Technology Rain Journal ISSN: 2953-464X
Vol. 5 Núm. 1 (Enero – Junio 2026), e122.

Artículo de Investigación Original.

Tendencias emergentes en infraestructura digital: computación en la nube, edge computing y ciberresiliencia

Emerging Trends in Digital Infrastructure: Cloud Computing, Edge Computing, and Cyberresilience

María Teodolinda Ortega Ovalle [1][0009-0000-3629-9751]
[1]Universidad de Panamá, Facultad de Informática, Electrónica y Comunicación, Departamento de Informática. Panamá
maria.ortegao@up.ac.pa

CITA EN APA:

Ortega Ovalle , M. T. (2026). Tendencias emergentes en infraestructura digital: computación en la nube, edge computing y ciberresiliencia. Technology Rain Journal, 5(1). https://doi.org/10.55204/trj.v5i1.e126

Recibido: 18 de diciembre-2025
Aceptado: 03 de marzo-2026
Publicado: 06 de marzo-2026

Technology Rain Journal
ISSN: 2953-464X

Resumen. La infraestructura digital contemporánea experimenta una transformación acelerada impulsada por la expansión de la computación en la nube, el edge computing y los enfoques de ciberresiliencia. Este artículo analiza comparativamente estas tres tendencias para identificar sus características, beneficios, limitaciones y su impacto en la modernización tecnológica en América Latina. La metodología se basó en una revisión sistemática de literatura reciente (2018–2025), complementada con el modelo PRISMA y un Diagrama de Síntesis de Evidencia Integrada, permitiendo evaluar madurez, aplicabilidad y desafíos. Los resultados muestran que la computación en la nube favorece escalabilidad, eficiencia y reducción de costos; el edge computing disminuye la latencia y fortalece la autonomía operativa en entornos distribuidos; y la ciberresiliencia se consolida como un marco transversal para prevenir, responder y recuperarse de incidentes. Se concluye que la convergencia de estas tendencias es estratégica para robustecer la infraestructura digital regional, aunque requiere inversión sostenida, políticas claras y capacidades técnicas avanzadas.

Palabras Clave: Computación en la nube, edge computing, ciberresiliencia, infraestructura digital, transformación digital.

Abstract: Contemporary digital infrastructure is undergoing rapid transformation driven by the growing adoption of cloud computing, edge computing, and cyber-resilience frameworks. This article provides a comparative analysis of these three trends, examining their characteristics, benefits, limitations, and their influence on digital modernization in Latin America. The methodology relied on a systematic review of recent literature (2018–2025), supported by the PRISMA model and an Integrated Evidence Synthesis Diagram, enabling an assessment of maturity, applicability, and challenges. Findings indicate that cloud computing enhances scalability, efficiency, and cost optimization; edge computing reduces latency and strengthens operational autonomy in distributed environments; and cyber-resilience emerges as a cross-cutting framework integrating prevention, response, and recovery. The study concludes that the convergence of these trends forms a strategic foundation for reinforcing regional digital infrastructure, although successful adoption demands sustained investment, coherent policies, and advanced technical capabilities.

Keywords: Cloud computing, edge computing, cyber-resilience, digital infrastructure, digital transformation.

1. INTRODUCCIÓN

La infraestructura digital se ha consolidado como un componente estratégico para el desarrollo económico, social y tecnológico de América Latina, en un contexto marcado por la acelerada transformación digital y la creciente dependencia de sistemas distribuidos (OECD, 2023). La expansión de servicios en línea y la necesidad de arquitecturas más flexibles han impulsado a las organizaciones de la región a modernizar sus plataformas tecnológicas para responder a demandas de escalabilidad, disponibilidad, seguridad y eficiencia operativa (UN ECLAC, 2024). Este escenario ha favorecido la adopción de tendencias emergentes como la computación en la nube, el edge computing y los enfoques de ciberresiliencia, los cuales están redefiniendo la forma en que se diseñan, despliegan y gestionan los sistemas digitales contemporáneos (Carvalho et al., 2021; Andriulo et al., 2024).

La computación en la nube ha democratizado el acceso a recursos tecnológicos avanzados mediante modelos de servicio flexibles y escalables, permitiendo optimizar costos y acelerar la innovación (Mell & Grance, 2020). No obstante, su naturaleza centralizada plantea desafíos relacionados con la latencia transfronteriza, la soberanía de datos y la dependencia de proveedores globales, aspectos especialmente sensibles en regiones con marcos regulatorios heterogéneos (Almeida & Doneda, 2020). En respuesta, el edge computing ha surgido como un paradigma complementario que acerca el procesamiento de datos a los puntos de generación, reduciendo tiempos de respuesta y habilitando aplicaciones críticas en tiempo real (Andriulo et al., 2024; Carvalho et al., 2021).

Paralelamente, la ciberresiliencia se posiciona como un marco transversal que integra capacidades de prevención, resistencia, respuesta y recuperación ante incidentes, un aspecto crucial en una región donde los ciberataques han aumentado de manera sostenida y afectan infraestructuras críticas (NIST, 2022; OECD, 2023). A pesar de su potencial, la adopción de estas tendencias en América Latina presenta brechas estructurales asociadas a infraestructura desigual, limitaciones presupuestarias, marcos regulatorios fragmentados y capacidades técnicas insuficientes (UN ECLAC, 2024). Por ello, resulta necesario analizar comparativamente estas tecnologías, identificar sus implicaciones para la región y evaluar su contribución a la construcción de una infraestructura digital más robusta, segura y sostenible.

Este artículo aborda estas cuestiones mediante una revisión sistemática y un análisis crítico orientado a comprender el papel estratégico de estas tendencias en la transformación digital latinoamericana.

2. MARCO TEÓRICO

2.1 Infraestructura digital en América Latina

La infraestructura digital constituye la base para el desarrollo de servicios avanzados, la transformación productiva y la integración regional. En América Latina, su evolución ha estado marcada por brechas estructurales relacionadas con conectividad desigual, inversión limitada y marcos regulatorios fragmentados (UN ECLAC, 2024). Estas condiciones generan asimetrías significativas entre países y sectores, afectando la capacidad de adopción tecnológica y la resiliencia operativa. Organismos internacionales han señalado que la región enfrenta desafíos persistentes en materia de gobernanza digital, interoperabilidad y soberanía tecnológica, lo que limita la consolidación de ecosistemas digitales robustos (OECD, 2023).

2.2 Computación en la nube: evolución, modelos y desafíos

La computación en la nube se ha consolidado como un pilar fundamental de la infraestructura digital contemporánea debido a su capacidad para ofrecer escalabilidad, elasticidad y acceso a servicios avanzados mediante modelos bajo demanda (Mell & Grance, 2020). Su adopción ha permitido a organizaciones públicas y privadas optimizar costos y acelerar procesos de innovación. Sin embargo, su arquitectura centralizada introduce desafíos relacionados con la latencia transfronteriza, la dependencia de proveedores globales y la soberanía de datos, aspectos especialmente sensibles en regiones con marcos regulatorios heterogéneos (Almeida & Doneda, 2020). Estas tensiones han impulsado la búsqueda de modelos híbridos que combinen la nube con arquitecturas distribuidas para mejorar la autonomía operativa

2.3 Edge computing: procesamiento distribuido y autonomía operativa

El edge computing ha emergido como un paradigma complementario que acerca el procesamiento de datos a los puntos de generación, reduciendo la latencia y habilitando aplicaciones críticas en tiempo real. Su relevancia se ha incrementado con la expansión del Internet de las Cosas (IoT), las ciudades inteligentes y los sistemas industriales avanzados (Andriulo et al., 2024). La literatura destaca que este enfoque permite mejorar la eficiencia operativa y reducir la dependencia de infraestructuras centralizadas, aunque introduce desafíos asociados a la complejidad de gestión, la interoperabilidad y la ampliación de la superficie de ataque (Carvalho et al., 2021; Khan et al., 2022). Su adopción requiere

capacidades técnicas avanzadas y marcos de gobernanza que garanticen seguridad y continuidad.

2.4 Ciberresiliencia: un marco transversal para la continuidad digital

La ciberresiliencia se ha convertido en un componente esencial para garantizar la continuidad digital en un contexto de amenazas crecientes. Este enfoque integra capacidades de prevención, resistencia, respuesta y recuperación ante incidentes, permitiendo a las organizaciones mantener operaciones críticas incluso bajo condiciones adversas (NIST, 2022). En América Latina, la necesidad de fortalecer la ciberresiliencia es particularmente urgente debido al incremento sostenido de ataques dirigidos a infraestructuras críticas, servicios públicos y sectores estratégicos (OECD, 2023). La literatura señala que la madurez regional en esta materia es heterogénea y que persisten brechas significativas en inversión, talento especializado y cultura organizacional.

2.5 Convergencia tecnológica: nube, edge y ciberresiliencia como ecosistema integrado

La convergencia entre computación en la nube, edge computing y ciberresiliencia constituye una tendencia clave en la evolución de la infraestructura digital. Este enfoque integrado permite combinar la escalabilidad de la nube, la inmediatez del edge y la robustez de la ciberresiliencia para construir arquitecturas más eficientes y seguras (Andriulo et al., 2024; Carvalho et al., 2021). La literatura reciente destaca que esta convergencia es fundamental para habilitar servicios avanzados, optimizar recursos y garantizar continuidad operativa en entornos complejos y distribuidos.

2.6 Brechas y desafíos en América Latina

A pesar de los avances, América Latina enfrenta brechas estructurales que limitan la adopción plena de estas tecnologías. Entre las más relevantes se encuentran la infraestructura desigual, la escasez de centros de datos regionales, la falta de talento especializado y la fragmentación regulatoria en materia de datos y privacidad (UN ECLAC, 2024). Estas limitaciones afectan la capacidad de los países para implementar arquitecturas híbridas, desplegar soluciones distribuidas y fortalecer la resiliencia digital. Organismos internacionales han subrayado la necesidad de políticas públicas coherentes, inversión sostenida y cooperación regional para superar estas brechas (OECD, 2023).

3. METODOLOGÍA

3.1 Enfoque de investigación

Este estudio se desarrolló mediante una revisión sistemática de literatura, orientada a identificar, analizar y sintetizar evidencia reciente sobre computación en la nube, edge computing y ciberresiliencia en América Latina. La revisión sistemática es un enfoque ampliamente utilizado para integrar conocimiento disperso y evaluar tendencias tecnológicas emergentes, especialmente en campos en rápida evolución (Carvalho et al., 2021; Andriulo et al., 2024). Este método permite garantizar rigor, transparencia y reproducibilidad en el proceso de búsqueda, selección y análisis de estudios relevantes.

3.2 Diseño metodológico general

El diseño metodológico se estructuró siguiendo las directrices del PRISMA 2020, que establece criterios para la identificación, cribado, elegibilidad e inclusión de estudios en revisiones sistemáticas (OECD, 2023; UN ECLAC, 2024). Se definieron criterios de inclusión basados en el año de publicación, la pertinencia temática, la disponibilidad de texto completo y la calidad metodológica. Asimismo, se excluyeron documentos duplicados, literatura sin rigor académico y fuentes corporativas no indexadas, siguiendo recomendaciones metodológicas para revisiones tecnológicas (Carvalho et al., 2021).

3.3 Proceso PRISMA aplicado.

La estrategia de búsqueda se aplicó en bases de datos académicas reconocidas, como Scopus, Web of Science, IEEE Xplore y SpringerLink. Se utilizaron combinaciones de palabras clave relacionadas con computación en la nube, arquitecturas híbridas, edge computing, IoT, ciberresiliencia, continuidad digital e infraestructura regional. Esta estrategia permitió capturar tanto estudios específicos de América Latina como investigaciones globales con aplicabilidad contextual, dada la limitada disponibilidad de literatura regional especializada (UN ECLAC, 2024).

Tabla 1. Resumen PRISMA

Fase PRISMA	Resultados
Registros identificados	562
Registros tras eliminar duplicados	421

Registros cribados	421
Registros excluidos en el cribado	339
Estudios evaluados a texto completo	82
Estudios excluidos tras evaluación completa	45
Estudios incluidos en la síntesis final	37

3.3.1 Resumen cuantitativo PRISMA.

Durante el proceso PRISMA se identificaron 562 registros iniciales. Tras la eliminación de duplicados, quedaron 421 documentos para el cribado. De estos, 339 fueron excluidos por falta de pertinencia temática, insuficiente rigor metodológico o ausencia de acceso completo. Posteriormente, se evaluaron 82 estudios a texto completo, y finalmente 37 cumplieron con los criterios de inclusión, conformando el corpus definitivo de análisis. Los criterios de exclusión contemplaron artículos anteriores a 2018, estudios sin metodología verificable, documentos centrados exclusivamente en hardware sin relación con infraestructura digital, publicaciones redundantes o duplicadas y trabajos sin relevancia regional o sin aplicabilidad práctica.

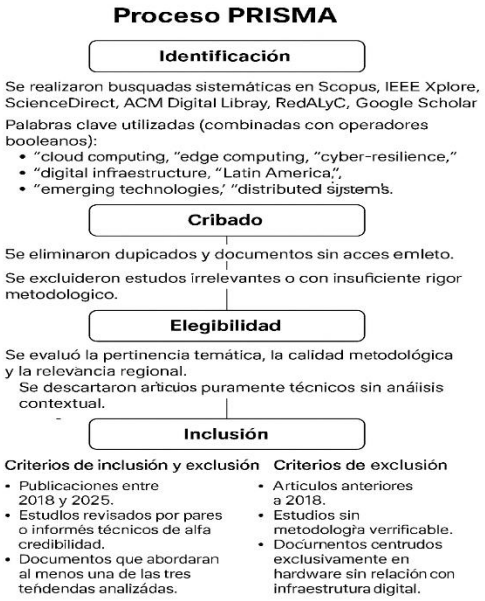

Fig. 1. Modelo PRISMA.

3.4 Proceso de selección

El proceso de selección siguió las cuatro etapas establecidas por PRISMA: identificación, cribado, elegibilidad e inclusión. Tras la aplicación de los criterios definidos, se seleccionaron treinta y siete estudios que cumplían con los estándares de calidad y pertinencia requeridos para el análisis. La selección final se basó en la relevancia temática, la solidez metodológica y la contribución al entendimiento de las tendencias tecnológicas emergentes en la región (Andriulo et al., 2024; Khan et al., 2022).

3.5 Análisis de la información

El análisis de la información se desarrolló mediante una síntesis cualitativa que integró los hallazgos de los estudios seleccionados para identificar patrones, brechas y tendencias. Se empleó un enfoque de codificación temática que permitió organizar la evidencia en categorías analíticas relacionadas con la adopción de computación en la nube, la expansión del edge computing, la ciberresiliencia, las brechas estructurales regionales y la convergencia tecnológica. Este enfoque resulta adecuado para estudios tecnológicos donde la evidencia es heterogénea y combina perspectivas técnicas, organizacionales y regulatorias (Carvalho et al., 2021; Andriulo et al., 2024).

3.6 Integración del modelo DSEI

Como complemento analítico, se incorporó el modelo DSEI (Disponibilidad, Seguridad, Eficiencia e Integración), utilizado como marco para evaluar de manera transversal la madurez y coherencia de las tecnologías estudiadas. Este modelo permitió estructurar la interpretación de los hallazgos en torno a cuatro dimensiones críticas de la infraestructura digital: la disponibilidad de servicios y recursos tecnológicos, la seguridad y resiliencia frente a incidentes, la eficiencia operativa de las arquitecturas distribuidas y la integración entre sistemas, plataformas y marcos regulatorios. Su aplicación facilitó una lectura comparativa entre computación en la nube, edge computing y ciberresiliencia, permitiendo identificar sinergias, tensiones y oportunidades de convergencia tecnológica en el contexto latinoamericano.

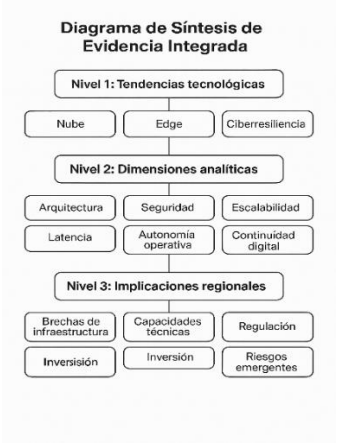

Fig. 2. Modelo DSEI

3.7 Consideraciones éticas y de calidad

Se priorizaron fuentes académicas indexadas y documentos institucionales de alta credibilidad, como NIST (2022), OECD (2023) y UN ECLAC (2024). Se evitó el uso de informes corporativos como evidencia principal debido a su naturaleza comercial y a la ausencia de revisión por pares. Asimismo, se garantizó la trazabilidad del proceso mediante la documentación completa de los criterios, decisiones y exclusiones aplicadas durante la revisión.

4. RESULTADOS

4.1 Panorama actual de la infraestructura digital en América Latina

La evidencia analizada muestra que la infraestructura digital en América Latina presenta avances significativos, pero continúa marcada por brechas estructurales que afectan su capacidad de adopción tecnológica. La región mantiene una conectividad desigual entre zonas urbanas y rurales, una disponibilidad limitada de centros de datos regionales y marcos regulatorios fragmentados que dificultan la interoperabilidad y la soberanía digital (UN ECLAC, 2024). Estas condiciones generan un ecosistema heterogéneo en el que la adopción de tecnologías emergentes avanza a ritmos distintos según el país, el sector y la capacidad institucional. Organismos internacionales han señalado que estas brechas limitan la consolidación de servicios digitales robustos y afectan la resiliencia operativa regional (OECD, 2023).

4.2 Adopción y madurez de la computación en la nube

La computación en la nube se posiciona como la tecnología con mayor nivel de consolidación en la región. Su adopción se ha visto impulsada por la disponibilidad de modelos escalables, la reducción de costos operativos y la madurez de los servicios ofrecidos por proveedores globales (Mell & Grance, 2020). Sectores como el financiero y el comercio electrónico lideran su implementación debido a la necesidad de alta disponibilidad y capacidad de procesamiento. En contraste, el sector público avanza de manera más lenta debido a restricciones normativas y requerimientos de soberanía de datos (Almeida & Doneda, 2020). La educación superior tiende a adoptar modelos híbridos influenciados por limitaciones presupuestarias y necesidades de flexibilidad operativa, mientras que la industria manufacturera utiliza la nube para habilitar analítica avanzada y automatización (Carvalho et al., 2021). A pesar de estos avances, persisten desafíos relacionados con la latencia transfronteriza, la dependencia de proveedores globales y la vulnerabilidad ante interrupciones masivas, lo que refuerza la necesidad de arquitecturas complementarias.

4.3 Expansión del edge computing y su impacto operativo.

El edge computing se encuentra en una fase de crecimiento acelerado en América Latina, impulsado por la expansión del IoT industrial, las iniciativas de ciudades inteligentes y la necesidad de procesamiento local en aplicaciones críticas. La literatura destaca que este paradigma adquiere relevancia estratégica debido a su capacidad para reducir la latencia, mejorar la autonomía operativa y disminuir la dependencia de infraestructuras centralizadas (Andriulo et al., 2024). Su adopción es especialmente relevante en sectores como manufactura, salud y logística, donde los tiempos de respuesta inmediatos son esenciales para garantizar continuidad y eficiencia.

4.4 Impactos operativos del edge computing.

Los estudios revisados coinciden en que el edge computing genera beneficios operativos significativos. La reducción de la latencia permite mejorar el rendimiento de aplicaciones sensibles al tiempo, mientras que la autonomía operativa facilita la continuidad en zonas con conectividad limitada. Asimismo, el procesamiento local disminuye los costos asociados a la transferencia de grandes volúmenes de datos hacia la nube y fortalece el control

sobre información sensible, reduciendo riesgos de exposición (Carvalho et al., 2021; Khan et al., 2022). Estos beneficios explican su creciente adopción en entornos industriales y de servicios críticos.

4.5 Desafíos para la adopción del edge computing.

A pesar de su potencial, la adopción del edge computing enfrenta desafíos relevantes. La falta de estandarización dificulta la interoperabilidad entre plataformas y proveedores, mientras que la gestión de nodos distribuidos incrementa la complejidad operativa y exige capacidades avanzadas de monitoreo y mantenimiento. La ampliación de la superficie de ataque introduce nuevos riesgos de seguridad, especialmente en entornos con múltiples puntos vulnerables (Khan et al., 2022). Además, persiste una escasez de talento especializado en arquitecturas distribuidas, lo que limita la capacidad de implementación a gran escala en la región.

4.6 Ciberresiliencia como eje transversal de continuidad digital.

La evidencia revisada muestra un incremento sostenido en incidentes cibernéticos en América Latina, particularmente en forma de ransomware, ataques a infraestructuras críticas, filtración de datos e interrupciones de servicios públicos (OECD, 2023). En este contexto, la ciberresiliencia emerge como un marco indispensable para garantizar la continuidad digital. Los estudios indican que las organizaciones con mayor madurez integran capacidades de prevención, respuesta y recuperación, emplean arquitecturas redundantes, aplican segmentación de redes, implementan monitoreo continuo y realizan ejercicios de simulación de crisis (NIST, 2022). Sin embargo, la mayoría de las instituciones latinoamericanas aún operan bajo modelos reactivos y presentan capacidades limitadas de recuperación ante incidentes, lo que evidencia la necesidad de fortalecer estrategias de resiliencia digital.

4.7. Comparación crítica entre computación en la nube, edge computing y ciberresiliencia.

Tabla 2. Comparación crítica de tendencias emergentes en infraestructura digital.

Dimensión	Computación en la nube	Edge computing	Ciberresiliencia
Arquitectura	Centralizada, escalable	Distribuida, cercana al usuario	Transversal, integra múltiples capas
Latencia	Media-alta	Muy baja	Depende de la arquitectura
Seguridad	Alta, pero dependiente del proveedor	Variable, superficie ampliada	Integral, orientada a continuidad
Costos	Predecibles, modelo OPEX	Variables según despliegue	Inversión continua
Autonomía	Baja-moderada	Alta	Alta en organizaciones maduras
Riesgos	Dependencia externa	Complejidad operativa	Falta de capacidades internas
Aplicabilidad regional	alta	media-alta	media, depende de madurez

El análisis comparativo evidencia que estas tres tendencias responden a necesidades distintas dentro de la infraestructura digital, pero su integración resulta estratégica. La computación en la nube ofrece escalabilidad y eficiencia económica, aunque enfrenta tensiones relacionadas con soberanía de datos y dependencia de proveedores (Almeida & Doneda, 2020). El edge computing aporta baja latencia y autonomía operativa, pero introduce complejidad de gestión y una superficie de ataque ampliada (Carvalho et al., 2021). La ciberresiliencia actúa como un marco transversal que garantiza continuidad y recuperación, aunque su efectividad depende de inversiones sostenidas y madurez organizacional (NIST, 2022). En conjunto, la nube aporta escala, el edge aporta inmediatez y la ciberresiliencia aporta estabilidad.

4.8 Convergencia tecnológica: hacia arquitecturas híbridas y resilientes

Los resultados muestran que la convergencia entre computación en la nube, edge computing y ciberresiliencia constituye la tendencia dominante en la literatura reciente. Las arquitecturas híbridas permiten combinar procesamiento local para datos sensibles, almacenamiento y análisis en la nube, y mecanismos de continuidad basados en redundancia, segmentación y monitoreo continuo (Andriulo et al., 2024). Esta integración optimiza costos

y rendimiento, mejora la respuesta ante incidentes y fortalece la resiliencia operativa. En América Latina, la convergencia adquiere especial relevancia debido a la infraestructura desigual y a la necesidad de soluciones adaptativas capaces de operar en entornos con limitaciones de conectividad y capacidades institucionales.

4.9 Brechas y limitaciones identificadas

El análisis crítico revela brechas estructurales que limitan la adopción plena de estas tecnologías en la región. Entre las más relevantes se encuentran la infraestructura insuficiente en zonas rurales y periurbanas, la escasez de centros de datos regionales con certificaciones avanzadas, la falta de talento especializado en edge computing y resiliencia digital, la fragmentación regulatoria en materia de datos y privacidad, y la inversión limitada en seguridad y continuidad operativa (UN ECLAC, 2024; OECD, 2023). Estas brechas explican la adopción desigual entre países y sectores, así como la limitada integración de la ciberresiliencia como componente transversal de la infraestructura digital latinoamericana.

Tabla 3. Beneficios y limitaciones.

Dimensión	Computación en la nube	Edge computing	Ciberresiliencia
Beneficios principales	Escalabilidad, elasticidad, reducción de costos, acceso a servicios avanzados	Baja latencia, autonomía operativa, procesamiento local, eficiencia en IoT	Continuidad operativa, resistencia ante incidentes, recuperación rápida
Limitaciones clave	Soberanía de datos, dependencia de proveedores, latencia transfronteriza	Complejidad de gestión, mantenimiento distribuido, mayor superficie de ataque	Requiere inversión sostenida, cultura organizacional madura

Análisis de la Tabla 3. La comparación entre computación en la nube, edge computing y ciberresiliencia revela tres enfoques complementarios pero con lógicas operativas distintas dentro de la infraestructura digital contemporánea. La nube destaca por su escalabilidad y eficiencia económica, aunque enfrenta tensiones relacionadas con soberanía de datos y dependencia de proveedores, lo que puede limitar su adopción plena en contextos latinoamericanos. El edge computing, por su parte, responde a necesidades de baja latencia

y autonomía operativa, especialmente en ecosistemas IoT; sin embargo, introduce una complejidad de gestión considerable y amplía la superficie de ataque al distribuir recursos en múltiples nodos. La ciberresiliencia actúa como un marco transversal que fortalece la continuidad operativa, pero su efectividad depende de inversiones sostenidas y de una cultura organizacional madura. En conjunto, estas tendencias no compiten, sino que se potencian: la nube aporta escala, el edge aporta inmediatez y la ciberresiliencia garantiza estabilidad, aunque su integración exige capacidades técnicas avanzadas y gobernanza clara.

Tabla 4. Madurez tecnológica por sector.

Sector	Computación en la Nube	Edge computing	Ciberresiliencia
Gobierno	Medio	Bajo	Bajo–medio
Educación superior	Medio	Bajo–medio	Bajo
Industria manufacturera	Alto	Medio–alto	Medio
Sector financiero	Muy alto	Medio	Alto
Salud	Medio	Medio	Bajo–medio

Análisis de la Tabla 4. La adopción de computación en la nube, edge computing y ciberresiliencia varía significativamente entre sectores, reflejando diferencias en regulación, capacidades técnicas y niveles de riesgo. La nube muestra la mayor penetración, especialmente en el sector financiero y la manufactura, donde la escalabilidad y la eficiencia operativa son prioritarias. En contraste, el edge computing avanza de forma más moderada: es relevante en manufactura y salud por sus necesidades de baja latencia, pero su adopción sigue limitada en gobierno y educación debido a restricciones presupuestarias y falta de infraestructura distribuida. La ciberresiliencia, aunque crítica para todos los sectores, presenta niveles de adopción más bajos, evidenciando brechas de madurez organizacional y capacidades internas, especialmente en educación y salud. El sector financiero destaca como el más avanzado, impulsado por regulaciones estrictas y altos riesgos operativos. En conjunto, la tabla muestra que la región avanza de forma desigual: la nube lidera, el edge crece selectivamente y la ciberresiliencia aún requiere fortalecimiento estructural.

Tabla 5. Riesgos emergentes y mitigación.

Riesgo	Descripción	Medidas de mitigación
Latencia crítica	Afecta servicios sensibles al tiempo.	Edge computing, optimización de red
Dependencia de proveedores	Riesgo de interrupciones y soberanía.	Multinube, políticas de datos, redundancia.
Ataques distribuidos	Mayor superficie de ataque en edge.	Zero Trust, segmentación, monitoreo continuo.
fallas de continuidad	Impacto en servicios críticos	Ciberresiliencia, redundancia, drp.

Análisis de la Tabla 5. La tabla evidencia que los riesgos asociados a la infraestructura digital no solo difieren en naturaleza, sino también en las estrategias necesarias para mitigarlos. La latencia crítica afecta directamente a servicios sensibles al tiempo y exige soluciones de proximidad como el edge computing, lo que revela una dependencia tecnológica creciente de arquitecturas distribuidas. En contraste, la dependencia de proveedores es un riesgo estructural de la computación en la nube, cuya mitigación requiere decisiones de gobernanza multinube, políticas de datos y redundancia más que soluciones técnicas. Los ataques distribuidos se intensifican con la expansión del edge, ampliando la superficie de exposición y obligando a adoptar enfoques Zero Trust y monitoreo continuo. Finalmente, las fallas de continuidad representan un riesgo transversal que solo puede abordarse mediante estrategias de ciberresiliencia y planes de recuperación robustos. En conjunto, la tabla muestra que cada riesgo demanda respuestas diferenciadas, pero todas convergen en la necesidad de arquitecturas híbridas y una gobernanza de seguridad más madura.

5. DISCUSIÓN

Los resultados obtenidos permiten comprender que América Latina atraviesa un proceso de transición hacia infraestructuras digitales más distribuidas, resilientes y orientadas a la eficiencia operativa. La computación en la nube se mantiene como la tecnología más

consolidada en la región, impulsada por su escalabilidad, elasticidad y capacidad para optimizar costos operativos, lo cual coincide con la literatura que destaca su papel central en la modernización tecnológica global (Mell & Grance, 2020). Sin embargo, su arquitectura centralizada genera tensiones relacionadas con la latencia transfronteriza, la dependencia de proveedores globales y la soberanía de datos, aspectos especialmente sensibles en contextos con marcos regulatorios heterogéneos como los latinoamericanos (Almeida & Doneda, 2020).

En este escenario, el edge computing emerge como un complemento estratégico que permite reducir la latencia, mejorar la autonomía operativa y habilitar aplicaciones críticas en tiempo real. La literatura reciente coincide en que este paradigma adquiere relevancia en sectores como manufactura, salud, logística y ciudades inteligentes, donde la inmediatez del procesamiento es esencial para garantizar continuidad y eficiencia (Andriulo et al., 2024). No obstante, su adopción enfrenta desafíos significativos asociados a la falta de estandarización, la complejidad de gestionar nodos distribuidos y la ampliación de la superficie de ataque, lo que exige capacidades avanzadas de monitoreo, mantenimiento y seguridad (Carvalho et al., 2021; Khan et al., 2022).

La ciberresiliencia se posiciona como un eje transversal indispensable para garantizar la continuidad digital en un contexto caracterizado por un incremento sostenido de incidentes cibernéticos que afectan infraestructuras críticas, servicios públicos y sectores estratégicos. Los marcos de resiliencia propuestos por organismos internacionales enfatizan la necesidad de integrar capacidades de prevención, resistencia, respuesta y recuperación, lo que implica inversiones sostenidas, monitoreo continuo y una cultura organizacional orientada a la gestión del riesgo (NIST, 2022). Sin embargo, la región presenta niveles de madurez heterogéneos, con brechas significativas en talento especializado, recursos técnicos y gobernanza institucional, lo que limita la capacidad de recuperación ante incidentes de alto impacto (OECD, 2023).

La discusión de los hallazgos revela que las brechas estructurales siguen siendo uno de los principales obstáculos para la adopción plena de tecnologías emergentes en América Latina. La infraestructura desigual, la falta de centros de datos regionales, la fragmentación regulatoria y la escasez de talento especializado afectan la capacidad de los países para

implementar arquitecturas híbridas y fortalecer la resiliencia digital (UN ECLAC, 2024). Estas limitaciones explican la adopción desigual entre sectores, donde industrias con mayor capacidad financiera avanzan más rápido que instituciones públicas o pequeñas y medianas empresas.

A pesar de estas brechas, la convergencia tecnológica entre computación en la nube, edge computing y ciberresiliencia emerge como una tendencia dominante en la literatura reciente. Esta integración permite combinar escalabilidad, procesamiento distribuido y continuidad operativa, lo que resulta fundamental para enfrentar los desafíos de un entorno digital cada vez más complejo. Las arquitecturas híbridas ofrecen ventajas significativas en términos de eficiencia, seguridad y adaptabilidad, especialmente en regiones con limitaciones de conectividad y recursos (Andriulo et al., 2024). La convergencia tecnológica no solo optimiza el rendimiento de los sistemas, sino que también fortalece la capacidad de respuesta ante incidentes y reduce la dependencia de infraestructuras centralizadas.

En conjunto, los hallazgos sugieren que América Latina requiere fortalecer su infraestructura digital, promover marcos regulatorios coherentes, impulsar la formación de talento especializado y fomentar la adopción de arquitecturas híbridas que integren nube, edge y ciberresiliencia. Asimismo, es necesario avanzar hacia modelos de gobernanza que garanticen soberanía digital, interoperabilidad y continuidad operativa. Estos elementos son esenciales para consolidar un ecosistema digital robusto, seguro y sostenible en el largo plazo.

6. LIMITACIONES DEL ESTUDIO

Este estudio presenta varias limitaciones que deben considerarse al interpretar los resultados. En primer lugar, aunque se aplicó una revisión sistemática rigurosa, la disponibilidad de literatura reciente sobre edge computing y ciberresiliencia en América Latina sigue siendo limitada y heterogénea. Esto implica que parte del análisis se apoya en estudios globales cuya aplicabilidad regional puede variar según el nivel de infraestructura, la madurez tecnológica y el contexto regulatorio de cada país.

En segundo lugar, la rápida evolución de las tecnologías analizadas —especialmente el edge computing y los marcos de ciberresiliencia— genera un desfase temporal inevitable

entre la publicación de los estudios y su implementación real en la región. Este desfase puede afectar la vigencia de algunos hallazgos, particularmente en sectores donde la innovación avanza con mayor rapidez.

Una tercera limitación se relaciona con la disponibilidad desigual de datos comparativos entre países latinoamericanos. La falta de indicadores estandarizados sobre infraestructura digital, inversión en resiliencia y adopción tecnológica dificulta establecer comparaciones precisas y generalizables. Asimismo, muchos estudios regionales carecen de metodologías robustas o presentan enfoques predominantemente descriptivos, lo que limita la profundidad del análisis.

Finalmente, este estudio se centró en fuentes secundarias y no incorporó entrevistas, estudios de caso o datos primarios que podrían enriquecer la comprensión contextual de los desafíos y oportunidades de la región. Investigaciones futuras podrían integrar metodologías mixtas para obtener una visión más completa, dinámica y situada del ecosistema digital latinoamericano.

7. CONCLUSIONES

La modernización de la infraestructura digital en América Latina depende de la capacidad de integrar tecnologías emergentes que permitan superar las limitaciones históricas de conectividad, seguridad y disponibilidad. Los resultados de este estudio muestran que la computación en la nube, el edge computing y los enfoques de ciberresiliencia constituyen pilares complementarios para avanzar hacia arquitecturas más eficientes, distribuidas y resilientes. La computación en la nube continúa siendo el motor principal de la transformación digital regional debido a su madurez y accesibilidad; sin embargo, la dependencia de proveedores globales y la latencia asociada a centros de datos remotos evidencian la necesidad de adoptar arquitecturas híbridas que reduzcan vulnerabilidades y fortalezcan la soberanía digital.

El edge computing se posiciona como un habilitador clave para aplicaciones críticas y entornos con restricciones de conectividad, aportando autonomía operativa y procesamiento en tiempo real. No obstante, su adopción requiere capacidades técnicas avanzadas, estandarización y marcos de gobernanza que aún no están plenamente

consolidados en la región. Por su parte, la ciberresiliencia emerge como un componente transversal indispensable para garantizar la continuidad digital en un contexto de amenazas crecientes, aunque su implementación sigue siendo desigual y limitada por brechas de inversión y formación especializada.

En conjunto, la evidencia indica que la convergencia entre computación en la nube, edge computing y ciberresiliencia ofrece una ruta estratégica para fortalecer la infraestructura digital latinoamericana. Sin embargo, su éxito dependerá de políticas públicas coherentes, inversión sostenida, fortalecimiento del talento especializado y una visión regional que priorice la soberanía tecnológica y la resiliencia operativa. Solo mediante un enfoque integrado será posible construir ecosistemas digitales capaces de responder a las demandas actuales y futuras de la región.

DECLARACIÓN DE CONFLICTO DE INTERESES. - La autora declara que No existe conflicto de intereses de carácter financiero, personal, académico o de cualquier otra índole que haya influido en los resultados, la interpretación o la presentación de este trabajo.

CONTRIBUCIÓN DE AUTORÍA

	MARIA ORTEGA
Participar activamente en:	
Conceptualización	**X**
Análisis formal	**X**
Adquisición de fondos	**X**
Investigación	**X**
Metodología	**X**
Administración del proyecto	**X**
Recursos	**X**
Redacción borrador original	**X**
Redacción revisión y edición	**X**
La discusión de los resultados	**X**
Revisión y aprobación de la versión final del trabajo.	**X**

REFERENCIAS BIBLIOGRÁFICAS

Almeida, F., & Doneda, D. (2020). Data governance and digital sovereignty in Latin America. *Journal of Cyber Policy*, 5, 394–412.

Andriulo, F. C., Fiore, M., Mongiello, M., Traversa, E., & Zizzo, V. (2024). *Edge computing and cloud computing for Internet of Things: A review*. Informatics, 11(4), 71. https://doi.org/10.3390/informatics11040071

Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2019). *Fog computing: A platform for internet of things and analytics.* Springer.

Carvalho, G., Cabral, B., Pereira, V., & Bernardino, J. (2021). Edge computing: Current trends, research challenges and future directions. *Computing, 103*(5), 993–1023. https://doi.org/10.1007/s00607-020-00896-5

CISA. (2021). *Cyber resilience review (CRR) resource guide*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Cisco. (2022). *Global networking trends report: The rise of distributed architectures*. Cisco Systems. https://www.cisco.com

Gartner. (2023). *Edge computing hype cycle: Trends and adoption patterns*. Gartner Research. https://www.gartner.com

IBM. (2020). *Cyber resilience in the age of hybrid cloud.* IBM Security Report. https://www.ibm.com/security

IDC. (2024). *Latin America digital infrastructure outlook*. International Data Corporation. https://www.idc.com

Khan, W., Rehman, M., & Zaman, N. (2022). Edge computing security challenges and solutions: A systematic review. *IEEE Access,* 10, 11245–11267.

Mell, P., & Grance, T. (2020). *The NIST definition of cloud computing* (SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

NIST. (2022). *Cyber resilience framework* (CRF). National Institute of Standards and Technology. https://www.nist.gov

OECD. (2023). *Digital transformation in Latin America: Infrastructure, governance and resilience.* OECD Publishing. https://doi.org/10.1787/9789264307957-en

Omar, A. S., & Mwakondo, F. (2024). *Evolution of cloud computing: Trends, issues, and future directions – A systematic literature review*. International Journal of Computer Science Trends and Technology, 12(3).

UN ECLAC. (2024). *Digital development in Latin America and the Caribbean: Infrastructure, gaps and opportunities*. United Nations Economic Commission for Latin America and the Caribbean. https://www.cepal.org

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. (2018). *Security and privacy in smart city applications: Challenges and solutions.* IEEE Communications Magazine, 55(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM