Artículo de Revisión

Revisión de marco Zero Trust en seguridad de la información sanitaria: aspectos claves y mejoras

Review of Zero Trust Frameworks in Healthcare Information Security: Key Aspects and Improvements

María de Fátima Caffo Villalobos: Universidad Nacional de Trujillo, Ingeniera en Sistemas
https://orcid.org/0009-0005-3236-9878

Luis Javier Castillo Rabanal: Universidad Nacional de Trujillo, Ingeniero en Sistemas,
https://orcid.org/0009-0006-2078-8781

Alberto Carlos Mendoza de los Santos: Universidad Nacional de Trujillo, Doctor en Ingeniería de Sistemas,
https://orcid.org/0000-0002-0469-915X

Autor de correspondencia: t1513301021@unitru.edu.pe

Recibido: 4 agosto 2025
Publicado: 25 septiembre 2025

DOI: https://doi.org/10.64424/rcu42202586

Resumen:
La rápida digitalización del sector salud con historias clínicas electrónicas, telemedicina y dispositivos conectados ha mejorado la atención, pero multiplicado los vectores de riesgo para la información clínica sensible. Hospitales y centros de salud son objetivos de ciberataques (acceso no autorizado, robo de datos, ransomware) que afectan la confidencialidad, integridad y continuidad asistencial. Ante las limitaciones de la seguridad perimetral, la arquitectura Zero Trust (ZTA) propone "nunca confiar, siempre verificar", verificación continua, principio de menor privilegio y segmentación granular para reducir la superficie de ataque. Para evaluar su aplicabilidad, realizamos una revisión sistemática (2020–2025) siguiendo PRISMA: búsquedas en bases indexadas, selección con criterios predefinidos y análisis cualitativo-comparativo de propuestas y evaluaciones empíricas. La revisión mostró avances consistentes en autenticación multifactor, microsegmentación y trazabilidad, con evaluaciones que reportaron eficacias superiores al 90% en escenarios controlados; sin embargo, emergen limitaciones en interoperabilidad, latencia operacional y ausencia de métricas estandarizadas. Concluimos que ZTA ofrece mejoras significativas para la protección de la información sanitaria, aunque su adopción efectiva requiere estandarización de métricas, pruebas en entornos clínicos reales y soluciones para interoperabilidad y latencia.

Palabras clave: Zero trust, PRISMA 2020, salud, ciberseguridad, evaluación, protección de datos.

Abstract:
The accelerated digitalization of healthcare through electronic health records, telemedicine platforms, and connected medical devices has improved care but multiplied exposure points for sensitive clinical information. Hospitals and healthcare centers are targets of cyberattacks (unauthorized access, data theft, ransomware) that affect confidentiality, integrity, and continuity of care. Given the limits of perimeter-based security, Zero Trust Architecture (ZTA) advocates "never trust, always verify," continuous verification, least privilege, and fine-grained segmentation to reduce attack surface. To assess applicability, we conducted a systematic review (2020–2025) following PRISMA: searches in indexed databases, selection with predefined criteria, and a qualitative-comparative analysis of proposed frameworks and empirical evaluations. The review found consistent advances in multi-factor authentication, micro-segmentation, and traceability, with reported effectiveness above 90% in controlled settings; however, limitations emerged in interoperability, operational latency, and absence of standardized metrics. We conclude that ZTA offers significant improvements for protecting health information, although effective adoption requires standardization of metrics, field testing in real clinical environments, and solutions for interoperability and latency.

Keywords: Zero trust, PRISMA 2020, healthcare, cybersecurity, evaluation, data protection.

Como citar la obra: Caffo Villalobos, M. F., Castilllo Rabana, L. J. y Mendoza de los Santos, A. C. (2025). Revisión de marcos Zero Trust en seguridad de la información sanitaria: aspectos clave y mejoras. *Revista Científica Unanchay*, 4(2), 148-160
doi: https://doi.org/10.64424/rcu42202586

Introducción

La digitalización del sector salud ha transformado de manera radical la gestión de los datos clínicos mediante la adopción de historias clínicas electrónicas, plataformas de telemedicina y dispositivos médicos interconectados. Estas tecnologías han mejorado la eficiencia y la atención al paciente, pero también han incrementado los puntos de exposición a riesgos de seguridad. En consecuencia, hospitales, clínicas y centros médicos se han convertido en objetivos prioritarios de ciberataques sofisticados, como accesos no autorizados, robo de información y ransomware, que generan consecuencias críticas para los pacientes y para la continuidad de los servicios.

Ante este panorama, la arquitectura Zero Trust (ZTA) se ha posicionado como un enfoque relevante bajo la premisa de “nunca confiar, siempre verificar”. Según Rose et al. (2020), su funcionamiento se basa en la validación continua de identidad, contexto y estado del dispositivo antes de otorgar acceso. De acuerdo con Adahman et al. (2022), principios como el mínimo privilegio, la autenticación permanente y la microsegmentación limitan los movimientos laterales y reducen la superficie de ataque, mientras que Gambo & Almulhem (2025) resaltan su utilidad en infraestructuras críticas altamente expuestas.

En cuanto a sus variantes, Dhiman et al. (2024) señalan que Zero Trust Network Access (ZTNA) y Secure Access Service Edge (SASE) representan los modelos más utilizados, diferenciándose en sus capacidades de control y complejidad de implementación. Asimismo, Edo et al. (2022) agregan que la selección depende del contexto organizacional y de las posibilidades de integración tecnológica de cada institución.

La literatura reciente confirma que el sector salud se encuentra entre los más afectados por incidentes de seguridad, lo que refuerza la necesidad de arquitecturas robustas y verificables como Zero Trust. Según HIPAA Journal (2025), los hospitales figuran entre los principales blancos de ataques que comprometen datos médicos sensibles. En esa misma línea, estudios como el de Tomlinson et al. (2024) muestran que la aplicación de autenticación multifactor y auditoría exhaustiva reduce de manera considerable los accesos indebidos, mientras que George et al. (2025) destacan que la segmentación de redes críticas y el cifrado integral incrementan la resiliencia frente a amenazas en entornos con dispositivos médicos interconectados.

 ISSN: 2953-6707

Desde un enfoque institucional, informes como el de KPMG (2015) advierten que, además de adoptar Zero Trust, resulta imprescindible modernizar sistemas heredados y fortalecer la capacitación del personal. En la misma línea, Wang et al. (2024) propusieron un modelo híbrido que integra blockchain y Zero Trust para descentralizar identidades y proteger datos clínicos mediante segmentación criptográfica. De manera complementaria, Koralla (2025) planteó soluciones basadas en autenticación continua y control de acceso contextual, mientras que Raheman (2024) enfatizó la necesidad de evolucionar hacia marcos resistentes a la computación cuántica mediante criptografía avanzada y biometría reforzada.

En síntesis, el aumento de incidentes que comprometen datos clínicos y las limitaciones de los modelos de seguridad perimetral refuerzan la urgencia de implementar enfoques más sólidos como Zero Trust en el sector sanitario. La pertinencia del estudio se justifica en la creciente frecuencia y magnitud de estos ataques. Informes del HIPAA Journal (2021, 2025) evidencian que hospitales y clínicas se encuentran entre los principales blancos de ciberataques, con millones de registros médicos expuestos en brechas recientes. De manera complementaria, el reporte de KPMG (2015) reveló que cerca del 80% de las organizaciones sanitarias encuestadas en EE.UU. habían sufrido incidentes de ciberseguridad, en gran parte debido a sistemas heredados, dispositivos inseguros y falta de procesos de protección integrados. A ello se suma la advertencia de Nadrag (2021), quien señala que los historiales clínicos robados poseen un alto valor en mercados ilícitos, lo que convierte a la información sanitaria en un objetivo prioritario para atacantes. Estas evidencias refuerzan la necesidad de examinar de manera sistemática los marcos Zero Trust, a fin de visibilizar logros y señalar áreas que requieren ajustes. En este contexto, surge la pregunta central de esta investigación: ¿Cuáles son los aspectos clave y las oportunidades de mejora de los marcos Zero Trust aplicados a la seguridad de la información en el sector salud?

En consecuencia, el objetivo general de esta investigación es analizar sistemáticamente la literatura científica sobre marcos Zero Trust en el sector salud, con el fin de identificar aspectos clave y oportunidades de mejora en la seguridad de la información sanitaria. Para ello, se plantean los siguientes objetivos específicos: (1) examinar cómo los marcos Zero Trust han sido aplicados o propuestos en el sector salud; (2) evaluar las fortalezas y debilidades reportadas en la literatura; (3) sistematizar los elementos comunes en su diseño e implementación; y (4) precisar oportunidades de mejora que contribuyan al fortalecimiento de la seguridad de la información sanitaria.

 ISSN: 2953-6707

Metodología

Se llevó a cabo una revisión sistemática bajo la guía PRISMA 2020 (Page et al., 2021), lo que garantizó transparencia y reproducibilidad en el proceso de búsqueda, selección y análisis de literatura sobre marcos de Zero Trust en el sector salud. La estrategia de búsqueda (Tabla 1) se aplicó en seis bases de datos académicas indexadas: MDPI, PubMed, IEEE Xplore, Google Scholar, ScienceDirect y Scopus utilizando cadenas de búsqueda combinadas con operadores booleanos

Tabla 1

Estrategia de búsqueda bibliográfica

BASE DE DATOS	CADENA DE BÚSQUEDA	REGISTROS
MPDI, PUBMED, IEEE XPLORE, RESEARCH GATE, GOOGLE ACADÉMICO, SCIENCE DIRECT	("zero trust" **OR** "zero trust architecture" **OR** "ZTNA") **AND** ("healthcare" **OR** "health sector") **AND** ("cybersecurity") **AND** ("evaluation" **OR** "comparison")	32
	("zero trust" **OR** "zero-trust architecture") **AND** "healthcare systems") **AND** (security **OR** cybersecurity **OR** "access control" **OR** "data protection")	51
	CANTIDAD	**83**

Nota. Autores, (2025)

Los criterios de inclusión y exclusión (Tabla 2) se definieron para asegurar la pertinencia, actualidad y alineación de los estudios con los objetivos de la investigación.

Tabla 2

Criterios de inclusión y exclusión

Criterios	Inclusión	Exclusión
Fuentes de información	Bases de datos académicas indexadas	Libros
Tiempo	Publicaciones entre los años 2020 a 2025.	Publicaciones anteriores a 2020
Idioma	Artículos en inglés	Artículos en otros idiomas
Área temática	Seguridad de la información en el sector salud	Artículos no relacionados con el tema
Acceso	Estudios de acceso libre	Estudios de pago o con DOI corrupto

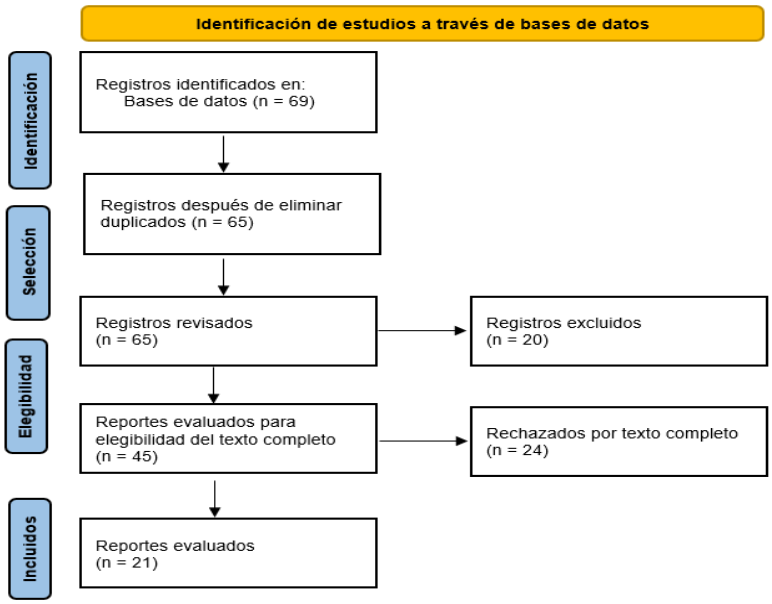
Nota. Autores, (2025)

 ISSN: 2953-6707

El cribado inicial identificó 69 registros. Tras eliminar duplicados, se revisaron 65, de los cuales 20 fueron descartados por no cumplir criterios de inclusión y 24 tras la revisión a texto completo, quedando 21 estudios finales (Figura 1).

Figura 1

Diagrama de flujo PRISMA



Nota. Autores, (2025)

En cuanto a la distribución geográfica, la mayoría de los estudios provienen de Estados Unidos, seguido por Canadá, Europa y Asia, lo que refleja que la investigación en Zero Trust en salud está más desarrollada en regiones con mayor madurez digital y experiencia en seguridad de la información (Figura 2)

Figura 2

Distribución de estudios por país

Nota. Autores, (2025)

 ISSN: 2953-6707

El análisis se llevó a cabo con un enfoque cualitativo-comparativo, orientado a identificar aspectos clave, fortalezas, debilidades y oportunidades de mejora en los marcos Zero Trust aplicados a la seguridad de la información sanitaria. Además, se consideró la calidad metodológica de los estudios incluidos en términos de claridad de objetivos, detalle de las métricas utilizadas y aplicabilidad de los resultados en entornos clínicos.

Resultados

Tema 1: Control de acceso y autenticación reforzada

La adopción de autenticación multifactor en el sector salud mostró un crecimiento considerable: del 34% en 2019 al 76% en 2025 (Mohile, 2025). En términos de efectividad, la autenticación de dos factores redujo accesos no autorizados en 67,9%, mientras que tres o más factores alcanzaron un 97,3% de reducción. La biometría se consolidó como mecanismo de alta eficacia, disminuyendo la escalación de privilegios en 92,7% y previniendo modificaciones no autorizadas en 98,3% (Sood et al., 2024).

Los sistemas de control de acceso contextual detectaron el 89,3% de intentos de uso indebido de credenciales válidas mediante análisis de patrones de comportamiento (Saha, 2025). En paralelo, la aplicación del principio de menor privilegio con provisión “just-in-time” redujo permisos permanentes en 91,7% y casos de abuso en 87,3%, con ventanas de acceso promedio de 4,3 horas (Saha, 2025). El control granular de acceso mediante atributos logró disminuir accesos indebidos en 97,8%, con una latencia mínima de 4,3 ms por consulta. Además, el enmascaramiento dinámico de datos se implementó en el 78,6% de las organizaciones encuestadas, reduciendo violaciones HIPAA relacionadas con exposición innecesaria en 93,7%.

Tabla 3

Síntesis de resultados sobre control de acceso y autenticación reforzada

Autor	Mecanismos	Resultados principales
Mobile (2025)	MFA	Adopción 76% en 2025 (34% en 2019)
Sood et al. (2024)	2FA/3FA+/biometría	2FA: -67,9% accesos indebidos; 3FA+: -97,3%; biometría: -92,7% escalación, -98,3% modificaciones
Saha (2025)	Autenticación contextual/JIT	Detección credenciales comprometidas: 89,3%; reducción permisos permanentes: 91,7%; abuso: -87,3%
	Control por atributos/enmascaramiento	-97,8% accesos indebidos, latencia 4,3 ms; enmascaramiento dinámico reduce violaciones HIPAA en 93,7%

Nota. Autores, (2025)

 ISSN: 2953-6707

Este nivel de adopción y efectividad refleja un compromiso creciente con la protección de la información sanitaria, reduciendo violaciones de datos clínicos y reforzando la confidencialidad e integridad de los registros.

Tema 2 : Arquitecturas adaptativas y segmentación clínica

En registros electrónicos de salud (EHR), un marco Zero Trust desplegado en entornos fog/edge con blockchain reportó un incremento en la tasa de finalización de tareas (85%, +15,29%) y una reducción en el tiempo medio de respuesta cercana al 39,66% (Kaur, 2025). En IoMT, se alcanzaron tasas de precisión de 99,84% y 98,1% en autenticación y monitoreo de dispositivos, lo que refuerza su potencial para diagnóstico y supervisión en tiempo real. No obstante, persisten limitaciones relacionadas con heterogeneidad tecnológica, dificultades de actualización y restricciones energéticas (Ahmed, 2025). En cuanto a políticas dinámicas, un modelo de segmentación y autorización basado en identidad logró una precisión del 92,7% en detección de amenazas internas (Ahmadi, 2025). Revisiones recientes resaltan la utilidad de motores de política contextuales apoyados en IA, aunque advierten que aún predominan prototipos experimentales (Zakhmi et al., 2025).

Respecto a escalabilidad, un marco en redes 5G alcanzó precisión superior al 97% en la toma de decisiones, manteniendo disponibilidad bajo alta carga, aunque con sobrecarga derivada de la verificación continua y complejidad en la calibración de umbrales (Alnaim, 2025). Finalmente, la microsegmentación se consolidó como práctica esencial para limitar movimientos laterales. Estudios de Kaur (2025), Alnaim (2025) y Shamsan (2024) muestran que la segmentación granular, soportada en SDN y blockchain, refuerza la seguridad entre dominios clínicos, aunque la integración con sistemas heredados sigue siendo un desafío.

Tabla 4

Síntesis de resultados sobre arquitecturas adaptativas y segmentación clínica

Autor	Contexto	Resultados principales
Kaur (2025)	EHR en fog/edge con blockchain	TCR 85% (+15,29%); -39,66% latencia
Ahmed (2025)	IoMT	Precisión 99,84% y 98,1% en monitoreo
Ahmadi (2025)	Políticas dinámicas	Detección amenazas internas: 92,7%
Zakhmi et al.(2025)	Revisión IA	Valor en políticas contextuales, limitación: prototipos
Alnaim (2025)	Escalabilidad en 5G	Precisión >97%; mantiene disponibilidad en alta carga
Kaur (2025), Alnaim (2025), Shamsan (2024)	Microsegmentación	Aislamiento granular de dominios clínicos, limitación: sobrecarga/integración

Nota. Autores, (2025)

 ISSN: 2953-6707

Las mejoras reportadas en TCR y reducción de latencia aseguran mayor disponibilidad de los historiales clínicos, mientras que la alta precisión en IoMT refuerza la confidencialidad de los datos generados por dispositivos médicos.

Tema 3: Ciberseguridad cuántica y criptografía

En redes 7G, un marco Zero Trust con técnicas cuánticas y post-cuánticas alcanzó una precisión del 87% en detección de anomalías, aunque enfrenta limitaciones relacionadas con madurez tecnológica, costes computacionales y compatibilidad con infraestructuras existentes (Ahmed, 2025).

La integración de blockchain permitió reforzar la trazabilidad e inmutabilidad de registros clínicos, aunque con latencia y problemas de gobernanza (Saleh, 2024). En IoT/IoMT, se alcanzaron valores de accuracy del 98% y recall del 96%, con latencias entre 100 y 800 ms (Aleisa, 2025). ZeroTrustBlock reportó interoperabilidad y trazabilidad con latencias de 150–500 ms (Thantharate & T., 2023), mientras que la incorporación de EigenTrust mejoró la resiliencia frente a nodos maliciosos, aunque mantuvo vulnerabilidad a colusión (Peepliwal, 2024).

En gestión de datos clínicos, Kaur (2025) mostró que la incorporación de blockchain en entornos fog/edge mejoró eficiencia y confiabilidad operativa, con registros inmutables y accesos controlados. Zhang (2025) propuso cifrado basado en atributos (ABE) para la nube, que ofrece control granular de acceso, pero presenta limitaciones en gestión de claves, privacidad y rendimiento.

Tabla 5

Síntesis de resultados sobre ciberseguridad cuántica y criptografía

Autor	Contexto	Resultados principales
Ahmed (2025)	7G cuántico	Precisión detección anomalías: 87%; limitaciones: costes, compatibilidad
Saleh (2024)	Blockchain en salud	Mayor trazabilidad, menor latencia y gobernanza
Aleisa (2025)	Blockchain IoT/IoMT	Accuracy 98%, Recall 96%, latencias 100 - 800 ms
Thabtharate & T. (2023)	ZeroTrustBlock	Interoperabilidad y trazabilidad; latencias 150 - 500 ms
Peepliwal (2024)	EigenTrust en blockchain	Resiliencia mayor; riesgo de colusión
Kaur (2025)	Fog/edge con blockchain	Eficiencia mayor, registros inmutables, control de acceso
Zhang (2025)	ABE en nube	Control granular; limitaciones: claves, privacidad, rendimiento

Nota. Autores, (2025)

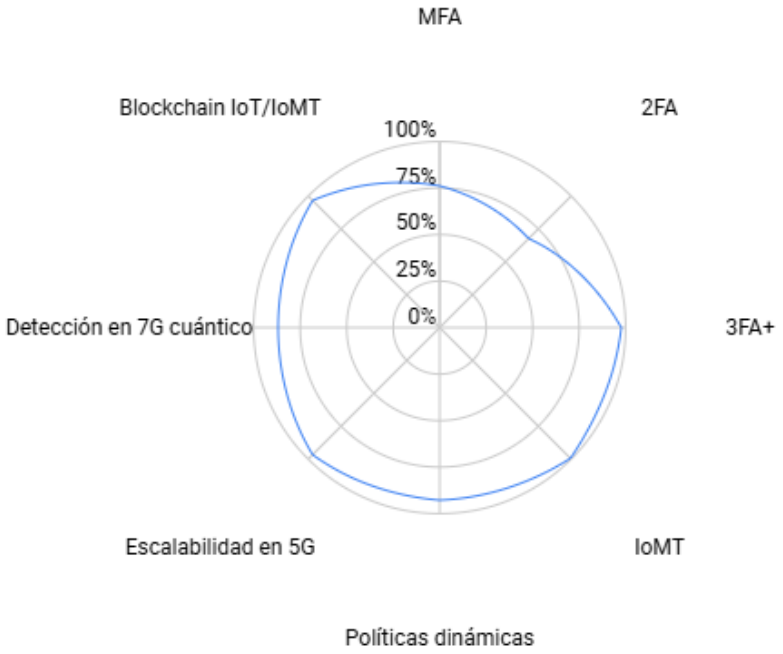
 ISSN: 2953-6707

La aplicación de estas técnicas de triangulación permitió obtener una valoración integral del impacto

Aunque las propuestas cuánticas alcanzan una precisión del 87%, se requieren validaciones en hospitales reales. Pese a la latencia en blockchain, sus beneficios en trazabilidad y auditoría son fundamentales para garantizar la integridad de la información sanitaria.

Figura 3

Comparación de efectividad de mecanismos Zero Trust en salud



Nota. Autores, (2025)

Tras el análisis de los resultados, el gráfico refleja que la mayoría de los mecanismos evaluados superan el 90% de efectividad, especialmente en IoMT, 3FA+ y blockchain. La adopción de MFA alcanza un 76% y el desempeño de 2FA se mantiene más limitado (67,9%), lo que señala la necesidad de mecanismos de autenticación más avanzados. En conjunto, la visualización evidencia tanto fortalezas consolidadas como áreas prioritarias de mejora en la seguridad de la información sanitaria.

ISSN: 2953-6707

Discusión

El análisis de los resultados confirma que los marcos Zero Trust aplicados en el sector salud han permitido avances significativos en seguridad de la información clínica, pero también revela limitaciones que condicionan su adopción práctica. Nuestros hallazgos coinciden con lo reportado por Mohile (2025), quien documenta un crecimiento sostenido de la autenticación multifactor en entornos hospitalarios, con reducciones de accesos indebidos similares a las observadas en esta revisión. De manera complementaria, Tomlinson et al. (2024) evidencian que el despliegue de controles de acceso basados en Zero Trust en instituciones sanitarias mejora la auditoría y reduce la exposición de credenciales, lo que respalda la relevancia de la autenticación contextual y la segmentación granular identificada en nuestro análisis.

En cuanto a la resiliencia frente a amenazas en infraestructuras críticas, George et al. (2025) destacan que la aplicación de Zero Trust en dispositivos médicos interconectados refuerza la continuidad asistencial y reduce la vulnerabilidad de los EHR, un resultado que se alinea con lo reportado en las investigaciones de Kaur et al. (2025), donde la combinación de Zero Trust y blockchain en entornos fog/edge incrementó la disponibilidad y trazabilidad de los registros clínicos. Sin embargo, estas evidencias también muestran que la latencia y los problemas de interoperabilidad persisten como retos estructurales.

Adicionalmente, Zakhmi et al. (2025) enfatizan que la integración de inteligencia artificial en motores de política adaptativos abre nuevas posibilidades de detección de amenazas, aunque advierten que la mayoría de propuestas aún se encuentran en fase experimental. Esta observación converge con lo señalado por Ahmed et al. (2025), quienes, al aplicar Zero Trust con técnicas cuánticas en entornos 7G, identifican limitaciones en compatibilidad y coste computacional, reflejando la brecha existente entre propuestas innovadoras y su viabilidad clínica real

Estos contrastes permiten concluir que, aunque Zero Trust ha demostrado efectividad superior al 90% en mecanismos como autenticación avanzada, microsegmentación y blockchain, su implementación en hospitales continúa condicionada por factores organizacionales, tecnológicos y económicos. Persiste la necesidad de estandarizar métricas comparativas (Sood et al., 2024) que permitan valorar de manera uniforme la eficacia y coste-beneficio de cada aproximación.

 ISSN: 2953-6707

Conclusiones

El estudio demuestra que los marcos Zero Trust aplicados al sector salud ofrecen beneficios claros en autenticación multifactor, segmentación granular, monitoreo adaptativo y trazabilidad criptográfica, alcanzando en la mayoría de los casos tasas de efectividad superiores al 90%. No obstante, su consolidación se ve limitada por la interoperabilidad con sistemas heredados, la latencia de la verificación continua, la inmadurez de tecnologías emergentes y la ausencia de métricas comparables que permitan evaluar resultados de manera uniforme.

De la evidencia analizada se desprenden aspectos clave que deben considerarse en futuras implementaciones: gestión estricta de identidades, autenticación contextual, segmentación de recursos críticos, monitoreo con telemetría y uso de criptografía resiliente. Estos elementos constituyen una base de referencia práctica para fortalecer la seguridad de la información sanitaria. El aporte de esta revisión radica en ofrecer una síntesis crítica que visibiliza avances y carencias, y que orienta investigaciones futuras hacia validaciones en hospitales reales, estudios de coste-beneficio e impacto organizacional. En conjunto, los hallazgos confirman que Zero Trust es una estrategia viable para reforzar la confidencialidad, integridad y disponibilidad de los datos clínicos, incrementando la confianza en los sistemas digitales de salud.

Referencias

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Computers & Security, 122, 102911. https://doi.org/10.1016/j.cose.2022.102911

Ahmadi, S. (2025). Autonomous Identity-Based Threat Segmentation for Zero Trust Architecture. Cyber Security And Applications, 100106. https://doi.org/10.1016/j.csa.2025.100106

Ahmed, S., Shihab, I. F., & 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

Aleisa, M. A. (2025). Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. IEEE Access, 1. https://doi.org/10.1109/access.2025.3529309

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

 ISSN: 2953-6707

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors, 24(4), 1328. https://doi.org/10.3390/s24041328

Edo, O. C., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal Of Emerging Technology And Advanced Engineering, 12(7), 140-147. https://doi.org/10.46338/ijetae0722_15

Gambo, M., Almulhem A. (2025). Zero Trust Architecture: A Systematic Literature Review. https://doi.org/10.48550/arXiv.2503.11659

George, N. A. A., Ogundipe, N. A. O., & Bello, N. A. B. (2025). Cybersecurity In healthcare systems: safeguarding electronic health records (EHRs) and medical devices against emerging cyber threats. World Journal Of Advanced Research And Reviews, 25(2), 2249-2262. https://doi.org/10.30574/wjarr.2025.25.2.0592

HIPAA Journal. (30 de enero de 2025). 2024 Healthcare Data Breach Report. https://www.hipaajournal.com/2024-healthcare-data-breach-report/

HIPAA Journal. (30 de diciembre de 2021). Largest Healthcare Data Breaches of 2021. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/

KPMG. (2015). HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increassed Capabilities. https://kpmg.com/

Kaur, N., Mittal, A., Lilhore, U. K., Simaiya, S., Dalal, S., Saleem, K., & Ghith, E. S. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP Journal On Wireless Communications And Networking, 2025(1). https://doi.org/10.1186/s13638-025-02431-6

Koralla, N. L. N. G. (2025). Zero Trust Architecture: A Comprehensive Framework for Modern Data Security. International Journal Of Advanced Research In Science Communication And Technology, 390-405. https://doi.org/10.48175/ijarsct-24449

Nadrag P. (3 de febrero de 2021). Stolen Patient Records a Hot Commodity on the Dark Web. https://capsuletech.com/blog/stolen-patient-records-a-hot-commodity-on-the-dark-web

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

 ISSN: 2953-6707

Peepliwal, A. K., Pandey, H. M., Prakash, S., Chowhan, S. S., Kumar, V., Sharma, R., & 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. https://doi.org/10.1016/j.bcra.2024.100232

Raheman, F. (2024). From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. Journal Of Computer And Communications, 12(03), 252-282. https://doi.org/10.4236/jcc.2024.123016

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain Research And Applications, 5(3), 100193. https://doi.org/10.1016/j.bcra.2024.100193

Thantharate, P., & Thantharate, A. (2023). ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. Big Data And Cognitive Computing, 7(4), 165. https://doi.org/10.3390/bdcc7040165

Tomlinson, E. W., Abrha, W. D., Kim, S. D., & Ortega, S. A. (2024). Cybersecurity Access Control: Framework Analysis in a Healthcare Institution. Journal Of Cybersecurity And Privacy, 4(3), 762-776. https://doi.org/10.3390/jcp4030035

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. Journal Of King Saud University - Computer And Information Sciences, 36(4), 102031. https://doi.org/10.1016/j.jksuci.2024.102031

Zakhmi, K., Ushmani, A., Mohanty, M. R., Agrawal, S., Banduni, A., & Kakatum, S. R. (2025). Evolving Zero Trust Architectures for AI-Driven Cyber Threats in Healthcare and Other High-Risk Data Environments: A Systematic Review. Cureus. https://doi.org/10.7759/cureus.85446

Mohile, N. K. (2025). Securing the healthcare ecosystem: Zero trust architecture protecting patient data across multiple access points. World Journal Of Advanced Engineering Technology And Sciences, 15(3), 371-378. https://doi.org/10.30574/wjaets.2025.15.3.0563

Sood, N., Parlapalli, R., Sharma, P., & Kashyap, R. (2024). Application of zero trust model in preventing medical errors. Frontiers In Health Services, 4. https://doi.org/10.3389/frhs.2024.1453804

Saha, N. S. (2025). Zero-trust database systems: The new frontier in data security. World Journal Of Advanced Research And Reviews, 26(1), 829-841. https://doi.org/10.30574/wjarr.2025.26.1.1112

 ISSN: 2953-6707