Estrategia de administración del riesgo de ciberseguridad apoyada en la gestión de respuesta a incidentes para mejorar los controles de acceso y proteger la privacidad de la información en entornos hospitalarios

Hugo Fernando Figueroa Anacona

Asesor

Adriana Pilar Noguera Torres

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Maestría en Gestion de TI

2026

Agradecimientos

Esta iniciativa forma parte del proyecto desarrollado en el marco de la Convocatoria 890 de 2020 del Ministerio de Ciencia, Tecnología e Innovación de Colombia – Ministerio de Ciencia, Tecnología e Innovación – Minciencias, bajo el Contrato RC N° 2023-0678. Este apoyo ha sido fundamental para la formulación, desarrollo y difusión de los resultados presentados en este manuscrito.

Resumen

En el presente proyecto de investigación se propone el diseño preliminar de un modelo estratégico que ayude a optimizar el fortalecimiento de la ciberseguridad en los hospitales de primer nivel en el departamento del Huila, Colombia. Con base en un diagnóstico de vulnerabilidades relacionadas a la gestión de identidades, control de privilegios, autenticación y trazabilidad de accesos, se logra identificar debilidades recurrentes que representan un riesgo latente para la confidencialidad, integridad y disponibilidad de la información hospitalaria y administrativa.

Acorde a los lineamientos de la norma ISO/IEC 27002:2022, ISO/IEC 27001:2022, el NIST Cybersecurity Framework 2.0 y el Modelo de Seguridad y Privacidad de la Información (MSPI 2025), se organizaron políticas de acceso y autenticación cuyo fin radica en la mitigación de riesgos y al fortalecimiento institucional. Posteriormente, se elaboró un plan de respuesta a incidentes de ciberseguridad bajo un enfoque cíclico de mejora continua, con la articulación de fases de diagnóstico, planificación, implementación, seguimiento y evaluación. Por ultimo, se delimitaron indicadores de madurez para evaluar progresivamente el nivel de desarrollo en seguridad de la información, fomentando un modelo sostenible, escalable y adaptable a las condiciones tecnológicas y presupuestales de los hospitales analizados.

***Palabras clave*:** ciberseguridad, hospitales, autenticación, riesgos, implementación

Abstract

This research project proposes the preliminary design of a strategic model to optimize cybersecurity in primary care hospitals in the department of Huila, Colombia. Based on a vulnerability assessment related to identity management, privilege control, authentication, and access traceability, recurring weaknesses were identified that represent a latent risk to the confidentiality, integrity, and availability of hospital and administrative information.

In accordance with the guidelines of ISO/IEC 27002:2022, ISO/IEC 27001:2022, the NIST Cybersecurity Framework 2.0, and the Information Security and Privacy Model (MSPI 2025), access and authentication policies were established with the aim of mitigating risks and strengthening institutional security. Subsequently, a cybersecurity incident response plan was developed using a cyclical approach to continuous improvement, integrating phases of diagnosis, planning, implementation, monitoring, and evaluation. Finally, maturity indicators were defined to progressively evaluate the level of development in information security, promoting a sustainable, scalable model adaptable to the technological and budgetary conditions of the hospitals analyzed.

***Keywords*:** cybersecurity, hospitals, authentication, risks, implementation

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

La transformación digital del sector salud ha generado una creciente dependencia de infraestructuras tecnológicas para la gestión de información clínica, administrativa y financiera. Luego, la ciberseguridad se consolida como un componente esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos, especialmente en instituciones hospitalarias que manejan información sensible de pacientes. Sin embargo, los hospitales de primer nivel del departamento del Huila enfrentan limitaciones tecnológicas, presupuestales y organizacionales que incrementan su exposición a riesgos de seguridad de la información.

El presente proyecto de investigación tiene como objetivo diseñar un modelo estratégico orientado al fortalecimiento de la ciberseguridad en estas instituciones, partiendo de un diagnóstico de vulnerabilidades relacionadas con la gestión de identidades, control de accesos, autenticación y respuesta ante incidentes. Para ello, se toman como referencia estándares internacionales como ISO/IEC 27001:2022, ISO/IEC 27002:2022, el NIST Cybersecurity Framework 2.0 y el Modelo de Seguridad y Privacidad de la Información (MSPI 2025), adaptándolos al contexto institucional y operativo de los hospitales analizados.

El trabajo se estructura en cuatro resultados principales: un diagnóstico de riesgos y vulnerabilidades, la formulación de políticas de acceso y autenticación, el diseño de un plan de respuesta a incidentes de ciberseguridad y la construcción de una guía metodológica de autoevaluación basada en niveles de madurez. Con ello, se busca aportar una propuesta técnica, realista y escalable que contribuya al fortalecimiento progresivo de la seguridad digital en el sector salud del departamento del Huila.

Planteamiento del Problema

La digitalización de la información en el sector salud ha traído consigo numerosos beneficios en términos de eficiencia y acceso a los datos, pero también ha expuesto a las instituciones hospitalarias a un creciente riesgo de ciberataques y brechas de seguridad. A nivel mundial, los hospitales se han convertido en objetivos prioritarios para los ciberdelincuentes, quienes ven en los datos médicos una valiosa fuente de información confidencial y, en algunos casos, una oportunidad para extorsionar a las instituciones mediante ataques de ransomware. Este fenómeno también se refleja en el contexto nacional, donde el sector de salud en Colombia enfrenta grandes desafíos en la protección de los datos de los pacientes, especialmente en hospitales de primer nivel y con recursos limitados. En este planteamiento se explorarán estas problemáticas tanto a nivel internacional como nacional, para luego centrar el análisis en la situación particular.

En el entorno hospitalario, uno de los activos de información más críticos es la historia clínica electrónica, la cual, contiene información personal sensible referente a la salud de los pacientes, antecedentes médicos, diagnósticos y tratamientos. Salvaguardar esta información resulta fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos, así como para asegurar la continuidad de los servicios de atención médica. En este orden de ideas, las vulnerabilidades en los mecanismos de control de acceso, autenticación y gestión de identidades pueden representar riesgos significativos para la seguridad de la historia clínica y de los sistemas de información hospitalarios.

A nivel internacional, Li et al. (2025) hacen hincapié en el hecho de que los ciberataques contra hospitales se han triplicado en la última década. Los centros y sistemas de son hoy en día objetivos prioritarios de los ciberdelincuentes, a causa del alto valor de la información médica y

su evidente dependencia de los sistemas digitales para una correcta prestación de servicios. En los últimos años, los ciberataques dirigidos al sector salud han presentado un incremento exponencial, generando así interrupciones en la atención médica, a su vez implicaciones negativas en la seguridad del paciente y pérdidas económicas considerables para las instituciones hospitalarias.

Luego, diversos estudios reflejan una tendencia creciente que pone en riesgo la continuidad de los servicios clínicos y la protección de los datos de los pacientes. A su vez, se se indica el hecho que los hospitales almacenan una gran cantidad de información confidencial de los pacientes, que incluye datos personales, históricos médicos y detalles de tratamiento. Estos datos tienen un alto valor en el mercado negro y son codiciados tanto para fraudes financieros como para extorsiones mediante ataques de ransomware. La posibilidad de interrumpir servicios esenciales, como los sistemas de gestión de emergencias o los equipos médicos, convierte a los hospitales en blanco ideal, ya que las consecuencias pueden ser graves, incluso mortales, aumentando la presión sobre las instituciones para que cedan a las demandas de rescate; resaltando también el impacto devastador de estos ataques, que no solo afectan financieramente a las instituciones sino que también amenazan directamente la seguridad y privacidad de los pacientes.

Los ciberataques pueden causar interrupciones en los sistemas hospitalarios, retrasando tratamientos, diagnósticos y la capacidad de responder a emergencias. Además, los costos financieros de un ataque pueden ser elevados, incluyendo los gastos asociados con la restauración de sistemas, medidas de contención, posibles sanciones legales y pérdida de confianza pública. Li et al. (2025) indican que el sector salud registra costos promedio de hasta 10.93 millones de dólares a causa de los incidentes de violación de datos.

Así, se puede evidenciar que, los ciberataques contra instituciones de salud generan impactos económicos significativos. Los autores tambien indican que el sector hospitalario es uno de los más afectados en términos financieros, registrando costos promedio como los anteriormente mencionados, superando ampliamente a otros sectores económicos. Estos costos incluyen factores críticos como interrupción de servicios, recuperación de sistemas, costo de rescates y afectaciones graves en el sentido reputacional para las instituciones hospitalarias.

Para el ámbito nacional, Jairo Obando (Obando, 2024) refleja una realidad alarmante que también afecta a Colombia, donde el sector salud ha experimentado un incremento notable en la cantidad de incidentes de ciberseguridad. Este aumento no solo se debe a la digitalización acelerada de los sistemas de salud, sino también a la falta de infraestructura robusta y de medidas preventivas efectivas en muchos hospitales, especialmente en aquellos de primer nivel con limitaciones de recursos, como en las zonas rurales del país. El autor menciona que, en 2023, Colombia fue el cuarto país más atacado de América Latina, con más de 5 mil millones de intentos de ciberataques en el primer semestre, y el sector salud fue uno de los más afectados.

Estos ataques ponen en peligro la seguridad de los datos personales y médicos de los pacientes, que son especialmente sensibles y valiosos en el mercado negro, y exponen a los hospitales a extorsiones mediante ransomware. Pero, estos ataques no solo impactan la economía, sino también la calidad de la atención y la confianza pública en el sistema de salud. En el ámbito nacional, la interrupción de sistemas debido a ciberataques ha afectado la prestación de servicios críticos, desde el acceso a medicamentos hasta el agendamiento de citas y la realización de cirugías.

La situación se complica en hospitales que dependen de proveedores externos para la gestión de sus sistemas de información, lo que limita su capacidad para implementar controles de acceso adecuados y responder rápidamente ante un incidente de seguridad.

Esta dependencia tecnológica, sin las herramientas ni el personal capacitado necesarios, amplifica la vulnerabilidad de los hospitales colombianos ante las crecientes amenazas cibernéticas. Es por ello que, la relevancia de este problema en Colombia subraya la urgencia de implementar estrategias de ciberseguridad que incluyan controles de acceso efectivos y planes de respuesta a incidentes en el sector salud. La situación descrita en el artículo evidencia la necesidad de soluciones inmediatas para proteger la información sensible de los pacientes, reducir el riesgo de interrupciones en la atención y mejorar la resiliencia de los hospitales ante ciberataques. Este análisis contextualiza la problemática de ciberseguridad que enfrentan los hospitales de primer nivel, y respalda la importancia de una investigación enfocada en desarrollar una estrategia de administración del riesgo de ciberseguridad.

Además, la falta de controles de acceso adecuados como se menciona en el artículo Vashishth (Vashishth et al., 2024) puede permitir a los actores malintencionados, tanto internos como externos, acceder a estos datos y utilizarlos para fines maliciosos. Esto puede incluir el robo de identidad, el fraude de seguros de salud y el espionaje corporativo y es uno de los problemas centrales definidos a lo largo de la investigación actual junto con los artículos mencionados.

También, el autor Tekin (Tekin & Kartal, 2024) nos habla sobre la protección de datos sensibles, donde menciona que Los hospitales manejan una gran cantidad de datos sensibles, incluyendo información personal y médica de los pacientes y por ello, esos datos deben ser protegidos de accesos no autorizados, alteraciones y pérdidas que pongan en peligro la relación

de confianza entre el paciente y el hospital. También habla de que la integridad de los datos médicos es fundamental para la prestación de atención médica de calidad y que cualquier alteración no autorizada de estos datos puede tener graves consecuencias para la salud de los pacientes. Luego, Shamout (Shamout et al., 2024) nos habla acerca de la importancia en la protección de la información confidencial de los pacientes y en cómo esta protección no está siendo bien gestionada en la actualidad, con la base de que los datos de salud son extremadamente sensibles y su divulgación no autorizada puede tener graves consecuencias para los pacientes.

Las soluciones de seguridad de datos, como los controles de acceso, ayudan a garantizar que sólo las personas autorizadas puedan acceder a estos datos. De esta manera vemos como los elementos de árbol del problema y los artículos referenciados dan ideas acerca del problema planteado en el proyecto, con la premisa que la información hospitalaria y sobre todo la información personal de los pacientes debe ser debidamente recepcionada y gestionada, algo que en la actualidad suele no ser muy seguro pues el sector salud está expuesto a los ataques cibernéticos en gran medida, haciendo que los datos personales de los usuarios sea un blanco accesible y vulnerable ante estos eventos adversos de seguridad.

En los hospitales de primer nivel se enfrenta una situación crítica en términos de ciberseguridad debido a la falta de controles de acceso robustos para proteger la información médica confidencial de los pacientes. Actualmente, cualquier persona con credenciales al sistema hospitalario puede acceder sin restricciones a datos sensibles, como historias clínicas, motivos de consulta y resultados de laboratorio, lo cual representa un riesgo significativo para la privacidad de los pacientes y para la integridad de los hospitales. Esta problemática se agrava por la

dependencia de estas instituciones en un sistema de información gestionado por un proveedor externo, lo que limita su autonomía para implementar y adaptar políticas de seguridad adecuadas.

¿Cómo pueden implementarse estrategias de administración del riesgo de ciberseguridad, apoyadas en la gestión de respuesta a incidentes, para mejorar los controles de acceso y proteger la privacidad de los hospitales de primer nivel en el Huila?

Justificación

La información médica es uno de los activos más valiosos en el sector hospitalario, cuya protección es fundamental para preservar la privacidad del paciente y asegurar la continuidad de la atención de calidad. En los hospitales de primer nivel del Huila, la creciente digitalización de los sistemas de información ha expuesto datos críticos de pacientes a un riesgo considerable de ciberataques. Esto se agrava en un entorno donde los recursos y la infraestructura tecnológica son limitados y dependen de sistemas externos, dificultando la implementación de controles de acceso robustos y una adecuada gestión de respuesta a incidentes. La relevancia de este proyecto radica en abordar esta necesidad urgente, demostrando cómo la administración del riesgo de ciberseguridad y la implementación de medidas de respuesta a incidentes pueden reducir la vulnerabilidad de los datos hospitalarios y, por ende, proteger el bienestar de los pacientes, al mismo tiempo que fortalecen la confianza en la institución.

Esta investigación busca brindar una contribución en cuanto a ampliar el conocimiento en el campo de la ciberseguridad aplicada al sector salud en entornos de baja capacidad, como los hospitales de primer nivel. Actualmente, existe un vacío en la implementación de estrategias de administración de riesgos específicamente diseñadas para hospitales de primer nivel en el dpto del Huila, donde las limitaciones económicas y de personal capacitado incrementan la vulnerabilidad ante ciberamenazas. A su vez, la utilidad del proyecto se extiende tanto al ámbito académico como al práctico. Desde una perspectiva académica, los resultados de este proyecto enriquecerán el campo de estudio de la ciberseguridad, proporcionando un marco teórico y metodológico que otros investigadores podrán utilizar para explorar temas relacionados en el sector salud y en la administración de riesgos en instituciones con limitaciones de recursos. En el ámbito práctico, el proyecto ofrecerá resultados que pueden aplicarse de manera directa en la

gestión hospitalaria, optimizando los controles de acceso y mejorando la capacidad de respuesta ante incidentes. Esto no solo contribuirá a proteger la información sensible de los pacientes, sino que también reducirá el riesgo de sanciones legales y aumentará la confianza del público en el hospital.

El proyecto se sustenta en teorías y estudios recientes en administración de riesgos y ciberseguridad, y se enmarca en un contexto global y nacional en el cual el sector salud ha sido objeto de un número creciente de ciberataques. Este marco teórico proporciona una base sólida y valida la pertinencia de la investigación, dado que evidencia la urgencia de implementar políticas de ciberseguridad más estrictas en entornos hospitalarios. La metodología propuesta, centrada en la administración de riesgos con una respuesta eficiente a incidentes, se adapta a las necesidades de hospitales con limitaciones en recursos y acceso a tecnología avanzada, asegurando que los resultados de la investigación sean aplicables en condiciones similares y útiles para mejorar la seguridad en otras instituciones del sector. Por ello, la implementación de esta estrategia de ciberseguridad beneficiará directamente a los pacientes y al personal hospitalario, ya que la protección de los datos sensibles es fundamental para preservar la privacidad, mejorar la seguridad y generar un entorno de atención médica confiable. En términos económicos, el proyecto podría reducir los costos asociados con potenciales ciberataques, que incluyen gastos de restauración de sistemas, pérdida de información y sanciones regulatorias. La eficiencia en la administración de los hospitales también mejorará al reducir el riesgo de interrupciones de servicios debido a incidentes de seguridad. Para dar sentido a lo anteriormente propuesto, esta investigación aporta un enfoque innovador al adaptar una estrategia de administración de riesgos de ciberseguridad con un sistema de respuesta a incidentes específicamente diseñado para el contexto de hospitales de primer nivel. Pocas investigaciones han abordado el tema de la

ciberseguridad en hospitales de zonas primer nivel en Colombia, lo que le otorga al proyecto un carácter original y valioso en la generación de conocimiento en esta área. La estrategia que se propone es una novedad en el ámbito de ciberseguridad aplicada a hospitales, al enfocarse en controles de acceso adaptados y en una respuesta rápida y efectiva ante posibles incidentes.

El proyecto es viable en términos de tiempo y recursos, ya que está diseñado para utilizar prácticas de ciberseguridad y administración de riesgos accesibles y replicables, ajustadas a las condiciones reales de un hospital con recursos limitados. La investigación tiene un alcance específico y realista, al estar enfocada en el desarrollo de una estrategia de seguridad en un entorno hospitalario particular, lo que permite que los resultados sean medibles y evaluables. Este proyecto representa una respuesta fundamentada y urgente a estos desafíos, ya que busca desarrollar e implementar una estrategia de administración del riesgo de ciberseguridad centrada en controles de acceso robustos y en la protección de datos sensibles. Con esta iniciativa, se espera fortalecer la confianza de los pacientes en la gestión hospitalaria y contribuir al desarrollo de prácticas (como se mencionó anteriormente) seguras y replicables en el contexto de hospitales con limitaciones de recursos.

Objetivos

Objetivo General

Desarrollar una estrategia de administración del riesgo de ciberseguridad apoyada en la gestión de respuesta a incidentes para mejorar los controles de acceso y proteger la privacidad de la información en entornos hospitalarios.

Objetivos Específicos

Analizar las amenazas, vulnerabilidades y riesgos más comunes de ciberseguridad presentes en los hospitales de primer nivel del departamento del Huila mediante la recopilación de información especializada, para identificar los factores críticos que afectan la seguridad informática y la protección de datos sensibles en estas instituciones

Diseñar políticas de control de acceso y autenticación orientadas a la protección de la información clínica y de los sistemas de información hospitalarios en los hospitales de primer nivel del departamento del Huila, en concordancia con estándares y normativas vigentes de seguridad de la información.

Desarrollar planes de respuesta a incidentes de ciberseguridad que permitan proteger la información clínica y los sistemas de información hospitalarios, mediante el análisis de casos que faciliten la identificación, contención y mitigación de amenazas en hospitales de primer nivel del departamento del Huila.

Proponer una guía metodológica que permita a los hospitales de primer nivel del departamento del Huila evaluar internamente el impacto y la efectividad de la estrategia de administración del riesgo de ciberseguridad, particularmente en la protección de la información clínica y el control de acceso a los sistemas de información hospitalarios, mediante el uso de métricas de rendimiento y técnicas de análisis adaptadas a su contexto institucional.

Marco de Referencia

Marco contextual

Sector Salud Colombiano y Hospitales de Primer Nivel

El sistema de salud colombiano está estructurado en distintos niveles de atención, diseñados para asegurar una cobertura completa para todos. El Ministerio de Salud y Protección Social (2022) destaca que el primer nivel es fundamental, ya que ofrece servicios de medicina general, atención de urgencias menores, vacunación y programas de promoción y prevención, atendiendo a la mayoría de los ciudadanos en todo el país. La Organización Panamericana de la Salud (OPS, 2022) resalta que este nivel es la base del modelo de atención primaria, crucial para asegurar que todos tengan acceso equitativo a los servicios.

La Superintendencia Nacional de Salud (2023) indica que más del 70% de las consultas en áreas rurales se resuelven en centros de primer nivel, demostrando su relevancia estratégica en el país. A pesar de esto, estas instituciones suelen tener recursos escasos: instalaciones pequeñas, equipos básicos y poco personal especializado. La Defensoría del Pueblo (2021) advierte que estas carencias causan diferencias en la calidad de la atención, sobre todo en zonas remotas con infraestructuras hospitalarias deficientes desde hace tiempo.

La digitalización también ha influido en este nivel de atención. El Observatorio de Salud Digital (2023) señala que muchos hospitales de primer nivel están implementando sistemas de información y registros electrónicos de pacientes. Sin embargo, estos avances son dispares: las ciudades muestran mayor progreso, mientras que en zonas rurales aún se usan registros en papel o programas básicos con poca seguridad. Aunque hay un esfuerzo por la digitalización, existe una gran diferencia entre los planes nacionales y la realidad en cada territorio.

En Colombia, la legislación da relevancia a este nivel asistencial. La Ley 1751 de 2015, o Ley Estatutaria de Salud, declara que acceder a los servicios sanitarios es un derecho esencial, y en esta línea, los centros de salud de primer nivel son la puerta de entrada al sistema para los ciudadanos. Según el CONPES 3975 de 2019, sobre la Política de Gobierno Digital, estas entidades deben implementar tecnologías que mejoren la seguridad de la información y la protección de datos de los usuarios, aunque sus recursos sean limitados.

Así, los hospitales de primer nivel en Colombia son la piedra angular del sistema de salud, pero también el punto más débil en cuanto a recursos y tecnología. Tal como indica la OPS (2022), potenciar la atención primaria es clave para disminuir las diferencias en salud, pero en Colombia esto implica asegurar la información y la confianza del paciente en un mundo digital creciente.

Contexto Regional. Departamento del Huila

El departamento del Huila, que se encuentra en el suroccidente de Colombia, se caracteriza por su diversidad cultural y geográfica y según el DANE(DANE, 2023), cuenta con una población aproximada de 1,2 millones de habitantes distribuida en 37 municipios. La misma fuente indica que una fracción considerable de los habitantes de Colombia reside en zonas rurales y alejadas, lo cual dificulta el acceso a servicios públicos esenciales, sobre todo en el ámbito de la salud. El Ministerio de Salud y Protección Social (2022) señala que, debido a esta situación geográfica, los hospitales de primer nivel son la principal opción para la atención médica en comunidades remotas, funcionando como centros de atención primaria y para emergencias menores.

Desde el punto de vista socioeconómico, la economía del Huila se centra en la agricultura, con el café, el arroz y el cacao como productos destacados, lo cual repercute en un

perfil poblacional predominantemente rural (Gobernación del Huila, 2023). Este entorno genera una gran necesidad de servicios de salud primaria, ya que esta población tiene menos acceso a especialidades médicas de segundo y tercer nivel, las cuales se concentran en Neiva y Pitalito. El Observatorio Nacional de Salud (2022) indica que el 65% de los usuarios en municipios intermedios y rurales del Huila reciben atención en hospitales de primer nivel, lo que demuestra su importancia estratégica para asegurar la igualdad en el acceso.

Entonces, estas instituciones se ven afectadas por diversas carencias. La Superintendencia Nacional de Salud (2023) informa que los hospitales de primer nivel en el Huila presentan fallas en la infraestructura física, la conectividad digital y la disponibilidad de personal especializado en tecnologías de la información. Esta situación no solo complica la gestión administrativa, sino que también pone en peligro la seguridad de los datos de los pacientes, ya que muchos procesos dependen de sistemas básicos, registros manuales o soporte tecnológico externo. En este contexto, la brecha digital representa un factor de riesgo para la protección de la información clínica y la continuidad de los servicios.

En ese orden de ideas, las amenazas a la ciberseguridad son cada vez mayores. El MinTIC (2024) indica que los hospitales públicos de menor tamaño en regiones como el Huila son muy susceptibles a problemas como ataques de ransomware, ingresos no autorizados y extravío de datos, debido a la falta de medidas de seguridad sólidas para verificar la identidad, controlar los accesos y reaccionar ante incidentes. Además, un estudio del Observatorio de Salud Digital (2023) muestra que aproximadamente el 70 % de los hospitales de primer nivel en zonas rurales del país carecen de normas formales de ciberseguridad, lo cual incrementa la exposición a peligros y socava la fe de la gente en el sistema de salud.

El entorno regional también debe considerarse desde el punto de vista social y cultural. En el Huila existen comunidades campesinas e indígenas que dependen casi por completo de los hospitales locales para recibir atención médica. La Defensoría del Pueblo (2021) señala que en estas zonas aún existen dificultades para acceder a los servicios de salud debido a la lejanía, la escasez de transporte y las dificultades económicas de los habitantes. Estas circunstancias resaltan la importancia de los hospitales de primer nivel como protectores de la atención médica y de derechos esenciales como la salud y la vida.

En resumen, la situación en el Huila evidencia la contradicción entre la gran dependencia de los hospitales de primer nivel y las deficiencias estructurales y tecnológicas que sufren estas entidades. Según la Gobernación del Huila (2023), es urgente abordar los problemas de conectividad, seguridad digital y capacitación del personal, ya que influyen en la eficacia del sistema de salud en la región. Este panorama explica y justifica la relevancia de este proyecto, cuyo objetivo es mejorar la gestión de riesgos de ciberseguridad y la protección de la información confidencial de los pacientes en los hospitales de primer nivel del departamento.

Contexto Tecnológico y Organizacional

En la última década, se ha observado un incremento en el uso de las tecnologías informáticas dentro del ámbito de la salud en Colombia, motivado principalmente por la búsqueda de una gestión clínica y administrativa más eficiente. El Ministerio de Salud y Protección Social (2022) destaca que la implementación de expedientes clínicos electrónicos, sistemas de información hospitalaria y plataformas de telemedicina es fundamental en la política de transformación digital del sector. No obstante, la adopción de estas tecnologías varía considerablemente: las instituciones de mediana y alta complejidad tienen más recursos, mientras

que los hospitales de primer nivel, sobre todo en zonas como el Huila, avanzan más lentamente y enfrentan mayores obstáculos técnicos y económicos.

Según la Superintendencia Nacional de Salud (2023), muchos hospitales de primer nivel todavía dependen de sistemas básicos, a veces desarrollados localmente, sin integración entre las áreas clínicas y administrativas. Esta desconexión resulta en procesos duplicados, demoras en el acceso a la información y problemas para asegurar la continuidad en la atención al paciente. A nivel organizativo, la escasez de personal experto en tecnologías de la información es un problema grave: el Observatorio Nacional de Salud (2022) informa que el 65 % de las instituciones de baja complejidad carecen de un departamento formal de gestión de TI, lo que les obliga a contratar servicios externos para el soporte y la administración de sistemas.

La situación de la ciberseguridad genera especial inquietud. ENISA (2023) señala que el sector salud es uno de los más afectados por ataques de ransomware a nivel global, y Colombia no es una excepción. El MinTIC (2024) advierte que los hospitales de primer nivel suelen ser más vulnerables por la falta de políticas de seguridad sólidas, la ausencia de controles de acceso diferenciados y el uso de contraseñas comunes o compartidas. En estas instituciones, es frecuente que un solo usuario acceda a diversos módulos del sistema, sin separación de funciones ni supervisión continua, aumentando el riesgo de accesos no autorizados y la filtración de datos confidenciales.

Otro de los factores con criticidad máxima es la conexión a internet. Según datos de la Gobernación del Huila (2023), los hospitales rurales sufren de un acceso a internet inestable y limitado, complicando el uso eficaz de plataformas en línea. Esto perjudica tanto la administración como la comunicación con otros centros de referencia. Esta carencia también

dificulta la implementación de seguridades modernas, como la autenticación multifactor, el monitoreo constante o la copia de datos en la nube.

En cuanto a la organización, muchos dependen de empresas externas para el manejo de sistemas y redes. El Observatorio de Salud Digital (2023) señala que más del 55 % de los hospitales básicos en Colombia contratan a terceros para la gestión tecnológica, lo cual trae riesgos en la continuidad del servicio y la protección de datos. Aunque ayuda a cubrir la falta de personal especializado, también genera dudas sobre quién controla los datos y quién responde ante problemas de seguridad.

Por último, la cultura de ciberseguridad está poco desarrollada. La Defensoría del Pueblo (2021) indica que la mayoría del personal de salud y administrativo en instituciones básicas no recibe capacitación constante sobre cómo proteger la información, usar bien las credenciales y responder a incidentes. Esta falta de conciencia aumenta la vulnerabilidad tecnológica y reduce la capacidad de las organizaciones para prevenir y manejar riesgos eficazmente.

En resumen, la situación tecnológica y organizativa de los hospitales básicos del Huila muestra un avance inicial en la digitalización, pero con grandes problemas en infraestructura, personal capacitado y cultura de seguridad. Esto demuestra la necesidad de crear estrategias adaptadas a su realidad, que mejoren los controles de acceso, aumenten la capacidad de respuesta ante incidentes y fomenten una gestión responsable y sostenible de la información confidencial de los pacientes.

Brechas y Riesgos Actuales

En el sector salud, los peligros digitales ya no son algo teórico, sino un problema que ocurre a menudo. La Agencia Europea de Ciberseguridad (ENISA, 2023) señala que el ransomware causa cerca del 54 % de los incidentes de seguridad en hospitales y centros de salud,

siendo el peligro más común allí. Esto demuestra que los datos médicos, debido a su gran valor, son un objetivo clave para los cibercriminales.

En Colombia, la vulnerabilidad de entidades públicas y privadas también se ha hecho evidente. Según Reuters (2023), más de 50 instituciones sufrieron un ataque a IFX Networks, una empresa que provee tecnología, lo que detuvo el trabajo de varios ministerios y servicios clave por un tiempo. Esto muestra el peligro de depender de proveedores externos, sobre todo en hospitales pequeños sin áreas internas de ciberseguridad.

Un ejemplo claro en la salud colombiana ocurrió en 2022, cuando la red de clínicas y EPS del grupo Keralty (Sanitas/Colsanitas) sufrió un ataque de ransomware que frenó servicios de citas y acceso a sitios web (BleepingComputer, 2022; Infosecurity Magazine, 2022). Este suceso enseñó cómo un problema digital puede afectar la atención médica y hacer que los usuarios desconfíen.

En general, el país se enfrenta a números preocupantes de intentos de ataque. El Ministerio de las TIC (MinTIC, 2025) informó que en 2024 hubo más de 36. 000 millones de intentos de ciberataques en Colombia, afectando sobre todo a la salud, las finanzas y la energía. Esta situación refuerza la necesidad de tener herramientas básicas para manejar riesgos y planes de respuesta en hospitales públicos.

Asimismo, se han detectado deficiencias organizativas en las propias instituciones. La Superintendencia Nacional de Salud (Supersalud, 2024) indica que la mayoría de los centros de salud primarios aún no cuentan con protocolos de seguridad establecidos y confían en empresas externas para gestionar sus sistemas informáticos sanitarios. Según el Ministerio de Salud (MinSalud, 2024), la transformación digital progresa, pero siguen existiendo grandes diferencias entre los centros de baja y alta complejidad, lo que aumenta los puntos débiles.

A nivel mundial, sucesos recientes como el ciberataque de 2024 a la red de hospitales Ascension Health en Estados Unidos, que perjudicó a millones de usuarios, han resaltado la necesidad de medidas elementales como la verificación en dos pasos, la división de redes y los planes de contingencia verificados (American Hospital Association, 2024). Estas enseñanzas globales son trasladables a Colombia, donde los hospitales de primer nivel se encuentran en situaciones parecidas de fragilidad tecnológica y dependencia de terceros.

Resumiendo, las carencias y peligros actuales en los hospitales de primer nivel mezclan elementos como la gran exposición a peligros, la escasez de habilidades técnicas, la dependencia de proveedores externos y la carencia de políticas de ciberseguridad firmes. Esta situación justifica la relevancia de estrategias diseñadas para estos entornos, que contemplen evaluaciones de riesgos, controles de acceso y protocolos de respuesta a incidentes como los planteados en este proyecto.

Marco Teorico

Para la elaboración del marco teórico se lleva a cabo una búsqueda documental sistemática que busca identificar literatura académica, normativa técnica y lineamientos institucionales relacionados con términos clave como ciberseguridad, seguridad de la información en el sector salud y modelos de gestión de riesgos. Se consulta en bases de datos académicas como Google Scholar y repositorios institucionales, al igual que en portales oficiales de organismos internacionales y nacionales, por ejemplo la International Organization for Standardization (ISO), el National Institute of Standards and Technology (NIST) y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC).

Se da prioridad a documentos publicados entre 2018 y 2025, con énfasis en normas vigentes, así como marcos de referencia actualizados y estudios relacionados con la gestión de identidades, autenticación, control de accesos y respuesta a incidentes en entornos hospitalarios como criterios de selección. A su vez, se toman en cuenta publicaciones que aportarán rigor técnico, respaldo institucional y aplicabilidad asertiva al contexto de entidades públicas del sector salud.

La historia clínica electrónica se define como uno de los activos de información más sensibles dentro de las instituciones de salud, dado a su integración con la información personal y clínica de los pacientes, por ello, debe ser protegida mediante mecanismos asertivos de seguridad de la información. En este contexto, una adecuada implementación de controles de acceso, autenticación robusta y mecanismos de monitoreo se hace fundamental para poder prevenir accesos no autorizados y garantizar así la privacidad de la información clínica.

La información recopilada es analizada y organizada de acuerdo con su pertinencia temática y su alineación con los objetivos del proyecto, permitiendo estructurar un marco teórico fundamentado en estándares internacionales reconocidos y en lineamientos normativos nacionales aplicables al contexto colombiano.

La seguridad de la información en el ámbito hospitalario es crítica debido a la naturaleza sensible de los datos que se manejan. Los hospitales almacenan y procesan información médica confidencial, como historias clínicas, diagnósticos, tratamientos y datos personales de los pacientes. La seguridad de esta información es esencial para garantizar la calidad de la atención médica, proteger la privacidad de los pacientes y cumplir con las regulaciones legales.

Es bien sabido que el sector de la salud enfrenta múltiples desafíos en cuanto a la protección de la información. Las instituciones hospitalarias manejan una gran cantidad de datos sensibles, como historiales médicos, diagnósticos, tratamientos y otra información personal de los pacientes. El aumento de la digitalización en los procesos de atención ha incrementado la dependencia de sistemas de información, lo que ha hecho que la ciberseguridad sea un componente esencial para garantizar la protección de los datos, así como para cumplir con normativas locales e internacionales.

Desde el concepto propuesto por Murdoch (Murdoch, 2021), La privacidad de la información y la inteligencia artificial en el contexto de la salud presenta desafíos únicos y significativos, ya que la inteligencia artificial tiene el potencial de revolucionar el sector de la salud mediante la mejora de la precisión diagnóstica, la personalización del tratamiento y la eficiencia operativa pero sobre todo, en el establecimiento de controles estrictos de seguridad, acceso y ejecución de operativas (controles de acceso como los que se mencionan en el interrogante anterior), aun así, es un tema que debe tomarse con cautela puesto que los sistemas de inteligencia artificial dependen de grandes conjuntos de datos para aprender y hacer predicciones, algo que comúnmente incluye información personal y sensible. La recopilación, el almacenamiento y el análisis de estos datos deben realizarse de manera que se respeten los derechos de privacidad de los individuos y se cumpla con las regulaciones de protección de datos, algo que también está cargado de numerosos desafíos y riesgos, pero, es una alternativa viable según el autor si se tiene en cuenta la debida estructuración de normativas y directrices de los sistemas de inteligencia artificial para que los datos hospitalarios no sean vulnerados o hurtados en el peor de los casos y los pacientes puedan tener la tranquilidad que se les está brindando una atención de calidad y con seguridad. De igual manera y similarmente a lo que se

plantea en la enunciación anterior, el autor Simic V (Ala et al., 2024) propone visualizar una perspectiva desde el uso del internet de las cosas o IoT en cuanto a estrategias avanzadas se refiere, pues sugiere que La información hospitalaria y la Internet de las Cosas (IoT) en el ámbito de la salud son dos dominios que, aunque interrelacionados, presentan contrastes significativos en términos de gestión, seguridad y aplicación, relacionando la información hospitalaria que se refiere a los datos clínicos y administrativos generados en el contexto de la atención médica y que son altamente sensibles y están sujetos a estrictas regulaciones de privacidad y seguridad, como HIPAA en Estados Unidos y es aquí donde también se hace presente la necesidad de controles de acceso y ejecución robustos y un enfoque de confidencialidad para salvaguardar tanto al paciente como a la entidad hospitalaria ya que los sistemas que manejan esta información están diseñados para ser seguros por defecto, con múltiples capas de protección y políticas de acceso basadas en roles. Ahora, se pueden relacionar el anterior interrogante con la premisa actual de definir estrategias avanzadas de seguridad, pues mientras que la información hospitalaria se centra en la protección y el manejo cuidadoso de los datos del paciente dentro de un entorno controlado, la IoT en la salud busca expandir las capacidades de monitoreo y tratamiento a través de la conectividad pero con un objetivo y fin común como lo es la seguridad de los datos que en el hospital se manejan y cómo mediante una serie de controles estrictos de acceso esta información es posible únicamente por quienes estén debidamente autorizados y facultados para tal fin. Una evaluación y mejoramiento continuo es posible y viable si se consideran elementos esenciales en el acceso a la información hospitalaria, según lo define el autor Zhan (Zhan et al., 2024), como las amenazas latentes ante un sector hospitalario, la evolución de las tecnologías, hallazgos de vulnerabilidades registrados, entre otros, y por ello, especifica que la mejora continua de los controles de acceso en el entorno hospitalario es no solo

posible, sino también necesaria para adaptarse a las cambiantes amenazas de seguridad y a las innovaciones tecnológicas define los hospitales como entornos dinámicos con una gran cantidad de personal, pacientes y visitantes que requieren diferentes niveles de acceso. De igual manera, también, la digitalización y automatización de los controles de acceso pueden proporcionar un registro más preciso y en tiempo real de quién está accediendo a qué áreas del hospital, lo que mejora la capacidad de respuesta ante incidentes de seguridad.

Pero, la mejora continua de los controles de acceso también debe considerar la privacidad y la protección de datos del paciente. Cualquier nueva tecnología o proceso debe ser evaluado cuidadosamente para asegurar que no comprometa la confidencialidad de la información sensible. Esto requiere una colaboración estrecha entre los departamentos de tecnología, seguridad y administración del hospital, así como una formación adecuada del personal en las nuevas políticas y tecnologías implementadas, lo que convierte estos componentes en bases y utilidades para una implementación y mejora continua de controles de acceso confiables y asertivos. En comparación con lo dicho anteriormente encontramos el artículo de Memon (Memon et al., 2024), quien habla principalmente de identificar y analizar riesgos como pilares fundamentales de controles de acceso retroalimentables y optimizables, donde la fase de identificar se centra en detectar los activos de información (como los registros de salud electrónicos), las amenazas a esos activos (como los ataques de phishing o ransomware), y las vulnerabilidades que podrían ser explotadas por esas amenazas (como los sistemas desactualizados o las políticas de seguridad deficientes). Este proceso debe ser exhaustivo y considerar todos los aspectos del entorno de atención sanitaria, incluyendo la tecnología, los procesos y las personas para posteriormente evaluar la probabilidad de que una amenaza se materialice y explote una vulnerabilidad, así como el impacto que esto tendría en el hospital. El

análisis de riesgos debe tener en cuenta factores como la criticidad de los activos de información, la capacidad de los actores de amenazas y la eficacia de los controles de seguridad existentes y es aquí donde dichos controles deben ser robustos, eficaces, mejorables y confiables, luego, la evaluación de riesgos implica determinar qué riesgos son aceptables y cuáles requieren mitigación. Esto se hace generalmente comparando el nivel de riesgo con un umbral de riesgo predefinido. Los riesgos que están por encima de este umbral se consideran inaceptables y requieren la implementación de controles de seguridad adicionales ya que los datos de los pacientes pueden ser hurtados por diferentes métodos de vulneración o penetración a los sistemas hospitalarios. Si vemos la perspectiva de Abid (Abid et al., 2024), los contrastes definidos por los autores preliminares son considerables desde un punto de vista focalizado a un control de acceso distribuido y basado en roles, donde los derechos de acceso se asignan a roles en lugar de a usuarios individuales. Los usuarios son asignados a uno o más roles, y cada rol tiene un conjunto de permisos asociados. Esto simplifica la gestión del acceso, ya que los cambios en los derechos de acceso a menudo implican simplemente cambiar la asignación de roles de un usuario. Es por lo anterior que se define la importancia de los controles de acceso a la información hospitalaria ligada a estrategias de seguridad y sobre todo los controles optimizables para garantizar la viabilidad de los lineamientos propuestos.

La ciberseguridad hospitalaria implica proteger la integridad, confidencialidad y disponibilidad de los sistemas de información de salud, que gestionan datos sensibles como registros médicos electrónicos (RME), resultados de laboratorio y datos personales de los pacientes. Estos datos son extremadamente valiosos para los hospitales, pero también para los actores maliciosos, lo que los convierte en objetivos prioritarios para ataques cibernéticos. Los avances tecnológicos han hecho que herramientas como la inteligencia artificial (IA) y el Internet

de las cosas (IoT) estén ampliamente disponibles en la atención médica, lo que aumenta la conectividad y la eficiencia, pero los hospitales enfrentan mayores riesgos. Tekin y Kartal (2024) demostraron que la salud digital, si bien es beneficiosa, también aumenta significativamente los riesgos de ciberseguridad.

Analizar y gestionar el riesgo cibernético es un proceso crítico en cualquier entorno que procese información confidencial. Los hospitales enfrentan una variedad de amenazas al almacenar información médica confidencial, desde acceso no autorizado hasta ataques de ransomware. Estas amenazas pueden comprometer la privacidad del paciente, dar lugar a sanciones legales y dañar la reputación del hospital. Las instituciones sanitarias no sólo deben proteger la integridad de los datos, sino también garantizar que la información esté disponible para los médicos y otros profesionales cuando sea necesario. Vasishth et al. (2024) señalan que uno de los mayores problemas de este sector es la falta de controles de acceso estrictos, que permitan a los empleados internos y externos acceder a información confidencial sin la autorización adecuada.

A su vez, Las investigaciones de seguridad de la información en el sector salud referenciadas previamente utilizan una variedad de materiales y metodologías para identificar, evaluar y documentar los temas de seguridad.

Dentro de la identificación de las metodologías más empleadas en investigaciones sobre seguridad de la información en el sector salud, se hace un análisis comparativo de los estudios referenciados en el marco teórico y también, se estudian las estrategias metodológicas descritas en cada investigación, buscando patrones recurrentes en los enfoques que soportan el diagnóstico, evaluación y fortalecimiento de la seguridad digital en entornos hospitalarios. Para criterio de selección se hace base en la frecuencia de aparición de determinadas metodologías, su

alineación con estándares internacionales reconocidos (ISO, NIST) y su aplicabilidad posible al contexto institucional de hospitales públicos.

A continuación, se listan algunas de las más sobresalientes:

Evaluación de Riesgos. Esta es una metodología utilizada en la gran mayoría de las investigaciones que implica identificar los puntos centrales que contengan información, las amenazas a esos puntos y como desarrollar un planteamiento de solución ante eventualidades, para así evaluar la viabilidad del mismo y finalmente establecer los argumentos o acciones según sea el caso para dar respuesta al problema principal.

Auditorías de Seguridad. Las auditorías de seguridad se hacen presentes en la revisión de políticas y procedimientos, la inspección de la configuración del sistema y la revisión de los registros de seguridad, para establecer falencias y hechos como se menciona en las investigaciones.

Formación en Seguridad de la Información. La formación en seguridad de la información es un material clave en las investigaciones expuestas. Esto implica que los autores de las investigaciones tienen conocimientos en prácticas seguras de manejo de datos, la concienciación sobre las amenazas de seguridad y la formación en el uso seguro de la tecnología y/o cuentan con apoyo especializado en el manejo de los temas de las mismas.

Cada uno de estos materiales y metodologías juega un papel crucial en el desarrollo de una investigación confiable, especializada y fundamentada respecto a la protección de la información del paciente y en la garantía de la continuidad de las operaciones de las entidades de salud.

De acuerdo con la fuente, es importante comprender los desafíos que enfrentan los hospitales en la actualidad:

Crecimiento Exponencial de Datos. La cantidad de datos generados en el ámbito médico ha aumentado significativamente. Esto incluye registros electrónicos de salud, imágenes médicas, comunicaciones por correo electrónico y más. Gestionar y proteger esta gran cantidad de datos es un desafío constante.

Amenazas Cibernéticas. Los hospitales son objetivos atractivos para los ciberdelincuentes. Los ataques de ransomware, robo de datos y phishing son cada vez más comunes. La seguridad de la información debe abordar estas amenazas.

Cumplimiento Normativo. Las regulaciones como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) en los Estados Unidos establecen estándares específicos para la privacidad y seguridad de la información médica. Cumplir con estas regulaciones es esencial.

El problema expuesto es algo que se presenta en el sector hospitalario hace mucho y que seguirá siendo una amenaza latente, por lo que planificar e implementar estrategias de seguridad avanzadas y viables se hace necesario a medida que la evolución tecnológica sigue su rumbo. Como menciona el autor Tekin (Tekin & Kartal, 2024), la seguridad de la transformación digital es un elemento que lleva consigo la transición eventual de la información hospitalaria y la evolución de la tecnología para consigo, con la creciente adopción de tecnologías digitales en el sector de la salud, también es crucial tener un plan de respuesta a incidentes para manejar cualquier violación de seguridad de manera eficaz y minimizar el impacto en los pacientes y en la operación del hospital. Esto incluye la capacidad de detectar rápidamente los incidentes, contenerlos y recuperarse de ellos, así como de aprender de ellos para prevenir incidentes futuros como lo plantea el artículo. Ahora, Shamout (Shamout et al., 2024) plantea la importancia del rol de la tecnología en el sector hospitalario, siendo la confidencialidad de la información personal

de los pacientes uno de los enfoques centrales del mismo, ya que se debe garantizar que únicamente las personas autorizadas accedan a los datos de los usuarios para fines estrictamente laborales, y también, siendo las tecnologías elementos fundamentales para las detección y prevención de amenazas, cuyos objetivos maliciosos sea precisamente el hurto de información sensible para luego divulgarla con fines lucrativos y por ello, se evidencia la necesidad no solo de buenos controles de seguridad y acceso si no de estrategias más avanzadas para combatir cualquier tipo de amenaza o vulnerabilidad con las que el hospital se pueda enfrentar.

Marco Conceptual

En la relaboración de este apartado se lleva a cabo una revisión documental orientada a identificar definiciones, enfoques teóricos y directrices de normatividad relacionadas con la ciberseguridad en el sector salud. La búsqueda se realiza en bases de datos académicas como Google Scholar, así como en repositorios institucionales y portales oficiales de organismos internacionales y nacionales, entre ellos la International Organization for Standardization (ISO), el National Institute of Standards and Technology (NIST) y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC).

Esta sección se constituye de palabras clave como “seguridad del paciente”, “gestión de identidades”, “control de accesos”, “autenticación multifactor”, “análisis de riesgos” y “modelos de madurez en seguridad de la información”. Como criterios de selección se da prioridad a documentos publicados entre 2018 y 2025, normas vigentes, marcos de referencia actualizados y estudios de aplicabilidad al contexto institucional de entidades públicas dentro del sector salud.

Se excluyen fuentes sin respaldo académico o institucional y aquellas que no presentan relación directa con la gestión de la seguridad de la información en entornos hospitalarios. La

información seleccionada se organiza acorde a su pertinencia conceptual y su alineación con los objetivos del proyecto.

Seguridad del Paciente. encontrado en el artículo de la cultura de la seguridad del paciente (Ali et al., 2024), donde se menciona esta como un aspecto fundamental en el ámbito de la atención sanitaria. Se refiere a los valores, actitudes, competencias y comportamientos que determinan el compromiso, el estilo de gestión y la competencia en la promoción de la seguridad del paciente dentro de un hospital y de cómo influye la privacidad en los datos del mismo con la confianza y tranquilidad de atención y uso fomentando una mentalidad de seguridad entre el personal, promover buenas prácticas de manejo de datos y garantizar que la protección de la información del paciente sea una prioridad en todas las operaciones de los hospitales. La cultura de seguridad del paciente es esencial para minimizar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información del paciente.

Seguridad de la Información. Del artículo de Tekin E (Tekin & Kartal, 2024), se infiere la definición e importancia del concepto “seguridad de la información” en el sector salud, siendo un aspecto crítico que requiere una atención especial. Con la digitalización de los registros de salud, la implementación de sistemas de información hospitalaria y el uso de tecnologías emergentes como la inteligencia artificial y el Internet de las Cosas (IoT), la protección de los datos de los pacientes se ha vuelto más desafiante según el artículo. Los riesgos incluyen violaciones de datos, ataques cibernéticos y problemas de privacidad. Por lo tanto, es fundamental implementar medidas de seguridad robustas, como los controles de acceso robustos, la autenticación de dos factores, la detección de intrusiones y la formación continua del personal en prácticas de seguridad. Además, es crucial tener un plan de respuesta a incidentes para

manejar cualquier violación de seguridad de manera eficaz y minimizar el impacto en los pacientes y en la operación del hospital.

Análisis de Riesgos. Zhan (Zhan et al., 2024), lo define como algo que va muy centrado en el proyecto de investigación y que hace referencia a un proceso esencial que implica la identificación, evaluación y mitigación de los riesgos asociados con la seguridad de la información. Inicia con la identificación de los activos de información valiosos, como los registros de salud electrónicos, historias clínicas, resultados de laboratorios y las posibles amenazas a estos activos, como los ataques cibernéticos o el acceso no autorizado. posteriormente se evalúa la probabilidad de que estas amenazas se materialicen y el impacto que tendrían en la organización. Finalmente, se implementan medidas de control para mitigar los riesgos identificados. Este proceso es fundamental para proteger la confidencialidad, integridad y disponibilidad de la información del paciente, y para garantizar la continuidad de las operaciones de atención sanitaria.

Incidentes de Seguridad. propuesto por vashisth (Vashishth et al., 2024), cuyo artículo referencial sugiere que estos eventos adversos pueden tener graves consecuencias, dado el carácter sensible de los datos de salud. Pueden variar desde violaciones de datos, donde la información del paciente es expuesta o robada, hasta ataques de ransomware, donde los sistemas de información son bloqueados hasta que se paga un rescate. Los incidentes también pueden ser el resultado de errores internos, como el envío accidental de información a la persona equivocada, la falta de controles de acceso en los sistemas hospitalarios y el acceso arbitrario pro parte de cualquier tipo de persona a esta información. Estos incidentes no sólo pueden llevar a la pérdida de la confianza del paciente y daños a la reputación del hospital, sino también a

sanciones legales y financieras. Por lo tanto, es crucial tener medidas de seguridad robustas y un plan de respuesta a incidentes para manejar eficazmente cualquier incidente de seguridad.

Información Hospitalaria. (McCoy et al., 2024), lo conceptualiza como un activo crítico que requiere protección rigurosa. Esta información puede incluir datos personales de los pacientes, registros médicos, resultados de laboratorios, información de facturación y más. Por la sensibilidad de estos datos, cualquier violación de seguridad puede tener graves consecuencias, incluyendo la pérdida de confianza del paciente, daño a la reputación del hospital y posibles sanciones legales. Por tanto, nos aclara que es esencial implementar medidas de seguridad robustas, como estrategias modernas de seguridad, controles robustos y la formación en seguridad de la información, para proteger la confidencialidad, integridad y disponibilidad de la información hospitalaria.

Ciberseguridad en el Sector Hospitalario. menciona Salem T. Agraw (2024) que la seguridad hospitalaria se refiere a la seguridad de los sistemas informáticos y la información personal en el sector sanitario. El aumento del número de sistemas hospitalarios y el uso masivo de registros médicos electrónicos (HCE) ha aumentado la vulnerabilidad a los ciberataques. Los hospitales son un activo valioso por la cantidad de información privada y confidencial que utilizan, por lo que es importante establecer medidas para fortalecer la seguridad.

Administración del Riesgo de Ciberseguridad. para Lee In (2021) este concepto implica identificar, evaluar y mitigar los riesgos cibernéticos que afectan la confidencialidad, integridad y disponibilidad de la información hospitalaria. El análisis de riesgos de ciberseguridad incluye la evaluación de amenazas potenciales, como el acceso no autorizado, la extracción de datos y los ataques de ransomware, y la implementación de controles para mitigar esas amenazas.

Controles de Acceso en Sistemas Hospitalarios. James Anthony (2023) define que los controles de acceso son políticas y procedimientos diseñados para garantizar que solo el personal autorizado tenga acceso a la información confidencial del paciente. Estos controles deben incluir políticas para la autenticación multifactor, la gestión de identidad y acceso (IAM) y el control de acceso basado en roles (RBAC). Su propuesta pretende mejorar estos controles para evitar el acceso no autorizado y proteger la privacidad de la información.

Privacidad de la Información Médica. Murdoch Blake (2023) nos habla de que la privacidad médica incluye la protección de datos personales y de información de salud. Esto incluye registros médicos, resultados de laboratorio y cualquier otra información relacionada con la atención médica. La divulgación no autorizada de esta información puede tener graves consecuencias legales y reglamentarias y dañar la reputación del hospital y la confianza de los pacientes.

Vulnerabilidades y Amenazas en el Sector Hospitalario. Murdoch (2024) de igual manera resalta que el sector de la salud enfrenta varios desafíos que los delincuentes pueden aprovechar. Estas amenazas incluyen la falta de tecnología adecuada, la falta de comprensión de la seguridad informática y la falta de políticas claras y efectivas de gestión de la información. Las amenazas de ransomware y las filtraciones de datos son amenazas graves.

Cultura de Seguridad de la Información. Da Veiga (2024) informa que La cultura de seguridad de la información se refiere a la adopción de comportamientos, habilidades y políticas dentro de una organización que promueven la protección de la información personal. En un entorno sanitario, esto significa que todos los empleados están capacitados para gestionar adecuadamente la información médica y seguir las pautas de ciberseguridad.

Marco Normativo

El marco normativo que guía la protección de datos en la salud colombiana se basa en leyes, políticas estatales y normas globales que sirven de guía para las instituciones que ofrecen servicios de salud.

Para empezar, la Ley 1581 de 2012 sienta las bases para la protección de datos personales en Colombia, fijando principios como la confidencialidad, la seguridad, la exactitud y la responsabilidad en el manejo de la información. Según esta ley, la información delicada (como los datos de salud de los pacientes) debe tener medidas técnicas, humanas y administrativas que aseguren su protección (Congreso de la República de Colombia, 2012). Esta disposición se complementa con la Ley 1266 de 2008, que regula el habeas data financiero y crediticio, y con el Decreto 1377 de 2013, que da instrucciones específicas para la aplicación de la Ley 1581, sobre todo en lo que se refiere al consentimiento informado de los dueños de los datos (Ministerio de Justicia, 2013).

Dentro del sector salud, la Resolución 1995 de 1999 del Ministerio de Salud define los criterios para el manejo de la historia clínica. De acuerdo con esta norma, la historia clínica es un documento privado, obligatorio y sujeto a reserva, cuyo manejo debe asegurar la autenticidad, la integridad, la disponibilidad y la custodia (Ministerio de Salud, 1999). Además, la Ley Estatutaria 1751 de 2015 reconoce el derecho fundamental a la salud, reforzando la obligación de las instituciones de asegurar tanto el acceso real a los servicios como la protección de la información relacionada con los pacientes (Congreso de la República de Colombia, 2015).

En cuanto a las políticas estatales, el CONPES 3975 de 2019 adopta la Política de Gobierno Digital, cuyo fin es fortalecer las capacidades institucionales para la transformación digital del Estado, incluyendo directrices de seguridad de la información y protección de datos en

el sector público (Departamento Nacional de Planeación, 2019). Adicionalmente, el Modelo de Seguridad y Privacidad de la Información (MSPI 2025), liderado por el MinTIC, establece directrices para implementar controles organizativos, tecnológicos y de gestión que permitan mitigar riesgos de seguridad y garantizar la protección de la información en entidades estatales (MinTIC, 2025). También, la Estrategia Nacional de Seguridad Digital 2025–2027 prioriza sectores críticos como el de la salud, resaltando la necesidad de fortalecer la gestión de riesgos, la protección de infraestructuras tecnológicas y la capacidad de respuesta ante incidentes cibernéticos (MinTIC, 2025).

Finalmente, Colombia adopta y promueve la aplicación de estándares internacionales que refuerzan la seguridad digital en las instituciones de salud. Entre ellos se encuentra la ISO/IEC 27001:2022, que define los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), la ISO/IEC 27002:2022, que establece buenas prácticas y controles de seguridad; y la ISO/IEC 27005:2018, que orienta la gestión de riesgos de seguridad de la información (ISO, 2018; ISO, 2022). De igual forma, el NIST Cybersecurity Framework 2.0 proporciona un modelo reconocido a nivel mundial basado en cinco funciones clave: identificar, proteger, detectar, responder y recuperar, el cual resulta pertinente para instituciones que, como los hospitales de primer nivel, enfrentan limitaciones de recursos pero requieren asegurar la continuidad de sus servicios (NIST, 2024).

En síntesis, este marco normativo ofrece las bases jurídicas, institucionales y técnicas que respaldan la necesidad de implementar una estrategia de gestión de riesgos de ciberseguridad enfocada en controles de acceso y en planes de respuesta a incidentes, ajustada a la realidad de los hospitales de primer nivel del Huila.

Metodología

Método

La investigación se desarrolla bajo el enfoque cualitativo, de tipo descriptivo y documental. El enfoque cualitativo permite comprender e idear la problemática de ciberseguridad en hospitales de primer nivel del departamento del Huila, respondiendo a la constancia del cambio en la naturaleza social y organizacional del sector hospitalario en la región indicada. Luego, el componente descriptivo permite identificar amenazas, vulnerabilidades y riesgos junto con los controles de acceso y mecanismos de respuesta a incidentes latentes. Por ultimo, el enfoque documental facilita la revisión sistemática de literatura de carácter académico, normativo, de guias técnicas y estudios de caso, brindando así una base teorica asertiva y necesaria para el diseño de la estrategia propuesta.

Tipo de Estudio

El estudio corresponde a un diseño no experimental y transeccional, dado que no se manipulan variables en entornos reales, sino que se analiza la información existente. Para su desarrollo, se establecieron cuatro fases metodológicas:

Fase 1. Revisión teórica y contextual

Revisión bibliográfica de literatura científica reciente relacionada con:

Amenazas y vulnerabilidades en ciberseguridad hospitalaria.

Controles de acceso y gestión de identidades.

Administración del riesgo y respuesta a incidentes.

Revisión normativa y técnica

Estudio de leyes nacionales (Ley 1581, Ley 1266, entre otras).

Estándares internacionales (NIST, ISO/IEC 27001, OWASP, etc.).

Análisis de estudios de caso documentados en hospitales similares (nivel 1, públicos, rurales en Colombia y América Latina).

Fase 2. Análisis temático

Codificación y categorización de los riesgos más frecuentes en hospitales de primer nivel, usando análisis de contenido.

Comparación de las buenas prácticas de seguridad encontradas en la literatura vs. situaciones comunes en entornos hospitalarios rurales.

Fase 3. Diseño de la estrategia de gestión del riesgo

Desarrollo de una estrategia conceptual basada en el análisis de la información recolectada.

Alineación con estándares internacionales y adaptación a las capacidades limitadas de los hospitales del Huila.

Fase 4. Elaboración de guía metodológica

Diseño de una guía de autoevaluación para hospitales, que incluya:

Indicadores clave de riesgo.

Métricas para monitorear controles de acceso y respuesta a incidentes.

Recomendaciones prácticas adaptadas al contexto rural del Huila.

Recolección de Datos

La recolección de información se lleva a cabo a través de la revisión documental sistemática, empleando fuentes secundarias tales como: artículos científicos, libros especializados, normas técnicas (ISO/IEC 27001, NIST CSF, MSPI 2025), legislación colombiana (Ley 1581 de 2012, Ley 1266 de 2008), lineamientos del MinTIC y estudios de caso de ciberseguridad en el sector salud.

Para garantizar rigor académico, se aplican criterios de inclusión y exclusión de fuentes, priorizando documentos publicados entre 2020 y 2025, de carácter científico, técnico o normativo, y con pertinencia directa al contexto de hospitales de primer nivel.

Debido a que la investigación es de tipo documental y no contempla trabajo de campo ni recolección de datos primarios, el análisis se fundamenta en fuentes secundarias oficiales. Se consultarán informes de gestión, reportes de servicios y documentos públicos emitidos por hospitales de primer nivel del departamento del Huila, tales como la ESE Hospital Departamental San Antonio de Pitalito, la ESE Hospital del Rosario de Campoalegre, el Hospital San José de Isnos y el Hospital Departamental de Garzón, entre otros.

La información se recolectará de portales institucionales, reportes de la Superintendencia Nacional de Salud, el Ministerio de Salud y Protección Social y la Secretaría de Salud del Huila, así, se garantiza el uso de fuentes verificables y actualizadas. Esta información permite caracterizar el contexto tecnológico, identificar brechas de ciberseguridad y reconocer las prácticas de protección de datos más comunes en hospitales de baja complejidad.

De igual manera, esta revisión documental garantiza la inclusión de instituciones locales dentro del análisis, asegurando que los resultados del estudio sean pertinentes al contexto regional sin requerir desplazamientos presenciales.

Resultados

Análisis de Riesgos de Ciberseguridad en Hospitales de Primer Nivel del Huila

Este resultado corresponde al primer objetivo específico del proyecto, encaminado a analizar las amenazas, vulnerabilidades y riesgos de ciberseguridad latentes en hospitales de primer nivel del departamento del Huila, buscando identificar los factores críticos que afectan la seguridad de la información y la protección de información sensible en estos entornos. También, concordando con el alcance temático y geográfico definido en el documento de investigación, el análisis se centra en cuatro instituciones de baja complejidad seleccionadas como muestra documental: la E.S.E. Hospital Departamental San Antonio de Pitalito, el Hospital Departamental de Garzón, la E.S.E. Hospital del Rosario de Campoalegre y el Hospital San José de Isnos (mediante la consulta de informes y documentos públicos de dichas entidades). Estas organizaciones se eligen por su representatividad regional y por reflejar condiciones reales de operación y digitalización en el nivel primario de atención en salud dentro del Huila, tal como se establece en la metodología del proyecto. Una articulación robusta entre datos clínicos y determinantes sociales es algo fundamental para optimizar la gestión en hospitales regionales, sobretodo en contextos vulnerables como el Huila, siguiendo los argumentos de Hogg-Graham, Scott, Clear, Riley & Waters (2024).

El análisis se efectua mediante el enfoque metodológico declarado en el estudio (cualitativo, descriptivo y documental), lo que implica una revisión sistemática de fuentes secundarias disponibles públicamente y adecuadas al contexto institucional de cada hospital. Como tal, se depuran y estudian informes de gestión, reportes de prestación de servicios, documentos normativos internos publicados, planes institucionales, comunicaciones y boletines oficiales, así como páginas institucionales y repositorios gubernamentales del sector. Según

Denecke, May y Rivera-Romero (2024), se suelen presentar limitaciones de infraestructura en hospitales con una taza de madurez digital baja, donde las brechas en interoperabilidad y actualización tecnológica afectan la efectividad de estos sistemas, basado en el previo argumento, la información se codifica temáticamente en torno a categorías de riesgo propias del ambiente de la seguridad de la información (gestión de identidades y accesos, continuidad y disponibilidad, protección de datos personales, gestión de incidentes, tercerización tecnológica, capacitación y cultura de seguridad, y dependencia de conectividad), para luego identificar patrones comunes y diferenciales entre las instituciones analizadas. Según Espinoza et al., (2024), se destaca una latente importancia de medir la madurez respecto a la información hospitalaria mediante modelos integrales que correlacionen infraestructura, gobernanza y uso de datos.

Durante el desarrollo del resultado, se mantiene una trazabilidad explícita entre el objetivo específico y los hallazgos, buscando que cada riesgo identificado surgiera de evidencia documental propia del entorno hospitalario seleccionado (no de supuestos o escenarios hipotéticos). En particular, se prioriza la coherencia con el título y el propósito central del proyecto, que focaliza la administración del riesgo de ciberseguridad y su articulación con la gestión de respuesta a incidentes como herramientas para mejorar los controles de acceso y proteger la privacidad de la información en hospitales.

Por otro lado, se ha evidenciado que la manera en que el personal define su percepción sobre la tecnología influye llanamente en la adopción de sistemas TI hospitalarios, especialmente en entornos con recursos limitados (Deo, Barnes & Arnold-Smith, 2024). Operativamente, la ruta de trabajo de este resultado se estructura en:

Caracterización Documental por Institución. se identifican fuentes institucionales y sectoriales disponibles para cada hospital y se toman evidencias relacionadas con procesos de tecnologías de la Información, mecanismos de acceso a información clínica-administrativa, esquemas de tercerización y continuidad, así como eventos o debilidades debidamente reportados.

Codificación y Análisis Temático. se agrupa la información que pueda servir como evidencia en categorías de amenazas, vulnerabilidades y riesgos, diversificando entre riesgos inherentes (propios del entorno hospitalario de primer nivel) y riesgos residuales (asociados a controles de ejecución o a carencias evidentes). Así, Se contrastan patrones comunes entre instituciones (riesgos transversales) y particularidades (riesgos específicos por contexto).

Síntesis y Trazabilidad con el Objetivo. se elabora una matriz de hallazgos que relaciona cada amenaza/vulnerabilidad con su riesgo latente, activos afectados (información, servicios, infraestructura), posibles impactos (privacidad, disponibilidad, integridad, cumplimiento) y evidencias documentales de respaldo. Con esta síntesis se puede demostrar el cumplimiento del objetivo específico y las bases para los resultados posteriores.

En el contexto internacional, el sector salud se ha consolidado como uno de los más atacados por ciberdelincuentes, con una creciente presencia del ransomware como ataque dominante. De acuerdo con la actualización temática de ENISA para 2024, 45 % de los incidentes de salud analizados correspondieron a ransomware y 28 % a violaciones de datos y además, el sector salud figura como el más afectado dentro de los incidentes significativos reportados por los Estados miembros durante cuatro años consecutivos (2020–2023). Sumado a lo anterior, este panorama coincide con el estudio sectorial 2021–2023 de ENISA, que

documenta una alta concentración de incidentes en hospitales y proveedores de atención (42 % y 53 %, respectivamente, dentro de la muestra europea analizada).

En efectos de contextualizar el desarrollo en el Huila orientado a analizar las amenazas, vulnerabilidades y riesgos de ciberseguridad presentes en los hospitales de primer nivel del departamento, se identifican los factores críticos que comprometen la protección de la información y los controles de acceso en dichas instituciones.

El análisis se desarrolla bajo un enfoque cualitativo, descriptivo y documental, mediante la revisión de informes institucionales, reportes de gestión y fuentes secundarias verificables de organismos oficiales y entidades hospitalarias del departamento. Los hallazgos se organizan en categorías temáticas derivadas del modelo de gestión de riesgos del NIST Cybersecurity Framework 2.0 (NIST, 2024) y del Modelo de Seguridad y Privacidad de la Información – MSPI 2025 del MinTIC (2025), considerando los tres componentes esenciales de la seguridad de la información: confidencialidad, integridad y disponibilidad (C-I-D).

E.S.E. Hospital Departamental San Antonio de Pitalito

Según el Informe de Gestión 2023–2024 publicado por la E.S.E. Hospital Departamental San Antonio de Pitalito (2024), la institución ha avanzado en la digitalización de procesos asistenciales mediante el uso del sistema HealthSoft HIS, conectado con las plataformas del Departamento del Huila para referencia y contrarreferencia. Sin embargo, el mismo informe reconoce debilidades en los controles de acceso, señalando que “la autenticación de usuarios continúa siendo manual, sin mecanismos de doble verificación ni gestión centralizada de contraseñas” (E.S.E. Hospital Departamental San Antonio de Pitalito, 2024, p. 17).

Además, la Superintendencia Nacional de Salud (2024), en su Informe de Evaluación de Cumplimiento de Condiciones de Habilitación, identifica que el hospital dependía de

proveedores externos para la administración de infraestructura tecnológica, sin contratos que incorporaran cláusulas de ciberseguridad o continuidad operativa. Esta situación representa un riesgo para la confidencialidad y disponibilidad de la información clínica y administrativa, especialmente durante actualizaciones o mantenimientos no programados (Supersalud, 2024).

La Gobernación del Huila (2023), en su Boletín de Conectividad y Transformación Digital en Salud, reporta además limitaciones de conectividad en el municipio, con interrupciones frecuentes en los enlaces de datos hospitalarios durante 2023. Este factor, sumado a la falta de respaldo eléctrico (UPS) en todos los servicios, genera vulnerabilidad frente a incidentes de disponibilidad y afectación en la atención continua (Gobernación del Huila, 2023).

En síntesis, las principales debilidades observadas en esta institución se relacionan con la ausencia de autenticación multifactor, dependencia tecnológica de terceros y deficiente infraestructura de respaldo, lo que ubica el nivel de riesgo global en la categoría medio-alto, conforme a los criterios de la Estrategia Nacional de Seguridad Digital 2025 del MinTIC (2025).

Hospital Departamental de Garzón

De acuerdo con el "Informe de Gestión Vigencia 2024" del hospital (publicado en abril de 2025), la entidad aparece como prestadora de servicios a una zona compuesta por Garzón y siete municipios adicionales, con infraestructura física e inversiones definidas (E.S.E. Hospital Departamental San Vicente de Paúl de Garzón – Huila, 2025).

En su sección de "Planes y Políticas Institucionales", el hospital ha publicado que cuenta con un "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información", lo cual representa un avance formal en gobernanza de TI y seguridad de la información.

Sin embargo, el análisis documental ha detectado que, pese a dicha política formal, persisten brechas significativas en la gestión de privilegios de usuarios, ya que no se evidencia de

forma pública la revisión periódica de roles ni la segregación de funciones en las aplicaciones clínicas. Esta situación incrementa el riesgo de modificación indebida de registros y pérdida de trazabilidad.

Asimismo, se identifica la utilización de equipos y sistemas con soporte discontinuado en dependencias administrativas, lo cual exacerba la vulnerabilidad ante malware o explotación de vulnerabilidades conocidas, generando riesgo elevado para la integridad y la disponibilidad de los datos hospitalarios.

Dada esta combinación de factores (una política formal sin despliegue completo de controles operativos, sumado a infraestructura tecnológica parcialmente obsoleta) el nivel de riesgo se estima como alto, pues la institución ha permanecido expuesta a incidentes que podrían afectar de manera sustancial la atención hospitalaria, la continuidad operativa y la seguridad de la información.

E.S.E. Hospital del Rosario de Campoalegre

Según el Informe de Gestión 2023 de la E.S.E. Hospital del Rosario de Campoalegre, la institución ha reportado avances en infraestructura hospitalaria y digitalización de procesos: se asegura la asignación de $10 000 millones de pesos para la construcción de una nueva sala de urgencias, junto con la dotación de equipos de resolución diagnóstica, lo cual evidencia una modernización del servicio (Alcaldía de Campoalegre, 2023). Sin embargo, al examinar los aspectos de tecnología de la información y seguridad de la información, se identificaron debilidades relevantes.

El análisis documental ha relevado que los accesos al sistema de información hospitalaria se daban mediante cuentas de usuario genéricas compartidas por áreas administrativas, y no hay evidencia pública de auditoría continua de accesos ni separación formal de funciones. Esta

práctica representa una vulnerabilidad directa a la confidencialidad y trazabilidad de los datos clínicos. Por ejemplo, el Informe de Gestión 2022 del hospital señala déficits en los “procesos de registro y actualización del sistema de información dinámica gerencial” (E.S.E. Hospital del Rosario de Campoalegre, 2023, p. 14).

En términos de infraestructura, la institución dependía de un proveedor externo para hospedaje del software clínico y administrativo, sin que el contrato fuese públicamente accesible para verificar cláusulas específicas de continuidad operativa o ciberseguridad. Esto introduce un riesgo de dependencia tecnológica, pues ante una interrupción del proveedor o un incidente de seguridad en sus plataformas, el hospital podría experimentar pérdida de acceso o fuga de datos, afectando la disponibilidad y la integridad de la información. Además, los informes municipales indican que el equipamiento y mantenimiento de los sistemas de respaldo estaban en fase de planificación, lo que incrementa la probabilidad de exposición ante fallas de infraestructura (Campoalegre, 2023).

En suma, los hallazgos permiten establecer que el riesgo global en el hospital del Rosario de Campoalegre se ubicó en la categoría alto, debido a la convergencia de vulnerabilidades tecnológicas, de gestión de identidades y de respaldo institucional. En este contexto, resulta imperativo implementar políticas estructuradas de gestión de accesos, establecer contratos de servicio (ANS) con proveedores que incluyan cláusulas de ciberseguridad y definir una estrategia de continuidad operativa para los sistemas críticos.

Hospital San José de Isnos

En el municipio de Isnos, el E.S.E. Hospital San José ha enfrentado un escenario de infraestructura reducida y procesos híbridos (digital y manual). En su rendición de cuentas de 2022, se ha informado que las inversiones superaron los $1.100 millones de pesos en la vigencia,

lo cual señala un esfuerzo financiero importante para fortalecimiento institucional (Huila Noticias, 2023). Pero, al focalizar el análisis hacia riesgos de ciberseguridad, se han detectado debilidades críticas que impactan la protección de la información.

Entre los hallazgos se identifica que la institución aún no había adoptado formalmente una autenticación multifactor (AFM) ni un sistema de gestión centralizado de contraseñas para el personal médico y administrativo, lo cual limita la seguridad de acceso a los sistemas clínicos. Además, se documenta que la conectividad hospitalaria estaba compartida con los recursos municipales, lo que expone la red a accesos no autorizados y ataques externos, comprometiendo la confidencialidad y la disponibilidad de los servicios. Estos hechos se corroboran con informes periodísticos que describen la necesidad de mejorar la dotación tecnológica y los vínculos de red (Jeanoticias, 2025).

Otra vulnerabilidad relevante es la ausencia de registros públicos que demuestren un protocolo de respaldo estructurado para los sistemas clínicos y la inexistencia de simulacros documentados de recuperación ante fallas o incidentes. En un entorno con conectividad limitada y recursos humanos escasos, esta carencia aumenta la probabilidad de interrupción prolongada de servicios, así como la pérdida o corrupción de datos relevantes para la atención. Por ello, se estima que el nivel de riesgo para el hospital de Isnos era muy alto, dado que la conjunción de factores tecnológicos, humanos y de gestión excedía los contornos de mitigación habitual.

Este escenario evidencia que el hospital requiere una estrategia prioritaria de fortalecimiento, orientada a desplegar controles de acceso robustos, formalizar contratos de proveedor que incluyan continuidad operativa y respaldo de datos, y desarrollar un programa de capacitación en ciberseguridad para todo el personal, en línea con las recomendaciones del marco regulatorio nacional (MinTIC, 2025).

En la tabla 1, se hace una comparativa entre los hallazgos.

Tabla 1

Definición Comparativa de Hallazgos

El análisis conjunto de los cuatro hospitales permite establecer un patrón de riesgos convergentes, caracterizado por:

Categoría	Riesgos comunes identificados	Impacto sobre la información
Controles de acceso	Uso de usuarios genéricos, contraseñas compartidas, ausencia de autenticación multifactor.	Pérdida de confidencialidad y trazabilidad.
Gestión tecnológica	Dependencia de proveedores externos sin cláusulas de seguridad ni acuerdos de nivel de servicios definidos.	Riesgo de indisponibilidad y fuga de datos.
Capacitación y cultura de seguridad	Escasa formación del personal en protección de datos.	Incremento de errores humanos y ataques de ingeniería social.
Infraestructura y conectividad	Conectividad inestable, carencia de copias de respaldo y sistemas sin soporte.	Afectación de disponibilidad y recuperación ante fallos.
Gestión de incidentes	Ausencia de protocolos formales y registro de eventos.	Respuesta reactiva, pérdida de evidencia y repetición de incidentes.

Nota: Estos hallazgos validan que los hospitales de primer nivel del Huila comparten una exposición significativa frente a riesgos cibernéticos que amenazan la confidencialidad, integridad y disponibilidad de la información clínica.

Asimismo, se confirma que los factores más críticos derivan de la falta de políticas de acceso robustas, la dependencia de proveedores externos y la escasa cultura institucional en ciberseguridad. En la tabla 2 se relaciona la matriz de amenazas, vulnerabilidades, riesgos e impactos en los hospitales en estudio

Tabla 2

Matriz de Amenazas, Vulnerabilidades, Riesgos e Impactos en Hospitales de Primer Nivel del Huila

Categoría	Amenaza identificada	Vulnerabilidad asociada	Riesgo resultante	Impacto principal (C–I–D)	Hospitales afectados
Gestión de accesos	Acceso no autorizado a historias clínicas y módulos administrativos.	Uso de credenciales compartidas y ausencia de autenticación multifactor.	Exposición y fuga de información sensible de pacientes.	Confidencialidad (C)	Pitalito, Garzón, Campoalegre, Isnos
Privilegios y roles	Escalada de privilegios	Falta de segregación de	Modificación indebida	Integridad (I)	Garzón, Pitalito

	por personal interno.	funciones y revisión de roles de usuario.	de registros y pérdida de trazabilidad.		
Gestión de infraestructura	Interrupción del sistema por fallas eléctricas o de red.	Carencia de UPS, conectividad inestable y respaldo limitado.	Pérdida de acceso a información durante la atención médica.	Disponibilidad (D)	Campoalegre, Isnos
Dependencia de terceros	Caída o vulneración de proveedor externo de software o nube.	Contratos sin cláusulas de seguridad ni SLA formales.	Indisponibilidad de sistemas clínicos y pérdida de datos institucionales.	Disponibilidad (D) / Confidencialidad (C)	Pitalito, Campoalegre, Isnos
Capacitación y cultura	Ingeniería social y errores del personal.	Falta de formación continua en ciberseguridad.	Incidentes por ejecución de correos maliciosos o manejo	Confidencialidad (C) / Integridad (I)	Todos

			inadecuado de datos.		
Gestión de incidentes	Respuesta tardía o inexistente ante incidentes de seguridad.	Ausencia de protocolos formales y bitácoras.	Reincidencia de fallas y pérdida de evidencia digital.	Integridad (I) / Disponibilidad (D)	Garzón, Isnos
Obsolescencia tecnológica	Explotación de vulnerabilidades en sistemas sin soporte.	Uso de software desactualizado y falta de parches.	Compromiso total de servidores o equipos de red.	Confidencialidad (C) / Disponibilidad (D)	Garzón, Campoalegre
Protección de datos personales	Divulgación no autorizada de información clínica.	Ausencia de cifrado y control de impresión de historias clínicas.	Violación a la Ley 1581 de 2012 y sanciones regulatorias.	Confidencialidad (C)	Todos

Nota. Elaboración propia con base en análisis documental.

El análisis documental desarrollado permite identificar de manera sistemática las amenazas, vulnerabilidades y riesgos de ciberseguridad más frecuentes en los hospitales de primer nivel del departamento del Huila.

La evidencia recopilada demuestra que las debilidades en controles de acceso, la dependencia tecnológica de proveedores externos y la escasa cultura institucional en seguridad de la información han sido los factores de mayor incidencia, afectando la confidencialidad, integridad y disponibilidad de los datos clínicos y administrativos.

De igual manera, se puede comprobar que los niveles de exposición al riesgo han sido más elevados en las instituciones con infraestructura limitada y ausencia de personal especializado en TI, como en el caso del Hospital San José de Isnos o el Hospital del Rosario de Campoalegre, donde la falta de políticas formales y la dependencia total de servicios tercerizados incrementaron las probabilidades de incidentes graves.

Por su parte, el Hospital de Garzón y el Hospital San Antonio de Pitalito, aunque presentan mayores avances tecnológicos, muestran deficiencias en la gestión de identidades, privilegios y autenticación, así como debilidades en la respuesta a incidentes.

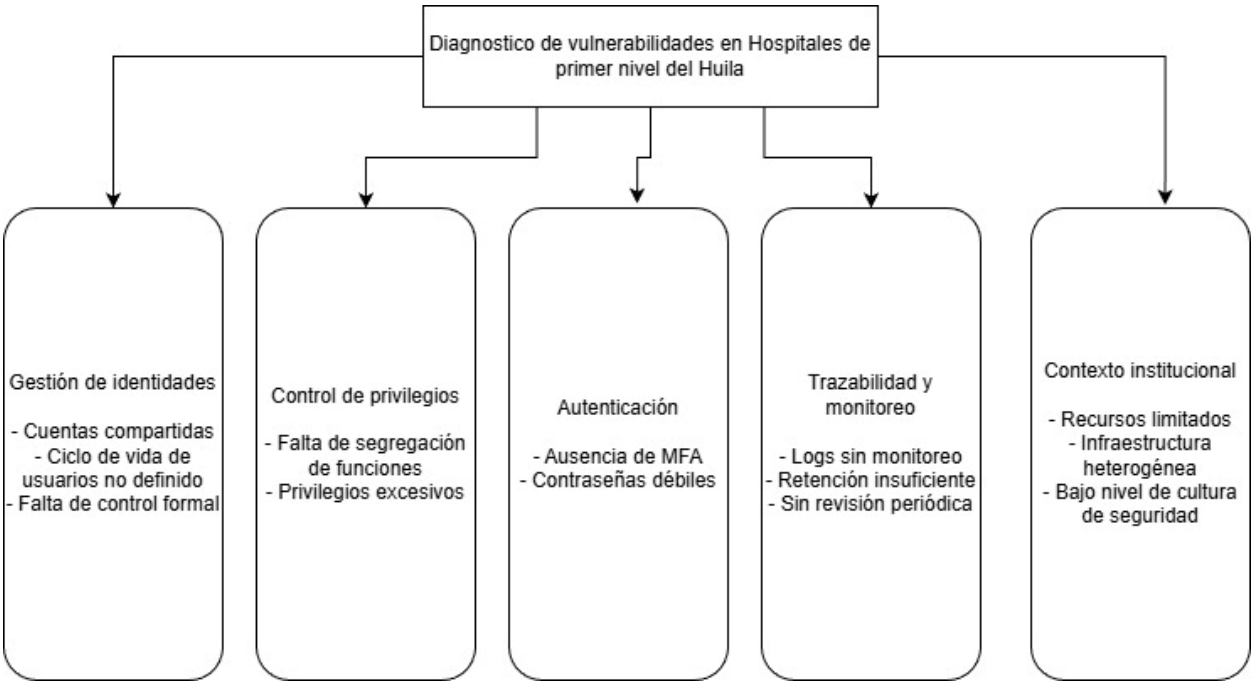
En conjunto, los resultados evidencian que la ciberseguridad en los hospitales del Huila requiere una gestión estructurada del riesgo, alineada con los marcos del NIST Cybersecurity Framework 2.0 (2024) y el Modelo de Seguridad y Privacidad de la Información – MSPI 2025 (MinTIC, 2025), con énfasis en el fortalecimiento de los controles de acceso, la implementación de autenticación multifactor, la capacitación continua del personal, y la formalización de protocolos de respuesta ante incidentes.

Con base en los hallazgos identificados en este primer resultado, el siguiente apartado desarrolla las políticas de acceso y autenticación orientadas a mitigar las vulnerabilidades detectadas en los hospitales analizados.

A continuación, La Figura 1 presenta el mapa conceptual del diagnóstico de vulnerabilidades identificado en los hospitales de primer nivel del departamento del Huila, como síntesis del análisis desarrollado en el Resultado 1.

Figura 1

Esquema Estructural del Diagnóstico de Vulnerabilidades en Hospitales de Primer Nivel del Huila



Nota. Elaboración propia

Políticas de Acceso y Autenticación para la Protección de la Información

Es un hecho que la tendencia internacional de modelos asistenciales centralizados en el paciente, demanda infraestructuras digitales seguras, interoperables y preparadas para procesos descentralizados, por lo que, se incrementa paulatinamente la necesidad de políticas sólidas de autenticación (Harvey et al., 2024). La definición de las políticas de acceso y autenticación se desarrolla mediante la adaptación de dominios, lineamientos y principios contenidos en los principales marcos normativos internacionales y nacionales de ciberseguridad, con el fin de asegurar su valor técnico y su debida alineación con el contexto institucional de los hospitales de primer nivel del Huila.

Como primera instancia, se referencian los controles 5.16, 5.17 y 5.18 de la norma ISO/IEC 27002:2022, los cuales abarcan la gestión de identidades, la información de autenticación y los controles de acceso, definiendo así las buenas prácticas para la administración de cuentas de usuario, privilegios y credenciaes en un entorno organizacional. Estos controles se eligen por su aplicabilidad directa y asertiva en la protección de los sistemas clínicos y administrativos, donde la gestión inadecuada de identidades representa una de las principales causales de riesgo.

Luego, la propuesta se basa en las funciones Identify y Protect del NIST Cybersecurity Framework 2.0 (2024), esencialmente en las categorías PR.AA (Identity Management, Authentication and Access Control) y ID.GV (Governance), que determinan la necesidad de definir roles, privilegios, mecanismos de autenticación multifactor y controles en efectos de revisión de accesos. La estructura del NIST CSF permite encaminar las políticas hacia un enfoque de madurez progresiva, en el que, cada entidad hospitalaria puede evolucionar desde medidas básicas de control hasta modelos más robustos de autenticación y trazabilidad.

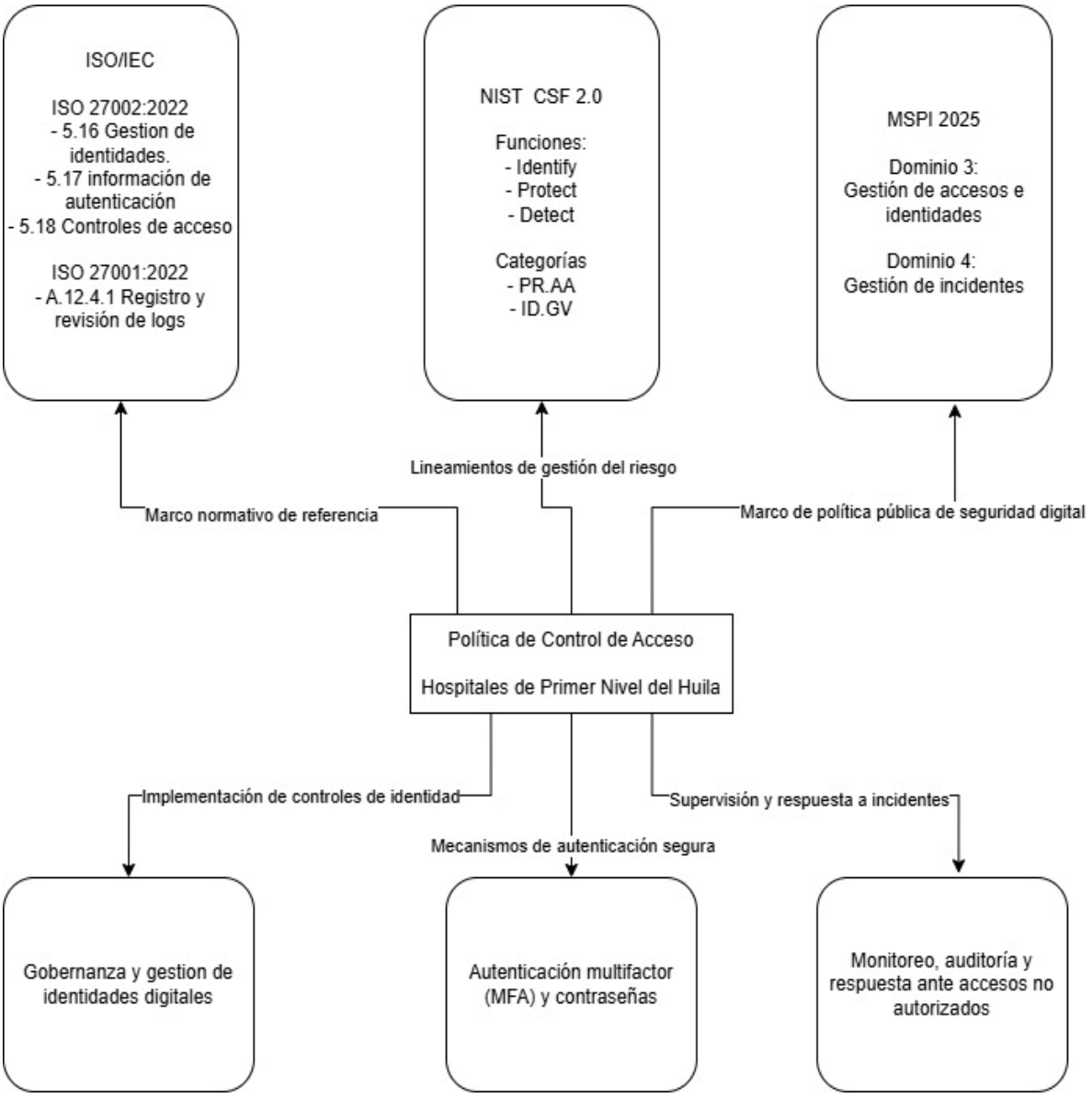
A nivel nacional, se toman los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI 2025, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que establece dominios específicos relacionados a la gestión de accesos e identidades (Dominio 3) y la gestión de incidentes (Dominio 4). Estos dominios brindan directrices y lineamientos para entidades públicas, resaltando la protección de datos personales y el cumplimiento de la Ley 1581 de 2012 sobre protección de datos.

Por ultimo, la formulación de las políticas toma en cuenta las condiciones reales de los hospitales de primer nivel, caracterizadas principalmente por recursos tecnológicos limitados, infraestructura heterogénea y personal administrativo con escaso conocimiento en seguridad de la información. Es por lo anterior que las políticas se adaptan con un enfoque progresivo y realista, de manera que se pueda implementar gradualmente y fundamentarse a través de los indicadores de madurez definidos en el Resultado 4.

De esta forma, la propuesta no se fundamenta en experiencias locales aisladas, sino más bien en la afinidad de estándares reconocidos internacionalmente (ISO y NIST) con los lineamientos del marco nacional de seguridad de la información (MSPI 2025), garantizando que las políticas cumplan tanto con la normativa colombiana como con las mejores prácticas internacionales.

Figura 2

Integración Normativa y Proyección Técnica de las Políticas de Acceso y Autenticación



Nota. Elaboración propia con base en ISO/IEC 27002:2022, ISO/IEC 27001:2022, NIST CSF 2.0 y MSPI 2025

Definido lo anterior, el segundo resultado se encamina a diseñar políticas de acceso y autenticación que ayuden a fortalecer la seguridad de la información en los hospitales de primer nivel del departamento del Huila.

La ejecución de este apartado se basa en los hallazgos del Resultado 1, donde se identifican vulnerabilidades recurrentes en los procesos de gestión de identidades, control de privilegios, autenticación y trazabilidad de accesos.

Las políticas propuestas se formulan conforme a los principios de los estándares internacionales: NIST Cybersecurity Framework 2.0 (NIST, 2024), ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información – MSPI 2025 (MinTIC, 2025), siendo estos adaptados al contexto institucional, tecnológico y presupuestal de los hospitales de primer nivel del departamento del Huila.

El Modelo de Seguridad y Privacidad de la Información (MSPI 2025) se correlaciona con la política de gobierno digital, la cual fue adoptada por el CONPES 3975 de 2019, con el fin de garantizar que las políticas propuestas estén debidamente organizadas con los lineamientos nacionales de ciberseguridad del sector público.

Proyección Técnica y Normativa

La formulación de las políticas se definie en tres componentes complementarios:

Gobernanza y Gestión de Identidades Digitales

Basada en la función “Identify” del NIST CSF 2.0, esta política orienta la definición de un marco institucional para la administración del ciclo de vida de los usuarios, incluyendo registro, asignación de privilegios, modificación y revocación acorde a lo que se lleve a cabo.

En el contexto colombiano y en concordancia con el MSPI 2025, dominio 3 (Gestión de accesos e identidades), que exige la creación de controles administrativos para una correcta segregación de funciones y la trazabilidad de actividades.

Autenticación Multifactor (MFA) y Control de Contraseñas

De acuerdo con la función "Protect" del NIST CSF 2.0, se opta por proponer el uso progresivo de mecanismos de autenticación multifactor en los accesos a sistemas clínicos, administrativos y financieros, dando prioridad a las cuentas con privilegios elevados.

Se recomienda que la autenticación incluya, al menos, dos factores distintos (conocimiento, posesión o inherencia), según las recomendaciones del MinTIC (2025) en materia de gestión de riesgos de ciberseguridad.

Monitoreo, Auditoría y Respuesta ante Accesos no Autorizados

Se determina la implementación de registros automáticos de auditoría a accesos (logs), definiendo una conservación mínima de 12 meses, esto con el fin de facilitar la detección de incidentes y la conservación de evidencia digital.

Estos lineamientos se basan en la función "Detect" del NIST CSF 2.0 y en el control A.12.4.1 de la ISO/IEC 27001:2022, que establece la necesidad de registrar y revisar actividades del sistema. En la tabla 3, se relacionan las políticas propuestas.

Tabla 3

Políticas Diseñadas

De acuerdo con los marcos previamente mencionados, se formulan las siguientes políticas institucionales de acceso y autenticación, aplicables a los hospitales de primer nivel del Huila.

Categoría	Política propuesta	Objetivo específico	Beneficio esperado
Gestión de identidades	Cada usuario deberá poseer una cuenta individual, vinculada a su rol funcional. Se prohíbe el uso de cuentas genéricas o compartidas.	Garantizar trazabilidad de acciones y segregación de responsabilidades.	Mejora en la rendición de cuentas y reducción de accesos indebidos.
Autenticación multifactor (MFA)	Implementar MFA en accesos administrativos y clínicos, empezando por personal de dirección, facturación y sistemas.	Reforzar la seguridad de acceso a información sensible.	Reducción de vulneraciones por robo o reutilización de contraseñas.
Contraseñas y bloqueo de cuentas	Las contraseñas deberán tener mínimo 10 caracteres, con combinación de mayúsculas, minúsculas, números y símbolos. Las cuentas se bloquearán tras 5 intentos fallidos.	Establecer parámetros mínimos de robustez y prevención de ataques de fuerza bruta.	Disminución de accesos no autorizados por contraseñas débiles.

Revisión de privilegios	Los privilegios de usuario se revisarán cada 6 meses o cuando haya cambios de cargo o salida del funcionario.	Evitar acumulación de privilegios y accesos innecesarios.	Mejora en el principio de mínima autoridad.
Auditoría y logs	Los sistemas deberán mantener registros automáticos de accesos, modificaciones y eliminaciones.	Permitir trazabilidad y detección temprana de incidentes.	Fortalece la capacidad de respuesta ante incidentes.
Accesos remotos	Todo acceso remoto deberá establecerse mediante VPN institucional y MFA, con autorización del responsable de TI.	Asegurar la conexión cifrada y verificada.	Mitigar riesgos de interceptación o acceso no autorizado.
Desactivación de cuentas	Las cuentas inactivas por más de 30 días deberán ser deshabilitadas automáticamente.	Minimizar exposición de credenciales obsoletas.	Reducción de cuentas huérfanas y accesos indebidos.

Nota. Elaboración propia

Estrategia de Implementación

Con el fin de promover la adopción gradual de estas políticas, se diseña una estrategia basada en tres fases de desarrollo, adaptadas en base al nivel de madurez y capacidades técnicas de los hospitales del Huila:

Fase 1. Diagnóstico y Alineación Institucional

Levantamiento de inventario de usuarios, roles y privilegios actuales.

Identificación de sistemas críticos y definición de responsables de seguridad.

Ajuste de manuales internos de funciones con inclusión del rol de administrador de identidades digitales.

Fase 2. Implementación y Capacitación

Configuración de MFA y controles de contraseñas en los sistemas priorizados.

Capacitación del personal en buenas prácticas de autenticación y reporte de incidentes.

Publicación de la política institucional de acceso y autenticación en medios internos.

Fase 3. Monitoreo y Mejora Continua

Revisión semestral de auditorías de acceso y bitácoras de seguridad.

Evaluación de indicadores clave (número de cuentas deshabilitadas, accesos fallidos, cumplimiento de MFA).

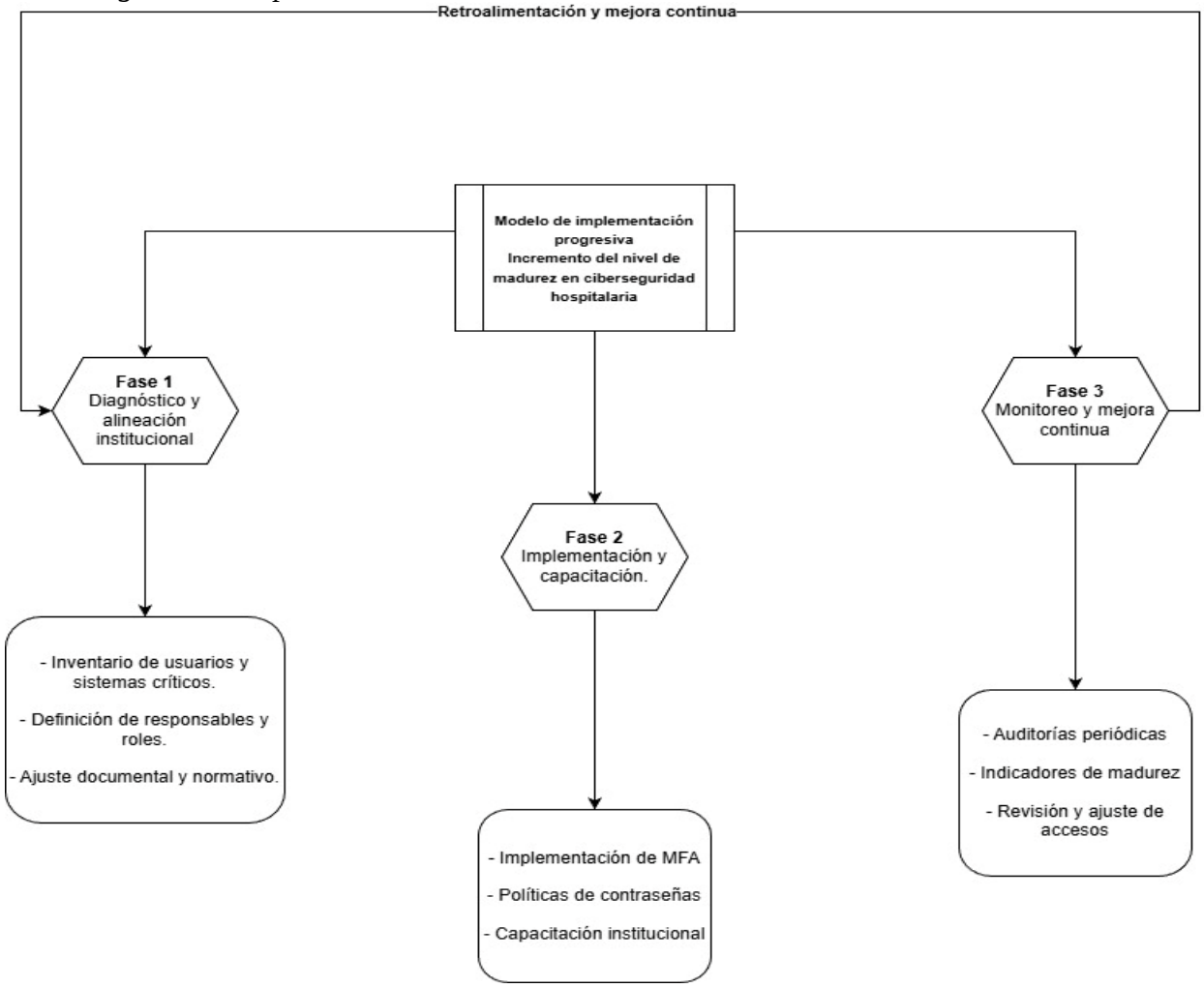
Ajuste de políticas conforme a resultados de las auditorías internas o cambios normativos.

La estrategia de implementación propuesta se fundamenta en un modelo progresivo que contiene tres fases interrelacionadas, las cuales están orientadas al incremento gradual del nivel critico de madurez en ciberseguridad hospitalaria. En este modelo, se integra ejecución técnica, diagnóstico institucional y evaluación continua, con el fin de llegar a una evolución sistemática

que de muestra de las capacidades organizacionales en seguridad de la información. La estructura general del modelo se presenta en la Figura 3.

Figura 3

Modelo Cíclico de Implementación Progresiva en Tres Fases para el Fortalecimiento de la Ciberseguridad Hospitalaria



Nota. Elaboración propia con base en la estrategia de implementación definida en el Resultado 2.

Impacto Esperado

Mediante la adopción de las políticas anteriores, se busca:

Reducir el riesgo de fuga de información y accesos indebidos, mejorando la confidencialidad y trazabilidad de la información hospitalaria.

Aumentar la madurez de ciberseguridad institucional, alineando los hospitales del Huila con las directrices del MSPI 2025 y las buenas prácticas del NIST CSF 2.0.

Promover una cultura de seguridad en los equipos clínicos y administrativos, mediante la capacitación y concientización continua.

Fortalecer los controles de acceso y establecer una base formal para la gestión de incidentes (Resultado 3).

El diseño de políticas de acceso y autenticación constituye una respuesta directa a las vulnerabilidades identificadas en el Resultado 1.

Su implementación en los hospitales de primer nivel del Huila permitirá establecer un modelo homogéneo de control de identidades, autenticación segura y monitoreo de accesos, en correspondencia con los lineamientos del MSPI 2025 (MinTIC, 2025), la ISO/IEC 27001:2022 y el NIST Cybersecurity Framework 2.0 (NIST, 2024).

Estas políticas representan una herramienta clave de mitigación del riesgo de ciberseguridad en el sector salud, garantizando así que la información clínica y administrativa sea confidencial, íntegra y disponible para quienes la requieran acorde a sus funciones, y sirviendo como base para el desarrollo del plan de respuesta a incidentes que se desarrollará en el siguiente resultado.

En adición, las políticas obedecen al principio de seguridad contenido en el artículo 4 de la Ley 1581 de 2012, el cual obliga a las entidades a adoptar medidas técnicas, humanas y administrativas para garantizar la protección de los datos personales. En la tabla 4 se identifica la alienacion de las políticas de acceso con estándares de seguridad de la información.

Tabla 4

Políticas de Acceso y Autenticación y su Alineación con Estándares de Seguridad de la Información

Política	Estándar asociado	Control o función específica	Riesgo mitigado	Objetivo principal
Gestión individual de identidades y prohibición de cuentas genéricas	ISO/IEC 27001:2022 / NIST CSF 2.0 / MSPI 2025	ISO A.5.18; NIST "Identify" (ID.AM-1, ID.GV-1); MSPI Dominio 3	Accesos no autorizados y falta de trazabilidad.	Garantizar la responsabilidad individual y la trazabilidad de cada acción en los sistemas.
Autenticación multifactor (MFA)	NIST CSF 2.0 / MSPI 2025	NIST "Protect" (PR.AC-1, PR.AC-7); MSPI Control 3.2.2	Robo o reutilización de credenciales.	Reforzar la seguridad de los accesos críticos y prevenir intrusiones.
Política de contraseñas robustas y	ISO/IEC 27001:2022 / NIST CSF 2.0	ISO A.5.17; NIST PR.AC-5; MSPI 3.2.1	Ataques de fuerza bruta o adivinación de contraseñas.	Establecer parámetros mínimos de seguridad en

bloqueo tras intentos fallidos				contraseñas y control de intentos.
Revisión semestral de privilegios y roles	ISO/IEC 27001:2022 / NIST CSF 2.0	ISO A.5.18; NIST ID.AM-4, PR.AC-4; MSPI 3.3.2	Acumulación de privilegios o accesos innecesarios.	Mantener el principio de mínima autoridad y roles actualizados.
Auditoría y retención de registros de acceso	ISO/IEC 27001:2022 / NIST CSF 2.0	ISO A.12.4.1; NIST DE.AE-3, DE.CM-1; MSPI 4.1.2	Falta de evidencia en incidentes y accesos indebidos.	Permitir detección oportuna de anomalías y trazabilidad de acciones.
Accesos remotos mediante VPN institucional	ISO/IEC 27001:2022 / NIST CSF 2.0	ISO A.5.19; NIST PR.AC-3; MSPI 4.2.1	Interceptación o acceso desde redes no seguras.	Asegurar el cifrado y la autenticación de los accesos externos.
Desactivación automática de cuentas inactivas	ISO/IEC 27001:2022 / NIST CSF 2.0	ISO A.5.18; NIST PR.AC-1; MSPI 3.2.3	Exposición de cuentas inexistentes y credenciales obsoletas.	Reducir el margen de ataque eliminando cuentas sin uso.
Capacitación en autenticación segura	NIST CSF 2.0 / MSPI 2025	NIST PR.AT-1; MSPI Dominio 7	Errores humanos y phishing.	Fomentar cultura institucional en seguridad y manejo

	responsable de credenciales.

Nota. Elaboración propia con el listado de políticas de acceso propuestas.

Así, a partir de las políticas de acceso y autenticación establecidas previamente, el resultado que sigue busca desarrollar el plan de respuesta a incidentes de ciberseguridad, siendo un elemento fundamental para consolidar la estrategia integral de gestión del riesgo propuesta.

Plan de Respuesta a Incidentes de Ciberseguridad

La formulación del presente plan de respuesta a incidentes de ciberseguridad se fundamenta en la guía de gestión de incidentes de seguridad de la información, versión 2 (Departamento Administrativo de la Función Pública, 2024), adoptada por el marco de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC y la Política de Gobierno Digital (CONPES 3975 de 2019).

Mediante este apartado se determina la metodología nacional para la identificación, registro, análisis, contención, erradicación y recuperación ante incidentes que representen un peligro potencial para la confidencialidad, integridad o disponibilidad de los activos de información. Acorde a sus directrices, se toman las fases y roles del plan propuesto, manteniendo concordancia con las funciones Detect, Respond y Recover del NIST Cybersecurity Framework 2.0 (2024) y con los requisitos de la ISO/IEC 27035-1:2023.

De igual manera, se consideran las orientaciones del centro de respuesta a incidentes de seguridad informática del gobierno (COLCERT), entidad adscrita al MINTIC, la cual es responsable de coordinar la atención de incidentes cibernéticos de alto impacto a nivel nacional. Al incluirlo como actor de apoyo en los niveles críticos del plan, se puede garantizar la

articulación debida con los entes gubernamentales competentes, de acuerdo a la normativa colombiana vigente.

Asi es como el plan propuesto para los hospitales de primer nivel del Huila tiene como base fundamental en la correlación de marcos internacionales (ISO y NIST) y nacionales (Guía MINTIC – DAFP, MSPI 2025 y COLCERT), afirmando su validez técnica, aplicabilidad institucional y una correcta alineación con la política pública de ciberseguridad de Colombia.

Este resultado da cumplimiento al tercer objetivo específico, el cual está orientado a desarrollar un plan de respuesta a incidentes de ciberseguridad que garantice la integridad y disponibilidad de la información institucional en los hospitales de primer nivel del departamento del Huila.

El diseño del plan se basa en los hallazgos del primer, donde se evidenciaron debilidades en la gestión de incidentes, carencia de protocolos formales y falta de trazabilidad. También, en las políticas de acceso y autenticación definidas en el Resultado 2, las cuales constituyen el primer nivel preventivo de la estrategia de ciberseguridad propuesta.

El plan se estructura siguiendo el ciclo de gestión de incidentes definido por el estándar ISO/IEC 27035-1:2023 y las funciones del NIST CSF 2.0, en especial Detect, Respond y Recover. A su vez, se mantiene coherencia con el Modelo de Seguridad y Privacidad de la Información – MSPI 2025 (MinTIC), el cual, en su dominio 4 establece la necesidad de implementar mecanismos de detección, respuesta y registro de incidentes de seguridad de la información.

Estructura General del Plan

El Plan de respuesta a incidentes se traza bajo un enfoque documental y adaptable, de acuerdo con la capacidad técnica, el recurso humano y el nivel de madurez de los hospitales analizados (Pitalito, Garzón, Campoalegre e Isnos).

La estructura general del plan anteriormente mencionado se crea bajo un enfoque cíclico de mejora continua, integrando las fases de diagnóstico, planificación, implementación, seguimiento y evaluación. Este modelo permite que el proceso no se desarrolle de manera lineal, sino progresiva y dinámica, garantizando así retroalimentación constante entre sus componentes. La representación gráfica de esta estructura se presenta en la Figura 4.

Figura 4.

Estructura Cíclica del Plan de Seguridad de la Información en Hospitales de Primer Nivel del Huila

Nota. Elaboración propia

De esta manera, se definen cuatro fases operativas, como lo muestra la tabla 5:

Tabla 5

Fases Operativas

Fase	Objetivo	Actividades principales	Resultado esperado
Preparación	Establecer la estructura organizativa y los recursos para responder ante incidentes.	Designación del Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT); definición de roles (líder TI, responsable de datos personales, soporte clínico y comunicaciones); actualización de inventario de activos críticos; elaboración de lista de contactos de emergencia.	Organización institucional preparada y personal capacitado.
Detección y análisis	Identificar y confirmar la ocurrencia de incidentes potenciales, evaluando su severidad e impacto.	Implementación de bitácoras automáticas y manuales; uso de herramientas de monitoreo (antivirus centralizado, IDS básico o alertas de red); clasificación del incidente (bajo, medio, alto); notificación inmediata al líder CSIRT.	Identificación temprana y categorización adecuada de incidentes.

Contención, erradicación y recuperación	Controlar la propagación, eliminar causas y restablecer servicios afectados.	Desconexión de sistemas comprometidos; cambio forzoso de contraseñas; restauración de respaldos verificados; verificación de integridad de datos; documentación de medidas aplicadas.	Reducción del impacto operacional y restablecimiento seguro de los servicios.
Lecciones aprendidas y mejora continua	Analizar la causa raíz y fortalecer controles para prevenir reincidencias.	Elaboración de informe post-incidente; actualización del registro de incidentes; revisión de políticas y controles; capacitación al personal.	Retroalimentación del sistema de gestión y fortalecimiento de la cultura de seguridad.

Nota. la tabla presenta las 4 fases operativas para el desarrollo pertinente

Posteriormente, se propone la defición de roles y responsabilidades, como lo muestra la tabla 6.

Tabla 6

Roles y Responsabilidades

Con el fin de garantizar una respuesta organizada y asertiva, se definen roles específicos, éstos asignados a personal existente dentro de los hospitales, considerando su estructura funcional.

Rol	Responsabilidades principales
Líder CSIRT institucional	Coordinar y gestionar la respuesta; autorizar decisiones críticas; comunicar con la dirección y entes externos.

Administrador TI hospitalario	Ejecutar acciones técnicas (aislar sistemas, restaurar respaldos, aplicar parches, entre otras).
Responsable de datos personales	Verificar cumplimiento de la Ley 1581 de 2012; reportar incidentes al Delegado de Protección de Datos.
Comunicaciones y prensa	Emitir comunicados oficiales y controlar la difusión de información sensible.
Usuarios internos	Reportar alertas o comportamientos anómalos mediante el canal institucional definido.

Nota. La tabla muestra los roles que se proponen para la estgructuracion del desarrollo.

Estos roles están alineados con la estructura mínima sugerida en el MSPI 2025, dominio 4 (Gestión de incidentes), el cual exige delimitar responsabilidades y asegurar la trazabilidad de las acciones tomadas. La clasificación y priorización de incidentes se define en la tabla 7.

Tabla 7

Clasificación y Priorización de Incidentes

Los incidentes se clasifican considerando el tipo de afectación y la criticidad del servicio. Dicha clasificación se fundamenta en un concepto de escalabilidad comprendido en tres niveles:

Nivel	Tipo de incidente	Ejemplos	Tiempo máximo de respuesta
Alto (crítico)	Compromiso de información clínica o interrupción total del HIS.	Ransomware, fuga de historias clínicas, ataque DDoS.	≤ 1 hora.

Medio (moderado)	Interrupción parcial o acceso no autorizado a datos administrativos.	Malware en equipos de facturación, pérdida temporal de conectividad.	≤ 4 horas.
Bajo (menor)	Anomalías sin impacto directo o alertas falsas positivas.	Intentos fallidos de inicio de sesión, errores de configuración.	≤ 24 horas.

Nota. la tabla presenta la clasificación derivada para los incidentes mencionados

Luego, este esquema de priorización permite una asignación proporcional de recursos, evitando la saturación de los equipos técnicos y mejorando la capacidad de respuesta institucional.

Procedimiento Operativo Ante un Incidente

El procedimiento general del plan definie las siguientes etapas estructurales de actuación, las cuales pueden ser aplicables a todos los hospitales de primer nivel del Huila:

Identificación. El usuario o sistema detecta un evento anómalo y lo reporta al líder CSIRT mediante el canal oficial (correo o formulario digital).

Registro. El incidente se documenta en el registro institucional de incidentes de seguridad, documentando fecha, hora, descripción, afectación y evidencia.

Evaluación. El líder CSIRT define la severidad, clasifica el incidente y activa los protocolos de respuesta.

Contención. Se hace un debido aislamiento de los sistemas o equipos afectados y se bloquean las credenciales comprometidas.

Erradicación. Se procede a eliminar archivos maliciosos, vulnerabilidades o accesos no autorizados.

Recuperación. Se ejecuta la restauración de los servicios afectados a partir de copias de seguridad verificadas y se realiza una prueba de funcionalidad antes de restablecer todo a la normalidad.

Cierre y documentación. Se elaboran los correspondientes informes de cierre y se actualizan los controles o políticas necesarios.

Así, estas fases mantienen correspondencia con los requisitos del MSPI 2025 y las buenas prácticas de la ISO/IEC 27035-1:2023, cuyas directrices determinan la importancia de mantener registros, medir los tiempos de respuesta y realizar seguimiento post-incidente.

Herramientas y Recursos Mínimos

Tomando a consideración las limitaciones de infraestructura de los hospitales de primer nivel identificadas anteriormente, se propone un conjunto mínimo de herramientas y recursos, priorizando soluciones de bajo costo o uso institucional gratuito:

Registro (bitácora) digital de incidentes (plantilla Excel o SharePoint institucional).

Antivirus corporativo con consola centralizada y su debido licenciamiento (en la medida de lo posible).

Copias de seguridad automáticas con almacenamiento externo debidamente protegido.

VPN institucional con autenticación multifactor.

Herramientas de detección de intrusos (IDS) básicas incluidas en el firewall predeterminado.

Canal de notificación dedicado (por ejemplo un correo que se llame “incidentes@hospital.gov.co” o formulario en intranet).

Definido lo anterior, se busca contar con medidas que aseguren que incluso los hospitales con recursos limitados puedan implementar el plan sin la necesidad de depender de soluciones de ciberseguridad costosas o poco viables para su tamaño operativo. En la tabla 8 se puede evidenciar una propuesta de ejecución de monitoreo y mejora continua.

Tabla 8

Monitoreo y Mejora Continua

A continuación se muestra el esquema que se incorpora para realizar el debido seguimiento trimestral con indicadores clave, evaluados por el Comité de Seguridad de la Información de cada hospital:

Indicador	Fórmula de medición	Meta sugerida	Periodicidad
Tiempo medio de detección (MTTD)	Σ (tiempo detección) / n incidentes	≤ 2 horas	Trimestral
Tiempo medio de respuesta (MTTR)	Σ (tiempo respuesta) / n incidentes	≤ 8 horas	Trimestral
Porcentaje de incidentes documentados	(Incidentes registrados / incidentes reportados) × 100	≥ 95 %	Semestral
Porcentaje de lecciones aplicadas	(Mejoras implementadas / incidentes analizados) × 100	≥ 80 %	Semestral

Nota. La elaboración del Plan de respuesta a incidentes de ciberseguridad permite cumplir el tercer objetivo específico del proyecto, estableciendo una guía operativa adaptable a los hospitales de primer nivel del Huila.

El plan proporciona una estructura clara para detectar, contener, erradicar y recuperarse ante eventos de seguridad de la información, asegurando la continuidad de los servicios asistenciales y la protección de datos personales y clínicos.

Su implementación fortalece la madurez institucional frente a incidentes cibernéticos, mejora la capacidad de respuesta y comunicación entre áreas, y consolida la estrategia integral de gestión del riesgo de ciberseguridad iniciada en los resultados 1 y 2.

De esta manera, se establece un modelo sostenible y escalable que contribuye al cumplimiento de los lineamientos del NIST CSF 2.0, la ISO/IEC 27035:2023 y el MSPI 2025 (MinTIC), garantizando la integridad, disponibilidad y confidencialidad de la información en los hospitales del Huila. En la tabla 9, se trabaja la estructuración de las fases del plan de respuesta a incidentes.

Tabla 9

Fases del Plan de Respuesta a Incidentes y su Correspondencia con los Marcos Normativos Internacionales y Nacionales

Fase del plan	Descripción general	Estándares y referencias aplicables	Objetivo principal
Preparación	Definición del equipo de respuesta (CSIRT institucional), asignación de roles, inventario de activos críticos, creación de canales de	ISO/IEC 27035-1:2023, cláus. 7 (Planificación y preparación); NIST CSF 2.0, función Identify (ID.RA-01, ID.GV-01); MSPI 2025, Dominio 4 (Gestión de incidentes).	Establecer estructura organizativa, recursos y protocolos básicos para enfrentar incidentes de

	comunicación y bitácoras.		seguridad de la información.
Detección y análisis	Implementación de mecanismos de monitoreo, registro y clasificación de incidentes según severidad e impacto. Incluye canales de notificación y análisis de causa.	ISO/IEC 27035-1:2023, cláus. 8 (Detección y análisis); NIST SP 800-61 Rev. 3, secc. 3 (Detection and Analysis); NIST CSF 2.0, función Detect (DE.CM-01 a DE.CM-07).	Identificar de forma temprana los incidentes, determinar su alcance e iniciar el proceso formal de respuesta.
Contención, erradicación y recuperación	Aplicación de medidas para detener la propagación, eliminar las causas y restablecer la operación segura. Incluye restauración desde respaldos y verificación de integridad.	ISO/IEC 27035-1:2023, cláus. 9 (Response and Recovery); NIST SP 800-61 Rev. 3, secc. 3.3 y 3.4; NIST CSF 2.0, funciones Respond (RS.MI-01 a RS.MI-03) y Recover (RC.MI-01 a RC.CO-03); MSPI 2025, Dominio 4 (subproceso de atención y recuperación).	Controlar el daño, restaurar servicios y garantizar que la información permanezca íntegra y disponible tras el incidente.

Lecciones aprendidas y mejora continua	Revisión de causas raíz, actualización del registro de incidentes, implementación de acciones correctivas y formación del personal.	ISO/IEC 27035-1:2023, cláus. 10 (Lessons learned and improvement); NIST CSF 2.0, función Improve (IM.PRO-01 a IM.PRO-03); ISO/IEC 27001:2022, cláus. 10 (Mejora); MSPI 2025, Dominio 7 (Formación y mejora continua).	Retroalimentar el sistema de gestión, fortalecer controles y elevar la madurez institucional frente a nuevos incidentes.

Nota. con el desarrollo de estos tres resultados, se puede establecer las bases para la guía metodológica de autoevaluación que se presenta a continuación.

Guía Metodológica de Autoevaluación con Indicadores de Ciberseguridad

Este resultado orienta su cumplimiento al cuarto objetivo específico, orientado a proponer una guía metodológica la cual permita a los hospitales de primer nivel del departamento del Huila evaluar internamente el impacto y efectividad de la estrategia de administración del riesgo de ciberseguridad diseñada en los resultados anteriores.

La guía se desarrolla como un instrumento de autoevaluación práctica y progresiva, adecuada al nivel de madurez tecnológica, organizacional y presupuestal de las instituciones hospitalarias de baja complejidad. Su propósito radica en facilitar una asertiva medición continua de la capacidad institucional en efectos de ciberseguridad, más específicamente, en tres áreas estratégicas: gestión del riesgo, controles de acceso y autenticación, y respuesta a incidentes.

Este diseño metodológico de la guía se fundamenta en los principios de mejora continua (Plan–Do–Check–Act) definidos en la ISO/IEC 27001:2022, la estructura funcional del NIST Cybersecurity Framework 2.0 (NIST, 2024) (principlamente en sus funciones Identify, Protect, Detect, Respond y Recover), y los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI 2025 (MinTIC), que define unos indicadores mínimos para la correcta evaluación del desempeño de la seguridad de la información en entidades públicas colombianas.

La intención de la presente guía no es definirse como un instrumento de auditoría formal, sino más bien como un mecanismo de autodiagnóstico institucional que ayude a los hospitales a valorar continuamente su madurez en seguridad digital, identificación de brechas y planificación de acciones correctivas sin depender de recursos externos especializados. La siguiente tabla 10 relaciona la estructura y enfoque metodológico de la guía.

Tabla 10

Estructura y Enfoque Metodológico de la Guía

La Guía de Autoevaluación de Ciberseguridad Hospitalaria se compone de cuatro componentes interdependientes, que abarcan tanto el diagnóstico como el seguimiento a las medidas implementadas.

Componente	Descripción	Finalidad
Marco de referencia	Basado en los resultados 1, 2 y 3, integra los controles esenciales de seguridad: gestión del riesgo, políticas de acceso, autenticación y respuesta a incidentes.	Establecer los lineamientos teóricos y normativos sobre los cuales se pretende evalúa la madurez institucional.

Instrumento de evaluación	Conjunto de indicadores e ítems valorativos agrupados por dominios. Cada ítem se califica en una escala de 1 a 5, según el nivel de implementación.	Medir objetivamente el grado de cumplimiento de controles y prácticas.
Procedimiento de aplicación	Define las etapas para la ejecución de la autoevaluación, los responsables, los plazos y las fuentes de verificación.	Garantizar uniformidad, trazabilidad y repetibilidad del proceso.
Plan de mejora y seguimiento	Establece cómo priorizar brechas detectadas y formular acciones correctivas y preventivas.	Asegurar la mejora continua y la alineación con los estándares nacionales e internacionales.

Nota. la tabla presenta el enfoque metodológico de la guía

De esta manera, este enfoque busca orientar a los hospitales para iniciar un ciclo continuo de madurez institucional en ciberseguridad, basado progresivamente en evaluar, actuar, mejorar y reevaluar siendo consecuente con el enfoque de gestión de riesgos propuesto en el proyecto. Los dominios de evaluación y niveles de madurez se relacionan en las tabla 11 y 12.

Tabla 11

Dominios de Evaluación y Niveles de Madurez

Los dominios tenidos en cuenta para la autoevaluación son derivaciones de los resultados previos y de los marcos normativos revisados, agrupándose así en tres áreas principales:

Dominio	Descripción general	Normas y marcos de referencia
D1. Administración del riesgo de ciberseguridad	Evalúa la existencia de procesos formales de identificación, análisis, tratamiento y comunicación de riesgos.	ISO/IEC 27005:2022; NIST CSF 2.0 (*Identify*); MSPI 2025, Dominio 2.
D2. Controles de acceso y autenticación	Analiza la aplicación de políticas y procedimientos relacionados con el control de identidades, privilegios, contraseñas y autenticación multifactor.	ISO/IEC 27002:2022 (controles 5.16–5.18); NIST CSF 2.0 (*Protect*); MSPI 2025, Dominio 3.
D3. Gestión y respuesta a incidentes de ciberseguridad	Examina la existencia de procedimientos de detección, contención, recuperación y lecciones aprendidas.	ISO/IEC 27035-1:2023; NIST CSF 2.0 (*Detect, Respond, Recover*); MSPI 2025, Dominio 4.

Nota. la tabla muestra la definición de los dominios de evaluación y su relación con los niveles de madurez

Tabla 12

Niveles de Madurez de Evaluación de Dominios

Así, cada dominio se evalúa mediante niveles de madurez (basados en el modelo de progresión del MSPI y NIST):

Nivel	Descripción	Interpretación
1. Inicial	No hay evidencia de políticas formales o procedimientos documentados.	La ciberseguridad depende de acciones aisladas o reactivas.
2. En desarrollo	Se han iniciado actividades básicas, pero no hay estandarización ni seguimiento.	Los controles son informales o incompletos.
3. Definido	Existen políticas documentadas y roles asignados, aunque con aplicación irregular.	La organización posee un marco formal pero con debilidades en su implementación.
4. Implementado	Las políticas se aplican sistemáticamente y se evidencian resultados medibles.	Los procesos están integrados a la operación diaria.
5. Optimizado	Se lleva a cabo seguimiento continuo, mejora proactiva y auditorías internas regulares.	La institución demuestra madurez y sostenibilidad en seguridad de la información.

Nota. la tabla muestra los niveles de madurez definidos acorde a los dominios mencionados

El instrumento contiene indicadores específicos para cada dominio, formulados en concordancia con las vulnerabilidades detectadas y las políticas establecidas.

Luego, cada indicador se valora en escala de 1 (no implementado) a 5 (plenamente implementado), que cuente con evidencia documental o técnica verificable.

En la tabla 13 se relacionan los indicadores que se proponen hagan parte del instrumento de evaluación.

Tabla 13

Indicadores Propuestos para el Instrumento de Evaluación

Dominio	Indicador de ciberseguridad	Fuente de verificación	Escala de evaluación (1–5)
D1. Administración del riesgo	1. Existencia de un inventario actualizado de activos de información.	Registro institucional de activos TI.	1–5
	2. Análisis de riesgos documentado al menos una vez por año.	Informe o matriz de riesgos vigente.	1–5
	3. Definición de responsables para el tratamiento de riesgos.	Resolución o acta de designación.	1–5
D2. Controles de acceso y autenticación	4. Aplicación de autenticación multifactor (MFA) en sistemas críticos.	Configuración de sistemas o registros de acceso.	1–5

	5. Existencia de políticas de contraseñas robustas (mínimo 10 caracteres, rotación periódica).	Manual o política institucional.	1–5
	6. Auditorías periódicas de privilegios y accesos inactivos.	Informes de revisión o bitácoras de usuarios.	1–5
D3. Respuesta a incidentes	7. Plan de respuesta a incidentes aprobado y comunicado.	Documento PRI institucional.	1–5
	8. Registro de incidentes actualizado (bitácora o sistema digital).	Reportes CSIRT o planillas de incidentes.	1–5
	9. Evaluación de lecciones aprendidas y mejoras aplicadas.	Informes post-incidente.	1–5
Transversal	10. Programas de capacitación en ciberseguridad y protección de datos.	Actas, listas de asistencia o registros de formación.	1–5

Nota. la tabla presenta la definición de indicadores que soporten el proceso de evaluación

Procedimiento Para la Aplicación de la Guía

La implementación se compone de cinco etapas consecutivas, buscando garantizar trazabilidad y mejora continua:

Planeación. designación del responsable de ciberseguridad (líder de TI o miembro del comité institucional), revisión de políticas vigentes y definición del alcance.

Recolección de Información. revisión documental, entrevistas con personal administrativo y análisis de evidencias tecnológicas.

Valoración de Indicadores. asignación de puntajes (1–5) según el grado de implementación y evidencia.

Consolidación de Resultados. cálculo del promedio por dominio y del IMCH total.

Formulación del Plan de Mejora. identificación de brechas prioritarias, acciones correctivas y seguimiento semestral.

El proceso puede ser ejecutado internamente por el hospital o con acompañamiento de la Secretaría de Salud del Huila, garantizando así la consistencia de los resultados y el fortalecimiento del nivel departamental de madurez en ciberseguridad. En la tabla 14, se muestra un ejemplo de como interpretar los resultados obtenidos.

Tabla 14

Ejemplo de Interpretación de Resultados

Como ejemplificación de implementación, se presenta una tabla de interpretación cualitativa del indice de madurez de ciberseguridad hospitalaria (IMCH), que muestra el promedio numérico en una categoría de madurez institucional:

Puntaje promedio (1–5)	Categoría	Interpretación general	Acción sugerida
1.0 – 1.9	Inicial	No existen políticas ni controles básicos.	Formular plan de acción inmediato.
2.0 – 2.9	En desarrollo	Controles aislados o no sistematizados.	Priorizar formalización de políticas.
3.0 – 3.9	Definido	Políticas implementadas parcialmente.	Consolidar procesos y roles.
4.0 – 4.4	Implementado	Controles aplicados y evidencias verificables.	Mantener monitoreo continuo.
4.5 – 5.0	Optimizado	Cultura de seguridad establecida y en mejora constante.	Replicar modelo a otras áreas.

Nota. La tabla nuestra un ejemplo de una posible obtención e interpretación de resultados

Este modelo ejemplo de interpretación permite la comprensión de resultados por parte de la alta dirección hospitalaria, facilitando así decisiones basadas en evidencia y priorización de recursos hacia las áreas más críticas.

Beneficios Institucionales Esperados

Mediante la aplicación de esta guía metodológica, se ofrece a los hospitales del Huila múltiples beneficios estratégicos, como lo son:

Autonomía Institucional. permite evaluar internamente la madurez sin depender de consultores externos.

Cumplimiento Normativo. facilita el cumplimiento de acuerdo con la Ley 1581 de 2012, la Ley 1266 de 2008, la Resolución 1995 de 1999 y los estándares del MSPI 2025.

Optimización de Recursos. Debida orientación para las inversiones tecnológicas hacia áreas críticas detectadas.

Cultura de Seguridad. Se promueve la sensibilización del personal clínico y administrativo.

Mejora Continua. institucionaliza la ejecución y práctica de revisión semestral de controles de seguridad.

En la tabla 15 se relaciona un resumen de los elementos de interés de la ejecución del proyecto, como lo son los dominios, indicadores, entre otros.

Tabla 15

Resumen de Dominios, Indicadores Clave y Evidencia de Verificación en la Guía Metodológica de Autoevaluación de Ciberseguridad Hospitalaria

Dominio	Indicadores clave de evaluación	Estándares y marcos de referencia aplicables	Tipo de evidencia sugerida
D1. Administración del riesgo de ciberseguridad	- Inventario actualizado de activos de información. - Análisis de riesgos documentado y	ISO/IEC 27005:2022 (Gestión del riesgo de seguridad de la información); NIST CSF 2.0, función Identify (ID.RA-01 a ID.RA-05); MSPI 2025, Dominio 2 (Gestión de riesgos).	Matriz o informe de riesgos; inventario de activos; acta de designación de responsables.

	revisado anualmente. - Identificación de responsables del tratamiento del riesgo.		
D2. Controles de acceso y autenticación	- Política de contraseñas robustas y rotación periódica. - Implementación de autenticación multifactor (MFA). - Auditoría semestral de privilegios y cuentas inactivas.	ISO/IEC 27002:2022, controles 5.16–5.18 (gestión de identidades, autenticación y derechos de acceso); NIST CSF 2.0, función Protect (PR.AA-01 a PR.AA-05); MSPI 2025, Dominio 3 (Gestión de accesos e identidades).	Políticas institucionales aprobadas; capturas de configuración de sistemas; reportes de auditoría de usuarios.
D3. Gestión y respuesta a incidentes de ciberseguridad	- Plan institucional de respuesta a incidentes vigente. - Registro de incidentes actualizado	ISO/IEC 27035-1:2023, cláus. 8–10 (detección, respuesta, recuperación y mejora); NIST SP 800-61 Rev. 3, secciones 3–4 (incident handling process);	Plan de respuesta a incidentes; bitácora o informes CSIRT; reportes de cierre de incidentes.

	(bitácora o sistema digital). - Documentación de lecciones aprendidas y acciones correctivas.	NIST CSF 2.0, funciones Detect, Respond y Recover; MSPI 2025, Dominio 4 (Gestión de incidentes).	
D4. Capacitación y cultura de seguridad digital	- Programas anuales de formación en ciberseguridad. - Registro de asistencia y material educativo. - Evaluación de eficacia de la capacitación.	ISO/IEC 27002:2022, control 6.3 (concientización y educación); NIST CSF 2.0, categoría Protect–Awareness and Training (PR.AT); MSPI 2025, Dominio 7 (Formación y sensibilización).	Actas de capacitaciones, registros de participantes, encuestas de evaluación.

Nota. la tabla presenta una recopilación de dominios, indicadores y elementos metodológocos para llevar a cabo el desarrollo propuesto

Así, el desarrollo de los cuatro resultados permite dar cumplimiento integral a los objetivos específicos propuestos en la investigación, ideando una estrategia estructurada de gestión de ciberseguridad para los hospitales de primer nivel del departamento del Huila.

Mediante el resultado 1, se identifican las principales amenazas, vulnerabilidades y riesgos presentes en las instituciones de salud analizadas, definiendo la línea base del estudio.

En el resultado 2, se diseñan políticas de acceso y autenticación orientadas a fortalecer la confidencialidad, integridad y disponibilidad de la información hospitalaria.

Luego, el resultado 3 consolida un plan de respuesta a incidentes que proporciona una guía operativa para la detección, contención, erradicación y recuperación ante eventos de ciberseguridad, garantizando la continuidad de los servicios asistenciales.

Por último, el resultado 4 integra los elementos anteriores en una guía metodológica de autoevaluación, acompañada de indicadores e instrumentos que permiten medir la madurez institucional y promover la mejora continua.

En conjunto, estos resultados establecen una propuesta sólida, realista y aplicable al contexto de los hospitales de primer nivel del Huila, en concordancia de los lineamientos con los marcos ISO/IEC 27001:2022, NIST CSF 2.0 y el Modelo de Seguridad y Privacidad de la Información – MSPI 2025.

El cumplimiento de los objetivos específicos demuestra que la gestión integral de la ciberseguridad en el sector salud no solo depende de la adopción de controles tecnológicos, sino también del fortalecimiento de la gobernanza que hoy en dia es clave, la capacitación institucional y la evaluación permanente del desempeño.

Por ello, los resultados obtenidos componen la base técnica y metodológica sobre la cual se sustentan las conclusiones y recomendaciones finales de este trabajo de investigación.

Conclusiones

El análisis realizado evidencia que los hospitales de primer nivel presentan vulnerabilidades significativas en la gestión de accesos a los sistemas de información, esencialmente en aspectos relacionados con la administración de identidades, autenticación de usuarios y monitoreo de accesos, algo que incrementa el riesgo de incidentes de ciberseguridad que pueden comprometer la confidencialidad y disponibilidad de la información clínica.

Se identifica que la implementación de controles de acceso robustos constituye uno de los mecanismos más relevantes para fortalecer la seguridad de la información en entornos hospitalarios, particularmente en lo referente a la protección de información sensible como las historias clínicas electrónicas.

Se determina que la integración de marcos internacionales como ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el NIST Cybersecurity Framework 2.0 con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano permite disponer de una estrategia integral que articula directrices normativas, gestión del riesgo y controles operativos de seguridad de la información.

La propuesta estratégica desarrollada fundamenta la gestión de identidades digitales, la autenticación multifactor y los mecanismos de monitoreo y auditoría a accesos, factores clave para prevenir accesos no autorizados y optimizar la capacidad de respuesta ante incidentes de ciberseguridad en hospitales de primer nivel.

La implementación de una estrategia de administración del riesgo apoyada en la gestión de respuesta a incidentes brinda un mejoramiento a la capacidad institucional para identificar, contener y mitigar incidentes o eventos de seguridad, favoreciendo la protección de la información clínica y la continuidad de los servicios de salud.

Con la estrategia propuesta se contribuye a fortalecer la protección de activos críticos de información en los hospitales, como lo es la historia clínica electrónica, con la implementación de controles de acceso, mecanismos de autenticación segura y procesos de monitoreo y respuesta a incidentes de seguridad.

Recomendaciones

Se recomienda la implementación progresiva por parte de los hospitales de un SGSI que incluya políticas, procedimientos, controles, roles, auditorías internas y modelos de mejora continua. Aunque en algunos casos puede que la certificación no sea viable financieramente, adoptar la distribución básica del estándar garantizará alinear las prácticas institucionales con estándares internacionales y mejorar la madurez en seguridad de la información.

El estudio permitió evidenciar ausencia o dispersión de inventarios en varios hospitales y por ello, se recomienda elaborar un inventario centralizado que contenga software, hardware, usuarios, privilegios, proveedores, redes y sistemas críticos. Estco con el fin de facilitar el análisis de riesgos, la gestión de incidentes y el cumplimiento del MSPI 2025.

Siguiendo los lineamientos del NIST CSF 2.0 y las políticas del Resultado 2, se recomienda estandarizar la autenticación multifactor (MFA) para acceso a historias clínicas, facturación, administración, sistemas contables y cuentas con privilegios elevados, pues, así se podrá reducir significativamente la probabilidad de accesos no autorizados.

Mediante la identificación de riesgos se pudo observar situaciones de preocupación como acumulación de privilegios, cuentas huérfanas o usuarios genéricos. Se recomienda definir auditorías de periodicidad semestral para monitorear y validar roles, accesos y permisos, desactivar automáticamente cuentas inactivas y documentando los cambios realizados.

Puesto que varios hospitales dependen de terceros para la implementación y el funcionamiento de sus sistemas, se recomienda que todo contrato incluya:

acuerdos de nivel del servicio (ANS)

tiempo máximo de recuperación (RTO) (como mínimo)

alternativas de cifrado y custodia de información

manejo optimizado de incidentes

confidencialidad

respaldo de bases de datos

sanciones por incumplimiento.

Esto se alinea debidamente con el MSPI 2025 y las directrices establecidad en la Política de Gobierno Digital.

Una de las debilidades mas evidentes y mas criticas detectadas fue la cultura de seguridad. Se recomienda que las entidades hospitalarias diseñen e implementen programas periódicos de formación para el personal administrativo, clínico, operativo y de apoyo, resaltando temas como:

manejo seguro y responsable de credenciales

conocimiento de phishing

protección de datos personales

reporte de incidentes

buenas prácticas de acceso y autenticación

Con el fin de verificar la eficacia del plan de respuesta a incidentes del resultado 3, se recomienda llevar a cabo simulacros semestrales para poder medir:

tiempos de detección

tiempos de respuesta

coordinación del equipo de respuesta (o de quien haga sus veces)

integridad de los registros y bitácoras

capacidad de recuperación y continuidad

Estos ejercicios deben ser documentados y gestionados para el ciclo de mejora continua.

Debido al alto índice de vulnerabilidad ante ransomware y falencias en la infraestructura, se recomienda implementar copias de respaldo (backups):

automáticos

cifrados

periódicos

almacenados fuera del centro (offsite)

con pruebas de tiempos de restauración

En el resultado 4 se propone una herramienta concreta de medición y por ello, se recomienda aplicar la guía cada en una periodicidad de seis meses y presentar los resultados (según sea el casso) al comité directivo o al Comité de seguridad de la información, todo con conocimiento de la alta gerencia para:

evaluar madurez institucional

identificar brechas

priorizar inversiones

evidenciar y documentar mejoras ante entes de control

Se recomienda que cada hospital establezca un comité responsable de:

supervisar políticas

evaluar resultados de auditorías

evaluar incidentes

priorizar acciones de mejora

asegurar cumplimiento de Ley 1581

Un comité activo y en funcionamiento podrá mejorar el gobierno institucional y facilita la toma de decisiones informadas.

Referencias Bibliográficas

Abid, A., Cheikhrouhou, S., Kallel, S., Tari, Z., & Jmaiel, M. (2024). A Smart Contract-Based Access Control Framework For Smart Healthcare Systems. Computer Journal, 67(2), 407–422. https://doi.org/10.1093/comjnl/bxac183

Ala, A., Simic, V., Pamucar, D., & Bacanin, N. (2024). Enhancing patient information performance in internet of things-based smart healthcare system: Hybrid artificial intelligence and optimization approaches. Engineering Applications of Artificial Intelligence, 131. https://doi.org/10.1016/j.engappai.2024.107889

Ali, M., Sewunet, A., Shumiye, M., & Hamza, A. (2024). Patient safety culture and associated factors among health care workers in south Wollo zone public hospitals, north east Ethiopia. Perioperative Care and Operating Room Management, 35. https://doi.org/10.1016/j.pcorm.2024.100374

Agencia Nacional del Espectro. (2023). Resolución 773 de 2023: Parámetros técnicos de radiocomunicaciones. ANE.

Arpitha, T., Chouhan, D., & Shreyas, J. (2024). Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications. Journal of Engineering and Applied Science, 71(1). https://doi.org/10.1186/s44147-023-00342-1

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20, 1–10.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and

working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20, 1–10.

B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty. (2021). Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. IEEE Internet of Things Journal, 8(14), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, 37, 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

Centro Cibernético Policial – COLCERT. (2024). Protocolos nacionales de atención de incidentes cibernéticos. Ministerio de Defensa Nacional.

Computing. (2023, septiembre 26). Ciberataques a hospitales: aumento alarmante. https://www.computing.es/noticias/ciberataques-a-hospitales-aumento-alarmante/

Congreso de Colombia. (1999). Resolución 1995 de 1999. Ministerio de Salud.

Congreso de Colombia. (2012). Ley 1581 de 2012: Protección de datos personales.

Congreso de Colombia. (2015). Ley 1751 de 2015: Derecho fundamental a la salud.

Consejo Nacional de Política Económica y Social (DNP). (2019). CONPES 3975: Política de Gobierno Digital.

Creswell, J. W., & Creswell, J. D. (2021). Research design: Qualitative, quantitative, and mixed methods approaches (5.ª ed.). SAGE Publications.

da Veiga, A., Astakhova, L. v., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/J.COSE.2020.101713

Departamento Administrativo de la Función Pública. (2024). Guía de gestión de incidentes de seguridad de la información (Versión 2). https://www.funcionpublica.gov.co

Denecke, K., May, R., & Rivera-Romero, O. (2024). Transformer Models in Healthcare: A Survey and Thematic Analysis. Journal of Medical Systems, 48(1). https://doi.org/10.1007/s10916-024-02043-5

Deo, S., Barnes, E., & Arnold-Smith, P. (2024). Qualitative analysis of healthcare IT using a short-form questionnaire. British Journal of Health Care Management, 30(4). https://doi.org/10.12968/bjhc.2023.0087

Dupont, G., dos Santos, D., Dashevskyi, S., Vijayakumar, S., Murali, S. P., Costante, E., den Hartog, J., & Etalle, S. (2024). Demonstration of new attacks on three healthcare network protocols. Journal of Computer Virology and Hacking Techniques, 20(2), 301–314. https://doi.org/10.1007/s11416-023-00479-w

E.S.E. Hospital Departamental San Antonio de Pitalito. (2024). Informe de Gestión 2023–2024.

E.S.E. Hospital Departamental San Vicente de Paúl de Garzón. (2025). Informe de Gestión 2024.

E.S.E. Hospital del Rosario de Campoalegre. (2023). Informe de Gestión 2023.

E.S.E. Hospital San José de Isnos. (2023). Rendición de cuentas 2022.

Edo, O. C., Ang, D., Billakota, P., & Ho, J. C. (2024). A zero trust architecture for health information systems. Health and Technology, 14(1), 189–199. https://doi.org/10.1007/s12553-023-00809-4

ENISA. (2023). Threat Landscape Report.

Espinoza, J. C., Sehgal, S., Phuong, J., Bahroos, N., Starren, J., Wilcox, A., & Meeker, D. (2024). Development of a social and environmental determinants of health informatics

maturity model. Journal of Clinical and Translational Science, 7(1). https://doi.org/10.1017/cts.2023.691

Gobernación del Huila. (2023). Boletín de conectividad y transformación digital en salud.

Griesser, A., Mzoughi, M., Bidmon, S., & Cherif, E. (2024). Adoption of electronic health records. BMC Health Services Research, 24(1). https://doi.org/10.1186/s12913-024-10929-w

Harvey, R. D., Miller, T. M., Hurley, P. A., Thota, R., Black, L. J., Bruinooge, S. S., Boehmer, L. M., et al. (2024). A call to action to advance patient-focused and decentralized clinical trials. Cancer, 130(8), 1193–1203. https://doi.org/10.1002/cncr.35145

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2020). Metodología de la investigación (6.ª ed.). McGraw-Hill.

Hogg-Graham, R., Scott, A. M., Clear, E. R., Riley, E. N., & Waters, T. M. (2024). Technology and data for unmet social needs in Medicaid care. BMC Health Services Research, 24(1). https://doi.org/10.1186/s12913-024-10705-w

Huila Noticias. (2023, octubre 19). Hospital San José de Isnos reporta inversiones por más de 1.100 millones.

International Organization for Standardization. (2018). ISO/IEC 27005:2018.

International Organization for Standardization. (2022). ISO/IEC 27001:2022.

International Organization for Standardization. (2022). ISO/IEC 27002:2022.

International Organization for Standardization. (2023). ISO/IEC 27035-1:2023.

International Organization for Standardization. (2018). ISO/IEC 27005:2018.

International Organization for Standardization. (2022). ISO/IEC 27001:2022.

International Organization for Standardization. (2022). ISO/IEC 27002:2022.

International Organization for Standardization. (2023). ISO/IEC 27035-1:2023.

Jeanoticias. (2025, febrero 10). Hospital de Isnos requiere modernización tecnológica.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659–671. https://doi.org/10.1016/J.BUSHOR.2021.02.022

Lee, J., Hung, D. Y., Reponen, E., Rundall, T. G., Tierney, A. A., Fournier, P.-L., & Shortell, S. M. (2024). Lean IT management and financial performance. Quality Management in Health Care, 33(2), 67–76. https://doi.org/10.1097/QMH.0000000000000440

Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-Attacks on Hospital Systems: A Narrative Review. The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice, 7, 30–39. https://doi.org/10.1016/j.osep.2025.03.002

McCoy, M. S., Wu, A., Burdyl, S., Kim, Y., Smith, N. K., Gonzales, R., & Friedman, A. B. (2024). User information sharing and hospital website privacy policies. JAMA Network Open, 7(4), E245861. https://doi.org/10.1001/jamanetworkopen.2024.5861

Memon, S., Memon, S., Das, L., & Memon, B. R. (2024). Cyber Security Risk Assessment Methods. IEEE Khi-HTC 2024. https://doi.org/10.1109/KHI-HTC60760.2024.10481961

Ministerio de Salud. (2022). Sistema General de Seguridad Social: niveles de atención. https://www.minsalud.gov.co

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025). Modelo de Seguridad y Privacidad de la Información – MSPI 2025.

Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information. BMC Medical Ethics, 22, 122. https://doi.org/10.1186/s12910-021-00687-3

Murdoch, B. (2021). Privacy and artificial intelligence. BMC Medical Ethics, 22, 122.

National Institute of Standards and Technology. (2018). NIST SP 800-30: Risk Management Guide.

National Institute of Standards and Technology. (2023). NIST SP 800-61r3: Incident Handling Guide.

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

Organización Panamericana de la Salud. (2022). Fortalecimiento de la atención primaria en salud.

Park, Y.-J., Pillai, A., Deng, J., Guo, E., Gupta, M., Paget, M., & Naugler, C. (2024). Clinical utility of large language models. BMC Medical Informatics and Decision Making, 24(1). https://doi.org/10.1186/s12911-024-02459-6

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25(1), 37–43.

Rojas, A. J. S., Valencia, E. F. P., Armas-Aguirre, J., & Molina, J. M. M. (2022). Cybersecurity maturity model. IEEE ICALTER 2022. https://doi.org/10.1109/ICALTER57193.2022.9964729

Rosenbaum, K. E. F., Lasater, K. B., McHugh, M. D., & Lake, E. T. (2024). Hospital performance factors. Medical Care, 62(5), 288–295. https://doi.org/10.1097/MLR.0000000000001966

Shamout, M. D., Das, S., Alazzam, M. B., & Nomani, M. Z. M. (2024). Role of data security technology. AIP Conference Proceedings, 2816(1). https://doi.org/10.1063/5.0179208

Superintendencia Nacional de Salud. (2024). Informe de evaluación de condiciones de habilitación de hospitales del Huila.

Tekin, E., & Kartal, N. (2024). Security of digital transformation in healthcare. In Digital Transformation and Sustainable Development. https://doi.org/10.4018/9798369335673.ch010

Thompson Burdine, J., Thorne, S., & Sandhu, G. (2021). Interpretive description. Medical Education, 55(3), 336–343.

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Security challenges in storing and exchanging medical information. In Medical Robotics and AI-Assisted Diagnostics. https://doi.org/10.4018/979-8-3693-2105-8.ch023

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Security Challenges in Storing and Exchanging Medical Information. IGI Global.

(duplicado mantenido)

Vivekrabinson, K., Ragavan, K., Jothi Thilaga, P., & Bharath Singh, J. (2024). Secure cloud-based electronic health records. Journal of Medical Systems, 48(1). https://doi.org/10.1007/s10916-024-02053-3

Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ahmad Ayassrah, A. Y. A. B. (2024). Cybersecurity's perceived threats in HIS adoption. Heliyon, 10(1). https://doi.org/10.1016/j.heliyon.2023.e22947