Ingeniería Investiga

Vol. 8, e1331, año 2026
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v8i00.1331

Artículo de revisión

Implementación de Arquitecturas Zero Trust: Revisión sistemática de beneficios y desventajas

Implementing Zero Trust Architectures: A Systematic Review of Benefits and Drawbacks

Alex Fidel Gil Villa[1]* | Sebastián Alberto Espinoza Dávalos[2] | Alberto Carlos Mendoza de los Santos[3]

Afiliación:

[1,2,3]Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La libertad, Perú

Autor de correspondencia: E-mail: *agilvi@unitru.edu.pe

Información del artículo:

Recibido: 05/08/2025
Aceptado: 29/09/2025
Publicado: 21/11/2025

Resumen

Ante la evolución constante de las amenazas digitales y las limitaciones inherentes a los enfoques tradicionales de seguridad, las arquitecturas Zero Trust (ZTA) se han desarrollado como una alternativa orientada a fortalecer la protección de los entornos digitales mediante principios de verificación continua y control de acceso contextual. Este estudio sintetiza y analiza sistemáticamente los beneficios cuantificables, limitaciones técnicas, desafíos organizacionales, soluciones propuestas y métricas de evaluación asociadas con la implementación de ZTA, considerando factores técnicos, culturales y estructurales que influyen en su adopción. A través de una revisión sistemática realizada en bases académicas especializadas, se analizaron veinte artículos seleccionados tras un proceso riguroso de filtrado. Los resultados evidencian mejoras significativas en la postura de seguridad y una reducción del riesgo de ataques, impulsadas por la microsegmentación y la autenticación continua; no obstante, se identificaron limitaciones relacionadas con la capacitación insuficiente, la complejidad operativa en entornos multicloud y la resistencia organizacional al cambio. Se concluye que la efectividad de la ZTA depende de su integración estratégica con marcos estandarizados y de una adecuada gestión del cambio dentro de las organizaciones.

Palabras clave: Arquitectura Zero Trust; ciberseguridad; seguridad de la información.

Abstract

Given the constant evolution of digital threats and the inherent limitations of traditional security approaches, Zero Trust Architectures (ZTA) have been developed as an alternative aimed at strengthening the protection of digital environments through continuous verification and contextual access control. This study systematically synthesizes and analyzes the quantifiable benefits, technical limitations, organizational challenges, proposed solutions, and evaluation metrics associated with the implementation of ZTA, considering the technical, cultural, and structural factors that influence its adoption. Through a systematic review conducted in specialized academic databases, twenty articles were analyzed following a rigorous filtering process. The results reveal significant improvements in security posture and a reduction in attack risk, driven by microsegmentation and continuous authentication; however, limitations were identified related to insufficient training, operational complexity in multicloud environments, and organizational resistance to change. It is concluded that the effectiveness of ZTA depends on its strategic integration with standardized frameworks and adequate change management within organizations.

Keywords: Zero Trust Architecture; cybersecurity; information security.

1. Introducción

La evolución del panorama de amenazas cibernéticas modificó significativamente los enfoques de seguridad adoptados por las organizaciones. En 2023, las brechas de seguridad generaron pérdidas promedio de 4,45 millones de dólares por incidente, con un incremento anual del 15 % en los ataques que superaron las defensas perimetrales tradicionales. En este contexto, las Arquitecturas Zero Trust (ZTA) representan una estrategia de seguridad que supera las limitaciones de los modelos basados en perímetro mediante la aplicación del principio "nunca confiar, siempre verificar", con el propósito de establecer entornos digitales más resilientes y adaptables (Verma et al., 2024; Syed et al., 2022).

La literatura reciente indica que la adopción de ZTA implica un cambio estructural en la gestión de la confianza dentro de los entornos digitales, al sustituir los perímetros de seguridad fijos por un modelo de verificación continua de identidades, dispositivos y flujos de información. Los resultados comparativos de dieciséis investigaciones muestran una reducción promedio del 78,3 % en la superficie de ataque y un mejor rendimiento en la detección de amenazas persistentes avanzadas (Khurshid et al., 2025; Ahmed et al., 2025). La aplicación de marcos de referencia como el NIST SP 800-207 permite alinear los principios del modelo Zero Trust con los objetivos de seguridad organizacional, promoviendo implementaciones sostenibles y escalables. Dado que las redes corporativas operan en entornos con alto nivel de riesgo, el control de acceso basado en atributos constituye un componente fundamental para mantener la integridad de los sistemas y restringir el acceso según criterios contextuales (He, 2022). Además de ello, la inteligencia artificial (IA) cumple un papel determinante en la implementación de la ZTA, especialmente cuando se integra con el análisis de comportamiento y con tecnologías emergentes orientadas a la seguridad. Esta integración potencia la entrega de servicios de protección adaptables y eficientes, permitiendo analizar e interpretar patrones de actividad de los usuarios para detectar accesos inusuales y aplicar políticas de seguridad dinámicas (Joshi, 2025). Las soluciones basadas en IA optimizan las operaciones internas y fortalecen la seguridad mediante monitoreo continuo en tiempo real, lo que mejora la detección temprana y la respuesta rápida ante amenazas potenciales. Las técnicas de aprendizaje automático (machine learning) han incrementado la precisión en la evaluación de confianza y la orquestación de los componentes del modelo ZTA (Cao et al., 2024).

La aplicación práctica de estas tecnologías ha mostrado mayor efectividad organizacional al implementar principios Zero Trust. En implementaciones que integran sistemas de gestión de identidades basados en IA, se ha logrado una verificación más precisa de usuarios y dispositivos, fortaleciendo los mecanismos de autenticación (Federici et al., 2022). Además, investigaciones de Ferretti et al. (2021) y DeCusatis et al. (2016) destacan la inclusión del análisis del recorrido de amenazas (threat path analysis) como elemento clave en la arquitectura Zero Trust, ya que combina tecnologías, datos y procesos para establecer defensas adaptadas a la evolución del panorama de amenazas digitales. Por lo descrito, el propósito del estudio fue sintetizar y analizar de forma sistemática los beneficios medibles, limitaciones técnicas, desafíos organizacionales y soluciones documentadas en la implementación de arquitecturas Zero Trust (ZTA), junto con las métricas de evaluación reportadas entre 2020 y 2025. Además, se realizó una evaluación crítica del impacto de ZTA en la transición del modelo tradicional de seguridad.

2. Metodología

La revisión se desarrolló bajo los lineamientos de la metodología PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) propuesta por Page et al. (2021), la cual establece una estructura estandarizada para la búsqueda, selección y análisis de literatura científica. Su aplicación garantizó transparencia, reproducibilidad y rigor metodológico, permitiendo recopilar evidencia reciente y relevante sobre la implementación de Arquitecturas Zero Trust (ZTA).

2.1. Estrategia de búsqueda

La recolección de información se realizó entre julio y agosto de 2025, utilizando las bases de datos IEEE Xplore, ACM Digital Library, DOAJ, ArXiv y ScienceDirect. Las palabras clave se definieron según su relación con el tema y se combinaron mediante operadores booleanos para optimizar la precisión y cobertura de la búsqueda. La Tabla 1 presenta las bases de datos consultadas, los términos utilizados, y el número de documentos obtenidos y seleccionados para el análisis posterior.

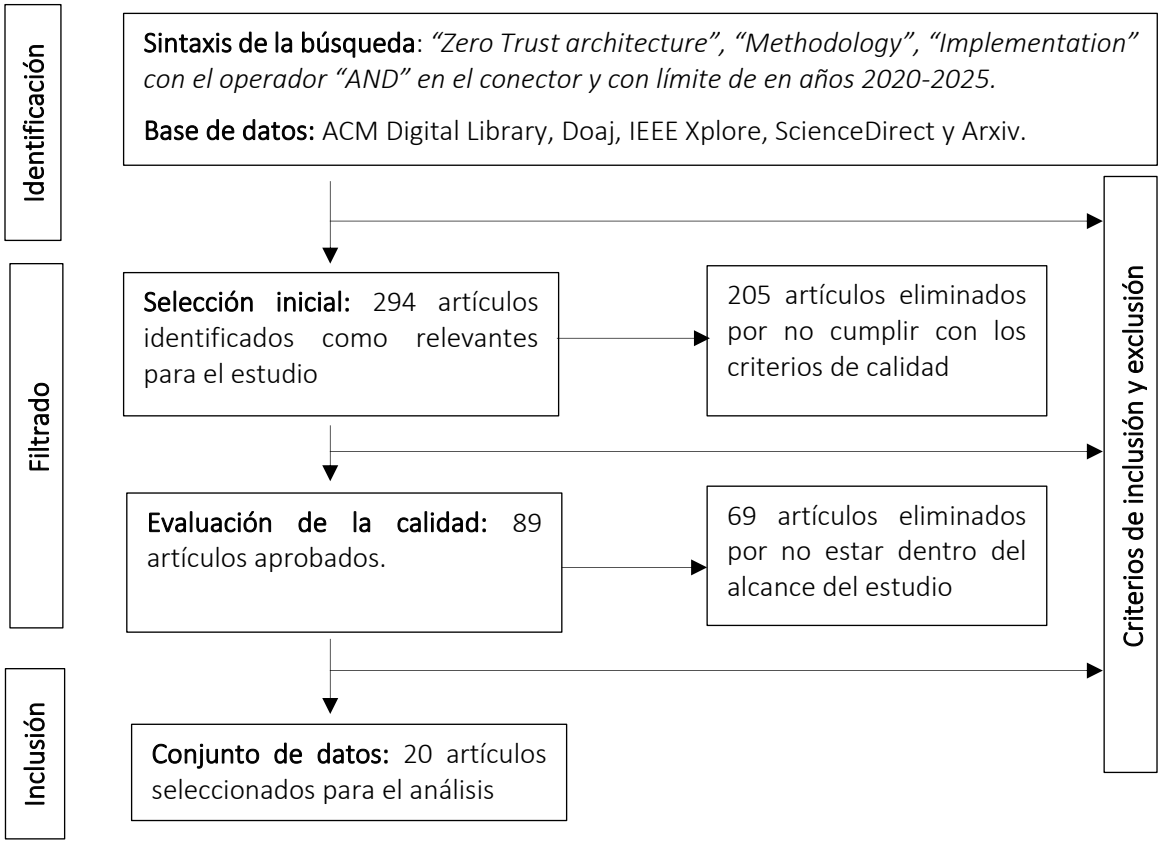
Tabla 1

Términos de búsqueda en base de datos académicos

Base de datos	Términos de búsqueda	Resultados	Seleccionados
ACM Digital Library	[All: "zero trust architecture"] AND [All: "methodology"] AND [All: "implementation"] AND [E-Publication Date: (01/01/2021 TO 12/31/2025)]	47	2
DOAJ	"Zero Trust architecture" AND "Methodology" OR "Implementation"	29	1
IEEE Xplore	("All Metadata": Architecture) AND ("All Metadata": Zero Trust) AND ("All Metadata": Implementation)	18	6
ScienceDirect	"Zero Trust architecture" AND "Methodology" AND "Implementation"	82	8
ArXiv	"Zero trust architecture"	49	3

Figura 1

Diagrama PRISMA para el proceso de recolección de datos



2.2. Criterios de inclusión y exclusión

Para asegurar la calidad, la coherencia temática y la validez científica de las fuentes, se establecieron criterios de inclusión y exclusión. Se incluyeron únicamente publicaciones comprendidas entre los años 2020 y 2025, con el fin de garantizar la actualidad del conocimiento y reflejar los avances más recientes en la materia. Asimismo, se consideraron los documentos disponibles en texto completo, redactados en español o inglés, y accesibles en línea a través de las bases de datos académicas seleccionadas. Por otro lado, se excluyeron los documentos que no guardaran una relación directa con la arquitectura Zero Trust o con aspectos específicos de la seguridad de la información, así como aquellos que presentaran duplicación de contenido o carecieran de respaldo académico verificable. También se descartaron los ensayos de opinión, notas breves, artículos sin revisión por pares y los trabajos pertenecientes a áreas ajenas al ámbito informático, como medicina, por no ajustarse a los objetivos de la investigación. Finalmente, la evaluación de calidad de las fuentes seleccionadas se basó en criterios como la relevancia temática, la claridad metodológica, la solidez teórica y el uso de referencias confiables y actualizadas. Además, se priorizó la accesibilidad de los estudios y su publicación en fuentes académicas reconocidas

2.3. Proceso de recolección de la información

El proceso de selección siguió el diagrama de flujo PRISMA, ilustrado en la Figura 1, que describe las fases de identificación, cribado, elegibilidad e inclusión de los documentos analizados. Este procedimiento permitió garantizar la pertinencia y consistencia de los estudios incorporados en la revisión.

3. Resultados

Tras la revisión sistemática de los estudios académicos en distintos entornos organizacionales, se identificaron múltiples perspectivas, enfoques tecnológicos y experiencias de despliegue. En la tabla 2, se presenta una síntesis de los principales beneficios reportados en términos de mejora de la postura de seguridad, así como las desventajas y limitaciones identificadas durante los procesos de implementación y operación de estas arquitecturas. Además de los hallazgos descritos, se elaboró una síntesis comparativa que permite identificar los principales beneficios, limitaciones y desafíos asociados con la implementación práctica de las arquitecturas Zero Trust en distintos niveles operativos. En la Tabla 3 se presentan los resultados estructurados por categorías: seguridad, operacional, organizacional y técnica, destacando tanto los avances alcanzados como las restricciones más recurrentes reportadas en la literatura reciente. De forma complementaria, la Tabla 4 reúne las métricas de evaluación empleadas para cuantificar el desempeño de la ZTA, clasificadas en tres categorías: seguridad, rendimiento y adopción. Estas métricas proporcionan un marco cuantitativo que permite estimar la efectividad de los algoritmos, los tiempos de respuesta, la reducción de falsos positivos y la eficiencia general de los sistemas bajo entornos de validación real y simulada.

Tabla 2

Análisis de los documentos seleccionados

N°	Autores y año	Limitaciones técnicas/ Desafíos organizacionales	Beneficios cuantificables y propuestas en Arquitectura Zero Trust ZTA
1	Syed et al. (2022)	La autenticación multi-factor requiere dispositivos secundarios y la micro-segmentación enfrenta restricciones en aplicaciones monolíticas no virtualizadas.	**Beneficios ZTA:** Autenticación persistente sin dispositivos adicionales, controles flexibles y evaluación de confianza implementada de manera automática. **Soluciones:** Marco completo que incorpora inteligencia de amenazas y información contextual. Suprime dependencias de hardware externo y brinda seguridad específica para infraestructuras esenciales.

Tabla 2 (Continuación/1)

N°	Autores y año	Limitaciones técnicas/ Desafíos organizacionales	Beneficios cuantificables y propuestas en Arquitectura Zero Trust ZTA
2	Khurshid et al. (2025)	Los sistemas AIoT de vigilancia convencionales muestran fallas críticas ante ataques adversarios dirigidos a modelos de machine learning, además de enfrentar limitaciones en su capacidad de expansión.	**Beneficios ZTA:** Entender de manera uniforme los principios de Zero Trust favorece una mejor conservación del conocimiento adquirido y permite una ejecución más efectiva en su aplicación práctica. **Soluciones:** Se plantea la implementación de una arquitectura de seguridad principalmente basada en autenticación constante y análisis de comportamiento mediante IA. Esta solución integra también criptografía resistente a la computación cuántica, mecanismos de privacidad diferencial y adaptabilidad dinámica para lograr sistemas de vigilancia más seguros y resistentes.
3	Katsis et al. (2022)	Los sistemas de red tradicionales poseen limitaciones ante ataques, además de presentar capacidades de mejora en su cuanto a su capacidad de expansión.	**Beneficios ZTA:** Implementación de defensas integrales que cubren tanto usuarios como recursos mediante microsegmentación. **Soluciones:** Se presenta NEUTRON, un framework que proporciona un pipeline automatizado que sirve para la especificación, gestión, pruebas y despliegue de políticas. Este, utiliza un enfoque basado en grafos para especificar políticas de seguridad de red complejas, además que trabaja en conjunto con la herramienta SPRT para verificación y análisis de impacto de cambios en políticas relacionadas a ZTA.
4	Peepliwal et al. (2025)	La integridad de los datos clínicos se ve comprometida por las limitaciones de los métodos tradicionales usados en ensayos clínicos.	**Beneficios ZTA:** ZTA verifica continuamente los datos y prioriza validar cada transacción antes de su ejecución. **Soluciones:** Utiliza el protocolo T-PBFT con EigenTrust, contratos inteligentes con control ABAC y almacenamiento distribuido IPFS con hashes en blockchain.
5	Zanasi et al. (2024)	La seguridad en infraestructuras industriales IoT es vulnerable por las limitaciones de los métodos tradicionales basados en confianza implícita.	**Beneficios ZTA:** ZTA permite microsegmentación con control detallado, gestión centralizada y validación de cada interacción entre recursos. **Soluciones:** Aplica SDN con microsegmentación automática, autenticación mutua mediante certificados digitales y el sistema NEST para gestión distribuida de certificados.
6	Zyoud y Lebai (2024)	Resistencia cultural organizacional hacia adopción de Zero Trust por falta de comprensión sobre beneficios de ZTA.	**Beneficios ZTA:** Disminución de resistencia cultural y mayor aceptación organizacional al comprender los beneficios de seguridad. **Soluciones:** Modelo de adopción culturalmente adaptado con estrategias de capacitación específicas. Promueve transformación cultural y asegura sostenibilidad de implementación ZTA.

Tabla 2 (Continuación/2)

N°	Autores y año	Limitaciones técnicas/ Desafíos organizacionales	Beneficios cuantificables y propuestas en Arquitectura Zero Trust ZTA
7	Joshi (2025)	Complejidad avanzada para verificación continua en entornos híbridos multi-nube con desafíos como la privacidad y el sesgo algorítmico.	**Beneficios ZTA:** Madurez tecnológica avanzada mediante automatización de políticas y benchmarking estandarizado. **Soluciones:** Zero Trust as CoAhmadde con IA, blockchain y edge computing. Optimiza precisión de evaluación de confianza, disminuye complejidad operacional y ofrece métricas objetivas de efectividad.
8	Ahmad et al. (2025)	Los algoritmos de gestión de confianza tradicionales en IoT 6G enfrentan limitaciones por dependencias centralizadas, falta de mecanismos adaptativos y vulnerabilidades ante ataques Sybil, replay y on-off.	**Beneficios ZTA:** Gestión de confianza descentralizada con verificación continua, evaluación comportamental en tiempo real y eliminación de autoridades centralizadas. **Soluciones:** Arquitectura AZTM con blockchain sin consenso, intercambio de claves ECDH y puntuación de confianza adaptativa. Mitiga ataques Sybil mediante cooldown timers y garantiza comunicación segura en entornos 6G IoT con baja latencia y eficiencia energética.
9	Wan et al. (2025)	Los métodos de seguridad actuales presentan limitaciones que exponen la protección de los datos industriales a vulnerabilidades.	**Beneficios ZTA:** ZTA valida identidades de forma continua, reduce la superficie de ataque y prioriza la verificación de identidad como paso inicial. **Soluciones:** Implementa autenticación continua mediante PUF y un protocolo multifactorial con generación de claves.
10	Ramachandran et al. (2024)	La ciberresiliencia en sistemas ICS/OT se ve afectada por las limitaciones de las defensas centralizadas tradicionales.	**Beneficios ZTA:** ZTA aplica microsegmentación con modo isla, detección distribuida en tiempo real y verificación continua de forma descentralizada. **Soluciones:** Incluye el algoritmo FTAS con IDS industrial distribuido, segmentación IT/OT mediante firewalls avanzados y procedimientos EOP automatizados.
11	Yeoh et al. (2023)	La seguridad organizacional es vulnerable por las limitaciones de los enfoques tradicionales basados en perímetros.	**Beneficios ZTA:** ZTA elimina la confianza implícita con verificación continua, aplica control adaptativo y valida tanto identidades como dispositivos. **Soluciones:** Propone un framework de 8 dimensiones con 43 factores críticos, un modelo de madurez de 6 niveles y procesos de seguridad automatizados y orquestados.
12	Hasan et al. (2024)	Los sistemas ciberfísicos presentan vulnerabilidades por el uso de métodos de diseño tradicionales que no integran la seguridad desde el inicio.	**Beneficios ZTA:** ZTA incorpora patrones de diseño con seguridad embebida, validación continua desde la etapa de diseño y verificación de componentes por separado. **Soluciones:** Aplica patrones Zero Trust con el framework Resolute-AADL, mecanismos PEP con separación del núcleo y carga de datos segura con verificación en tiempo de ejecución.

Tabla 2 (Continuación/3)

N°	Autores y año	Limitaciones técnicas/ Desafíos organizacionales	Beneficios cuantificables y propuestas en Arquitectura Zero Trust ZTA
13	Sasada et al. (2023)	Los programas de entrenamiento en ciberseguridad existentes fallan en proporcionar habilidades necesarias para la arquitectura de sistemas, como diseño y escalabilidad del sistema.	**Beneficios ZTA:** Permite adquirir habilidades esenciales para arquitectos de sistemas independientemente del nivel de experiencia en seguridad. **Soluciones:** Programa de entrenamiento CYTØRUS basado en Zero Trust Architecture que incluye conferencias introductorias, entrenamiento práctico y sesiones de discusión. Utiliza modelo ARCS para medir motivación y efectividad educativa en participantes estudiantes y profesionales.
14	Ahmadi (2025)	La detección y contención de amenazas cibernéticas es débil debido a las limitaciones de las políticas de acceso estáticas tradicionales.	**Beneficios ZTA:** ZTA aplica análisis de comportamiento continuo con puntuación de riesgo en tiempo real, segmenta identidades comprometidas de forma autónoma y se adapta dinámicamente a nuevas amenazas. **Soluciones:** Emplea modelos de *machine learning* para ajustar permisos según contexto, segmentación automatizada con grafos y análisis de comportamiento con evaluación de anomalías y factores contextuales.
15	Al-Zewairi et al. (2025)	Los sistemas tradicionales de detección de intrusiones tienen consigo ciertas limitaciones de gran magnitud en cuanto al reconocimiento de ataques de malware desconocidos en redes IoT, dando consecuencias como la generación de altas tasas de falsos positivos.	**Beneficios ZTA:** Este modelo brinda un sistema de múltiples etapas que aumenta la efectividad en la detección de ataques desconocidos, gracias a esto disminuye notablemente los falsos positivos y se adapta tanto a redes IoT como tradicionales. **Soluciones:** Incorporar el modelo de arquitectura ZTA con algoritmos híbridos de aprendizaje automático, como también de clustering DBSCAN optimizado y evaluación sobre datasets como CIC-IDS-2017, Bot-IoT e IoT-23, gracias esto alcanza una alta precisión en la identificación de amenazas.
16	Verma et al. (2024)	Tras las amenazas constantes y evolucionadas atraviesan defensas perimetrales convencionales como VPNs y firewalls exponiendo datos de suma importancia en la empresa.	**Beneficios ZTA:** Gracias a esto presenta una limitación eficaz de amenazas persistentes avanzadas (APTs), mayor visibilidad frente a actividades maliciosas y respuesta más eficiente ante incidentes de seguridad. **Soluciones:** La incorporación del principal principio de esta arquitectura que es “jamás confiar, siempre verificar”, mediante la autenticación continua y controles de acceso. Gracias a esto disminuye los intervalos de tiempo de detección y nos brinda una protección adaptable.

Tabla 2 (Continuación/4)

N°	Autores y año	Limitaciones técnicas/ Desafíos organizacionales	Beneficios cuantificables y propuestas en Arquitectura Zero Trust ZTA
17	Polinati (2025)	La seguridad en nubes híbridas es vulnerable por las limitaciones de las políticas tradicionales fragmentadas.	**Beneficios ZTA:** ZTA aplica verificación continua sin confianza inherente, unifica políticas de seguridad en entornos multinube y valida cada acceso por separado. **Soluciones:** Incluye arquitectura Zero Trust con IAM centralizado, cifrado AES con MFA y gestión automatizada de políticas con monitoreo activo de amenazas.
18	Nasiruzzaman et al. (2025)	Los modelos perimetrales tradicionales en ciberseguridad son vulnerables por la confianza implícita, el movimiento lateral y una superficie de ataque extendida.	**Beneficios ZTA:** ZTA aplica verificación constante, microsegmentación adaptable y políticas de mínimo privilegio enfocadas en los datos. **Soluciones:** Implementa una arquitectura sin perímetro basada en el principio "nunca confiar, siempre verificar", con controles dinámicos y respuesta automatizada.
19	Ahmed et al. (2025)	La ciberseguridad en redes 7G es vulnerable por las limitaciones de los métodos clásicos de detección estática.	**Beneficios ZTA:** ZTA incorpora detección cuántica de anomalías en tiempo real, microsegmentación dinámica y verificación continua mejorada con tecnología cuántica. **Soluciones:** Utiliza redes neuronales cuánticas (QNN) con arquitectura híbrida clásico-cuántica, puntuación de anomalías mediante superposición y entrelazamiento, y microsegmentación cuántica con optimización variacional.
20	Ali et al. (2024)	La seguridad en entornos MEC se ve comprometida por las limitaciones de los métodos tradicionales de autenticación.	**Beneficios ZTA:** ZTA utiliza autenticación basada en confianza con validación constante, lógica difusa para evaluación y prioriza la verificación de dispositivos. **Soluciones**: Emplea una metodología difusa dual con blockchain, autenticación multifactor con PUF y biometría, y el algoritmo SARSA para descarga de tareas.

Tabla 3

Comparación de Beneficios vs Desventajas de ZTA

Aspectos	Beneficios	Limitaciones y desafíos
Seguridad	- Autenticación continua - Control acceso adaptativo - Escalabilidad mejorada	- Vulnerabilidad plana de control - Complejidad en entornos híbridos
Operacional	- Automatización de políticas - Microsegmentación granular - Visibilidad mejorada	- Sobrecarga de rendimiento - Latencia incrementada (100ms-4s)
Organizacional	- Mejor postura de seguridad - Cumplimiento regulatorio - Integración con IA/ML	- Resistencia cultural - Falta de capacitación - Costos de implementación
Técnico	- Autenticación continua - Control acceso adaptativo - Escalabilidad mejorada	- Dependencia dispositivos MFA - Limitadas aplicaciones monolíticas - Complejidad algoritmos

Tabla 4

Métricas de Evaluación ZTA por Categoría

Categorías	Métricas clave	Rango/Valor (%)	Fuente
Seguridad	Precisión en detección	85-98 %	Verma et al. (2024)
	Accuracy algoritmos ZT	85 %	
	F1-Score evaluación	85 %	
	AUC (Area Under ROC)	92 %	
	Tasa falsos positivos	10 %	
	Tasa falsos negativos	18 %	
Rendimiento	Tiempo entrenamiento	120 s	
	Tiempo inferencia	10 ms	
	Respuesta tiempo real	<50 ms	Joshi (2025)
	Reducción latencia	-57,1 %	
Adopción	Mejora tasa detección	+4,7 %	
	Reducción falsos positivos	-39,4 %	
	Reducción superficie ataque	78,3 %	
	Tiempo implementación	2-5 años	Zyoud y Lebai (2024)

4. Discusión

La adopción de Arquitecturas Zero Trust (ZTA) aporta beneficios en seguridad y eficiencia operativa, aunque enfrenta limitaciones técnicas y organizacionales. Estos resultados confirman patrones observados en la literatura reciente, pero también evidencian vacíos que requieren nuevas líneas de investigación.

4.1. Beneficios identificados

En primer lugar, fortalece la protección de la información sensible mediante la aplicación estricta del principio "nunca confíes, siempre verifica". Este enfoque incrementa la detección de amenazas y mejora la capacidad de respuesta ante incidentes, según lo demuestran Verma et al. (2024) y Syed et al. (2022). Asimismo, Al-Zewairi et al. (2025) confirman que la verificación continua de identidades y los sistemas de detección en múltiples etapas permiten identificar ataques desconocidos tanto en redes tradicionales como en entornos IoT. De forma complementaria, Khurshid et al. (2025) señalan que esta arquitectura ofrece una defensa sólida frente a ataques basados en inteligencia artificial, posibilitando además la recuperación automática frente a intrusiones en sistemas AIoT. Por otro lado, la ZTA evidencia una destacada capacidad de integración tecnológica. Joshi (2025) indica que el modelo presenta un alto grado de madurez al incorporar inteligencia artificial, blockchain, computación cuántica y *edge computing*, lo que permite automatizar políticas de seguridad y estandarizar la evaluación de confianza. En la misma línea, Ahmed et al. (2025) muestran que la ZTA posibilita la detección de anomalías en tiempo real y la microsegmentación adaptativa en redes 7G, confirmando su adaptabilidad frente a tecnologías emergentes. De igual modo, Al-Zewairi et al. (2025) reportan la eficacia de algoritmos híbridos de *machine learning* y *clustering* optimizado para la evaluación de amenazas desconocidas. Finalmente, en el ámbito industrial, Zanasi et al. (2024) evidencian la efectividad de la microsegmentación automatizada y la autenticación mutua mediante certificados digitales, lo que refuerza la seguridad perimetral y reduce la superficie de ataque. En conjunto, estos resultados confirman que la ZTA constituye una herramienta estratégica para fortalecer los sistemas de ciberseguridad organizacional (Figura 2).

4.2. Patrones de implementación exitosa

En relación con los mecanismos de adopción, la implementación de la ZTA requiere un proceso gradual basado en la adaptación tecnológica y organizacional. Para ello, se recomienda establecer un plan estructurado que contemple la definición de impulsores y casos de uso, el desarrollo de políticas, el diseño arquitectónico, la evaluación del nivel de preparación

tecnológica, la ejecución de proyectos piloto, la capacitación del personal y un despliegue progresivo por fases. Esta secuencia favorece la coherencia operativa y minimiza los riesgos durante la adopción del modelo.

Además, la integración con marcos estandarizados como el NIST SP 800-207, fortalece la alineación entre el principio central de la ZTA ("nunca confiar, siempre verificar") y los objetivos estratégicos institucionales. Este enfoque, según Ahmad et al. (2025), mejora la gobernanza de la seguridad y amplía la capacidad de respuesta ante amenazas. En paralelo, modelos complementarios como CISA ZTM, Forrester ZTX y Gartner CARTA aportan esquemas de madurez, evaluación continua del riesgo y ecosistemas extendidos que favorecen la implementación tanto en el sector público como en el privado. La relación entre los principales marcos de referencia y su aplicabilidad en distintos sectores se detalla en la Tabla 5.

De manera complementaria, Ahmad et al. (2025) destacan que el uso de blockchain sin consenso y la gestión de confianza descentralizada aumentan la eficacia de la autenticación continua y reducen la complejidad operativa en entornos 6G IoT. En este contexto, la Figura 3 muestra la variación en los tiempos de integración de los principales componentes técnicos, reflejando la necesidad de planificación escalonada.

4.3. Limitaciones y desafíos identificados

A pesar de los avances observados, la implementación de Zero Trust enfrenta desafíos considerables relacionados con la complejidad operativa, la sobrecarga de rendimiento y la resistencia organizacional. Mantener la verificación continua en entornos híbridos y multicloud demanda una alta capacidad técnica, además de generar problemas asociados a la privacidad y sesgos algorítmicos (Joshi, 2025). Adicionalmente, Zanasi et al. (2024) documentan aumentos de latencia de hasta 100 ms durante los procesos de re-enrollment y retrasos de varios segundos en clientes Windows, lo que evidencia un impacto directo en el rendimiento operativo. De igual modo, la exposición del plano de control constituye una vulnerabilidad crítica. Este componente, encargado de la gestión de políticas y decisiones de seguridad, representa un punto único de fallo que, si es comprometido, puede otorgar acceso a recursos esenciales o interrumpir funciones clave. Por tanto, se recomienda reforzar la superficie de ataque mediante la incorporación de redundancias y la ejecución sistemática de pruebas de failover.

Figura 2

Indicadores cuantitativos consolidados de efectividad ZTA

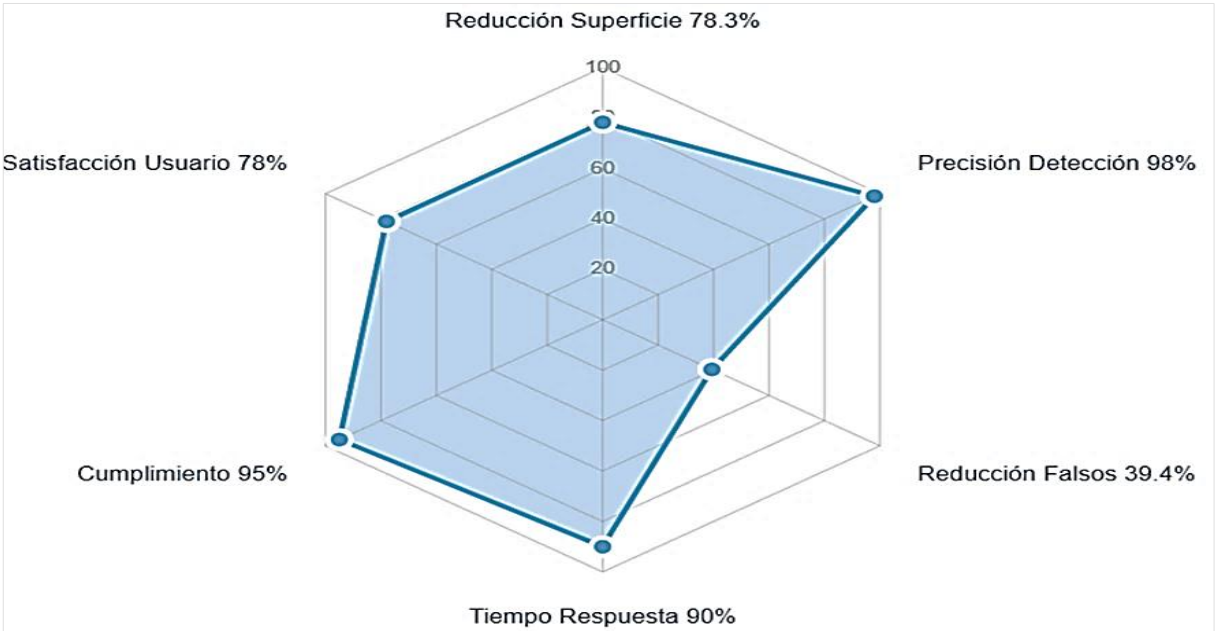


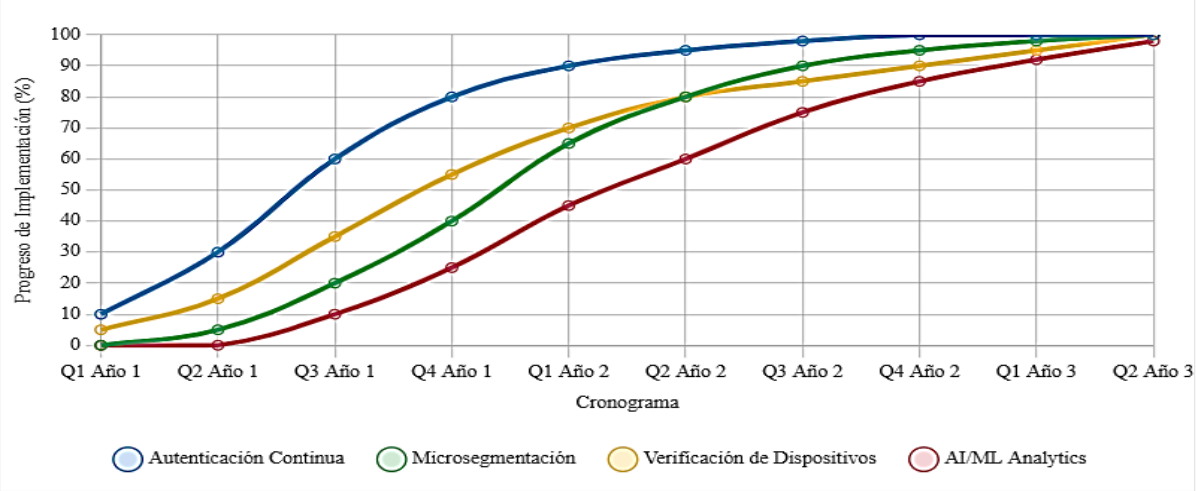
Tabla 5

Comparación de beneficios vs desventajas de ZTA

Marco/Estándar	Organización	Características	Aplicabilidad
NIST SP 800-207	NIST	Principios fundamentales ZTA	Universal
CISA ZTM	CISA	Modelo de madurez 5 niveles	Sector público US
Forrester ZTX	Forrester	Ecosistema extendido	Empresarial
Gartner CARTA	Gartner	Evaluación continua riesgo	Grandes empresas

Figura 3

Progreso de adopción por componentes técnicos principales



Por otra parte, Zyoud y Lebai (2024) resaltan la resistencia cultural como una de las principales barreras para la adopción efectiva del modelo. La falta de comprensión sobre los fundamentos de la ZTA y el desconocimiento de sus beneficios dificultan la aceptación entre los empleados. En el contexto de los Emiratos Árabes Unidos, la cultura organizacional y nacional influye decisivamente en los niveles de adopción, demostrando que los valores culturales y la madurez en seguridad son determinantes para su éxito. Finalmente, Syed et al. (2022) señalan que la autenticación multifactor continúa dependiendo de mecanismos secundarios y que la microsegmentación enfrenta restricciones en entornos no virtualizados. Asimismo, Al-Zewairi et al. (2025) identifican que los sistemas tradicionales de detección presentan altas tasas de falsos positivos frente a malware desconocido, lo que exige el desarrollo de mecanismos de análisis multi-etapa más precisos y resilientes.

4.4. Tendencias y direcciones futuras

En términos de proyección tecnológica, se consolida una tendencia hacia la convergencia de la arquitectura Zero Trust con la inteligencia artificial y el machine learning. Esta integración permite mejorar la detección de amenazas, automatizar la gestión de políticas y optimizar la administración de sistemas en tiempo real, promoviendo una toma de decisiones más inteligente y adaptativa. Asimismo, Ahmed et al. (2025) y Joshi (2025) evidencian avances en el desarrollo de arquitecturas preparadas para la era post-cuántica, fundamentadas en soluciones criptográficas resistentes a la computación cuántica. Estas aproximaciones buscan garantizar la sostenibilidad y resiliencia de los sistemas de seguridad frente a amenazas futuras derivadas del poder de procesamiento cuántico. Por último, la expansión del modelo hacia ecosistemas industriales, sistemas ciberfísicos y entornos de edge computing demuestra su versatilidad y aplicabilidad en contextos críticos. La evidencia respalda su eficacia en el Internet de las Cosas industrial, consolidando a la ZTA como una estrategia adaptable, escalable y de largo

alcance dentro de la gestión moderna de la ciberseguridad.

5. Conclusiones

La evidencia analizada demuestra que la adopción de la arquitectura Zero Trust (ZTA) mejora de manera significativa la seguridad organizacional al reemplazar los enfoques perimetrales tradicionales por un modelo de verificación continua y control dinámico. Este paradigma permite una gestión más precisa de accesos e identidades, fortaleciendo la capacidad de respuesta ante amenazas persistentes avanzadas y reduciendo la superficie de ataque.

La integración de tecnologías emergentes, como la inteligencia artificial, el análisis de comportamiento y la gestión automatizada de identidades, optimiza los mecanismos de detección y mitigación de incidentes. Estos avances validan la eficacia del principio central de la arquitectura Zero Trust, basado en la verificación constante y la confianza mínima.

Asimismo, se identifica que la falta de alineación entre la infraestructura tecnológica y los principios de Zero Trust constituye una de las principales causas de fallos en su implementación. En contraste, las organizaciones que adoptan estrategias graduales sustentadas en marcos estandarizados, como el NIST SP 800-207, alcanzan niveles superiores de madurez, coherencia operativa y resiliencia cibernética.

Contribución de los autores

A. F. Gil: Conceptualización, investigación, metodología, administración del proyecto, recursos, visualización y redacción del borrador original **S. A. Espinoza:** Conceptualización, investigación, metodología, administración del proyecto, recursos y redacción del borrador original **A. C. Mendoza:** Supervisión, validación, redacción, revisión y edición.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés relacionado con esta publicación.

6. Referencias bibliográficas

Ahmad, I., Gimhana, S., Ahmad, I., y Harjula, E. (2025). Adaptive Trust Architecture for Secure IoT Communication in 6G. *IEEE Networking Letters*, *7*(2), 113–116. https://doi.org/10.1109/lnet.2025.3566909

Ahmadi, S. (2025). Autonomous identity-based threat segmentation for zero trust architecture. *Cyber Security and Applications*, *100106*, 100106. https://doi.org/10.1016/j.csa.2025.100106

Ahmed, S., Shihab, I. F., y Khokhar, A. (2025). Quantum-driven zero trust architecture with dynamic anomaly detection in 7G technology: A neural network approach. *Measurement: Digitalization*, *2–3*(100005), 100005. https://doi.org/10.1016/j.meadig.2025.100005

Ali, B., Gregory, M. A., Li, S., y Dib, O. A. (2024). Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in Multi-access Edge Computing. *Computer Networks*, *241*(110197), 110197. https://doi.org/10.1016/j.comnet.2024.110197

Al-Zewairi, M., Almajali, S., Ayyash, M., Rahouti, M., Martinez, F., y Quadar, N. (2025). Multi-stage enhanced zero trust intrusion detection system for unknown attack detection in Internet of Things and traditional networks. *ACM Transactions on Privacy and Security*, *28*(3), 1–28. https://doi.org/10.1145/3725216

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., y Li, G. (2024). Automation and orchestration of Zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, *21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2

DeCusatis, C., Liengtiraphan, P., Sager, A., y Pinelli, M. (2016, 18 al 20 de noviembre). Implementing zero trust cloud networks with transport access control and first

packet authentication [conferencias]. *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, Estados Unidos. https://doi.org/10.1109/SmartCloud.2016.22

Federici, F., Martintoni, D., y Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics*, *12*(3), 566. https://doi.org/10.3390/electronics12030566

Ferretti, L., Magnanini, F., Andreolini, M., y Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security*, *110*(102419), 102419. https://doi.org/10.1016/j.cose.2021.102419

Hasan, S., Amundson, I., y Hardin, D. (2024). Zero-trust design and assurance patterns for cyber–physical systems. *Journal of Systems Architecture*, *155*(103261), 103261. https://doi.org/10.1016/j.sysarc.2024.103261

He, Y., Huang, D., Chen, L., Ni, Y., y Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), 1–13. https://doi.org/10.1155/2022/6476274

Joshi, H. (2025). Emerging technologies driving zero trust maturity across industries. *IEEE Open Journal of the Computer Society*, *6*, 25–36. https://doi.org/10.1109/ojcs.2024.3505056

Katsis, C., Cicala, F., Thomsen, D., Ringo, N., y Bertino, E. (2022, 24 al 27 de abril). Neutron: A graph-based pipeline for zero-trust network architectures [conferencia]. *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy*. Baltimore, Estados Unidos. https://doi.org/10.1145/3508398.3511499

Khurshid, K., Usman Hadi, M., Al Bataineh, M., y Saeed, N. (2025). Securing AIoT Surveillance: Techniques, Challenges, and Solutions. *IEEE Open Journal of the Communications Society*, *6*, 6517–6550. https://doi.org/10.1109/ojcoms.2025.3593311

Nasiruzzaman, Ali, M., Salam, I., y Miraz, M. H. (2025). The evolution of zero Trust Architecture (ZTA) from concept to implementation. En *arXiv [cs.CR]*. https://doi.org/10.48550/ARXIV.2504.11984

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., … (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista española de cardiología*, *74*(9), 790–799. https://doi.org/10.1016/j.recesp.2021.06.016

Peepliwal, A. K., Pandey, H. M., Prakash, S., Chowhan, S. S., Kumar, V., Sharma, R., y Mahajan, A. (2024). A prototype model of zero trust architecture blockchain with EigenTrust-based practical byzantine fault tolerance protocol to manage decentralized clinical trials. *Blockchain: Research and Applications*, *100232*, 100232. https://doi.org/10.1016/j.bcra.2024.100232

Phiayura, P., y Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE access: practical innovations, open solutions*, *11*, 19487–19511. https://doi.org/10.1109/access.2023.3248622

Polinati, A. K. (2025). Hybrid cloud security: Balancing performance, cost, and compliance in multi-cloud deployments. En *arXiv [cs.CR]*. https://doi.org/10.48550/ARXIV.2506.00426

Ramachandran, H., Smith, R., Awuson K., Al-Hadhrami, T., y Acharya, P. (2025).

Towards net zero resilience: A futuristic architectural strategy for cyber-attack defence in industrial control systems (ICS) and operational technology (OT). *Computers, Materials & Continua*, *82*(2), 3619–3641. https://doi.org/10.32604/cmc.2024.054802

Sasada, T., Kawai, M., Masuda, Y., Taenaka, Y., y Kadobayashi, Y. (2023). Factor analysis of learning motivation difference on cybersecurity training with zero trust architecture. *IEEE access: practical innovations, open solutions*, *11*, 141358–141374. https://doi.org/10.1109/access.2023.3341093

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., y Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE access: practical innovations, open solutions*, *10*, 57143–57179. https://doi.org/10.1109/access.2022.3174679

Verma, P. K., Singh, B., Shubham, P., Sharma, K., y Prasad Joshi, R. (2024). Evaluating the effectiveness of Zero Trust Architecture in protecting against advanced persistent threats. *ADCAIJ Advances in Distributed Computing and Artificial Intelligence Journal*, *13*, e31611. https://doi.org/10.14201/adcaij.31611

Wan, T., Shi, B., y Wang, H. (2025). A continuous authentication scheme for zero-trust architecture in industrial internet of things. *Alexandria Engineering Journal*, *122*, 555–563. https://doi.org/10.1016/j.aej.2025.03.012

Yeoh, W., Liu, M., Shore, M., y Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security*, *133*(103412), 103412. https://doi.org/10.1016/j.cose.2023.103412

Zanasi, C., Russo, S., y Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*(103414), 103414. https://doi.org/10.1016/j.adhoc.2024.103414

Zyoud, B., y Lebai, S. (2024). The role of information security culture in zero trust adoption: Insights from UAE organizations. *IEEE access: practical innovations, open solutions*, *12*, 72420–72444. https://doi.org/10.1109/access.2024.3402341