innova SCIENCE JOURNAL ISSN:3091-1680

OM EDITORIAL

Artículo Científico

Modelo de ciberseguridad para la protección de historias clínicas electrónicas en un centro médico privado.

Cybersecurity model for the protection of electronic health records in a private medical center.

Nolasco-Paulino, Juan Gabriel[1]; Mateo-Salas, Gabriel Elías[2].

[1] Universidad Abierta para Adultos (UAPA); República Dominicana, Santo Domingo; https://orcid.org/0009-0002-6269-1006; 100079919@p.uapa.edu.do

[2] Universidad Abierta para Adultos (UAPA); República Dominicana, Santo Domingo; https://orcid.org/0009-0001-2132-7710; 100079662@p.uapa.edu.do

[1] Autor Correspondencia

https://doi.org/10.63618/omd/isj/v4/n2/277

Cita: Nolasco-Paulino, J. G., & Mateo-Salas, G. E. (2026). Modelo de ciberseguridad para la protección de historias clínicas electrónicas en un centro médico privado. Innova Science Journal, 4(2), 359-366. https://doi.org/10.63618/omd/isj/v4/n2/277

Recibido: 12/11/2025
Aceptado: 10/04/2026
Publicado: 30/04/2026

Resumen: El sector sanitario registra los costos más elevados derivados de brechas de datos a nivel global, situación que se agrava en instituciones con infraestructuras tecnológicas limitadas. El objetivo de esta investigación fue proponer un modelo integral de ciberseguridad para la protección de las historias clínicas electrónicas en un centro médico privado de Santo Domingo, período 2026–2027. Se empleó un enfoque cuantitativo descriptivo, aplicando un instrumento de 28 ítems en escala Likert de cuatro puntos a una muestra censal de 25 participantes del personal médico, administrativo y técnico; la confiabilidad fue evaluada mediante el coeficiente Alfa de Cronbach (α = 0.87). Los resultados evidenciaron un nivel de madurez de seguridad medio (media global = 3.05), con vulnerabilidades críticas en seguridad perimetral (media = 2.81) y monitoreo de eventos (media = 3.12). Se diseñó el Modelo Integral de Ciberseguridad para la Protección de Historias Clínicas Electrónicas, estructurado en cinco capas que integran control de acceso IAM/MFA, segmentación VLAN, escritorios virtuales VDI, monitoreo SIEM y respaldo cifrado. La implementación del modelo propuesto contribuye al fortalecimiento de la seguridad de la información clínica y al cumplimiento normativo en entornos sanitarios digitales.

Palabras clave: ciberseguridad; historia clínica electrónica; protección de datos; seguridad de la información; sector salud dominicano.

Abstract: The healthcare sector records the highest costs derived from data breaches globally, a situation exacerbated in institutions with limited technological infrastructure. The objective of this research was to propose an integral cybersecurity model for the protection of electronic health records (EHR) at a private medical center in Santo Domingo during the 2026–2027 period. A quantitative descriptive approach was used, applying a 28-item four-point Likert scale instrument to a census sample of 25 medical, administrative, and technical staff members; reliability was evaluated using Cronbach's alpha (α = 0.87). Results revealed a medium-level security maturity (overall mean = 3.05), with critical vulnerabilities in perimeter security (mean = 2.81) and event monitoring (mean = 3.12). The Integrated Cybersecurity Model for the Protection of Electronic Health Records was designed, structured in five layers integrating IAM/MFA access control, VLAN segmentation, VDI virtual desktops, SIEM monitoring, and encrypted backup. The proposed model contributes to strengthening clinical information security and regulatory compliance in medium-sized digital healthcare environments.

Keywords: cybersecurity; electronic health records; data protection; information security; Dominican healthcare sector.

1. Introducción

La transformación digital del sector salud ha permitido mejorar significativamente la gestión de la información clínica mediante la implementación de sistemas de historias clínicas electrónicas (HCE). La Organización Mundial de la Salud reconoce que la digitalización sanitaria representa uno de los pilares fundamentales para el fortalecimiento de los sistemas de salud a nivel global (World Health Organización, 2021), sin embargo, la digitalización de la información médica también ha incrementado la exposición de los sistemas de salud a amenazas cibernéticas, convirtiendo a las instituciones médicas en objetivos prioritarios de ataques informáticos.

IBM Security (2023) reporta que el costo promedio de una brecha de datos en el sector sanitario supera los USD 10 millones, siendo el más elevado entre todos los sectores analizados por doceavo año consecutivo, esta situación es consistente con lo señalado por Kruse et al. (2017), quienes documentaron que las amenazas cibernéticas en el sector salud han crecido sostenidamente y representan un riesgo crítico para la continuidad operativa de las instituciones médicas.

La información contenida en las HCE representa un activo crítico por su alto valor médico, legal y administrativo (Lian, 2020).

Entre las amenazas más frecuentes se encuentran ataques de ransomware, accesos no autorizados y fugas de información (Kortján et al., 2023). La Agencia de la Unión Europea para la Ciberseguridad confirma que el sector sanitario continúa siendo uno de los más afectados por incidentes de seguridad a nivel global (ENISA, 2023). En el contexto latinoamericano, muchas instituciones operan con infraestructuras tecnológicas heredadas y controles de seguridad limitados (Sendelj & Ognjanovic, 2022). La seguridad de los datos clínicos en entornos digitales exige una combinación de controles perimetrales y mecanismos de cifrado robustos (Urquijo Morales et al., 2023; Sivan & Zukarnain, 2021).

En la República Dominicana, el Ministerio de Salud Pública ha establecido la digitalización de los servicios de salud como prioridad dentro de su Estrategia Nacional de Salud Digital 2022–2030 (Ministerio de Salud Pública de la República Dominicana, 2022), sin embargo, investigaciones en el contexto latinoamericano evidencian que la adopción de HCE en instituciones de tamaño medio frecuentemente no va acompañada de controles de seguridad adecuados (Pérez & Gómez, 2020).

La adopción de marcos como ISO/IEC 27001 y el Marco de Ciberseguridad del NIST permite fortalecer la gestión de la seguridad mediante controles técnicos, organizacionales y procedimentales (ISO/IEC, 2022; NIST, 2020). Alasmary y Alshaikh (2021) señalan que los desafíos de ciberseguridad en sistemas de salud requieren soluciones integrales que combinen controles tecnológicos con una cultura organizacional orientada a la seguridad. Bada et al. (2019) destacan que las campañas de concientización son un complemento necesario para que los controles técnicos sean efectivos. Ahmad et al. (2021) sostienen que las organizaciones que adoptan estrategias de seguridad multi-capa logran reducir significativamente su exposición a incidentes. Investigaciones en el ámbito nacional evidencian que la protección de las HCE requiere una combinación de controles tecnológicos, políticas organizacionales y mecanismos de monitoreo continuo (Godoy Veas, 2025).

El objetivo de la presente investigación es proponer un modelo integral de ciberseguridad orientado a la protección de las historias clínicas electrónicas en un centro médico privado de Santo Domingo, República Dominicana, durante el período 2026-2027, alineado con estándares internacionales y adaptado a la realidad operativa del sector salud dominicano.

2. Materiales y Métodos

2.1 Diseño del estudio

La investigación se desarrolló bajo un enfoque cuantitativo de tipo aplicado, con un diseño descriptivo y no experimental, fue transversal, ya que la recolección de los datos se realizó en un único momento durante el período de investigación.

El diseño descriptivo permitió identificar las vulnerabilidades existentes en la infraestructura tecnológica, las políticas de acceso y las prácticas organizacionales relacionadas con la gestión de la información clínica. No existen aspectos de carácter ético que limiten la investigación; la participación fue voluntaria y los datos recopilados fueron tratados de forma anónima y confidencial.

2.2 Población y muestra

La población estuvo compuesta por el personal médico, administrativo y técnico del centro médico privado objeto de estudio. Se aplicó un muestreo censal, conformado por 25 participantes con interacción directa con los sistemas de información clínica, distribuidos en personal clínico (n=19), administrativo (n=5) y técnico de TI (n=1), los criterios de inclusión fueron: personal activo con acceso a los sistemas de HCE durante el período de estudio y con al menos tres meses de antigüedad en la institución.

2.3 Instrumento y técnicas de recolección de datos

Se utilizó un instrumento estructurado de 28 ítems basado en escala tipo Likert de cuatro niveles (1=Nunca, 2=Casi nunca, 3=Casi siempre, 4=Siempre). Las dimensiones evaluadas incluyeron: (a) Control de acceso y autenticación (P1–P7); (b) Gestión de dispositivos y red (P8–P14); (c) Seguridad perimetral (P15–P21); y (d) Monitoreo y cumplimiento (P22–P28). El instrumento fue validado mediante juicio de expertos. La confiabilidad fue evaluada mediante el coeficiente Alfa de Cronbach, obteniendo α = 0.87 global, lo que indica una consistencia interna buena (George & Mallery, 2003).

2.4 Procedimiento y análisis estadístico

El procesamiento y análisis de los datos se realizó mediante Microsoft Excel. Los métodos estadísticos incluyeron: (a) Coeficiente Alfa de Cronbach para la confiabilidad; (b) Estadística descriptiva (medias y desviaciones estándar) por dimensión; y (c) Análisis comparativo por perfil de usuario. La escala de interpretación de medias fue: 1.00–2.49 = Bajo; 2.50–3.24 = Medio; 3.25–4.00 = Alto.

3. Resultados

El análisis de los datos permitió identificar el nivel de madurez de seguridad de la información en el centro médico e identificar las principales vulnerabilidades asociadas a la protección de las HCE.

3.1 Confiabilidad del instrumento

La confiabilidad del instrumento fue evaluada mediante el coeficiente Alfa de Cronbach. En la Tabla 1 se presentan los valores obtenidos por dimensión.

Tabla 1.

Valores del coeficiente Alfa de Cronbach por dimensión

Dimensión	Ítems	α de Cronbach
D1: Control de Acceso y Autenticación	P1–P7	0.72
D2: Gestión de Dispositivos y Red	P8–P14	0.89
D3: Seguridad Perimetral	P15–P21	0.67
D4: Monitoreo y Cumplimiento	P22–P28	0.74
Global	P1–P28	**0.87**

Nota. Valores α > 0.80 indican buena consistencia interna; entre 0.60 y 0.79 son aceptables (George & Mallery, 2003).

3.2 Resultados descriptivos por dimensión

Se realizó un análisis descriptivo de los resultados obtenidos en cada dimensión evaluada, como se muestra en la Tabla 2.

Tabla 2.

Estadísticos descriptivos por dimensión de seguridad

Dimensión	Media	Desv. Est.	Nivel	% Resp. Positivas (3–4)
D1: Control de Acceso y Autenticación	3.18	0.41	Medio	68%
D2: Gestión de Dispositivos y Red	3.42	0.38	Alto	79%
D3: Seguridad Perimetral	2.81	0.52	Medio	52%
D4: Monitoreo y Cumplimiento	3.12	0.45	Medio	65%
Media General	3.05	0.44	Medio	66%

Nota. Escala: 1.00–2.49 = Bajo; 2.50–3.24 = Medio; 3.25–4.00 = Alto.

3.3 Análisis comparativo por perfil de usuario

En la Tabla 3 se presenta el análisis comparativo de las medias obtenidas por perfil de usuario.

Tabla 3.

Medias comparativas por dimensión y perfil de usuario

Dimensión	Clínico (n=19)	Administrativo (n=5)	TI (n=1)	Media Global
D1: Control de Acceso y Autenticación	3.11	3.51	3.00	3.21
D2: Gestión de Dispositivos y Red	3.04	4.00	2.71	3.25
D3: Seguridad Perimetral	3.16	2.80	3.14	3.03
D4: Monitoreo y Cumplimiento	2.98	2.26	3.43	2.89
Media General por Perfil	3.07	3.14	3.07	3.09

Nota. Datos recopilados durante el período de estudio 2026-2027.

3.4 Análisis específico por dimensión

En relación con el control de acceso, los resultados evidenciaron debilidades en los mecanismos de acceso a los sistemas de información clínica, con usuarios que podían acceder a información médica sin restricciones estrictas basadas en roles.

En la dimensión de gestión de dispositivos, se identificó la presencia de una red plana sin segmentación lógica, con uso de dispositivos personales para acceder a los sistemas clínicos, incrementando el riesgo de exposición (Lian, 2020).

El análisis de la seguridad perimetral reveló la ausencia de herramientas avanzadas como IPS, DLP y mecanismos de filtrado de aplicaciones, incrementando la superficie de ataque (Jalali & Kaiser, 2018).

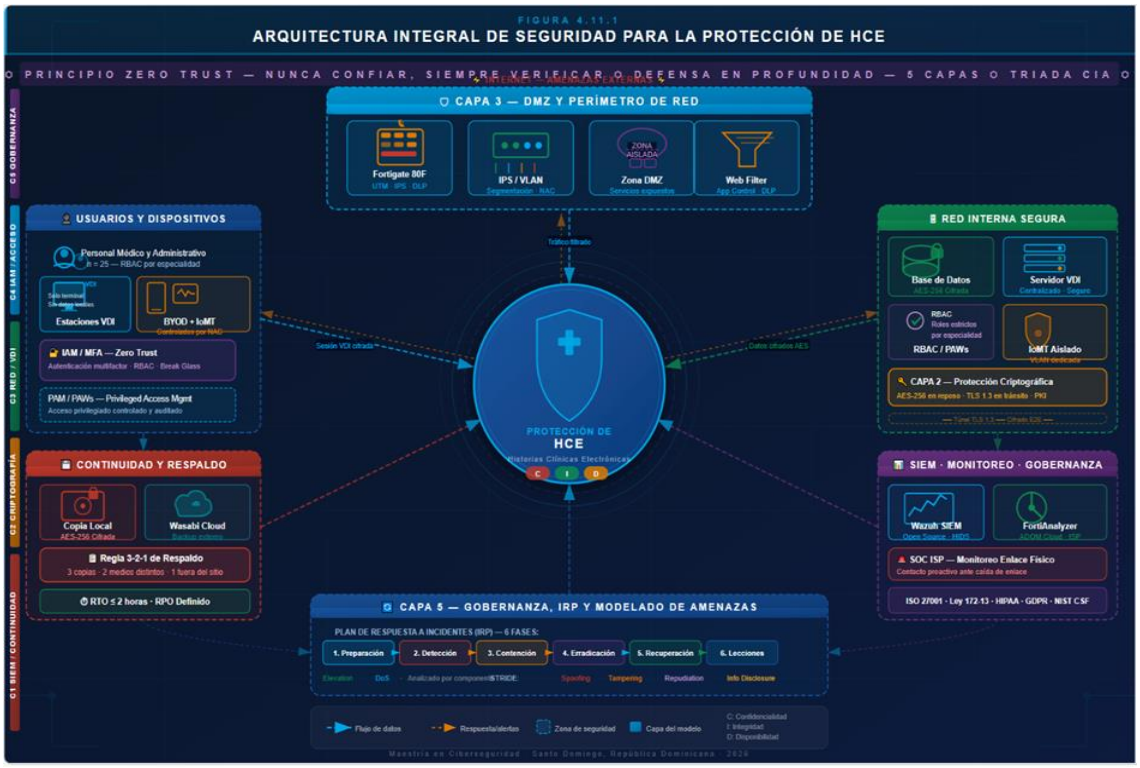
En relación con el monitoreo, el centro médico no contó con herramientas de monitoreo centralizado, lo que limitó la capacidad de detección temprana de incidentes (Sendelj & Ognjanovic, 2022).

3.5 Arquitectura del modelo de seguridad propuesto

A partir del análisis del diagnóstico, se desarrolló el modelo de ciberseguridad. La arquitectura general del modelo propuesto se presenta en la Figura 1.

Figura 1.

Arquitectura multicapa del Modelo Integral de Ciberseguridad para la protección de las HCE



Nota. Los cinco bloques funcionales del modelo: (1) DMZ y Perímetro con Firewall Fortigate 80F e IPS/VLAN; (2) Usuarios y Dispositivos con IAM/MFA y VDI; (3) Red Interna Segura con VLAN y RBAC; (4) Backups y Respaldo con cifrado local y Wasabi; (5) Monitoreo y Gobernanza con Wazuh/FortiAnalyzer.

4. Discusión

Los resultados del estudio evidencian que el centro médico analizado presenta un nivel de madurez de seguridad medio (media global = 3.05), coherente con lo documentado por Alasmary y Alshaikh (2021), quienes señalan que las instituciones de salud de tamaño medio enfrentan desafíos particulares de ciberseguridad derivados de recursos limitados y amenazas crecientes.

En cuanto al control de acceso, los mecanismos actuales no se basan completamente en roles estrictos ni en principios de mínimo privilegio, situación que coincide con lo planteado por Godoy Veas (2025), quien sostiene que la protección efectiva de las HCE requiere modelos estructurados de control de acceso.

El uso de dispositivos personales representa una fuente crítica de riesgo, coherente con Lian (2020), y la virtualización de escritorios (VDI) constituye la estrategia más eficaz para mitigar este riesgo, respaldada también por Sivan y Zukarnain (2021) sobre la seguridad en accesos remotos en salud.

La ausencia de controles perimetrales avanzados coincide con Jalali y Kaiser (2018), quienes indican que esta carencia incrementa significativamente la probabilidad de ataques de ransomware. La implementación de firewalls de próxima generación alineados con el Marco NIST (2020) constituye una medida fundamental para reducir la superficie de ataque. Urquijo Morales et al. (2023) confirman que la protección de datos clínicos en entornos digitales exige una combinación de controles perimetrales y mecanismos de cifrado robustos.

La carencia de monitoreo centralizado limita la detección temprana de incidentes, coherente con Sendelj y Ognjanovic (2022). ENISA (2023) señala que las organizaciones sanitarias con capacidades de detección y respuesta reducen el impacto de los incidentes de forma significativa. Desde una perspectiva teórica, los resultados se alinean con la norma ISO/IEC 27001:2022 (ISO/IEC, 2022), que establece la necesidad de implementar controles técnicos y organizacionales orientados a proteger la información sensible mediante la gestión sistemática de riesgos.

Los hallazgos confirman lo planteado por Bada et al. (2019): la efectividad de los controles técnicos depende en gran medida de la concientización del personal. Ahmad et al. (2021) refuerzan que las estrategias multi-capa reducen significativamente la exposición a incidentes en organizaciones con infraestructuras tecnológicas heterogéneas. El alcance de este estudio se limita a un único centro médico de tamaño medio, por lo que los resultados deben interpretarse con cautela para su generalización a otros contextos sanitarios.

5. Conclusiones

La investigación evidenció que el centro médico analizado presenta un nivel de madurez de seguridad medio (media = 3.05), lo que refleja avances importantes, pero aún insuficientes para garantizar una protección integral de las historias clínicas electrónicas. Las brechas identificadas, especialmente en seguridad perimetral (D3, media = 2.81) y monitoreo de eventos (D4, media = 3.12), ponen de manifiesto la necesidad de fortalecer componentes críticos del sistema de ciberseguridad, consolidando este ámbito como una prioridad institucional.

En este contexto, el principal aporte del estudio radica en la propuesta de un Modelo Integral de Ciberseguridad para la Protección de Historias Clínicas Electrónicas, estructurado bajo un enfoque multicapa que integra herramientas tecnológicas y buenas prácticas. Este modelo ofrece una base sólida para mejorar la protección de la información sensible en el sector salud y orientar la toma de decisiones hacia esquemas más seguros y eficientes.

Sin embargo, la efectividad de este modelo no depende únicamente de su implementación tecnológica, sino también del fortalecimiento de las capacidades del personal mediante procesos continuos de formación y concienciación, fundamentales para una adecuada gestión de la seguridad de la información. Finalmente, se plantea como líneas futuras la aplicación práctica del modelo en instituciones reales, la evaluación de su impacto en la reducción de riesgos y su adaptación a entornos digitales basados en la nube, considerando los desafíos emergentes en el ámbito de la ciberseguridad en salud.

Referencias Bibliográficas

Ahmad, T., Maynard, S. B., & Park, S. (2021). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 32(2), 359–370.

Alasmary, W., & Alshaikh, M. (2021). Cybersecurity challenges in healthcare systems. Journal of Healthcare Engineering, 2021, 1–10. https://doi.org/10.1155/2021/6698105

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour? Computers & Security, 82, 145–155.

European Union Agency for Cybersecurity (ENISA). (2023). Threat landscape for the health sector. ENISA.

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference (4th ed.). Allyn & Bacon.

Godoy Veas, J. (2025). Modelos de control de acceso para la protección de historias clínicas electrónicas en sistemas hospitalarios. Revista Latinoamericana de Seguridad Informática, 10(1), 33–48.

IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/security/data-breach

ISO/IEC. (2022). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059

Kortján, T., Põiklik, P., & Maigre, R. (2023). Data loss prevention in healthcare: A practical guide to selecting and implementing DLP solutions. Computers & Security, 125, 103056.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.

Lian, Z. (2020). Security risks in electronic health record systems and mobile healthcare applications. International Journal of Medical Informatics, 141, 104234. https://doi.org/10.1016/j.ijmedinf.2020.104234

Ministerio de la Presidencia de la República Dominicana. (2013). Ley Orgánica No. 172-13 sobre protección de datos de carácter personal. Gaceta Oficial de la República Dominicana.

Ministerio de Salud Pública de la República Dominicana. (2022). Estrategia nacional de salud digital 2022–2030. Santo Domingo.

NIST. (2020). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.

Pérez, M., & Gómez, L. (2020). Implementación de historias clínicas electrónicas en sistemas hospitalarios latinoamericanos. Revista Panamericana de Salud Pública, 44, e112.

Sendelj, R., & Ognjanovic, I. (2022). Cyber resilience in healthcare information systems: Security monitoring and incident response. Computers & Security, 115, 102603. https://doi.org/10.1016/j.cose.2022.102603

Sivan, R., & Zukarnain, Z. (2021). Security and privacy in cloud-based e-health system. Symmetry, 13(5), 742. https://doi.org/10.3390/sym13050742

Urquijo Morales, Y., Orellana García, A., & Vega Izaguirre, L. (2023). Seguridad de los datos: El desafío de la historia clínica en la nube. Universidad de las Ciencias Informáticas. https://repositorio.uci.cu/handle/123456789/10693

World Health Organization. (2021). Global strategy on digital health 2020–2025. World Health Organization.

AGRADECIMIENTOS

Los autores agradecen al personal médico, administrativo y técnico del centro médico objeto de estudio por su disposición y participación en el proceso de recolección de datos, así como a la Universidad Abierta para Adultos (UAPA) por el apoyo institucional brindado durante el desarrollo de esta investigación, por ultimo y no menos importante, agradecer a nuestra asesora de tesis Zoily Morales quien nos apoyó durante todo el trayecto que duro la tesis.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.