

Evaluación de estilos arquitectónicos y su impacto en los atributos de seguridad y disponibilidad para sistemas de información clínica

Evaluation of architectural styles and their impact on security and availability attributes in clinical information systems

Gonzalo Fabian Barrionuevo Escobar¹, Christian Fernando Barragán Quizhpe², Flor Gabriela Soliz Poveda³, Alysson Valeria Urrea Camacho⁴, Andrea Coraima Espin Lasso⁵, Amanda Cristina Carlosama Calderon⁶

Cita:

Barrionuevo Escobar, G. F., Barragán Quizhpe, C. F., Soliz Poveda, F. G., Urrea Camacho, A. V., Espin Lasso, A. C., & Carlosama Calderon, A. C. (2026). Evaluación de estilos arquitectónicos y su impacto en los atributos de seguridad y disponibilidad para sistemas de información clínica. *Salud ConCiencia*, 5(2), e106.

Recibido: 02/07/2026

Revisado: 13/07/2026 al 08/10/2026

Corregido: 15/10/2026

Aceptado: 19/10/2026

Publicado: 26/10/2026

Licencia:

Los contenidos de este artículo están bajo una licencia de Creative Commons Attribution 4.0 International (CC BY 4.0). Los autores conservan los derechos morales y patrimoniales de sus obras.

The contents of this article are under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. The authors retain the moral and patrimonial rights of their works.

1-2 Universidad Estatal de Bolívar (UEB), 3-6 Investigador Externo

¹gonzalo.barrionuevo@ueb.edu.ec, ²cbarragan@ueb.edu.ec, ³florbioquim@hotmail.com, ⁴alysson.urrea@iess.gob.ec, ⁵acoraimaespinl@gmail.com, ⁶accarlosamac29@gmail.com

¹0009-0002-1974-8046, ²0000-0003-4699-9553, ³0009-0009-1578-5748, ⁴0009-0001-6629-6444, ⁵0009-0003-8248-4925, ⁶0009-0007-8252-4287

Resumen: Los sistemas de información clínica (CIS) manejan datos médicos críticos, enfrentando el desafío constante de equilibrar la alta disponibilidad de los servicios con la máxima seguridad y privacidad de la información. El estilo arquitectónico subyacente dicta cómo se abordan estos atributos de calidad. Se aplicó la metodología PRISMA para realizar una revisión sistemática de la literatura reciente, evaluando los impactos de estilos arquitectónicos como monolítico, Arquitectura Orientada a Servicios (SOA), Microservicios (MSA) y arquitecturas descentralizadas (Blockchain) en el entorno de la salud. Los hallazgos sugieren la implementación de modelos híbridos que combinen la escalabilidad de los microservicios con la inmutabilidad de Blockchain y enfoques Zero-Trust para el desarrollo de nuevos ecosistemas hospitalarios. La arquitectura de microservicios domina actualmente por su capacidad para garantizar la disponibilidad continua, pero requiere obligatoriamente de tecnologías complementarias criptográficas y de control de acceso granular para mitigar las vulnerabilidades de seguridad inherentes a los sistemas distribuidos.

Palabras clave: Arquitectura de software, microservicios, blockchain, seguridad, disponibilidad, sistemas de información clínica.

Abstract: Clinical information systems (CIS) handle critical medical data, facing the constant challenge of balancing high service availability with maximum information security and privacy. The underlying architectural style dictates how these quality attributes are addressed. The PRISMA methodology was applied to conduct a systematic literature review, evaluating the impacts of architectural styles such as monolithic, Service-Oriented Architecture (SOA), Microservices (MSA), and decentralized architectures (Blockchain) in the healthcare environment. Findings suggest implementing hybrid models combining the scalability of microservices with the immutability of Blockchain and Zero-Trust approaches for developing new hospital ecosystems. Microservices architecture currently dominates due to its ability to guarantee continuous availability, but it obligatorily requires complementary cryptographic technologies and granular access control to mitigate the security vulnerabilities inherent in distributed systems.

Keywords: Software architecture, microservices, blockchain, security, availability, clinical information systems

INTRODUCCIÓN

La revolución digital ha transformado radicalmente la prestación de servicios de salud, impulsando la adopción masiva de Registros Médicos Electrónicos (EHR), dispositivos médicos interconectados y plataformas de telemedicina. En la actualidad, los Sistemas de Información Clínica (CIS) constituyen el núcleo operativo indiscutible de las instituciones médicas. La gestión de esta inmensa cantidad de información heterogénea impone exigencias técnicas sumamente rigurosas: requiere garantizar una disponibilidad constante para respaldar decisiones médicas críticas en tiempo real, mientras se salvaguarda la privacidad y seguridad de datos altamente sensibles frente a un panorama creciente de amenazas cibernéticas y normativas regulatorias estrictas. (Alorbany et al., 2025)

Tradicionalmente, gran parte de los ecosistemas hospitalarios fueron construidos bajo arquitecturas monolíticas. Aunque este enfoque centralizado facilitaba el desarrollo, las pruebas y el despliegue inicial, en la actualidad presenta limitaciones severas frente a la creciente demanda de procesamiento y almacenamiento. Los sistemas monolíticos exhiben un alto nivel de acoplamiento interno que dificulta la escalabilidad horizontal y los hace susceptibles a puntos únicos de fallo. En estos entornos, un error o la saturación en un solo módulo puede requerir el reinicio completo de la aplicación, comprometiendo la disponibilidad de servicios vitales para la atención del paciente (Dragoni et al., 2017)

Para mitigar estos problemas estructurales, la ingeniería de software ha liderado una transición ineludible hacia paradigmas distribuidos, tales como la Arquitectura Orientada a Servicios (SOA), las arquitecturas

modulares y, de manera prominente, la arquitectura de microservicios (MSA). La adopción de microservicios permite descomponer aplicaciones clínicas complejas en componentes independientes y funcionalmente aislados, lo que mejora drásticamente la resiliencia organizativa y la tolerancia a fallos. A través de la contenerización y las herramientas de orquestación en la nube, los hospitales pueden escalar servicios específicos como portales de telemedicina, sistemas de facturación o motores de procesamiento de imágenes de manera dinámica según la demanda (Bathelt et al., 2025).

Sin embargo, esta evolución arquitectónica no está exenta de compromisos significativos. Si bien la descentralización maximiza la disponibilidad y la agilidad de los despliegues, expande exponencialmente la superficie de ataque del sistema. A diferencia de los monolitos protegidos por un único perímetro de seguridad, en las arquitecturas basadas en microservicios cada interfaz de programación de aplicaciones (API) y canal de comunicación inter-servicio se convierte en un vector potencial de intrusión, exigiendo modelos de seguridad mucho más granulares y complejos (Rameshreddy Katkuri, 2025).

Ante estos desafíos, la literatura reciente resalta la necesidad de integrar tecnologías complementarias para proteger la integridad y privacidad del dato médico en entornos distribuidos. Paradigmas como Zero-Trust Architecture (ZTA), la tecnología Blockchain y el almacenamiento direccionable por contenido están siendo evaluados para garantizar que la información no solo esté disponible, sino que sea inmutable y esté controlada exclusivamente por el paciente a través de contratos inteligentes y mecanismos criptográficos avanzados. Asimismo, el uso de estándares de interoperabilidad semántica, como HL7 FHIR, se ha vuelto crucial para unificar estos servicios dispares de manera estandarizada (Amanna & Shinde, 2025a)

METODOLOGÍA

Criterios de Inclusión

Para la selección de artículos científicos utilizados en esta investigación, se establecieron criterios de inclusión con el objetivo de garantizar la calidad, pertinencia y actualidad de la información analizada.

En este sentido se incluyeron únicamente estudios que cumplieron con las siguientes condiciones:

Artículos científicos publicados entre los años 2021 y 2026, asegurando la actualidad de la información.

Investigaciones relacionadas con la arquitectura de software, incluyendo estilos como microservicios, SOA y arquitecturas distribuidas.

Estudios enfocados en el ámbito de la salud, especialmente en sistemas de información clínica.

Artículos que analicen atributos de calidad, tales como seguridad, disponibilidad, rendimiento y escalabilidad

Publicaciones indexadas en bases de datos académicas reconocidas.

La aplicación de estos criterios permitió seleccionar estudios relevantes y confiables, asegurando la validez de la información utilizada en el desarrollo de la investigación.

Criterios de exclusión

Se excluyeron aquellos estudios que no cumplieran con los criterios establecidos, tales como:

Artículos publicados antes del año 2021

Documentos que no estuvieran relacionados con el ámbito de la salud o sistemas de información clínica.

Estudios que no abordaran aspectos de arquitectura de software o atributos de calidad.

Fuentes no científicas, como blogs, páginas web sin respaldo académico o documentos sin autor identificado.

Artículos duplicados o con acceso restringido al texto completo.

Estrategia de Búsqueda

La estrategia de búsqueda se diseñó de acuerdo con las recomendaciones PRISMA 2020 para garantizar la transparencia, exhaustividad y reproducibilidad en la identificación de estudios sobre estilos arquitectónicos y su impacto en la seguridad y disponibilidad de sistemas de información clínica. Se definieron tres bloques conceptuales principales: 1. Estilos arquitectónicos (microservicios, modulares, descentralizadas, SOA); 2. sistemas clínicos (EHR, HIS); y 3. atributos de calidad (seguridad, disponibilidad, privacidad).

Se consultaron bases de datos especializadas en ingeniería de software y salud: IEEE Xplore, Scopus, PubMed y Google Scholar, seleccionadas por su cobertura de publicaciones en arquitecturas de software aplicadas a EHR y HIS, como se evidencia en los registros recuperados, contenido centrado a microservicios en registros dentales (Arcila-Díaz & Valdivia, 2022); arquitecturas modulares en dominio médico (Bathelt et al., 2025); espacios de datos descentralizados (Klementi et al., 2024).

Las cadenas de búsqueda utilizaron operadores booleanos, términos controlados y sinónimos en inglés. Se priorizaron publicaciones 2016-2026 con acceso directo sin pasar por pasarelas de pagos. De forma específica, la búsqueda se realizó de esta manera:

IEEE Xplore/Scopus: ("software architecture" OR "architectural style" OR "architectural pattern" OR microservices OR "modular architecture") AND ("clinical information system" OR "health information system" OR EHR OR HIS) AND (security OR availability OR privacy).

PubMed: ("Electronic Health Records"[Mesh] OR "Health Information Systems") AND ("Software Architecture" OR microservices) AND (Security OR Availability).

Inicialmente se recuperaron 48 fuentes de información relevantes de estas fuentes, filtrando duplicados y aplicando límites de tiempo (2016-2026) y de idioma (inglés/español). Esta estrategia se llevó a cabo el 14 de abril de 2026, llevando un registro de fechas, cadenas exactas y resultados como base para la realización de un informe siguiendo el modelo PRISMA.

Proceso de selección

El proceso de selección de la evidencia científica se ejecutó bajo los lineamientos de la declaración PRISMA. Este método garantiza que la selección de artículos sea transparente, sistemática y reproducible, minimizando el sesgo del investigador. Este se dividió en 4 fases:

Fase 1:

Se realizó una búsqueda exhaustiva en bases de datos de alto impacto técnico y científico: IEEE Xplore, ScienceDirect, Scopus y Google Scholar. Se utilizaron operadores booleanos (AND, OR) para combinar términos como "Software Architecture", "Clinical Information Systems", "Cybersecurity", "Availability". En esta etapa inicial, se identificaron un total de 48 registros potenciales. Cuales fueron exportados a un gestor bibliográfico para detectar y eliminar duplicados.

Fase 2:

Se evaluaron los títulos y resúmenes de los artículos identificados. Se aplicó un filtro de relevancia para descartar estudios que, aunque trataban sobre arquitecturas de software, no se centraban en el dominio crítico de la salud o no analizaban específicamente los atributos de calidad de seguridad y disponibilidad. Aquellos artículos que carecían de rigor técnico o que no habían sido publicados en los últimos 5 años fueron excluidos en esta.

Fase 3:

Se procedió a la revisión a texto completo de los artículos preseleccionados. Para determinar su inclusión definitiva, se aplicaron criterios de evaluación técnica, verificando que los estudios aportaran datos sobre:

Comparativas de rendimiento entre microservicios y monolitos.

Modelos de seguridad aplicados a la nube clínica.

Protocolos de autenticación.

Fase 4:

Finalmente, se seleccionaron 29 artículos que cumplieron con todos los estándares de calidad. Estos estudios constituyen la base documental para el análisis de resultados, destacando investigaciones recientes como las de (Mehrtak et al., 2021) y (Amanna & Shinde, 2025b), las cuales aterrizan conceptos de Zero Trust y seguridad en la nube en entornos hospitalarios reales.

Extracción de Datos

Tabla 1

Tabla de resultados del manuscrito

oprule ID	Requisito / Categoría	Contexto / Referencia	Hallazgos Clave
01	Disponibilidad, Autenticación, Integridad, Confidencialidad	PHR Integrado (Estudio [20])	Fuerte en identificar requisitos, pero carece de un modelo de referencia claro.
02	Confidencialidad, Integridad, Compartición Segura	Blockchain para interoperabilidad de EHR (Estudio [21])	Prioriza la privacidad del paciente y la integridad de los datos mediante descentralización.
03	Confidencialidad, Integridad, Disponibilidad	Tecnología EHR general	Analiza problemas de seguridad, pero no ofrece recomendaciones específicas para implementarlas.
04	Acceso, Emergencia, Anonimización, Auditoría	Revisión general de requerimientos	Identifica brechas de investigación y soluciones existentes para requisitos de EHR.

Tabla 2

Tabla de resultados del manuscrito

oprule Requisito	Módulo Analizado	Resultado	Evidencia
Acceso	e-SUS APS Management	Met	El modelo se basa en roles (perfiles profesionales de médicos/enfermeros).
Auditoría	Base de datos interna	Met	Obligatorio registrar justificación al acceder a datos fuera de horas de atención.
Anonimización	Vista del Ciudadano	Not Met	No se eliminan datos personales (PHI) como CPF o teléfono.
Integridad	No asignado	Not Met	Los datos no están cifrados por defecto; la responsabilidad recae en el administrador municipal.
Consentimiento	Módulo Ciudadano	Met	Opt-out: el ciudadano debe solicitar explícitamente el bloqueo de compartir datos.
Logoff Automático	Configuración de Seguridad	Met	Existe un timeout configurable para sesiones inactivas.

Categorías de Seguridad (Security Requirements):

Audit Control: ¿El sistema registra quién accede a qué?

Integrity: ¿Tiene el sistema mecanismos contra alteraciones no autorizadas?

Secure Transmission: ¿La información viaja cifrada?

Authentication: ¿Cómo verifican la identidad del usuario (contraseñas, biometría, MFA)?

Automatic Logoff: ¿Se cierra la sesión sola si el usuario se va?

Categorías de Privacidad (Privacy Requirements):

Access Control: ¿Quién tiene permiso para ver qué datos?

Emergency Access: ¿Existe un protocolo "Break-the-Glass" para emergencias?

Anonymization: ¿Se eliminan datos personales (PII) para investigación?

Consent: ¿El paciente tiene control sobre compartir sus datos?

RESULTADOS Y DISCUSIÓN

Se realizó el proceso de identificación, filtrado y selección de artículos científicos siguiendo la metodología PRISMA 2020. Como resultado, obtuvieron 29 estudios relevantes que cumplieron con todos los criterios establecidos.

Tabla 3

Tabla de resultados del manuscrito

oprul N	Autores, fecha	Revista	Lugar	Estilo arquitectónico	Aporte Principal
1	Arcila-Díaz & Valdivia (2022)	International Journal of computing	Colombia	Microservicios	Mejora de disponibilidad en registros médicos
2		Cureus	Estados Unidos	EHR Security	Riesgos y vulnerabilidades en bases de datos clínicos
3		Frontiers in Medicine	Estonia	Arquitectura descentralizada	Espacios de datos médicos distribuidos
4	Boda & Immaneni (2021)	UERET	India	Kubernetes + Microservicios	Estabilidad y seguridad clínica
5		Journal of Medicine Systems	Alemania	Arquitectura Modular	Aplicaciones modulares en salud
6	Mehrtak et al. (2021)	Journal of Medicine and life	Iran	Cloud Computing	Seguridad en la nube medica
7	Remolina Medina (2022)	Revistas Científicas Anfibios	Colombia	Blockchain	Privacidad y contratos inteligentes
8		IEEE cloud Computing	Italia	Microservicios	Migración desde monolitos
9	Sharma & Chaturvedi (2021)	ESP JETA	India	Cloud Services	Optimización de escalabilidad
10	Dragoni et al.(2017)	Springer	Italia	Microservicios	Evolución y limitación arquitectónicas

Impacto en la Disponibilidad y Escalabilidad

Este apartado referente al impacto en la disponibilidad y escalabilidad es un factor crítico especialmente en el apartado de sistemas de información clínica, donde la continuidad del servicio y la capacidad de adaptación es esencial y en ciertos caso de vida o muerte, se evidencia el uso de diversos estilos arquitectónicos en este tipo de proyectos donde marcan la funcionalidad y una influencia directa en estos proyectos, esto condiciona tanto la resiliencia del sistema como la capacidad de crecimiento.

Selección del estilo arquitectónico

Al hablar de la disponibilidad esta se relación directamente con la capacidad del sistema de mantenerse operativo aun cuando existan fallos, interrupciones o incluso incrementos de la demanda por lo que para este aspecto se presentan estilos arquitectónicos con comportamientos diferenciados, como son:

Arquitectura monolítica

Esta arquitectura destaca por un alto acoplamiento entre sus diversos componentes lo que permite que si existe un fallo en un modelo compromete la funcionalidad del sistema, así también según (Dragoni et al., 2017) recientemente se señala que este enfoque presenta limitación en términos de tolerancia a fallos dado que ante la recuperación después de errores suele requerir el reinicio completo del sistema lo que lo hace poco usable en el contexto médico.

Arquitectura de microservicios

Esta arquitectura introduce el enfoque desacoplado basado en servicios independientes, esta mejora significativamente la disponibilidad puesto que cada servicio puede estar desplegado, escalado y recuperado de manera autónoma ante cualquier fallo lo que permite contener cualquier fallo sin comprometer el funcionamiento del sistema completo.

Según (Taibi et al., 2017) destaca que el uso de patrones como circuit breakers o retries y balance de carga que reduce el tiempo de inactividad, esto permite la implementación de redundancia y replicación de servicios para mantener la operabilidad de forma continua. En el contexto medico la convierte en la arquitectura que permite garantiza el acceso continuo a los módulos críticos como el agendamiento de consultados o el apartado de resultados de laboratorio.

Así mismo si nos referimos a las arquitecturas basadas en eventos se puede decir que estas están orientadas a ser incrementales en aspectos como la disponibilidad aun si existe algún modulo caído. Según (Kleppmann, s. f.) estos sistemas y su uso destacan porque permiten absorber fallos parciales sin la interrupción completa en el flujo de trabajo y el de información, esto es calve para el sistema al hablar de sistemas con alta dependencia de datos.

Ahora si nos referimos a la escalabilidad en los microservicios se puede decir que el escalado horizontal

permite la replicación de forma independiente según la demanda esto implica que es escalado automática, la gestión de contenedores y el balanceo dinámico de carga. Según (Sharma & Chaturvedi, 2021) estos aspectos mejoran significativamente la eficiencia operativa, así como la adaptación del sistema en tiempo real lo que es crucial para sistemas de la índole médica.

Impacto en la Seguridad y Privacidad

El impacto de la seguridad y la privacidad en la arquitectura de sistemas clínicos es sólo un requerimiento técnico, sino una barrera crítica que determina la viabilidad legal y ética de cualquier software de salud. Este impacto se analiza desde diversas dimensiones tecnológicas:

Descentralización y control del paciente (privacidad)

Uno de los mayores impactos analizados es el cambio del paradigma hacia la soberanía del dato. Tradicionalmente, los sistemas han sido silos centralizados dónde el paciente pierde el control.

Impacto: El uso de redes descentralizadas y almacenamiento direccionable por contenido permite que los datos no residen en una única base de datos vulnerable.

Klementi propone una arquitectura de referencia para espacios de datos de salud personales utilizando redes descentralizadas, lo que mitiga el riesgo de filtraciones masivas centralizadas (Klementi et al., 2024). Por otro lado, Remolina Medina destaca cómo los contratos inteligentes en Blockchain garantizan que solo el paciente autorice quién accede a su información, impactando positivamente en la autonomía de la privacidad. (Remolina Medina, 2022)

Ampliación de la superficie de ataque (Seguridad en microservicios)

Si bien los microservicios mejoran la disponibilidad, introducen retos de seguridad debido a la comunicación constante entre servicios a través de la red.

Impacto: Cada punto de conexión (API) es un punto potencial de intrusión. Esto obliga a pasar de una seguridad perimetral (un "muro" alrededor del sistema) a una seguridad granular.

Basil revisa las preocupaciones de seguridad inherentes a las bases de datos de registros de salud, señalando que la fragmentación de datos requiere protocolos de cifrado más robustos. (Basil et al., 2022) Boda y Immaneni mencionan que el uso de Kubernetes para orquestar estos microservicios añade capas de seguridad necesarias, pero también complejidad en la configuración de políticas de red. (Boda & Immaneni, 2021)

APLICACIONES PRÁCTICAS

Los hallazgos de esta revisión permiten identificar aplicaciones prácticas que pueden ser puestas en marcha hoy en día en hospitales, clínicas y centros de diagnóstico que dependen de sistemas de información clínica con operación continua. En estos entornos, la arquitectura de microservicios puede usarse para la separación de módulos críticos, tales como: admisión, agenda médica, laboratorio, farmacia e historial clínico; de modo que una falla puntual no interrumpa por completo la prestación de servicios, mejorando así la disponibilidad del sistema para la realización de operaciones.

De igual manera, la incorporación de mecanismos de seguridad granular, como autenticación multifactor, control de acceso por roles, cifrado de comunicaciones y detalles de auditoría permanente, constituye una aplicación directa para la protección de datos clínicos sensibles en arquitecturas distribuidas. A la par, la utilización de blockchain o esquemas descentralizados termina siendo especialmente útil en escenarios de interoperabilidad entre instituciones, donde se requiere una adecuada trazabilidad, integridad de registros y mayor control del paciente sobre el acceso a su información.

FUTURA LÍNEA DE APLICACIÓN

Como línea futura de investigación, resulta oportuno profundizar en modelos arquitectónicos híbridos que integren características como microservicios, blockchain y enfoques Zero-Trust dentro de ecosistemas hospitalarios ya implementados en entornos reales. Esta combinación podría ofrecer respuestas más equili-

bradas entre: escalabilidad, resiliencia, privacidad y defensa ante amenazas; pero, todavía requiere mayor evidencia empírica en materia de costos, complejidad de implementación, rendimiento y sostenibilidad en instituciones de salud con distintas capacidades en cuanto a los recursos tecnológicos.

CONCLUSIONES

La revisión de los estudios seleccionados evidencia que la elección del estilo arquitectónico influye de manera directa en la disponibilidad y la seguridad de los sistemas de información clínica. Las arquitecturas monolíticas ofrecen simplicidad operativa inicial, pero su elevado acoplamiento puede dificultar el escalado y la recuperación ante fallos. Las arquitecturas orientadas a servicios y, especialmente, los microservicios favorecen la modularidad, el despliegue independiente y la continuidad de componentes críticos, aunque estas ventajas dependen de una configuración y administración adecuadas.

En términos de seguridad y privacidad, la distribución de servicios amplía los puntos de acceso y las comunicaciones que deben protegerse. Por ello, la adopción de microservicios no garantiza por sí misma la confidencialidad ni la integridad de los datos clínicos: requiere controles complementarios, como autenticación multifactor, autorización granular basada en roles, cifrado de comunicaciones, auditoría y políticas de confianza cero (Zero Trust). Las soluciones descentralizadas y blockchain ofrecen mecanismos potencialmente útiles para la trazabilidad y el control de acceso, pero también introducen desafíos de interoperabilidad, gobernanza y complejidad técnica.

En consecuencia, la evidencia analizada respalda considerar arquitecturas híbridas adaptadas a los requisitos de cada institución, combinando la disponibilidad y escalabilidad de servicios desacoplados con controles de seguridad y mecanismos de trazabilidad. La selección no debe basarse únicamente en tendencias tecnológicas, sino en una evaluación explícita de criticidad clínica, tolerancia a fallos, capacidades de operación, protección de datos, interoperabilidad y recursos disponibles.

Los hallazgos proceden de una revisión documental y no de pruebas comparativas de rendimiento, disponibilidad o incidentes de seguridad en sistemas hospitalarios implementados. Por tanto, no permiten establecer una superioridad universal ni cuantificar mejoras atribuibles a un estilo determinado. Se recomienda que investigaciones posteriores validen las propuestas híbridas mediante prototipos y estudios de campo, utilizando indicadores reproducibles de disponibilidad, recuperación ante fallos, superficie de ataque, costos de operación y cumplimiento de requisitos de privacidad.

FINANCIACIÓN

La investigación no contó con financiamiento externo. El desarrollo del trabajo se apoyó únicamente en los recursos académicos institucionales proporcionados por la ESPOCH, especialmente el acceso a bases de datos científicas y material bibliográfico en línea, utilizados exclusivamente como soporte para la búsqueda y revisión de información.

CONFLICTO DE INTERESES

Los autores manifiestan que no presentan conflictos de intereses, ya sean financieros o no financieros, relacionados con la realización de esta investigación. Esta declaración se formula conforme a los principios de transparencia y divulgación promovidos por PRISMA 2020 para revisiones sistemáticas.

CONTRIBUCIÓN DE AUTORÍA

Tabla 4

Matriz de contribuciones CRediT (propuesta sujeta a confirmación)

Contribución	A1	A2	A3	A4	A5	A6
Conceptualización	X	X	X	X	X	X
Análisis formal	X	X	X	X	X	X
Investigación	X	X	X	X	X	X
Metodología	X	X	X	X	X	X
Recursos	X	X	X	X	X	X
Curación de datos	X	—	—	—	—	—
Redacción: borrador	X	X	X	X	X	X
Redacción: revisión y edición	X	X	X	X	X	X
Supervisión	X	—	—	—	—	—
Aprobación de versión final	X	X	X	X	X	X

A1–A6: autores en orden de firma. Asignación editorial propuesta; requiere validación.

REFERENCIAS

- Alorbany, A., Sheta, M., Hagag, A., Elshaarawy, M., Elharty, Y., & Fares, A. (2025). AI-Driven Electronic Health Records System for Enhancing Patient Data Management and Diagnostic Support in Egypt (arXiv:2502.05603; Versión 1). arXiv. <https://doi.org/10.48550/arXiv.2502.05603>
- Amanna, A., & Shinde, I. (2025a). Securing Generative AI in Healthcare: A Zero-Trust Architecture Powered by Confidential Computing on Google Cloud (arXiv:2511.11836). arXiv. <https://doi.org/10.48550/arXiv.2511.11836>
- Amanna, A., & Shinde, I. (2025b). Securing Generative AI in Healthcare: A Zero-Trust Architecture Powered by Confidential Computing on Google Cloud (arXiv:2511.11836). arXiv. <https://doi.org/10.48550/arXiv.2511.11836>
- Arcila-Díaz, J. C., & Valdivia, C. (2022). A Microservice-based Software Architecture for Improving the Availability of Dental Health Records. *International Journal of Computing*, 475-481. <https://doi.org/10.47839/ijc.21.4.2783>
- Basil, N. N., Ambe, S., Ekhtor, C., & Fonkem, E. (2022). Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus*, 14(10), e30168. <https://doi.org/10.7759/cureus.30168>
- Bathelt, F., Lorenz, S., Weidner, J., Sedlmayr, M., & Reinecke, I. (2025). Application of Modular Architectures in the Medical Domain—A Scoping Review. *Journal of Medical Systems*, 49(1), 27. <https://doi.org/10.1007/s10916-025-02158-3>
- Boda, V. V. R., & Immaneni, J. (2021). Healthcare in the Fast Lane: How Kubernetes and Microservices Are Making It Happen. *International Journal of Emerging Research in Engineering and Technology*, 2(3), 33-42. <https://doi.org/10.63282/3050-922X.IJERET-V2I3P104>
- Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: Yesterday, Today, and Tomorrow. En M. Mazzara & B. Meyer (Eds.), *Present and Ulterior Software Engineering* (pp. 195-216). Springer International Publishing. https://doi.org/10.1007/978-3-319-67425-4_12
- Klementi, T., Piho, G., & Ross, P. (2024). A reference architecture for personal health data spaces using decentralized content-addressable storage networks. *Frontiers in Medicine*, 11. <https://doi.org/10.3389/fmed.2024.1411013>
- Kleppmann, M. (s. f.). *Designing Data-Intensive Applications*. Recuperado 26 de abril de 2026, de <https://www.oreilly.com/library/view/designing-data-intensive-applications/9781491903063/>
- Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, 14(4), 448-461. <https://doi.org/10.25122/jml-2021-0100>
- Rameshreddy Katkuri. (2025). Revolutionizing healthcare with secure and scalable microservices. *World Journal of Advanced Research and Reviews*, 26(1), 1731-1739. <https://doi.org/10.30574/wjarr.2025.26.1.1235>
- Remolina Medina, C. E. (2022). Beneficios y limitaciones del Blockchain en contratos inteligentes en el sector salud. Una revisión de la literatura. *Revista Científica Anfibios*, 5(2), 57-71.
- Sharma, S., & Chaturvedi, R. (2021). Optimizing Scalability and Performance in Cloud Services: Strategies and Solutions. *ESP Journal of Engineering & Technology Advancements (ESP JETA)*, 1(2), 116-133.
- Taibi, D., Lenarduzzi, V., & Pahl, C. (2017). Processes, Motivations, and Issues for Migrating to Microservices Architectures: An Empirical Investigation. *IEEE Cloud Computing*, 4(5), 22-32. <https://doi.org/10.1109/MCC.2017.4250931>