Universidad CENFOTEC

Escuela de Ciberseguridad

Tema:

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

Elaborado por:

Jimena María Azofeifa Porras

Fecha: Junio, 2026

Resumen

Este proyecto aborda la creciente problemática de ciberseguridad en el sector salud costarricense ante la falta de estudios comparativos entre organizaciones públicas y privadas de distintos tamaños. Mediante un enfoque descriptivo, correlacional y propositivo, y con base en una revisión sistemática de algunos estudios relacionados, se identificaron brechas significativas: el sector público muestra mayor madurez en seguridad, mientras que las instituciones privadas pequeñas presentan deficiencias por falta de capacitación, recursos limitados y baja percepción del riesgo. Como respuesta, se propone un modelo progresivo de implementación basado en estándares internacionales (ISO 27001) que combina medidas técnicas, educativas y organizacionales, permitiendo avanzar desde controles básicos hasta estrategias avanzadas de detección y recuperación. La investigación busca fortalecer la protección de datos de los pacientes y promover una cultura de seguridad digital sostenible, aportando una guía práctica para elevar la resiliencia cibernética del sector y mejorar la confianza, continuidad operativa y cumplimiento normativo.

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

Abstract

This research project addresses the growing cybersecurity problem in the Costa Rican healthcare sector, given the lack of comparative studies between public and private organizations of different sizes. Using a descriptive, correlational, and propositive approach, and based on a systematic review of related studies, significant gaps were identified: the public sector shows greater security maturity, while small private institutions exhibit deficiencies due to lack of training, limited resources, and low risk perception. In response, a progressive implementation model based on international standards (ISO 27001) is proposed, combining technical, educational, and organizational measures, allowing institutions to advance from basic controls to advanced detection and recovery strategies. The research aims to strengthen patient data protection and promote a sustainable digital security culture, providing a practical guide to enhance the sector's cyber resilience and improve trust, operational continuity, and regulatory compliance.

Keywords: Cybersecurity, Healthcare, Costa Rica, Data protection, ISO 27001, Vulnerabilities, Digital education, Cyber resilience, Risk management.

INTRODUCCIÓN

En los últimos años, Costa Rica ha experimentado una transformación significativa en su sistema de salud debido a la digitalización de los procesos clínicos y administrativos. La implementación de plataformas electrónicas y la interconexión entre instituciones públicas y privadas han permitido mejorar la gestión de la información médica, agilizar la atención a los pacientes y optimizar el uso de los recursos sanitarios. Herramientas como el Expediente Digital Único en Salud (EDUS) han facilitado el acceso a historiales clínicos, recetas y resultados de laboratorio, contribuyendo a una atención más eficiente, continua y segura para millones de personas en el país.

Sin embargo, este avance tecnológico también ha traído consigo nuevos desafíos relacionados con la seguridad de la información. La digitalización masiva de los datos clínicos ha incrementado la exposición a riesgos como accesos no autorizados, filtraciones de información y ciberataques, lo que puede afectar tanto la privacidad de los pacientes como la continuidad de los servicios médicos. En este contexto, la trazabilidad de los datos, es decir, la capacidad de registrar quién accede, modifica o consulta la información, se convierte en un elemento esencial para garantizar la transparencia, la auditoría y la confianza en los sistemas de salud digitales.

A nivel nacional, los incidentes de ciberseguridad registrados en los últimos años han evidenciado la vulnerabilidad de las instituciones públicas y privadas ante amenazas informáticas. Estos eventos, junto con el creciente número de denuncias por uso indebido de datos personales, demuestran la necesidad urgente de fortalecer las medidas de protección y los mecanismos de control en el manejo de la información sensible. Aunque Costa Rica cuenta con marcos legales como la Ley N.° 8968 para la protección de datos personales, su implementación efectiva dentro de las organizaciones de salud aún presenta importantes brechas.

Ante esta realidad, resulta fundamental analizar y comparar las prácticas de seguridad de la información en las diferentes organizaciones de salud del país, considerando sus características, recursos y niveles de madurez tecnológica. La adopción de estándares

internacionales, como la norma ISO/IEC 27001, puede ofrecer un marco estructurado para mejorar la protección de los datos clínicos y reducir los riesgos asociados a la digitalización.

Por ello, el presente estudio tiene como propósito evaluar los niveles de riesgo y las capacidades de protección de datos en organizaciones de salud costarricenses, con el fin de identificar vulnerabilidades, proponer lineamientos estratégicos y contribuir al fortalecimiento de la ciberseguridad en el sector sanitario. De esta manera, se busca asegurar que la transformación digital continúe siendo una herramienta que mejore la calidad de la atención médica sin comprometer la confidencialidad, integridad y disponibilidad de la información de los pacientes.

MÉTODO

El presente proyecto tiene como propósito evaluar comparativamente los niveles de riesgo y las capacidades de protección de datos en organizaciones de salud costarricenses, con el fin de proponer lineamientos estratégicos que fortalezcan la seguridad de la información. Debido a la naturaleza del problema y su orientación a la solución, la investigación se clasifica como investigación aplicada, ya que busca generar aportes prácticos directamente implementables en el sector salud.

El alcance de este 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.

Desde la dimensión epistemológica, la investigación se fundamenta en el análisis de la realidad organizacional mediante la recopilación de información a través de los documentos recopilados y revisión documental. Estos instrumentos permiten identificar patrones, evaluar el cumplimiento de normativas como la Ley N.° 8968 y analizar la adopción de estándares internacionales como ISO/IEC 27001.

En la dimensión axiológica, el estudio se orienta hacia la generación de valor mediante la identificación de buenas prácticas y la formulación de recomendaciones estratégicas. Se

prioriza el respeto por la confidencialidad, la ética en el manejo de la información y la protección de los derechos de los pacientes.

Desde la dimensión ontológica, el objeto de estudio se centra en los riesgos, amenazas y vulnerabilidades que afectan los sistemas de información en el sector salud, tales como accesos no autorizados, pérdida de datos, interrupciones en la disponibilidad de sistemas y ciberataques.

Asimismo, el desarrollo metodológico incorpora principios de Design Science Research (Ciencia del Diseño), lo que permite no solo analizar la situación actual, sino también proponer soluciones estructuradas basadas en evidencia. Este enfoque facilita la identificación de problemas, la definición de requerimientos y el diseño de propuestas alineadas con estándares internacionales.

Fases del proceso metodológico

El proceso de investigación se organiza en tres fases principales:

1. Fase de relevancia

En esta etapa se analiza el contexto de la ciberseguridad en el sector salud costarricense, incluyendo amenazas, marco legal y prácticas actuales. Esto permite definir el problema y justificar la investigación.

2. Fase de rigor

Se diseñan y aplican los instrumentos de recolección de datos, tales como encuestas, entrevistas y matrices de análisis documental. Además, se establecen criterios de evaluación basados en estándares como ISO 27001 para medir el nivel de madurez en seguridad de la información.

3. Fase de diseño

Se realiza el análisis comparativo de los datos recolectados, identificando brechas y oportunidades de mejora. A partir de estos resultados, se desarrollan recomendaciones estratégicas adaptadas al contexto costarricense.

Integración de tablas, figuras e ilustraciones en el método.

Como resultado del análisis de términos recurrentes, se generó la siguiente Figura.

Como parte del enfoque metodológico, se incorporan tablas, figuras e ilustraciones como herramientas clave para el análisis, organización e interpretación de la información.

Las tablas son utilizadas para estructurar y sistematizar los datos obtenidos en la revisión de literatura, permitiendo comparar estudios según variables como autores, año, tipo de investigación, área de estudio y principales hallazgos. Este proceso facilita la identificación de patrones y tendencias relevantes dentro del análisis comparativo.

Por otra parte, las figuras e ilustraciones cumplen una función analítica y explicativa, ya que permiten representar visualmente resultados derivados del proceso de investigación. Entre estas se incluyen evaluaciones de calidad de fuentes (como las clasificaciones de Scimago), modelos conceptuales y representaciones gráficas del análisis realizado.

En particular, herramientas visuales como la nube de palabras permiten identificar conceptos clave recurrentes en la literatura analizada, contribuyendo a la construcción del marco conceptual y al fortalecimiento del análisis cualitativo.

Todas las representaciones visuales utilizadas en el estudio han sido elaboradas a partir de los datos recolectados mediante los instrumentos definidos, asegurando coherencia entre la evidencia empírica y su representación gráfica.

En conjunto, el uso de estos recursos visuales fortalece la rigurosidad metodológica, mejora la claridad en la presentación de resultados y facilita la comprensión del análisis comparativo desarrollado.

Los resultados obtenidos se representan visualmente en las siguientes figuras:

Ilustración 1

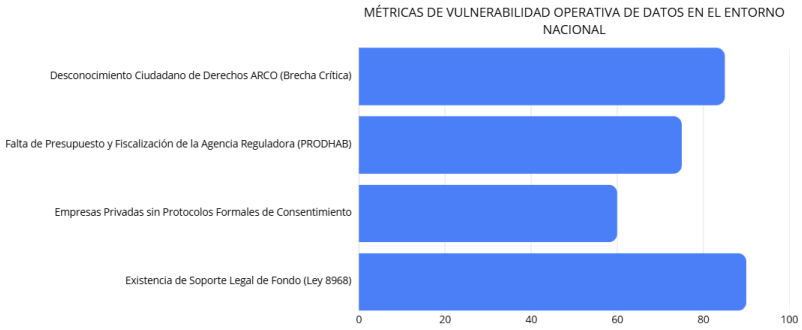

Figura 2. Métricas de vulnerabilidad operativa de datos en el entorno nacional

(Fuente: Elaboración propia con Canva)

Ilustración 1

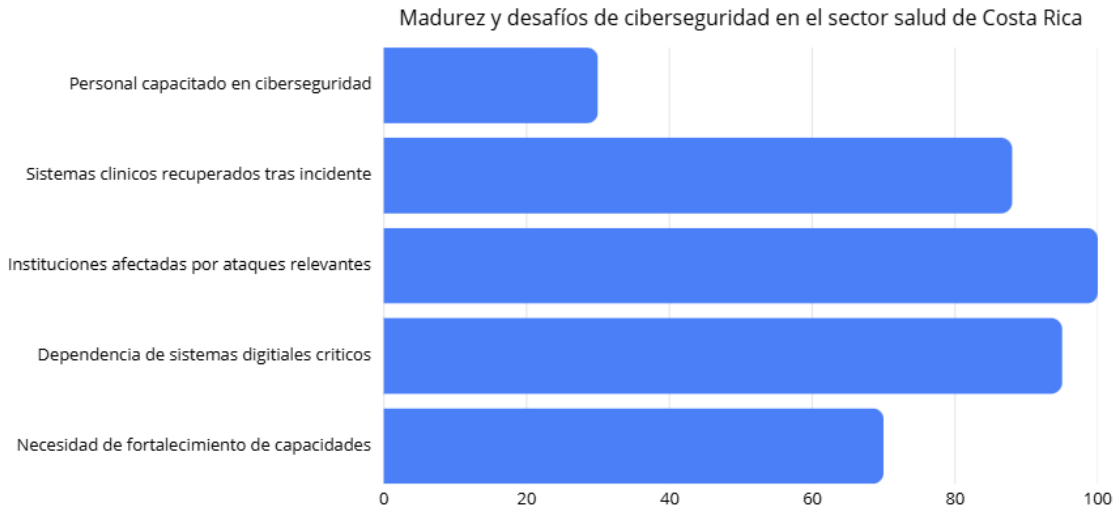

Ilustración 3

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.

La matriz de resultados evidencia que las principales vulnerabilidades del sector salud en Costa Rica están relacionadas con el acceso no autorizado a datos personales, los ciberataques, las debilidades de proveedores externos y la falta de capacitación en ciberseguridad. Estas amenazas afectan directamente la confidencialidad, integridad y disponibilidad de la información clínica, poniendo en riesgo tanto la privacidad de los pacientes como la continuidad de los servicios médicos. Casos como el ataque a la CCSS en 2022 demuestran el impacto que pueden tener estas vulnerabilidades sobre la operación de las instituciones de salud.

Asimismo, la matriz destaca la necesidad de fortalecer la seguridad mediante controles alineados con la norma ISO/IEC 27001. Entre las principales medidas propuestas se encuentran el uso de cifrado y autenticación multifactor, la implementación de herramientas avanzadas de protección contra amenazas, la gestión de riesgos en proveedores externos, la capacitación continua del personal y el fortalecimiento de los procesos de auditoría y cumplimiento normativo. Estas acciones permitirían reducir significativamente los riesgos de seguridad y avanzar hacia una mayor madurez en la protección de la información dentro del sector salud.

ANÁLISIS

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.

A continuación se detallan los resultados del análisis en las siguientes matrices:

Matriz de Diagnostico de o Brechas:

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 destaca que 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.

RESULTADOS

Los resultados obtenidos se detallan en la Matriz siguiente

Matriz de Tratamiento de Riesgos y Plan de Mitigación

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.
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.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
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.
Control Operativo	Institucionalizar programas progresivos de concienciación en ciberseguridad (*Security Awareness*).	Adopción de prácticas seguras adaptadas a las particularidades del personal médico y administrativo.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
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.
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.

Categoría del Control	Acción de Mitigación Propuesta (Optimizada)	Resultado Esperado / Métrica
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.

CONCLUSIONES

El análisis comparativo demostró 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.

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.

El plan de implementación propuesto ofrece una hoja de ruta práctica y

adaptable a las capacidades de cada institución. Su enfoque escalonado que combina controles técnicos, estrategias educativas y mecanismos de gobernanza permite una adopción gradual sin comprometer la operatividad del sector salud. Este modelo reconoce las diferencias entre organizaciones y propone un sistema de mejora continúa sustentado en indicadores de madurez, comités de ciberseguridad y procesos de capacitación continua. En conjunto, se establece una base sólida para fortalecer la resiliencia del ecosistema sanitario nacional frente a amenazas cibernéticas.

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.

Bibliografía

Alfaro, J. M. (2022). *Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia.*

Cordero, Z. R. (2009). La investigación aplicada: una forma de conocer las realidades con evidencia científica. *Revista educación*.

Fatima, m. (3 de abril de 2023). *Los 12 métodos más comunes para el análisis de datos.* Obtenido de linkedin: https://es.linkedin.com/pulse/los-12-m%C3%A9todos-m%C3%A1s-comunes-para-el-an%C3%A1lisis-de-datos-fatima-barrera

Glassdoor. (2008-2004). *Glassdoor*. Obtenido de Glassdoor: https://www.glassdoor.com

González, W. J. (2007). *Las ciencias de diseño: racionalidad limitada, predicción y prescripción.* Netbiblo.

Gorman, B. (14 de July de 2023). *Distintos tipos de hackers: sombreros blancos, negros, grises, etc.* Obtenido de AVG: https://www.avg.com/es/signal/types-of-hackers

Hewlett Packard Enterprise. (2024). *HPE Glossary*. Obtenido de ¿Qué es el acceso remoto?: https://www.hpe.com/lamerica/es/what-is/remote-access.html

IBM. (2023). *IBM*. Obtenido de ¿Qué es un sistema de detección de intrusiones (IDS)?: https://www.ibm.com/mx-es/topics/intrusion-detection-system

Real Academia Española. (2019). *Diccionario del estudiante*. Obtenido de Real Academia Española: https://www.rae.es/diccionario-estudiante/intruso

Red Hat. (27 de Setiembre de 2023). *¿Qué son los sistemas de detección y prevención de intrusos (IDPS)?* Obtenido de Red Hat: https://www.redhat.com/es/topics/security/what-is-an-IDPS

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarret, D. S., Álava Cruzatty, J. E., Parrales Anzúle, G. R., Álava Mero, J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades vol 46.* 3Cienacias.

Tuteja, A. (18 de agosto de 2024). *Cómo pueden las pymes convertir el riesgo de ciberseguridad en una oportunidad*. Obtenido de World Economic Forum: https://es.weforum.org/stories/2024/08/las-pymes-pueden-convertir-el-riesgo-de-ciberseguridad-en-una-oportunidad-como-hacerlo/

Ubunto. (2019). *Ubunto manuals*. Obtenido de https://manpages.ubuntu.com