Resistances
Journal of the Philosophy of History

Confidencialidad en las historias clínicas digitales, análisis de la ley orgánica de protección de datos personales, Ecuador

Confidentiality in digital medical records, analysis of the personal data protection law, Ecuador

Flavio David Ramírez Ortega, Jaime Arturo Moreno Martínez

Resumen

El objetivo general de esta investigación es analizar la confidencialidad de las historias clínicas digitales en Ecuador en relación con la Ley de Protección de Datos Personales. La técnica utilizada es documental con un enfoque cualitativo, lo que posibilita analizar en detalle el acatamiento de las regulaciones y las prácticas vigentes en la salvaguarda de la información médica. Los hallazgos indican que, pese a los progresos en la ley, aún existen vulnerabilidades en el sistema, tales como la utilización de contraseñas insuficientes y la ausencia de autenticación multifactorial, lo que pone en peligro la información de los pacientes ante accesos no permitidos. En el debate, se resalta la importancia de incorporar tecnologías de seguridad de vanguardia y de formar de forma constante al personal sanitario para potenciar la salvaguarda de la información. Las conclusiones resaltan la relevancia de establecer una cultura organizacional que aprecie la privacidad del paciente, además del acatamiento efectivo de la ley a través de acciones tecnológicas y educativas para proteger la información médica en el entorno ecuatoriano.

Palabras clave: historias clínicas digitales; Confidencialidad; Ley de protección de datos; Sistema de salud; investigación

Flavio David Ramírez Ortega
Universidad Católica de Cuenca | Cuenca | Ecuador | flavio.ramirez.64@est.ucacue.edu.ec
https://orcid.org/0009-0004-7420-0029
Jaime Arturo Moreno Martínez
Universidad Católica de Cuenca | Cuenca | Ecuador | jaime.moreno@ucacue.edu.ec
http://orcid.org/0000-0001-8836-3524

http://doi.org/10.46652/resistances.v5i10.179
ISSN 2737-6230
Vol. 5 No. 10 julio-diciembre 2024, e240179
Quito, Ecuador

Enviado: septiembre, 11, 2024
Aceptado: noviembre, 26, 2024
Publicado: diciembre, 23, 2024
Publicación Continua

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

The general objective of this research is to analyze the confidentiality of digital medical records in Ecuador in relation to the Personal Data Protection Law. The technique used is documentary with a qualitative approach, which makes it possible to analyze in detail the compliance with regulations and current practices in the safeguarding of medical information. The findings indicate that, despite progress in the law, there are still vulnerabilities in the system, such as the use of insufficient passwords and the absence of multifactor authentication, which endangers patient information in the event of unauthorized access. In the debate, the importance of incorporating state-of-the-art security technologies and of constantly training healthcare personnel to enhance the safeguarding of information was highlighted. The conclusions highlight the relevance of establishing an organizational culture that appreciates patient privacy, in addition to effective compliance with the law through technological and educational actions to protect medical information in the Ecuadorian environment.
Keywords: Digital medical records; Confidentiality; Data protection law; Health system; Research

Introducción

En los sistemas sanitarios actuales, la digitalización de los expedientes clínicos ha representado un progreso considerable en cuanto a accesibilidad y eficacia en la asistencia sanitaria. No obstante, este avance ha planteado significativos retos vinculados con la salvaguarda de la privacidad de los pacientes y la privacidad de la información médica. En Ecuador, la Ley Orgánica de Protección de Datos Personales establece un marco regulatorio para asegurar la protección de los datos personales, sin embargo, su efectiva aplicación se topa con múltiples obstáculos tecnológicos, organizativos y humanos. Estos retos, unidos a una creciente necesidad de sistemas digitales, requieren un análisis crítico de las prácticas vigentes para detectar áreas de mejora y asegurar que los derechos esenciales de los pacientes sean respetados en todo momento (La Ley Orgánica de Protección de Datos Personales de Ecuador, 2021).

La privacidad de la información médica es un elemento crucial para mantener la relación de confianza entre los pacientes y las instituciones sanitarias. No obstante, varias investigaciones han demostrado que las instituciones de Ecuador muestran vulnerabilidades importantes en la administración de estos datos. Por ejemplo, la utilización de contraseñas débiles y la ausencia de autenticación multifactorial son costumbres habituales que promueven accesos no autorizados y exponen datos delicados a peligros superfluos. Estas deficiencias no solo ponen en riesgo la privacidad del paciente, sino que también producen un efecto adverso en la visión pública sobre la seguridad del sistema de salud (Salazar y Avila, 2023). Igualmente, la escasa formación del personal de salud en prácticas de ciberseguridad incrementa estos riesgos, evidenciando la imperiosa necesidad de establecer programas de capacitación que traten estas carencias.

También se perciben desigualdades en la aplicación de medidas de seguridad entre el sector público y el sector privado. Aunque algunas clínicas privadas han implementado tecnologías de vanguardia, como sistemas de encriptación y controles de acceso rigurosos, los hospitales públicos

se encuentran con limitaciones presupuestarias que restringen su habilidad para actualizar sus infraestructuras. Esto resulta en una mayor vulnerabilidad a las brechas de seguridad, particularmente en contextos donde los medios tecnológicos no alcanzan para cumplir con las demandas de la legislación actual (Martínez y Pérez, 2022). En este contexto, resulta imprescindible investigar soluciones que posibiliten un acceso equitativo a las tecnologías de protección de datos, destacando la seguridad de la información médica como un factor crucial en la provisión de servicios de alta calidad.

La Ley Orgánica de Protección de Datos Personales representa un progreso importante en la normativa de la gestión de información personal en Ecuador. No obstante, la literatura muestra que su uso ha sido inequitativo y, en ciertas situaciones, superficial. Investigaciones anteriores han indicado que la carencia de una supervisión eficaz y la falta de auditorías periódicas restringen la habilidad de las instituciones para acatar las normas legales. Por ejemplo, Alegre et al. (2024), enfatizan que naciones que han instaurado sistemas de vigilancia integral han conseguido disminuir significativamente las violaciones a la seguridad, subrayando la relevancia de fusionar acciones tecnológicas con políticas organizativas robustas.

Además, los peligros vinculados a la insuficiente protección de las historias clínicas digitales no se restringen solamente al campo jurídico. Hay consecuencias éticas que se deben tener en cuenta, dado que cualquier infracción a la privacidad de la información puede poner en riesgo la dignidad y la privacidad de los pacientes. Esto resalta la importancia de adoptar una visión multidimensional en la administración de la información médica, fusionando valores éticos con el uso de tecnologías de vanguardia, como el cifrado AES-256 y la autenticación multifactorial, que han probado su eficacia en prevenir accesos no permitidos (Keshta & Odeh, 2021).

Por otro lado, la capacitación constante del personal de salud se presenta como un elemento esencial para asegurar la adecuada implementación de las regulaciones de protección de datos. Investigaciones actuales subrayan que la formación constante puede potenciar de manera significativa el entendimiento y uso de las leyes, promoviendo una cultura organizacional que considere la privacidad de los pacientes como una prioridad. Sin embargo, se ha notado que las entidades públicas muestran más deficiencias en este campo, lo que subraya la importancia de implementar programas de capacitación específicos que traten estas desigualdades y fomenten la observancia de las normativas en todos los estratos del sistema sanitario (Zúñiga & Martínez, 2019).

En este marco, el objetivo de este estudio es examinar a fondo las condiciones actuales de privacidad de los historiales clínicos digitales en Ecuador, reconociendo los riesgos más significativos y sugiriendo soluciones factibles para su reducción. La razón de este análisis se basa en la imperiosa necesidad de armonizar las prácticas vigentes con las normativas legales, asegurando no solo la protección de la información médica, sino también el incremento de la confianza en el sistema de

salud. La relevancia de este asunto va más allá del campo tecnológico, dado que abarca elementos éticos, jurídicos y organizativos que resultan cruciales para asegurar un cuidado médico de alta calidad en un contexto digital.

En este contexto, este estudio propone la hipótesis de que la adecuada aplicación de la Ley Orgánica de Protección de Datos Personales en Ecuador, respaldada en la utilización de tecnologías de ciberseguridad de vanguardia y en la formación constante del personal de salud, posibilitará disminuir considerablemente los peligros vinculados a la vulnerabilidad de los registros clínicos digitales. No solo potenciará la protección de la información, sino que también reforzará la credibilidad de los pacientes en el sistema sanitario.

Para tratar este problema, se plantean las siguientes cuestiones de investigación, dirigidas a orientar el progreso del estudio y afrontar los retos propuestos:

1. ¿Cuáles son los riesgos tecnológicos, organizativos y jurídicos más significativos a los que se enfrentan las instituciones sanitarias en Ecuador para salvaguardar las historias clínicas digitales?

2. ¿Hasta qué punto la puesta en marcha de la Ley Orgánica de Protección de Datos Personales ha optimizado la administración de la información médica en Ecuador?

3. ¿Qué elementos favorecen la vulnerabilidad de la información médica digital en centros hospitalarios públicos y privados?

4. ¿De qué manera la formación del personal de salud influye en la implementación de medidas de salvaguarda de datos en el contexto clínico?

5. ¿Cuáles son las tecnologías de ciberseguridad más eficaces para proteger la privacidad de los historiales clínicos digitales en el escenario ecuatoriano?

Antecedentes de investigación

La protección de la información médica digital surge como un asunto crucial en la administración de los sistemas sanitarios actuales, especialmente en situaciones donde la digitalización progresa rápidamente. En Ecuador, gestionar correctamente las historias clínicas electrónicas representa un reto crucial, dado que no solo requiere asegurar la privacidad de los datos médicos, sino también lidiar con las debilidades resultantes de una implementación deficiente de medidas de seguridad tecnológica. Redrobán (2023), resalta que la pandemia de COVID-19 impulsó de manera notable la implementación de instrumentos digitales en el sistema de salud de Ecuador, lo que, consecuentemente, aumentó la vulnerabilidad de los datos médicos a potenciales infracciones

de privacidad. Este suceso evidenció las deficiencias en las políticas de ciberseguridad, poniendo de manifiesto la necesidad de un enfoque más completo y sólido para salvaguardar la información delicada.

El análisis destaca la disparidad en la aplicación de medidas de seguridad entre los sectores público y privado. Martínez y Pérez (2022), indican que, pese a que la Ley Orgánica de Protección de Datos Personales proporciona directrices precisas, la escasez de recursos en los hospitales públicos restringe su habilidad para incorporar tecnologías de vanguardia como sistemas de encriptación y autenticación multifactorial. En cambio, las clínicas privadas, al disponer de más recursos económicos, han conseguido establecer infraestructuras tecnológicas más sólidas que aseguran un nivel elevado de seguridad en la gestión de la información médica. Esta desigualdad provoca un ambiente de vulnerabilidad en el sector público, impactando directamente en la confianza de los pacientes en el sistema de salud.

En el contexto global, la implementación de normas de ciberseguridad como la ISO/IEC 27002 ha probado ser eficaz para reducir los riesgos vinculados a la gestión de datos médicos. Salazar y Avila (2023), sostienen que, en naciones como Chile y Colombia, la puesta en marcha de dichas regulaciones ha facilitado una notable disminución de incidentes de acceso no permitido. Este modelo podría ajustarse al entorno de Ecuador, donde las entidades de salud todavía se encuentran con retos significativos en cuanto a infraestructura tecnológica y supervisión. La conformidad con normas internacionales no solo incrementaría la protección de la información médica, sino que también potenciaría la interoperabilidad entre sistemas, un elemento crucial en la administración contemporánea de la información de salud.

Además, los peligros éticos y jurídicos vinculados a la gestión de historias clínicas digitales son elementos esenciales que necesitan un enfoque prioritario. Alegre et al. (2024), indican que las violaciones a la privacidad médica no solo implican penalizaciones jurídicas, sino que también afectan de manera significativa la relación de confianza entre los pacientes y los centros de salud. Para Ecuador, este problema es especialmente significativo, dado que la sensación pública de inseguridad en la gestión de datos médicos podría neutralizar los progresos alcanzados en la digitalización del sistema de salud. Por esta razón, es crucial que las entidades se esfuercen en asegurar la salvaguarda de los datos a través de acciones específicas y transparentes.

Otro aspecto crucial detectado es la ausencia de formación en ciberseguridad entre los expertos sanitarios. Zúñiga y Martínez (2019), subrayan que numerosas instituciones de salud de Ecuador carecen de programas de capacitación continua para su personal, lo que resulta en comportamientos inapropiados como la utilización de contraseñas poco seguras o la ausencia de conocimiento sobre protocolos fundamentales de seguridad. Esta circunstancia no solo incrementa la vulnerabilidad de los sistemas de información, sino que también amenaza la integridad de la información médica. La puesta en marcha de programas de formación estructurados y constantes

podría ser una estrategia eficaz para disminuir estas deficiencias y promover una cultura organizacional que valore la protección de la información.

La literatura también resalta la relevancia de llevar a cabo auditorías periódicas y supervisiones eficaces para asegurar el acatamiento de las regulaciones vigentes. Redrobán (2023), subraya que, pese a que la Ley Orgánica de Protección de Datos Personales impone sanciones a las entidades que violan la legislación, la ausencia de mecanismos de control restringe su eficacia. En este contexto, resulta esencial que las entidades sanitarias implementen una política proactiva que fusiona acciones tecnológicas, programas de formación y auditorías regulares para asegurar una correcta administración de los datos médicos.

Así mismo, tener en cuenta las soluciones tecnológicas y organizativas, es imprescindible tener en cuenta el rol de los pacientes en la administración de su información médica. De acuerdo con Condori (2024), un incremento en la implicación de los pacientes en la gestión de sus datos podría aportar de manera significativa a robustecer la seguridad de los sistemas. Esto abarca tácticas como brindar a los pacientes acceso a sus historiales médicos y sensibilizarlos acerca de la relevancia de salvaguardar su privacidad. La participación de los pacientes en este procedimiento no solo incrementa la claridad, sino que también promueve un sentimiento de responsabilidad compartida en la salvaguarda de la información médica.

Metodología

Tipo de investigación

Este estudio utiliza un enfoque documental cualitativo, diseñado para examinar en detalle la privacidad de los datos médicos digitales en el marco de la Ley Orgánica de Protección de Datos Personales en Ecuador. Este método posibilita examinar de manera sistemática las prácticas vigentes de protección de datos y valorar el marco regulatorio correspondiente, empleando instrumentos de análisis exhaustivos que ofrecen un marco robusto para la interpretación de la información recolectada.

Criterios de Inclusión, Fuentes de Información y Universo

Para asegurar la estricta realización del análisis, se establecieron criterios concretos de inclusión y exclusión que orientaron la elección de recursos. Los artículos presentados fueron publicados desde 2018 hasta 2024, dando prioridad a investigaciones vinculadas a la ciberseguridad en la administración de datos médicos, análisis de leyes y análisis de casos vinculados al sector de la salud en Ecuador y naciones con situaciones parecidas. Se descartaron fuentes que no tuvieran una

relación directa con el tema de estudio o que no satisficieran los criterios de calidad académica, como revisiones no arbitradas o publicaciones sin un respaldo bibliográfico apropiado.

El grupo de estudio contempló artículos e investigaciones accesibles en bases de datos académicas internacionales prestigiosas, como Scopus, SciELO entre otras, además de documentos jurídicos y regulaciones pertinentes. Para obtener estos datos, se emplearon términos como "confidencialidad médica", "ciberseguridad en salud", "datos médicos digitales" y "Ley Orgánica de Protección de Datos Ecuador", tanto en idioma inglés como español. Esto posibilitó llevar a cabo una investigación detallada y adquirir un panorama extenso de los progresos y retos en la salvaguarda de la información médica digital.

Estrategias de Análisis y Validez de los Resultados

El estudio se organizó en tres etapas

Etapa inicial: Se llevó a cabo una revisión exhaustiva de los documentos escogidos para detectar asuntos fundamentales, como los riesgos vinculados a la gestión de datos médicos y tácticas para reducirlos

Segunda etapa: Se implementaron matrices de sistematización para ordenar la información de acuerdo con categorías establecidas previamente: marco regulatorio, retos tecnológicos, repercusión organizacional y capacitación del personal

Tercera Etapa: Se realizó un análisis interpretativo para establecer vínculos entre los descubrimientos y las cuestiones de investigación, lo que posibilitó la generación de conclusiones sólidas y consistentes con los propósitos del estudio

Para asegurar la validez y confiabilidad de los hallazgos, se implementaron normas como la triangulación metodológica, fusionando datos teóricos con investigaciones empíricas y regulaciones. Esta metodología facilitó la comparación de puntos de vista y mejoró la comprensión de los datos, garantizando una perspectiva completa del problema en estudio (Burgos et al., 2019).

Resultados

Marco normativo

La legislación en vigor en Ecuador para salvaguardar la información médica, especialmente la Ley Orgánica de Protección de Datos Personales (LOPDP), proporciona un fundamento só-

lido para asegurar la privacidad de los datos en el sector de la salud. Dentro de sus normativas fundamentales se encuentran la clasificación de datos delicados y la exigencia de poner en marcha acciones técnicas y organizativas que garanticen la privacidad y protección de la información personal (La Ley Orgánica de Protección de Datos Personales de Ecuador, 2021). No obstante, el estudio de esta regulación revela fortalezas y debilidades que inciden en su aplicación eficaz en las instituciones sanitarias.

Una de las mayores ventajas de la LOPDP radica en su concordancia con normas internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en lo que respecta a la definición de datos delicados, necesidades de consentimiento informado y obligaciones de los responsables de la gestión de datos (Ochoa et al., 2024). Esto garantiza que la legislación de Ecuador se ajuste a las mejores prácticas internacionales en relación con la salvaguarda de la información personal. Además, la instauración de una Superintendencia de Protección de Datos robustece el marco institucional para supervisar la observancia de estas normativas, proporcionando un medio para administrar incidentes vinculados a la privacidad de los datos (Salazar y Avila, 2023).

Sin embargo, la puesta en marcha de la ley se topa con retos considerables, particularmente en el sector público. La escasez de recursos financieros y tecnológicos restringe la habilidad de los hospitales y centros sanitarios públicos para implementar estrategias de seguridad sólidas, tales como el encriptado sofisticado de datos y la verificación multifactorial (Zúñiga & Martínez, 2019). Además, la falta de auditorías periódicas y programas de formación específicos para el personal de salud complica el cumplimiento de las regulaciones, dejando a numerosas instituciones vulnerables ante accesos no permitidos y la pérdida de datos.

La observancia de las regulaciones también fluctúa significativamente entre entidades del sector público y privado. Aunque las clínicas privadas han implementado políticas rigurosas de administración de datos que comprenden controles de acceso, seguimiento de actividades y almacenamiento seguro, los hospitales públicos tienden a funcionar con acciones más elementales y menos eficientes (Salazar y Avila, 2023). Este desbalance no solo perjudica la seguridad de los datos médicos, sino que también aumenta la posibilidad de penalizaciones legales y la pérdida de la confianza de los pacientes.

Otro factor importante es la visión del personal de salud acerca de la ley y su aplicación. Los hallazgos de sondeos efectuados sobre el tema indican que, pese a que la mayoría de los empleados están al tanto de la normativa, escasos son quienes entienden completamente sus consecuencias prácticas (Ochoa et al., 2024). Esto resalta la importancia de programas de capacitación continua que instruyan sobre cómo aplicar medidas de seguridad en sus labores cotidianas, además de las repercusiones legales de no acatar las estipulaciones de la LOPDP.

El marco legal ecuatoriano ofrece una estructura jurídica apropiada para la salvaguarda de la información médica, aunque su efectividad se basa en su aplicación práctica en todos los estratos del sistema sanitario. Para tratar estas falencias, es vital que las entidades den prioridad a la inversión en tecnologías de seguridad, la elaboración de políticas organizativas definidas y la formación del personal. Solo mediante estas acciones podremos asegurar la privacidad de los datos médicos y adherirnos a los estándares fijados en la legislación.

Vulnerabilidades tecnológicas en la gestión de datos médicos digitales.

En Ecuador, la administración de datos médicos digitales se topa con varias debilidades tecnológicas que ponen en riesgo la privacidad y protección de los datos de los pacientes. Entre las principales carencias se incluyen la utilización de contraseñas frágiles, la ausencia de autenticación multifactorial y la implementación restringida de sistemas de encriptación sólidos. Estas fallas incrementan considerablemente el peligro de accesos no permitidos, modificación de datos delicados y pérdida de información (Zúñiga & Martínez, 2019).

Además, el sector público se topa con más obstáculos en la implementación de tecnologías de seguridad de vanguardia debido a restricciones en el presupuesto. Por otro lado, ciertas entidades privadas han progresado en la instauración de sistemas de administración de identidades y cifrado de datos acorde a normas internacionales, aunque estas prácticas no son homogéneas en todo el sector (Ochoa et al., 2024).

Otro aspecto crucial detectado es la falta de auditorías periódicas de los sistemas tecnológicos, lo que dificulta la detección proactiva de vulnerabilidades. El estudio de (La Ley Orgánica de Protección de Datos Personales de Ecuador, 2021) indica la importancia de llevar a cabo auditorías regulares para asegurar el acatamiento de las normativas, no obstante, la ausencia de supervisión restringe la eficacia de estas leyes en la realidad. Esto expone a numerosas instituciones a peligros de ciberseguridad, tales como malware y accesos no autorizados, que pueden poner en riesgo seriamente la privacidad de los pacientes.

Respecto a los procedimientos de backup de datos, los sistemas de respaldo en numerosas instituciones públicas son deficientes, lo que podría resultar en la pérdida de datos esenciales en caso de errores del sistema. Pese a que ciertas entidades privadas poseen políticas de respaldo y recuperación de datos más sofisticadas, todavía existen posibilidades de optimización en la administración global de la seguridad de la información (Salazar y Avila, 2023).

Las debilidades tecnológicas en la administración de datos médicos digitales en Ecuador evidencian la imperiosa necesidad de perfeccionar las políticas de seguridad, poner en práctica tecnologías de vanguardia y realizar auditorías periódicas para reducir los peligros y asegurar la salvaguarda de la información médica.

Prácticas organizativas y la capacitación del personal sanitario respecto al manejo de datos médicos.

En el estudio de las prácticas y la formación del personal de salud en relación con la gestión de datos médicos, se mostró una gran disparidad entre las entidades del sector público y privado en Ecuador. Estas discrepancias afectan directamente la seguridad de los datos médicos y evidencian la imperiosa necesidad de implementar políticas organizativas más sólidas que den prioridad a la capacitación constante del personal. Se ha reconocido la formación como un elemento crucial para disminuir los riesgos vinculados a la manipulación de datos delicados, no obstante, su aplicación es restringida y desequilibrada (Zúñiga & Martínez, 2019).

En el sector público, una proporción considerable de las entidades carece de programas de formación constante en ciberseguridad. Este déficit educativo se refleja en acciones incorrectas, como la utilización de contraseñas poco fiables, el acceso compartido a sistemas de información y la ignorancia sobre los peligros vinculados a las infracciones a la información médica. Por otro lado, las clínicas privadas han demostrado un mayor interés en la capacitación del personal, lo cual se manifiesta en una adopción más eficiente de medidas de seguridad como la autenticación multifactorial y la supervisión de accesos (Salazar y Avila, 2023).

La información recolectada señala que menos del 30% de los hospitales públicos brindan seminarios o talleres centrados en la gestión segura de la información médica. En contraparte, más del 60% de las clínicas privadas llevan a cabo formación constante, lo que aporta de manera significativa a la reducción de errores humanos vinculados a la seguridad de la información (Ochoa et al., 2024). Estas cifras resaltan la desigualdad entre ambos sectores y subrayan la necesidad de implementar políticas estandarizadas a escala nacional que fomenten la formación constante como un elemento crucial para la seguridad de la información.

Además, es claro el efecto de estas formaciones en la protección de los datos en las instituciones que han dado prioridad a este tema. Las entidades que cuentan con programas de capacitación regulares han reportado una disminución del 40% en incidentes vinculados a accesos no permitidos y pérdida de datos sensibles. En gran parte, esto se debe a que una formación apropiada aumenta la conciencia del personal acerca de la relevancia de poner en práctica medidas preventivas como la utilización de contraseñas complejas, el encriptado de datos y la administración de accesos basada en roles.

Otro descubrimiento significativo es la falta de políticas definidas que incorporen la formación como un elemento esencial en las estrategias organizativas de numerosas instituciones públicas. La ausencia de auditorías periódicas y sistemas de valoración de habilidades empeora esta circunstancia, complicando la supervisión del efecto de los programas de capacitación actuales. Esta debilidad organizacional no solo pone en riesgo la privacidad de los datos médicos, sino que

también pone a las instituciones en peligro de enfrentar posibles castigos legales por violar la Ley Orgánica de Protección de Datos Personales

Por otro lado, las entidades privadas que incorporan políticas organizativas acordes a normas internacionales, como la ISO/IEC 27002, han demostrado resultados más favorables en cuanto a la observancia de las normas y el manejo seguro de datos. Estas entidades no solo proporcionan formación técnica, sino que también llevan a cabo simulacros y evaluaciones regulares para asegurar que el equipo esté capacitado para gestionar incidentes de seguridad. Estas prácticas constituyen un patrón a seguir que el sector público podría ajustar para incrementar la protección de los datos médicos en la nación (Salazar y Avila, 2023).

En el ámbito organizacional, se notó que las entidades que fomentan una cultura de seguridad de la información exhiben índices de vulnerabilidad más bajos. Esto abarca no solo la formación técnica, sino también la concienciación del personal acerca de la relevancia de la privacidad y las repercusiones jurídicas de las infracciones de la información. Una sólida cultura organizacional facilita que la protección de la información sea vista como una obligación conjunta por todos los trabajadores, sin importar su posición en la institución.

Los descubrimientos subrayan la relevancia de robustecer las prácticas organizativas y la formación del personal de salud en la gestión de datos médicos. La desigualdad detectada entre los sectores público y privado pone de manifiesto la necesidad de una intervención del gobierno que impulse políticas estandarizadas, auditorías periódicas y programas de capacitación obligatoria. Estas medidas son fundamentales para asegurar la salvaguarda eficaz de los datos médicos y el acatamiento de las regulaciones vigentes**.**

Discusión

El debate sobre los hallazgos logrados en esta investigación subraya la relevancia de examinar de manera crítica la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en el escenario ecuatoriano, valorando tanto sus progresos como las áreas que necesitan reforzamiento. El marco legal es robusto en su estructura, acorde con normas globales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, lo que sitúa a Ecuador como una nación con leyes de vanguardia en el ámbito de la privacidad de datos (La Ley Orgánica de Protección de Datos Personales de Ecuador , 2021). No obstante, su implementación muestra diferencias notables entre los sectores público y privado, lo que pone en riesgo la protección homogénea de los datos médicos digitales en la nación.

Uno de los descubrimientos fundamentales es la desigualdad en la puesta en marcha de medidas de seguridad tecnológica entre ambos ámbitos. Aunque las clínicas privadas han progresado en la implementación de prácticas como la autenticación multifactorial y la encriptación de datos,

los hospitales públicos se encuentran con graves restricciones debido a limitaciones presupuestarias y escasez de formación del personal (Salazar y Avila, 2023). Este desbalance no solo amenaza la privacidad de los pacientes en el sector público, sino que también provoca una visión desfavorable acerca de la capacidad del sistema sanitario para asegurar la privacidad de la información delicada.

Desde una perspectiva legal, el artículo 15 de la LOPDP resalta la necesidad de establecer acciones técnicas y organizativas apropiadas para asegurar la protección de la información personal. No obstante, los hallazgos muestran que la ausencia de auditorías regulares y sistemas de supervisión eficaces restringe la habilidad de las instituciones para acatar este mandato. Esta desigualdad evidencia la exigencia de políticas más estrictas que contemplen sanciones pertinentes y estrategias de mejora constante para minimizar las carencias presentes (Martínez y Pérez, 2022).

El estudio también demuestra que las prácticas organizativas son esenciales para el acatamiento de las regulaciones. Las entidades que han puesto en marcha políticas de organización claras y programas de capacitación continua han demostrado una reducción considerable en los incidentes relacionados con seguridad. Este descubrimiento resalta la relevancia de promover una cultura organizacional enfocada en la seguridad de la información, conforme a lo dictado en el artículo 14 de la LOPDP, que requiere que los encargados del manejo de datos aseguren su salvaguarda a través de una correcta administración de riesgos (Ochoa et al., 2024).

Además, se reconoce como una de las principales falencias en el sistema la ausencia de formación constante del personal de salud. De acuerdo con los datos estudiados, menos del 30% de las entidades públicas brindan capacitación constante en seguridad de datos, en cambio, más del 60% de las clínicas privadas poseen programas de formación estructurados (Zúñiga & Martínez, 2019). Este aspecto subraya la importancia de implementar regulaciones que fuercen a todas las entidades, sin importar su ámbito, a incorporar programas de capacitación regular como requisito esencial para su funcionamiento.

Desde un punto de vista ético, la insuficiente salvaguarda de la información médica pone en riesgo no solo la privacidad de los pacientes, sino también su dignidad y su confianza en el sistema sanitario. Las infracciones a la privacidad pueden conllevar consecuencias legales y emocionales para los pacientes, impactando su voluntad para divulgar datos médicos esenciales (Alegre et al., 2024). Así pues, es vital que las entidades adopten una actitud proactiva para salvaguardar los datos, implementando tecnologías de vanguardia y robusteciendo las políticas de acceso y seguimiento de la información.

En cambio, la incorporación de normas internacionales como la ISO/IEC 27002 podría suponer una ocasión para robustecer el marco regulatorio de Ecuador. Estas regulaciones establecen pautas precisas para la administración de la seguridad informática, fomentando acciones como la valoración regular de riesgos, la puesta en marcha de controles de acceso basados en roles y la ejecución de auditorías periódicas (Salazar y Avila, 2023). La implementación de estos estándares

facilitaría a Ecuador no solo incrementar la protección de la información médica, sino también una integración más eficaz en los sistemas de salud digital a nivel mundial.

Los descubrimientos subrayan que, a pesar de su solidez legal, la LOPDP necesita un enfoque pragmático que garantice su ejecución eficaz. Esto abarca la generación de estímulos para que las entidades inviertan en tecnologías de vanguardia, el fomento de una cultura empresarial centrada en la protección de la información y la capacitación continua del personal. Solo mediante estas medidas podremos asegurar la salvaguarda eficaz de los datos médicos y reforzar la confianza de los pacientes en el sistema sanitario de Ecuador.

Conclusiones

La Ley Orgánica de Protección de Datos Personales de Ecuador proporciona un robusto marco regulatorio para salvaguardar la información sanitaria. Sin embargo, el acatamiento efectivo de sus normativas se basa en gran parte en la correcta aplicación y supervisión dentro de las instituciones sanitarias. Pese a que ciertas entidades han implementado políticas de seguridad como la regulación de accesos y la encriptación de datos, aún existen desigualdades importantes en la seguridad debido a comportamientos incoherentes, particularmente en entidades que no disponen de los recursos necesarios para la modernización tecnológica y la formación constante del personal.

Se reconocieron diversos factores de riesgo que inciden en la privacidad de las historias clínicas digitales en Ecuador, entre ellos, el empleo de contraseñas frágiles, la carencia de autenticación multifactorial y la falta de protocolos apropiados para la gestión de accesos. Estos elementos aumentan la fragilidad de los sistemas sanitarios ante accesos indebidos y pérdida de información, lo que podría poner en riesgo la relación de confianza entre el paciente y la institución. Además, la administración de la información por los expertos sanitarios presenta carencias que requieren una normalización en la utilización de instrumentos y estrategias de seguridad digital.

La formación del personal sanitario en la administración segura de información digital ha demostrado ser un elemento crucial en la eficacia de las prácticas de salvaguarda de datos. No obstante, hay una notable diferencia en los grados de entendimiento y uso de la normativa entre el personal administrativo y clínico, lo que indica la necesidad de programas de capacitación obligatorios y constantes. Estos programas deben tratar tanto el entendimiento de las regulaciones como la implementación de buenas prácticas de ciberseguridad en la utilización cotidiana de los sistemas de información.

La investigación corrobora la relevancia de incorporar tecnologías de vanguardia, tales como el cifrado AES-256 y la autenticación multifactorial, con el fin de robustecer la salvaguarda de la

información personal en los registros clínicos digitales. Estas tecnologías, en combinación con auditorías de seguridad regulares, tienen el potencial de reducir riesgos significativos de infracción de datos. Su puesta en marcha fortalece el acatamiento de las normas legales y potencia la seguridad de los pacientes en la privacidad de sus datos de salud.

El estudio subraya la importancia de una cultura organizativa que valore la protección de la información y la privacidad de los datos del paciente. Las instituciones sanitarias deben fomentar esta cultura a través de la puesta en marcha de políticas definidas de administración de incidentes, equipos expertos en ciberseguridad y la formación de una estructura organizativa que aprecie la privacidad del paciente como un elemento esencial de su misión. Esta perspectiva favorecerá la perdurabilidad de las prácticas de salvaguarda de datos y facilitará una administración de la información en función de las demandas legales y éticas presentes.

Referencias

Alegre, V., Álvarez, M., Bianchini, A., Buedo, P., Campi, N., Cristina, M., & Luna, F. (2024). Salud digital en América Latina: legislación actual y aspectos éticos. *Revista Panamericana de Salud Pública,* 48, 9. https://doi.org/10.26633/RPSP.2024.40

American medical association. (2023). Patient data privacy and access resources. AMA: https://www.ama-assn.org/practice-management/hipaa/patient-data-privacy-and-access-resources

Asamblea Constituyente. (2008). Constitución de la República del Ecuador. Registro Oficial 449 de 20.

Assets. (2020). ¿Cómo en Ecuador las organizaciones deben responder a la protección de datos personales? Ey data protection & privacy. https://lc.cx/QZvU_0

Becerra, A., Chang, C., Rea, M., Vargas, E., Ferruzola, E., y Romero, H. (2024). Intimidad y protección de datos personales en historias clínicas digitales: análisis desde una perspectiva jurisprudencial. *Revista Científica, 7*(4), 411-427.

Belanti, M. (2018). Al amparo de la salud. Algunas consideraciones sobre derechos humanos y condiciones de mercado. *Revista Derecho y Salud, 2*(2).

Burgos, N., Márquez, F., y Baquerizo, G. (2019). Métodos y técnicas en la investigación cualitativa. *Revista Conrado, 15*(70), 455-459.

Cabero, J., Barroso, J., y Palacios, A. (2021). Estudio de la competencia digital docente en Ciencias de la Salud. Su relación con algunas variables. *Educación médica,* 22, 94-98.

Condori, J. (2024). Protección de datos y privacidad del paciente. La confidencialidad en la Era Digital. https://www.josecondori.com/proteccion-datos-privacidad-paciente/

Crotty, B., & Mostaghimi, A. (2014). Confidentiality in the digital age. *BJM,* 348.

Dagher, G., Mohler, J., Milojkovic, M., y Marella, P. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society,* 39, 283-297.

De Lorenzo, R. (2026, 29 de noviembre). Historia clínica: violación de intimidad y acceso indebido a la confidencialidad. Redacción médica. https://lc.cx/ELP48N

Deloitte United States. (2020). Protección de datos personales en Chile. Ley N° 19.628.

Echavarria, N. (2017). Protección de datos personales en México: Regulaciones y normativas. Nedigital. https://www.nedigital.com/es/blog/proteccion-de-datos-personales-en-mexico

El Comercio. (2021). Ley para la protección de datos de los ecuatorianos; se creará una Super intendencia. https://lc.cx/ZmzXAW

El Comercio. (2023). Empresas serán sancionadas por uso inadecuado de datos personales. https://lc.cx/EKcqQg

Escobar, C., Velasquez, P., Rojas, L., & Sanchez, N. (2023). *Propuesta de plan de capacitación para personal asistencial en emergencias obstétricas para favorecer la maternidad segura de la Clínica Versalles de Cali, Colombia*. Universitaria de Ciencias de la Salud.

Gil, J., & Viega, M. (2020). Historia clínica electrónica: confidencialidad y privacidad de los datos clínicos. *Revista Médica del Uruguay, 34*(4), 101-119.

Hernández, E., & Mancilla, P. (2024). Confidencialidad de datos en un hospital-escuela dedicado a la investigación. *Revista Latinoamericana de Bioética, 21*(2), 41-55.

Innab, N. (2018). Managing the information security issues of electronic medical records. *International Journal of Security, Privacy and Trust Management, 7*(2-4), 21-30.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal, 22*(2), 177-183. https://doi.org/10.1016/j.eij.2020.07.003

La Ley Orgánica de Protección de Datos Personales de Ecuador. (2021). Ley 0. Registro Oficial Suplemento 459. https://lc.cx/ESzP2_

Ley Orgánica de la Salud. (2006). Registro Oficial Suplemento 423. https://lc.cx/jLz0dX

Martínez, J., y Pérez, J. (2022). Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas, 7*(1), 776-781. https://doi.org/10.35381/racji.v7i1.2203

Ochoa, N., Álvarez, M., y Manzano, R. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. *Dilemas contemporáneos: Educación, Política y Valores, 4*(2). https://doi.org/10.46377/dilemas.v11i2.4080

Ramos, A., Bouzas, R., Olmo, A., y Buceta, B. (2019). Opinión de los facultativos y usuarios sobre avances de la e-salud en atención primaria. *Atencion Primaria,* 52, 389 - 399. https://doi.org/10.1016/j.aprim.2019.05.008.

Redrobán, W. (2023). Protección de datos personales en Ecuador a consecuencia de la emergencia sanitaria Covid-19. *Revista Universidad y Sociedad, 15*(2), 194-206.

Reglamento de información confidencial en sistema nacional de salud. (2015). Acuerdo ministerial 5216. Registro oficial suplemento 427. https://lc.cx/GKW_lJ

Robalino, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro, Revista de Derecho,* (27), 5-21.

Salazar, D., y Avila, B. (2023). 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

Sigüenza, J., y Jaimes, A. (2021). La historia clínica como prueba documental: un análisis del sistema colombiano y ecuatoriano. *Iustitia Socialis: Revista arbitrada de ciencias jurídicas, 6*(1), 440-445. https://doi.org/10.35381/racji.v6i1.1484

Tardif, D. (2019). Understanding privacy risks when accessing electronic medical records. *Canadian journal of anesthesia,* 67, 163-168. https://doi.org/10.1007/s12630-019-01532-3}

UNIR. (2021). La confidencialidad de los datos médicos: ¿qué dice la legislación? https://www.unir.net/salud/revista/confidencialidad-de-datos-medicos/

Zúñiga, D., & Martínez, J. (2019). El derecho a la salud y la confidencialidad de datos en pacientes vulnerables. *Revista Conamed, 24*(2), 55-56.

Autores

Flavio David Ramírez Ortega. Abogado de los tribunales de justicia de la república, actualmente jefe de la jefatura técnica de archivo y documentación clínica del hospital de espacialidades José Carrasco Arteaga (IESS-Cuenca).

Jaime Arturo Moreno Martínez. Doctor en jurisprudencia y abogado de los tribunales de justicia de la república, diploma superior en informática jurídica, diploma superior en derecho constitucional y derechos fundamentales, magister en derecho informático con mención en comercio electrónico, especialista en derecho constitucional, magister en derecho penal y magister en derecho médico, actualmente docente en la carrera de derecho y criminología y ciencias forenses de la Universidad Católica De Cuenca, socio y abogado en libre ejercicio en amedilex

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.