Ingeniería Investiga

Vol. 8, e1342, año 2026
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v8i00.1342

Artículo de revisión

Zero Trust en la gestión de identidades y accesos en la nube: Una revisión de modelos, ventajas y limitaciones

Zero Trust in Cloud Identity and Access Management: A Review of Models, Advantages and Limitations

Daily Ashley Cordova Urbina[1]* | Sergio Heli Diaz Sifuentes[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: *T1043300421@unitru.edu.pe

Información del artículo:

Recibido: 28/08/2025
Aceptado: 18/11/2025
Publicado: 28/11/2025

Resumen

La creciente adopción de la computación en la nube y de entornos digitales ha incrementado la frecuencia de ataques y la probabilidad de accesos no autorizados, frente a los cuales los modelos tradicionales de gestión de identidades y accesos (IAM) resultan insuficientes. En este contexto, el enfoque Zero Trust emerge como una alternativa más sólida que replantea la seguridad. La investigación tuvo como objetivo analizar los modelos de IAM aplicados a la computación en la nube bajo el enfoque Zero Trust, así como identificar sus ventajas y limitaciones. Mediante la metodología PRISMA, se realizó una búsqueda en tres bases de datos y, tras aplicar los criterios de inclusión, se analizaron 22 manuscritos. Los resultados evidencian 15 modelos de IAM basados en Zero Trust que integran inteligencia artificial, blockchain y control de acceso dinámico, ofreciendo mayor seguridad en ámbitos como 5G, IoT, nube y salud. No obstante, persisten limitaciones relacionadas con la complejidad, los costos, la escalabilidad y la privacidad. En conclusión, estos modelos no solo fortalecen la seguridad, sino que también constituyen una línea de investigación y desarrollo orientada a reformular la protección de recursos en diversos sectores.

Palabras clave: gestión de la información; protección de datos; tecnologías emergentes.

Abstract

The growing adoption of cloud computing and digital environments has increased the frequency of attacks and the likelihood of unauthorized access, against which traditional identity and access management (IAM) models prove insufficient. In this context, the Zero Trust approach emerges as a more robust alternative that redefines security. The aim of this research was to analyze IAM models applied to cloud computing under the Zero Trust framework, as well as to identify their advantages and limitations. Using the PRISMA methodology, a search was conducted across three databases, and after applying inclusion criteria, 22 manuscripts were analyzed. The results reveal 15 IAM models based on Zero Trust that integrate artificial intelligence, blockchain, and dynamic access control, offering enhanced security in areas such as 5G, IoT, cloud, and healthcare. Nevertheless, limitations remain regarding complexity, costs, scalability, and privacy. In conclusion, these models not only strengthen security but also represent a line of inquiry and development aimed at reformulating resource protection across diverse sectors.

Keywords: data protection; emerging technologies; information management.

1. Introducción

La computación en la nube, los entornos distribuidos y las superficies de ataque se han vuelto muy complejos y los enfoques perimetrales tradicionales presentan límites estructurales para garantizar los principios de la confidencialidad, integridad y disponibilidad. En este sentido, Zero Trust se ha consolidado como paradigma de referencia pues desplaza la confianza implícita por verificación continua y control de acceso de grano fino a lo largo del ciclo de vida de identidades, dispositivos y servicios. La literatura reciente coincide en que la seguridad en nube efectiva debe combinar segmentación, autenticación adaptativa y telemetría ininterrumpida, acentuando los requisitos de control de acceso, así como el cumplimiento en sistemas distribuidos (Arif et al., 2025; Golightly et al., 2023; Sarkar et al., 2022).

La parte central en la que se encuentra el núcleo de Zero Trust es la parte de la Gestión de Identidades y Accesos (IAM) como plano de control. La evolución desde políticas estáticas a decisiones contextuales, basadas en riesgo y alimentadas con datos en tiempo real, se produce con técnicas de aprendizaje automático y detección de anomalías para incrementar la sensibilidad ante amenazas internas y movimientos laterales (Belal y Sundaram, 2022; Lilhore et al., 2025). Al mismo tiempo, la automatización y la orquestación de la arquitectura Zero Trust han surgido como factores diferenciales en la focalización de la confianza, la aplicación de políticas y el monitoreo continuo en servidores de múltiples nubes y entornos 5G/6G (Cao et al., 2024).

La operacionalización en plataformas comerciales confirma beneficios y expone fricciones: las implementaciones sobre Azure reportan mejoras en visibilidad y reducción de riesgos asociados a privilegios, aunque enfrentan costos de adopción, complejidad de configuración y fatiga de usuario (Dakić et al., 2025). A su vez, la segmentación de amenazas basada en identidad, el análisis de comportamiento y el control contextual incrementan la eficacia, aunque persisten desafíos vinculados con la privacidad, el sesgo algorítmico y la gobernanza de datos (Ahmadi, 2025; Liu et al., 2024).

Las tecnologías emergentes que sustentan los modelos de Gestión de Identidades y Accesos (IAM) bajo el paradigma Zero Trust cumplen funciones complementarias. Entre ellas, blockchain actúa como libro mayor distribuido e inmutable, registrando y verificando operaciones, lo que reduce puntos únicos de fallo y mejora la trazabilidad de las transacciones de identidad y autenticación en la nube. En este marco, Du et al. (2023) han propuesto esquemas que combinan blockchain con pruebas de conocimiento cero, habilitando una autenticación segura y resistente a ataques de intermediario en entornos cloud.

Incluso, el cifrado basado en atributos a nivel de política (*Ciphertext-Policy Attribute-Based Encryption*, CP-ABE) permite implementar control de acceso granular en sistemas multi-nube, en coherencia con el principio de mínimo privilegio propio de Zero Trust. Según Tian (2025), se han desarrollado algoritmos de acceso anónimo para almacenamiento multi-cloud que integran CP-ABE con esquemas jerárquicos de gestión de identidades, logrando autenticar usuarios según atributos, reducir sobrecargas criptográficas y reforzar la protección de datos distribuidos.

Adicionalmente, la criptografía poscuántica se incorpora como mecanismo indispensable para preservar la solidez del ecosistema Zero Trust frente a amenazas derivadas de la computación cuántica. Hrishikesh (2025) advierte que algoritmos clásicos como RSA (Rivest–Shamir–Adleman) y Elliptic Curve Cryptography (ECC) podrían verse comprometidos por ataques cuánticos, lo que hace necesario adoptar esquemas resistentes para proteger claves, canales de autenticación y operaciones críticas en sistemas IAM modernos.

A partir de este estado del arte, el presente artículo tiene como objetivo analizar los modelos de Gestión de Identidades y Accesos (IAM) en la computación en la nube bajo el enfoque Zero Trust, junto con sus principales ventajas y limitaciones.

2. Metodología

Se aplicaron las directrices establecidas en *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). Page et al. (2021) señala que este marco fue diseñado para garantizar que la documentación se presente de manera clara y comprensible. La metodología desempeña un papel esencial en la elaboración de revisiones sistemáticas y metaanálisis, pues asegura un análisis riguroso y detallado, reduciendo la posibilidad de errores sistemáticos y sesgos en la selección de estudios. Además, este marco metodológico no solo ordena el flujo de información, sino que también reduce sesgos potenciales al obligar a justificar decisiones clave en la búsqueda, depuración y exclusión de literatura.

2.1. Estrategia de búsqueda

La búsqueda inicial comenzó el 25 de septiembre de 2025, empleando términos clave definidos en función del objetivo y la relación con el tema de estudio. La información se recopiló en tres motores de búsqueda (ScienceDirect, Scopus y SpringerLink) utilizando las palabras clave detalladas en la Tabla 1, para posteriormente ser analizada.

2.2. Criterios de inclusión y exclusión

Durante el proceso se establecieron criterios específicos para preservar la originalidad y reducir posibles sesgos. Los criterios de inclusión y exclusión se presentan en la Tabla 2.

2.3. Proceso de recolección de la información

La selección de artículos se realizó de manera rigurosa para garantizar confiabilidad y originalidad en el manuscrito, así como seguridad para los lectores interesados en el tema. El procedimiento se representa en la Figura 1 mediante el diagrama de flujo de PRISMA, donde se especifica que, tras aplicar la estrategia de búsqueda y los criterios definidos, se seleccionaron únicamente los manuscritos pertinentes al objeto de investigación.

Tabla 1
Términos de búsqueda en base de datos

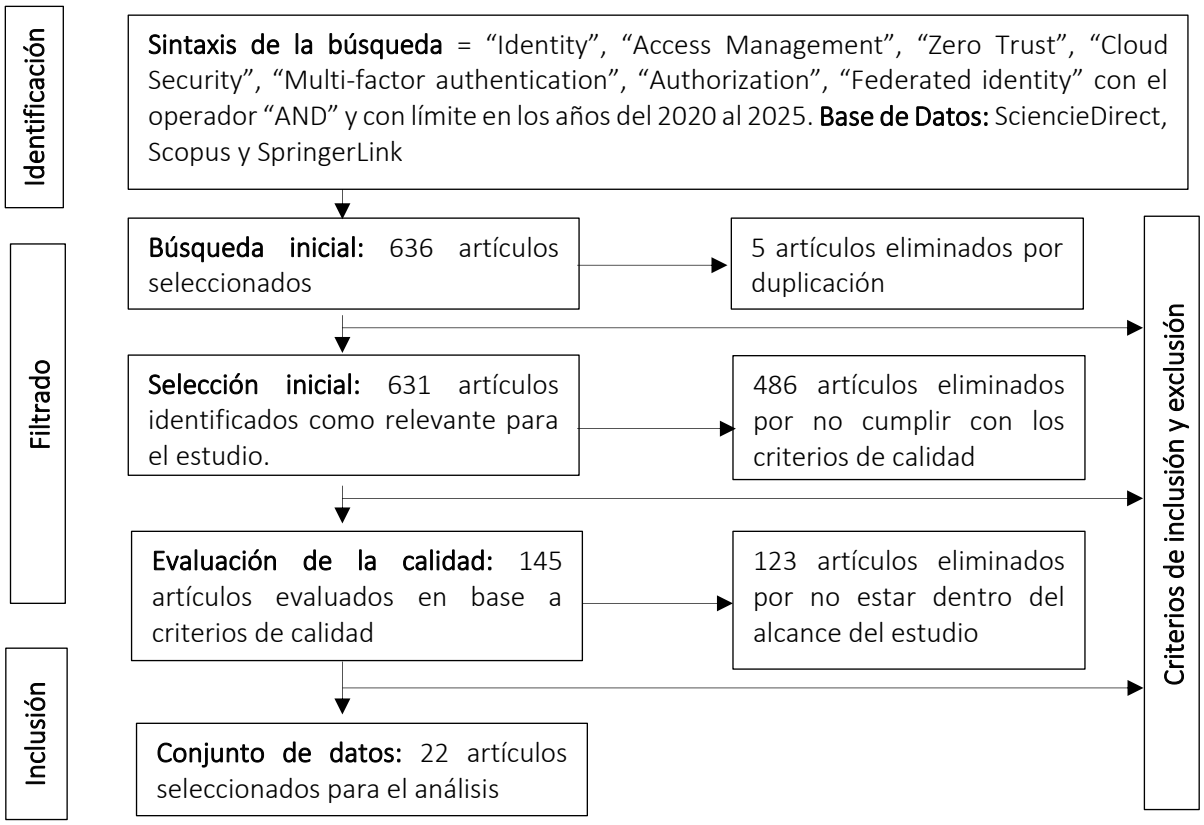
Base de datos	Términos de búsqueda	Resultados
Science Direct	Digital Identity and Access Management and Zero Trust and Cloud Security and Multi-factor authentication and Authorization and Federated identity	323
Scopus	(Identity) OR (Access Management) AND (Zero Trust) AND (Cloud Security))	145
Springer Link	Digital Identity and Access Management and Zero Trust and Cloud Security and Multi-factor authentication and Authorization and Federated identity	168

Tabla 2
Criterios empleados en la revisión

Criterios de inclusión	Criterios de exclusión
Artículos en relación a Gestión de Identidades y acceso a la Nube basadas en modelos Zero Trust	Documentos que no aborden el tema de investigación y que estén en formato de ejemplares.
Publicados entre los años 2020 y 2025	Publicados antes del 2020
Escritos en inglés o español	Idioma distinto al inglés o español
De libre acceso	Acceso restringido

Figura 1

Diagrama PRISMA del proceso de recolección de datos



3. Resultados

Tras el análisis de los manuscritos seleccionados para la revisión, la información se organizó en la Tabla 3, con el propósito de mostrar de manera estructurada la contribución de cada estudio, destacando sus innovaciones, alcances y contribuciones técnicas en distintos contextos tecnológicos. Esta organización permite identificar tendencias clave como identidad descentralizada, autenticación continua y enfoques basados en inteligencia artificial, blockchain y arquitecturas cloud-native.

Adicionalmente, la Figura 2 presenta la arquitectura de Zero Trust, donde la Gestión de Identidades y Accesos (IAM) cumple una función central como plano de control encargado de la autenticación continua, la evaluación contextual de riesgo y la orquestación dinámica de políticas. El modelo ilustra cómo las identidades (usuarios, dispositivos y servicios) son evaluadas por el motor de políticas Zero Trust, compuesto por el *Policy Engine*, el *Policy Administrator* y el *Policy Enforcement Point*, en combinación con tecnologías habilitadoras como MFA, análisis de comportamiento, inteligencia artificial y aprendizaje automático para evaluación de riesgo, además de monitoreo constante. Las decisiones resultantes permiten aplicar autenticación continua y control de acceso contextual en entornos multi-nube, IoT y 5G.

A continuación, la Tabla 4 presenta 15 modelos de IAM con enfoque Zero Trust, los cuales reflejan la evolución de las arquitecturas de seguridad hacia diseños descentralizados y adaptativos, aplicando el principio de "Nunca confiar, siempre verificar". Estos modelos abarcan distintos dominios y combinan diversas tecnologías de apoyo. Posteriormente, se realiza un subanálisis de los 15 modelos identificados, agrupados en cuatro sectores tecnológicos principales que se muestran en la Tabla 5, donde se evidencia que la madurez del enfoque Zero Trust IAM varía según el sector.

Tabla 3

Análisis de los documentos seleccionados

N°	Autores y año	Aporte
1	Glöckler et al. (2024)	Muestran cómo la gestión de identidades y accesos (IAM) empresarial puede fortalecerse mediante *Self-Sovereign Identity* (SSI), un enfoque descentralizado y sin contraseñas. Al identificar y categorizar los requisitos de IAM en cuatro dimensiones (seguridad y cumplimiento, operabilidad, tecnología y usuario) y probar un prototipo con expertos, evidencia que SSI aporta beneficios clave como automatización, interoperabilidad, privacidad y principio de mínimo privilegio.
2	Alnaim (2025)	Presenta un marco adaptativo de Zero Trust (SecureChain-ZT) que integra IA, blockchain y microsegmentación para gestionar políticas de seguridad en entornos 5G altamente dinámicos. Sus resultados demuestran que la autenticación continua, el monitoreo en tiempo real y la actualización automática de políticas pueden mejorar drásticamente la precisión en la detección de amenazas y la eficiencia en la gestión de accesos.
3	Cao et al. (2024)	Ofrecen una visión crítica sobre la automatización y orquestación de Zero Trust Architecture (ZTA), resaltando cómo la integración de técnicas de inteligencia artificial puede potenciar funciones clave como la evaluación de confianza, autenticación, detección de ataques y monitoreo. Su relevancia radica en que identifica las brechas actuales en la aplicación de AI a ZTA y plantea oportunidades de investigación futura, especialmente en entornos de cloud computing y 5G/6G.
4	Ahmadi (2025)	Propone un marco de Zero Trust impulsado por IA, que introduce segmentación dinámica de identidades, análisis de comportamiento y control de acceso contextual como mejoras frente a los modelos tradicionales de políticas estáticas. Su contribución es clave porque muestra cómo la gestión adaptativa de accesos en tiempo real permite mitigar amenazas internas y persistentes avanzadas, reforzando la resiliencia organizacional sin afectar la productividad. Además, al señalar retos como la privacidad y la escalabilidad, y proponer la integración futura de federated learning y blockchain.
5	Du et al. (2023)	Presentan HIDA, un protocolo de autenticación basado en Hyperledger Fabric y pruebas de conocimiento cero, diseñado para superar las limitaciones de los métodos tradicionales de IAM en la nube, como los puntos únicos de fallo, baja eficiencia y falta de privacidad. Su relevancia radica en demostrar, mediante simulaciones y análisis formales, que es posible establecer canales de autenticación más seguros, descentralizados y eficientes, fortaleciendo el acceso bajo un enfoque Zero Trust.
6	Bernabé et al. (2025)	Proponen un modelo descentralizado de gestión de identidades y accesos (DIM) bajo principios Zero Trust, aplicado al Computing Continuum, donde conviven entornos distribuidos y heterogéneos. Su enfoque destaca el uso de DIDs, credenciales verificables y blockchain para lograr autenticación y autorización seguras, interoperables y con preservación de la privacidad, permitiendo a los usuarios controlar sus propios atributos de identidad.
7	Liu et al. (2024)	Ofrecen una visión estratégica del modelo Zero Trust aplicado al IoT, identificando vulnerabilidades en diferentes capas (percepción, red y aplicación) y mostrando cómo medidas como autenticación continua, segmentación, IAM y control de acceso dinámico pueden mitigar riesgos. Su valor reside en que no solo analiza el estado actual de la literatura mediante bibliometría, sino que también identifica tendencias emergentes como Zero Trust en nube, edge y blockchain.

Tabla 3 (Continuación/1)

N°	Autores y año	Aporte
8	Hrishikesh (2025)	Muestra cómo tecnologías emergentes como IA, blockchain, computación cuántica, edge y 5G/6G están transformando la implementación de Zero Trust, ampliando sus capacidades de evaluación dinámica de confianza, control de accesos contextuales y gestión descentralizada de identidades. Su relevancia radica en que conecta la evolución tecnológica con los principios de IAM bajo Zero Trust, evidenciando tanto oportunidades (como la autenticación continua, la criptografía resistente a la computación cuántica y los enfoques descentralizados de identidad) como desafíos relacionados con privacidad, sesgo algorítmico y complejidad operativa.
9	Alshomrani y Li (2022)	Presentan un protocolo de autenticación continua para IoT basado en Zero Trust (PUFDCA), que combina funciones físicamente no clonables (PUF) y verificación en tiempo real de ubicación. Su relevancia radica en demostrar cómo aplicar los principios de "nunca confiar, siempre verificar" en entornos con dispositivos de bajo costo y alta vulnerabilidad, logrando un equilibrio entre ligereza y seguridad.
10	Golightly et al. (2023)	Ofrecen una visión amplia de las técnicas modernas de control de acceso, evaluando su aplicación en cloud computing, blockchain, IoT y SDN, lo que lo conecta directamente con el análisis de IAM bajo Zero Trust en entornos de nube. Su relevancia radica en que, además de revisar las fortalezas y limitaciones de distintos modelos, resalta tendencias como el uso de IA para decisiones de autorización inteligentes, la necesidad de modelos unificados y la compatibilidad con regulaciones como el GDPR.
11	Sarkar et al. (2022)	Realizan una comparación de modelos, marcos y pruebas de concepto de Zero Trust aplicados a redes en la nube, identificando sus características, fortalezas y limitaciones. Su relevancia radica en que evidencia cómo Zero Trust permite mayor granularidad, visibilidad y automatización en la gestión de accesos, pero también muestra que su implementación aún es incipiente y requiere investigación adicional y validación en entornos reales.
12	Lilhore et al. (2025)	Al introducir SmartTrust, un marco de seguridad para la nube basado en Zero Trust que combina deep learning híbrido (CNN, LSTM, Transformers), refuerzo adaptativo y blockchain para la detección en tiempo real de amenazas como insider threats, escalamiento de privilegios y brechas de datos. Su relevancia radica en demostrar cómo los enfoques tradicionales (reglas estáticas o MFA) resultan insuficientes frente a ataques complejos, y cómo la autenticación continua y el análisis contextual dinámico pueden mejorar significativamente la protección.
13	Bartakke y Kashyap (2024)	Analizan cómo la computación en la nube puede integrarse con el modelo de seguridad Zero Trust, destacando tanto sus beneficios como sus desafíos. Desde una perspectiva práctica, subraya que la verificación continua de usuarios, dispositivos y aplicaciones es esencial para reducir riesgos como fugas de datos, accesos no autorizados y brechas de seguridad en entornos distribuidos.
14	Tian (2025)	Muestra cómo un algoritmo de acceso anónimo basado en CP-ABE puede fortalecer la seguridad y privacidad en sistemas de almacenamiento multi-nube bajo un enfoque Zero Trust. Su propuesta mejora la eficiencia de cifrado/descifrado, reduce la sobrecarga de almacenamiento y garantiza un control de acceso más granular, aspectos clave en la gestión de identidades y accesos (IAM) en entornos distribuidos.

Tabla 3 (Continuación/2)

N°	Autores y año	Aporte
15	Mukta et al. (2025)	Muestran cómo la integración de SSI, DID y CapBAC bajo principios Zero Trust ofrece una arquitectura descentralizada y flexible para la gestión y delegación de accesos en entornos dinámicos como IoT. Su enfoque permite decisiones de acceso basadas en capacidades y evaluaciones continuas de confianza, resolviendo limitaciones de los modelos tradicionales estáticos. Además, el uso de blockchain para la trazabilidad y la inmutabilidad de registros refuerza la transparencia y seguridad, alineándose con los desafíos de confianza y escalabilidad en ecosistemas distribuidos.
16	Peepliwal et al. (2024)	Realizan un modelo prototipo de Zero Trust Architecture integrado con blockchain e IoT para ensayos clínicos descentralizados (DCTs). Su propuesta, denominada z-TAB, combina Hyperledger Fabric con el protocolo EigenTrust-PBFT, lo que fortalece la inmutabilidad, trazabilidad y consenso en la gestión de datos clínicos. Además, garantiza que toda interacción se valide bajo principios Zero Trust, reduciendo riesgos de accesos no autorizados y fallas en el consenso.
17	Chen et al. (2021)	Proponen un sistema de conciencia y protección de seguridad para entornos de salud inteligente en 5G, fundamentado en Zero Trust Architecture (ZTA). Su contribución principal es el marco 4-D (sujeto, objeto, comportamiento y entorno), que permite construir modelos de acceso dinámicos, con autenticación continua, control de acceso de grano fino y análisis de comportamiento en tiempo real. La validación a nivel industrial demuestra la aplicabilidad práctica de ZTA en un sector crítico como la salud, evidenciando cómo Zero Trust puede reforzar la seguridad extrema a extremo en contextos de alta movilidad y grandes volúmenes de datos.
18	Dakić et al. (2025)	Muestran una aplicación práctica de Zero Trust en entornos de nube con Azure, específicamente en organizaciones medianas. Su valor está en evidenciar cómo las herramientas de Microsoft (Conditional Access, Privileged Identity Management, MFA, passwordless authentication) permiten trasladar los principios de Zero Trust a escenarios reales, reduciendo incidentes de acceso privilegiado y mejorando la visibilidad de identidades y dispositivos. Además, señala los retos de implementación, como la complejidad en configuraciones, la fatiga del usuario y los altos costos iniciales
19	Ziegler et al. (2025)	Abordan la respuesta a incidentes en modelos de Self-Sovereign Identity (SSI). Aunque SSI promete mayor control y privacidad de las identidades, su naturaleza descentralizada complica la aplicación de procesos tradicionales de respuesta a incidentes, que suelen ser centralizados. El trabajo propone procesos de respuesta incidentales tanto centralizados como descentralizados, adaptados a diferentes actores y escenarios del ecosistema SSI, lo que permite visualizar cómo estos mecanismos pueden complementar modelos IAM en la nube.
20	Arif et al. (2025)	Muestran cómo las arquitecturas cloud-native requieren un enfoque de seguridad integral que incluye IAM como parte central de sus mecanismos de confianza. Al revisar herramientas como cifrado en tránsito y en reposo, IAM cloud-native, control en tiempo real y service mesh, el estudio refuerza la importancia de aplicar Zero Trust en entornos dinámicos y distribuidos. Además, sus conclusiones resaltan que la seguridad debe abordarse en múltiples capas (aplicación, red, infraestructura y cumplimiento).

Tabla 3 (Continuación/3)

N°	Autores y año	Aporte
21	Belal y Sundaram (2022)	Ofrecen una visión sistemática sobre cómo las técnicas de Machine Learning y Deep Learning están transformando la seguridad en entornos cloud. Al presentar una taxonomía de amenazas definida por la Cloud Security Alliance y evaluar 42 estudios de caso, evidencian que los mecanismos tradicionales de autenticación y control de acceso resultan insuficientes frente a ataques avanzados. Asimismo, muestran cómo los modelos de IA permiten clasificación de actividades, detección de intrusiones, autenticación adaptativa y preservación de la privacidad, elementos esenciales para fortalecer la verificación continua y el principio de mínimo privilegio en Zero Trust.
22	Al-Hammuri et al. (2024).	Un enfoque innovador conecta los principios de Zero Trust con la reducción de errores médicos en sistemas de salud basados en la nube. El marco propuesto de gestión de accesos consciente del contexto integra microservicios, análisis semántico y sintáctico mediante modelos de lenguaje, y un sistema de puntuación de confianza. Con ello se refuerza la seguridad de usuarios, dispositivos y datos, al tiempo que se previenen fallos humanos y clínicos, responsables de gran parte de las vulnerabilidades en salud digital. Este aporte demuestra cómo Zero Trust puede trascender la ciberseguridad técnica para convertirse en un mecanismo de protección integral en entornos médicos, preservando tanto la integridad de la información como la seguridad de los pacientes, y enriqueciendo la discusión sobre su aplicabilidad en telemedicina y hospitales inteligentes.

Figura 2

Arquitectura Zero Trust orientada a IAM

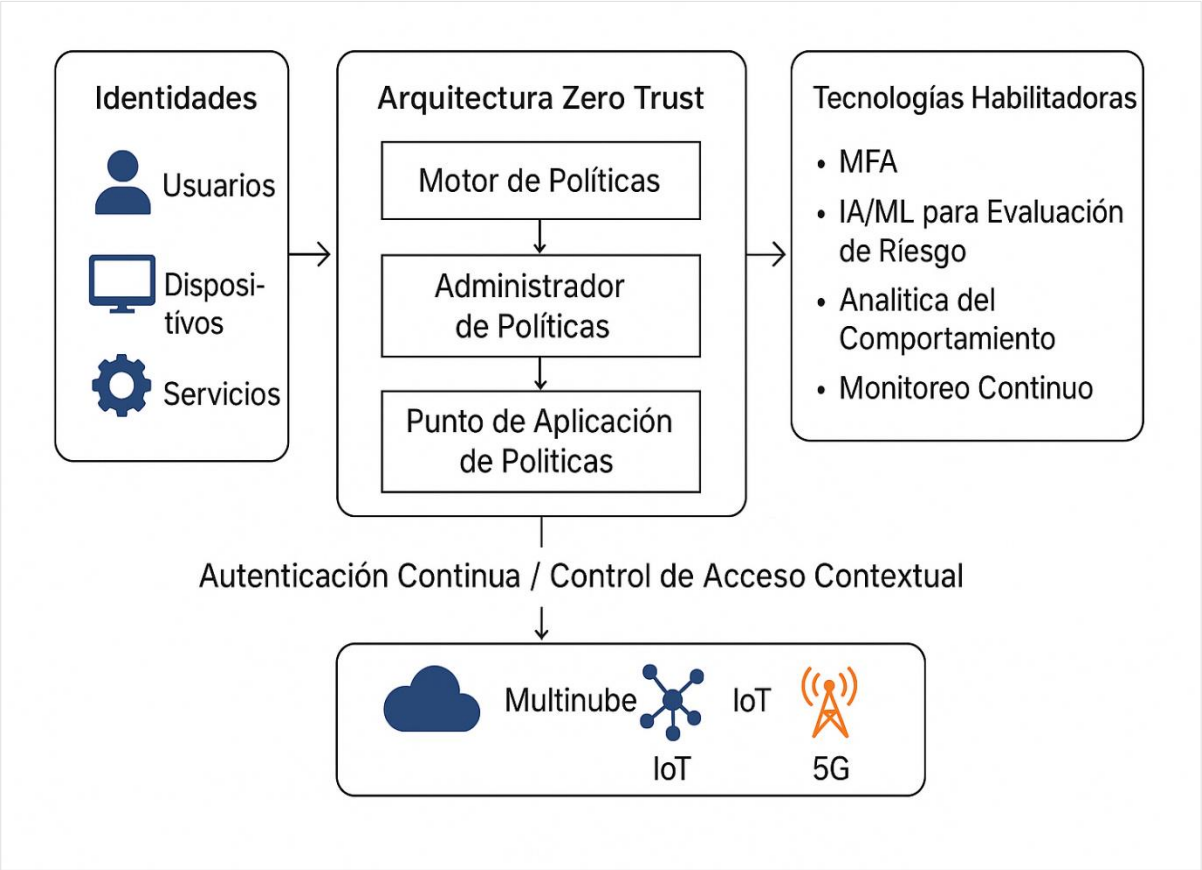


Tabla 4

Análisis de los modelos IAM bajo Zero Trust

Modelo IAM bajo Zero Trust	Contexto de aplicación	Tecnologías clave	Ventajas principales	Limitaciones
Adaptive Zero Trust Policy Framework (SecureChain-ZT)	Redes 5G y telecomunicaciones	IA, blockchain, microsegmentación	Alta precisión en autenticación (≈98 %), detección avanzada de intrusiones.	Elevado costo computacional y complejidad de despliegue en tiempo real.
ZTA Automatizada y Orquestada	Nube, entornos corporativos	IA, automatización, DevSecOps	Automatiza evaluación de confianza y políticas de acceso.	Escasez de marcos estandarizados, dependencia de IA aún en fase experimental.
Identidad Autónoma con Segmentación de Amenazas	Corporativo, IoT distribuido	IA, analítica de comportamiento, control contextual	Aislamiento dinámico de identidades comprometidas.	Problemas de privacidad en análisis de comportamiento y alto consumo de recursos.
Decentralised Identity Management (DIM)	Multi-dominio, Continuum computing	SSI, blockchain, credenciales verificables	Identidad auto-soberana, interoperabilidad entre dominios.	Sobrecarga en latencia por operaciones descentralizadas, escalabilidad limitada.
Zero Trust en IoT (visión bibliométrica)	IoT y Edge	IAM continuo, SDP, segmentación	Autenticación continua, multifactor en dispositivos IoT.	Dificultad de implementación en dispositivos con bajos recursos.
Zero Trust con Tecnologías Emergentes	Multisectorial, nube híbrida	IA, ML, blockchain, criptografía poscuántica	Extensible, adaptable y con resiliencia a futuro.	Riesgo de sesgo algorítmico en IA, costos altos de integración tecnológica.
PUFDCA (Protocol for IoT Devices).	IoT, autenticación continua.	PUF, CSI, Zero Trust.	Verificación estática y dinámica de dispositivos.	Riesgo de falsos positivos y dependencia de hardware PUF.
ZTA en Nube (comparativa)	Cloud computing	Microsegmentación, IAM granular, automatización	Mayor visibilidad y control de accesos.	Aún inmaduro en despliegues comerciales, falta de frameworks unificados.
SmartTrust Framework	Cloud corporativo	Deep learning (CNN, LSTM, Transformer), RL, blockchain	Alta detección de amenazas (≈99 %), adaptable a ataques dinámicos.	Elevada complejidad y demanda de cómputo, latencias en blockchain logging.

Tabla 4 (Continuación/1)

Modelo IAM bajo Zero Trust	Contexto de aplicación	Tecnologías clave	Ventajas principales	Limitaciones
Zero Trust en Cloud (modelo conceptual)	Estrategias cloud empresariales	IAM en capas, monitoreo continuo	Refuerza seguridad en entornos multicloud.	Costos elevados de implementación, gestión difícil para PYMES.
Zero Trust con CP-ABE	Multi-nube	Cifrado jerárquico + CP-ABE	Control de acceso fino y anónimo.	Requiere CA centralizada (punto único de fallo), gestión de revocaciones limitada
Zero Trust delegado con Blockchain (CapBAC + SSI)	IoT y ecosistemas distribuidos	Blockchain, SSI, DID, CapBAC	Delegación flexible de accesos con trazabilidad.	Complejidad en revocación de privilegios y sobrecarga de blockchain
z-TAB (Zero Trust Blockchain para Ensayos Clínicos)	Salud, clinical trials	Blockchain, IoT, PBFT, Zero Trust	Seguridad y trazabilidad de datos médicos.	Complejidad regulatoria, alto consumo de recursos en consenso PBFT.
Zero Trust en 5G Smart Healthcare	Sanidad y telemedicina	IAM dinámico, 5G, Zero Trust	Autenticación continua en usuarios, apps y servicios.	Falta de estándares maduros en salud, dificultad de integración con sistemas heredados.
ZTCloudGuard (Healthcare + IA)	Nube y hospitales inteligentes	Context-aware IAM, ML, microservicios	Prevención de errores médicos (F1 ≈93,5 %).	Basado en dataset sintético, aún no probado a gran escala.

Tabla 5

Subanálisis por sectores de aplicación de los modelos

Sector	Modelo representativos	Características principales	Retos identificados
Salud digital y 5G	ZTCloudGuard, Zero Trust en 5G Smart Healthcare, z-TAB	Autenticación continua, control contextual, prevención de errores clínicos, trazabilidad médica.	Gobernanza de datos, cumplimiento regulatorio y latencia en consensos blockchain
IoT y Edge Computing	PUFDCA, Zero Trust en IoT, Zero Trust delegado con Blockchain	Autenticación ligera, segmentación dinámica, gestión descentralizada de identidades	Heterogeneidad del hardware, consumo energético y limitaciones de recursos
Cloud Computing y entornos corporativos	SmartTrust, ZTA Automatizada, Zero Trust en Cloud, Adaptive ZT Policy Framework	Integración IA–DevSecOps, microsegmentación, automatización de políticas	Complejidad de configuración, costos de despliegue y fatiga del usuario
Identidad descentralizada y SSI	DIM, Zero Trust con CP-ABE, Identidad Autónoma, HIDA	Identidad auto-soberana, cifrado jerárquico, control de acceso granular	Escalabilidad limitada, sobrecarga criptográfica y gestión de claves compleja.

4. Discusión

Los resultados de la revisión señalan que 15 modelos de Gestión de Identidades y Accesos bajo el enfoque de Zero Trust tienen el mismo hilo conductor: IAM es el plano de control para el acceso continuo, la evaluación de riesgo y el control de acceso contextual, en las nubes, en el IoT y en el 5G, y que incorporan tecnologías tales como IA, blockchain, atributos criptográficos e identidad autosoberana, que permiten materializar efectivamente la idea, con el concepto de "nunca confíes, siempre verifica", frente a las amenazas avanzadas y entornos distribuidos (Ahmadi, 2025; Lilhore et al., 2025).

El subanálisis por sectores revela diferencias de madurez evidentes. En el ámbito de la salud digital y del 5G, los modelos que se emplean ponen por delante la trazabilidad de datos clínicos y la prevención de errores médicos a través de una constante autenticación y control contextual. Sin embargo, todavía tienen desafíos en cuanto a gobernanza de datos, cumplimiento regulatorio y lentitud en los mecanismos de consenso (Chen et al., 2021; Peepliwal et al., 2024). En IoT y Edge, las propuestas se enfocan en la segmentación dinámica y autenticación ligera de dispositivos con recursos limitados. Esto genera dificultades para gestionar identidades y escalar en ecosistemas muy diversos (Alshomrani & Li, 2022; Liu et al., 2024). En el ámbito de la computación en la nube y los entornos empresariales, se combinan DevSecOps e inteligencia artificial con modelos como SmartTrust y arquitecturas automatizadas Zero Trust para optimizar la detección de amenazas y el control de accesos; sin embargo, implican un alto costo de implementación, complejidad en la configuración y agotamiento del usuario (Dakić et al., 2025; Sarkar et al., 2022). Para finalizar, en la identidad descentralizada, los enfoques que se basan en SSI, CP-ABE y blockchain fortalecen la privacidad y el control del usuario; sin embargo, muestran problemas relacionados con la gestión de claves, la escalabilidad y una sobrecarga criptográfica (Bernabé et al., 2025; Tian, 2025; Mukta et al., 2025).

Los modelos Zero Trust IAM son más eficaces que las estrategias convencionales de seguridad perimetral y políticas estáticas al detectar amenazas y disminuir el movimiento lateral. Esto se respalda con tasas de detección que en ciertos esquemas basados en IA y microsegmentación alcanzan hasta el 98-99 % (Alnaim, 2025; Lilhore et al., 2025). No obstante, este avance implica costos más altos y mayor complejidad, a causa del requerimiento de infraestructuras sofisticadas, supervisión constante y habilidades de automatización que no siempre tienen acceso las empresas pequeñas o con recursos escasos (Bartakke & Kashyap, 2024; Golightly et al., 2023). En cuanto a la escalabilidad, los resultados muestran que el uso de Zero Trust IAM se basa en la habilidad de cada entidad para administrar un alto número de eventos, identidades y políticas sin afectar el funcionamiento de los sistemas.

Un elemento importante es que la diversidad de las medidas utilizadas en los estudios hace imposible llevar a cabo metaanálisis cuantitativos sólidos. Algunos trabajos, por un lado, se enfocan en indicadores cualitativos acerca del cumplimiento normativo y la experiencia de usuario, así como en la latencia o el consumo de recursos. Otros trabajos, por otro lado, informan sobre indicadores como F1-score, tasa de detección o precisión de clasificación. Esta variedad complica la comparación directa entre los modelos y restringe el alcance general de los resultados. Por lo tanto, se nota que es necesario avanzar hacia marcos de benchmarking en Zero Trust IAM con conjuntos de métricas comparables reducidos (como la detección de amenazas, los falsos positivos, el impacto en la experiencia del usuario, el costo de implementación y la escalabilidad). Tener estos benchmarks facilitaría una evaluación más imparcial de la relación entre el costo y el beneficio de Zero Trust en comparación con métodos tradicionales, lo cual orientaría las decisiones de adopción y migración en cada sector.

Por último, Zero Trust IAM contribuye a optimizar el control de accesos y la seguridad. Sin embargo, también revela que su aplicación continúa afectada por desafíos como la falta de métricas unificadas, los costos, la escalabilidad y la complejidad operativa. Al aplicar los modelos analizados en escenarios reales de nube, IoT,

salud y corporativos, estas restricciones deben tomarse en cuenta.

5. Conclusiones

Se identificaron y analizaron 15 modelos de gestión de identidades y accesos en distintos contextos tecnológicos bajo el enfoque Zero Trust. En general, los resultados corroboran que IAM se establece como plano de control para implementar autenticación continua, evaluación contextual del riesgo y control de acceso granular. Esto fortalece la defensa de recursos en ámbitos como la nube, IoT, salud digital e identidad descentralizada. El subanálisis por sectores reveló que la madurez de Zero Trust IAM no es uniforme: mientras dominios como salud y cloud corporativo presentan propuestas más desarrolladas, otros, como identidad descentralizada e IoT, aún enfrentan desafíos significativos relacionados con rendimiento, gobernanza y escalabilidad.

Desde la perspectiva práctica, los modelos de IAM Zero Trust aportan ventajas claras frente a los enfoques convencionales, al reducir accesos no permitidos y mejorar la visibilidad de identidades y actividades. No obstante, su despliegue implica inversiones considerables en automatización, infraestructura y gestión del cambio organizacional, y se ve limitado por la ausencia de marcos y métricas que permitan una evaluación objetiva de su costo-beneficio. En consecuencia, una línea futura prioritaria es el establecimiento de benchmarks y estudios empíricos en entornos productivos que respalden decisiones estratégicas sobre diseño, migración y gestión de identidades en la nube bajo Zero Trust.

Contribución de los autores

D. A. Cordova: Conceptualización, curación de datos, análisis formal, investigación, metodología, recursos, visualización, redacción del borrador original, revisión y edición. **S. H. Diaz:** Conceptualización, investigación, metodología, recursos, validación, redacción del borrador original, revisión y edición. **A. C. Mendoza:** Conceptualización, administración del proyecto, supervisión, visualización y redacción del borrador original.

Conflictos de interés

Los autores manifiestan que no tienen conflictos de interés respecto a esta publicación.

6. Referencias bibliográficas

Ahmadi, S. (2025). Autonomous identity-based threat segmentation for zero trust architecture. *Cyber Security and Applications*, *3*, 100106. https://doi.org/10.1016/j.csa.2025.100106

Al-Hammuri, K., Gebali, F., y Kanan, A. (2024). ZTCloudGuard: Zero Trust Context-Aware Access Management Framework to Avoid Medical Errors in the Era of Generative AI and Cloud-Based Health Information Ecosystems. *AI (Switzerland)*, *5*(3), 1111-1131. https://doi.org/10.3390/ai5030055

Alnaim, A. K. (2025). Adaptive Zero Trust Policy Management Framework in 5G Networks. *Mathematics*, *13*(9), 1501. https://doi.org/10.3390/math13091501

Alshomrani, S., y Li, S. (2022). PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wireless Communications and Mobile Computing*, *2022*(2), 6367579. https://doi.org/10.1155/2022/6367579

Arif, T., Jo, B., y Park, J. H. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors*, *25*(8), 2350. https://doi.org/10.3390/s25082350

Bartakke, J., y Kashyap, R. (2024). The Usage of Clouds in Zero-Trust Security Strategy: An Evolving Paradigm. *Journal of Information and Organizational Sciences*, *48*(1), 149-165. https://doi.org/10.31341/jios.48.1.8

Belal, M. M., y Sundaram, D. M. (2022). Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. *Journal of King Saud University - Computer and*

Information Sciences, *34*(10, Part B), 9102-9131. https://doi.org/10.1016/j.jksuci.2022.08.035

Bernabé, J. M., Cánovas, E., García-Rodríguez, J., M. Zarca, A., y Skarmeta, A. (2025). Decentralised Identity Management solution for zero-trust multi-domain Computing Continuum frameworks. *Future Generation Computer Systems*, *162*, 107479. https://doi.org/10.1016/j.future.2024.08.003

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

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., y Zhai, Y. (2021). A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. *IEEE Internet of Things Journal*, *8*(13), 10248-10263. https://doi.org/10.1109/JIOT.2020.3041042

Dakić, V., Morić, Z., Kapulica, A., y Regvart, D. (2025). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. *Journal of Cybersecurity and Privacy*, *5*(1), 2. https://doi.org/10.3390/jcp5010002

Du, Z., Jiang, W., Tian, C., Rong, X., y She, Y. (2023). Blockchain-Based Authentication Protocol Design from a Cloud Computing Perspective. *Electronics (Switzerland)*, *12*(9), 2140. https://doi.org/10.3390/electronics12092140

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*, *66*(4), 421-440. https://doi.org/10.1007/s12599-023-00830-x

Golightly, L., Modesti, P., Garcia, R., y Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, *1*, 100015. https://doi.org/10.1016/j.csa.2023.100015

Hrishikesh, J. (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

Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alhazmi, A., y Khan, M. M. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture. *Journal of Cloud Computing*, *14*(1), 35. https://doi.org/10.1186/s13677-025-00764-7

Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., y Liu, Q. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity*, *7*(1), 20. https://doi.org/10.1186/s42400-024-00212-0

Mukta, R., Pal, S., Chowdhury, K., Hitchens, M., Paik, H., y Kanhere, S. S. (2025). Zero Trust Driven Access Control Delegation Using Blockchain. *Blockchain: Research and Applications*, *100319*, 100319. https://doi.org/10.1016/j.bcra.2025.100319

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., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Alonso-Fernández, S. (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. 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*, *5*(4), 100232. https://doi.org/10.1016/j.bcra.2024.100232

Sarkar, S., Choudhary, G., Kumar Shandilya, S. K., Azath, A., y Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability (Switzerland)*, *14*(18), 11213. https://doi.org/10.3390/su141811213

Tian, J. (2025). Zero trust anonymous access algorithm for multi cloud storage system based on CP-ABE. *Egyptian Informatics Journal*, *30*(100681), 100681. https://doi.org/10.1016/j.eij.2025.100681

Ziegler, L., Grabatin, M., Pöhn, D., y Hommel, W. (2025). Designing a security incident response process for self-sovereign identities. *EURASIP Journal on Information Security*, *2025*(1), 12. https://doi.org/10.1186/s13635-025-00195-6