Experior
Revista de investigación ADEN

Experior: Revista de Investigación de ADEN University
ISSN L 2953-3090
Vol. 5 (2) julio-/diciembre 2026

De protección perimetral a ciberresiliencia: nuevo paradigma de seguridad en nube híbrida

From Perimeter Protection to Cyber Resilience: A New Security Paradigm in Hybrid Cloud

Juan Rigoberto Castillo Serracín
Universidad de Panamá, Panamá
juan.castillos@up.ac.pa
https://orcid.org/0009-0006-5821-7028

Kathia Carmona
Universidad de Panamá, Panamá
kathia.carmona@up.ac.pa
https://orcid.org/0009-0004-4692-3115

Odessa Aranda
Universidad de Panamá, Panamá
odessa.aranda@up.ac.pa
https://orcid.org/0000-0002-3698-1141

Recibido: 13/01/2026.
Aceptado: 21/04/2026.
Publicado: 15/07/2026.

Cómo citar: Castillo Serracín, J., Carmona, K., Aranda, O. (2026). De protección perimetral a ciberresiliencia: nuevo paradigma de seguridad en nube híbrida. *Experior, 5*(2), 105-118. https://doi.org/10.56880/experior52.1

Resumen

La adopción generalizada de la nube híbrida ha disuelto las fronteras físicas de la infraestructura empresarial, dejando obsoletos los modelos de seguridad basados en el perímetro estático. Este estudio analiza el cambio de paradigma desde la protección tradicional hacia la ciberresiliencia, con el objetivo general de proponer un modelo estratégico que integre la automatización, la Inteligencia Artificial y los principios de Zero Trust como pilares fundamentales. Utilizando una metodología cualitativa, descriptiva y analítica, la investigación se basó en una revisión bibliográfica estructurada orientada al análisis crítico de contenido y la triangulación de estándares globales (NIST, ISO) con informes de la industria. Los resultados confirman la hipótesis de trabajo: la seguridad efectiva en entornos distribuidos depende de una transformación cultural hacia la resiliencia sistémica y no solo de la capacidad tecnológica. Se evidencia que, si bien la arquitectura de Confianza Cero resuelve el control de acceso, la integración de orquestación SOAR e IA es crítica para mitigar la brecha de talento humano del 54% y garantizar la soberanía de los datos. Se concluye que el futuro de la seguridad híbrida reside en la defensa autónoma, capaz de aprender y reconfigurarse en tiempo real para asegurar la continuidad operativa.

Palabras clave: ciberresiliencia, nube híbrida, seguridad informática, Inteligencia Artificial, soberanía de datos.

Abstract

The widespread adoption of hybrid cloud has dissolved the physical boundaries of enterprise infrastructure, rendering static perimeter-based security models obsolete. This study analyzes the paradigm shift from traditional protection towards cyber resilience, with the general objective of proposing a strategic model that integrates automation, Artificial Intelligence, and Zero Trust principles as fundamental pillars. Using a qualitative, descriptive, and analytical methodology, the research was based on a Structured Literature Review oriented towards critical content analysis and the triangulation of global standards (NIST, ISO) with industry reports. The results confirm the working hypothesis: effective security in distributed environments depends on a cultural transformation towards systemic resilience and not solely on technological capability. It is evidenced that, while Zero Trust architecture resolves access control, the integration of SOAR orchestration and AI is critical to mitigate the 54% human talent gap and guarantee data sovereignty. It is concluded that the future of hybrid security lies in autonomous defense, capable of learning and reconfiguring itself in real-time to ensure operational continuity.

Keywords: Cyber resilience, Hybrid Cloud, Computer Security, Artificial Intelligence, Data Sovereignty.

Introducción

En la última década, la arquitectura de la información empresarial ha sufrido una metamorfosis irreversible, transitando de centros de datos monolíticos y aislados hacia ecosistemas distribuidos y heterogéneos. La adopción de la nube híbrida se ha consolidado como una estrategia operativa y el estándar por defecto para la innovación corporativa, permitiendo a las organizaciones capitalizar la escalabilidad de la nube pública sin renunciar al control de sus infraestructuras privadas (Varghese & Buyya, 2018). Sin embargo, esta expansión de la superficie digital ha disuelto las fronteras físicas que tradicionalmente definían la seguridad informática, dejando obsoletos los modelos de defensa basados en el perímetro estático (Rose *et al.*, 2020).

La convergencia de entornos con infraestructuras locales (*on-premises*), nubes privadas y servicios de nube pública ha generado una complejidad sistémica sin precedentes. En este nuevo escenario, la noción de un perímetro seguro es una falacia técnica; los datos fluyen dinámicamente entre servidores locales, proveedores de hiperescala y dispositivos en el borde (*Edge Computing*), lo que incrementa la superficie de ataque en infraestructuras de IoT críticas (Zhukabayeva *et al.*, 2025). Esta complejidad expone a las organizaciones a vectores de ataque laterales y persistentes que desafían los controles tradicionales (Buck *et al.*, 2021). Como señalan Zissis & Lekkas (2012), la seguridad en la nube ya no puede depender de muros cortafuegos (*firewalls*), sino que exige una redefinición hacia la protección centrada en los datos y la identidad.

Esta transición tecnológica ha exacerbado una vulnerabilidad crítica, que es la asimetría entre la velocidad de la innovación digital y la capacidad de aseguramiento organizacional (Arafah *et al.*, 2025). Mientras que la automatización y la Inteligencia Artificial actúan como motores de agilidad operativa, también han sido adoptadas por actores maliciosos para orquestar

ataques más sofisticados. En regiones emergentes como América Latina, este desafío se ve magnificado por factores estructurales. Según estudios recientes de la industria, barreras como la escasez de talento especializado identificada por el 54% de los líderes de TI como el freno principal y la complejidad regulatoria sobre la soberanía de los datos, crean una brecha de seguridad que los modelos tradicionales no logran cerrar (IDC, 2023).

En este contexto, los paradigmas de ciberseguridad convencionales, enfocados en la prevención y el bloqueo de intrusiones, resultan insuficientes. La persistencia de las amenazas avanzadas obliga a las organizaciones a asumir que el compromiso del sistema es inevitable. Por consiguiente, la estrategia debe evolucionar desde una postura defensiva perimetral hacia un enfoque de ciberresiliencia: la capacidad de una organización para anticipar, resistir, recuperarse y evolucionar ante condiciones adversas o ataques ciberfísicos (NIST, 2021). Este enfoque es ratificado por organismos globales que posicionan la resiliencia como el nuevo estándar de gobernanza tecnológica (World Economic Forum, 2024).

La presente investigación se justifica por la necesidad crítica de articular un marco estratégico que equilibre la dicotomía entre innovación y seguridad, una urgencia derivada de la evolución asimétrica de las ciberamenazas, que ahora utilizan Inteligencia Artificial para superar las barreras perimetrales estáticas en cuestión de segundos (Microsoft, 2024b). Este estudio es particularmente relevante en el actual panorama regulatorio, donde la soberanía de datos y el cumplimiento normativo en sectores críticos como la banca y el gobierno exigen arquitecturas que garanticen la integridad de la información sin sacrificar la interoperabilidad. Ante este escenario, se evidencia que la mera implementación de herramientas tecnológicas aisladas carece de eficacia si no se integra en una cultura organizacional madura y en una gobernanza de datos robusta.

El problema central que aborda esta investigación radica en la obsolescencia de las estrategias de seguridad perimetral frente a la naturaleza ubicua y descentralizada de la nube híbrida. A pesar de la inversión masiva en tecnología, las organizaciones continúan operando bajo una falsa sensación de seguridad, ignorando que la identidad y el contexto de acceso son los nuevos perímetros de control. Esta desconexión entre la arquitectura técnica desplegada y la estrategia de seguridad aplicada incrementa exponencialmente el riesgo operativo y reputacional.

A partir de esta problemática, surge la siguiente interrogante que guía la investigación: ¿De qué manera se puede articular un modelo estratégico de seguridad que, integrando la automatización, la Inteligencia Artificial y los principios de *Zero Trust*, permita transitar efectivamente de la defensa perimetral a la ciberresiliencia en entornos de nube híbrida?

Para afrontar esta complejidad, la investigación tiene como objetivo general analizar el cambio de paradigma desde la protección perimetral hacia la ciberresiliencia en entornos híbridos, con la finalidad de proponer un modelo estratégico que integre la automatización, la inteligencia artificial y los principios de *Zero Trust* (Confianza Cero) como pilares fundamentales.

Bajo esta perspectiva, se sostiene la hipótesis de trabajo de que la adopción efectiva de la nube híbrida no depende únicamente de la capacidad

tecnológica, sino de una transformación cultural y estratégica hacia la resiliencia sistémica. Se prevé que las organizaciones que logren orquestar una defensa automatizada y adaptativa, priorizando la recuperación del servicio y la integridad de los datos sobre el blindaje perimetral, serán las únicas capaces de sostener una ventaja competitiva segura en la economía digital del siglo XXI.

Metodología

La presente investigación se enmarca en un enfoque cualitativo con un diseño no experimental, bibliográfico y documental. La naturaleza del estudio es de carácter descriptivo-analítico y propositivo, puesto que busca tanto caracterizar la taxonomía actual de amenazas en la nube híbrida como articular teóricamente la transición hacia un nuevo modelo de gestión basado en la ciberresiliencia. Este alcance propositivo trasciende la revisión literaria para formular un Modelo de Gestión Estratégica, el cual se diferencia de los estándares técnicos aislados al integrar la orquestación automatizada (SOAR) y el factor humano como variables críticas para la viabilidad operativa.

La estrategia de investigación se estructuró mediante una revisión bibliográfica sistematizada, priorizando la actualidad tecnológica en un horizonte temporal acotado a los últimos cuatro años (2021-2025). Para garantizar la replicabilidad del estudio, el proceso de recolección de datos se rigió por un protocolo de búsqueda estricto mediante el uso de operadores booleanos en bases de datos académicas de alto impacto (IEEE Xplore, ACM Digital Library, Google Scholar) y repositorios técnicos. Las cadenas de búsqueda principales se configuraron como: *("Hybrid Cloud Security" OR "Zero Trust") AND ("Artificial Intelligence") AND ("Cyber-resilience")*.

El muestreo intencional derivó en un corpus total de 28 documentos analizados, seleccionados tras aplicar criterios de inclusión rigurosos que filtraron fuentes puramente comerciales. La muestra final quedó estratificada de la siguiente manera: (a) 9 artículos científicos y capítulos de libros revisados por pares sobre arquitecturas distribuidas y aprendizaje automático; (b) 6 estándares y marcos de referencia globales (incluyendo NIST SP 800-207, NIST SP 800-53, NIST SP 800-160 Vol. 2, ISO/IEC 27001, COBIT 2019 y el Modelo de Responsabilidad Compartida de AWS); y (c) 13 informes técnicos de industria sobre brechas de talento y amenazas emergentes (provenientes de Microsoft, IBM, Fortinet, IDC, entre otros).

Para el procesamiento de la información, se utilizó como instrumento de recolección una Matriz de Categorización diseñada *ad hoc*, la cual permitió clasificar los hallazgos en tres ejes temáticos: la obsolescencia del perímetro, las capacidades de la Inteligencia Artificial (IA) en defensa activa y los principios de *Zero Trust*. Esta herramienta garantizó la validez de constructo mediante un enfoque de triangulación hermenéutica, validando la consistencia de los resultados al contrastar sistemáticamente tres niveles de fuentes: el deber ser académico (teoría), el marco regulatorio (normativa) y la realidad operativa de las amenazas (práctica).

Finalmente, el análisis trascendió la mera sumarización para realizar una síntesis integradora que justifica la fase propositiva de la investigación. Se evidenció que, si bien los estándares existentes definen los controles técnicos, carecen de una estrategia de implementación que mitigue la escasez de talento

humano. En respuesta, el modelo resultante no busca reinventar los controles de seguridad, sino orquestarlos, proponiendo la automatización como el habilitador indispensable de la resiliencia sistémica en entornos donde la gestión manual es ya inoperable.

Resultados

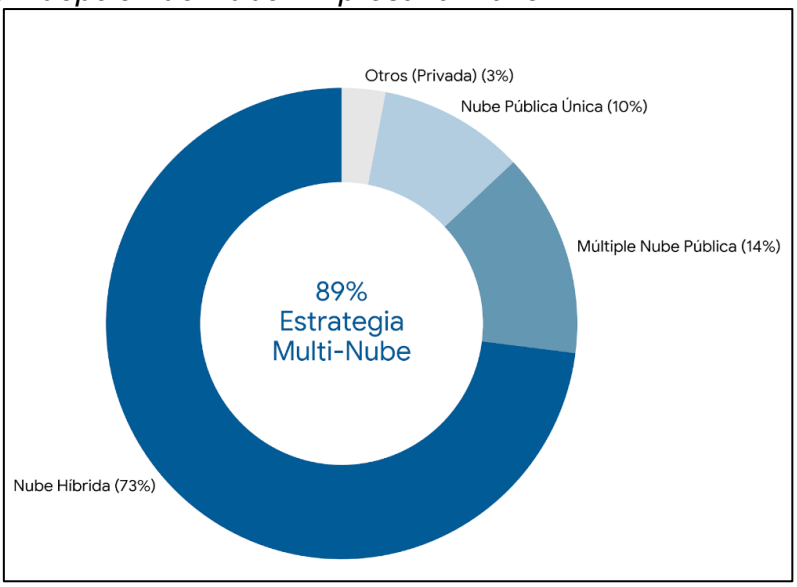
El análisis documental y la triangulación de informes de industria confirman la hipótesis de trabajo planteada: la seguridad basada en el perímetro físico es insuficiente para proteger los ecosistemas de nube híbrida debido a la latencia operativa y la descentralización de los activos. A continuación, se presentan los hallazgos estructurados en cuatro dimensiones críticas: la obsolescencia de la infraestructura tradicional, el impacto económico de la automatización, la propuesta de un modelo de defensa autónoma y el análisis de riesgos asociados.

1. La ubicuidad híbrida y la disolución del perímetro

La revisión de datos de mercado evidencia que la infraestructura empresarial ha mutado de forma irreversible. Como se observa a continuación en la Figura 1, la adopción de estrategias multi-nube alcanza un 89%, validando que el entorno operativo estándar ya no es un centro de datos aislado, sino un entorno de responsabilidad compartida donde la configuración segura es crítica (Amazon Web Services, 2024).

Figura 1

Estado de la Adopción de Nube Empresarial 2025



Nota. Adaptado de Flexera (2025).

El análisis de esta dispersión confirma que las organizaciones están abandonando el modelo tradicional de castillo y foso (*castle-and-moat*) en favor de arquitecturas centradas en la identidad. Este paradigma, descrito por Rose *et al.* (2020), opera bajo la premisa de una defensa perimetral rígida donde se otorga confianza implícita a cualquier entidad que logre acceder a la red interna,

permitiendo un movimiento lateral irrestricto. Dado que esta confianza ciega es insostenible en entornos distribuidos, la estrategia se ha reorientado hacia la validación continua de credenciales.

En un entorno donde los datos residen simultáneamente en infraestructuras locales (*on-premises*) y nubes públicas, la distinción entre interno (confiable) y externo (no confiable) es una falacia técnica. Al contrastar estos datos con el estándar NIST SP 800-207, se valida la necesidad de implementar una arquitectura de Confianza Cero (Zero Trust) bajo los pilares de verificación continua y acceso mínimo definidos por Rose *et al*. (2020). Investigaciones recientes confirman que este modelo es el único capaz de mitigar la desconfianza inherente en redes abiertas (Rajendran *et al*., 2025).

A diferencia del modelo tradicional dependiente de VPNs estáticas, que otorgan acceso amplio a la red permitiendo que un actor malintencionado se desplace libremente una vez dentro del perímetro (NSA, 2021), el modelo híbrido exige una micro-segmentación dinámica. Esta técnica descompone la red en zonas de seguridad aisladas hasta el nivel de la carga de trabajo individual, restringiendo el tráfico este-oeste y garantizando que el compromiso de un activo no derive en la infección total del ecosistema (*Rose et al.,* 2020). Este hallazgo es consistente con la telemetría de amenazas en América Latina (Fortinet, 2025), donde se registran promedios superiores a los 1,600 intentos de intrusión por segundo, una volumetría que hace colapsar cualquier defensa perimetral manual.

Sin embargo, esta saturación no es un fenómeno aislado reportado por un único proveedor; la triangulación de datos con otros líderes de la industria confirma una tendencia sistémica en la región. Como se evidencia en la Tabla 1, existe una convergencia en los indicadores de frecuencia y volumen reportados por distintas firmas de ciber-inteligencia para el periodo 2023-2024.

Tabla 1.
Triangulación de telemetría de amenazas en América Latina (2023-2024)

Fuente de Inteligencia	Métrica Clave Reportada	Interpretación Operativa
Fortinet (*FortiGuard Labs*)	200 mil millones de intentos de intrusión anuales (~1,600 por segundo).	Evidencia una saturación volumétrica diseñada para desbordar firewalls perimetrales por denegación de servicio o fuerza bruta.
Kaspersky (Panorama de Amenazas)	3 millones de intentos de ataque de malware diarios registrados en la región.	Demuestra la persistencia de la amenaza; cada día, una organización enfrenta millones de variantes de código malicioso automatizado.
Check Point (*Threat Intelligence*)	1,273 ataques semanales por organización en Latinoamérica (la tasa más alta a nivel global).	Indica una frecuencia de impacto. A diferencia del volumen bruto, esto confirma que cada empresa es un blanco activo constante.

Nota. Datos compilados a partir de los informes regionales de Fortinet (2025), Kaspersky (2023) y Check Point Research (2024).

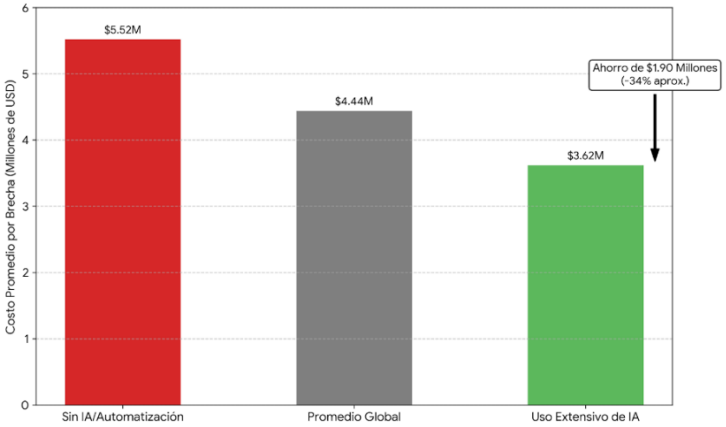
2. Impacto económico: correlación entre automatización y rentabilidad

Uno de los hallazgos más significativos de esta investigación, validado por los reportes globales de IBM (2025), es la relación inversamente proporcional entre la madurez de la Inteligencia Artificial y el costo financiero de las brechas de seguridad. Esta correlación se fundamenta en que el impacto monetario de un incidente no es estático, sino que escala exponencialmente con el tiempo de permanencia del atacante en la red (*dwell time*).

Mientras que los modelos de defensa manuales incurren en altos costos operativos derivados de la investigación forense prolongada y la interrupción de servicios críticos, la implementación de IA defensiva actúa como un mecanismo de contención financiera inmediata. Al automatizar la detección, se limita el volumen de datos exfiltrados y se preserva la continuidad del negocio, transformando lo que sería un evento catastrófico en un incidente operativo manejable. A continuación, en la Figura 2, se ilustra esta diferencia financiera.

Figura 2

Impacto económico de la IA y automatización en la ciberresiliencia



Nota. Datos procesados a partir de IBM Cost of a Data Breach Report (2025).

El análisis de estos datos permite desglosar el significado operativo del ahorro del 34% (una reducción de costos de 5.52 a 3.62 millones de dólares). Este margen no proviene de una reducción en licenciamiento de software, sino de la drástica disminución del Tiempo Medio de Contención (MTTC). Las organizaciones que integran orquestación automatizada (SOAR) reducen el ciclo de vida de una brecha en 80 días en comparación con aquellas que dependen de procesos manuales, según confirma el reporte global de IBM (2025). Esta métrica es determinante al analizar la realidad de América Latina, donde el tiempo de permanencia (*dwell time*) de un atacante suele ser superior al promedio global debido a la gestión artesanal de los Centros de Operaciones de Seguridad (SOC).

Un ejemplo pragmático de esta asimetría se observa en el sector financiero latinoamericano. Mientras que instituciones bancarias en países como Brasil y Colombia que han adoptado arquitecturas de respuesta autónoma logran contener incidentes de *ransomware* en cuestión de horas, organizaciones con madurez tecnológica baja en la región enfrentan tiempos de inactividad que promedian las tres semanas (Lumu Technologies, 2023). En este contexto, la

automatización no solo reduce días de exposición, sino que mitiga el daño reputacional irreversible asociado a la filtración prolongada de datos de clientes, un riesgo existencial en mercados altamente regulados.

3. La brecha de talento como barrera estructural

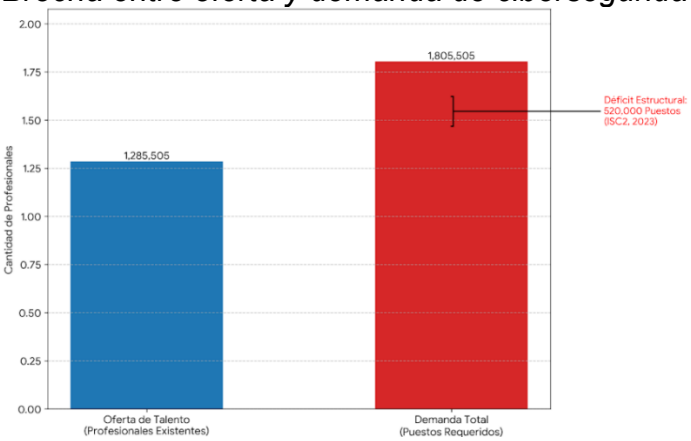
Para el contexto latinoamericano, esta eficiencia económica es vital debido a factores sistémicos que trascienden la capacidad de contratación. Si bien los datos de International Data Corporation (2023) revelan que el 54% de los líderes de TI identifican la escasez de habilidades como su barrera más crítica, la triangulación con el *Cybersecurity Workforce Study* de ISC2 (2023) confirma que el déficit en la región asciende a 1.3 millones de profesionales no cubiertos.

Matemáticamente, es imposible cerrar esta brecha mediante métodos de reclutamiento tradicionales, dado que existe un desajuste cualitativo de competencias (*skills mismatch*). Según el reporte de ManpowerGroup (2024), aunque existe una oferta de graduados en carreras de informática y sistemas, el 78% de los empleadores en tecnología reporta dificultades para encontrar perfiles con las certificaciones de ciberseguridad operativa necesarias. Esto evidencia que poseer un título universitario en sistemas no equivale a tener la capacidad combativa para gestionar un SOC. Por consiguiente, la automatización deja de ser una ventaja competitiva para convertirse en un requisito de supervivencia: la IA no reemplaza al analista, sino que mitiga la vulnerabilidad sistémica generada por la falta de personal calificado, permitiendo gestionar un volumen de alertas que humanamente sería inabarcable.

Esta disparidad cualitativa se materializa en cifras críticas al analizar el panorama regional. Para dimensionar la magnitud del desafío en el mercado local, la Figura 3 ilustra la brecha cuantitativa existente entre la fuerza laboral disponible y los requerimientos operativos de las organizaciones. Como se detalla a continuación, la oferta de talento actual es insuficiente para cubrir la demanda proyectada, lo que resulta en un déficit estructural que pone en riesgo la resiliencia de la infraestructura digital en América Latina.

Figura 3

Brecha entre oferta y demanda de ciberseguridad en América Latina



Nota. Basada en la triangulación de datos de IDC (2023), ISC2 (2023) y ManpowerGroup (2024).

Como se puede observar en la Figura 3, el 54% de los líderes de TI identifica la escasez de habilidades como su barrera crítica (International Data Corporation, 2023). Asimismo, el 78% de la dificultad de contratación se atribuye a un desajuste de competencias (ManpowerGroup, 2024), lo que confirma que la escasez de especialistas en la región no es un problema coyuntural, sino una limitación estructural inabarcable mediante mecanismos de reclutamiento tradicionales.

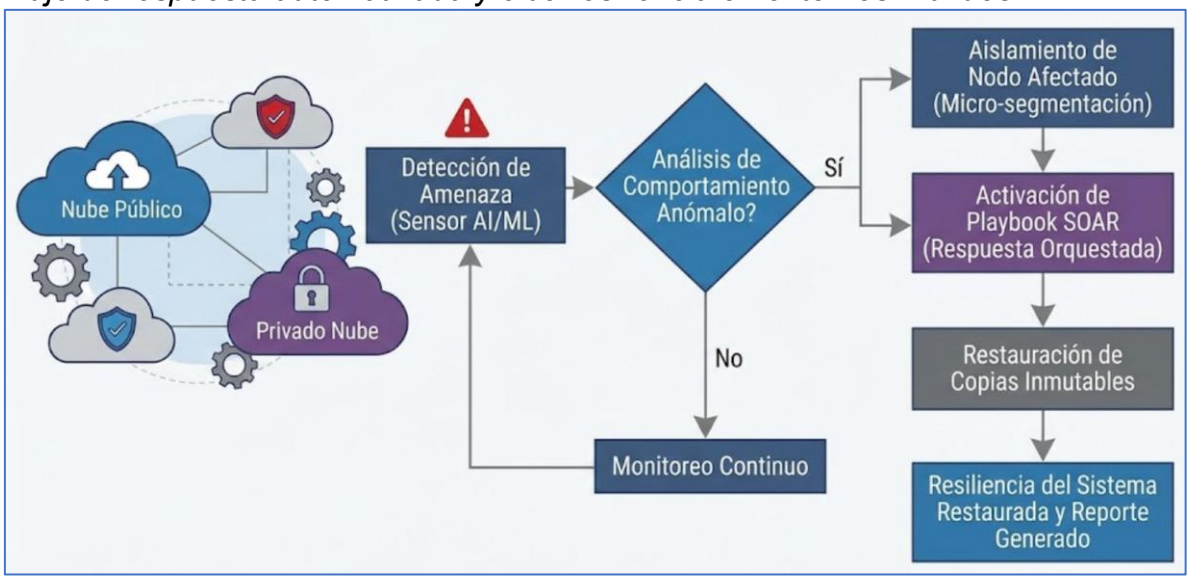
Ante este escenario, donde el déficit regional supera el millón de profesionales, las organizaciones latinoamericanas se ven obligadas a transitar de un modelo de defensa basado en capital humano intensivo hacia uno centrado en la eficiencia operativa. En consecuencia, la implementación de arquitecturas de confianza cero y la automatización de la respuesta ante incidentes dejan de ser opciones tecnológicas para convertirse en imperativos estratégicos que permiten compensar la falta de personal especializado mediante la optimización de las capacidades instaladas.

4. Propuesta de Modelo: Arquitectura de Defensa Autónoma Híbrida (ADAH)

En respuesta a la necesidad de articular una estrategia que trascienda la teoría y resuelva la asimetría de talento detectada, se propone el modelo de Defensa Autónoma Híbrida (ADAH). Este modelo orquesta tres pilares fundamentales que operan en ciclo cerrado, como se esquematiza en la Figura 4.

Figura 4

Flujo de respuesta automatizada y ciberresiliencia en entornos híbridos



Nota. basada en la integración de arquitectura NIST y flujos SOAR.

El modelo ADAH estructura la defensa en tres capas cognitivas:

1. Capa de detección (El "Ojo"): utiliza algoritmos de aprendizaje automático para establecer líneas base de comportamiento (UEBA). A diferencia de un SIEM tradicional, detecta anomalías sutiles (exfiltración lenta) sin

necesidad de firmas previas, utilizando modelos de *Deep Learning* para predecir vectores de ataque desconocidos (Dua & Du, 2016).

2. Motor de decisión (El "Cerebro"): actúa técnicamente como el Punto de Decisión de Políticas (PDP), ejecutando un algoritmo de confianza que pondera múltiples atributos más allá de la identidad del usuario. Basado en principios Zero Trust, este motor abandona la validación estática para aplicar una evaluación continua durante toda la sesión, analizando variables contextuales como la salud del dispositivo, la geolocalización y la sensibilidad del dato solicitado (Rose *et al*., 2020). Si el nivel de confianza calculado desciende por debajo del umbral aceptable en cualquier momento, el sistema revoca los privilegios instantáneamente o fuerza una re-autenticación escalonada (MFA), eliminando la confianza implícita persistente (Rose *et al*., 2020).
3. Orquestación de respuesta (La "Mano"): activa playbooks de SOAR para la contención inmediata (ej. aislar un nodo infectado en milisegundos), garantizando la continuidad operativa. La integración de SOAR con sistemas SIEM permite reducir la latencia de respuesta de manera drástica frente a la gestión manual (Upadhyaya *et al.*, 2022; Christian *et al*., 2022).

Transición de la Aumentación a la Autonomía Operativa La arquitectura propuesta representa un cambio de paradigma respecto a los modelos de gestión tradicionales, los cuales basan su eficacia en la aumentación humana para el análisis y validación de alertas. Dada la realidad estructural de la región, el modelo ADAH reorienta el uso de la telemetría avanzada para transitar de una lógica de asistencia técnica a una de sustitución operativa.

Bajo este enfoque, la tecnología deja de ser una herramienta de soporte para convertirse en el ejecutor primario. Esto permite evolucionar el ciclo de decisión de un esquema *"Human-in-the-loop"* (dependiente de validación manual) hacia uno de *"Human-on-the-loop"* (supervisión pasiva y auditoría posterior). De esta manera, la automatización se establece como la línea de defensa definitiva, garantizando la contención de amenazas en tiempos de máquina (*machine-speed*) sin depender de la disponibilidad de talento humano.

5. Análisis comparativo y evaluación de riesgos

Finalmente, para validar la pertinencia del modelo propuesto frente a los paradigmas existentes, se presenta en la Tabla 2 una matriz comparativa de evolución.

Tabla 2

Matriz comparativa de la evolución de paradigmas de seguridad

Criterio de análisis	Modelo Perimetral (tradicional)	Modelo Zero Trust (transicional)	Modelo ciberresiliencia (emergente)
Filosofía base	"Confiar, pero verificar" (*trust but verify*)	"Nunca confiar, siempre verificar" (*never trust, always verify*)	"Asumir la brecha" (*asume breach*)

Definición del perímetro	Estático: basado en la red física y firewalls	Lógico: basado en la identidad y el contexto de usuario	Dinámico: basado en el comportamiento y los datos
Mecanismo de defensa	Preventivo: bloqueo de intrusiones en el borde	Granular: microsegmentación y mínimos privilegios	Adaptativo: detección, respuesta y recuperación automatizada
Rol de la automatización (IA)	Nulo o reactivo (análisis de logs *post-mortem*)	De apoyo (análisis de políticas de acceso)	Central/proactivo (orquestación SOAR y detección de anomalías)
Viabilidad en Nube Híbrida	Baja: genera puntos ciegos y cuellos de botella	Alta: reduce la superficie de ataque efectiva	Óptima: garantiza la continuidad operativa ante fallos

Nota. a partir de la triangulación de estándares NIST e ISO.

Interpretación crítica y riesgos asociados. Si bien la Tabla 2 posiciona a la ciberresiliencia cognitiva como el estado óptimo, el análisis debe considerar los riesgos inherentes a la autonomía sistémica. La dependencia excesiva de la automatización introduce el riesgo de falsos positivos que podrían interrumpir operaciones legítimas si los umbrales de sensibilidad no se calibran correctamente siguiendo los catálogos de controles del NIST SP 800-53 (Joint Task Force, 2020).

Surge el desafío de los ataques adversarios, donde los actores de amenaza utilizan técnicas de *poisoning* para envenenar los datos de entrenamiento de los modelos defensivos. Por tanto, aunque el modelo perimetral es inviable por su ineficacia ante ataques modernos, la transición hacia la defensa autónoma requiere una gobernanza estricta alineada con marcos internacionales de gestión como la ISO/IEC 27001 (2022). Como se verá a continuación, esta gobernanza se apoya en la clasificación automatizada en tiempo real para mitigar que la propia automatización se convierta en un vector de ataque.

Bajo este esquema de gobernanza, la automatización gestiona la clasificación de datos sensibles mediante motores de descubrimiento continuo que operan en tiempo real. Según Microsoft (2024a), el uso de clasificadores basados en inteligencia artificial y huellas digitales de datos permite identificar, etiquetar y segmentar activos de información en el instante en que son creados o movilizados.

Al eliminar la dependencia de la clasificación manual, la cual resulta estática y propensa al error humano, la automatización facilita la aplicación de políticas dinámicas basadas en la criticidad del dato. Esto asegura que, ante una anomalía detectada, el sistema restrinja el acceso a la información de manera quirúrgica, garantizando la integridad de los activos incluso en entornos de alta volatilidad (Microsoft, 2024a).

Este análisis confirma que la viabilidad técnica en la nube híbrida no depende de muros más altos, sino de sistemas más inteligentes capaces de operar bajo condiciones de estrés. Al asegurar que estos sistemas cumplan con los objetivos de gobierno de TI de COBIT 2019 (ISACA, 2018), la organización puede priorizar de manera estratégica la recuperación del servicio sobre el

bloqueo estático, transformando la seguridad en un habilitador de resiliencia alineado con el negocio.

Conclusiones

La investigación realizada permite responder a la pregunta central del estudio y validar la hipótesis de trabajo: la seguridad en la nube híbrida no es un problema de capacidad de bloqueo perimetral, sino de gestión de la complejidad y velocidad de respuesta. Se concluye que la única manera de articular un modelo estratégico efectivo es mediante la transición del control estático hacia la Arquitectura de Defensa Autónoma Híbrida (ADAH**)** propuesta. Los resultados evidencian que, si bien el modelo *Zero Trust* resuelve la validación de identidad, es insuficiente por sí solo; la viabilidad operativa depende críticamente de la orquestación (SOAR) y la Inteligencia Artificial para cerrar la brecha estructural de talento humano, permitiendo reducir el tiempo medio de contención (MTTC) de días a minutos.

Desde una perspectiva crítica, el estudio demuestra que la ciberresiliencia es, ante todo, un desafío de soberanía de datos. La tecnología de nube híbrida actúa como un habilitador de negocios solo cuando la organización es capaz de clasificar sus activos no por su ubicación física, sino por su sensibilidad regulatoria. Por tanto, el éxito del modelo no reside en la compra de herramientas, sino en la madurez para automatizar la decisión de seguridad, transformando la defensa en un proceso cognitivo que aprende y se reconfigura en tiempo real sin intervención humana reactiva.

Como hoja de ruta para la implementación de estos hallazgos, se establecen directrices operativas diferenciadas. En el ámbito académico, para mitigar la brecha de talento del 54% identificada en los resultados, se recomienda a las instituciones abandonar la enseñanza exclusiva de seguridad perimetral y adoptar laboratorios de Ingeniería de Respuesta. Esto implica integrar en los planes de estudio el diseño de *playbooks* automatizados en plataformas SOAR, evaluando a los estudiantes no por la configuración de firewalls, sino por la métrica de reducción de tiempos de respuesta ante incidentes simulados.

Simultáneamente, para las organizaciones que operan en sectores regulados, se plantea sustituir las políticas de seguridad genéricas por la implementación de Matrices de Taxonomía de Datos. Esta acción concreta requiere etiquetar los activos de información según su nivel de confidencialidad antes de cualquier migración, aplicando controles de cifrado granular que aseguren la soberanía del dato independientemente de si este reside en una infraestructura local o en una nube pública.

Finalmente, como estrategia transversal para contrarrestar la asimetría de los ataques automatizados, se recomienda al sector privado y gubernamental la adopción de protocolos estándar de intercambio de amenazas, tales como STIX/TAXII. Esta medida permite transitar de una defensa aislada hacia una inmunidad ecosistémica, donde la detección de un compromiso en una entidad actualice automáticamente las reglas de defensa del resto del sector, validando así la resiliencia sistémica como el nuevo estándar de seguridad.

Referencias

Amazon Web Services. (2024). *Shared Responsibility Model*. AWS Cloud Security. https://aws.amazon.com/compliance/shared-responsibility-model/

Arafah, M., Al-Banna, A., & Aladawi, A. (2025). Cybersecurity in the Age of Digital Transformation: Protecting Assets, Infrastructure, and Innovation. En A. Aldweesh (Ed.), *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 265-290). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-1370-2.ch013

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust network architecture. *Computers & Security*, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436

Check Point Research. (2024). *2024 Security Report*. Check Point Software Technologies. https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2024&fw=f28ef

Christian, J., Paulino, L., & Sá, A. (2022). A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response. Lecture Notes in Computer Science, 13608, 102-115. Springer. https://doi.org/10.1007/978-3-031-21280-2_7

Dua, S., & Du, X. (2016). *Data Mining and Machine Learning in Cybersecurity*. CRC Press. https://doi.org/10.1201/b10867

Flexera. (2025). *2025 State of the Cloud Report*. Flexera. https://www.flexera.com/stateofthecloud

Fortinet. (2025). *2025 Global Threat Landscape Report*. FortiGuard Labs. https://www.fortiguard.com/threat-landscape-report

IBM. (2025). Cost of a Data Breach Report 2025. IBM Security. https://www.ibm.com/reports/data-breach

IDC. (2023). IDC FutureScape: Latin America IT Industry 2024 Predictions. International Data Corporation. https://www.idclatin.com/2023/Events/13_Dec_LA/FutureScapeLA2024.pdf

ISACA. (2018). *COBIT 2019 Framework: Governance and Management Objectives*. https://www.isaca.org/resources/cobit

ISC2. (2023). *ISC2 Cybersecurity Workforce Study 2023: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. ISC2. https://www.isc2.org/Research

Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53, Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kaspersky. (2023). *Redefining the Human Factor in Cybersecurity*. Kaspersky. https://www.kaspersky.com/blog/human-factor-360-report-2023/

Lumu Technologies. (2023). *2023 Ransomware Flashcard Report*. Lumu. https://lumu.io/resources/2023-ransomware-flashcard-report/

ManpowerGroup. (2024). *Global Talent Shortage 2024*. ManpowerGroup. https://go.manpowergroup.com/talent-shortage-2024

Microsoft. (2024a). *Información sobre la clasificación automatizada de datos*. https://learn.microsoft.com/es-es/purview/apply-sensitivity-label-automatically

Microsoft. (2024b). *Microsoft Digital Defense Report 2024*. Microsoft Security. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

National Security Agency. (2021). *Embracing a Zero Trust security model* (Cybersecurity Information Sheet). https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

NIST. (2021). *NIST SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Organización Internacional de Normalización. (2022). *Sistemas de gestión de la seguridad de la información — Requisitos* (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

Rajendran, R. K., Mohana Priya, T., Goundar, S., Madhavi, K. R., Avanija, J., & Avula, B. R. (2025). Zero Trust Architecture in Cloud Security. En *Convergence of Cybersecurity and Cloud Computing* (pp. 515-530). IGI Global. https://www.researchgate.net/profile/Basi-Reddy-Avula/publication/387897412_Zero_Trust_Architecture_in_Cloud_Security/links/699d233542f94d1212ae271f/Zero-Trust-Architecture-in-Cloud-Security.pdf

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Upadhyaya, S. K., & Vivek, S. (2022, August). Revisiting a Privacy-Preserving Location-based Service Protocol using Edge Computing. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-5). https://doi.org/10.1145/3538969.3544432

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, 79(3), 849-861. https://doi.org/10.1016/j.future.2017.09.020

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*, 25(1), 213. https://doi.org/10.3390/s25010213

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006