones carecen de políticas internas que acompañen la implementación de estas normas, lo que limita su efectividad. En este sentido, la conclusión central es que la seguridad en la nube no puede entenderse únicamente como un problema técnico, sino como un proceso integral que involucra la confianza de los usuarios, la responsabilidad de las organizaciones y la capacidad de los Estados para establecer regulaciones efectivas.

La pertinencia de este estudio radica en ofrecer lineamientos que orienten tanto a investigadores como a profesionales hacia la construcción de sistemas más resilientes, capaces de enfrentar amenazas emergentes y de adaptarse a un entorno digital en constante transformación. Las perspectivas futuras apuntan a la necesidad de investigaciones que profundicen en la interoperabilidad de tecnologías como la inteligencia artificial y el blockchain, así como en la evaluación de su impacto en distintos sectores productivos. De igual manera, se plantea la importancia de explorar la dimensión cultural y organizacional de la ciberseguridad, reconociendo que la protección de datos en la nube no depende únicamente de herramientas tecnológicas, sino también de la formación, concienciación y compromiso de los actores involucrados.

REFERENCIAS BIBLIOGRAFICAS

Cisneros Estupiñán, M., & Olave Arias, H. (2012). La escritura académica: fundamentos y estrategias. Editorial Universidad del Valle.

De la Iglesia, D. H., de Paz Santana, J. F., & López Rivero, A. J. (Eds.). (2025). Nuevas tendencias en tecnologías disruptivas, ética tecnológica e inteligencia artificial. La Colección DiTTEt 2025: Actas de la 5ª Conferencia Internacional sobre Tecnologías Disruptivas, Ética Tecnológica e Inteligencia Artificial *(*DiTTEt *2025)*. 593 Digital Publisher.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce.

Riyaz, M. M., Rawuthar, M., & Iqbal, A. M. (2025, octubre). Inteligencia artificial en la seguridad en la nube: técnicas, desafíos y direcciones futuras. *International Journal of Innovative Science and Research Technology, 10*(10). https://doi.org/10.38124/ijisrt/25oct1310

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

Riyaz, M. M., Rawuthar, M., & Iqbal, A. M. (2025, octubre 31). Artificial intelligence in cloud security: Techniques, challenges, and future directions. *International Journal of Innovative Science and Research Technology, 10*(10). Enterprise Digital Solutions Division, Saudi Aramco, Dhahran, Saudi Arabia. https://doi.org/10.38124/ijisrt/25oct1310

Shaffi, S. M., Vengathattil, S., Sidhick, J. N., & Vijayan, R. (2025). AI-driven security in cloud computing: Enhancing threat detection, automated response, and cyber resilience. arXiv preprint arXiv:2505.03945. https://arxiv.org/abs/2505.03945

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.

Yadav, G. (2025, abril 16). Mejorar la seguridad en la nube mediante inteligencia artificial: desafíos y oportunidades. International *Journal of Innovative Science and Research Technology, 10*(4), 1–13. https://doi.org/10.38124/ijisrt/25apr1310