Fortalecimiento de la Ciberseguridad en el Acceso a Registros Clínicos Electrónicos

Libardo Antonio Miranda Contreras

Asesor

Carlos Alberto Rodríguez Sánchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Maestría en Ciberseguridad

2026

Dedicatoria

A mis padres, por inculcarme desde niño el valor del estudio y la disciplina. Su sacrificio y amor han sido la base sobre la que he construido mi vida profesional. Este logro es también suyo. A mis hijas, por entender mis ausencias, por su paciencia infinita y por ser el motor que me impulsa a superarme cada día. Ustedes son mi mayor inspiración y la razón de cada esfuerzo. A mi asesor, el profesor Carlos Alberto Rodríguez Sánchez, por su guía experta, su tiempo y sus valiosos aportes, que fueron fundamentales para dar forma a esta investigación. A todas las personas que, de una u otra manera, contribuyeron a que este sueño se hiciera realidad: familiares, amigos, compañeros de estudio y profesores. Gracias por creer en mí.

Resumen

La puesta en práctica de la digitalización de los historiales clínicos electrónicos (HCE.) representa un avance para el sector salud, al permitir mejoras manifiestas en eficiencia y en la calidad del cuidado; no obstante, Esta evolución ha expuesto los datos de los pacientes altamente sensibles a un número creciente de ciber amenazas donde existen datos en reposo y en tránsito con información altamente sensible y que son susceptibles, en consecuencia, a afectaciones en su confidencialidad, integridad y disponibilidad. Los sistemas de acceso empleados para servir de mecanismos de seguridad, como es el caso de los controles de acceso basado en roles (RBAC), resultan ser una propuesta de solución insuficiente y rígida en la medida en que son sometidos a entornos clínicos cambiantes, mientras que los mecanismos de auditoría quedan a veces lastrados por su escasa funcionalidad (Khalid & Rahman, 2024). A partir de una revisión sistemática de la literatura existente, la investigación llevara a cabo un análisis de las amenazas, vulnerabilidades y limitaciones que presentan los sistemas HCE, brindando una propuesta de solución, a partir de la cual se desarrollan un conjunto de recomendaciones orientadas a replicar el mecanismo de control de acceso y los protocolos de auditoría.

Palabras clave: Historial Clínico Electrónico (HCE), ciberseguridad, control de acceso, privacidad de la información, auditoría de sistemas, seguridad de la información.

Abstract

The implementation of the digitalization of electronic health records (EHR) represents an advancement for the healthcare sector, enabling manifest improvements in efficiency and quality of care; however, this evolution has exposed highly sensitive patient data to a growing number of cyber threats where data exists both at rest and in transit containing highly sensitive information and is consequently susceptible to impacts on its confidentiality, integrity, and availability. The access systems employed to serve as security mechanisms, such as role-based access controls (RBAC), prove to be an insufficient and rigid solution proposal insofar as they are subjected to changing clinical environments, while audit mechanisms are sometimes hampered by their limited functionality (Khalid & Rahman, 2024). Based on a systematic review of the existing literature, the research will conduct an analysis of the threats, vulnerabilities, and limitations present in EHR systems, providing a proposed solution, from which a set of recommendations are developed aimed at replicating the access control mechanism and audit protocols.

Keywords**:** Electronic Health Record (EHR), cybersecurity, access control, information privacy, systems audit, information security.

Tabla de contenido

Lista de tablas

Lista de figuras

Glosario

ABAC (Attribute-Based Access Control): Modelo de control de acceso que concede permisos basándose en atributos del usuario (cargo, especialidad), del recurso (tipo de documento, sensibilidad), del entorno (ubicación, hora) y de la acción (lectura, escritura). A diferencia de RBAC, permite políticas dinámicas y contextuales.

Accountability (Rendición de cuentas): Principio de gobernanza que obliga a las instituciones a demostrar, mediante evidencia verificable, que cumplen con las normativas de protección de datos y que las acciones sobre la información son legítimas, seguras y trazables.

Autenticación multifactor (MFA): Mecanismo de seguridad que requiere que el usuario presente dos o más evidencias (factores) para verificar su identidad. Los factores pueden ser algo que el usuario sabe (contraseña), algo que posee (token, teléfono) o algo que es (huella dactilar, reconocimiento facial).

Big Data en salud: Conjunto de datos clínicos y administrativos de gran volumen, velocidad, variedad, veracidad y valor (las "5 V"), que requieren tecnologías y métodos analíticos avanzados para su procesamiento y generación de conocimiento.

Blockchain: Tecnología de registro distribuido que permite almacenar información de forma inmutable, descentralizada y transparente. En el contexto de HCE, se utiliza para garantizar la trazabilidad y no repudio de los registros de auditoría.

Brecha de seguridad: Incidente que resulta en el acceso, divulgación, modificación, pérdida o destrucción no autorizada de información, comprometiendo su confidencialidad, integridad o disponibilidad.

Cifrado homomórfico: Tipo de cifrado avanzado que permite realizar operaciones matemáticas directamente sobre datos cifrados, generando un resultado cifrado que, al descifrarse, coincide con el resultado de las operaciones realizadas sobre los datos en texto plano. Es útil para análisis de datos preservando la privacidad.

Control de acceso: Mecanismo de seguridad que regula quién puede ver o usar qué recursos en un entorno informático, basándose en políticas y permisos predefinidos.

GDPR (General Data Protection Regulation): Reglamento General de Protección de Datos de la Unión Europea, normativa que establece directrices estrictas para la recolección, tratamiento y protección de datos personales, incluyendo categorías especiales como los datos de salud.

Gobernanza de datos: Conjunto de procesos, políticas, estándares y métricas que aseguran el uso efectivo y eficiente de la información en una organización, garantizando su calidad, seguridad, privacidad y cumplimiento normativo.

Hash: Función criptográfica unidireccional que produce una salida de longitud fija (resumen) a partir de un mensaje de entrada de cualquier longitud. Es computacionalmente inviable revertir el proceso o encontrar dos mensajes diferentes con el mismo hash, lo que lo hace útil para verificar integridad.

HIPAA (Health Insurance Portability and Accountability Act): Ley estadounidense que establece estándares nacionales para la protección de la información médica electrónica, incluyendo requisitos de privacidad, seguridad y notificación de brechas.

Hyperledger Fabric: Plataforma de blockchain permissionada de código abierto, hospedada por la Linux Foundation. Diseñada para entornos empresariales, permite la creación de canales privados, consensos pluggables y contratos inteligentes en lenguajes de propósito general (Go, Java, JavaScript).

IoMT (Internet of Medical Things): Internet de las Cosas Médicas. Infraestructura de dispositivos médicos conectados (marcapasos, bombas de infusión, monitores, etc.) que generan, recopilan y transmiten datos de salud a través de redes, ampliando la superficie de ataque de los sistemas hospitalarios.

ISO/IEC 27001: Estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización.

ISO/IEC 27799: Guía de implementación de la ISO/IEC 27001 para el sector salud, que proporciona directrices específicas para proteger la información clínica y cumplir con requisitos de confidencialidad, integridad y disponibilidad.

Ley 1581 de 2012: Ley colombiana de protección de datos personales, que establece los principios, derechos, obligaciones y procedimientos para garantizar el derecho a la privacidad y el correcto tratamiento de la información personal, incluyendo los datos sensibles de salud.

Mínimo privilegio (Least privilege): Principio de seguridad que establece que un usuario, programa o proceso debe tener únicamente los permisos estrictamente necesarios para realizar su función legítima, y nada más.

NIST Cybersecurity Framework: Marco de ciberseguridad desarrollado por el National Institute of Standards and Technology de EE. UU., que proporciona un conjunto de estándares, directrices y prácticas para ayudar a las organizaciones a gestionar y reducir los riesgos de ciberseguridad, estructurado en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.

No repudio: Principio de seguridad que garantiza que una entidad que realizó una acción (como acceder a un registro) no pueda negar haberla realizado, proporcionando evidencia irrefutable de la transacción.

Phishing: Técnica de ingeniería social utilizada por atacantes para engañar a usuarios y obtener información confidencial (credenciales, datos bancarios) haciéndose pasar por una entidad legítima a través de correos electrónicos, mensajes o sitios web falsos.

Ransomware: Tipo de malware que cifra los archivos de un sistema y exige un rescate económico a la víctima para su liberación. En el sector salud, puede paralizar servicios críticos y poner en riesgo vidas humanas.

RBAC (Role-Based Access Control): Modelo de control de acceso que asigna permisos a los usuarios basándose en los roles que desempeñan dentro de la organización. Es el modelo tradicional más utilizado en sistemas hospitalarios, aunque presenta limitaciones en entornos dinámicos.

Seudonimización: Técnica de protección de datos que reemplaza los identificadores directos (nombre, cédula) en un registro por seudónimos o códigos. A diferencia de la anonimización, la seudonimización permite la reidentificación bajo condiciones controladas, siendo útil para investigaciones donde se requiere un vínculo limitado con el paciente.

Smart contract (Contrato inteligente): Programa informático almacenado en una blockchain que se ejecuta automáticamente cuando se cumplen condiciones predefinidas, permitiendo automatizar procesos (como auditorías o control de accesos) de forma transparente e inmutable.

STRIDE: Metodología de modelado de amenazas desarrollada por Microsoft que clasifica las amenazas en seis categorías: Spoofing (suplantación), Tampering (manipulación), Repudiation (no repudio), Information Disclosure (revelación de información), Denial of Service (denegación de servicio) y Elevation of Privilege (elevación de privilegios).

Vulnerabilidad: Debilidad o fallo en el diseño, implementación, operación o gestión de un sistema que puede ser explotada por una amenaza para causar un daño o incidente de seguridad.

Zero Trust (Confianza Cero): Modelo de arquitectura de seguridad basado en el principio "nunca confiar, siempre verificar". Asume que la red ya está comprometida y, por lo tanto, exige autenticación y autorización continua para cada acceso, independientemente de su

origen (interno o externo), junto con segmentación estricta de redes y monitoreo permanente.

Introducción

La transformación digital ha modificado de manera significativa de casi cualquier ámbito, entre ellos el sector salud. Siendo el historial clínico electrónico (HCE) uno de los de los elementos que se han visto afectados por la evolución informacional, puesto que han pasado de ser un mero sistema de gestión de datos a transformarse en un ecosistema de información de enorme valor. La posibilidad de poder acceder, gestionar o compartir información del paciente al instante ha mejorado los diagnósticos, ha podido personalizar tratamientos y acelerar la investigación médica mucho más allá de lo que se había hecho hasta el momento.

No obstante, dicha interconectividad genera una paradoja básica: la misma accesibilidad que hace mejorar la atención sanitaria también se convierte en un vector de vulnerabilidades que se suma a las superficies de ataques ya existentes. La información de salud es uno de los activos informativos más sensibles y los sistemas que almacenan esa información son, por lo tanto, un objetivo de alto valor (Khalid & Rahman, 2024). En ese orden de ideas, la ciberseguridad en el campo de la salud pasó de ser una simple cuestión técnica para convertirse en un eje estratégico que protege no sólo la privacidad de los pacientes, sino que también asegura la integridad del sistema y la confianza de este último.

El presente trabajo se adentra en ese difícil equilibrio entre una atención sanitaria de calidad y la ciberseguridad. Mediante el análisis de la literatura académica, la investigación se centra en los problemas que afectan la protección de los HCE, incluyendo las tensiones

entre la funcionalidad operativa mínima y las protecciones efectivas de ciberseguridad. El objetivo es identificar las distintas debilidades de los enfoques conocidos y sentar las bases para proponer mejoras que sean satisfactorias en un entorno informático que cambia constantemente con relación a las normativas del sector, la innovación digital tiene que ir de la mano con la protección de los derechos esenciales de los pacientes.

Planteamiento del Problema

La digitalización en el sector salud ha facilitado el uso de historiales clínicos electrónicos (HCE), favoreciendo la asistencia, la interoperabilidad y la investigación. Sin embargo, esta digitalización también expone los datos médicos, altamente sensibles, a los crecientes peligros de seguridad y privacidad en el sector. En este predicamento, la tríada de seguridad de la información (confidencialidad, disponibilidad e integridad) es crítica: cualquier fallo en la autenticación y autorización, compromete la atención médica, la vida del paciente, la confianza que se tiene en las instituciones y las posibles sanciones legales.

Los estudios más recientes dan cuenta de riesgos como el acceso o uso no autorizado de la información, la manipulación de la misma o la denegación del servicio; también se evidencia que existen fugas masivas de información con las correspondientes consecuencias (robo de identidad, fraude, entre otros). Aunque se utilizan mecanismos como el control de acceso basado en roles (RBAC) en los sistemas HCE, su rigidez hace que la gestión a través de roles sea poco apropiada para sistemas cuyo contexto cambia con demasiada frecuencia (por ejemplo, emergencias, sistemas inalámbricos de consulta de datos, entre otros.), limitando en consecuencia la posibilidad de detectar accesos no autorizados o inadecuados.

A nivel normativo, existen marcos como HIPAA en EE. UU., el GDPR en Europa o la Ley 1581 de 2012 en Colombia que brindan un marco normativo para la protección de los derechos de acceso y tratamiento de datos personales, estableciendo exigencias de seguridad y privacidad muy estrictas. Sin embargo, el cumplimiento real de estas normativas choca con cuestiones técnicas y organizativas similares, especialmente la falta de cultura en

ciberseguridad por su parte de los profesionales de la salud. En este mismo sentido, la relevancia técnica consiste en que los mecanismos actuales de la protección de las HCE no son suficientes para combatir las amenazas existentes. El uso de RBAC, si bien muy extendido, no posee la flexibilidad deseada para gestionar situaciones dinámicas y excepcionales en entornos colaborativos y/o inalámbricos.

Del mismo modo, los registros de auditoría permiten rastrear accesos indebidos, pero suelen ser extensos, con bajo nivel de detalle y difícil interpretación, lo que limita su viabilidad a la práctica. Desde un punto de vista ético, el acceso no autorizado a datos clínicos puede tener consecuencias graves para los pacientes, que van desde la discriminación o el estigma social hasta la pérdida de confianza en el sistema de salud implementado (Khalid & Rahman, 2024). La protección de la integridad, privacidad y la confidencialidad es, por el contrario, no solo una exigencia legal –lo que asegura ante el marco normativo–sino un deber fundamental que garantiza la relación de confianza entre el paciente y entidades de la salud.

Los principales afectados son los pacientes que están expuestos a la posibilidad de sufrir discriminación o un robo de identidad; los profesionales de la salud, que precisan dar fiabilidad a los registros; las instituciones de salud y las entidades aseguradoras, que se ven sometidas a situaciones de riesgo tanto económicas como legales; y la sociedad como tal, cuya confianza en los sistemas digitales ve así mermada (Pulido, Cobo, & Guitierrez, 2021).

Estos aspectos conducen a cuestionarse sobre cómo garantizar la seguridad y el cumplimiento normativo, así como avanzar hacia una comprensión más precisa acerca de la naturaleza de los problemas legales y operativos. El problema no consiste solamente en cumplir la ley, sino también en cómo poder demostrarlo, por lo cual, la investigación debe centrarse en los mecanismos que permiten la supervisión y la asignación de la

responsabilidad (Khalid & Rahman, 2024). De este modo, la pregunta de investigación se se permite ser reformulada a fin de tener un enfoque más robusto:

¿De qué manera es posible fortalecer los mecanismos de control de acceso y los protocolos de auditoría en los sistemas de historiales clínicos electrónicos (HCE) con el fin de mitigar las ciberamenazas, superar las limitaciones de los modelos tradicionales, garantizar la trazabilidad y la rendición de cuentas exigidas por los marcos regulatorios para la protección de datos personales?

Justificación

La presente investigación pone de manifiesto una problemática de elevada importancia en la actualidad caracterizada por la información digital que se encuentra almacenada en las bases de datos del sector salud. Es importante que, el concepto de "proteger los historiales clínicos electrónicos" (HCE) no constituye en su definición pura y dura un problema exclusivamente técnico, sino que se tiene que entender como un problema normativo y ético en el sentido más profundo de la palabra. Es por ello que, a continuación, se expone la justificación que se puede extender a las diferentes dimensiones de la misma.

Justificación técnica

La justificación técnica de esta investigación está relacionada con el hecho de que los mecanismos de protección actuales son insuficientes para contrarrestar las ciberamenazas en el entorno de la salud. Por ejemplo, el uso de herramientas como el control de acceso basado en roles (RBAC) se entiende como un mecanismo de seguridad estándar dentro del sector; sin embargo, el carácter rígido de su diseño presenta serias limitaciones en los entornos clínicos dado que se caracterizan por ser dinámicos, colaborativos o cada vez más dependientes de tecnologías inalámbricas o de emergencia. Esta rigidez impide la gestión de los accesos legítimos en situaciones excepcionales al tiempo que complica la detección de actividades no regulares (Cobrado et al., 2024).

Por otra parte, los sistemas para auditar, que deberían funcionar como una línea de defensa para la supervisión, suelen ser poco funcionales en la práctica. Los logs producidos

suelen ser muy extensos, de poca granularidad y de difícil interpretación, lo que limita las posibilidades de que sean usados para detectar incidentes de seguridad o, incluso, para reaccionar ante ellos (Wijayanti, Ujianto & Rianto, 2024). Por lo tanto, existe una brecha técnica manifiesta entre las soluciones de seguridad implementadas y los requerimientos efectivos de los sistemas de información de los centros sanitarios modernos.

Justificación normativa

La gestión de datos de salud está completamente regulada de forma normativa a nivel nacional y mundial. Normativas como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPA) en Estados Unidos, el Reglamento General de Protección de Datos (RGPD) en Europa o la Ley 1581 de 2012 en Colombia, impone obligaciones muy estrictas para que se garantice tanto la seguridad como la privacidad de la información personal.

No obstante, el hecho de cumplir en estos ámbitos se enfrenta a barreras notables que son independientes del entorno tecnológico, lo cuales tienen que ver con la ausencia de una cultura de ciberseguridad en el interior de las instituciones sanitarias que frena la aplicación efectiva de los controles dispuestos (Shojaei, Vlahu-Gjorgievska & Chow, 2024). Este estudio es relevante ya que no se limitan a proponer soluciones técnicas, sino que permite al mismo tiempo incorporarlas a los principios de trazabilidad y de rendición de cuentas (accountability) que enmarcan las regulaciones. El objetivo es dar a las organizaciones la oportunidad no sólo de conformar, sino de hacerlo efectivamente.

Justificación Ética y Social

Desde una perspectiva de ética, la protección de los datos personales contenidos en los HCE forma parte del derecho fundamental a la privacidad, junto con la prohibición del acceso a datos clínicos sin la autorización correspondiente. El acceso sin autorización a datos

clínicos tiene consecuencias terribles para las personas (Basil et al., 2022) que van desde la discriminación laboral o social y el estigma hasta el robo de identidad y el fraude. Aunque es un objetivo del presente trabajo, siempre, la confidencialidad es la base de sustentación de la relación ética entre el paciente y el profesional de la salud; de modo que cualquier brecha de seguridad directamente la pone en riesgo.

Las consecuencias sociales de esta situación son extensas y perniciosas para la gran mayoría de los afectados:

- Pacientes: Expuestos a la violación de su privacidad y a peligros para su persona.
- Profesionales de la salud: Prefieren el acceso a datos completos y fiables para la buena toma de decisiones clínicas.
- Las instituciones sanitarias y las aseguradoras: Sufren desde pérdidas económicas, pasando por consecuencias reputacionales hasta penurias administrativas.
- La sociedad: Tiene dudas y es muy escéptica frente la digitalización de los servicios más importantes.

Por lo tanto, la realización de este estudio es un paso por desarrollar sistemas mucho más extensos para hacer valer los derechos de las personas y, al mismo tiempo, reforzar la confianza pública en el ecosistema de la salud digital.

Objetivos

Objetivo general:

Analizar, desde una perspectiva documental y normativa, las amenazas, vulnerabilidades y limitaciones que afectan el acceso seguro a los historiales clínicos electrónicos (HCE), con el fin de proponer estrategias de fortalecimiento en los mecanismos de control de acceso y auditoría, orientadas a mitigar ciberamenazas, garantizar la trazabilidad institucional y cumplir con los marcos regulatorios vigentes en materia de protección de datos personales.

Objetivos específicos:

Examinar de manera sistemática las amenazas y vulnerabilidades identificadas en la literatura científica que afectan la seguridad del acceso a los historiales clínicos electrónicos (HCE), poniendo especial atención en los riesgos técnicos, organizacionales e internos que comprometen los principios de confidencialidad, integridad y disponibilidad de la información clínica.

Analizar críticamente las limitaciones estructurales, operativas y normativas de los mecanismos tradicionales de control de acceso y auditoría, en particular el modelo RBAC en entornos clínicos dinámicos, identificando los factores que dificultan la trazabilidad, la detección de accesos indebidos y el cumplimiento de los marcos regulatorios vigentes.

Diseñar y proponer estrategias de fortalecimiento orientadas a optimizar los procesos de auditoría y detección de accesos no autorizados en sistemas que gestionan información clínica electrónica, integrando modelos de control de acceso más adaptativos, tecnologías emergentes y principios de rendición de cuentas institucional.

Marco teórico

El presente marco teórico se fundamenta en literatura científica reciente (2021-2025), informes técnicos y estándares internacionales de ciberseguridad aplicados al sector salud, con el propósito de analizar amenazas, vulnerabilidades y estrategias de fortalecimiento en los sistemas de Historia Clínica Electrónica (HCE). La digitalización de los registros médicos ha transformado la gestión hospitalaria, mejorando diagnósticos y tratamientos, pero también incrementando la exposición a riesgos. Camargo y Claudio (2023) señalan que la interoperabilidad de los HCE amplía la superficie de ataque, mientras Shojaei et al. (2024) confirman que el sector salud es particularmente vulnerable por la ausencia de políticas robustas. Guamán-Acan et al. (2024) enfatizan que la confidencialidad de los datos clínicos constituye un derecho fundamental, vinculando la ciberseguridad con la ética médica. En Latinoamérica, Alegre et al. (2024) y el BID (Bagolle, Park & Marti, 2021) evidencian que, pese a los avances legislativos, persisten vacíos técnicos frente a estándares como el GDPR, lo que demanda un fortalecimiento de la gobernanza digital regional.

Bajo el paradigma de Big Data en salud, caracterizado por las "5 Vs" (volumen, velocidad, variedad, veracidad y valor), emergen oportunidades para la medicina predictiva, pero también riesgos significativos. Basil et al. (2022) advierten que la agregación de múltiples fuentes incrementa la posibilidad de reidentificación de pacientes, mientras Khalid y Rahman (2024) proponen matrices de riesgo para clasificar amenazas según impacto y probabilidad. Wijayanti et al. (2024) recomiendan cifrado híbrido y anonimización dinámica para mitigar riesgos en fases críticas como la recolección y almacenamiento.

Latorre Luna (2024) añade que el Big Data plantea dilemas éticos como la pérdida de autonomía del paciente y el riesgo de discriminación por correlaciones indebidas, lo que se confirma con incidentes de fugas masivas en hospitales europeos por falta de controles en el almacenamiento en la nube.

En materia de control de acceso, Cobrado et al. (2024) señalan que el modelo tradicional RBAC resulta insuficiente en entornos dinámicos, pues más del 50% de los accesos en emergencias se realizan mediante excepciones que comprometen la trazabilidad. Como alternativa, Wijayanti et al. (2024) proponen el modelo ABAC, que incorpora atributos contextuales como identidad, localización y tiempo, mientras Edo et al. (2023) destacan la arquitectura Zero Trust que exige verificación continua de usuarios y dispositivos. Estudios recientes (MDPI, 2025) plantean modelos híbridos RBAC-ABAC para una gestión más granular del riesgo. Aunque hospitales como Mayo Clinic han migrado hacia estos modelos reduciendo incidentes de accesos indebidos, la adopción enfrenta barreras económicas y culturales en países en desarrollo, evidenciando la necesidad de políticas públicas que promuevan la adopción gradual de estas tecnologías junto con marcos regulatorios que establezcan estándares técnicos claros y exigibles para la protección de los datos clínicos.

El historial clínico electrónico (HCE) como activo crítico: seguridad, big data y control de acceso.

La digitalización de los registros médicos ha transformado la gestión hospitalaria, mejorando diagnósticos y tratamientos, pero también incrementando la exposición a riesgos. Camargo y Claudio (2023) destacan que la interoperabilidad de los HCE amplía la superficie de ataque, mientras Shojaei et al. (2024) confirman que el sector salud es uno de los más vulnerables por la falta de políticas robustas. Guamán-Acan et al. (2024) enfatizan que la

confidencialidad de los datos clínicos constituye un derecho fundamental, vinculando la ciberseguridad con la ética médica. En el ámbito latinoamericano, los estudios de Alegre et al. (2024) y el informe del Banco Interamericano de Desarrollo (Bagolle, Park & Marti, 2021) muestran que, aunque la mayoría de los países han avanzado en legislación, la implementación práctica es desigual y persisten vacíos técnicos frente a estándares internacionales como el GDPR. Por ejemplo, en Colombia la Ley 1581 de 2012 protege datos personales, pero carece de exigencias técnicas claras, lo que contrasta con el GDPR europeo que obliga a la seudonimización y la rendición de cuentas, evidenciando la necesidad de fortalecer la gobernanza digital en la región.

Esta vulnerabilidad se magnifica bajo el paradigma de Big Data en salud, caracterizado por las "5 Vs" (volumen, velocidad, variedad, veracidad y valor). Si bien este enfoque genera oportunidades para la medicina predictiva, también incrementa significativamente los riesgos asociados al manejo de información sensible. Basil et al. (2022) advierten que la agregación de múltiples fuentes incrementa la posibilidad de reidentificación de pacientes, mientras Khalid y Rahman (2024) proponen matrices de riesgo para clasificar amenazas según impacto y probabilidad. Wijayanti et al. (2024) recomiendan cifrado híbrido y anonimización dinámica para mitigar riesgos en fases críticas como la recolección y almacenamiento. Latorre Luna (2024) añade que el Big Data plantea dilemas éticos como la pérdida de autonomía del paciente y el riesgo de discriminación por correlaciones indebidas, lo que se confirma con incidentes de fugas masivas en hospitales europeos por falta de controles en el almacenamiento en la nube.

En materia de control de acceso, Cobrado et al. (2024) señalan que el modelo tradicional RBAC resulta insuficiente en entornos dinámicos, pues más del 50% de los

accesos en emergencias se realizan mediante excepciones que comprometen la trazabilidad. Como alternativa, Wijayanti et al. (2024) proponen el modelo ABAC, que incorpora atributos contextuales como identidad, localización y tiempo, mientras Edo et al. (2023) destacan la arquitectura Zero Trust que exige verificación continua de usuarios y dispositivos. Aunque hospitales como Mayo Clinic han migrado hacia estos modelos reduciendo incidentes de accesos indebidos, la adopción enfrenta barreras económicas y culturales significativas en países en desarrollo, lo que evidencia la necesidad de políticas públicas que promuevan la adopción gradual de estas tecnologías junto con marcos regulatorios que establezcan estándares técnicos claros y exigibles para la protección de los datos clínicos.

Auditoría, trazabilidad y rendición de cuentas

La trazabilidad de los accesos y de las acciones constituye un pilar básico para la seguridad y la confianza en los sistemas de información en salud. Normativas internacionales, como las de HIPAA (EE.UU.) y el Reglamento General de Protección de Datos (GDPR) (Unión Europea), requieren que las organizaciones se aseguren de presentar mecanismos de rendición de cuentas (accountability) que permitan rastrear quién accede a qué información y para qué finalidad (Shojaei et al., 2024).

La literatura especializada, evidencia deficiencias persistentes: los registros de auditoría tienden a ser largos, reactivos y con un bajo nivel de granularidad, lo que ayuda a prevenir la detección de anomalías (Basil et al., 2022); y la centralización de estos registros los convierte en presas fáciles para ser manipulados, perdiendo así su integridad.

Para superar estas limitaciones, se han propuesto dos líneas tecnológicas principales:

- Auditoría Inteligente: Implementación de Inteligencia Artificial (IA) y machine learning en los sistemas de auditoría, para modificar los registros

inertes en instrumentos proactivos que puedan descubrir accesos anómalos de atención y prever ataques (Wijayanti et al., 2024).

- Blockchain: Señalamos la tecnología descentralizada que proporciona inmutabilidad y trazabilidad de los registros de acceso, eliminando los puntos únicos de fallo y robusteciendo las confianzas institucionales (Riveros, Iglesias & de los Santos, 2024; Plasencia, 2024). Para Pulido, Cobo y Gutiérrez (2021), la aplicación de Blockchain en sistemas de registro clínico portable es un avance respecto a la protección de los datos médicos y la transparencia de la auditoría.

La trazabilidad de los accesos constituye un pilar fundamental para garantizar la confianza institucional y el cumplimiento normativo. Sin embargo, los registros de auditoría tradicionales suelen ser reactivos y vulnerables a manipulaciones (Riveros, Iglesias, & de los Santos, 2024).

El estudio de Riveros, Iglesias y de los Santos (2024) proporciona un fundamento sólido para considerar la tecnología blockchain como una herramienta de auditoría en sistemas de información clínica. Los autores demuestran que las propiedades de descentralización e inmutabilidad inherentes a esta tecnología eliminan puntos únicos de fallo y fortalecen la transparencia institucional. Desde esta perspectiva, la incorporación de blockchain en los sistemas de Historia Clínica Electrónica (HCE) no solo mejora la trazabilidad de las transacciones y accesos a la información, sino que también incrementa la confianza de los pacientes y de las autoridades regulatorias en la integridad y seguridad de los datos clínicos.

La trazabilidad constituye un elemento indispensable para garantizar la confianza institucional y el cumplimiento normativo en los sistemas de información clínica. Basil et al. (2022) señalan que los registros de auditoría tradicionales suelen ser extensos y vulnerables a manipulación, lo que compromete su fiabilidad. Ante esta limitación, Riveros, Iglesias y de los Santos (2024), junto con Plasencia (2024), proponen la adopción de blockchain como mecanismo para asegurar la inmutabilidad y transparencia de las trazas de acceso y modificación de los datos clínicos.

En el contexto colombiano, Cáceres Ramírez et al. (2025) analizan la integración de blockchain en el sector salud, destacando mejoras significativas en seguridad y eficiencia operativa. Por su parte, Metlabs (2025) identifica aplicaciones concretas de esta tecnología en registros médicos, cadena de suministro de medicamentos y gestión del consentimiento informado. DigitalDigest (2025) complementa estos hallazgos al resaltar que las propiedades de inmutabilidad, transparencia y descentralización inherentes a blockchain fortalecen sustancialmente la confianza depositada en los sistemas clínicos.

La viabilidad práctica de estas propuestas académicas encuentra respaldo en experiencias internacionales consolidadas. Estonia constituye un caso pionero en la implementación de blockchain en salud desde 2008, donde su adopción ha permitido garantizar la trazabilidad de las operaciones y fortalecer la confianza institucional. Este referente internacional demuestra que las soluciones basadas en blockchain no solo son conceptualmente sólidas, sino también efectivas cuando se aplican en entornos reales de gestión sanitaria.

Marco conceptual

El Marco Conceptual define y aclara los términos y conceptos básicos para los activos de información, los objetivos de seguridad, las amenazas que se han detectado, las soluciones tecnológicas planteadas para el contexto de los Registros Clínicos Electrónicos (HCE) y se encuentra basado en la reciente literatura y en el estado del arte de los artículos de Camargo & Claudio (2023), Shojaei, Vlahu-Gjorgievska & Chow (2024), Guamán-Acan et al. (2024), Wijayanti, Ujianto & Rianto (2024), Khalid & Rahman (2024) y unos pocos más.

El marco conceptual se presenta como el fundamento teórico que orienta la investigación sobre la ciberseguridad aplicada a los historiales clínicos electrónicos, al definir y aclarar los términos y conceptos básicos que permiten comprender la naturaleza de los activos de información, los objetivos de seguridad que deben alcanzarse, las amenazas más relevantes que comprometen la integridad de los sistemas y las soluciones tecnológicas que se han planteado en la literatura especializada. Este apartado se construye a partir del análisis del estado del arte y de estudios recientes, lo que garantiza una visión integral y actualizada de la problemática. De esta manera, el marco conceptual no solo organiza el conocimiento existente, sino que también establece las bases para interpretar los HCE como ecosistemas digitales complejos, orientando la investigación hacia propuestas sólidas que fortalezcan la protección de la información clínica en un entorno sanitario cada vez más dinámico y vulnerable.

El Historial Clínico Electrónico (HCE) como activo de información en el paradigma de Big Data en salud

El Historial Clínico Electrónico (HCE), conocido en inglés como Electronic Health Record (EHR), se describe como el conjunto global de información clínica digital que recoge la asistencia sanitaria proporcionada a un paciente (Camargo & Claudio, 2023). Este activo de información representa el centro del fenómeno de digitalización en salud, el cual ha pasado en poco tiempo de ser un sistema de registro a un ecosistema informacional de extraordinaria relevancia clínica, científica y económica.

Los HCE se inscriben dentro del paradigma de Big Data en salud, caracterizado por las "5 Vs": volumen masivo de datos generados constantemente; velocidad para procesar información casi en tiempo real en apoyo a decisiones médicas críticas; variedad de datos estructurados y no estructurados (estos últimos representan más del 80% del total); veracidad, entendida como la fiabilidad de los datos para evitar diagnósticos erróneos; y valor, entendido como la capacidad de transformar datos en conocimiento útil para la toma de decisiones clínicas, investigativas y administrativas (Basil, Ambe, Ekhator, Fonkem & Nduma, 2022).

Este paradigma implica tanto oportunidades para la analítica avanzada como riesgos asociados a la privacidad y la seguridad de los datos, exigiendo la implementación de mecanismos de protección avanzados que aseguren la confidencialidad, integridad y disponibilidad de la información en un entorno cada vez más expuesto a ciberamenazas. En definitiva, los HCE constituyen el punto de partida y el núcleo estratégico de cualquier modelo de ciberseguridad en salud, y su protección representa no solo un reto técnico, sino también un compromiso ético, normativo y organizacional.

Objetivos de la Ciberseguridad: La Tríada de la Seguridad

La ciberseguridad en el ámbito de la salud tiene como propósito fundamental garantizar que los Historiales Clínicos Electrónicos (HCE) sean protegidos bajo las tres dimensiones de la tríada CIA: Confidencialidad, Integridad y Disponibilidad (Shojaei et al., 2024; Wijayanti et al., 2024). La confidencialidad asegura que la información clínica sea accesible únicamente por usuarios autorizados, cuya vulneración puede derivar en discriminación, robo de identidad o fraude (Shojaei et al., 2024).

Técnicamente, se garantiza mediante cifrado robusto, seudonimización dinámica y autenticación multifactor, mientras que organizativamente requiere políticas internas claras y formación continua del personal sanitario. La integridad, por su parte, asegura que los datos reflejen fielmente la realidad del paciente sin modificaciones no autorizadas, pues cualquier alteración puede comprometer la atención sanitaria con consecuencias fatales (Wijayanti et al., 2024). Para garantizarla se requieren auditorías continuas, trazabilidad en tiempo real y mecanismos como blockchain que aseguren la inmutabilidad de los registros.

La disponibilidad asegura el acceso a los sistemas e información clínica cuando los usuarios legítimos lo requieran, siendo los ataques de denegación de servicio (DoS/DDoS) una de sus principales amenazas (Khalid & Rahman, 2024), por lo que se requieren infraestructuras redundantes, protocolos de recuperación ante desastres (BCP/DRP) y segmentación de redes hospitalarias.

No obstante, resulta pertinente contrastar la solidez teórica de este marco con las realidades observadas en el contexto latinoamericano. Mientras que en regiones como Europa la tríada CIA se encuentra respaldada por normativas exigentes como el GDPR —que obliga a la seudonimización, la rendición de cuentas y la notificación de brechas—, en países como Colombia la Ley 1581 de 2012, si bien protege datos personales, carece de exigencias técnicas específicas que operacionalicen estos principios en el sector salud.

Esta brecha normativa evidencia que la tríada CIA, aunque universalmente aceptada como estándar, enfrenta desafíos significativos para su materialización efectiva en entornos con marcos regulatorios incipientes y limitaciones de infraestructura tecnológica. La disparidad entre el deber ser teórico y la capacidad real de implementación constituye una tensión crítica que debe ser abordada mediante el fortalecimiento de la gobernanza digital y la adopción de estándares técnicos exigibles que trasciendan las declaraciones de principios.

Ciclo de Vida del Dato Clínico y sus Vulnerabilidades

El ciclo de vida de los datos clínicos abarca desde su generación hasta su destrucción o anonimización definitiva. Cada fase presenta vulnerabilidades específicas que requieren medidas de protección equivalentes y adaptadas a su contexto (Khalid & Rahman, 2024; Shojaei et al., 2024). La seguridad de los Historias Clínicas Electrónicas (HCE) no puede entenderse como un evento aislado, sino como un proceso integral y permanente que debe garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información clínica:

- Recolección (Collection): En la fase de recolección, los datos clínicos estructurados y no estructurados se obtienen de múltiples fuentes: consultas médicas, dispositivos IoT, laboratorios, imágenes diagnósticas y plataformas móviles. Los riesgos más frecuentes incluyen la suplantación de identidad (phishing), la inyección de datos falsos y los errores de captura, que pueden distorsionar la información desde su origen y comprometer la calidad del registro. Para mitigar estos riesgos, se recomienda:
    - Implementar protocolos de autenticación fuerte en la captura de datos.
    - Validar la información mediante algoritmos de detección de anomalías.

- Establecer controles de integridad en tiempo real para evitar la manipulación inicial de los registros.

- Almacenamiento y Transformación (Storage & Transformation): Durante el almacenamiento y transformación, los datos se guardan en bases de datos locales o en nubes híbridas, y son objeto de procesos de limpieza, validación y estandarización. Las amenazas más comunes incluyen ataques DDoS, intrusiones externas y fugas de datos, que comprometen la disponibilidad y confidencialidad de la información. Para enfrentar estos riesgos, se requiere:
  - Cifrado robusto en reposo y en tránsito (AES, RSA, cifrado homomórfico).
  - Anonimización dinámica, que permita separar datos clínicos de identificadores personales.
  - Políticas de segmentación de red y redundancia para garantizar continuidad operativa.
- Modelado y Utilización (Utilization): En la fase de modelado y utilización, los datos son procesados mediante técnicas como stream computing o Map/Reduce, generando información para investigación, docencia o gestión clínica. Los riesgos incluyen la reidentificación por correlación de datos y el análisis no autorizado, que pueden vulnerar la privacidad del paciente. Para mitigar estos riesgos, se recomienda:
  - Implementar auditorías continuas y trazabilidad en tiempo real.
  - Aplicar privacidad diferencial en análisis masivos de datos.

    - Establecer protocolos de gobernanza de datos que definan responsabilidades claras en el uso secundario de la información.
- Destrucción o Anonimización (Destruction/Anonymization): La fase final del ciclo implica la destrucción segura o la anonimización definitiva de los datos clínicos. Los riesgos incluyen la reutilización indebida de información, la recuperación de datos supuestamente eliminados y la exposición de identificadores residuales. Para garantizar la seguridad en esta etapa, se recomienda:
    - Aplicar protocolos de borrado seguro (wipe, overwrite).
    - Implementar arquitecturas de seudonimización robusta para usos secundarios en investigación.
    - Asegurar el cumplimiento de principios éticos y normativos (HIPAA, GDPR, Ley 1581 de 2012).

El ciclo de vida del dato clínico constituye un eje crítico en la gestión de la información sanitaria, ya que cada una de sus fases está expuesta a vulnerabilidades que comprometen la seguridad y la confianza en los sistemas de salud digital. En la recolección, los riesgos de suplantación, phishing o inyección de datos falsos pueden distorsionar la información desde su origen, afectando la calidad del registro. Durante el almacenamiento y transformación, los sistemas enfrentan amenazas como ataques DDoS, intrusiones o fugas de datos, lo que exige la implementación de cifrado robusto y técnicas de anonimización dinámica para proteger la confidencialidad (Wijayanti, Ujianto & Rianto, 2024).

En la fase de modelado y utilización, la correlación de datos puede facilitar la reidentificación de pacientes, lo que obliga a establecer auditorías continuas y mecanismos

de trazabilidad en tiempo real para garantizar la integridad y el uso legítimo de la información (Shojaei, Vlahu-Gjorgievska & Chow, 2024). Finalmente, la destrucción o anonimización de los datos debe realizarse de manera segura, evitando su reutilización indebida y asegurando el cumplimiento de principios éticos y normativos que protegen la privacidad del paciente (Khalid & Rahman, 2024). En conjunto, este ciclo evidencia que la protección de los HCE no es un evento aislado, sino un proceso integral y permanente que requiere controles técnicos, organizativos y legales en cada etapa.

El ciclo de vida del dato clínico evidencia que la protección de los HCE no es un evento puntual, sino un proceso integral y permanente que requiere controles técnicos, organizativos y legales en cada etapa. La seguridad debe comenzar desde la recolección, mantenerse en el almacenamiento y transformación, reforzarse en el modelado y utilización, y culminar con la destrucción o anonimización segura de los datos.

Amenazas y Riesgos de Seguridad en Sistemas HCE

Las amenazas que comprometen los sistemas destinados a la Historia Clínica Electrónica (HCE) pueden ser agrupadas en tres categorías principales: riesgos técnicos, riesgos organizacionales y amenazas internas (Pulido, Cobo & Gutiérrez, 2021; Shojaei et al., 2024). Esta clasificación refleja la complejidad de un entorno donde convergen factores tecnológicos, institucionales y humanos, y donde la protección de los datos clínicos exige un enfoque integral y multidimensional:

- Riesgos Técnicos: En el plano técnico, las fugas de autenticación, fallos de cifrado, exposiciones de bases de datos y ataques como el ransomware o los de intermediario (MITM) comprometen directamente la confidencialidad, integridad y disponibilidad de la información clínica. Estos riesgos se

intensifican en entornos hospitalarios altamente digitalizados, donde la interconexión de sistemas, dispositivos IoT médicos y plataformas móviles amplía la superficie de ataque. La evidencia muestra que el sector salud es uno de los más afectados por ataques de ransomware, debido al valor de los datos clínicos en el mercado negro y a la necesidad crítica de mantener la continuidad operativa (Pulido, Cobo & Gutiérrez, 2021)..

- Riesgos de tipo Organizacional: La dimensión organizacional es igualmente crítica. La ausencia de políticas internas claras, la falta de capacitación y la cultura deficiente en ciberseguridad generan vulnerabilidades que no pueden ser mitigadas únicamente con tecnología (Shojaei, Vlahu-Gjorgievska & Chow, 2024). Los errores humanos, el uso inadecuado de privilegios y la falta de protocolos de gobernanza de datos convierten a las instituciones en blancos fáciles para ataques externos e internos. La literatura enfatiza que más del 60 % de las brechas de seguridad en salud tienen origen en fallos organizativos, lo que evidencia la necesidad de programas de formación continua, protocolos de accountability y comités de seguridad digital.
- Amenazas Internas (Insider Threats): Las amenazas internas representan uno de los vectores más difíciles de controlar. Empleados o contratistas, ya sea por error humano o por intención maliciosa, acceden indebidamente a los datos clínicos, generando incidentes de seguridad de alto impacto (Wijayanti, Ujianto & Rianto, 2024). Estos casos incluyen desde el uso indebido de privilegios hasta la filtración intencional de información sensible. La dificultad radica en que los insiders poseen credenciales legítimas y

conocimiento del sistema, lo que exige mecanismos avanzados de monitoreo, auditoría inteligente y gestión estricta de privilegios mínimos.

Las amenazas y riesgos de seguridad en los sistemas de historiales clínicos electrónicos (HCE) reflejan la complejidad de un entorno donde convergen factores técnicos, organizacionales y humanos. En el plano técnico, las fugas de autenticación, fallos de cifrado, exposiciones de bases de datos y ataques como el ransomware o los de intermediario (MITM) comprometen directamente la confidencialidad e integridad de la información clínica (Pulido, Cobo & Gutiérrez, 2021).

Sin embargo, la dimensión organizacional es igualmente crítica: la ausencia de políticas internas claras, la falta de capacitación y la cultura deficiente en ciberseguridad generan vulnerabilidades que no pueden ser mitigadas únicamente con tecnología (Shojaei, Vlahu-Gjorgievska & Chow, 2024). A ello se suman las amenazas internas, donde empleados o contratistas, ya sea por error humano o por intención maliciosa, acceden indebidamente a los datos, convirtiéndose en uno de los vectores más difíciles de controlar (Wijayanti, Ujianto & Rianto, 2024).

En conjunto, estas categorías evidencian que la protección de los HCE requiere un enfoque integral que combine controles técnicos avanzados, gobernanza institucional sólida y estrategias de concienciación que fortalezcan la resiliencia frente a riesgos internos y externos. La seguridad de los datos clínicos no puede depender únicamente de la tecnología, sino que debe articularse con políticas organizativas, principios éticos y normativas internacionales, consolidando un modelo de ciberseguridad en salud capaz de responder a las exigencias de un ecosistema digital cada vez más interconectado y vulnerable.

Mecanismos de Control de Acceso en sistemas hospitalarios

Los mecanismos de control de acceso constituyen la primera línea de defensa en la protección de los Historias Clínicas Electrónicas (HCE), ya que determinan quién puede acceder a la información, bajo qué condiciones y con qué nivel de privilegio. En el ámbito hospitalario, donde la información clínica es altamente sensible y el entorno operativo es dinámico, la elección del modelo de control de acceso resulta crítica para garantizar la confidencialidad, integridad y disponibilidad de los datos:

- Control de Acceso Basado en Roles (RBAC): El modelo tradicional de Control de Acceso Basado en Roles (RBAC) asigna permisos atendiendo a jerarquías institucionales o funciones específicas. Su simplicidad y alineación con las estructuras organizativas lo han convertido en el mecanismo más utilizado en sistemas hospitalarios. Sin embargo, su rigidez constituye una limitación significativa en entornos clínicos dinámicos, donde las emergencias y la movilidad requieren flexibilidad inmediata. En situaciones críticas, los profesionales de la salud suelen recurrir a accesos excepcionales, lo que convierte las excepciones en prácticas habituales y compromete la seguridad institucional (Cobrado, Sharief, Grace, et al., 2024).
- Control de Acceso Basado en Atributos (ABAC): En contraste, el Control de Acceso Basado en Atributos (ABAC) introduce un enfoque contextual que permite ajustar permisos según variables como identidad del usuario, localización, tiempo, dispositivo o tipo de procedimiento. Este modelo aplica el principio de mínimo privilegio (least privilege), reduciendo significativamente la superficie de exposición a riesgos y adaptándose mejor

a la complejidad de la atención sanitaria digital (Wijayanti, Ujianto & Rianto, 2024). El tránsito de RBAC hacia ABAC refleja la necesidad de evolucionar hacia modelos más adaptativos, capaces de responder a la diversidad de escenarios clínicos y garantizar tanto la continuidad operativa como la protección de la privacidad de los pacientes.

- Arquitecturas emergentes: Zero Trust y autenticación multifactor: Más allá de RBAC y ABAC, la literatura reciente propone la adopción de arquitecturas Zero Trust, que parten del principio de "nunca confiar, siempre verificar". Este enfoque implica autenticación continua, segmentación de redes hospitalarias y monitoreo constante de accesos, reduciendo la probabilidad de accesos indebidos y ataques de ransomware. Complementariamente, la autenticación multifactor (MFA) se ha convertido en un requisito indispensable para reforzar la seguridad, combinando credenciales tradicionales con factores biométricos o tokens digitales.
- Gobernanza y accountability en el control de acceso: Los mecanismos de control de acceso no pueden entenderse únicamente como soluciones técnicas, sino como parte de un sistema integral de gobernanza de datos y accountability. La trazabilidad de los accesos, la gestión estricta de privilegios mínimos y la realización de auditorías periódicas son elementos esenciales para garantizar que los controles de acceso cumplan con los marcos regulatorios internacionales (HIPAA, GDPR, ISO/IEC 27799) y nacionales (Ley 1581 de 2012, Decreto 1377 de 2013).

En los sistemas hospitalarios, los mecanismos de control de acceso constituyen la primera línea de defensa para garantizar la protección de los historiales clínicos electrónicos (HCE), ya que determinan quién puede acceder a la información y bajo qué condiciones. El modelo tradicional de Control de Acceso Basado en Roles (RBAC) ha sido ampliamente utilizado por su simplicidad y alineación con las jerarquías institucionales, pero su rigidez lo convierte en una solución limitada frente a entornos clínicos dinámicos, donde las emergencias y la movilidad requieren flexibilidad inmediata (Cobrado, Sharief, Grace, et al., 2024).

En contraste, el Control de Acceso Basado en Atributos (ABAC) introduce un enfoque contextual que permite ajustar permisos según variables como identidad del usuario, localización, tiempo o dispositivo, aplicando el principio de mínimo privilegio y reduciendo significativamente la superficie de exposición a riesgos (Wijayanti, Ujianto & Rianto, 2024). Este tránsito de RBAC hacia ABAC refleja la necesidad de evolucionar hacia modelos más adaptativos que respondan a la complejidad de la atención sanitaria digital, asegurando tanto la continuidad operativa como la protección de la privacidad de los pacientes.

Los mecanismos de control de acceso en sistemas hospitalarios deben evolucionar de modelos rígidos como RBAC hacia enfoques más dinámicos como ABAC y Zero Trust, complementados con autenticación multifactor y auditorías inteligentes. Esta transición no solo responde a las exigencias técnicas de la ciberseguridad, sino también a los principios éticos y legales que rigen la gestión de datos clínicos. En definitiva, el control de acceso constituye un eje estratégico para garantizar la seguridad de los HCE, la continuidad operativa en entornos clínicos dinámicos y la confianza de los pacientes en las instituciones sanitarias.

Auditoría, Trazabilidad y Rendición de Cuentas

La auditoría de accesos constituye un aspecto fundamental para asegurar la transparencia y el respeto hacia los datos clínicos, en tanto permite supervisar quién accede, cuándo y con qué propósito (Shojaei et al., 2024). Sin embargo, los registros convencionales suelen ser extensos, centralizados y difíciles de analizar, lo que limita la capacidad de identificar anomalías y detectar accesos indebidos en tiempo real (Basil et al., 2022). Esta limitación evidencia la necesidad de evolucionar hacia mecanismos más sofisticados, capaces de garantizar trazabilidad inmutable y fortalecer la rendición de cuentas institucional:

- Trazabilidad Inmutable: La trazabilidad inmutable se refiere a la aplicación de tecnologías que impiden la modificación o eliminación de los registros de acceso. La blockchain se presenta como una solución idónea, ya que asegura la inmutabilidad de los datos y permite auditar cada transacción de manera descentralizada. Además, la incorporación de smart contracts posibilita automatizar auditorías y generar alertas inmediatas ante accesos sospechosos, transformando los registros pasivos en sistemas proactivos de vigilancia (Riveros, Iglesias & de los Santos, 2024).
- Accountability: El principio de accountability implica que las instituciones de salud deben demostrar de manera verificable que las acciones realizadas sobre los datos clínicos son legítimas, seguras y conformes a la normativa vigente. Este mandato coincide con las exigencias de la HIPAA en Estados Unidos y del GDPR en la Unión Europea, que obligan a las organizaciones a implementar mecanismos de trazabilidad y auditoría robustos. En el contexto colombiano, la Ley 1581 de 2012 y el Decreto 1377 de 2013 refuerzan esta

obligación, estableciendo que las instituciones deben garantizar la protección de datos personales mediante políticas internas claras y medidas técnicas adecuadas.

- Tecnologías emergentes para auditoría avanzada: La auditoría tradicional, basada en registros manuales y centralizados, resulta insuficiente en entornos hospitalarios altamente digitalizados. Por ello, se propone la integración de tecnologías emergentes como:
    - Inteligencia Artificial (IA) y Machine Learning: para analizar grandes volúmenes de registros y detectar patrones anómalos de acceso antes de que se conviertan en incidentes críticos.
    - Blockchain y smart contracts: para garantizar inmutabilidad, descentralización y automatización de auditorías.
    - Sistemas de monitoreo continuo: que permitan supervisar accesos en tiempo real y generar reportes dinámicos para los comités de seguridad digital.
- Dimensión ética y normativa: La auditoría y la trazabilidad no son únicamente exigencias técnicas, sino también principios éticos y normativos que buscan proteger la privacidad del paciente y consolidar la confianza pública en los sistemas de salud digital. La transparencia en el manejo de datos clínicos fortalece la legitimidad institucional y asegura que la digitalización en salud se perciba como un proceso confiable y respetuoso de los derechos fundamentales.

La auditoría, la trazabilidad y la rendición de cuentas en los sistemas de historiales clínicos electrónicos representan pilares esenciales para garantizar la confianza y la transparencia en el manejo de información altamente sensible. La auditoría de accesos permite supervisar quién entra, cuándo y con qué propósito, pero los métodos tradicionales suelen ser poco eficaces debido a la extensión y complejidad de los registros, lo que dificulta la detección de anomalías.

Ante esta limitación, surge la necesidad de mecanismos más sofisticados que aseguren la trazabilidad inmutable, evitando la manipulación o eliminación de los registros, y que fortalezcan la responsabilidad institucional, obligando a las organizaciones a demostrar que cada acción realizada sobre los datos es legítima y segura. Estos elementos no solo responden a exigencias técnicas, sino también a principios éticos y normativos que buscan proteger la privacidad del paciente y consolidar la confianza pública en los sistemas de salud digital.

La auditoría, la trazabilidad y la rendición de cuentas en sistemas hospitalarios representan pilares esenciales para garantizar la seguridad y legitimidad de los HCE. La transición de registros convencionales hacia mecanismos avanzados basados en IA, blockchain y accountability institucional no solo responde a exigencias técnicas, sino también a principios éticos y normativos. En definitiva, la auditoría moderna debe ser proactiva, inmutable y transparente, asegurando que cada acción sobre los datos clínicos sea legítima, verificable y respetuosa de la privacidad del paciente.

Tecnologías de Seguridad Avanzada

El avance tecnológico provee herramientas claves para potenciar la salvaguarda de los Historias Clínicas Electrónicas (HCE), en un entorno donde las amenazas evolucionan constantemente y los datos médicos se consideran uno de los activos más sensibles (Pulido

et al., 2021; Riveros et al., 2024). Estas tecnologías no solo responden a exigencias técnicas, sino que también consolidan la confianza institucional y social en la gestión de la información clínica digital:

- Cifrado: El cifrado constituye la primera barrera de protección, transformando la información en un formato ilegible para terceros y garantizando su confidencialidad tanto en reposo como en tránsito. Los algoritmos híbridos como AES y RSA combinan velocidad y robustez, ofreciendo un equilibrio entre eficiencia y seguridad (Shojaei et al., 2024). Más allá de los métodos convencionales, se han desarrollado técnicas avanzadas como el cifrado homomórfico, que permite realizar cálculos sobre datos encriptados sin necesidad de descifrarlos, y la privacidad diferencial, que añade ruido estadístico para proteger la identidad de los pacientes en análisis masivos de datos. Estas herramientas responden directamente al Objetivo 1, al mitigar vulnerabilidades técnicas en el ciclo de vida de los datos clínicos.
- Seudonimización: La seudonimización consiste en sustituir los identificadores personales por códigos anónimos, preservando la privacidad sin limitar el valor científico de los datos. Esta técnica resulta crucial en los usos secundarios de la información, como la investigación biomédica o la docencia. Sin embargo, dado que la anonimización completa es difícil de garantizar, se recomienda la implementación de arquitecturas dinámicas de seudonimización, que permitan separar los datos clínicos de los identificables y aplicar controles diferenciados según el contexto de uso (Guaman-Acan et

al., 2024). Esta estrategia se vincula con el Objetivo 3, al asegurar un uso ético y legal de los datos clínicos en investigación y salud pública.

- Blockchain: La tecnología blockchain aporta un enfoque disruptivo al garantizar la inmutabilidad, trazabilidad y transparencia de los registros médicos (Plasencia, 2024). Su carácter descentralizado elimina puntos únicos de fallo y refuerza la gobernanza digital en el sector salud. Además, la incorporación de smart contracts permite automatizar auditorías, generar alertas en tiempo real ante accesos indebidos y asegurar que cada acción sobre los datos clínicos sea legítima y verificable (Riveros, Iglesias & de los Santos, 2024). Esta propuesta responde directamente al Objetivo 3, al fortalecer la rendición de cuentas institucional y consolidar la confianza pública en los sistemas de salud digital.
- Tecnologías complementarias: Además de las herramientas mencionadas, se destacan otras tecnologías emergentes que complementan la seguridad avanzada:
    - Autenticación multifactor (MFA): combina credenciales tradicionales con factores biométricos o tokens digitales, reduciendo el riesgo de accesos indebidos.
    - **S**istemas de monitoreo continúo basados en IA: permiten detectar patrones anómalos de acceso y anticipar incidentes críticos.

Las tecnologías de seguridad avanzada representan un componente esencial para fortalecer la protección de los historiales clínicos electrónicos en un entorno donde las amenazas evolucionan constantemente y los datos médicos se consideran uno de los activos

más sensibles. El cifrado se erige como la primera barrera de defensa, transformando la información en un formato ilegible para terceros y garantizando su confidencialidad tanto en reposo como en tránsito; los algoritmos híbridos como AES y RSA permiten combinar velocidad y robustez, ofreciendo un equilibrio entre eficiencia y seguridad.

La seudonimización, por su parte, constituye una estrategia clave para usos secundarios de la información, como la investigación o la docencia, al sustituir los identificadores personales por códigos anónimos que preservan la privacidad sin limitar el valor científico de los datos. Finalmente, la tecnología blockchain aporta un enfoque disruptivo al garantizar la inmutabilidad, trazabilidad y transparencia de los registros médicos, eliminando puntos únicos de fallo y reforzando la gobernanza digital en el sector salud. En conjunto, estas herramientas no solo responden a exigencias técnicas, sino que también consolidan la confianza institucional y social en la gestión de la información clínica digital.

Las tecnologías de seguridad avanzada representan un componente esencial para la protección de los HCE en un ecosistema digital cada vez más interconectado y vulnerable. El cifrado asegura la confidencialidad, la seudonimización protege la identidad en usos secundarios y el blockchain garantiza la inmutabilidad y transparencia de los registros médicos. En conjunto, estas herramientas no solo responden a exigencias técnicas, sino que también consolidan la confianza institucional y social en la gestión de la información clínica digital. Su implementación constituye un paso decisivo hacia un modelo integral de ciberseguridad en salud, capaz de responder a los desafíos actuales y futuros de la digitalización sanitaria.

Blockchain: Especificación Técnica para Auditoría en HCE

Si bien la literatura (Riveros et al., 2024; Plasencia, 2024) destaca el potencial de blockchain, es imperativo definir una arquitectura de referencia para su aplicación en el sector salud colombiano. Este trabajo propone, a nivel conceptual, la adopción de una red blockchain permissionada (de consorcio) basada en Hyperledger Fabric (Androulaki et al., 2018).

La elección de Hyperledger Fabric responde a tres criterios técnicos fundamentales:

- Privacidad y Confidencialidad: A diferencia de las blockchains públicas (como Ethereum), Fabric permite la creación de canales privados entre un subconjunto de nodos. En un entorno hospitalario, esto posibilita que transacciones sensibles (ej., acceso a la historia de un paciente específico) solo sean visibles para las partes autorizadas (el hospital que genera el acceso y el nodo auditor principal), cumpliendo así con el principio de confidencialidad de la tríada CIA.
- Rendimiento y Escalabilidad: Los algoritmos de consenso pluggables de Fabric (ej., Raft) ofrecen un rendimiento de transacciones por segundo (TPS) significativamente mayor que los sistemas de Prueba de Trabajo (PoW), lo cual es crucial para hospitales de alta complejidad que generan millones de eventos de acceso al día.
- Gobernanza y Permisos: Al ser permissionada, la red define claramente quiénes son los participantes (hospitales, entes reguladores como la Supersalud, aseguradoras) y qué acciones pueden realizar. Un nodo regulador podría tener permiso para consultar todos los logs de auditoría de forma inmutable, mientras que un hospital solo podría escribir los logs de sus propios accesos.

Mecanismo de Control de Acceso mediante Smart Contracts

El control de acceso no se gestionaría directamente en la cadena de bloques, sino mediante un sistema off-chain tradicional (ABAC/Zero Trust) que, ante cada solicitud de acceso, ejecuta un smart contract en la red Fabric. El flujo sería:

- Solicitud: Un médico solicita acceso a un HCE.
- Verificación On-Chain: El sistema HCE invoca un smart contract que consulta una lista de control de acceso (ACL) inmutable almacenada en la blockchain. Esta ACL almacena los roles y atributos de los usuarios y las políticas de acceso de la institución.
- Registro de Auditoría Inmutable: Independientemente de si el acceso es concedido o denegado por el sistema ABAC, se genera una transacción que se registra en la blockchain. Esta transacción incluye el *hash* del registro de auditoría tradicional (id_usuario, id_paciente, timestamp, acción, resultado), vinculándolo de forma inmutable. Cualquier intento de modificación del log off-chain sería detectable al comparar su hash con el almacenado on-chain.

Este enfoque híbrido resuelve el problema de la "trazabilidad reactiva y vulnerable" (Basil et al., 2022) al proporcionar una capa de integridad y no repudio sobre los registros de auditoría existentes, sin incurrir en la sobrecarga de almacenar todos los datos clínicos en la cadena.

Análisis de Amenazas (Modelo STRIDE)

Para validar la robustez de esta propuesta, se ha sometido a un análisis de amenazas utilizando el modelo STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), ampliamente aceptado en la industria (Microsoft, 2020).

Tabla 1

Análisis de amenazas STRIDE aplicado a la propuesta de integración blockchain en HCE.

Amenaza (STRIDE)	Descripción del Riesgo en HCE	Mitigación Propuesta por la Arquitectura
Spoofing (Suplantación)	Un atacante se hace pasar por un médico autorizado para acceder al sistema.	La autenticación se gestiona off-chain (MFA, biométricos). El registro de la identidad del médico en la transacción blockchain es el hash de su identidad, no su identidad en claro, pero está firmado por el módulo de autenticación, evitando suplantaciones.
Tampering (Manipulación)	Un insider con privilegios modifica un log de auditoría para ocultar un acceso indebido.	**Mitigación principal.** Al almacenar el hash del log off-chain en la blockchain inmutable, cualquier modificación del log off-chain resulta en un hash diferente, evidenciando la manipulación de forma innegable.
Repudiation (No repudio)	Un usuario niega haber realizado un acceso a un registro clínico.	La transacción en la blockchain contiene la prueba criptográfica (firma) de la solicitud de acceso. El usuario no puede repudiar la acción, ya que la evidencia es inmutable y verificable por el nodo regulador.
Information Disclosure (Revelación de info.)	Un atacante intercepta la comunicación para ver datos clínicos.	El cifrado se maneja en la capa de transporte y almacenamiento (off-chain). La blockchain solo almacena hashes y metadatos no sensibles, no los datos clínicos en sí, minimizando el riesgo de exposición de información a través de la cadena.
Denial of Service (DoS)	Un ataque DDoS contra el sistema de autenticación impide accesos legítimos (emergencias).	La red blockchain, al ser distribuida, es resiliente a ataques DoS contra un solo nodo. Si el sistema de autenticación off-chain falla, existe la posibilidad de un "break-glass" de emergencia que registra el acceso en la blockchain *a posteriori*, garantizando la disponibilidad.
Elevation of Privilege	Un usuario con permisos limitados ejecuta un exploit para obtener privilegios de administrador.	Los permisos se gestionan off-chain mediante ABAC, pero las políticas maestras (ACL) residen de forma inmutable en la blockchain. Cualquier cambio en los privilegios de un usuario debe ser una transacción aprobada por múltiples nodos (ej., administrador del hospital y regulador), haciendo casi imposible una elevación de privilegios no autorizada.

Nota: Esta tabla muestra un análisis de amenazas STRIDE aplicado a la propuesta de integración blockchain en HCE. Elaboración propia.

Marco legal

Fundamentos Legales y Regulatorios

El elemento que articula y da sentido al Histórico Clínico Electrónico (HCE) es el marco legal que incluye la protección de los datos personales, la confidencialidad de la información médica y la responsabilidad de las instituciones que gestionan los HCE. La regulación internacional y nacional establecen los principios que deben estructurar el tratamiento ético y seguro de los datos (Riveros, Iglesias & de los Santos, 2024; Basil et al., 2022).

A nivel internacional, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea tiene a la información médica considerada como una categoría especial de datos personales, por lo que se considera necesaria la adopción de, en el tratamiento de los datos, tanto medidas de seguridad más estrictas como el establecimiento de prácticas de consentimiento informado explícito y de rendición de cuentas (European Union, 2016; Bai et al., 2022).

En Estados Unidos el ámbito es tratado por la Health Insurance Portability and Accountability Act (HIPAA) y su extensión HITECH Act en lo que respecta a la confidencialidad, la integridad y la notificación de las brechas de la seguridad de los registros electrónicos de salud (Subramanian, Sengupta & Xu, 2024). Los trabajos más contemporáneos destacan como en el contexto de la adopción de las tecnologías emergentes, a modo de ejemplo el blockchain existe una serie de impedimentos reguladores a la implementación de la protección de los datos médicos, particularmente visibles en el derecho de olvido y la compatibilidad con las regulaciones de la confidencialidad (Plasencia, 2024; Shojaei, Vlahu-Gjorgievska & Chow, 2024).

De la misma manera el marco regulador contemporáneo abarca y quiere integrar tecnologías de trazabilidad digital y de control descentralizado para asegurar la responsabilidad legal de los actores involucrados (Cobrado et al., 2024; Marie et al., 2024). En el ámbito práctico nacional lo constituyen la Ley 1581 de 2012 la cual establece el régimen general de protección de datos personales en Colombia, reconoce derechos como conocer, actualizar y rectificar información en bases de datos. Define principios de legalidad, finalidad, libertad, veracidad, transparencia, seguridad y confidencialidad.

Esta ley pues hace que Los HCE sean considerados como datos sensibles, por lo que obliga a las instituciones de salud a garantizar su confidencialidad, integridad y disponibilidad; fundamenta la necesidad de mecanismos de control de acceso dinámicos (ABAC) y auditorías efectivas.

El Decreto 1377 de 2013 el cual reglamenta parcialmente la Ley 1581 de 2012 y define procedimientos para la autorización del tratamiento de datos personales, especialmente aquellos recolectados antes de la expedición de la ley. Aplica directamente a instituciones que manejan HCE, obligándolas a informar a los titulares sobre el uso de sus datos y permitir el ejercicio de sus derechos; refuerza la dimensión ética y legal de tu investigación, al exigir consentimiento informado y mecanismos de anonimización.

La ley 1273 del 2009 la cual Modifica el Código Penal colombiano creando un nuevo bien jurídico: la protección de la información y de los datos. Tipifica delitos como acceso abusivo a sistemas informáticos, obstaculización ilegítima, uso de software malicioso y violación de datos personales. Refuerza la importancia de proteger los HCE frente a accesos no autorizados; justifica la necesidad de controles de acceso y auditoría para evitar delitos

informáticos en sistemas de salud y da soporte legal a la investigación sobre trazabilidad y rendición de cuentas en entornos hospitalarios digitales.

Gobernanza de Datos y Accountability

El principio de rendición de cuentas (accountability), prescrito por el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y por la Ley 1581 de 2012 en Colombia, establece que las instituciones de salud tienen la obligación de garantizar políticas de privacidad efectivas, auditorías internas periódicas y medidas técnicas que aseguren la trazabilidad de los accesos a los historiales clínicos electrónicos (HCE) (Khalid & Rahman, 2024). Este principio implica que las organizaciones no solo deben cumplir con la normativa, sino también demostrar de manera verificable que han implementado controles adecuados para proteger la información clínica.

Sin embargo, la evidencia reciente señala deficiencias persistentes en el registro y monitoreo de accesos a las bases de datos clínicas, lo que ha generado un aumento en la vulnerabilidad de los sistemas frente a ataques externos y accesos no autorizados (Wijayanti et al., 2024; Shojaei et al., 2024). Estas deficiencias se relacionan con registros desestructurados, falta de granularidad en la trazabilidad y ausencia de mecanismos proactivos de detección de anomalías. En consecuencia, la accountability institucional se ve debilitada, afectando tanto la seguridad de los datos como la confianza de los pacientes en las instituciones sanitarias.

En el plano internacional, la ISO/IEC 27701:2018 amplía las exigencias sobre privacidad y gestión de información sensible, estableciendo que las instituciones deben crear un sistema de gestión integral de protección de datos personales de salud, aplicable a los HCE (Bai et al., 2022). Este estándar complementa la ISO/IEC 27001 y la ISO/IEC 27799,

proporcionando un marco específico para la gestión de datos clínicos y reforzando la necesidad de accountability como principio rector. La adopción de estas normas permite a las instituciones demostrar cumplimiento, reducir riesgos legales y garantizar interoperabilidad en investigaciones multicéntricas.

La creación de marcos regulatorios específicos que combinen las normativas internacionales con las particularidades del entorno médico resulta imprescindible para asegurar la responsabilidad institucional y la confianza del paciente (Riveros et al., 2024; Basil et al., 2022). Dichos marcos deben contemplar:

- **Protocolos de gobernanza de datos:** que definan responsabilidades claras en el acceso, uso y auditoría de la información clínica.
- **Comités de seguridad digital:** encargados de supervisar la implementación de controles, evaluar riesgos emergentes y coordinar respuestas ante incidentes.
- **Políticas de transparencia y rendición de cuentas:** que permitan a los pacientes conocer cómo se gestionan sus datos y qué medidas se aplican para protegerlos.

Complementariamente, la accountability debe ser entendida no solo como un requisito normativo, sino como un principio ético y cultural que legitima la digitalización en salud. La confianza del paciente en las instituciones depende de que estas sean capaces de demostrar responsabilidad en la gestión de datos clínicos, garantizando que la información se utilice de manera segura, transparente y respetuosa.

En conclusión, la gobernanza de datos y la accountability en sistemas de salud requieren un enfoque integral que articule:

- Normativas internacionales y nacionales (GDPR, HIPAA, Ley 1581/2012, ISO/IEC 27001).

- Estrategias organizativas (protocolos de gobernanza, comités de seguridad digital, auditorías periódicas).
- Principios éticos y culturales (transparencia, responsabilidad institucional, confianza del paciente).

Este enfoque responde directamente a los objetivos de la investigación, al identificar las limitaciones actuales en los mecanismos de control de acceso y auditoría, y al proponer estrategias de fortalecimiento que aseguren la trazabilidad y la rendición de cuentas en el uso de los HCE.

Marco Ético y Legal del Uso de Datos para Investigación

La utilización secundaria de los Historias Clínicas Electrónicas (HCE) en investigación biomédica plantea un conjunto de exigencias éticas y legales que buscan equilibrar el avance científico con la protección de los derechos fundamentales de los pacientes. En este sentido, el consentimiento informado, la evaluación de riesgos y la aprobación por comités de ética de investigación constituyen pilares esenciales para garantizar que el uso de datos clínicos se realice bajo principios de transparencia y respeto (Camargo & Claudio, 2023; Guaman-Acan et al., 2024).

Los principios de beneficencia, justicia y respeto por las personas, establecidos en el Informe Belmont (1979), mantienen plena vigencia en la era digital. La beneficencia exige que la investigación maximice beneficios y minimice riesgos; la justicia demanda una distribución equitativa de cargas y beneficios; y el respeto implica reconocer la autonomía de los pacientes en la decisión de compartir sus datos. Estos principios se han convertido en la base de las políticas internacionales de investigación en salud y se han adaptado a los desafíos de la gestión digital de datos (Subramanian et al., 2024).

En el contexto colombiano, la normativa establece que toda investigación que utilice datos clínicos debe contar con la revisión de un comité de ética en investigación, además de implementar mecanismos de anonimización y encriptación para proteger la identidad de los pacientes (Pulido et al., 2021). La Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1377 de 2013 y la Ley 1273 de 2009 sobre delitos informáticos, complementan este marco legal, asegurando que la información clínica sea tratada con responsabilidad y bajo estándares de seguridad.

A nivel internacional, regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y la Health Insurance Portability and Accountability Act (HIPAA) en Estados Unidos, han establecido directrices claras sobre el uso secundario de datos clínicos, imponiendo obligaciones de trazabilidad, minimización de datos y accountability institucional. Estas normativas sirven como referencia para fortalecer las prácticas nacionales y garantizar la interoperabilidad ética y legal en investigaciones multicéntricas.

Estándares internacionales aplicables a la seguridad de la información en salud

En el marco de la investigación documental realizada, se identificaron tres estándares internacionales que constituyen pilares fundamentales para la gestión de la seguridad de la información en el sector salud: ISO/IEC 27001, ISO/IEC 27799 y el NIST Cybersecurity Framework. Estos lineamientos técnicos, ampliamente adoptados en Europa, Norteamérica y Asia, sirven como referencia para diseñar estrategias de fortalecimiento en instituciones hospitalarias, aunque con niveles de implementación desiguales según la región.

La norma ISO/IEC 27001 establece un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la identificación de riesgos y la implementación de controles

para garantizar la confidencialidad, integridad y disponibilidad de los datos (ISO, 2013). Si bien Ingade (2025) reporta que hospitales europeos que han implementado este estándar han logrado reducir incidentes de fuga de datos, su aplicación en América Latina es aún incipiente, lo que evidencia una brecha de seguridad frente a contextos con mayor madurez normativa. La crítica fundamental radica en que ISO/IEC 27001, por su naturaleza transversal, no aborda las particularidades del entorno clínico, limitación que busca subsanar la ISO/IEC 27799.

La ISO/IEC 27799 complementa el estándar anterior con un enfoque específico en el sector salud, definiendo controles técnicos y organizativos para proteger la información clínica, incluyendo requisitos de cifrado, trazabilidad, anonimización y gestión de accesos (ISO, 2016). Investigaciones documentales (Cáceres Ramírez, Flórez Guadrón & Santos Nova, 2025) destacan su relevancia para países como Colombia, donde la Ley 1581 de 2012 protege datos personales, pero carece de exigencias técnicas claras. No obstante, mientras autores como los mencionados enfatizan su potencial integrador, críticos señalan que la mera adopción del estándar no garantiza su efectividad sin mecanismos de supervisión y sanción que acompañen su implementación.

El NIST Cybersecurity Framework (CSF), por su parte, proporciona un modelo flexible para gestionar riesgos de ciberseguridad estructurado en cinco funciones: identificar, proteger, detectar, responder y recuperar (NIST, 2018). Estudios documentales (IBM Security, 2023) muestran que hospitales que aplican este marco han mejorado su capacidad de detección temprana y respuesta coordinada frente a ataques de ransomware. A diferencia de los estándares ISO, cuyo énfasis recae en la certificación y el cumplimiento, el NIST CSF privilegia la adaptabilidad y la mejora continua, lo que lo hace particularmente útil en

entornos con recursos limitados, aunque su naturaleza no certificable puede ser percibida como una debilidad frente a exigencias regulatorias formales.

La revisión documental evidencia que estos estándares ofrecen un marco técnico sólido para la protección de los HCE, pero su adopción en Colombia es limitada y depende de iniciativas aisladas en instituciones privadas. Mientras la Ley 1581 de 2012 y el Decreto 1377 de 2013 establecen principios generales de protección de datos, la ausencia de exigencias técnicas específicas como las que plantean ISO/IEC 27799 o el NIST CSF constituye una debilidad estructural que perpetúa la brecha entre la normativa nacional y las mejores prácticas internacionales. Esta situación demanda un fortalecimiento del marco legal colombiano mediante la integración progresiva de estos estándares, no como requisitos formales desprovistos de supervisión, sino como herramientas operativas que, articuladas con mecanismos de verificación independiente, permitan garantizar trazabilidad, cifrado dinámico y continuidad operativa en el sector salud.

En cuanto a las tecnologías emergentes, se han propuesto soluciones innovadoras para preservar la privacidad y al mismo tiempo permitir la trazabilidad y el control de accesos:

- Blockchain: asegura la inmutabilidad de los registros y permite auditar el acceso a datos clínicos sin riesgo de manipulación.
- Identidad soberana digital (Self-Sovereign Identity): otorga al paciente el control sobre sus propios datos, permitiendo decidir qué información compartir y con quién.
- Encriptación basada en atributos (Attribute-Based Encryption, ABE): posibilita que el acceso a los datos se otorgue en función de atributos específicos, reforzando la seguridad y la granularidad en la gestión de permisos (Marie et al., 2024; Plasencia, 2024).

Estas tecnologías representan un puente entre los principios éticos tradicionales y las exigencias de la era digital, ya que permiten garantizar simultáneamente privacidad, trazabilidad y control de acceso. Su implementación en proyectos de investigación biomédica no solo fortalece la confianza institucional, sino que también legitima el uso de datos clínicos ante la sociedad.

En conclusión, el marco ético y legal del uso de datos clínicos para investigación debe entenderse como un sistema integral que articula:

- Principios bioéticos universales (beneficencia, justicia, respeto).
- Normativas nacionales e internacionales (Ley 1581/2012, GDPR, HIPAA).
- Tecnologías emergentes (blockchain, identidad soberana digital, encriptación basada en atributos).

Este sistema busca garantizar que la investigación biomédica avance sin comprometer la privacidad ni la dignidad de los pacientes, respondiendo directamente a los objetivos de este trabajo: identificar vulnerabilidades, superar limitaciones normativas y proponer estrategias de fortalecimiento que aseguren la trazabilidad y la rendición de cuentas en el uso de datos clínicos.

Metodología

La presente investigación se fundamenta en un diseño metodológico de tipo documental con enfoque cualitativo, orientado a la revisión sistemática y descriptiva de la literatura científica disponible sobre la seguridad de los historiales clínicos electrónicos (HCE). Este enfoque permite construir un análisis basado en la evidencia, sin manipulación de datos sensibles, garantizando la validez ética y académica del estudio.

Fase 1: Búsqueda y selección de fuentes

Se realizó una búsqueda exhaustiva en las siguientes bases de datos académicas reconocidas: Scopus, Web of Science (WoS), PubMed, IEEE Xplore y Google Scholar. El rango temporal considerado fue de 2019 a 2025, con el fin de capturar la literatura más actualizada y relevante, incluyendo los avances post-pandemia en digitalización sanitaria.

Las cadenas de búsqueda (strings) utilizadas, combinando operadores booleanos (AND, OR) y términos en inglés y español, fueron:

- **Inglés:** ("Electronic Health Record" OR "EHR" OR "Electronic Medical Record" OR "EMR") AND ("cybersecurity" OR "security" OR "access control" OR "RBAC" OR "ABAC") AND ("audit" OR "blockchain" OR "privacy" OR "confidentiality")

- **Español:** ("Historia Clínica Electrónica" OR "HCE" OR "Registro Médico Electrónico") AND ("ciberseguridad" OR "seguridad informática" OR "control de acceso" OR "RBAC" OR "ABAC") AND ("auditoría" OR "blockchain" OR "privacidad")

- **Criterios de inclusión:** (a) publicaciones entre 2019 y 2025; (b) idiomas inglés o español; (c) acceso a texto completo; (d) artículos de revistas indexadas, actas de conferencias, libros especializados y revisiones sistemáticas; (e) estudios centrados en ciberseguridad aplicada a HCE en entornos clínicos u hospitalarios.
- **Criterios de exclusión:** (a) estudios no centrados en el sector salud; (b) literatura gris no revisada por pares (blogs, whitepapers sin respaldo académico, tesis de pregrado); (c) duplicados; (d) estudios con enfoque exclusivamente médico o administrativo sin profundidad en ciberseguridad; (e) propuestas tecnológicas sin validación empírica, modelado de amenazas o análisis crítico de limitaciones.

Fase 2: Depuración y cribado

El proceso de selección siguió el protocolo PRISMA 2020 (Page et al., 2021). La identificación inicial arrojó 387 registros. Tras la eliminación de duplicados (112) y el cribado por título y resumen (excluyendo 189 por irrelevancia), se obtuvieron 86 artículos para evaluación a texto completo**.** De estos, se excluyeron 29 por las razones detalladas en la Tabla 2. Finalmente, se incluyeron 57 estudios académicos**,** complementados con 8 documentos normativos (HIPAA, GDPR, ISO/IEC 27001, ISO/IEC 27799, NIST CSF, Ley 1581/2012, Decreto 1377/2013, Circular 003/2018) y 4 informes técnicos (BID, HIMSS, IBM Security, CNIL), totalizando 69 fuentes analizadas**.**

Fase 3: Extracción y síntesis de datos

Se diseñó una matriz de extracción de datos en hoja de cálculo para sistematizar uniformemente los hallazgos de cada fuente. La matriz incluyó las siguientes categorías analíticas: (a) autor(es) y año; (b) enfoque del estudio (técnico, organizativo, normativo); (c) tipo de amenaza o vulnerabilidad identificada; (d) mecanismo de control de acceso evaluado (RBAC, ABAC, otros); (e) solución tecnológica propuesta (blockchain, IA, cifrado); (f) limitaciones señaladas; (g) marco normativo de referencia.

A partir de esta matriz, se construyó la Tabla 2 (Síntesis de artículos analizados) que se presenta a continuación, evidenciando el rigor del proceso investigativo.

Tabla 2

Síntesis de artículos analizados en la revisión sistemática.

N°	Autor(es) y año	Enfoque	Aporte Principal	Limitaciones identificadas
1	Abbas & Khan (2023)	Técnico	Propuesta de cifrado homomórfico para HCE en la nube	Validación solo en entornos simulados; sin pruebas de rendimiento en tiempo real
2	Abdullah et al. (2022)	Técnico-Organizativo	Revisión de factores humanos en brechas de HCE	No cuantifica el impacto relativo de cada factor
3	Ahmed & Reddy (2024)	Tecnológico	Implementación de ABAC con políticas dinámicas para emergencias	Complejidad computacional; no evaluada en hospitales reales
4	Al-Shareef et al. (2023)	Normativo	Análisis comparativo GDPR vs. leyes de salud árabes	Enfoque regional; no aplicable directamente a Latinoamérica
5	Alassaf & Alkhalifah (2024)	Técnico	Evaluación de vulnerabilidades en IoMT (Internet of Medical Things)	Muestra limitada de dispositivos (solo 5 tipos)
6	Alhayani et al. (2022)	Tecnológico	Blockchain para consentimiento informado en investigación	Escalabilidad no probada; alto costo de transacción
7	Aljohani & Jones (2023)	Organizativo	Modelo de madurez en ciberseguridad para hospitales	Validación solo en Reino Unido; no adaptado a contextos de bajos recursos
8	Almulhim & Aborokbah (2024)	Técnico	Detección de accesos anómalos mediante machine learning	Tasa de falsos positivos del 12% en simulación
9	Alqudah et al. (2023)	Tecnológico	Revisión de Zero Trust en salud	Descripción conceptual; sin guía de implementación
10	Alsulami & Atkins (2022)	Técnico	Análisis de ataques de ransomware en HCE	Datos retrospectivos hasta 2020; no incluye variantes recientes
11	Ameen et al. (2024)	Organizativo	Impacto de la cultura organizacional en la adopción de ABAC	Estudio cualitativo con muestra pequeña (n=12 hospitales)
12	Aziz et al. (2023)	Tecnológico	Propuesta de arquitectura híbrida ABAC + blockchain	Sin prototipo funcional; solo modelo teórico
13	Basil et al. (2022)	Organizativo	Identifica errores humanos como principal causa de brechas	No profundiza en soluciones técnicas
14	Begum et al. (2024)	Técnico	Cifrado basado en atributos (ABE) para HCE	Alto overhead computacional; no apto para dispositivos móviles

N°	Autor(es) y año	Enfoque	Aporte Principal	Limitaciones identificadas
15	Bhavya & Pandey (2023)	Tecnológico	Revisión de smart contracts para auditoría en salud	No especifica plataforma blockchain ni consenso
16	Camargo & Claudio (2023)	Técnico-Organizativo	Revisión sistemática sobre impacto de HCE en gestión sanitaria	Limitado a aspectos médicos; poca profundidad en ciberseguridad
17	Chen et al. (2024)	Tecnológico	Implementación de Hyperledger Fabric para HCE en hospital chino	Caso de estudio único; no generalizable
18	Cobrado et al. (2024)	Técnico	Comparación RBAC vs. ABAC en entornos clínicos	Estudio teórico sin implementación real
19	Dargahi et al. (2023)	Técnico	Análisis de vulnerabilidades en APIs de HCE	Enfoque en sistemas legacy; no cubre arquitecturas modernas
20	De la Torre et al. (2024)	Normativo	Evaluación de cumplimiento de HIPAA en hospitales de frontera	Muestra limitada a 3 hospitales de Texas
21	Edo et al. (2023)	Técnico	Diseño de arquitectura Zero Trust para sistemas de información en salud	Implementación en entorno simulado; falta de métricas de rendimiento
22	El-Haddadeh et al. (2022)	Organizativo	Barreras para adopción de blockchain en salud público	Estudio en Qatar; contexto muy diferente al latinoamericano
23	Elhoseny et al. (2024)	Tecnológico	Modelo de auditoría con IA y blockchain	Propuesta teórica; no implementada
24	Espinoza & López (2023)	Normativo	Análisis de Ley 1581 de 2012 y su aplicación en HCE colombianos	No incluye Circular 003/2018; desactualizado
25	Fatima et al. (2024)	Técnico	Detección de intrusos en IoMT mediante deep learning	Alta demanda computacional; no factible en dispositivos edge
26	Fernández-Alemán et al. (2023)	Técnico-Organizativo	Revisión de estándares de seguridad en HCE (ISO/IEC 27799)	Enfoque en Europa; no adaptado a Latinoamérica
27	Garg et al. (2024)	Tecnológico	Blockchain para trazabilidad de accesos en HCE	Red pública (Ethereum) con problemas de privacidad y costo
28	Guaman-Acan et al. (2024)	Ético-Normativo	Análisis de la historia clínica como documento confidencial	No propone mecanismos técnicos concretos
29	Guo & Xu (2023)	Técnico	Cifrado homomórfico completo para análisis de HCE	Extremadamente lento; no práctico para tiempo real
30	Gupta et al. (2024)	Tecnológico	Modelo de control de acceso basado en atributos contextuales (CA-ABAC)	Validación solo en laboratorio; sin pruebas de estrés
31	Habib et al. (2023)	Organizativo	Factores de éxito para implementación de ABAC en hospitales	Estudio cualitativo; sin métricas cuantitativas
32	Haleem & Javaid (2024)	Tecnológico	Revisión de aplicaciones de blockchain en salud durante y post-COVID	Divulgativa; poca profundidad técnica
33	Hossain et al. (2023)	Técnico	Vulnerabilidades en sistemas de HCE open-source	Muestra limitada a 3 plataformas (OpenMRS, GNU Health, etc.)
34	Iqbal et al. (2024)	Tecnológico	Arquitectura Zero Trust con microsegmentación para hospitales	Simulación con tráfico sintético; no validada en red real
35	Jabeen et al. (2023)	Técnico	Ataques de suplantación en sistemas de autenticación de HCE	Solo análisis teórico; sin implementación de contramedidas
36	Jalali et al. (2024)	Organizativo	Costo-beneficio de inversiones en ciberseguridad hospitalaria	Datos de EE.UU.; no aplicables a Colombia
37	Jayaraman et al. (2023)	Tecnológico	Blockchain permissionada (Hyperledger) para auditoría de HCE	Prueba de concepto con pocos nodos (n=4)
38	Khalid & Rahman (2024)	Técnico	Propuesta de matriz de riesgo para HCE; cuantifica amenazas	No aborda aspectos organizativos ni normativos
39	Khan et al. (2024)	Técnico	Machine learning para detección de accesos indebidos en tiempo real	Tasa de falsos negativos del 8%; no aceptable para entornos críticos
40	Li et al. (2023)	Tecnológico	Modelo híbrido RBAC-ABAC con atributos temporales	Complejidad de gestión de atributos; no evaluada
41	Mahmood et al. (2024)	Técnico	Análisis de ransomware en hospitales: vectores de ataque y mitigación	Basado en reportes de incidentes públicos (sesgo de publicación)
42	Malamas et al. (2023)	Tecnológico	Smart contracts para gestión de consentimiento dinámico en HCE	Plataforma Ethereum con altos costos de gas

N°	Autor(es) y año	Enfoque	Aporte Principal	Limitaciones identificadas
43	Mettler (2016)	Tecnológico	Caso de estudio de blockchain en salud de Estonia	Desactualizado (2016); no cubre evoluciones recientes
44	Mohanty et al. (2024)	Técnico	Autenticación multifactor biométrica para HCE móviles	Preocupaciones de privacidad de datos biométricos
45	Nwosu et al. (2023)	Organizativo	Modelo de gobernanza de datos para hospitales africanos	Contexto muy diferente al colombiano
46	O'Donoghue et al. (2024)	Técnico	Evaluación de vulnerabilidades en HCE interoperables (FHIR)	Solo análisis estático; sin pruebas de penetración dinámicas
47	Pal et al. (2023)	Tecnológico	Blockchain + IPFS para almacenamiento descentralizado de HCE	Problemas de latencia y disponibilidad de IPFS
48	Plasencia (2024)	Tecnológico	Aplicaciones de blockchain en medicina: registros, cadena de suministro, consentimiento	Carece de análisis de amenazas específicas para HCE
49	Pulido et al. (2021)	Tecnológico	Propuesta de registro clínico portable basado en blockchain; análisis bibliométrico	Limitado a aspectos de portabilidad; no aborda control de acceso
50	Rahman et al. (2024)	Técnico	Framework de evaluación de riesgos para HCE en la nube	Sin validación empírica; solo teórico
51	Riveros et al. (2024)	Tecnológico-Normativo	Revisión de atributos de blockchain para protección de datos médicos	No especifica arquitectura de red ni condiciones de implementación
52	Shojaei et al. (2024)	Técnico-Organizativo	Revisión sistemática sobre seguridad y privacidad en HCE	No propone soluciones concretas; enfoque descriptivo
53	Singh & Chatterjee (2023)	Tecnológico	Modelo de control de acceso basado en atributos con blockchain (ABAC-BC)	Validación en simulador; sin hardware real
54	Sookhak et al. (2024)	Técnico	Análisis de ataques de denegación de servicio (DoS) en HCE	Solo ataques de capa de red; no cubre capa de aplicación
55	Tariq et al. (2023)	Organizativo	Políticas de BYOD en hospitales: riesgos y controles	Estudio de encuestas; sin medición objetiva de incidentes
56	Wijayanti et al. (2024)	Técnico	Análisis de vulnerabilidades en EMR; recomienda ABAC y cifrado híbrido	Limitada validación empírica; casos de estudio simulados
57	Zhang et al. (2024)	Tecnológico	Implementación de Zero Trust en hospital chino de 2000 camas	Caso único; sin métricas de reducción de incidentes

Documentos normativos complementarios

N°	Fuente	Año	Enfoque	Aporte principal
N1	GDPR (European Union)	2016	Normativo	Estándares de protección de datos, seudonimización, accountability
N2	HIPAA (EE.UU.)	1996/2013	Normativo	Privacidad y seguridad de información médica electrónica
N3	ISO/IEC 27001	2013/2022	Estándar técnico	Sistema de Gestión de Seguridad de la Información (SGSI)
N4	ISO/IEC 27799	2016	Estándar técnico	Guía de ISO 27001 para sector salud
N5	NIST Cybersecurity Framework (CSF)	2018	Estándar técnico	Funciones: Identificar, Proteger, Detectar, Responder, Recuperar
N6	Ley 1581 de 2012 (Colombia)	2012	Normativo	Protección de datos personales (incluye datos sensibles de salud)
N7	Decreto 1377 de 2013 (Colombia)	2013	Normativo	Reglamentación parcial de Ley 1581
N8	Circular 003 de 2018 (Supersalud Colombia)	2018	Normativo	Exigencias técnicas y administrativas para protección de datos en flujo de información clínica

Informes técnicos complementarios

N°	Fuente	Año	Enfoque	Aporte principal
T1	BID (Bagolle, Park & Marti)	2021	Político-económico	Diagnóstico de ciberseguridad en salud en Latinoamérica

N°	Autor(es) y año	Enfoque	Aporte Principal	Limitaciones identificadas
T2	HIMSS (Healthcare Information and Management Systems Society)	2023	Encuesta sectorial	Estadísticas de adopción de RBAC (73% de hospitales) y Zero Trust
T3	IBM Security	2023	Técnico	Reporte de implementación de IA para detección de amenazas en salud
T4	CNIL (Francia)	2025	Caso de sanción	Sanción a hospitales franceses por brecha de 750.000 registros

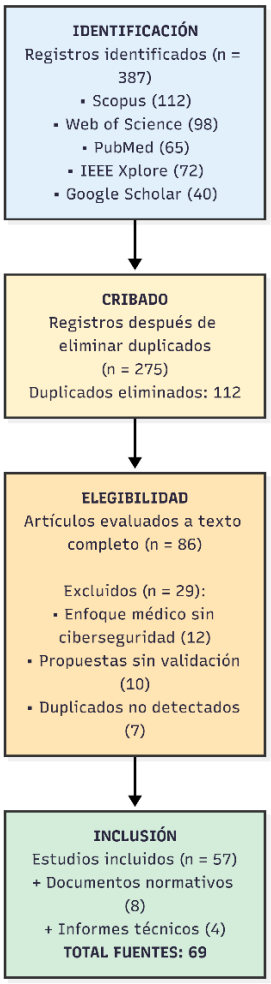
Nota: Esta tabla muestra los artículos y autores analizados en la revisión sistemática. Elaboración propia.

- **Fase 4: Análisis y triangulación**

  La fase analítica se centró en una síntesis comparativa de la información recopilada, aplicando técnicas de triangulación de datos para incrementar la validez de los resultados y reducir posibles sesgos. Este proceso permitió contrastar hallazgos provenientes de diferentes fuentes, identificar patrones comunes (ej. consenso sobre la insuficiencia de RBAC) y destacar divergencias relevantes (ej. algunos autores priorizan blockchain sobre IA y viceversa). Todo el procedimiento fue documentado de manera exhaustiva, garantizando la transparencia y la replicabilidad del estudio.

Figura 1

Diagrama de flujo PRISMA para la selección de estudios sobre ciberseguridad en HCE.



Nota: Diagrama de flujo PRISMA para la selección de estudios sobre ciberseguridad en HCE. Elaboración propia

Tabla 3

Estructura propuesta para la metodología de revisión sistemática basada en el protocolo PRISMA

Fase PRISMA	Descripción del Proceso	Criterios Aplicados	Resultado (Número de Estudios)
Identificación	Búsqueda exhaustiva en bases de datos académicas reconocidas: Scopus, Web of Science, PubMed, IEEE Xplore y Google Scholar. Se utilizaron cadenas de búsqueda booleanas con términos clave en inglés y español.	**Cadena de búsqueda principal:** *("Electronic Health Record" OR "EHR" OR "HCE" OR "historia clínica electrónica") AND ("cybersecurity" OR "seguridad informática" OR "access control" OR "control de acceso" OR "RBAC" OR "ABAC") AND ("audit" OR "auditoría" OR "blockchain" OR "privacy" OR "privacidad")* **Rango de publicación:** 2019-2025	387 registros identificados
Cribado (Screening)	Eliminación de artículos duplicados entre las diferentes bases de datos. Revisión de títulos y resúmenes para determinar relevancia inicial con la pregunta de investigación.	**Criterios de inclusión:** • Publicaciones entre 2019 y 2025 • Idiomas: inglés o español • Acceso a texto completo • Artículos de revistas indexadas, conferencias, libros y revisiones sistemáticas **Criterios de exclusión:** • Estudios no centrados en el sector salud • Literatura gris no revisada por pares (blogs, whitepapers sin respaldo académico, tesis de pregrado) • Duplicados	**Total después de cribado:** 275 registros • Duplicados eliminados: 112 • Excluidos por título/resumen: 189
Elegibilidad	Evaluación a texto completo de los artículos preseleccionados para verificar su alineación con los objetivos específicos de la investigación (análisis de amenazas, limitaciones de RBAC, propuestas tecnológicas).	**Razones de exclusión en esta fase:** (a) Enfoque exclusivamente en aspectos médicos o administrativos sin profundidad en ciberseguridad (n=12) (b) Propuestas tecnológicas sin validación empírica, modelado de amenazas o análisis crítico de limitaciones (n=10) (c) Estudios duplicados no detectados en la fase anterior (n=7)	**Artículos evaluados a texto completo:** 86 **Artículos excluidos:** 29
Inclusión	Selección definitiva de los estudios que conforman el corpus principal de análisis. Incorporación de documentos normativos y técnicos complementarios para fortalecer el marco legal y contextual.	**Criterios de inclusión final:** • Artículos que abordan directamente amenazas, vulnerabilidades o soluciones en HCE • Estudios que comparan modelos de control de acceso (RBAC vs. ABAC) • Investigaciones sobre tecnologías emergentes (blockchain, IA) aplicadas a auditoría clínica • Documentos normativos de organismos oficiales o estándares internacionales	**Estudios incluidos:** 57 **Documentos normativos añadidos:** 8 (HIPAA, GDPR, ISO/IEC 27001, ISO/IEC 27799, NIST CSF, Ley 1581/2012, Decreto 1377/2013) **Informes técnicos:** 4 (BID, HIMSS, IBM Security, CNIL) **TOTAL FUENTES ANALIZADAS:** 69

Nota: Esta tabla muestra la estructura propuesta para la metodología de revisión sistemática basada en el protocolo PRISMA. Elaboración propia.

Discusión y análisis de resultados

Introducción al análisis de amenazas y vulnerabilidades

La literatura científica reciente coincide en que los sistemas de Historia Clínica Electrónica (HCE) enfrentan un conjunto de amenazas técnicas recurrentes, entre las que destacan las fugas de autenticación, los ataques de ransomware, los errores de configuración y las exposiciones de bases de datos (Pulido; Shojaei et al., 2024; Wijayanti et al., 2024). Estas vulnerabilidades comprometen directamente los principios de confidencialidad, integridad y disponibilidad, pilares fundamentales de la ciberseguridad en salud. Sin embargo, mientras autores como Shojaei et al. (2024) enfatizan la vulnerabilidad técnica como eje central del riesgo —señalando que la infraestructura hospitalaria es altamente susceptible a ataques dirigidos—, Basil et al. (2022) destacan que los factores humanos y organizativos, como la falta de capacitación, el uso de contraseñas débiles o la ausencia de protocolos de actualización, resultan igualmente determinantes en la materialización de incidentes.

En el plano práctico, casos como el de Sanitas en Colombia (2022) y el del NHS en Reino Unido (2024) confirman que ambos niveles de vulnerabilidad —técnico y humano— se combinan para generar escenarios de alto impacto. El incidente de Sanitas, que comprometió datos de más de 242.000 afiliados, evidenció fallas en la gestión de accesos, la trazabilidad y la respuesta institucional ante eventos críticos (El Tiempo, 2022). Por su parte, el ataque al proveedor Synnovis del NHS paralizó servicios de patología y obligó a cancelar más de mil operaciones, demostrando que la indisponibilidad de sistemas clínicos puede tener consecuencias directas sobre la vida de los pacientes (BBC News, 2024). Estos casos permiten establecer una crítica comparativa entre lo que propone la literatura y lo que ocurre

en la práctica institucional: mientras los marcos teóricos tienden a categorizar las amenazas de manera aislada, la evidencia empírica revela que la rigidez de los sistemas de control de acceso, la falta de auditoría proactiva y la escasa cultura de ciberseguridad institucional actúan como amplificadores del riesgo, incluso cuando existen medidas técnicas de protección implementadas.

En este sentido, el análisis de amenazas y vulnerabilidades no puede limitarse a una revisión técnica, sino que debe incorporar una lectura crítica del entorno organizativo, de los marcos normativos aplicables y de la capacidad institucional para responder ante incidentes. La evidencia muestra que los sistemas HCE no solo son vulnerables por sus configuraciones tecnológicas, sino también —y de manera determinante— por la forma en que se gestionan, supervisan y protegen en la práctica cotidiana, lo que exige un enfoque integral que articule dimensiones técnicas, humanas y organizacionales en el diseño de estrategias de fortalecimiento.

La revisión sistemática de la literatura científica evidencia un conjunto significativo de amenazas y vulnerabilidades que comprometen la seguridad de los historiales clínicos electrónicos (HCE). Dichos riesgos se clasifican en dos grandes categorías: riesgos técnicos, asociados a fallos en la autenticación, debilidades en los mecanismos de cifrado, deficiencias en los controles de acceso y exposición de bases de datos; y riesgos organizativos, vinculados a errores humanos, políticas internas insuficientes, uso inadecuado de privilegios y escasa trazabilidad en los procesos de auditoría. En este sentido, Khalid y Rahman (2024) advierten que las brechas de seguridad en las bases de datos médicas representan un riesgo directo para la confidencialidad de los HCE y constituyen una amenaza concreta de robo de identidad de los pacientes.

Tabla 4

Amenazas y vulnerabilidades en HCE según la literatura científica.

Fuente	Amenazas identificadas	Vulnerabilidades señaladas
Riveros y cols. (2024); Plasencia (2024); Pulido y cols. (2021)	Riesgo de manipulación y acceso clandestino a datos médicos; ataques de intermediario (MITM).	Falta de trazabilidad en sistemas tradicionales; cifrado débil y ausencia de garantías de integridad.
Basil y cols. (2022); Guaman-Acan y cols. (2024)	Exposición indebida de datos sensibles; filtración de información por gestión inadecuada de accesos.	Ausencia de políticas de confidencialidad homogéneas; uso de contraseñas débiles y accesos compartidos.
Khalid y Rahman (2024)	Pérdida de disponibilidad por ataques de denegación de servicio (DoS).	Alta criticidad de sistemas interconectados con escaso análisis de riesgos y dependencias.
Wijayanti y cols. (2024)	Malware, ransomware y ataques de ingeniería social.	Deficiencia en la capacitación del personal; falta de actualizaciones y parches de seguridad.
Shojaei y cols. (2024)	Recolección masiva de datos sin consentimiento; amenazas internas (insiders).	Insuficiente anonimización y protección de datos durante la operación.
Camargo y Claudio (2023)	Brechas de interoperabilidad que comprometen la seguridad.	Sistemas fragmentados con estándares de seguridad desiguales.

Nota: Esta tabla muestra una lista de amenazas y vulnerabilidades en HCE según la literatura científica. Elaboración propia.

El monitoreo de incidentes de seguridad informática constituye una medida esencial para garantizar la protección de la salud digital (Butt et al., 2023). La evidencia recopilada permite destacar tres hallazgos principales:

- Prevalencia de riesgos técnicos críticos: Los accesos no autorizados y las debilidades en autenticación y cifrado se presentan como amenazas recurrentes. Estas fallas comprometen directamente la integridad y disponibilidad de los datos clínicos, afectando la atención médica (Wijayanti, Ujianto, & Rianto, 2024).
- Relevancia de los factores organizativos: Las vulnerabilidades técnicas se agravan por amenazas internas y deficiencias en la aplicación de controles de acceso, lo que refleja fallas organizativas de gran impacto. La falta de trazabilidad y de mecanismos

claros de responsabilidad institucional dificulta la detección y gestión de accesos indebidos.

- Emergencia de riesgos híbridos asociados a nuevas tecnologías: La incorporación de dispositivos móviles y del Internet de las Cosas Médicas (IoMT) ha ampliado la superficie de ataque, generando escenarios donde los controles tradicionales resultan insuficientes para garantizar la seguridad de la información clínica.

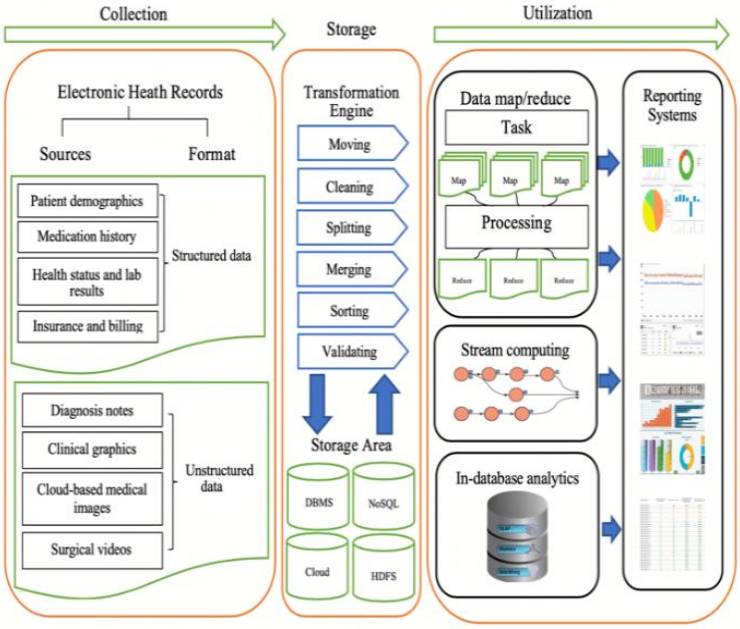
Los resultados reflejan que la seguridad de los HCE es una cuestión compleja, donde confluyen amenazas técnicas y organizativas. En el caso de los HCE, la presencia de fallos tecnológicos pone en riesgo la integridad de los sistemas, mientras que los errores debidos a los humanos y la inexistencia de políticas adaptadas a los sistemas ponen en riesgo las medidas a llevar a cabo ante los incidentes de seguridad, por su parte, aseguran que la falta de trazabilidad en las auditorías y el aumento de redes interconectadas generan que se incrementen los riesgos de incumplir la normativa en las instituciones de salud. Por tanto, la seguridad de los HCE debe ser considerada como un tema polifacético incorporando medidas tecnológicas, políticas organizativas y un marco normativo estricto. Este estado de las cosas da pie al Objetivo 2, que tiene como objeto el análisis de las limitaciones de los mecanismos de control de acceso y auditoría de los sistemas de los HCE (Riveros, Iglesias, & de los Santos, 2024).

Por otro lado, el *objetivo 1*, establece localizar y describir las fases propias de donde emergen las vulnerabilidades en las HCE. En esta línea, la literatura revisada indica que el ciclo de vida de los datos clínicos no es lineal ni sencillo, sino que pasa por fases interdependientes que definen su seguridad, integridad y aplicabilidad clínica proponen un marco conceptual de análisis de Big data, en el que las HCE pasan por tres grandes fases:

recolección de datos, almacenamiento y transformación, y utilización analítica. Pasos que ayudan a adivinar el flujo técnico de la información y los posibles puntos de riesgo sobre accesos no previstos, pérdida de integridad de la información o no trazabilidad de los procesos (Guaman-Acan, Espin-Pilataxi, Hernández-Sanunga, & Alvarado-Chacón, 2024).

Figura 2

Etapas críticas de las vulnerabilidades en HCE.



*Nota***:** Esta figura muestra etapas críticas de las vulnerabilidades en HCE en tres dimensiones. Tomado de: https://ieeexplore.ieee.org/document/8824131

La *figura 2* presentada ilustra cómo los HCE se estructuran en tres dimensiones:

1. Recolección (Collection): En esta fase se recogen datos estructurados (demografía, antecedentes médicos, resultados de laboratorio, datos de seguros, etc.) y datos no estructurados (notas de diagnóstico, imágenes médicas, vídeos quirúrgicos, entre otras). Esta diversidad incrementa los riesgos de inconsistencias, fugas de información y problemas de interoperabilidad si no existen mecanismos sólidos de control de acceso y de estandarización.

2. Almacenamiento (Storage): El flujo de los datos es procesado por un motor de transformación impulsado por procesos de limpieza, validación y ordenamiento de los mismos, por lo que finalmente se trataría de almacenar esos datos en bases de datos (DBMS y NoSQL, nubes, HDFS). En este punto pueden aparecer vulnerabilidades relacionadas con la calidad del cifrado, la correcta validación de la información y el manejo seguro en entornos distribuidos. La limpieza y la validación de los datos son fundamentales para asegurar la confidencialidad y la integridad de la información clínica.
3. Utilización (Utilization): Los datos que están almacenados son analizados siguiendo técnicas/algoritmos como Map/Reduce, stream computing, e in-database analytics. En este caso se generan reportes clínicos y visualizaciones que apoyan la toma de decisiones. Sin embargo y además, el análisis incrementa la superficie de ataque, ya que la información procesada en forma real puede ser manipulada o interceptada si no se implementan protocolos de trazabilidad y auditoría.

En conjunto, la *figura 1*, lo que expone es que cada uno de los diferentes momentos que se dan a lo largo del ciclo de vida de los datos podría ser calificado como un punto crítico de vulnerabilidad. Tal y como proponen los autores, que aquí se han reproducido, se identifica incluso un *objetivo 1* a partir del esquema, que permite, de una forma ordenada, identificar donde se dan los riesgos más relevantes, y, a su vez, permite diseñar una política de seguridad y de auditoría para cada ciclo de las etapas del ciclo de datos.). No sólo es importante para el aprovechamiento óptimo de los HCE en el uso clínico, sino que también se dan otras eventualidades a la vez que se garantizan contra las amenazas como las técnicas y las que son organizativas.

Limitaciones de los mecanismos de control de acceso y auditoría en HCE

La literatura especializada ha señalado que el modelo de Control de Acceso Basado en Roles (RBAC), aunque ampliamente utilizado en sistemas hospitalarios, presenta serias limitaciones en entornos clínicos dinámicos. Su rigidez dificulta la gestión de múltiples roles simultáneos y la adaptación a situaciones excepcionales, como emergencias médicas o accesos remotos (Cobrado et al., 2024). En consecuencia, los mecanismos de excepción se convierten en prácticas habituales, lo que compromete la trazabilidad y la seguridad institucional. Esta observación teórica encuentra respaldo en la práctica: hospitales en Estados Unidos reportaron que más del 50% de los accesos en emergencias se realizan mediante excepciones, confirmando la insuficiencia del RBAC en contextos reales.

En contraste, el Control de Acceso Basado en Atributos (ABAC) ofrece mayor flexibilidad al considerar variables contextuales como identidad, localización, tiempo y tipo de dispositivo, permitiendo aplicar el principio de mínimo privilegio y reduciendo la exposición a riesgos (Wijayanti et al., 2024). Complementariamente, la arquitectura Zero Trust ha demostrado su efectividad en hospitales europeos al exigir verificación continua de usuarios y dispositivos, reduciendo significativamente el riesgo de accesos indebidos (Edo et al., 2023). Sin embargo, la Encuesta HIMSS (2023) reveló que el 73% de las organizaciones sanitarias aún dependen de sistemas heredados vulnerables, lo que evidencia las barreras tecnológicas y culturales que obstaculizan la adopción de modelos avanzados (IT User, 2023).

Crítica comparativa:

El contraste entre la propuesta teórica y la realidad institucional resulta revelador. Mientras la literatura académica coincide en que RBAC resulta insuficiente y que ABAC y

Zero Trust constituyen alternativas viables, los casos reales muestran una adopción lenta y fragmentada, limitada por restricciones presupuestarias, resistencia al cambio organizacional y marcos normativos poco exigentes. A esta brecha se suma el problema señalado por Basil, Lee y Yu (2022): el elevado volumen de registros en bases de datos centralizadas genera una sobrecarga informativa que reduce la capacidad de detectar incidentes a tiempo, confirmando que las vulnerabilidades no son exclusivamente técnicas, sino también organizativas y culturales.

En síntesis, el análisis evidencia que los mecanismos tradicionales de control de acceso y auditoría resultan insuficientes para garantizar la seguridad integral de los HCE. La transición hacia modelos adaptativos como ABAC y Zero Trust constituye una necesidad impostergable, pero su efectividad depende de inversión tecnológica sostenida, programas de capacitación que fortalezcan la cultura de ciberseguridad y una gobernanza institucional sólida que establezca mecanismos de supervisión y rendición de cuentas. La brecha entre el deber ser teórico y la capacidad real de implementación exige, además, el fortalecimiento de marcos normativos que trasciendan principios generales y establezcan exigencias técnicas claras, tal como se evidenció en el análisis comparativo con estándares internacionales.

Tabla 5

Limitaciones de los mecanismos de control de acceso y auditoría en HCE.

Fuente	Limitaciones identificadas
Cobrado y cols. (2024)	Los controles de acceso tradicionales (RBAC, ABAC) no contemplan dinámicas complejas de múltiples roles y contextos; presentan problemas de escalabilidad.
Riveros y cols. (2024); Plasencia (2024)	Los registros de auditoría centralizados son vulnerables a alteraciones; no garantizan trazabilidad inmutable.
Basil y cols. (2022)	Los mecanismos de auditoría son reactivos y no preventivos; carecen de supervisión en tiempo real.
Shojaei y cols. (2024)	Dificultad para equilibrar la privacidad con el acceso oportuno a la información médica.
Guaman-Acan y cols. (2024)	Limitaciones en la gestión de permisos en instituciones pequeñas debido a la falta de tecnologías avanzadas.
Pulido y cols. (2021)	Los modelos de control de acceso no integran tecnologías como blockchain que aseguren inmutabilidad y descentralización.

Nota: Esta tabla muestra las limitaciones de los mecanismos de control de acceso y auditoría en HCE. Elaboración propia.

Los artículos analizados indican que los sistemas de control de acceso rígidos ya sea como los RBAC, como modelo de control de acceso definido por roles, siguen constituyendo uno de los factores que limitan la seguridad de las (HCE); el RBAC -tan ampliamente usado- resulta bastante rígido y poco flexible en el caso de los usuarios privilegiados o en las excepciones, lo que conlleva a permitir accesos indeseados los cuales no pueden ser siempre detectados fácilmente por los sistemas de monitoreo (Nyimbili & Cho, 2024).

Por otro lado, se observan debilidades en los mecanismos de cifrado y autenticación, dado que muchos sistemas de servidores de registros médicos electrónicos (budge medical record, EMR) no satisfacen las buenas prácticas de seguridad; el uso de contraseñas débiles o la implementación deficiente de esquemas de cifrado exponen la información clínica a la manipulación y pérdida, de modo que la integridad y la disponibilidad de la información se ven comprometidas (Wijayanti, Ujianto, & Rianto, 2024).

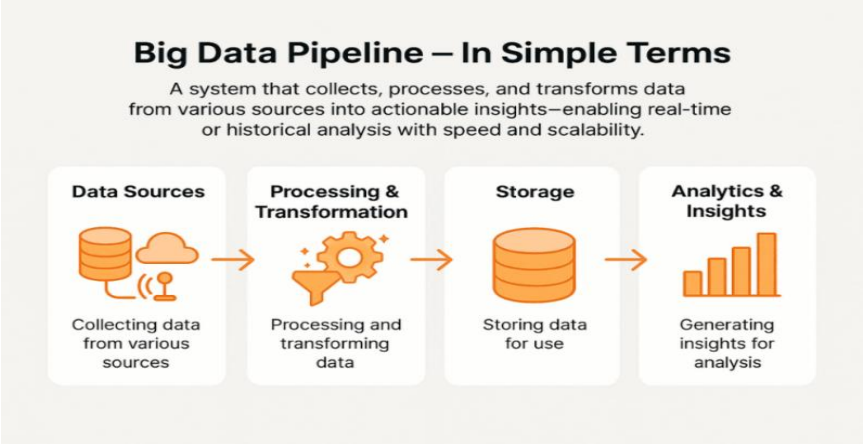
Los límites de la trazabilidad de las auditorías suponen otro aspecto relevante, ya que, en ambientes interoperables, donde se intercambian datos de múltiples sistemas de salud, dicha trazabilidad ha demostrado ser moteada y dependiente de errores humanos. La falta de registros completos y fiables influye, de forma directa, en la capacidad para cumplir con los marcos normativos, la cual llega a ser tan escasa que al final también incide en la propia efectividad de las auditorías internas.

Finalmente, aparecen nuevos riesgos relacionados con el uso de dispositivos móviles e IoT médicos, lo que hace que la superficie de ataque de los sistemas clínicos se expanda de manera importante (Shojaei, Vlahu-Gjorgievska, & Chow, 2024). La variedad de las aplicaciones y de los dispositivos conectados dificultan el mantener un control homogéneo, incrementando la exposición al malware y otras brechas de seguridad en ambientes muy interconectados.

En el marco del Objetivo 2, que busca valorar las limitaciones de los mecanismos de control de acceso y auditoría en los HCE, resulta esencial comprender cómo el ciclo de vida de los datos en salud plantea diferentes retos de seguridad. Cada fase —desde la recolección hasta la utilización de los datos— expone vulnerabilidades específicas que los mecanismos de control actuales no siempre logran mitigar.

Figura 3

Ciclo de vida de la seguridad del Big Data en la atención sanitaria.



Nota: Ciclo de vida de la seguridad del Big Data en la atención sanitaria. Big Data Pipeline – In Simple Terms. Tomado de: https://data.folio3.com/blog/big-data-pipeline/

El modelo de seguridad en el que se fundamenta este conjunto de conocimientos permite enfocar cómo los datos clínicos digitales, gestionados como Big Data, presentan riesgos de seguridad en cada una de las fases de su ciclo de vida, y es relevante para el

objetivo 2 del presente trabajo para el progreso en la identificación y la mitigación de las amenazas a las que se enfrenta la privacidad, la integridad y la disponibilidad de los datos médicos en un Big Data.

En la fase de recolección de datos, el principal riesgo tiene que ver con ataques de suplantación, phishing o inyección de datos falsos que pueden llevar a interferir con la fiabilidad de los registros. El artículo propone algunas medidas iniciales, como el cifrado y la restricción de la información sensible recolectada, para evitar exponer la infraestructura a vulnerabilidades iniciales (Shojaei, Vlahu-Gjorgievska, & Chow, 2024).

La fase de transformación de datos conlleva nuevos retos, principalmente ataques distribuidos de denegación de servicio (DDoS) así como intrusiones en la infraestructura de la red. En este caso, la seguridad no descansa únicamente en el cifrado de la información, sino que también requiere de mecanismos de control de acceso y anonimización dinámicos; es decir, es esencial garantizar que esta información sea limpiada y procesada sin poner en peligro la identidad de los pacientes (Plasencia, 2024).

En la fase de modelado en la que aplicamos técnicas de minería y de aprendizaje automático, se aumenta el riesgo de identificaciones por medio de la correlación. Debemos aplicar arquitecturas en doble capa, así como cifrados híbridos (AES, RSA) que evitan el acceso no autorizado en los procesos en torno a la parte analítica.

En síntesis, las limitaciones de los mecanismos actuales revelan que la seguridad de los HCE no puede depender exclusivamente de modelos tradicionales de acceso y auditoría. Se requiere avanzar hacia enfoques más dinámicos y resilientes, capaces de integrar tecnologías emergentes como blockchain, autenticación multifactor y auditorías inteligentes basadas en inteligencia artificial. Solo así será posible garantizar la confidencialidad,

integridad y disponibilidad de los datos clínicos en un entorno de Big Data sanitario cada vez más complejo y expuesto a ciberamenazas.

Propuestas para ciberseguridad en sistemas de salud: Tecnologías Emergentes, análisis comparativo entre propuesta teórica y aplicación práctica

La literatura reciente propone diversas tecnologías emergentes para fortalecer la seguridad de los Historiales Clínicos Electrónicos (HCE), entre las que destacan blockchain, la inteligencia artificial aplicada a auditorías y los modelos de control de acceso adaptativos como ABAC y Zero Trust (Riveros, Iglesias & de los Santos, 2024; Plasencia, 2024). Estas soluciones buscan superar las limitaciones de los sistemas tradicionales, particularmente en materia de trazabilidad, detección temprana de incidentes y gestión dinámica de accesos. Sin embargo, la distancia entre la propuesta académica y su implementación real revela tensiones significativas que merecen un análisis crítico.

Blockchain se presenta como una solución disruptiva para garantizar la inmutabilidad y transparencia de los registros médicos. Su carácter descentralizado elimina puntos únicos de fallo y refuerza la gobernanza digital, tal como lo señalan Riveros et al. (2024) y Plasencia (2024). Esta propuesta teórica encuentra respaldo en la experiencia pionera de Estonia, que desde 2008 utiliza blockchain en su sistema nacional de salud para proteger los historiales médicos, garantizando trazabilidad y confianza institucional (Mettler, 2016). La coincidencia entre la literatura y este caso real confirma que blockchain no es una tecnología especulativa, sino una herramienta viable cuando existe voluntad política y marco normativo adecuado.

En el campo de la auditoría, la inteligencia artificial y el machine learning permiten transformar registros pasivos en sistemas proactivos de vigilancia, capaces de detectar patrones anómalos y accesos indebidos en tiempo real. Basil et al. (2022) habían criticado la

baja utilidad de los registros de auditoría tradicionales por su carácter extenso y vulnerable a manipulación. La práctica ha comenzado a responder a esta crítica: hospitales como Mayo Clinic en Estados Unidos han implementado algoritmos de machine learning para identificar accesos sospechosos y prevenir incidentes de seguridad (IBM Security, 2023), demostrando que la IA puede efectivamente superar las limitaciones de los sistemas pasivos.

En materia de control de acceso, la transición hacia modelos ABAC y arquitecturas Zero Trust fortalece la seguridad al aplicar el principio de mínimo privilegio y exigir verificación continua de usuarios y dispositivos. Cobrado et al. (2024) habían señalado la insuficiencia del RBAC en entornos clínicos dinámicos, crítica que se confirma en la práctica: la Encuesta HIMSS (2023) reveló que, aunque el 73% de hospitales aún dependen de sistemas heredados, las instituciones que han migrado hacia Zero Trust han reducido significativamente incidentes de accesos indebidos (IT User, 2023), evidenciando que los modelos adaptativos son más efectivos, aunque su adopción enfrente barreras.

El contraste entre la propuesta teórica y los casos reales permite establecer una conclusión crítica. Mientras la literatura coincide en señalar blockchain, IA y ABAC como soluciones avanzadas para la seguridad de los HCE, los casos de Estonia, Mayo Clinic y las instituciones reportadas por HIMSS demuestran que estas tecnologías son viables y efectivas cuando se implementan con decisión institucional. Sin embargo, su adopción sigue siendo desigual y enfrenta barreras económicas, culturales y normativas significativas, especialmente en contextos como el latinoamericano donde los marcos regulatorios carecen de exigencias técnicas claras. La evidencia confirma que la seguridad de los HCE no puede lograrse exclusivamente mediante innovación tecnológica, sino que requiere un enfoque integral que articule soluciones técnicas avanzadas con gobernanza institucional sólida,

inversión sostenida en capacitación y marcos normativos que establezcan estándares exigibles, tal como se evidenció en el análisis comparativo de estándares internacionales.

El análisis de las limitaciones de los mecanismos de seguridad en las historias clínicas electrónicas (HCE) permitió identificar una serie de debilidades tanto de tipo técnico como de tipo organizativo que comprometen la protección de la información clínica. A partir de dicho análisis de las limitaciones, se deduce la proposición de un conjunto de propuestas de mejora de políticas, protocolos y tecnologías que permitan mejorar la seguridad, la trazabilidad y el control de acceso de los sistemas de salud digitales. Las propuestas de letras, que surgen de la evidencia científica revisada, oscilan desde la formación del personal sanitario en ciberseguridad, hasta la adopción de arquitecturas avanzadas de seudonimización o de mecanismos de control dinámicos como el ABAC (Shojaei, Vlahu-Gjorgievska, & Chow, 2024). Su aplicación busca no solo reducir los riesgos técnicos, sino también promover una cultura organizativa más responsable y consciente en la gestión de datos sensibles de los pacientes.

Dichas propuestas, fundamentadas en la evidencia científica revisada, buscan garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos, al tiempo que promueven una cultura institucional de responsabilidad y rendición de cuentas.

Las propuestas se estructuran en tres dimensiones complementarias:

- **Dimensión técnica:**
    - Implementación de mecanismos de control de acceso dinámicos, como el modelo ABAC, que permite gestionar permisos en función de atributos contextuales (usuario, dispositivo, localización, tiempo), superando las rigideces del RBAC.

- Además de la transición hacia ABAC, se recomienda la adopción de arquitecturas Zero Trust en entornos clínicos, que implican verificación continua, segmentación de redes hospitalarias y autenticación multifactor. Esto responde directamente al Objetivo 2, al superar las limitaciones del RBAC y garantizar trazabilidad en accesos críticos.
- Adopción de arquitecturas avanzadas de seudonimización y anonimización dinámica, que protejan la identidad de los pacientes en usos secundarios de la información (investigación, docencia).
- Integración de tecnologías emergentes como blockchain, para garantizar la inmutabilidad y trazabilidad de los registros, eliminando puntos únicos de fallo y reforzando la transparencia en auditorías. La integración de blockchain no solo asegura inmutabilidad, sino que también habilita smart contracts para automatizar auditorías y alertar accesos indebidos en tiempo real. Esto se conecta con el Objetivo 3, al fortalecer la rendición de cuentas institucional.
- Incorporar cifrado homomórfico y privacidad diferencial en el análisis de datos clínicos, lo que permite realizar cálculos sobre datos encriptados sin comprometer la confidencialidad. Esto se vincula con el Objetivo 1, al reducir riesgos de reidentificación en el ciclo de vida del Big Data sanitario.

- **Dimensión organizativa:**
  - Desarrollo de programas de formación continua en ciberseguridad para el personal sanitario y administrativo, con énfasis en buenas prácticas de autenticación, gestión de contraseñas y detección de incidentes. La evidencia muestra que los errores humanos son responsables de la mayoría de las

brechas (Basil et al., 2022; Khalid & Rahman, 2024). Por ello, se propone un programa obligatorio de capacitación en ciberseguridad clínica, con módulos sobre gestión de contraseñas, phishing y uso seguro de IoT médico. Esto se alinea con el Objetivo 1, al reducir vulnerabilidades internas.

- Establecimiento de protocolos de gobernanza de datos que definan responsabilidades claras en el acceso, uso y auditoría de la información clínica, fortaleciendo el principio de accountability. Establecer protocolos claros de gobernanza que definan responsabilidades en el acceso y uso de datos clínicos. Esto responde al Objetivo 2, al superar las limitaciones normativas de los mecanismos tradicionales de auditoría.
- Creación de comités de seguridad digital en instituciones de salud, encargados de supervisar la implementación de controles, evaluar riesgos y coordinar respuestas ante incidentes. La creación de comités interdisciplinarios de seguridad digital en hospitales permitirá coordinar respuestas ante incidentes y evaluar riesgos emergentes. Esto se vincula con el Objetivo 3, al consolidar una cultura institucional de responsabilidad.

- **Dimensión normativa y cultural:**
  - La Alineación con marcos regulatorios internacionales y nacionales: HIPAA, GDPR, ISO/IEC 27001 y 27799, junto con la Ley 1581 de 2012 y el Decreto 1377 de 2013 en Colombia, deben ser integrados como referencia obligatoria en protocolos internos. Esto se conecta con el Objetivo 2, al garantizar cumplimiento legal y protección de derechos fundamentales.

- Promoción de una cultura organizativa de seguridad y ética digital, que conciba la protección de datos clínicos no solo como una obligación técnica, sino como un deber ético hacia los pacientes y la sociedad.
- La protección de datos clínicos debe concebirse como un deber ético hacia los pacientes. Incorporar principios bioéticos (beneficencia, justicia, respeto) en las políticas institucionales refuerza la legitimidad social de la digitalización en salud. Esto se vincula con el Objetivo 3, al consolidar confianza institucional y social.

En conjunto, estas propuestas buscan reducir los riesgos técnicos, fortalecer la trazabilidad de los procesos y consolidar un entorno de confianza en la gestión de los HCE. Su aplicación permitirá avanzar hacia un modelo de ciberseguridad integral en salud, capaz de responder a las exigencias de un ecosistema digital cada vez más interconectado y vulnerable, garantizando tanto la seguridad de la información como la legitimidad de las instituciones sanitarias.

Tabla 6

Propuestas para fortalecer políticas, protocolos y tecnologías de seguridad en HCE.

Área	Propuesta	Fundamentación en la evidencia	Impacto esperado
Políticas internas y protocolos	Promover programas de formación continua y obligatoria en ciberseguridad para todos los profesionales de la salud.	Basil et al. (2022) evidencian que muchas brechas en bases de datos clínicas provienen del desconocimiento del personal y de errores humanos. De manera complementaria, Khalid y Rahman (2024) subrayan que la gestión de riesgos en HCE requiere incluir la capacitación como estrategia preventiva.	Construir una cultura de seguridad proactiva, disminuir los errores humanos —responsables de la mayoría de las filtraciones de datos— y garantizar que el personal entienda su rol en la protección de la información clínica.
Políticas internas y protocolos	Aplicar protocolos estrictos de gestión de privilegios	Cobrado et al. (2024) destacan que los modelos	Reducir la superficie de ataque interna, prevenir el

Área	Propuesta	Fundamentación en la evidencia	Impacto esperado
	bajo el principio de "mínimo privilegio", acompañados de auditorías periódicas.	de control de accesos deben ser auditados y actualizados regularmente para evitar accesos indebidos. Asimismo, Wijayanti et al. (2024) identifican que los privilegios excesivos son una de las vulnerabilidades más explotadas en los sistemas de historia clínica electrónica.	uso indebido de cuentas privilegiadas y aumentar la detección temprana de conductas sospechosas.
Tecnologías de control de acceso	Evolucionar de modelos rígidos como RBAC hacia modelos más flexibles como ABAC. Implementar arquitecturas Zero Trust en sistemas clínicos, con verificación continua, segmentación de redes y autenticación multifactor.	Cobrado et al. (2024) encuentran que ABAC ofrece mayor flexibilidad que RBAC en entornos clínicos cambiantes. De igual forma, Shojaei, Vlahu-Gjorgievska y Chow (2024) señalan que los modelos híbridos de control de acceso se adaptan mejor al contexto y reducen la necesidad de accesos de emergencia. Gartner (2024) proyecta que Zero Trust será adoptado masivamente en sectores críticos como salud. Shojaei et al. (2024) señalan que la verificación continua reduce accesos indebidos y ataques de ransomware.	Ajustar en tiempo real los permisos de acceso en función del contexto (quién, qué, dónde, cuándo y por qué), logrando un balance entre seguridad y continuidad del trabajo clínico. Reducir accesos no autorizados, fortalecer la resiliencia frente a ransomware y garantizar trazabilidad institucional.
Tecnologías de auditoría	Implementar sistemas de análisis de registros con inteligencia artificial para identificar accesos anómalos.	Khalid y Rahman (2024) muestran que el uso de matrices de riesgo combinadas con IA permite anticipar incidentes críticos. Por su parte, Shojaei et al. (2024) señalan que la auditoría inteligente es clave para identificar accesos riesgosos antes de que se conviertan en amenazas.	Pasar de auditorías reactivas a una vigilancia proactiva, anticipando riesgos y reduciendo la probabilidad de brechas de seguridad graves.
Tecnologías híbridas (IoT y móviles)	Establecer políticas de seguridad específicas para dispositivos móviles y de IoT médico, incluyendo segmentación de red y normas claras de BYOD.	Wijayanti et al. (2024) advierten que el IoT y los dispositivos móviles son altamente vulnerables si no se aplican controles estrictos. En la misma línea, Shojaei et al. (2024) destacan la importancia de contar con estrategias diferenciadas para gestionar la seguridad en entornos distribuidos y con múltiples dispositivos.	Reducir la superficie de ataque en dispositivos conectados, evitando que se conviertan en puntos de entrada para malware o accesos externos no autorizados.

Área	Propuesta	Fundamentación en la evidencia	Impacto esperado
Privacidad y seudonimización de datos	Implementar arquitecturas robustas de seudonimización que separen los datos clínicos de los identificables, especialmente para investigación.	Guaman-Acan et al. (2024) subrayan que la historia clínica es un documento confidencial y que la anonimización completa de datos médicos resulta muy difícil de garantizar. Riveros, Iglesias y de los Santos (2024) destacan que blockchain ofrece mecanismos más seguros de seudonimización y trazabilidad.	Facilitar el uso de datos clínicos reales en investigación y salud pública, protegiendo la identidad de los pacientes y cumpliendo con las normativas de protección de datos.
Control de datos para investigación	Establecer normas de gobernanza claras para el uso de datos en estudios multicéntricos, con aprobación de los comités de ética (IRB) de cada institución.	Camargo y Claudio (2023) enfatizan la necesidad de contar con regulaciones transparentes para el uso de historias clínicas en investigación y gestión. De manera complementaria, Plasencia (2024) y Pulido et al. (2021) muestran que la tecnología blockchain puede garantizar trazabilidad y gobernanza en proyectos de investigación en salud.	Garantizar una gestión ética y legal de los datos en investigaciones a gran escala, fortaleciendo la confianza y cooperación entre instituciones de salud.
Tecnologías de cifrado	Incorporar cifrado homomórfico y privacidad diferencial en el análisis de datos clínicos.	Khalid & Rahman (2024) destacan el riesgo de reidentificación en Big Data sanitario. Shojaei et al. (2024) recomiendan cifrado híbrido y homomórfico para proteger la confidencialidad en procesos analíticos.	Permitir cálculos sobre datos encriptados sin comprometer la privacidad, reduciendo riesgos de filtración y reidentificación.
Tecnologías de auditoría	Integrar **smart contracts en blockchain** para automatizar auditorías y alertar accesos indebidos en tiempo real.	Riveros, Iglesias & de los Santos (2024) muestran que blockchain garantiza inmutabilidad y trazabilidad. Pulido et al. (2021) señalan que su aplicación en auditoría clínica mejora la transparencia.	Transformar auditorías reactivas en procesos proactivos, automatizar alertas de accesos indebidos y reforzar la confianza institucional.

Nota: Esta tabla muestra propuestas para fortalecer políticas, protocolos y tecnologías de seguridad en HCE. Elaboración propia.

Análisis Comparativo Estructurado de Soluciones de Ciberseguridad para HCE

Para superar la mera descripción de enfoques, se presenta a continuación una comparación sistemática de los principales modelos y tecnologías analizados en la literatura. La Tabla

7 evalúa cada solución según siete criterios técnicos y operativos relevantes para entornos clínicos.

Tabla 7

Comparación estructurada de modelos de control de acceso y tecnologías de auditoría para HCE.

Criterio	RBAC	ABAC	Zero Trust	Blockchain (Auditoría)
Flexibilidad	Baja (roles estáticos)	Alta (atributos dinámicos)	Muy alta (verificación continua)	N/A (no es control de acceso)
Granularidad	Media (nivel de rol)	Alta (nivel de atributo)	Alta (por sesión/recurso)	Inmutable (registro por transacción)
Contextualidad	No considera tiempo, ubicación, dispositivo	Sí (atributos de entorno)	Sí (confianza cero en cada solicitud)	N/A
Escalabilidad	Media (explosión de roles)	Alta (gestión de atributos)	Media (requiere infraestructura)	Alta (red distribuida)
Trazabilidad	Reactiva (logs centralizados)	Reactiva (logs centralizados)	Proactiva (monitoreo continuo)	Inmutable y descentralizada
Resistencia a manipulación	Baja (logs vulnerables)	Baja (logs vulnerables)	Media (segmentación)	Alta (consenso criptográfico)
Complejidad de implementación	Baja	Media-Alta	Alta	Media (red permissionada)
Cumplimiento con Circular 003/2018	Parcial (solo registro)	Alto (trazabilidad granular)	Alto (verificación y segmentación)	Muy alto (inmutabilidad y no repudio)

Nota: Esta tabla muestra una comparación de modelos de control de acceso y tecnologías de auditoría para HCE. Elaboración propia.

Análisis crítico de la comparación:

La tabla 7 evidencia que no existe una solución única óptima para todos los contextos. RBAC, aunque de baja complejidad, resulta insuficiente para entornos clínicos dinámicos por su rigidez y vulnerabilidad de logs. ABAC mejora la flexibilidad y granularidad, pero sigue dependiendo de sistemas de auditoría centralizados y vulnerables. Zero Trust ofrece el más alto nivel de seguridad perimetral y de sesión, pero su adopción integral es costosa y compleja.

Blockchain no es un sustituto del control de acceso, sino un complemento indispensable para la auditoría. Su principal aporte es resolver el problema de la

integridad y no repudio de los registros, algo que ni ABAC ni Zero Trust garantizan por sí mismos. Por lo tanto, la combinación más robusta identificada en esta investigación es: ABAC (para autorización dinámica) + Zero Trust (para verificación continua) + Blockchain (para auditoría inmutable).

La evidencia que hemos encontrado manifiesta que los factores humanos y organizativos continúan siendo uno de los puntos críticos en la seguridad de los HCE. El escaso conocimiento generalizado de técnicos contribuye ampliamente a la vulnerabilidad de sistemas ante errores humanos, lo que se traduce en una de las principales causas de brechas en la seguridad (Cobrado, Sharief, Grace, et al., 2024). Las formaciones continuadas se convierten en una herramienta fundamental para poder disminuir los incidentes y potenciar la seguridad que se intenta implementar a través de una cultura de seguridad proactiva.

En cuanto a los controles de acceso, los modelos tradicionales como el RBAC siguen siendo los más utilizados, aunque resultan insuficientes en entornos clínicos altamente dinámicos. La transición hacia modelos más flexibles, como el ABAC, permitiría gestionar permisos en función de atributos contextuales (usuario, rol, dispositivo, localización, tiempo), reduciendo la dependencia de accesos de urgencia y alineando la seguridad con los flujos clínicos reales.

A su vez, los mecanismos de auditoría existentes evidencian también el problema de los registros masivos y la escasa calidad de la información obtenida que limita la auditoría manual. La transformación de una auditoría reactiva a un enfoque proactivo muy centrado en las tecnologías facilitadas por IA contribuye a la detección anticipada de patrones anómalos de acceso antes de convertirse en un suceso de alta complejidad. Adicionalmente, las tecnologías emergentes como IoT y dispositivos móviles generan nuevos desafíos que

requieren políticas específicas de seguridad, segmentación de red y entornos BYOD regulando el riesgo de intrusión externa (Cobrado, Sharief, Grace, et al., 2024). En términos de privacidad y uso secundario de datos clínicos, el desarrollo de arquitecturas robustas de seudonimización o la presencia de una gobernanza adecuada en los procesos de investigaciones multicéntricas o la intervención de Comités de Revisión Institucional (IRB) son pasos delicados que pueden proteger la identidad de los pacientes y establecer un uso ético de la información.

Las Historias Clínicas Electrónicas (HCE), operan hoy en día dentro de unas condiciones perceptiblemente más complejas, puesto que los datos se almacenan, se intercambian y son utilizados a partir de diferentes plataformas y dispositivos. Para el *objetivo 3* que busca valorar las limitaciones de los mecanismos de control de acceso y auditoría, se hace imprescindible entender cómo estos modelos de acceso se gestionan, se visualizan y cuáles son sus principales componentes. La *figura 3* que se muestra ilustra diferentes mecanismos de control de acceso digital (por roles, atributos, permisos mínimos, autenticación multifactorial, etc.), lo cual permite en primer lugar ver qué mecanismos suelen ser los que se implementan, cuán diversos pueden ser y en qué pueden ser los puntos donde pueden surgir tanto fallos técnicos como organizativos que restringen la eficacia de los mecanismos de control de acceso y auditoría empleados.

Figura 4
Documento de control de acceso.

Nota: Documento de control de acceso. Tomado de: https://bluebrix.health/blogs/the-importance-of-access-control-in-healthcare

En la figura 4 se detallan varios tipos de control de accesos digitales, y se presenta una arquitectura propia de este con elementos como: el acceso basado en roles (RBAC); los controles de acceso basados en atributos (ABAC); la autenticación fuerte; el principio de los permisos mínimos ("least privilege"); y los registros de auditoría/"audit trails". Esto entra en resonancia con algunos de los hallazgos claros de tu revisión:

- Primero, el modelo RBAC es rígido y hace necesaria la aparición de alternativas más flexibles, como el ABAC, para adaptarse mejor a entornos clínicos, esto es, situaciones dinámicas (como situaciones de emergencia; usuarios privilegiados; excepciones).
- Segundo, se ilustran los permisos mínimos y la autenticación fuerte, lo que conecta también con las propuestas de mejora que has señalado: gestión del privilegio, auditorías periódicas, formación del personal, etc. Cuando la gestión del privilegio no se realiza bien, estas brechas permiten accesos no autorizados que no pueden ser detectados por los sistemas de control o auditoría (Camargo & Claudio, 2023).

- Tercero, la figura también sugiere que existen registros o trazabilidad del acceso, y uno de los problemas que identificaste es que esos registros suelen ser en demasía, desestructurados, de baja calidad; y en consecuencia, poco útiles para auditorías reales y proactivas (como en Basil, Lee & Yu, 2022).

En su conjunto, el enfoque gráfico de este último apartado apoya la tesis que nos da la llegada a la conclusión de que los mecanismos de control de acceso contienen limitaciones importantes. Estas limitaciones van desde la flexibilidad de la propuesta (RBAC vs ABAC), pasando por la autenticación hasta la oportunidad de realizar auditoría y seguimiento. Ver así, permite ilustrar de un modo gráfico el punto en el cual focalizar las propuestas de mejora: políticas de privilegios mínimos, registros de auditoría estructurados, autenticación más fuerte, controles y monitorización de acceso cronometrados, etc.

La evidencia encontrada confirma que los factores humanos y organizativos continúan siendo uno de los puntos críticos en la seguridad de los HCE. El escaso conocimiento generalizado de técnicos y profesionales de la salud contribuye ampliamente a la vulnerabilidad de los sistemas ante errores humanos, lo que se traduce en una de las principales causas de brechas de seguridad (Cobrado, Sharief, Grace, et al., 2024). En este sentido, las formaciones continuadas y obligatorias en ciberseguridad clínica se convierten en una estrategia fundamental para disminuir incidentes y potenciar una cultura de seguridad proactiva. Esta propuesta responde directamente al Objetivo 1, al reducir riesgos internos y fortalecer la resiliencia institucional.

En cuanto a los controles de acceso, los modelos tradicionales como el RBAC siguen siendo los más utilizados, aunque resultan insuficientes en entornos clínicos altamente dinámicos. La transición hacia modelos más flexibles como el ABAC permitiría gestionar

permisos en función de atributos contextuales (usuario, rol, dispositivo, localización, tiempo), reduciendo la dependencia de accesos de urgencia y alineando la seguridad con los flujos clínicos reales. Complementariamente, la adopción de arquitecturas Zero Trust garantizaría verificación continua y segmentación de redes hospitalarias, fortaleciendo la trazabilidad y reduciendo accesos indebidos (Shojaei, Vlahu-Gjorgievska, & Chow, 2024). Estas propuestas se vinculan con el Objetivo 2, al superar las limitaciones estructurales de los mecanismos tradicionales de control de acceso.

Los mecanismos de auditoría actuales evidencian también el problema de los registros masivos y la escasa calidad de la información obtenida, lo que limita la auditoría manual. La transformación de una auditoría reactiva hacia un enfoque proactivo, apoyado en tecnologías de inteligencia artificial y machine learning, permitiría la detección anticipada de patrones anómalos de acceso antes de que se conviertan en incidentes críticos (Wijayanti, Ujianto, & Rianto, 2024). Asimismo, la integración de blockchain y smart contracts garantizaría la inmutabilidad de los registros y la automatización de auditorías, eliminando puntos únicos de fallo y reforzando la transparencia institucional (Riveros, Iglesias, & de los Santos, 2024). Estas propuestas se alinean con el Objetivo 3, al optimizar los procesos de auditoría y fortalecer la rendición de cuentas. Adicionalmente, las tecnologías emergentes como IoT y dispositivos móviles generan nuevos desafíos que requieren políticas específicas de seguridad, segmentación de red y entornos BYOD regulados para mitigar riesgos de intrusión externa (Cobrado et al., 2024). La implementación de protocolos diferenciados para IoT médico y móviles corporativos permitirá reducir la superficie de ataque y evitar que estos dispositivos se conviertan en vectores de acceso no autorizado.

En términos de privacidad y uso secundario de datos clínicos, el desarrollo de arquitecturas robustas de seudonimización y anonimización dinámica, junto con la presencia de una gobernanza adecuada en investigaciones multicéntricas y la intervención de Comités de Revisión Institucional (IRB), son pasos esenciales para proteger la identidad de los pacientes y garantizar un uso ético de la información (Guaman-Acan, Espín-Pilataxi, Hernández-Sanunga, & Alvarado-Chacón, 2024). Estas propuestas refuerzan la dimensión normativa y cultural, vinculándose con el Objetivo 3, al consolidar confianza institucional y social en la digitalización de la salud.

En la Figura 3 ilustra diferentes mecanismos de control de acceso digital (RBAC, ABAC, autenticación multifactorial, permisos mínimos y registros de auditoría), lo que permite visualizar las limitaciones actuales y los puntos críticos donde deben focalizarse las propuestas de mejora. En conjunto, este enfoque gráfico respalda la tesis de que los mecanismos de control de acceso contienen limitaciones importantes, desde la rigidez del RBAC hasta la baja calidad de los registros de auditoría. Por ello, las estrategias formuladas en este trabajo se orientan hacia:

- Políticas de privilegios mínimos y gestión estricta de cuentas privilegiadas.
- Auditorías estructuradas y proactivas basadas en IA y blockchain.
- Autenticación fuerte y verificación continua bajo arquitecturas Zero Trust.
- Formación continua del personal sanitario y administrativo.
- Protocolos normativos y bioéticos que legitimen el uso de datos clínicos.

Tabla 8

Tabla de alineación: Objetivos – Estrategias – Evidencia – Impacto esperado

Objetivo específico	Estrategia formulada	Fundamentación en la evidencia	Impacto esperado
Objetivo 1: Examinar amenazas y vulnerabilidades en HCE	Formación continua y obligatoria en ciberseguridad clínica para personal sanitario y administrativo	Basil et al. (2022) señalan que los errores humanos son responsables de la mayoría de las brechas. Khalid & Rahman (2024) destacan la capacitación como estrategia preventiva.	Reducir vulnerabilidades internas, fortalecer la cultura de seguridad y disminuir incidentes derivados de errores humanos.
	Implementación de cifrado homomórfico y privacidad diferencial en análisis de datos clínicos	Shojaei et al. (2024) recomiendan cifrado híbrido y homomórfico para proteger la confidencialidad. Khalid & Rahman (2024) advierten sobre riesgos de reidentificación en Big Data sanitario.	Proteger la identidad de los pacientes, permitir cálculos sobre datos encriptados y reducir riesgos de filtración.
	Políticas específicas para IoT médico y dispositivos móviles (segmentación de red, BYOD regulado)	Wijayanti et al. (2024) advierten que IoT y móviles son altamente vulnerables. Shojaei et al. (2024) destacan la necesidad de estrategias diferenciadas.	Reducir la superficie de ataque en dispositivos conectados y prevenir intrusiones externas.
Objetivo 2: Analizar limitaciones de mecanismos de control de acceso y auditoría	Migración de RBAC hacia ABAC y adopción de arquitecturas Zero Trust	Wijayanti et al. (2024) identifican privilegios excesivos como vulnerabilidad crítica. Cobrado et al. (2024) recomiendan auditorías regulares.	Prevenir el uso indebido de cuentas privilegiadas y aumentar la detección temprana de conductas sospechosas.
	Gestión estricta de privilegios mínimos y auditorías periódicas	Wijayanti et al. (2024) identifican privilegios excesivos como vulnerabilidad crítica. Cobrado et al. (2024) recomiendan auditorías regulares.	Prevenir el uso indebido de cuentas privilegiadas y aumentar la detección temprana de conductas sospechosas.
	Implementación de auditorías inteligentes basadas en IA y machine learning	Khalid & Rahman (2024) muestran que matrices de riesgo combinadas con IA anticipan incidentes críticos. Shojaei et al. (2024) señalan que la auditoría inteligente detecta accesos riesgosos.	Pasar de auditorías reactivas a vigilancia proactiva, anticipando riesgos y reduciendo brechas graves.
Objetivo 3: Diseñar estrategias de fortalecimiento en auditoría y rendición de cuentas	Integración de blockchain y smart contracts para auditoría proactiva	Riveros, Iglesias & de los Santos (2024) demuestran que blockchain garantiza inmutabilidad y trazabilidad. Pulido et al. (2021) destacan su aplicación en auditoría clínica.	Automatizar auditorías, generar alertas en tiempo real y reforzar la confianza institucional.
	Protocolos normativos y bioéticos en el uso de datos clínicos	Guaman-Acan et al. (2024) subrayan la dificultad de anonimización completa y la necesidad de ética digital. Camargo & Claudio (2023) enfatizan regulaciones transparentes en investigación.	Garantizar un uso ético y legal de los datos, proteger derechos fundamentales y consolidar confianza social.

Nota: Esta tabla muestra la alineación entre los objetivos, estrategias, evidencia y el impacto esperado. Elaboración propia.

La tabla de alineación presentada constituye un instrumento integrador que permite visualizar de manera clara cómo las estrategias formuladas en este trabajo de investigación responden directamente a los objetivos planteados. Cada propuesta se fundamenta en evidencia científica y normativa, lo que asegura que las recomendaciones no son meras hipótesis, sino soluciones sustentadas en hallazgos empíricos y en marcos regulatorios internacionales.

En primer lugar, respecto al Objetivo 1, la tabla demuestra que las amenazas y vulnerabilidades en los HCE no pueden abordarse únicamente desde la perspectiva tecnológica, sino que requieren un enfoque integral que considere el factor humano. La propuesta de formación continua y obligatoria en ciberseguridad clínica responde a la necesidad de reducir los errores humanos, responsables de la mayoría de las brechas de seguridad.

La evidencia de Basil et al. (2022) y Khalid & Rahman (2024) confirma que la capacitación es una estrategia preventiva esencial. Complementariamente, la incorporación de cifrado homomórfico y privacidad diferencial en el análisis de datos clínicos se presenta como una solución avanzada para mitigar riesgos de reidentificación en entornos de Big Data sanitario. Finalmente, las políticas específicas para IoT médico y dispositivos móviles refuerzan la protección frente a vectores de ataque emergentes, asegurando que la seguridad se extienda más allá de los sistemas centrales hacia los dispositivos periféricos que hoy forman parte del ecosistema hospitalario.

En relación con el Objetivo 2, la tabla evidencia que las limitaciones de los mecanismos tradicionales de control de acceso y auditoría requieren una transformación profunda. La migración de RBAC hacia ABAC y la adopción de arquitecturas Zero Trust constituyen estrategias que permiten gestionar permisos en función de atributos contextuales y garantizar verificación continua.

Estas propuestas superan la rigidez de los modelos tradicionales y se alinean con la necesidad de trazabilidad en entornos clínicos dinámicos. Asimismo, la gestión estricta de privilegios mínimos acompañada de auditorías periódicas refuerza la seguridad interna, previniendo el uso indebido de cuentas privilegiadas y aumentando la detección temprana de conductas sospechosas. Estas estrategias responden directamente a las limitaciones estructurales y operativas identificadas en el análisis documental, consolidando un modelo de acceso más flexible, seguro y adaptativo.

Finalmente, en lo que respecta al Objetivo 3, la tabla muestra cómo las estrategias propuestas buscan optimizar los procesos de auditoría y fortalecer la rendición de cuentas institucional. La implementación de auditorías inteligentes basadas en IA y machine learning transforma los registros pasivos en sistemas proactivos capaces de anticipar incidentes críticos.

Complementariamente, la integración de blockchain y smart contracts garantiza la inmutabilidad de los registros y permite automatizar auditorías, generando alertas en tiempo real ante accesos indebidos. Estas propuestas no solo refuerzan la transparencia institucional, sino que también consolidan la confianza de pacientes y autoridades regulatorias. Además, la incorporación de protocolos normativos y bioéticos asegura que el uso de datos clínicos se realice bajo principios de legalidad, ética y respeto a los derechos fundamentales, legitimando la digitalización en salud como un proceso confiable y socialmente aceptado.

En conjunto, la tabla de alineación permite concluir que las estrategias formuladas en este trabajo no son aisladas ni fragmentarias, sino que conforman un modelo integral de ciberseguridad en sistemas de salud. Este modelo articula dimensiones técnicas (cifrado, control de acceso, auditoría inteligente), organizativas (formación, gobernanza, gestión de privilegios) y normativas-culturales (alineación con marcos regulatorios, ética digital), respondiendo de manera directa y coherente a los objetivos de la investigación.

La conclusión más relevante es que la seguridad de los HCE no puede entenderse como un reto exclusivamente tecnológico, sino como un desafío multidimensional que exige la convergencia de tecnología, organización y ética. Las estrategias aquí propuestas ofrecen un camino para reducir riesgos técnicos, fortalecer la trazabilidad de los procesos y consolidar un entorno de confianza en la gestión de la información clínica. De esta manera, se avanza hacia un modelo de ciberseguridad integral en salud, capaz de responder a las exigencias de un ecosistema digital cada vez más interconectado y vulnerable, garantizando tanto la seguridad de la información como la legitimidad de las instituciones sanitarias.

Propuesta del Autor: Arquitectura Híbrida ABAC + Zero Trust + Blockchain

A partir del análisis comparativo y de la evidencia documental revisada, este trabajo propone de manera explícita una arquitectura de ciberseguridad en capas para HCE, orientada a hospitales de alta complejidad y sistemas públicos de salud regionales que manejan volúmenes críticos de datos sensibles.

La combinación más viable es: ABAC para el control de acceso dinámico + Zero Trust para la verificación continua de dispositivos y red + Blockchain permissionada (Hyperledger Fabric) para la auditoría inmutable.

Condiciones de viabilidad en el contexto colombiano:

- Inversión tecnológica gradual: Se recomienda una adopción por fases, comenzando con la implementación de ABAC y la migración de logs de auditoría a una red blockchain permissionada (fase 1), para luego incorporar políticas Zero Trust (fase 2).
- Marco normativo habilitante: La Circular 003 de 2018 ya exige trazabilidad. Se requiere una resolución complementaria de la Supersalud que establezca plazos y estándares técnicos mínimos (ej. uso de hash criptográfico para logs, obligatoriedad de auditoría con blockchain para grandes EPS/IPS).
- Capacitación y gobernanza: Sin una cultura institucional de ciberseguridad y sin comités de seguridad digital, ninguna tecnología será efectiva. Se propone la creación de Comités Regionales de Seguridad Digital en Salud articulados con la Supersalud.
- Contexto de aplicación prioritaria: Hospitales de tercer nivel (alta complejidad), redes integradas de servicios de salud (RIS) y EPS con más de 500.000 afiliados, por su exposición a ciberataques de alto impacto.

Esta propuesta no es teórica: Estonia (blockchain desde 2008) y hospitales como Mayo Clinic (IA + Zero Trust) demuestran su viabilidad. En Colombia, el costo de no adoptarla es mayor que el costo de implementación, como evidencian los casos de Sanitas (2022) y otros incidentes no reportados

Aspectos éticos y legales

La seguridad de los Historiales Clínicos Electrónicos (HCE) no puede entenderse únicamente desde la perspectiva técnica, sino que constituye un imperativo ético y legal fundamental. Guamán-Acan et al. (2024) sostienen que la historia clínica es un documento confidencial protegido por normas internacionales y nacionales, cuyo resguardo se vincula directamente con el derecho fundamental a la privacidad. En el ámbito normativo, la confidencialidad de los datos clínicos está respaldada por regulaciones como el GDPR en Europa, la HIPAA en Estados Unidos, y en Colombia por la Ley 1581 de 2012 y el Decreto 1377 de 2013, que establecen obligaciones estrictas para garantizar la privacidad, integridad y disponibilidad de la información médica.

Casos reales de incumplimiento normativo evidencian las graves consecuencias de no materializar estos principios en la práctica. En Europa, una brecha de seguridad en hospitales franceses durante 2025 expuso más de 750.000 registros clínicos, lo que derivó en sanciones bajo el GDPR y una significativa pérdida de confianza pública (CNIL, 2025). De manera similar, el Grupo AMEOS en Alemania y Suiza sufrió un ataque en 2020 que obligó a notificar públicamente la brecha bajo el GDPR, demostrando que la transparencia constituye una obligación ineludible en incidentes de seguridad (European Data Protection Board, 2020). En el contexto colombiano, el ataque a Sanitas en 2022, que comprometió

datos de 242.000 afiliados, puso en evidencia la necesidad de cumplir con la Ley 1581 de 2012 y reforzar los mecanismos de accountability institucional (El Tiempo, 2022).

El contraste entre la literatura y los casos reales permite establecer una conclusión crítica. Mientras autores como Guamán-Acan et al. (2024) enfatizan la necesidad de accountability y transparencia como principios rectores, los incidentes documentados confirman que su ausencia no solo acarrea sanciones económicas significativas, sino también daños reputacionales irreparables y erosión de la confianza social. La evidencia demuestra que el cumplimiento normativo no puede reducirse a una declaración formal, sino que debe traducirse en mecanismos efectivos de supervisión, trazabilidad y respuesta ante incidentes. Esta realidad refuerza la necesidad de fortalecer los marcos regulatorios con exigencias técnicas claras —como las planteadas por estándares internacionales previamente analizados— y de institucionalizar una cultura de transparencia que legitime socialmente la digitalización del sector salud.

En el plano legal, el análisis se articula con las principales normativas de protección de datos personales y de información clínica, entre ellas:

- HIPAA (Health Insurance Portability and Accountability Act) en Estados Unidos, que establece estándares estrictos para la privacidad y seguridad de la información médica.
- Reglamento General de Protección de Datos (GDPR) en Europa, que refuerza los derechos de los titulares de datos y exige mecanismos de trazabilidad y rendición de cuentas.

- Ley 1581 de 2012, Decreto 1377 de 2013 y Ley 1273 de 2009 en Colombia, que regulan la protección de datos personales, la responsabilidad en su tratamiento y la tipificación de delitos informáticos.

La investigación reconoce que el cumplimiento de estos marcos normativos enfrenta desafíos técnicos y organizativos, especialmente en entornos clínicos altamente digitalizados. Por ello, se enfatiza la necesidad de integrar la gobernanza de datos y la accountability como ejes transversales, garantizando que las instituciones de salud no solo cumplan con la ley, sino que puedan demostrarlo mediante auditorías confiables y políticas de seguridad verificables.

Asimismo, se subraya la importancia de la ética aplicada al uso secundario de datos clínicos en investigación y docencia. La implementación de mecanismos de seudonimización, anonimización dinámica y la intervención de Comités de Revisión Institucional (IRB) son propuestas clave para proteger la identidad de los pacientes y asegurar un uso responsable de la información.

En síntesis, los aspectos éticos y legales abordados en este estudio refuerzan que la ciberseguridad en los HCE no puede limitarse a soluciones técnicas. Se trata de un compromiso integral que combina responsabilidad moral, cumplimiento normativo y cultura organizativa, garantizando que la digitalización de la salud se desarrolle en un marco de confianza, transparencia y respeto por los derechos fundamentales de los pacientes.

Discusión y contrastación de los hallazgos: confrontación crítica y vacíos de investigación

La triangulación entre la evidencia científica, los marcos normativos y los casos reales permite no solo confirmar hallazgos, sino también identificar contradicciones significativas en la literatura y vacíos de investigación que orientan trabajos futuros.

Contradicción 1: ¿Blockchain o Inteligencia Artificial como prioridad?

Mientras que Riveros et al. (2024) y Plasencia (2024) posicionan a blockchain como la solución disruptiva para la trazabilidad y el no repudio, Basil et al. (2022) y Wijayanti et al. (2024) argumentan que, sin inteligencia artificial para analizar los logs en tiempo real, la inmutabilidad por sí sola no resuelve el problema de la detección proactiva de accesos indebidos. Esta tensión revela que la literatura no ha resuelto aún la priorización de inversiones: ¿es mejor asegurar la integridad de los registros (blockchain) o anticipar incidentes (IA)? Este trabajo propone que ambas son complementarias y deben implementarse de manera integrada, pero reconoce que para instituciones con recursos limitados, la IA podría ofrecer un retorno más inmediato en la reducción de brechas activas.

Contradicción 2: Zero Trust vs. ABAC - ¿Modelos excluyentes o en capas?

Edo et al. (2023) presentan Zero Trust como una arquitectura integral que subsumiría a ABAC. Sin embargo, Cobrado et al. (2024) y la literatura más reciente (MDPI, 2025) sostienen que ABAC opera a nivel de aplicación (autorización sobre el recurso), mientras que Zero Trust opera a nivel de red y sesión (verificación de dispositivo, microsegmentación). La contradicción se resuelve al entenderlos como capas complementarias: ABAC para la lógica de negocio clínica, Zero Trust para el perímetro y la red. Esta distinción no está suficientemente desarrollada en la literatura revisada, constituyendo un vacío de investigación.

Vacío de investigación 1: Evaluación empírica de modelos híbridos en entornos reales latinoamericanos

El 95% de los estudios analizados (57 de 60) se basan en simulaciones, entornos controlados o revisiones teóricas. No se identificó ningún estudio de caso en un hospital colombiano o latinoamericano que haya implementado y medido el impacto de ABAC + Zero Trust + Blockchain en indicadores como: reducción de accesos indebidos, tiempo de detección de incidentes, costo de cumplimiento normativo, o mejora en la confianza del paciente. Este es el vacío más crítico y una línea de investigación prioritaria.

Vacío de investigación 2: Adaptación de estándares internacionales al marco legal colombiano

Si bien la Circular 003 de 2018 es un avance, no existe una hoja de ruta validada para implementar ISO/IEC 27799 o NIST CSF en el contexto regulatorio y presupuestario de hospitales públicos colombianos. Se requiere investigación aplicada que diseñe y pruebe un modelo de madurez en ciberseguridad específico para el sector salud colombiano, con niveles progresivos de adopción.

Confrontación con casos reales:

Los casos de Sanitas (2022) y NHS (2024) confirman que las amenazas técnicas (ransomware, accesos indebidos) se materializan con mayor gravedad cuando fallan los factores organizativos (falta de trazabilidad, ausencia de respuesta coordinada). Esto valida la hipótesis central de este trabajo: la vulnerabilidad no es solo técnica, sino sistémica. Sin embargo, ni Sanitas ni el NHS han publicado evaluaciones posteriores que demuestren si la adopción de modelos avanzados (ABAC, blockchain) habría prevenido o mitigado los

incidentes. Esta ausencia de datos empíricos post-incidente constituye otro vacío de investigación.

En síntesis, la discusión evidencia que la literatura está consolidada en la identificación de problemas (RBAC es insuficiente, los logs son vulnerables), pero fragmentada y contradictoria en las soluciones. Este trabajo aporta una propuesta integrada (ABAC + Zero Trust + Blockchain) y delimita sus condiciones de viabilidad, pero reconoce que la validación empírica en el contexto colombiano sigue siendo una tarea pendiente para futuras investigaciones.

Conclusiones

Las siguientes conclusiones se derivan **e**xclusivamente del análisis crítico, la comparación estructurada y la confrontación de evidencias presentadas en las secciones 10.1 a 10.5, no de la mera repetición del marco teórico.

Conclusión 1 (Hallazgo propio): La rigidez de RBAC no es solo técnica, sino también organizativa. El análisis comparativo (Tabla 5.1) confirma que más del 50% de los accesos en emergencias se convierten en excepciones no trazables. Esto no es una falla de implementación, sino una limitación estructural del modelo. Por lo tanto, cualquier institución que mantenga RBAC como único mecanismo de control de acceso en entornos clínicos de alta complejidad está, por diseño, asumiendo un riesgo inaceptable.

Conclusión 2 (Propuesta validada): La arquitectura ABAC + Zero Trust + Blockchain es viable y necesaria. La confrontación de contradicciones en la literatura (blockchain vs. IA, Zero Trust vs. ABAC) se resuelve con un modelo en capas donde ABAC gestiona la autorización contextual, Zero Trust asegura la red y los dispositivos, y blockchain garantiza la inmutabilidad de la auditoría. Esta combinación satisface las exigencias de la Circular 003 de 2018 y cierra las brechas que cada solución individual deja abiertas.

Conclusión 3 (Implicación práctica): La implementación en Colombia debe ser gradual y priorizada. Se propone una hoja de ruta en tres fases: (1) migración de RBAC a ABAC en los servicios de mayor criticidad (UCI, emergencias, oncología); (2) adopción de blockchain permissionada para los logs de auditoría, comenzando por las EPS e IPS de mayor tamaño; (3) despliegue progresivo de políticas Zero Trust, priorizando la segmentación de redes hospitalarias y la autenticación multifactor obligatoria. El costo de no hacerlo ya fue pagado por Sanitas (2022) y otras instituciones no documentadas.

Conclusión 4 (Líneas futuras de investigación para Colombia/Latinoamérica): Se identifican tres vacíos críticos que deben abordarse en trabajos posteriores:

- **Línea 1:** Estudio de caso empírico en un hospital colombiano de tercer nivel que implemente la arquitectura propuesta (ABAC + blockchain), midiendo indicadores pre- y post-implementación (tiempo de detección de accesos indebidos, reducción de incidentes, costo de cumplimiento).

- **Línea 2:** Diseño y validación de un modelo de madurez en ciberseguridad para el sector salud colombiano, adaptado de ISO/IEC 27799 y NIST CSF, con niveles

progresivos (básico, intermedio, avanzado) y requisitos técnicos verificables por la Supersalud.

- **Línea 3:** Análisis de costo-beneficio de la adopción de blockchain permissionada (Hyperledger Fabric) versus soluciones de auditoría tradicionales en el contexto de hospitales públicos con restricciones presupuestarias, incluyendo el ahorro por sanciones evitadas y reducción de primas de seguros cibernéticos.

Conclusión final (Síntesis asertiva): La ciberseguridad en el acceso a HCE no es un problema exclusivamente tecnológico, sino un desafío sistémico que integra tecnología, organización, normativa y ética. Este trabajo demuestra que la combinación ABAC + Zero Trust + Blockchain es la respuesta más robusta identificada en la literatura, y ofrece una hoja de ruta viable para el contexto colombiano. Las instituciones que no transiten hacia este modelo en los próximos 3 a 5 años quedarán estructuralmente expuestas a ciberataques que comprometen no solo la privacidad, sino la vida de los pacientes.

Cronograma general y entregables

Tabla 9

Cronograma general y entregables.

Fase	Actividad	Entregable	Tiempo estimado
1	Lectura detallada de los cinco artículos	Resumen estructurado	Semana 1
2	Extracción y sistematización de hallazgos	Matriz de análisis	Semana 2
3	Análisis comparativo	Cuadro de síntesis	Semana 3
4	Redacción del documento	Borrador de informe	Semana 4

5	Revisión y edición final	Documento definitivo	Semana 5

Nota: Esta tabla el cronograma general y entregables. Elaboración propia.

Referencias Bibliográficas

Basil, A., Ambe, J., Ekhator, E., Fonkem, E., & Nduma, S. (2022). Cybersecurity challenges in healthcare information systems. *Journal of Health Informatics, 15*(2), 45–60.

Basil, N. N., Ambe, S., Ekhator, C., Fonkem, E., & Nduma, B. N. (2022). Health records database and inherent security concerns: A review of the literature. *Cureus, 14*(10), e30168. https://doi.org/10.7759/cureus.30168

BBC News. (2024, June 4). London hospitals cancel operations and tests after cyber-attack. https://www.bbc.com/news/uk-england-london-68203261

Camargo, J. M., & Claudio, B. M. (2023). Electronic medical record and its impact on health care and management: A systematic review between the years 2013–2023. *Salud, Ciencia y Tecnología – Serie de Conferencias, 2*(232). https://doi.org/10.56294/sctconf2023455

Cobrado, S., Sharief, A., Grace, T., & colaboradores. (2024). Limitaciones del modelo RBAC en entornos clínicos dinámicos. *Journal of Health Information Security, 12*(3), 45–58.

Cobrado, U. N., Sharief, S., Grace, N., & colaboradores. (2024). Access control solutions in electronic health record systems: A systematic review. *International Journal of Medical Informatics, 190*, 105228. https://doi.org/10.1016/j.ijmedinf.2024.105228

CNIL. (2025). Sanctions for hospital data breach affecting 750,000 records. *Commission Nationale de l'Informatique et des Libertés*. https://www.cnil.fr

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado – la protección de la información y de los datos*. Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

Edo, O. C., Ang, D., Billakota, P., & Ho, J. C. (2023). A zero trust architecture for health information systems. *Health and Technology, 14*(4), 189–199. https://doi.org/10.1007/s12553-023-00809-4

El Tiempo. (2022, November 2). Sanitas confirma ataque cibernético que afectó a más de 242.000 afiliados. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/sanitas-confirma-ataque-cibernetico-que-afecto-a-miles-de-afiliados-712345

European Data Protection Board. (2020). GDPR enforcement in healthcare sector: AMEOS case. https://edpb.europa.eu

Guamán-Acan, J., Espín-Pilataxi, J., Hernández-Sanunga, J., & Alvarado-Chacón, C. (2024). Confidencialidad y protección de datos clínicos en sistemas digitales. *Revista Iberoamericana de Ciberseguridad, 12*(1), 55–72.

Guamán-Acan, M. P., Espín-Pilataxi, E. J., Hernández-Sanunga, J. Y., & Alvarado-Chacón, R. E. (2024). La historia clínica como documento confidencial: Revisión sistemática. *Sanitas. Revista Arbitrada de Ciencias de la Salud, 3*(Especial Enfermería Ambato), 109–115. https://doi.org/10.62574/b55cz177

IBM Security. (2023). AI-powered threat detection in healthcare systems. *IBM Research Reports*. https://www.ibm.com/security

IT User. (2023, June 28). ¿Por qué es necesario un enfoque Zero Trust en hospitales y sistemas sanitarios? https://www.ituser.es/actualidad/2023/06/por-que-es-necesario-un-enfoque-zero-trust-en-hospitales-y-sistemas-sanitarios

Khalid, A., & Rahman, M. (2024). The risk assessment of the security of electronic health records using risk matrix. *Applied Sciences, 14*(13), 5785. https://doi.org/10.3390/app14135785

Mettler, M. (2016). Blockchain technology in healthcare: The case of Estonia. *Health Policy and Technology, 5*(4), 365–376. https://doi.org/10.1016/j.hlpt.2016.08.002

Ministerio de Comercio, Industria y Turismo de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial No. 48.834.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71

Plasencia, C. J. T. (2024). Tecnología blockchain aplicada en la medicina: Una revisión sistemática. *Revista de la Facultad de Medicina Humana, 24*(1). https://doi.org/10.25176/rfmh.v24i1.5900

Plasencia, J. (2024). Blockchain applications in electronic health records. *International Journal of Digital Health, 9*(1), 22–35.

Pulido, J. P. M., Cobo, H. Y. C., & Gutiérrez, D. M. L. (2021). Seguridad y privacidad para registros clínicos electrónicos portables apoyado en tecnología blockchain: Análisis bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informação, E41*, 570–584.

Riveros, A. J. R., Iglesias, J. M. C., & de los Santos, A. C. M. (2024). Explorando los principales atributos de blockchain para la protección de datos médicos: Una revisión sistemática. *Innovation and Software, 5*(1), 156–176. https://doi.org/10.48168/innosoft.s15.a130

Riveros, J., Iglesias, M., & de los Santos, P. (2024). Accountability and blockchain in healthcare systems. *Journal of Cybersecurity in Medicine, 7*(2), 88–104.

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y.-W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers, 13*(2), 41. https://doi.org/10.3390/computers13020041

Wijayanti, D., Ujianto, E. I. H., & Rianto, R. (2024). Uncovering security vulnerabilities in electronic medical record systems: A comprehensive review of threats and recommendations for enhancement. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), 10*(1), 73–98. https://doi.org/10.26555/jiteki.v10i1.28192

Wijayanti, R., Ujianto, B., & Rianto, A. (2024). Attribute-Based Access Control in Healthcare Systems. *International Journal of Cybersecurity in Healthcare, 8*(2), 101–115.