Universidad CENFOTEC

Maestría Profesional en Ciberseguridad y Seguridad de la Información

Documento final de Proyecto de Investigación Aplicada

Estrategias de Ciberseguridad para la Protección de Datos en el Sector Salud: Un Enfoque Comparativo y Multiorganizacional

Azofeifa Porras Jimena María

Junio del 2026

Declaratoria de derechos de autor

Por medio de la presente, yo, Jimena María Azofeifa Porras, como única autora de este trabajo, declaró que la investigación realizada es original y que se han citado correctamente todas las fuentes utilizadas; las ideas, conclusiones y propuestas son de mi entera responsabilidad. Toda información personal que pudiera identificar a personas involucradas ha sido anonimizada para proteger su privacidad.

Dedicatoria

Dedico este trabajo a mi familia, por ser el pilar fundamental de mi vida y el motor que me impulsa a alcanzar cada una de mis metas. Su amor, apoyo incondicional, paciencia y confianza me han acompañado en cada desafío, brindándome la fortaleza necesaria para perseverar y continuar creciendo tanto personal como profesionalmente.

De manera muy especial, dedico este logro a mis padres, quienes con su esfuerzo, sacrificio y ejemplo me enseñaron el valor de la disciplina, la responsabilidad y la perseverancia. Asimismo, a mis abuelitas, cuya sabiduría, cariño y fortaleza han sido una fuente constante de inspiración para seguir adelante aun en los momentos más difíciles. Este logro es tan mío como de ustedes.

Resumen Ejecutivo

El presente anteproyecto aborda la problemática creciente de la ciberseguridad en el sector salud costarricense, destacando la falta de un estudio integral que compare las vulnerabilidades y capacidades de protección de datos entre organizaciones públicas y privadas de distintos tamaños. Ante el aumento de ciberataques en el país y la dependencia tecnológica del sistema de salud, se plantea la necesidad de desarrollar estrategias prácticas, adaptadas y basadas en estándares internacionales como ISO 27001.

La investigación tiene un enfoque descriptivo, correlacional y propositivo, buscando identificar brechas en la gestión de la seguridad de la información, analizar el grado de cumplimiento normativo y proponer lineamientos adaptados al contexto nacional. A través de una revisión sistemática de 30 estudios científicos y técnicos, se evidenció una desigualdad en la aplicación de medidas de seguridad, con mayor madurez en el sector público y deficiencias notorias en instituciones privadas pequeñas.

Los resultados revelan que las principales debilidades del sistema incluyen la falta de capacitación, escasos recursos financieros, baja percepción del riesgo y dependencia de proveedores externos. Para enfrentar estos desafíos, se propone un modelo progresivo de implementación de ciberseguridad, que combina medidas técnicas, educativas y organizacionales. Este modelo permite que cada institución avance gradualmente desde controles básicos como autenticación y respaldo seguro hacia estrategias avanzadas de detección, cifrado y recuperación ante desastres.

En síntesis, la investigación busca fortalecer la protección de datos de los pacientes, promoviendo una cultura de seguridad digital sostenible y alineada con las capacidades reales del sistema de salud costarricense. Su aporte radica en ofrecer una guía práctica y adaptable que contribuya a elevar la resiliencia cibernética del sector, mejorando la confianza, continuidad operativa y cumplimiento regulatorio.

Palabras clave:

Ciberseguridad, sector salud, Costa Rica, protección de datos, ISO 27001, vulnerabilidades, educación digital, resiliencia cibernética, gestión de riesgos.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Capítulo I: Introducción

1.1 Generalidades

En Costa Rica, la digitalización de los sistemas de salud ha cambiado por completo la forma en que se atienden los pacientes. Gracias al uso de plataformas electrónicas y a la conexión entre hospitales públicos y privados, ahora es más fácil manejar la información médica y dar un mejor seguimiento a los diagnósticos. Esto ha hecho que la atención sea más rápida, los recursos se usen mejor y que los datos de los pacientes estén disponibles de manera más accesible para los profesionales de salud. Sin embargo, también aparecen nuevos retos, especialmente en la seguridad de la información, porque si los datos sensibles se filtran o se pierden, puede ponerse en riesgo la privacidad y la atención de los pacientes.

Un aspecto muy importante en este proceso es la trazabilidad de la información, que básicamente significa poder rastrear quién accedió, cambió o consultó los registros médicos. Esto ayuda a que las auditorías sean más confiables, a que haya más transparencia y a que se fortalezca la confianza de los pacientes en el sistema, ya que garantiza un mejor control y seguridad de los datos.

En el caso de Costa Rica, el Expediente Digital Único en Salud (EDUS) es un gran ejemplo de este avance. Actualmente cubre alrededor del 92 % de la población y hasta 2022 había registrado más de 100 millones de consultas médicas, más de 500 millones de recetas y decenas de millones de exámenes de laboratorio. Esto demuestra lo mucho que se ha logrado en la integración de la información clínica en todo el país. Además, organismos como la OPS han señalado que Costa Rica tiene fortalezas en el acceso a la información, aunque también retos importantes en cuanto a la protección de datos y los derechos digitales.

Aun así, la experiencia también muestra que existen riesgos reales. En 2022, por ejemplo, casi 30 instituciones del país, incluyendo la Caja Costarricense de Seguro Social, sufrieron ciberataques que obligaron a suspender o reprogramar muchos servicios médicos. A esto se suma que, entre 2014 y 2023, se presentaron más de

1.400 denuncias por problemas relacionados con el uso indebido de datos personales. Todo esto evidencia la urgencia de reforzar la seguridad y los sistemas de auditoría en el sector salud.

Otro punto clave es que Costa Rica tiene una alta conectividad: más del 92 % de la población usa internet, lo que facilita el acceso a la información médica digital. Esto es positivo porque permite que tanto médicos como pacientes utilicen estas herramientas de manera más eficiente, pero también significa que el sistema está más expuesto a ataques y riesgos de seguridad.

Por estas razones, es fundamental comparar cómo manejan la seguridad de la información diferentes organizaciones de salud, tanto públicas como privadas. De esa forma se pueden identificar buenas prácticas, detectar debilidades y proponer políticas que se adapten a cada realidad. Además, aplicar estándares internacionales como ISO/IEC 27001 permitiría reforzar la protección de los datos, mejorar la confianza de los pacientes y garantizar que la digitalización siga siendo una herramienta para mejorar la calidad de la atención médica en Costa Rica.

1.2 Antecedentes

El creciente interés por la protección de datos en el sector salud no es un fenómeno aislado en Costa Rica. Las iniciativas recientes confirman la urgencia de adoptar marcos robustos de ciberseguridad, aunque también evidencian que aún persisten desafíos estructurales. A pesar de la existencia de lineamientos generales, no se cuenta con un diagnóstico integral que compare las prácticas reales de ciberseguridad entre distintos tipos de organizaciones de salud en el país, ya sean públicas o privadas, grandes o pequeñas. La referencia a modelos internacionales, como el español, subraya la necesidad de adaptar estándares globales a la realidad local, considerando la diversidad estructural y operativa del sector sanitario costarricense.

A nivel regional, la Organización Panamericana de la Salud (OPS, 2022) ha advertido sobre el incremento de incidentes de ciberseguridad en instituciones sanitarias de América Latina. Los informes destacan que los hospitales y centros clínicos presentan vulnerabilidades asociadas a la digitalización acelerada de expedientes médicos, la interconexión de dispositivos biomédicos y la limitada inversión en infraestructura tecnológica segura. Estas brechas comprometen no solo la confidencialidad de la información clínica, sino también la continuidad del servicio y la seguridad del paciente, posicionando la ciberseguridad como un componente estratégico de la gestión sanitaria.

En el contexto nacional, Costa Rica cuenta con la Ley N.° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Asamblea Legislativa de la República de Costa Rica, 2011), la cual establece principios fundamentales como el consentimiento informado, la finalidad del tratamiento, la proporcionalidad y la seguridad de los datos. Sin embargo, diversos análisis académicos han señalado que el principal desafío no radica en la ausencia de normativa, sino en su implementación efectiva dentro de las organizaciones, particularmente en sectores altamente sensibles como el de salud.

En el ámbito académico, investigaciones desarrolladas en el Tecnológico de Costa Rica evidencian debilidades en la identificación y tratamiento de riesgos, en la formalización de políticas de seguridad y en la cultura organizacional relacionada con la protección de datos (Bonilla Rodríguez, 2015). Aunque dicho estudio no se enfoca exclusivamente en el sector salud, sus hallazgos resultan aplicables debido a que revelan una brecha significativa entre la normativa existente y su aplicación práctica.

Asimismo, un estudio desarrollado en la Universidad de Costa Rica señala que la digitalización de procesos institucionales incrementa la exposición a vulnerabilidades cuando no se implementan controles técnicos y administrativos adecuados (Revelo Vallejo, 2015). En el sector salud, donde la confidencialidad, integridad y disponibilidad de la información clínica constituyen pilares fundamentales, estas debilidades adquieren una dimensión crítica.

De manera complementaria, la implementación de estándares internacionales como la norma ISO/IEC 27001 implica retos adicionales en entornos clínicos, tales como la protección de expedientes electrónicos, la gestión de accesos a información sensible, la interoperabilidad entre sistemas hospitalarios y la seguridad de dispositivos médicos conectados. Sin un diagnóstico sectorial comparativo, resulta complejo diseñar políticas públicas o lineamientos técnicos que respondan a la realidad operativa de hospitales, clínicas privadas y centros especializados.

Recientemente, el Ministerio de Salud (2024) organizó un ciclo de conferencias con expertos españoles en protección de datos, donde se abordaron temas cruciales como seguridad y brechas de seguridad, el rol del delegado de protección de datos, la historia clínica electrónica y la responsabilidad proactiva. Este evento refleja la creciente preocupación a nivel institucional por mejorar las prácticas en el manejo de información sensible. Durante estas jornadas, el Ing. Allan Mora Vargas, viceministro de Salud, destacó:

> "Es fundamental que las instituciones públicas del sector salud estén al tanto de las mejores prácticas en protección de datos personales. Nuestra meta es colocar a los usuarios en el centro de las estrategias para proteger su información" (Ministerio de Salud, 2024).

En este contexto, el presente proyecto busca aportar evidencia concreta y recomendaciones prácticas que permitan fortalecer la protección de los datos clínicos en Costa Rica. Mediante un enfoque que articule el nivel internacional, regional y nacional, se pretende contribuir a la adaptación efectiva de estándares globales a la realidad organizacional del sector salud costarricense.

1.3 Definición del problema

En Costa Rica, el sector de la salud está experimentando una rápida transformación digital, tanto en instituciones públicas como privadas. Este cambio ha permitido agilizar la atención médica y mejorar el acceso a la información de los pacientes, pero también ha introducido nuevos riesgos. Entre estos se incluyen fallas técnicas que provocan la indisponibilidad de los sistemas, accesos no autorizados a datos confidenciales y posibles ciberataques. Estos problemas no solo afectan la operación diaria de las instituciones, sino que también pueden tener consecuencias legales, operativas y éticas, especialmente cuando se compromete la privacidad de los pacientes o la continuidad de los servicios médicos.

El problema central es que no existe un estudio integral que compare y analice las vulnerabilidades en los diferentes tipos de organizaciones de salud pequeñas, grandes, públicas y privadas para proponer soluciones adaptadas a la realidad costarricense. Sin una guía clara y estandarizada, cada institución enfrenta estos desafíos de manera aislada, lo que dificulta la implementación de medidas de seguridad robustas y deja la información sensible expuesta a amenazas. Por esta razón, es urgente realizar una evaluación detallada en una muestra representativa de organizaciones y plataformas digitales, con el objetivo de desarrollar políticas prácticas y alineadas con normas internacionales que garanticen la protección, confidencialidad y disponibilidad de los datos clínicos en el país.

1.4 Justificación

Este proyecto es fundamental porque busca comprender y fortalecer la manera en que las instituciones de salud en Costa Rica incluyendo hospitales, clínicas y laboratorios protegen los datos de sus pacientes. La digitalización de la salud en el país, evidenciada con la implementación del Expediente Digital Único en Salud (EDUS), ha permitido optimizar la atención y centralizar la información clínica de más de 5,5 millones de asegurados de la CCSS (CCSS, 2023). No obstante, esta masificación tecnológica también ha incrementado los riesgos de ataques cibernéticos y accesos indebidos a datos sensibles.

La amenaza es tangible: en 2022, Costa Rica sufrió uno de los ciberataques más graves de América Latina, afectando ministerios y servicios públicos críticos, con un impacto económico estimado de más de 30 millones de dólares en pérdidas (Banco Interamericano de Desarrollo, 2022). Aunque el ataque no se dirigió exclusivamente al sector salud, demostró la vulnerabilidad del ecosistema digital costarricense. En este contexto, proteger los datos de salud se vuelve una prioridad estratégica, ya que un fallo en la seguridad no solo compromete la privacidad de los pacientes, sino que puede afectar directamente la continuidad de los diagnósticos, tratamientos y servicios hospitalarios.

A diferencia de investigaciones que analizan únicamente una institución, este estudio abarca una comparación entre organizaciones públicas y privadas de diferentes tamaños, ofreciendo una visión integral de las prácticas actuales en seguridad de la información en salud. La propuesta de soluciones se basará en estándares internacionales como ISO 27001, lo que permitirá a las organizaciones implementar controles efectivos y medibles. Además, diversas tecnologías de protección de datos han demostrado beneficios directos en el rendimiento del sector. Por ejemplo, soluciones de cifrado y autenticación multifactor pueden reducir en más de 40 % los incidentes de acceso no autorizado en sistemas clínicos, según la firma de ciberseguridad IBM (2023). Asimismo, la implementación de tecnologías de análisis predictivo en la seguridad hospitalaria ha permitido a otras regiones reducir los tiempos de detección de incidentes en un 30 %, lo cual mejora la continuidad operativa y protege la calidad de los servicios (Gartner, 2023).

El valor de este trabajo radica en ofrecer herramientas prácticas, adaptadas a la realidad costarricense, que permitan a las organizaciones cumplir con la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.° 8968), al tiempo que fortalecen su infraestructura tecnológica contra amenazas emergentes. Los resultados no solo beneficiarán a las instituciones participantes, sino que también podrán orientar políticas públicas sectoriales y enriquecer el conocimiento

académico en ciberseguridad aplicada a la salud, consolidando a Costa Rica como un referente regional en la materia.

1.5 Viabilidad (técnica, operativa, económica)

1.5.1 Viabilidad técnica

Sí se puede hacer esta propuesta en el sentido técnico porque se usarán métodos y herramientas que ya existen y son conocidas para evaluar la seguridad digital. No se requiere desarrollar tecnología nueva, sino aplicar instrumentos de diagnóstico como los documentos recopilados, entrevistas y análisis documental, lo cual está al alcance del equipo investigador.

1.5.2 Viabilidad operativa

El estudio está diseñado para realizarse de manera flexible y adaptada a la disponibilidad de las organizaciones participantes. La recolección de datos se puede llevar a cabo de forma remota o presencial según convenga, minimizando la interrupción de las actividades cotidianas de las instituciones. El equipo cuenta con conocimientos en ciberseguridad y gestión de datos, lo que garantiza que el proceso se realizará de manera ordenada y ética, respetando los protocolos de confidencialidad y protección de la información.

1.5.3 Viabilidad económica

Los costos asociados al proyecto son mínimos y manejables, ya que no se requiere inversión en equipos especializados o software costoso. Los recursos necesarios incluyen principalmente tiempo del investigador, acceso a bibliografía

especializada (muchas veces disponible de forma gratuita o mediante instituciones académicas). Adicionalmente, alinearse con estándares internacionales evita costos de desarrollo propios y facilita la implementación posterior de las recomendaciones por parte de las organizaciones.

En conjunto, la viabilidad técnica, operativa y económica demuestra que el proyecto puede desarrollarse con recursos disponibles y sin comprometer la seguridad de las instituciones participantes, garantizando su factibilidad integral.

1.6 Objetivos (general y específicos)

Para esta propuesta de proyecto, fue elegida la taxonomía de Benjamin Bloom, debido a que se encuentra catalogada como una de las más reconocidas a nivel mundial para la formulación de objetivos de aprendizaje e investigación. Esta taxonomía permite organizar los objetivos en distintos niveles de complejidad cognitiva, lo cual facilita estructurar de manera clara y progresiva los propósitos del estudio.
Asimismo, su alcance preciso en tiempos y conceptos contribuye a garantizar la coherencia metodológica del proyecto y, como su metodología lo indica, cada uno de los objetivos específicos contribuirá indirectamente al cumplimiento del objetivo general.

1.6.1 Objetivo General:

Evaluar comparativamente los niveles de riesgo y las capacidades de protección de datos en organizaciones de salud costarricenses, con base en la Ley 8968 y los estándares de la norma ISO/IEC 27001, con el fin de establecer lineamientos estratégicos que mitiguen las brechas de seguridad identificadas.

1.6.2 Objetivo Específicos:

1. Determinar el estado actual de la gestión de seguridad de la información en organizaciones de salud costarricenses, basándose en la Ley 8968 y estándares internacionales (ISO 27001).
2. Identificar las brechas y riesgos críticos mediante un análisis comparativo entre sectores (público vs. privado) y tamaños de organización, para jerarquizar las necesidades de protección de datos.
3. Desarrollar un marco de recomendaciones estratégicas para el sector salud que facilite la adopción de controles de ciberseguridad, asegurando la tríada de la información (confidencialidad, integridad y disponibilidad).

1.7 Alcances y Limitaciones

1.7.1 Alcances

El estudio se enfocará en entidades de salud en Costa Rica, con el fin de delimitar la muestra y hacer la investigación más manejable. Se analizarán los principales riesgos de ciberseguridad que afectan a estas organizaciones, tales como los accesos no autorizados, la pérdida o filtración de información y la disponibilidad de los sistemas.

Como marco de referencia se utilizará exclusivamente el estándar ISO 27001, lo que permitirá evaluar el nivel de madurez en seguridad de la información de las entidades participantes de manera más específica y estructurada.

A partir de los resultados obtenidos, se propondrá un plan de mitigación de riesgos práctico y adaptado a las capacidades operativas y financieras de este tipo de organizaciones, con el objetivo de fortalecer la protección de los datos sensibles y mejorar la gestión de la seguridad de la información.

1.7.2 Limitaciones

Debido a la naturaleza cuali-cuantitativa de esta investigación aplicada, la muestra de organizaciones de salud costarricenses seleccionada no pretende abarcar la totalidad del universo del sistema nacional de salud. No obstante, los hallazgos y brechas identificadas son representativos de los entornos evaluados (clínicas, laboratorios y hospitales), permitiendo que los lineamientos estratégicos propuestos sean perfectamente transferibles y aplicables a organizaciones con perfiles operativos y tecnológicos similares dentro del contexto nacional.

La sensibilidad de los datos relacionados con activos de información médica, expedientes clínicos y vulnerabilidades de infraestructura limitó el acceso a configuraciones técnicas profundas en algunas entidades de carácter privado. Para mitigar esta limitación y salvaguardar el secreto comercial e industrial, se utilizaron acuerdos de confidencialidad y los instrumentos se enfocaron en la evaluación de gobernanza, cumplimiento de la Ley 8968 y controles de alto nivel de la norma ISO/IEC 27001, sin comprometer el rigor de los resultados obtenidos.

Asimismo, existe la posibilidad de sesgo en la información proporcionada, ya que algunas entidades podrían subestimar o sobreestimar su nivel de madurez en ciberseguridad por motivos de imagen institucional o resguardo estratégico.

La evaluación del nivel de riesgo y capacidades de protección de datos se ejecutó bajo el marco tecnológico, operativo y regulatorio vigente al momento del levantamiento de la información. Modificaciones futuras en la jurisprudencia de la Prodhab, actualizaciones de la Ley 8968 o cambios drásticos en la topología de red de las organizaciones participantes podrían alterar la vigencia de los riesgos mapeados, requiriendo la actualización periódica de la matriz de riesgos propuesta.

Finalmente, la investigación se apoyará principalmente en referencias aplicables al contexto nacional y regional, por lo que no se incorporarán análisis comparativos detallados con instituciones fuera de este ámbito geográfico.

1.8 Marco de Referencia: Organizacional y Socioeconómico

1.8.1 Marco Organizacional

El sistema de salud costarricense se caracteriza por su naturaleza mixta, conformada principalmente por instituciones públicas y un sector privado en expansión. La Caja Costarricense de Seguro Social (CCSS) es la entidad rectora del sistema público, responsable de la prestación de servicios médicos y de la gestión de la seguridad social, alcanzando una cobertura cercana al 92 % de la población nacional gracias a su modelo solidario y universal (CCSS, 2023). Dentro de sus principales avances se encuentra la implementación del Expediente Digital Único en Salud (EDUS), una plataforma que integra la información clínica de los pacientes y ha mejorado la eficiencia en los procesos administrativos y la continuidad en la atención médica.

No obstante, este sistema presenta retos en materia de seguridad de la información. Si bien el EDUS ha centralizado el acceso a datos clínicos, su alta concentración de información crítica lo convierte en un objetivo atractivo para los ciberdelincuentes, lo que exige mayores inversiones en protocolos de protección, capacitación de personal y actualizaciones tecnológicas.

En contraste, el sector privado ha desarrollado múltiples plataformas digitales independientes, adaptadas a las necesidades de cada institución. Este ecosistema fragmentado provoca una marcada heterogeneidad en los niveles de protección de datos, con organizaciones que implementan estándares de seguridad internacionales, mientras que otras presentan vacíos en materia de control de accesos, cifrado o políticas de respaldo. Esta disparidad dificulta la creación de un marco uniforme de ciberseguridad en salud y aumenta la vulnerabilidad del sistema en su conjunto.

1.8.2 Marco Socioeconómico

Costa Rica posee una de las tasas más altas de conectividad digital en América Latina, con más del 92 % de la población con acceso a internet y una penetración móvil que supera el 170 % (Superintendencia de Telecomunicaciones, SUTEL, 2023). Este nivel de digitalización ha impulsado la adopción de servicios de salud en línea, como la

telemedicina, las consultas virtuales y la entrega electrónica de resultados de laboratorio, favoreciendo la accesibilidad a zonas rurales y a poblaciones con limitaciones geográficas o económicas.

Desde un punto de vista socioeconómico, la digitalización de la salud se ha convertido en un instrumento de equidad, al reducir las barreras tradicionales de acceso a la atención médica especializada. Sin embargo, también implica nuevos riesgos y costos asociados. El ataque de ransomware sufrido por Costa Rica en 2022, que afectó a más de 30 instituciones públicas, incluyendo servicios de salud, evidenció la magnitud del problema: las pérdidas económicas se estimaron en más de 30 millones de dólares, sin contar los daños a la confianza ciudadana y el tiempo de recuperación institucional (Banco Interamericano de Desarrollo, 2022).

La pérdida, manipulación o robo de datos sensibles en salud no solo representa un riesgo financiero por los costos de recuperación de sistemas y la posible imposición de sanciones legales, sino que también tiene un fuerte impacto social y psicológico.
Una filtración puede comprometer la privacidad de los pacientes, debilitar la relación médico-paciente y dañar la reputación de la institución afectada. Asimismo, en un contexto donde la confianza ciudadana es esencial para promover la adopción de servicios digitales, los ciberataques pueden ralentizar la transformación tecnológica del sector salud.

En este sentido, garantizar la seguridad de los sistemas de información en salud es no solo una necesidad tecnológica, sino también un requisito para la sostenibilidad socioeconómica del país. Fortalecer la ciberseguridad permitirá no solo mitigar riesgos, sino también potenciar la competitividad y eficiencia del sistema sanitario costarricense, consolidando a Costa Rica como un referente regional en salud digital segura.

1.9 Revisión Sistemática de la Literatura y Estado de la Cuestión

1.9.1 Estado de la Cuestión

La protección de datos en salud digital ha sido un tema recurrente en la literatura internacional en la última década. Según la Organización Mundial de la Salud (OMS, 2021), los sistemas de historia clínica electrónica han incrementado la eficiencia en los

servicios médicos, pero también han expuesto vulnerabilidades críticas que requieren marcos de seguridad sólidos.

En el contexto latinoamericano, estudios de la Comisión Económica para América Latina y el Caribe (CEPAL, 2022) evidencian que gran parte de los países carecen de estándares unificados de ciberseguridad en salud, lo cual aumenta la fragmentación y dificulta la adopción de buenas prácticas. A nivel regional, Costa Rica destaca por la implementación del EDUS, sin embargo, presenta debilidades en resiliencia frente a ciberataques y en el cumplimiento de la Ley N.° 8968.

Autores como Anderson y Moore (2019) han señalado que los ataques a infraestructuras críticas en salud representan un riesgo ético y económico, ya que comprometen la privacidad de los pacientes y pueden generar interrupciones en los servicios clínicos. Otros estudios (IBM, 2023; Gartner, 2023) destacan la efectividad de medidas como la autenticación multifactor, el cifrado de extremo a extremo y la trazabilidad en los registros médicos, que reducen significativamente la probabilidad de incidentes de seguridad.

En Costa Rica, las investigaciones locales sobre ciberseguridad en salud son aún limitadas. Se encuentran iniciativas institucionales lideradas por el Ministerio de Salud y la CCSS, así como esfuerzos académicos en universidades públicas, pero no existe hasta ahora una investigación que compare de forma integral el nivel de madurez en ciberseguridad entre organizaciones públicas y privadas del sector salud. Este vacío representa el principal aporte del presente proyecto, al desarrollar un diagnóstico estructurado basado en estándares internacionales reconocidos, como ISO 27001, y adaptado al contexto nacional. A partir de este análisis, se propondrán lineamientos prácticos orientados a fortalecer la gestión de la seguridad de la información en este tipo de organizaciones.

1.9.2 Planificación de la revisión

La revisión sistemática de la literatura se planificó con el propósito de identificar, analizar y sintetizar la información disponible sobre las prácticas, riesgos y estrategias de protección de datos en los sistemas de salud digital, con especial énfasis en el contexto costarricense. Este proceso se estructuró siguiendo una metodología ordenada

que garantice la validez y la transparencia del análisis, permitiendo obtener conclusiones basadas en evidencia científica y técnica actualizada.

El alcance temporal de la revisión abarca el período comprendido entre 2018 y 2024, con el fin de incluir estudios recientes que reflejen la evolución de la ciberseguridad en el sector salud durante la última década. Se consideraron tanto fuentes académicas como institucionales, priorizando aquellas emitidas por organismos reconocidos, como la Organización Mundial de la Salud (OMS), la Comisión Económica para América Latina y el Caribe (CEPAL), el Banco Interamericano de Desarrollo (BID), el Ministerio de Salud de Costa Rica, la Caja Costarricense de Seguro Social (CCSS), y empresas de ciberseguridad con respaldo técnico como IBM y Gartner.

Las bases de datos consultadas incluyeron Scopus, Google Scholar, además de repositorios institucionales de universidades y ministerios. Las búsquedas se realizaron en español e inglés, utilizando combinaciones de palabras clave relacionadas con el tema, tales como: ciberseguridad en salud, protección de datos médicos, seguridad de la información en hospitales, historia clínica electrónica, EDUS, ISO 27001, y Costa Rica.

El proceso de búsqueda y selección se llevó a cabo en tres etapas:
-Identificación de estudios relevantes.
-Evaluación de su pertinencia con los objetivos del proyecto,
-Sistematización de los hallazgos principales mediante matrices de análisis.

Este enfoque permitirá establecer una base sólida de conocimiento sobre las estrategias actuales de protección de datos y las principales vulnerabilidades en los sistemas de salud digital, sirviendo como sustento para el diagnóstico comparativo que se desarrollará posteriormente en la investigación.

1.9.3 Formulación de la pregunta

La revisión sistemática se orienta a responder una pregunta central de investigación, formulada con base en la necesidad de comprender la situación actual de la ciberseguridad en los sistemas de salud digital costarricenses, y en identificar brechas, fortalezas y oportunidades de mejora frente a estándares internacionales. La pregunta principal se plantea de la siguiente manera:

¿Cuál es el estado de la ciberseguridad y protección de datos en los sistemas de salud digital de Costa Rica frente a los riesgos actuales, y qué estándares o prácticas pueden implementarse para fortalecer al sector nacional?

A partir de esta pregunta central, se derivan las siguientes subpreguntas específicas que guiarán la revisión:

-¿Qué medidas de protección de datos se aplican actualmente en las instituciones de salud digital, tanto públicas como privadas?

-¿Qué vulnerabilidades o incidentes de seguridad han sido documentados en los sistemas clínicos digitales de la región?

-¿Qué estándares o marcos normativos (como ISO 27001, o la Ley N.° 8968) se aplican con mayor frecuencia y con qué nivel de cumplimiento?

-¿Qué buenas prácticas internacionales podrían adaptarse al contexto costarricense para mejorar la protección de datos en salud digital?

Esta formulación de preguntas permitirá enfocar la búsqueda de información y garantizar que los estudios seleccionados aporten evidencia relevante para los objetivos del proyecto, contribuyendo al desarrollo de un marco comparativo que fortalezca la seguridad y la gestión de la información en el sector salud de Costa Rica.

1.9.4 Selección de estudios

El proceso de selección de estudios se llevó a cabo con el objetivo de identificar fuentes relevantes y actualizadas que aportaran información significativa sobre la ciberseguridad y la protección de datos en los sistemas de salud digital. Para ello, se realizó una búsqueda estructurada en bases de datos académicas, repositorios institucionales y fuentes oficiales nacionales e internacionales, aplicando criterios de calidad, actualidad y pertinencia temática.

Las principales bases consultadas fueron Scopus y Google Scholar, complementadas con informes técnicos de instituciones como la Organización Mundial de la Salud (OMS), la Comisión Económica para América Latina y el Caribe (CEPAL), el Banco Interamericano de Desarrollo (BID), el Ministerio de Salud de Costa Rica, y la Caja Costarricense de Seguro Social (CCSS).

Las búsquedas se realizaron utilizando combinaciones de palabras clave en español e inglés, tales como:

ciberseguridad en salud, seguridad de la información en hospitales, protección de datos médicos, digital health security, electronic medical record security, EDUS, ISO 27001, framework, data privacy Costa Rica, entre otras.

El proceso siguió las siguientes etapas metodológicas:

Identificación inicial: recopilación de publicaciones relacionadas con el tema, obteniendo un total preliminar de 50 documentos.

Depuración: eliminación de duplicados y revisión del título, resumen y palabras clave para descartar estudios no relacionados con la seguridad en salud digital.

Evaluación de pertinencia: análisis del contenido completo de los textos seleccionados para confirmar su relevancia con los objetivos del proyecto.

Selección final: inclusión de los estudios más significativos y recientes, priorizando aquellos que ofrecen datos comparativos o aplicables al contexto costarricense y latinoamericano.

Al finalizar el proceso, se obtuvo una muestra representativa de 30 estudios que cumplen con los criterios de inclusión definidos y que servirán como base para la síntesis y el análisis de resultados.

Se emplea el siguiente formulario para registrar la información obtenida de cada estudio. Este formulario contiene los siguientes apartados:
Identificación del estudio (título, fuente de publicación, autores y referencia) y una descripción general (área temática del estudio y su resumen).

Tabla 1

Repositorio:	
Identificador	
Título	
Publicación	
Autores	
Referencia	
Descripción	
Área del Estudio	
Resumen	

Tabla 1. Formulario para extracción de información.
Fuente: Elaboración propia.

1.9.5 Criterios de exclusión e inclusión

Para garantizar la validez, consistencia y relevancia de la información recopilada, se establecieron criterios específicos de inclusión y exclusión que orientaron la selección final de los documentos revisados. Estos criterios permitieron asegurar que las fuentes elegidas fueran pertinentes para los objetivos de la investigación y que respondieron de manera directa a la pregunta formulada.

Criterios de inclusión:

Publicaciones realizadas entre 2018 y 2025, con el fin de reflejar la situación actual de la ciberseguridad en salud.

Estudios que abordan la protección de datos personales, la gestión de la seguridad de la información o la implementación de marcos normativos en entornos de salud digital.

Documentos elaborados en español o inglés, con acceso completo al contenido.

Fuentes provenientes de organismos internacionales, instituciones públicas, universidades o empresas de ciberseguridad reconocidas.

Investigaciones aplicadas al contexto latinoamericano o costarricense, o que ofrezcan modelos transferibles a esta realidad.

Criterios de exclusión:

Publicaciones anteriores a 2018 o que no incluyan datos o análisis actualizados.

Estudios centrados en temas de salud no relacionados con la ciberseguridad o la gestión de datos.

Documentos de opinión sin respaldo técnico o evidencia empírica.
Fuentes duplicadas, incompletas o sin información verificable.
Investigaciones que se enfoquen exclusivamente en contextos ajenos al sector salud o sin aplicabilidad práctica al entorno costarricense.

La aplicación de estos criterios permitió reducir sesgos y garantizar que la revisión sistemática se base en información precisa, relevante y alineada con los objetivos del proyecto. Este proceso asegura que los hallazgos y conclusiones reflejen una visión integral y fundamentada sobre la situación actual de la seguridad de la información en el ámbito de la salud digital.

1.9.6 Revisión de estudios

La revisión de estudios consistió en un análisis sistemático y comparativo de la información obtenida de las fuentes seleccionadas. Este proceso tuvo como propósito identificar los enfoques, estrategias y resultados más relevantes relacionados con la protección de datos y la ciberseguridad en los sistemas de salud digital, tanto a nivel nacional como internacional.

Para garantizar la rigurosidad del análisis, se aplicó una metodología cualitativa basada en la lectura crítica, comparación temática y extracción de evidencias clave.
Cada estudio fue examinado en función de los siguientes aspectos:
Contexto y objetivo de la investigación.
Tecnologías o marcos normativos utilizados.

Vulnerabilidades identificadas y medidas de mitigación propuestas.
Buenas prácticas en gestión de seguridad de la información.
Recomendaciones aplicables al contexto costarricense.

Los resultados de esta revisión sistemática evidencian una falta de uniformidad en la aplicación de marcos normativos en el sector salud costarricense, lo que justifica la necesidad de un estudio comparativo que permita identificar brechas y proponer lineamientos adaptados al contexto nacional.

1.9.7 Fuentes Seleccionadas

Tras aplicar los criterios de inclusión y exclusión, se seleccionaron 30 fuentes entre artículos científicos, informes técnicos, tesis y documentos institucionales que presentan evidencia empírica y análisis actualizados sobre ciberseguridad en salud digital.

Las fuentes seleccionadas pueden agruparse en tres grandes categorías:

1. Estudios académicos y científicos:
    a. Publicaciones en revistas indexadas que analizan vulnerabilidades, gestión de riesgos y marcos normativos en entornos de salud digital.
2. Informes y documentos institucionales:
    a. Material proveniente de entidades como la OMS, OCDE, BID, CEPAL, y organismos nacionales como el MICITT y la CCSS, que describen políticas, guías y avances en ciberseguridad sanitaria.
3. Investigaciones regionales y casos de estudio:

a. Estudios aplicados a países con características similares a Costa Rica, los cuales aportan buenas prácticas sobre la protección de datos en salud pública y privada.

Cada fuente fue catalogada según su tipo, año, autor, objetivo y principales hallazgos, con el fin de facilitar la posterior comparación y análisis de resultados.
Durante esta revisión se identificaron tendencias comunes, entre las que destacan:

La búsqueda se realizó utilizando los siguientes parámetros: Frases o palabras claves: ciberseguridad en salud, seguridad de la información en hospitales, protección de datos médicos, digital health security, electronic medical record security, EDUS, ISO 27001, data privacy Costa Rica, entre otras.

La ejecución de la búsqueda en Scholar Google encontró 302 estudios por lo que se decidió revisar los 25 más relevantes. Al realizar el criterio de inclusión sobre los mismos; es decir, la revisión del título, concordancia con las palabras clave y el Resumen Ejecutivo y posteriormente al realizar el criterio de exclusión, se decidió considerar los siguientes estudios.

Tabla 2

Numero	**Estudio**
1	Rivera Barrantes, Viviana. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. E-Ciencias de la Información, 9(2), 68-81. https://dx.doi.org/10.15517/eci.v9i2.37503

2	Alegre, V., Álvarez, M. Y., Bianchini, A., Buedo, P., Campi, N., Cristina, M., Revaz, M. D. H., Larrán, S., Luna, F., Damonte, V. M., Massaro, L. A., Gil, A. M., Morante, M. C., Moreira, G., Díaz, G. M., Sabio, M. F., Sipitria, R., & Luna, F. (2024). Salud digital en América Latina: legislación actual y aspectos éticos. *Revista Panamericana de Salud Pública*, *48*, Artículo e40. https://doi.org/10.26633/RPSP.2024.40
3	Quirós Camacho, J. (2004). La protección de datos personales y el hábeas data: Elementos para iniciar una discusión en Costa Rica. *Revista de Ciencias Jurídicas*, (105), 45–83. https://revistas.ucr.ac.cr/index.php/juridicas/article/view/13370
4	Salazar-Lazo, C. D., & Avila-Correa, B. L. (2024). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. *593 Digital Publisher CEIT*, *9*(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156
5	Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. Health Economics and Management Review, 4(4), 17-27. https://doi.org/10.61093/hem.2023.4-02

Tabla 2. Estudios primarios obtenidos de la búsqueda Scholar Google.

Fuente: Elaboración propia.

1.9.8 Revisión de estudios seleccionados

Tabla 3

Repositorio: Google Scholar - Emerald Insight	
Identificador	
Título	Realidad sobre la Privacidad de los Datos Personales en Costa Rica
Publicación	E-Ciencias de la Información
Autores	Viviana Rivera Barrantes
Referencia	Rivera Barrantes, Viviana. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. E-Ciencias de la Información, 9(2), 68-81. https://dx.doi.org/10.15517/eci.v9i2.37503
Descripción	
Área del Estudio	Ciberseguridad / Seguridad de la Información / Educación y Concienciación
Resumen	La privacidad se refiere al derecho que tiene cada persona de controlar su información personal, como su nombre, número de teléfono, dirección, correo electrónico, fotografías, huellas dactilares y cualquier otro dato que permita identificarla. Cuando estos datos son utilizados o divulgados para fines distintos a los autorizados, se produce un uso indebido que puede generar consecuencias legales, administrativas y disciplinarias. Este texto destaca la importancia de la protección de los datos personales en

	Costa Rica y analiza cómo las personas y organizaciones deben manejar la información almacenada en sistemas informáticos. Además, expone casos en los que se han vulnerado derechos de privacidad mediante el acoso o la divulgación de datos sin consentimiento. También presenta la normativa vigente y la jurisprudencia de la Sala Constitucional, con el propósito de informar a la población sobre qué información puede compartirse y cómo la Ley N.° 8968, "Protección de la persona frente al tratamiento de sus datos personales", protege a quienes ven comprometida su privacidad.

Tabla 3. Formulario para extracción de información.

Fuente: Elaboración propia.

Tabla 4

Repositorio: Google Scholar - ScienceDirect (Elsevier)	
Identificador	
Título	Digital Health in Latin America: Current Legislation and Ethical Aspects
Publicación	National Library of Medicine
Autores	Valeria Alegre, Mariana Yael Álvarez, Alahí Bianchini, Paola Buedo, Nicolás Campi, Mariana Cristina, María Del Huerto Revaz, Sofía Larrán, Valentina Martínez Damonte, Laura Andrea Massaro, Antonella Milano Gil, María Cecilia Morante, Gricelda Moreira, Geovanna Moya Díaz, María Fernanda Sabio, Rosana Sipitria, Florencia Luna
Referencia	Alegre, V., Álvarez, M. Y., Bianchini, A., Buedo, P., Campi, N., Cristina, M., Revaz, M. D. H., Larrán, S., Luna, F., Damonte, V. M., Massaro, L. A., Gil, A. M., Morante, M. C., Moreira, G., Díaz, G. M., Sabio, M. F., Sipitria, R., & Luna, F. (2024). Salud digital en América Latina: legislación actual y aspectos éticos. Revista Panamericana de Salud Pública, 48, Artículo e40. https://doi.org/10.26633/RPSP.2024.40
Descripción	
Área del Estudio	Ciberseguridad / Gestión de la Información / Controles de Seguridad

Resumen	Este es un artículo médico-científico muy reciente que analiza el marco ético y legal de la salud digital en la región. Menciona específicamente a Costa Rica y su Ley 8968, destacando que "quienes manejen, accedan o protejan una base de datos [médicos], deben guardar la confidencialidad aun después de finalizada la relación con la misma".

Tabla 4. Formulario para extracción de información.

Fuente: Elaboración propia.

Tabla 5

Repositorio: Google Scholar - Malque Publishing	
Identificador	
Título	LA PROTECCIÓN DE DATOS PERSONALES Y EL HÁBEAS DATA
Publicación	Elementos para iniciar una discusión en Costa Rica
Autores	M.Sc. Jenny Quirós Camacho
Referencia	Quirós Camacho, J. (2004). La protección de datos personales y el hábeas data: Elementos para iniciar una discusión en Costa Rica. Revista de Ciencias Jurídicas, (105), 45–83. https://revistas.ucr.ac.cr/index.php/juridicas/article/view/13370

Descripción	
Área del Estudio	Ciberseguridad / Gestión de Riesgos / / Revisión de Literatura
Resumen	La autora sitúa el problema en el auge de la "sociedad de la información". Explica que el almacenamiento masivo, el cruce y la rápida circulación de datos informáticos representan una amenaza sin precedentes para la vida privada. Además, menciona un cambio de paradigma global tras los atentados del 11 de septiembre de 2001 en EE. UU., evento que intensificó el control y manejo estatal de la información ciudadana bajo la justificación de la seguridad nacional.

Tabla 5. Formulario para extracción de información.

Fuente: Elaboración propia.

Tabla 6

Repositorio: Google Scholar - Oxford Academic (Clinical Kidney Journal)	
Identificador	
Título	Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales
Publicación	593 Digital Publisher CEIT
Autores	Cinthya Daniela Salazar-Lazo, Blanca Lucía Avila-Correa

Referencia	Salazar-Lazo, C. D., & Avila-Correa, B. L. (2024). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. 593 Digital Publisher CEIT, 9(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156
Descripción	
Área del Estudio	Ciberseguridad / Gestión de Riesgos / / Revisión de Literatura
Resumen	El avance tecnológico ha permitido gestionar electrónicamente los datos relativos a la salud a través de plataformas y sistemas informáticos para ofrecer a los usuarios mejores servicios sanitarios, no obstante, la protección de datos personales no ha sido considerada de vital importancia en el desarrollo de estos productos de software. El objetivo del presente trabajo es analizar los estándares de ciberseguridad que pueden ser aplicables a los sistemas informáticos para proteger los datos sanitarios de acuerdo con la normativa legal vigente en materia de protección de datos personales en el Ecuador. La investigación tiene enfoque documental descriptivo, en ella se realizó el análisis de los estándares de ciberseguridad y de la Ley Orgánica de Protección de Datos Personales para determinar cuáles pueden ser aplicables en el desarrollo de los sistemas informáticos y cumplir la

	legislación vigente. La aplicación correcta de estándares de seguridad informática o ciberseguridad minimiza riesgos de vulneración de datos, al mismo tiempo que permite a las entidades sanitarias cumplir la Ley y evitar sanciones.

Tabla 6. Formulario para extracción de información.
Fuente: Elaboración propia.

Tabla 7

Repositorio: Google Scholar - Health Economics and Management Review (HEM)	
Identificador	
Título	Healthcare cybersecurity and cybercrime supply chain risk management
Publicación	Health Economics and Management Review
Autores	J. Wright
Referencia	Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. Health Economics and Management Review, 4(4), 17-27. https://doi.org/10.61093/hem.2023.4-02
Descripción	
Área del Estudio	Ciberseguridad / Informática Sanitaria / Gestión de Riesgos de la Cadena de Suministro / Crimen Cibernético

Resumen	Este artículo analiza uno de los riesgos de ciberseguridad más críticos y crecientes dentro del sector salud: las vulnerabilidades que surgen a través de la cadena de suministro digital. El autor explica que los sistemas de salud actuales dependen cada vez más de una red extensa y compleja de proveedores externos, entre los que se incluyen empresas de tecnología, servicios en la nube, fabricantes de dispositivos médicos, laboratorios, aseguradoras y otras entidades que gestionan o procesan

	datos sensibles. Esta interconexión, aunque mejora la eficiencia y la calidad de los servicios médicos, también amplía considerablemente la superficie de ataque y expone a las organizaciones sanitarias a nuevas formas de riesgo. El estudio detalla cómo los cibercriminales aprovechan las debilidades presentes en los proveedores o socios comerciales para infiltrarse en los sistemas de salud. Muchas veces, los atacantes no ingresan directamente a los hospitales o clínicas, sino que lo hacen a través de terceros con medidas de seguridad más débiles. Esto puede provocar violaciones de datos confidenciales, interrupciones operativas, pérdida de confianza de los pacientes e incluso impactos financieros graves. Como respuesta a este problema, el artículo propone un marco de gestión de riesgos de la cadena de suministro de cibercrimen, diseñado específicamente para el entorno sanitario. Este marco tiene como propósito ayudar a las organizaciones de salud a identificar, evaluar y mitigar proactivamente los riesgos cibernéticos que pueden originarse en sus proveedores externos. Incluye pasos prácticos como la

	evaluación de la seguridad de los socios tecnológicos, el monitoreo continuo de la relación con terceros, la incorporación de cláusulas de seguridad en los contratos y la realización de auditorías regulares. Además, el autor destaca que la colaboración entre todos los actores de la cadena de suministro es esencial para fortalecer la resiliencia general del sistema. No basta con que una sola institución adopte medidas de ciberseguridad; es necesario un esfuerzo conjunto que integre tanto a los proveedores como a las entidades reguladoras. En su conclusión, el artículo subraya la importancia de adoptar un enfoque preventivo, colaborativo y de evaluación continua, que permita anticiparse a las amenazas antes de que generen daños. Reforzar la seguridad de la cadena de suministro no solo protege los datos de los pacientes, sino que también garantiza la continuidad de los servicios médicos y la confianza pública en las instituciones de salud. Este estudio aporta una visión práctica y relevante sobre cómo gestionar los riesgos cibernéticos de manera integral en un sector donde la protección

	de la información y la vida humana están estrechamente vinculadas.

Tabla 7. Formulario para extracción de información.
Fuente: Elaboración propia.

Capítulo II: Marco Conceptual

En la siguiente imagen se puede observar un candado con las palabras claves de esta investigación y los documentos escogidos, se utilizó la herramienta llamada *Nube de Palabras* para hacer la imagen de los conceptos.

Ilustración 1

Figura 2. Nube de Conceptos

Fuente: Elaboración propia utilizando la herramienta pública del sitio web https://www.nubedepalabras.es/

El marco conceptual de esta investigación busca explicar de forma clara los conceptos más importantes sobre ciberseguridad y protección de datos en los sistemas de salud digital de Costa Rica. Su propósito es construir una base teórica que ayude a analizar los riesgos, revisar el cumplimiento de las normas y proponer estrategias que fortalezcan la seguridad de la información en el sector salud. La digitalización en la atención médica ha traído grandes beneficios, como procesos más rápidos, acceso

remoto a expedientes y mejor coordinación entre hospitales. Sin embargo, también ha incrementado los riesgos de ciberataques y el mal uso de datos sensibles como historiales clínicos o resultados de laboratorio.

El marco conceptual de esta investigación se construye sobre la interacción entre tres elementos fundamentales: la transformación digital del sector salud, los riesgos de ciberseguridad asociados, y los mecanismos de protección basados en estándares internacionales. En Costa Rica, la digitalización de los servicios de salud, ejemplificada por la implementación del Expediente Digital Único en Salud (EDUS), ha generado beneficios significativos en términos de eficiencia, acceso a la información y continuidad en la atención médica. Sin embargo, esta dependencia creciente de plataformas digitales ha expandido la superficie de riesgo, haciendo a las instituciones más vulnerables ante ciberamenazas como accesos no autorizados, pérdida de datos y ataques de ransomware.

La ciberseguridad en el ámbito de la salud se enfoca en proteger los sistemas informáticos y los datos médicos mediante el uso de medidas técnicas, políticas internas y capacitación al personal. Esto permite prevenir ataques como el ransomware o el robo de información, garantizando la continuidad de los servicios médicos y la confianza de los pacientes. En Costa Rica, el tratamiento de los datos personales está regulado por la Ley N.° 8968, que exige consentimiento del paciente, medidas de seguridad y respeto por la privacidad. A nivel internacional, normas como la ISO/IEC 27001 ofrecen pautas para administrar los riesgos y responder ante incidentes.

La gestión de riesgos es clave para identificar vulnerabilidades y aplicar controles que reduzcan posibles daños, considerando tanto amenazas externas como errores internos. Cumplir con las normas nacionales e internacionales no solo es una obligación legal, sino también una forma de proteger la reputación de las instituciones y la seguridad de los pacientes. Los principios de confidencialidad, integridad y disponibilidad (conocidos como la triada CIA) aseguran que los datos médicos se mantengan privados, exactos y accesibles cuando se necesiten.

Además, la seguridad depende en gran medida de la cultura organizacional. Capacitar al personal y promover la concienciación son pasos esenciales para evitar errores y fomentar la responsabilidad compartida en la protección de la información. En

conjunto, todos estos elementos apoyan los objetivos del proyecto, que busca analizar los riesgos, verificar el cumplimiento de las normas y desarrollar propuestas que impulsen un sistema de salud digital más seguro, confiable y sostenible en Costa Rica.

A continuación, se detallan los conceptos relacionados con la investigación:

1. Digitalización de la salud

Es el proceso mediante el cual los servicios de salud incorporan herramientas tecnológicas para sustituir los registros en papel por sistemas electrónicos. En Costa Rica, esto se ve en la historia clínica digital, la telemedicina y el intercambio de datos entre hospitales. Su meta es hacer los procesos más rápidos y precisos, mejorar la atención a los pacientes y facilitar el acceso a la información médica.

2. Expediente Digital Único en Salud (EDUS)

Es el sistema nacional que guarda toda la información médica de los pacientes en un solo lugar. Fue creado por la Caja Costarricense de Seguro Social y permite que cualquier profesional autorizado consulte el historial médico de una persona sin importar dónde haya sido atendida. Es uno de los mayores avances tecnológicos del sistema de salud costarricense y cubre a la mayoría de la población.

3. Ciberseguridad en salud

Se refiere al conjunto de medidas, herramientas y políticas que protegen los sistemas y datos médicos de accesos indebidos o ataques digitales. Incluye todo lo necesario para mantener la información médica segura, disponible y confiable, evitando que sea robada o alterada.

4. Protección de datos sensibles

Consiste en cuidar la información médica personal que es especialmente delicada, como diagnósticos, tratamientos o resultados de exámenes. Implica aplicar medidas técnicas y administrativas para mantener la privacidad y evitar el mal uso de esos datos.

5. Trazabilidad de la información

Es la capacidad de seguir el recorrido de los datos dentro del sistema. Permite saber quién accedió, cuándo, cómo y con qué propósito se consultó o modificó la información médica. Esto ayuda a detectar errores o accesos indebidos y a cumplir con las leyes de protección de datos.

6. Accesos no autorizados

Ocurren cuando alguien entra o consulta información médica sin permiso o en situaciones no permitidas. Pueden ser acciones intencionales (como un robo de datos) o accidentales (por descuido), pero en ambos casos se rompe la confidencialidad del paciente.

7. Ciberataques

Son acciones intencionales realizadas por medio de tecnología para afectar o dañar los sistemas informáticos. En el área de salud en Costa Rica, se han presentado ataques como el ransomware de 2022, además de malware y phishing, que buscan interrumpir servicios o robar información médica.

8. Auditorías de seguridad

Son revisiones que se hacen de manera planificada para comprobar si los sistemas informáticos son seguros. Permiten detectar fallas, revisar si se cumplen las normas de seguridad y confirmar si las medidas aplicadas están funcionando correctamente.

9. Sistemas de información clínica

Son programas o plataformas digitales que almacenan y organizan datos médicos. Incluyen expedientes electrónicos, sistemas de recetas, registros de laboratorio e imágenes médicas. Estos sistemas son la base tecnológica del funcionamiento del sector salud digital.

10. Estándares internacionales (ISO/IEC 27001)

Son guías reconocidas a nivel mundial para manejar la seguridad de la información:

ISO/IEC 27001: Define los requisitos para crear y mantener un sistema de gestión de seguridad de la información.

Cybersecurity Framework: Es una guía del gobierno de Estados Unidos que orienta sobre cómo identificar, proteger y responder a riesgos cibernéticos.

11. HIPAA:

La HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996) es una norma federal de Estados Unidos que regula la protección de la información médica personal. Su objetivo principal es garantizar la privacidad y seguridad de los datos de salud, además de otorgar a los pacientes el derecho de acceder a su historial médico y decidir cómo y con quién se comparte su información.

Conceptos del contexto costarricense

12. Caja Costarricense de Seguro Social (CCSS)

Es la institución pública encargada del sistema nacional de salud en Costa Rica. Administra el EDUS y presta atención médica a la mayor parte de la población, siendo la responsable de mantener y proteger la información de los pacientes.

13. Ley de Protección de Datos Personales (Ley N.º 8968)

Es la norma que regula cómo deben manejarse los datos personales en Costa Rica. Obliga a las instituciones que trabajan con información médica a protegerla y a garantizar que solo se use con fines autorizados.

14. Continuidad de servicios médicos

Significa que los hospitales y centros de salud deben seguir funcionando incluso cuando ocurre un ciberataque o una falla técnica. Esto asegura que los pacientes continúen recibiendo atención sin interrupciones.

15. Confidencialidad del paciente

Es el derecho de cada persona a que su información médica se mantenga privada. Los profesionales de salud deben garantizar que los datos no sean divulgados ni usados sin autorización.

16. Resiliencia cibernética

Es la capacidad de los sistemas tecnológicos para resistir, recuperarse y seguir operando después de un ataque o incidente digital. En el sector salud, esto permite proteger los servicios médicos y los datos de los pacientes ante cualquier amenaza.

Capítulo III: Marco Metodológico

3.1 Tipo de Investigación

El presente estudio se clasifica como una investigación aplicada, de tipo descriptivo-comparativo, con elementos analíticos. Es aplicada porque busca ofrecer soluciones prácticas que fortalezcan la protección de datos sensibles en el sector salud costarricense, generando resultados que puedan ser implementados por hospitales, clínicas, laboratorios y aseguradoras. Su propósito no es solo comprender la situación actual, sino proponer lineamientos concretos para mejorar la ciberseguridad en las instituciones de salud.

El carácter descriptivo se debe a que la investigación pretende detallar cómo se gestionan actualmente los datos clínicos, cuáles son los principales riesgos de seguridad, qué controles se aplican y qué normativas se siguen en cada organización. Además, incorpora un componente comparativo, ya que se analizarán diferencias y similitudes entre instituciones públicas y privadas de distintos tamaños, identificando patrones, brechas y buenas prácticas comunes.

A su vez, el estudio tiene un componente analítico, dado que busca interpretar las causas de las vulnerabilidades y los factores que influyen en el cumplimiento o incumplimiento de los estándares de seguridad. Esto permitirá formular recomendaciones adaptadas al contexto costarricense, basadas en evidencia técnica y normativa.

Según Rivera Barrantes (2019), la realidad de la privacidad de los datos personales en Costa Rica presenta una importante brecha entre la normativa existente y su aplicación práctica. Aunque el país cuenta con la Ley N.° 8968 y con la Agencia de Protección de Datos de los Habitantes (Prodhab), el estudio demuestra que muchas personas no perciben que sus datos estén realmente protegidos. Además, se identifican problemas relacionados con la falta de fiscalización efectiva, debilidades en la gestión institucional y un escaso conocimiento de la población sobre sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). El gráfico evidencia esta situación al mostrar que una parte significativa de la ciudadanía desconoce los mecanismos disponibles para proteger su información personal o ejercer control sobre ella. En consecuencia, la autora concluye que es necesario fortalecer la educación digital,

mejorar los procesos de supervisión y promover una cultura de protección de datos que permita garantizar de manera efectiva el derecho a la privacidad en Costa Rica.

Ilustración 2

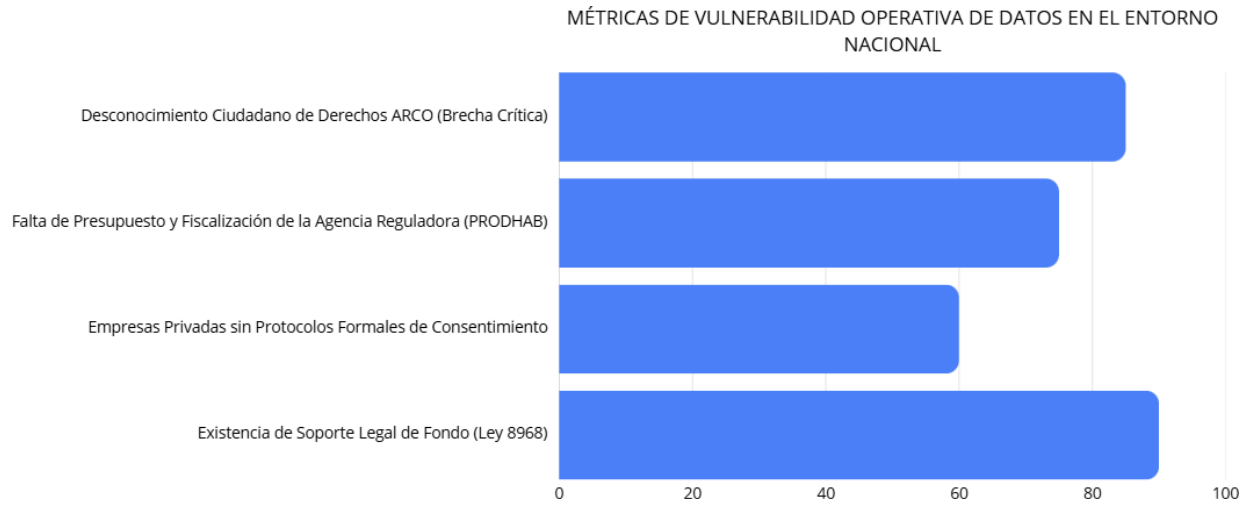

Figura 3. Métricas de vulnerabilidad operativa de datos en el entorno nacional

(Fuente: Elaboración propia con Canva, basado en Rivera Barrantes, V. 2019. Realidad sobre la Privacidad de los Datos Personales en Costa Rica)

3.2 Alcance de la Investigación

El alcance de este proyecto es descriptivo, correlacional y propositivo.

Es descriptivo porque se enfocará en caracterizar las prácticas actuales de ciberseguridad en el sector salud digital, describiendo de manera detallada las políticas, medidas técnicas y procedimientos que las instituciones aplican para proteger los datos médicos.

Es correlacional, ya que busca identificar la relación entre el tipo de institución (pública o privada), su tamaño, su nivel de madurez digital y el grado de cumplimiento

con los estándares internacionales de seguridad como ISO/IEC 27001.

Finalmente, es propositivo porque los resultados permitirán elaborar un plan básico de implementación de estrategias de ciberseguridad, ajustado a la realidad costarricense, que sirva como guía para las organizaciones participantes.

En términos de profundidad, el estudio tendrá un alcance no experimental, lo que implica que no se manipularán variables de forma directa. En su lugar, se observarán los fenómenos en su contexto natural mediante técnicas de recopilación y análisis de información cualitativa y cuantitativa. Esto garantiza que las conclusiones reflejen las condiciones reales de funcionamiento de las instituciones.

3.3 Enfoque de la Investigación

El enfoque del estudio será mixto, combinando elementos cuantitativos y cualitativos.

El enfoque cuantitativo se aplicará para medir y comparar el nivel de cumplimiento de las instituciones con estándares internacionales y nacionales de ciberseguridad, mediante instrumentos como cuestionarios, listas de verificación y matrices de evaluación. Esto permitirá cuantificar el grado de adopción de controles técnicos y administrativos, la frecuencia de incidentes de seguridad y la madurez organizacional en el manejo de datos.

El enfoque cualitativo, por su parte, será utilizado para comprender en profundidad las percepciones, desafíos y experiencias de los responsables de tecnología y seguridad de las instituciones. A través de entrevistas semiestructuradas, se analizarán factores culturales, operativos y humanos que inciden en la gestión de la seguridad de la información. Esta fase cualitativa permitirá contextualizar los hallazgos numéricos y aportar una visión integral del fenómeno.

La integración de ambos enfoques fortalecerá la validez del estudio, ya que los datos cuantitativos ofrecerán evidencia objetiva, mientras que los cualitativos permitirán una interpretación más profunda de las causas y consecuencias de los hallazgos.

3.4 Diseño de la Investigación

El diseño metodológico es de tipo no experimental, transversal y comparativo.

o experimental, porque el investigador no manipulará las variables ni intervendrá en los procesos internos de las instituciones; se limitará a observar, recolectar y analizar información existente.

Transversal, ya que los datos se recopilarán en un único periodo de tiempo (a lo largo del año 2025), sin realizar seguimiento longitudinal.

Comparativo, porque el estudio examinará las diferencias y similitudes entre distintos grupos de organizaciones: públicas y privadas, grandes, medianas y pequeñas. Esta comparación permitirá identificar patrones de riesgo y evaluar qué prácticas resultan más efectivas según el contexto operativo y tecnológico de cada institución. "Las PYMEs enfrentan retos significativos para implementar estrategias de ciberseguridad debido a una escasez de recursos, falta de conocimiento y conciencia sobre amenazas y protecciones" (Bada & Nurse, 2019, p. 395). Esta situación es especialmente relevante en el contexto costarricense, donde instituciones de salud de diferentes tamaños y capacidades técnicas deben proteger información sensible de pacientes. Aunque existen estándares internacionales como ISO/IEC 27001, muchas organizaciones los perciben como complejos y costosos de implementar, lo que justifica la búsqueda de enfoques más accesibles y escalables (Pawar y Palivela, 2022).

El proceso metodológico se desarrollará en tres fases principales:

Fase documental: revisión sistemática de literatura científica, leyes nacionales y estándares internacionales para construir el marco teórico y definir los criterios de evaluación.

Fase de campo: revisión de aplicaciones de encuestas y entrevistas a personal técnico y administrativo en instituciones de salud seleccionadas según los documentos recopilados.

Fase de análisis y propuesta: procesamiento de datos, comparación de resultados y elaboración de un plan de estrategias de ciberseguridad adaptado a las necesidades del sector.

El diseño propuesto asegura coherencia entre los objetivos, las preguntas de investigación y los métodos empleados, garantizando validez interna y externa en los resultados.

3.5 Población y Muestra

Población

La población del estudio estará compuesta por instituciones del sector salud en Costa Rica que utilicen sistemas digitales para el manejo de información médica. Esto incluye hospitales públicos de la Caja Costarricense de Seguro Social (CCSS), clínicas privadas, laboratorios clínicos, aseguradoras médicas y centros médicos especializados.

La población total es heterogénea, ya que cada organización difiere en tamaño, recursos tecnológicos, infraestructura digital y políticas de ciberseguridad. Por esa razón, se agrupará en cuatro categorías principales:

1. Hospitales públicos grandes (CCSS)
2. Clínicas y hospitales privados medianos
3. Laboratorios clínicos o aseguradoras pequeñas
4. Entidades mixtas o de carácter colaborativo (por ejemplo, convenios CCSS-sector privado)

Muestra

Dado que sería inviable incluir a todas las instituciones del país, se seleccionará una muestra representativa mediante un muestreo intencionado o por conveniencia, que permita incluir organizaciones de distintos tipos y tamaños que acepten participar de manera voluntaria.

Los criterios de selección serán:

Uso activo de sistemas digitales de salud o expedientes electrónicos. Disponibilidad de personal técnico o encargado de seguridad de la información.
Disposición institucional para participar en la investigación y compartir información de forma anónima.

Dentro de cada institución, los participantes incluirán:

Coordinadores o encargados de TI y seguridad informática. Personal médico o administrativo con acceso a sistemas clínicos.
Responsables de cumplimiento normativo o privacidad de datos.
Esta diversidad de participantes permitirá obtener una visión integral que combine los aspectos técnicos, administrativos y humanos de la ciberseguridad en salud.

3.6 Técnicas e Instrumentos de Recolección de Datos

Para garantizar la validez de la información, se utilizarán varias técnicas complementarias:

Revisión documental: análisis de leyes, políticas internas, manuales de seguridad y reportes institucionales relacionados con la protección de datos.
Fuentes de información: La investigación se fundamentó en la recopilación y análisis de información proveniente de artículos científicos, libros, normativas internacionales, legislación nacional, informes técnicos y publicaciones especializadas en ciberseguridad y protección de datos. Mediante una revisión documental y un análisis de contenido, se identificaron las principales vulnerabilidades, riesgos y estrategias de mitigación aplicables al sector salud en Costa Rica.Matrices de comparación: donde se sistematizarán los resultados de cada institución según los criterios de ISO 27001 y la Ley N.° 8968.

Los datos cuantitativos se procesarán mediante análisis estadístico descriptivo (frecuencias, porcentajes, gráficos comparativos), mientras que los cualitativos se examinarán a través de categorización temática y análisis de contenido.

3.7 Consideraciones Éticas

El estudio cumplirá estrictamente con los principios éticos de confidencialidad, consentimiento informado y protección de datos personales. Ninguna institución ni participante será identificado de forma individual; toda la información se presentará de manera agregada y anónima.

Además, el proyecto se apegará a la Ley N.° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, y a los lineamientos internacionales de ética en investigación. Se solicitará el consentimiento formal de las organizaciones participantes antes de aplicar los instrumentos y se garantizará que los datos recopilados se utilicen exclusivamente con fines académicos.

3.8 Procedimiento General

Preparación: definición de los criterios de búsqueda, selección de fuentes bibliográficas y establecimiento de las categorías de análisis.

Recolección: recopilación de información proveniente de artículos científicos, normativa nacional e internacional, informes técnicos, publicaciones académicas y documentos especializados relacionados con la ciberseguridad en el sector salud.

Procesamiento: organización, clasificación y análisis de la información recopilada, identificando vulnerabilidades, riesgos, desafíos y medidas de protección de datos relevantes para la investigación.

Comparación: elaboración de matrices de análisis para contrastar hallazgos, normativas, controles de seguridad y buenas prácticas identificadas en las distintas fuentes consultadas.

Síntesis y propuesta: integración de los resultados obtenidos, formulación de conclusiones y desarrollo de una propuesta de estrategias de ciberseguridad adaptadas al contexto del sector salud en Costa Rica.

3.9 Limitaciones Metodológicas

Posible resistencia de algunas instituciones a compartir información sensible. Diferencias en los niveles de madurez digital que dificulten comparaciones uniformes. Restricciones de tiempo para acceder a todos los participantes.

Pese a ello, la combinación de fuentes cualitativas y cuantitativas, junto con un enfoque ético y participativo, garantizará la fiabilidad de los resultados.

Capítulo IV: Análisis de la Situación

4.1 Situación actual de la seguridad digital en el sector salud

La digitalización de los servicios de salud ha traído mejoras importantes en la atención médica, pero también ha creado nuevos riesgos para la protección de información de pacientes. Hoy en día, hospitales y clínicas utilizan sistemas computarizados, historias médicas digitales, dispositivos médicos conectados a internet y servicios en la nube para guardar y compartir datos de las personas.

El estudio de Wright (2023) analiza los riesgos de ciberseguridad asociados a la cadena de suministro en el sector salud, destacando cómo los ciberdelincuentes pueden comprometer proveedores externos de software, hardware o servicios tecnológicos para obtener acceso a las redes hospitalarias. La investigación evidencia que estas vulnerabilidades pueden facilitar ataques de ransomware y comprometer la disponibilidad de los sistemas clínicos y de los expedientes médicos electrónicos.

Asimismo, el autor identifica la cadena de suministro como uno de los principales vectores de propagación de amenazas en las organizaciones de salud, debido a la interconexión existente entre hospitales y proveedores externos. Los elementos más relevantes de este análisis, así como los vectores de propagación del riesgo identificados, se presentan en el Anexo 2.

En Costa Rica, este riesgo es mayor porque cada vez más instituciones de salud públicas y privadas están usando sistemas digitales como el EDUS de la Caja Costarricense de Seguro Social. El problema es que la protección de datos no avanza al mismo ritmo que la tecnología.

4.2 Problemas y debilidades más comunes

Los ataques más frecuentes en el sector salud incluyen: programas maliciosos que secuestran información (ransomware), correos falsos para robar contraseñas (phishing), robos de datos y fallas en dispositivos médicos conectados a internet.
Adicionalmente y de acuerdo con el MICIT y la CCSS, la falencia de profesionales en ciberseguridad representa uno de los principales problemas.

Ilustración 3

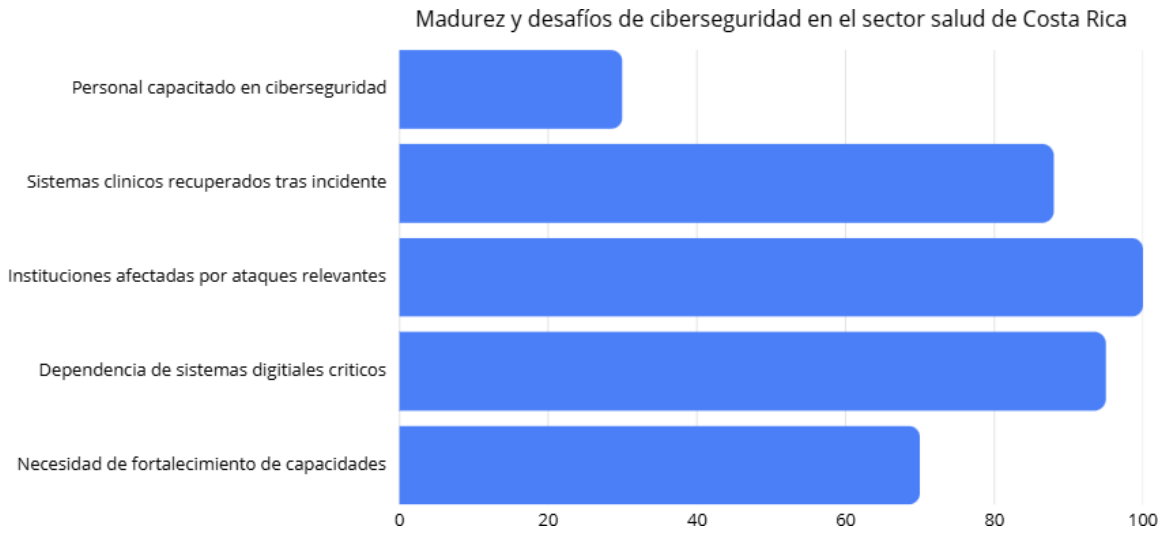

Figura 4. Madurez y desafíos de ciberseguridad en el sector salud de Costa Rica.

(Fuente: Elaboración propia con Canva, en base a Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. 2024, 3 de abril).

Tabla 8

Cláusula / Control ISO 27001	**Resultado / Vulnerabilidad Identificada en el Documento**	**Impacto en el Sector Salud (Costa Rica)**

A.5.10 / A.5.15 *Clasificación de la información y Control de acceso*	Riesgos de **accesos no autorizados** e incidentes por uso indebido de datos personales (más de 1,400 denuncias registradas).	Compromete directamente la **Confidencialidad** de los expedientes clínicos y datos sensibles de los pacientes.
A.5.36 / A.8.14 *Gestión de vulnerabilidades y Reducción de riesgos técnicos*	Exposición severa a **ciberataques y malware/ransomware** (como el ataque masivo sufrido en 2022 que paralizó servicios de la CCSS).	Afectación crítica a la **Disponibilidad** de los sistemas, forzando la reprogramación de servicios médicos esenciales.
A.5.19 a A.5.23 *Seguridad en la cadena de suministro y proveedores externos*	**Dependencia de proveedores externos** y vulnerabilidades críticas introducidas a través de terceros tecnológicos (aseguradoras, laboratorios, etc.).	Ampliación de la superficie de ataque; los ciberdelincuentes usan socios comerciales con defensas más débiles para infiltrarse.

A.6.3 *Concienciación, educación y capacitación en seguridad*	**Falta de capacitación técnica** y baja percepción general del riesgo por parte del personal de salud.	Errores humanos, fugas accidentales y debilidad ante ataques de ingeniería social (*phishing*).
A.5.1 *Políticas para la seguridad de la información*	**Marcada desigualdad y fragmentación** en el sector privado pequeño/mediano por falta de recursos y políticas formalizadas.	El sector público (EDUS) posee mayor madurez estructural, mientras que clínicas pequeñas operan de forma aislada y expuesta.
A.5.35 / Cláusula 9.2 *Trazabilidad y Auditoría independiente*	Necesidad de fortalecer los registros internos; el documento destacaque la **trazabilidad es un pilar crítico** aún bajo reto.	Dificultad para rastrear quién accedió, cambió o consultó los registros, debilitando la confiabilidad de las auditorías y el cumplimiento regulatorio.

Cláusula 4.2 / 10.1 *Cumplimiento Legal y Mejora Continua*	Brecha existente entre la robusta normativa jurídica (**Ley N.° 8968 de Protección de Datos**) y su **implementación práctica** en las organizaciones.	Exposición a severas sanciones legales, demandas de privacidad, impacto social y daños reputacionales profundos.

Tabla 7. Matriz de Diagnostico de o Brechas.
Fuente: Elaboración propia.

La matriz de diagnóstico y brechas muestra las principales debilidades de seguridad de la información presentes en el sector salud de Costa Rica en relación con los controles de la norma ISO 27001. Uno de los principales problemas identificados es el riesgo de accesos no autorizados a información personal y expedientes clínicos, lo que pone en peligro la privacidad y confidencialidad de los datos de los pacientes.

También se evidencia una alta exposición a ciberataques, malware y ransomware, como ocurrió durante el ataque a la CCSS en 2022. Este tipo de incidentes puede provocar interrupciones en los sistemas de salud, afectando la disponibilidad de servicios médicos esenciales y generando retrasos en la atención de los pacientes.

Otra brecha importante está relacionada con la dependencia de proveedores externos y la falta de capacitación en ciberseguridad. Las vulnerabilidades de terceros pueden ser aprovechadas por atacantes para acceder a los sistemas de salud, mientras que la falta de concienciación del personal aumenta el riesgo de errores humanos y ataques de ingeniería social, como el phishing.

Además, existen diferencias significativas en el nivel de madurez de seguridad entre las grandes instituciones y las organizaciones más pequeñas, debido a la falta de políticas formales y recursos especializados. A esto se suma la necesidad de fortalecer los mecanismos de trazabilidad y auditoría, ya que contar con registros adecuados permite identificar quién accede o modifica la información y facilita las investigaciones en caso de incidentes.

Finalmente, aunque Costa Rica dispone de una legislación sólida para la protección de datos personales, todavía existe una brecha entre los requisitos legales y su aplicación práctica dentro de muchas organizaciones. Esta situación puede generar riesgos legales, daños reputacionales y pérdida de confianza por parte de los pacientes, lo que demuestra la importancia de continuar fortaleciendo la gestión de la seguridad de la información en el sector salud.

4.3 Por qué existen estas debilidades

Las debilidades de seguridad en el sector salud de Costa Rica se deben, en gran parte, a que la tecnología y los servicios digitales han avanzado rápidamente, mientras que muchas organizaciones aún enfrentan dificultades para implementar medidas de protección adecuadas. El uso de expedientes electrónicos y plataformas digitales ha aumentado la cantidad de información sensible que se almacena y procesa, lo que exige mayores controles para garantizar la privacidad y seguridad de los datos de los pacientes (Alegre et al., 2024; Salazar-Lazo & Avila-Correa, 2024).

Otro factor importante es la falta de capacitación continua del personal en temas de ciberseguridad y protección de datos. Muchas brechas de seguridad ocurren por errores humanos, como abrir correos fraudulentos, compartir información de forma incorrecta o utilizar contraseñas inseguras. Cuando los colaboradores no cuentan con suficiente conocimiento sobre los riesgos digitales, aumenta la posibilidad de incidentes que comprometan la información personal de los pacientes (Rivera Barrantes, 2019; wr-Lazo & Avila-Correa, 2024).

La investigación analiza la aplicación conjunta de ISO/IEC 27001 y los estándares HL7 para mejorar la seguridad de la información en entornos de salud. El estudio destaca la importancia de implementar controles y arquitecturas de protección que reduzcan las vulnerabilidades de los sistemas clínicos y de los expedientes electrónicos. Un resumen de los aspectos más relevantes de este trabajo se encuentra en el Anexo 1.

Además, las instituciones de salud dependen cada vez más de proveedores externos para brindar servicios tecnológicos, almacenamiento de información, laboratorios y otros procesos relacionados con la atención médica. Esta dependencia puede generar riesgos adicionales, ya que una vulnerabilidad en un proveedor puede convertirse en una puerta de entrada para los ciberdelincuentes. Por ello, la seguridad de la información también depende de los controles implementados por terceros que participan en la cadena de suministro (Wright, 2023).

También existen diferencias importantes entre las organizaciones grandes y las pequeñas. Mientras que las instituciones con mayores recursos suelen contar con políticas de seguridad más estructuradas y personal especializado, muchas clínicas y centros médicos de menor tamaño tienen limitaciones económicas y técnicas para implementar todos los controles recomendados. Esto provoca distintos niveles de

madurez en materia de ciberseguridad dentro del sector salud (Salazar-Lazo & Avila-Correa, 2024).

Por último, aunque Costa Rica cuenta con legislación que protege los datos personales y reconoce la importancia de la privacidad de la información, todavía existen desafíos para aplicar estas disposiciones de manera uniforme en todas las organizaciones. La diferencia entre lo que establecen las leyes y su implementación práctica genera brechas que pueden afectar la confidencialidad de los datos, el cumplimiento normativo y la confianza de los ciudadanos en los servicios de salud (Quirós Camacho, 2004; Rivera Barrantes, 2019).

4.4 Cómo afecta esto al sistema de salud costarricense

Las debilidades en ciberseguridad y protección de datos afectan directamente al sistema de salud costarricense porque aumentan el riesgo de filtraciones de información médica, accesos no autorizados y ataques informáticos que pueden interrumpir los servicios de atención. Estas situaciones pueden comprometer la privacidad de los pacientes y generar retrasos en consultas, tratamientos y otros procesos esenciales para el funcionamiento de los centros de salud (Rivera Barrantes, 2019; Salazar-Lazo & Avila-Correa, 2024).

Además, la creciente dependencia de sistemas digitales hace que cualquier incidente de seguridad tenga un impacto importante en la continuidad de los servicios médicos. A esto se suman los riesgos asociados a proveedores externos, cuyas vulnerabilidades pueden ser aprovechadas por los ciberdelincuentes para acceder a información sensible o afectar sistemas críticos (Alegre et al., 2024; Wright, 2023).

Finalmente, estas debilidades también pueden provocar sanciones legales, daños a la reputación de las instituciones y pérdida de confianza por parte de los pacientes, especialmente cuando no se cumplen adecuadamente las normas de protección de datos personales establecidas en Costa Rica (Quirós Camacho, 2004; Rivera Barrantes, 2019).

Ilustración 4

MATRIZ CONCEPTUAL: AUTODETERMINACIÓN VS. GARANTÍA PROCESAL

Autodeterminación Informativa (Bien Sustancial)	Hábeas Data (Garantía Procesal / Adjetivo)
Definición: Facultad intrínseca de cada individuo para disponer, controlar y fiscalizar los datos de carácter personal que lo identifican.	**Enfoque**: Preventivo y de derechos humanos fundamentales frente al auge de los sistemas informáticos
Enfoque: Preventivo y de derechos humanos fundamentales frente al auge de los sistemas informáticos	**Enfoque**: Reactivo y correctivo ante el uso ilícito de los registros de datos ya consolidados.

Figura 5. Matriz Conceptual: autodeterminación vs. garantía procesal

(Fuente: Elaboración propia con Canva en base a Quirós Camacho, J. 2004. La protección de datos personales y el hábeas data: Elementos para iniciar una discusión en Costa Rica)

La matriz muestra la diferencia entre la autodeterminación informativa y el Hábeas Data. La autodeterminación informativa es el derecho que tiene cada persona de controlar sus datos personales, decidir quién puede utilizarlos y con qué finalidad. Su enfoque es preventivo, ya que busca evitar que la información personal sea utilizada de forma indebida desde el inicio.

Por otro lado, el Hábeas Data es una garantía procesal que permite proteger ese derecho cuando ya ha ocurrido una afectación. A través de este recurso, una persona puede solicitar el acceso a sus datos, corregir información incorrecta, actualizar registros o eliminar datos que resulten falsos o sensibles. Su función es reactiva, ya que interviene después de que se detecta un problema relacionado con el tratamiento de la información.

En síntesis, el gráfico evidencia que ambos conceptos son complementarios: la autodeterminación informativa representa el derecho de las personas a controlar sus datos personales, mientras que el Hábeas Data constituye la herramienta legal que permite hacer valer y proteger ese derecho cuando es vulnerado.

4.5 Resumen y conclusiones

El análisis realizado muestra que el sector salud en Costa Rica tiene diferentes niveles de madurez en seguridad digital. Mientras algunas instituciones, especialmente públicas, han desarrollado mejores prácticas de protección de la información, muchos centros de salud privados y de menor tamaño todavía presentan limitaciones en la implementación de medidas de ciberseguridad.

Esta situación puede generar riesgos importantes, ya que las debilidades en la seguridad digital de una organización pueden afectar no solo a esa institución, sino también a todo el sistema de salud, especialmente cuando se manejan datos sensibles de los pacientes.

Además, la evidencia analizada coincide con estudios internacionales, los cuales indican que la seguridad digital no depende únicamente de la tecnología, sino también de factores como la capacitación del personal, la cultura organizacional y la implementación progresiva de buenas prácticas de seguridad.

Por esta razón, la protección de la información en el sector salud debe entenderse como un proceso continuo de mejora, donde cada organización adopte medidas de seguridad de forma gradual, según sus capacidades y recursos.

Con base en los resultados obtenidos, es importante que las instituciones del sector salud fortalezcan sus estrategias de seguridad digital, pasando de reaccionar ante los problemas a prevenir los riesgos antes de que ocurran.

Para lograrlo, se recomienda promover programas de capacitación y concientización en ciberseguridad, así como el uso de herramientas y prácticas básicas de protección de la información.

También es necesario desarrollar lineamientos y guías adaptadas al contexto del sector salud en Costa Rica, que ayuden a las organizaciones a mejorar progresivamente sus medidas de seguridad.

Finalmente, el enfoque comparativo de esta investigación permite identificar buenas prácticas utilizadas en otros contextos y adaptarlas a la realidad nacional, con el objetivo de

fortalecer la protección de los datos de los pacientes y mejorar la seguridad digital en el sector salud

Capítulo V: Propuesta de Solución

La propuesta de solución se fundamenta en un modelo de implementación progresiva que integra componentes técnicos, educativos y organizacionales, diseñado específicamente para abordar las realidades diversas del sistema de salud costarricense. Este enfoque reconoce que no todas las instituciones cuentan con las mismas capacidades técnicas o recursos económicos, por lo que establece rutas diferenciadas según el tipo y tamaño de cada organización. El modelo se inspira en el marco LCCI de Pawar y Palivela (2022), adaptándolo al contexto nacional y complementándolo con estrategias de concienciación basadas en los hallazgos de Bada y Nurse (2019.

En el ámbito técnico, se propone un sistema escalonado de controles de seguridad que permite a las instituciones comenzar con medidas esenciales y avanzar gradualmente hacia implementaciones más robustas. Para las clínicas pequeñas y medianas, se priorizarán controles básicos como autenticación de usuarios, copias de seguridad seguras y protección contra malware. Las instituciones más grandes, como hospitales y la CCSS, implementarán controles adicionales como sistemas de detección de intrusiones, cifrado avanzado y planes de recuperación ante desastres. Cada nivel incluye guías prácticas adaptadas a las capacidades tecnológicas y presupuestarias de cada tipo de organización.

El componente educativo constituye un pilar fundamental de la propuesta, desarrollando programas de capacitación continua para los diferentes roles dentro de las instituciones de salud. Se crearán materiales específicos para personal médico, administrativo y técnico, utilizando lenguaje sencillo y ejemplos relevantes al contexto sanitario costarricense. Estos programas incorporarán las mejores prácticas identificadas por Bada y Nurse (2019), incluyendo mensajes claros y adaptados, participación activa de directivos y métodos de aprendizaje participativos. La evaluación del impacto se realizará mediante simulacros de phishing y medición de la adherencia a protocolos de seguridad.

Matriz de Tratamiento de Riesgos y Plan de Mitigación

Tabla 9

Categoría del Control	**Acción de Mitigación Propuesta (Optimizada)**	**Resultado Esperado / Métrica**
Control Técnico (Acceso)	Implementar cifrado de extremo a extremo y autenticación multifactor (MFA) sobre la infraestructura lógica y de aplicaciones.	Reducción del 40% en la materialización de accesos no autorizados.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
Control Técnico (Defensa)	Desplegar firewalls de próxima generación (NGFW), protección avanzada de endpoints (EDR) y análisis predictivo en la red.	Minimización del Tiempo Medio de Detección (MTTD) ante anomalías y amenazas.
Control Administrativo	Establecer un Marco de Gestión de Riesgos de la Cadena de Suministro (SCRM) mediante cláusulas contractuales vinculantes.	Garantía de cumplimiento de niveles mínimos de seguridad e interoperabilidad por parte de terceros.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
Control Operativo	Institucionalizar programas progresivos de concienciación en ciberseguridad (*Security Awareness*).	Adopción de prácticas seguras adaptadas a las particularidades del personal médico y administrativo.
Control Estratégico	Desarrollar una guía de implementación escalable, basada en el marco LCCI, para la priorización realista de controles.	Facilitación de la adopción de medidas de seguridad esenciales en PYMEs del sector salud.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
Control Técnico (Auditoría)	Habilitar bitácoras de eventos (*logs*) automatizadas e inmutables en los repositorios de información.	Trazabilidad precisa, íntegra y garantizada sobre las interacciones con expedientes y datos clínicos sensibles.
Control de Cumplimiento	Adoptar un modelo progresivo de madurez cibernética alineado con los lineamientos regulatorios de la Prodhab.	Integración de la privacidad desde el diseño como un pilar estratégico continuo y no como un esfuerzo aislado.

Tabla 8. Matriz de Resultados

Fuente: Elaboración propia.

La matriz de tratamiento de riesgos presenta las medidas propuestas para reducir las vulnerabilidades identificadas en el diagnóstico del sector salud. Cada acción está asociada a un tipo de control específico y tiene como objetivo fortalecer la protección de la información médica y garantizar la continuidad de los servicios de salud.

En el ámbito técnico, se propone implementar cifrado de extremo a extremo y autenticación multifactor (MFA) para proteger el acceso a los sistemas y a los datos clínicos. Estas medidas ayudan a reducir significativamente el riesgo de accesos no autorizados y fortalecen la confidencialidad de la información de los pacientes. Asimismo, se recomienda el uso de firewalls de nueva generación, soluciones de protección para equipos finales y herramientas de monitoreo avanzado para detectar amenazas de forma más rápida y eficiente.

Desde la perspectiva administrativa, la matriz plantea fortalecer la gestión de riesgos relacionados con proveedores externos mediante contratos que incluyan requisitos mínimos de seguridad. Esto busca reducir los riesgos derivados de terceros y garantizar que las organizaciones que manejan información sensible mantengan niveles adecuados de protección.

A nivel operativo, se propone desarrollar programas permanentes de capacitación y concienciación en ciberseguridad dirigidos tanto al personal médico como administrativo. El objetivo es disminuir los errores humanos y promover buenas prácticas de seguridad en el uso diario de los sistemas de información.

La matriz también incorpora medidas estratégicas orientadas a facilitar la adopción de controles de seguridad en organizaciones con recursos limitados, especialmente pequeñas y medianas empresas del sector salud. Para ello, se plantea una guía de implementación escalable que permita aplicar las medidas de manera progresiva según las capacidades de cada institución.

Por último, se incluyen controles relacionados con la auditoría y el cumplimiento normativo. Se recomienda mantener registros automatizados e inalterables de las

actividades realizadas en los sistemas para garantizar la trazabilidad de la información. Además, se propone adoptar un modelo de madurez en ciberseguridad alineado con los requisitos regulatorios nacionales, promoviendo una mejora continua en la protección de datos personales y en el cumplimiento de la normativa vigente.

En resumen, la Tabla 9 muestra cómo solucionar las brechas identificadas en la Tabla 8, mediante controles técnicos, administrativos, operativos y estratégicos que permitan fortalecer la ciberseguridad y la protección de los datos de los pacientes en el sistema de salud costarricense.

Capítulo VI: Conclusiones

La revisión y el análisis de la información recopilada demostraron que los riesgos de seguridad digital en el sector salud costarricense varían según el tamaño y tipo de organización. Las instituciones públicas cuentan con estructuras más formalizadas y recursos para implementar controles técnicos, mientras que las privadas, especialmente las pequeñas y medianas, presentan mayores vulnerabilidades debido a la limitada asignación de presupuesto y falta de personal especializado. Esta disparidad confirma la necesidad de priorizar estrategias diferenciadas que fortalezcan los mecanismos de autenticación, respaldo de información y monitoreo continuo en las organizaciones con menor madurez digital.

La matriz de tratamiento de riesgos permitió identificar una serie de controles orientados a mitigar las vulnerabilidades detectadas en el sector salud costarricense. Entre las principales medidas propuestas destacan la implementación de mecanismos de protección técnica, como el cifrado de datos, la autenticación multifactor y herramientas avanzadas de monitoreo y detección de amenazas, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de la información clínica.

Asimismo, se concluye que la mejora de la ciberseguridad requiere un enfoque integral que combine controles técnicos, administrativos y operativos. En este sentido, resulta fundamental fortalecer la gestión de proveedores externos, promover programas permanentes de capacitación para el personal y establecer mecanismos de auditoría y cumplimiento normativo. Estas acciones, complementadas con una estrategia de implementación escalable, permitirán reducir los riesgos existentes y mejorar progresivamente la protección de los datos de los pacientes y la continuidad de los servicios de salud.

El estudio evidenció un cumplimiento parcial de las normas de protección de datos personales y de los marcos internacionales de seguridad. Aunque la Ley N.° 8968 se reconoce como una referencia obligatoria, su aplicación práctica sigue siendo inconsistente, especialmente en instituciones privadas que no poseen mecanismos formales de auditoría o certificación. En contraste, las organizaciones públicas muestran avances en políticas de seguridad y controles administrativos, pero aún enfrentan desafíos en la actualización tecnológica y la capacitación del personal. Se concluye que una estandarización progresiva, basada en marcos como ISO 27001, es fundamental para cerrar las brechas normativas existentes.

En conclusión, los resultados del proyecto reflejan la urgencia de fortalecer la ciberseguridad en los sistemas de salud digital costarricenses mediante estrategias integrales, colaborativas y sostenibles. El cumplimiento normativo, la educación digital y la implementación gradual de controles son pilares esenciales para garantizar la protección de los datos sensibles de los pacientes y consolidar la confianza en los servicios de salud.

Referencias bibliográficas

- Ochoa Chaves, L., Jimenez Alvarado, O., & Martínez de Lemos, F. (2023, julio). *Expediente Digital Único en Salud (EDUS) de Costa Rica: buenas prácticas, historia e implementación*. BID. Recuperado 15 de octubre de 2025, de https://publications.iadb.org/es/expediente-digital-unico-en-salud-edus-de-costa-rica-bue nas-practicas-historia-e-implementacion

- García, R. Q. (s. f.). *Profesionales de la salud se capacitarán en protección de datos*. Ministerio de Salud Costa Rica. https://www.ministeriodesalud.go.cr/index.php/prensa/61-noticias-2024/1906-profesional es-de-la-salud-se-capacitaran-en-proteccion-de-datos

- *Vista de La transformación digital de la Caja Costarricense de Seguro Social: más de una década de implementación del EDUS | Gestión en Salud y Seguridad Social*. (s. f.). https://www.binasss.sa.cr/ojssalud/index.php/gestion/article/view/211/417

- Yafimau, A. (2024, 31 octubre). *Prevenir lo prevenible: Uso del análisis predictivo en la atención sanitaria*. Innowise. https://innowise.com/es/blog/predictive-analytics-in-healthcare/

- *Cost of a data breach 2025 | IBM*. (s. f.). https://www.ibm.com/reports/data-breach

- Asamblea Legislativa de la República de Costa Rica. (2011). *Ley N.° 8968: Protección de la persona frente al tratamiento de sus datos personales*. La Gaceta N.° 170.

- Barrett, M. P. (2020, 27 enero). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecu rity-version-11

- Digital Health and Innovation (DHI). (2021, 18 agosto). *Global strategy on digital health 2020-2025*. https://www.who.int/publications/i/item/9789240020924

- *8 principios para la transformación digital del sector salud*. (s. f.). OPS/OMS | Organización Panamericana de la Salud. https://www.paho.org/es/sistemas-informacion-salud-digital/8-principios-para-transforma cion-digital-sector-salud

-*MICITT fortalece ciberseguridad en sector salud | Presidencia de la República de Costa Rica*. (2024, 5 abril). Presidencia de la Republica de Costa Rica. Recuperado 11 de noviembre

de 2025, de

https://www.presidencia.go.cr/noticias/micitt-fortalece-ciberseguridad-en-sector-salud

-*Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-412.* https://doi.org/10.1108/ICS-07-2018-0080

-*Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1),* 100080. https://doi.org/10.1016/j.jjimei.2022.100080

-*Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2024). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. Multidisciplinary Reviews, 6, 2023ss080.* https://doi.org/10.31893/multirev.2023ss080

-*Carlo Barbieri, Luca Neri, Stefano Stuard, Flavio Mari, José D Martín-Guerrero Clinical Kidney Journal, Volume 16, Issue 11, November 2023, Pages 1878–1884, https://doi.org/10.1093/ckj/sfad168*

-*Wright, J (2023). Healthcare cybersecurity and cybercrime supply chain risk management.*

Health Economics and Management Review, 4(4), 17-27.

https://doi.org/10.61093/hem.2023.4-02

-*Bonilla-Rodríguez, Esteban. (2015). Diseño de un plan de continuidad del negocio para el área de sostenimiento del departamento de facilidades en una empresa de manufactura de dispositivos médicos. Instituto Tecnológico de Costa Rica.* https://repositoriotec.tec.ac.cr/handle/2238/6375

-*Revelo Vallejo, Ericka. (2015). Crisis de la Caja Costarricense de Seguro Social (1981-1982): debate, actores y perspectivas. Universidad de Costa Rica.* https://repositoriotec.tec.ac.cr/handle/2238/6375

- Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2024, 3 de abril). *MICITT fortalece ciberseguridad en sector salud*. https://www.micitt.go.cr/el-sector-informa/micitt-fortalece-ciberseguridad-en-sector-salud

Anexos

Anexo 1

ESTUDIO 5 • RIESGO EN CADENA DE SUMINISTRO

Healthcare cybersecurity and cybercrime supply chain risk management

Cita en formato APA 7ª:
Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, 4(4), 17-27. https://doi.org/10.61093/hem.2023.4-02

Contexto del estudio:
El autor aborda una de las amenazas más complejas y actuales del sector salud a nivel internacional: el cibercrimen enfocado en la cadena de suministro (*Supply Chain Cyber-Risks*). Wright demuestra que los delincuentes rara vez atacan el firewall principal de un gran hospital; en su lugar, vulneran a los proveedores secundarios de software médico, plataformas de mantenimiento de equipos de soporte vital o servicios logísticos tercerizados. Al comprometer un eslabón débil, logran acceso total a las redes hospitalarias para desplegar ataques destructivos de *ransomware* y secuestro de expedientes clínicos.

VECTORES DE PROPAGACIÓN DEL RIESGO EN LA CADENA DE SUMINISTRO MÉDICA

Eslabón 1: Proveedores Externos (Software/Hardware Médico)
Terceros integrados con accesos remotos a la red interna del centro de salud para soporte de equipos o bases de datos compartidas.

Eslabón 2: Vector de Infiltración Transversal (Punto Débil)
Explotación de credenciales comprometidas o vulnerabilidades de día cero en herramientas de gestión de software de proveedores.

Eslabón 3: Impacto Crítico Final en el Núcleo Clínico
Despliegue de malware (Ransomware) en los sistemas internos del hospital, cifrando expedientes activos y deteniendo cirugías o consultas médicas.

ESTUDIO 4 • CONTROL TÉCNICO SANITARIO

Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales

Cita en formato APA 7ª:
Salazar-Lazo, C. D., & Avila-Correa, B. L. (2024). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. *593 Digital Publisher CEIT*, 9(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156

Contexto del estudio:
Este trabajo ofrece un enfoque técnico-operativo directo para el sector salud. Las autoras analizan la convergencia crítica entre la norma internacional de seguridad de la información **ISO/IEC 27001** y los estándares globales de interoperabilidad y comunicación de datos médicos **HL7 (Health Level Seven)**. Su meta es definir un marco de arquitectura tecnológica que neutralice las brechas físicas y lógicas que sufren los servidores clínicos y los expedientes electrónicos frente a los ataques informáticos avanzados.

MODELO DE BLINDAJE DE DATOS SANITARIOS (INTEROPERABILIDAD SEGURA)

Marco ISO/IEC 27001 (Seguridad Corporativa)

- Control estricto de accesos lógicos basados en perfiles clínicos.
- Cifrado simétrico de bases de datos de pacientes (en reposo y en tránsito).
- Auditoría automatizada de logs y transacciones del expediente electrónico.

Protocolos HL7 / FHIR (Interoperabilidad Médica)

- Estandarización del intercambio seguro de mensajes clínicos.
- Validación estructural de datos compartidos entre laboratorios y hospitales.
- Garantía de integridad y no repudio en la transmisión de telemedicina.

Anexo 2

ESTUDIO 4 • CONTROL TÉCNICO SANITARIO

Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales

Cita en formato APA 7ª:
Salazar-Lazo, C. D., & Avila-Correa, B. L. (2024). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. *593 Digital Publisher CEIT*, 9(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156

Contexto del estudio:
Este trabajo ofrece un enfoque técnico-operativo directo para el sector salud. Las autoras analizan la convergencia crítica entre la norma internacional de seguridad de la información **ISO/IEC 27001** y los estándares globales de interoperabilidad y comunicación de datos médicos **HL7 (Health Level Seven)**. Su meta es definir un marco de arquitectura tecnológica que neutralice las brechas físicas y lógicas que sufren los servidores clínicos y los expedientes electrónicos frente a los ataques informáticos avanzados.

MODELO DE BLINDAJE DE DATOS SANITARIOS (INTEROPERABILIDAD SEGURA)

Marco ISO/IEC 27001 (Seguridad Corporativa)

- Control estricto de accesos lógicos basados en perfiles clínicos.
- Cifrado simétrico de bases de datos de pacientes (en reposo y en tránsito).
- Auditoría automatizada de logs y transacciones del expediente electrónico.

Protocolos HL7 / FHIR (Interoperabilidad Médica)

- Estandarización del intercambio seguro de mensajes clínicos.
- Validación estructural de datos compartidos entre laboratorios y hospitales.
- Garantía de integridad y no repudio en la transmisión de telemedicina.