Vulnerabilidades y brechas de seguridad en la transmisión de imágenes DICOM a través de redes públicas: revisión documental

Ayarith Yeritza Granados Vivanco

Cesar Enrique Pérez Guerra

Diana Carolina Narváez Artunduaga

Michelle Andrea Guzmán Carrillo

Stephany Taborda Herrera

Asesor

Alberto Guzmán Avilés

Universidad Nacional abierta y a distancia - UNAD

Escuela de Ciencias de la Salud - ECISA

Tecnología en Radiología e Imágenes Diagnósticas

2026

Dedicatoria.

Los autores dedicamos este proyecto a nuestras familias por su apoyo incondicional, a nuestros padres por ser el motor de nuestras vidas.

A nosotros, Ayarith Yeritza Granados Vivanco, Cesar Enrique Pérez Guerra, Diana Carolina Narváez Artunduaga, Michelle Andrea Guzmán Carrillo y Stephany Taborda Herrera, sin nuestro esfuerzo y dedicación no lo hubiéramos logrado**.**

Agradecimientos.

De corazón queremos agradecer a Dios por permitirnos alcanzar esta meta, por darnos sabiduría para superar los retos que se nos presentaron en el camino.

A nuestras familias por su tiempo y apoyo permanente, son los pilares de nuestras vidas.

A la UNAD por brindarnos espacios de formación y por permitirnos crecer como personas y futuros profesionales.

A los tutores, por su tiempo y compromiso que guiaron nuestro conocimiento para culminar con éxito este diplomado.

A todas las personas que de una u otra manera hicieron parte de este sueño, gracias por confiar en nosotros.

Resumen

La transmisión de imágenes en formato DICOM ha tenido grandes avances en la interoperabilidad entre sistemas, plataformas de IA y servicios de radiología. Sin embargo, cuando estos datos se transfieren a través de redes públicas, se aumentan los riesgos de ciberseguridad que comprometen la integridad, confidencialidad y disponibilidad de la información clínica. El propósito de esta investigación es analizar las brechas y vulnerabilidades más usuales en la transmisión de imágenes, mediante una revisión documental con diseño no experimental, basada en literatura científica, técnica y normativa, basados en Hernández et al. (2014). Los hallazgos muestran fallos como la ausencia de cifrado robusto, el envío de metadatos en texto claro, el uso de protocolos inseguros o desactualizados, configuraciones deficientes, accesos remotos no autorizados, debilidades en la autenticación, tráfico sin protección y vulnerabilidades en redes públicas. Asimismo, se identificaron riesgos asociados a ataques Man in the Middle, interceptación de datos, manipulación adversarial de imágenes y compromisos en la integridad diagnóstica. Los resultados señalan que las instituciones de salud tienen deficiencias en la implementación de mecanismos como TLS, VPN, autenticación multifactor, control de accesos, monitoreo continuo y políticas adecuadas de ciberseguridad. Se concluye que la mitigación de estas brechas requiere estrategias integrales que incluyan cifrado de extremo a extremo, protocolos actualizados, prácticas seguras de configuración, fortalecimiento institucional, capacitación del personal y la adopción de medidas robustas que garanticen la protección de las imágenes médicas y la seguridad del paciente en entornos digitales interconectados.

Palabras clave: DICOM, ciberseguridad, metadatos, ataques Man in the Middle.

Abstract

The transmission of images in DICOM format has achieved major advances in interoperability between systems, AI platforms, and radiology services. However, when these data are transferred through public networks, cybersecurity risks increase, compromising the integrity, confidentiality, and availability of clinical information. The purpose of this research is to analyze the most common gaps and vulnerabilities in image transmission through a non-experimental documentary review based on scientific, technical, and regulatory literature, following Hernández et al. (2014). The findings reveal failures such as the absence of robust encryption, the transmission of metadata in plain text, the use of insecure or outdated protocols, poor configuration practices, unauthorized remote access, weak authentication mechanisms, unprotected traffic, and vulnerabilities associated with public networks. Likewise, risks were identified related to Man-in-the-Middle attacks, data interception, adversarial image manipulation, and compromises in diagnostic integrity. The results indicate that healthcare institutions exhibit deficiencies in the implementation of mechanisms such as TLS, VPNs, multifactor authentication, access control, continuous monitoring, and adequate cybersecurity policies. It is concluded that mitigating these gaps requires comprehensive strategies that include end-to-end encryption, updated protocols, secure configuration practices, institutional strengthening, staff training, and the adoption of robust measures that ensure the protection of medical images and patient safety in interconnected digital environments.

Keywords: DICOM, cybersecurity, metadata, Man-in-the-Middle attacks.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

La digitalización de los sistemas de salud ha permitido grandes avances en la gestión, almacenamiento y transmisión de imágenes médicas, con el uso del estándar DICOM. Este protocolo ha facilitado la interoperabilidad entre dispositivos médicos, sistemas de información como RIS y PACS, y plataformas de teleradiología, optimizando los procesos diagnósticos y la atención en salud.

No obstante, el creciente uso de redes públicas para la transmisión de imágenes introdujo vulnerabilidades a la ciberseguridad. La exposición de datos clínicos sensibles, la falta de cifrado en la comunicación, las configuraciones inseguras de servidores y la vulnerabilidad de los metadatos son riesgos críticos para la confidencialidad, integridad y disponibilidad de la información médica (Cervera y Goussens, 2024). En este contexto, la dependencia de redes públicas o infraestructuras que no están bajo control directo de las instituciones sanitarias exacerba las vulnerabilidades existentes.

Asimismo, la transmisión de imágenes médicas en formato DICOM mediante redes públicas es un punto crítico dentro la ciberseguridad radiológica. La integración de sistemas PACS, RIS y modalidades diagnósticas de alto alcance, la superficie de ataque se amplía y aparecen las vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de la información clínica.

Según el análisis de la literatura reciente, se evidencia que gran parte de los incidentes de ciberseguridad en salud se relacionan con las inadecuadas configuraciones de servidores, la falta de cifrado de datos y la exposición inadvertida de puertos y servicios DICOM. La transmisión de imágenes médicas en formato DICOM a través de redes públicas es una práctica común por el crecimiento de la teleradiología y la interconexión entre instituciones de salud. Sin embargo, este proceso implica riesgos que afectan la

confidencialidad**,** integridad**,** disponibilidad **y** autenticidad de la información clínica, especialmente cuando las transferencias se realizan sin mecanismos de protección adecuados.

La información clínica transportada por archivos DICOM integra imágenes diagnósticas y metadatos sensibles que hacen parte del Protected Health Information (PHI), y las brechas de seguridad comprometen los sistemas informáticos hospitalarios y la confidencialidad, integridad y disponibilidad de los datos del paciente.

Entonces, se hace necesario comprender las vulnerabilidades de las redes públicas durante la transmisión de imágenes para instaurar formas de mitigación que garanticen la protección de los datos sensibles del paciente y la confiabilidad del diagnóstico médico.

El presente estudio tiene como objetivo analizar las brechas de seguridad en la transmisión de imágenes DICOM a través de redes públicas, reportadas en la literatura, identificando sus principales vulnerabilidades, factores asociados e impacto en los sistemas de salud, proponiendo algunas recomendaciones basadas en la evidencia para fortalecer la seguridad informática en entornos radiológicos. Asimismo, busca proponer estrategias de mitigación basadas en la evidencia científica, con el fin de fortalecer la protección de los datos clínicos en entornos digitales cada vez más interconectados y dependientes de infraestructuras externas.

Este propósito responde a los hallazgos de autores como Marco et al. (2020), quienes subrayan que las arquitecturas RIS/PACS requieren modelos de seguridad integrales, y a las recomendaciones de organismos como la ISO/IEC y el U.S. Department of Health y Human Services, que establecen lineamientos esenciales para proteger la información radiológica frente a amenazas tecnológicas, operativas y humanas.

Algunos autores han demostrado que las vulnerabilidades técnicas, las malas configuraciones y la ausencia de protocolos de seguridad robustos generan fallos que comprometen la privacidad de los pacientes y la confiabilidad diagnóstica (Marco et al., 2020. Evaluar el impacto de estas brechas permite comprender la magnitud del riesgo y orientar la implementación de medidas de protección que fortalezcan la seguridad de la información clínica.

La revisión literaria de esta investigación, analiza los riesgos más habituales, los fallos técnicos asociados a la infraestructura DICOM y las vulnerabilidades que permiten la explotación de los sistemas PACS, RIS y nodos DICOM cuando se utilizan redes no seguras. Adicionalmente, se presentan recomendaciones basadas en evidencia científica para el fortalecimiento de los protocolos de seguridad.

El crecimiento de la radiología digital y la interoperabilidad entre sistemas como DICOM, PACS y RIS ha optimizado los procesos clínicos y el acceso a la información diagnóstica. Sin embargo, este avance también ha aumentado la superficie de exposición frente a amenazas cibernéticas, debido a la interconexión de redes hospitalarias, la expansión de los servicios de telesalud y la incorporación de dispositivos IoT médicos. Esta convergencia tecnológica, aunque beneficiosa para la eficiencia operativa, introduce nuevas brechas asociadas al cifrado insuficiente, la exposición de servidores y la presencia de configuraciones inseguras que pueden comprometer la integridad de las imágenes diagnósticas y los datos clínicos asociados.

Más allá de las vulnerabilidades propias del protocolo DICOM, la literatura evidencia que los riesgos en radiología emergen de la interacción entre factores tecnológicos, operativos, organizacionales y humanos. Cuando estos elementos no son gestionados adecuadamente, se convierten en puntos críticos que facilitan ataques

cibernéticos, accesos no autorizados, alteración de imágenes y manipulación maliciosa de la información clínica (Cervera y Goussens, 2024). Además, se suman amenazas avanzadas como el malware especializado y los ataques adversariales sobre modelos de inteligencia artificial, capaces de modificar imperceptiblemente una imagen médica y alterar los resultados diagnósticos sin levantar sospechas, lo que plantea nuevos desafíos (Goodfellow et al., 2015).

Entonces, emerge la necesidad de un enfoque integral que aborde la infraestructura tecnológica, los procesos institucionales, la gobernanza de datos y el componente humano. En este sentido, los marcos regulatorios y estándares internacionales, como HIPAA, GDPR, el NIST Cybersecurity Framework y la norma ISO/IEC 27001 que establecen lineamientos para gestionar riesgos, garantizar la confidencialidad, la disponibilidad y la integridad de los datos clínicos (Parlamento Europeo, 2016), y para fortalecer los niveles de madurez en seguridad de la información (Zambrano y Mora, 2024). No obstante, su efectividad depende de la implementación real dentro de los entornos hospitalarios y de la articulación coherente entre políticas institucionales, capacidades tecnológicas y recursos especializados (Bernal, 2024).

Por lo tanto, el análisis de estos factores permite comprender que la ciberseguridad en radiología no depende solo de herramientas técnicas, sino además de un enfoque integral de la infraestructura, los procesos institucionales y el conocimiento humano.

Planteamiento del Problema

El uso de la IA en radiología ha cambiado el diagnóstico por imágenes, optimizando la detección temprana de diagnósticos, mejorando los tiempos de respuesta y apoyando la toma de decisiones clínicas (Esteva et al., 2019), además del almacenamiento, intercambio y análisis de imágenes médicas mediante el uso de estándares como DICOM, facilitando la interoperabilidad entre sistemas, plataformas, servidores y equipos médicos. Sin embargo, estos avances tecnológicos han traído consigo nuevos riesgos asociados a la ciberseguridad, interconectividad y protección de datos médicos (Galiano, 2022).

Uno de los principales riesgos es la presencia de brechas de seguridad en las transmisiones de las imágenes médicas, cuando no cuentan con mecanismos de cifrado o autenticación. Asimismo, con vulnerabilidad de los sistemas de IA frente a los llamados adversarial attacks (Goodfellow et al., 2015), que consisten en la manipulación intencional de imágenes médicas mediante alteraciones sutiles, muchas veces imperceptibles para el ojo humano, pero suficientes para inducir errores significativos en los algoritmos de diagnóstico. En radiología, estas manipulaciones pueden provocar falsos diagnósticos, afectando directamente la seguridad del paciente y la calidad de la atención en salud.

Además, la exposición de metadatos en los archivos DICOM, la configuración incorrecta de servidores de imágenes, el uso de puertos abiertos sin control de acceso y la transmisión de información en texto claro (cleartext) son otras de las brechas de seguridad más frecuentes en los sistemas de radiología digital, usadas con ataques Man in the Middle o accesos no autorizados a servidores de almacenamiento de imágenes médicas.

De igual forma, al aumentar la transmisión de datos y de estudios, se acrecientan los ataques por el uso de redes públicas sin la implementación de protocolos de seguridad

robustos como cifrado TLS, redes privadas virtuales (VPN) o mecanismos de autenticación segura.

Adicionalmente, la falta de protocolos claros de ciberseguridad, la limitada capacitación del personal y la dependencia de los sistemas automatizados incrementan la probabilidad de que estos ataques pasen desapercibidos, comprometiendo la integridad, confidencialidad y disponibilidad de los datos médicos y exponiendo a las instituciones de salud y a los profesionales a riesgos legales, éticos y reputacionales (ISO/IEC, 2022; OMS, 2021).

En este escenario, resulta fundamental analizar y comprender las vulnerabilidades de los sistemas de IA en la transmisión de imágenes médicas y el estándar DICOM, con el fin de identificar las brechas de seguridad más comunes y contribuir al fortalecimiento de estrategias de ciberseguridad que garanticen la protección de la información clínica.

A partir de este análisis surge la pregunta problema: ¿Cuáles son las brechas de seguridad más comunes en la transmisión de imágenes DICOM a través de redes públicas según la literatura reciente?

Justificación

El estudio del estándar DICOM y sus implicaciones en ciberseguridad es significativo debido a su rol clave en la gestión, almacenamiento y transmisión de imágenes diagnósticas en el entorno hospitalario actual con el almacenamiento y distribución de estudios diagnóstico. DICOM actúa como el lenguaje común que une diferentes técnicas de imagen, estaciones de trabajo, sistemas PACS y RIS e instituciones médicas. Sin embargo, cualquier vulnerabilidad en la implementación pone en riesgo la confidencialidad de los datos, la integridad de los diagnósticos y la seguridad del paciente (Henao y Moscoso, 2013).

La progresiva digitalización de los servicios de salud con la expansión de la telemedicina acrecienta la exposición a vulnerabilidades como ransomware, ataques man in the middle, explotación de fallas en los sistemas de almacenamiento y transmisión de datos y configuraciones inseguras a través de redes públicas (Castañeda et al., 2024). Además, se evidencia que los sistemas PACS y las infraestructuras de imágenes médicas pueden presentar debilidades en la protección de datos, especialmente cuando no se implementan mecanismos adecuados de cifrado o control de acceso (Marco et al., 2020).

De igual forma, el estándar DICOM no cuenta con mecanismos de seguridad robustos, lo que ha permitido que algunas implementaciones presenten vulnerabilidades explotables por ciberdelincuentes, como la exposición de servidores de imágenes médicas en internet, el uso de puertos abiertos sin control de acceso y la transmisión de datos sin cifrado adecuado (Galiano, 2022), lo que facilitan los ataques de interceptación de comunicaciones o el acceso no autorizado a repositorios de imágenes médicas.

Asimismo, los archivos DICOM contienen metadatos con información delicada de los pacientes, PHI, como datos clínicos, nombres, fechas, identificadores del paciente. Por

esta razón, es necesaria la implementación de robustas medidas seguras como cifrado de datos y protocolos de transmisión seguros y anonimización (Huraca, 2025). Los mecanismos de protección como IPsec, SSL/TLS o redes privadas virtuales (VPN) robustecen la seguridad en la transmisión de imágenes y reduce el riesgo de exposición de información clínica sensible (Lugo et al., 2011).

En este escenario, la falta de buenas prácticas de ciberseguridad en el sector salud generan grandes consecuencias, como la filtración de datos clínicos, interrupción de servicios médicos o pérdida de confianza por parte de los pacientes (Bernal, 2024).

Según Bohórquez, (2025) se evidencia que en las instituciones sanitarias hay dificultades para responder a incidentes de seguridad informática, lo que destaca la necesidad de fortalecer las políticas de protección de datos y los mecanismos de defensa frente a amenazas digitales. Además, e l aumento en la digitalización de la historia clínica electrónica trae consigo nuevos retos relacionados con la seguridad de la información médica y el acceso a los datos de salud en entornos digitales (González, 2023). Estas problemáticas comprometen la confidencialidad de la información clínica, la integridad y disponibilidad, debido al riesgo de alteración de registros médicos, accesos no autorizados, pérdida de trazabilidad, interrupción de servicios hospitalarios por ataques cibernéticos y posibles fallos en la continuidad asistencial que pueden afectar directamente la atención y seguridad del paciente.

Por esta razón, entender la arquitectura del estándar que incluye metadatos, UID, modelo SOP y negociación SCU/SCP, es decisivo para identificar los puntos críticos de riesgo y establecer controles técnicos adecuados, como el cifrado mediante TLS, la segmentación de red y la autenticación robusta.

En el ámbito académico y profesional, es importante que los profesionales entiendan el funcionamiento del estándar DICOM, su dimensión ética, legal y de seguridad informática. La identificación de brechas de seguridad y la implementación adecuada de estrategias de mitigación refuerzan la resiliencia institucional ante incidentes cibernéticos, asegura la continuidad del servicio y protege la confianza del paciente en los sistemas de salud digitales como debe ser. Asimismo, las mejores prácticas en ciberseguridad para servicios de teleradiología deben implementar mecanismos de cifrado, monitoreo de redes, control de accesos y auditorías de seguridad para proteger la transmisión de imágenes médicas (Mathur et al., 2025).

Por ende, el estudio exhaustivo del estándar DICOM y sus vulnerabilidades es una necesidad estratégica que garantiza la calidad diagnóstica, la protección de datos clínicos y el cumplimiento normativo en el entorno sanitario actual. Es decir, que el análisis de los riesgos de transmisión de imágenes médicas por redes públicas contribuye a mejorar las prácticas de ciberseguridad en la salud, favoreciendo la protección de datos, diagnósticos más seguros y el cumplimiento de la normativa vigente.

Objetivos

Objetivo General

Analizar las brechas de seguridad en la transmisión de imágenes DICOM a través de redes públicas, así como sus vulnerabilidades críticas, factores técnicos y operativos asociados.

Objetivos Específicos

Identificar los principales riesgos, vulnerabilidades y fallos de seguridad reportados en la literatura relacionados con la transmisión de imágenes médicas DICOM en redes públicas.

Analizar los factores tecnológicos, operativos, organizacionales y humanos, incluyendo servidores DICOM, PACS, RIS e infraestructura de red, que favorecen la aparición y explotación de brechas de seguridad.

Evaluar el impacto de las brechas de seguridad en la confidencialidad, integridad, disponibilidad y posible manipulación de la información clínica durante la transferencia de imágenes médicas.

Proponer recomendaciones, protocolos de seguridad y buenas prácticas para mitigar riesgos y fortalecer la protección de los datos médicos durante la transmisión de archivos DICOM en redes públicas, basadas en la evidencia documental.

Marco Teórico

Fundamentos del Estándar DICOM

El estándar DICOM es el protocolo más usado en radiología para el almacenamiento y transmisión de imágenes, fue desarrollado por el American College of Radiology (ACR) y la National Electrical Manufacturers Association (NEMA), la primera versión se usó en 1985 y se oficializó en 1993, se creó para tener un formato estándar, interoperable y compatible entre equipos médicos, sistemas hospitalarios y plataformas de almacenamiento (National Electrical Manufacturers Association, s.f.).

Su implementación en radiología, ha integrado dispositivos con modalidades de imagen como tomografía computarizada, resonancia magnética en las infraestructuras digitales (García, 2014).

DICOM también establece los protocolos de comunicación para intercambiar la información entre dispositivos y sistemas, es decir, equipos de adquisición de imágenes, estaciones de trabajo, servidores de almacenamiento y sistemas de información, permitiendo la interoperabilidad entre diversas tecnologías (Varma, 2012).

Estructura del Archivo DICOM

Los componentes del sistema DICOM son dos, los datos de imagen y los metadatos o cabeceras. Los datos de imagen tienen información de los píxeles, es la representación digital de las estructuras anatómicas obtenidas por TC, RM, ultrasonido o radiografía (García, 2014).

Los metadatos contienen información del estudio y del paciente, como la identificación del paciente, número de la historia, la modalidad de imagen, la fecha y hora, los parámetros del equipo, el UID y la sede que lo generó, esta clasificación permite que

cada imagen sea bien interpretada, almacenada, recuperada y compartida entre los sistemas y plataformas (Henao y Moscoso, 2013).

Sistema de Etiquetas Tag System e Identificadores Únicos UID

Dentro del sistema DICOM, se encuentran los metadatos, que se componen del sistema Tag System, que se encarga de organizar la información con etiquetas o tags, que a su vez está compuesto por un grupo y un elemento que identifican la información almacenada en el archivo, para acceder a datos relevantes del estudio, como la información del paciente y los parámetros de adquisición de la imagen.

También cuenta con Identificadores Únicos (UID)**,** que reconocen cada estudio, serie o imagen dentro del ecosistema de radiología digital. Este sistema de identificación es esencial para garantizar la correcta gestión, almacenamiento y recuperación de las imágenes médicas dentro de repositorios o servidores clínicos (Varma, 2012).

Digitalización de Imágenes Médicas y Riesgos de Seguridad

La tecnología de digitalización ha aumentado los riesgos de la integración de imágenes médicas en plataformas electrónicas de gestión hospitalaria, afectando la ciberseguridad, especialmente en lo relacionado con la protección de datos sensibles de los pacientes y la integridad de los estudios diagnósticos (González, 2023).

Bohórquez (2025) advierte que el uso de aplicaciones digitales presenta brechas en la confidencialidad, sobre todo cuando los sistemas de historia clínica se conectan con redes externas que carecen de controles de seguridad adecuados. Estas debilidades pueden ser aprovechadas por atacantes para acceder a información clínica, alterar estudios diagnósticos o comprometer la disponibilidad de los servicios médicos (Galiano, 2022).

Brechas de Seguridad en la Transmisión de Imágenes DICOM

El incremento de los sistemas digitales y la conexión a internet generan nuevas inquietudes en la seguridad de la información. Por ende, las imágenes almacenadas o transmitidas con el estándar DICOM pueden ser objetivos permisibles para ataques informáticos, si no se cuenta con las medidas correctas de seguridad. Según Arias (2019), el uso de direcciones IP públicas en los sistemas hospitalarios expone la información a accesos no autorizados, lo que se desmejora con los sistemas de imágenes médicas conectados a redes externas sin controles de acceso o cifrado de datos.

Igualmente, los PACS a través de los archivos DICOM, pueden ser vulnerables cuando no cuentan con mecanismos de seguridad robustos, configuraciones abiertas, permitiendo que terceros sin autorización puedan acceder, descargar o incluso modificar los estudios. Este tipo de exposición es un riesgo significativo para la privacidad de los pacientes y para la confiabilidad de los diagnósticos médicos (Marco et al., 2020).

Vulnerabilidades en la Transmisión de Imágenes Médicas

De igual forma, el sector salud tiene retos de rápida respuesta ante incidentes de seguridad informática. Bernal (2024) señala que las sanitarias tienen poco nivel de reacción y preparación ante ataques cibernéticos, especialmente con ransomware o filtración de información clínica, lo que evidencia la necesidad de robustecer los protocolos de seguridad y las estrategias de protección de datos médicos en los sistemas de información hospitalarios.

Otro aspecto crítico es el uso de puertos de comunicación en los sistemas DICOM, donde queda demostrado que muchos servidores utilizan el puerto 104**,** y que cuando este puerto se encuentra expuesto en redes públicas sin mecanismos de cifrado, puede ser

detectado por escaneo de red, permitiendo atacantes en los servidores médicos, admitiendo el acceso a la información transmitida (Rapid7, 2026).

Servicios DICOM, Roles de SCU y SCP

En el sistema DICOM, la comunicación entre dispositivos se hace con un modelo de roles específicos para el intercambio de información, que son los Service Class User (SCU) que corresponden al sistema que inicia la solicitud de un servicio dentro de la red, y el Service Class Provider (SCP) que se encarga de recibir la solicitud y prestar el servicio, como el de almacenar o transferir imágenes (Álzate, 2009). Este modelo establece una comunicación organizada entre dispositivos de diagnóstico, estaciones de trabajo y servidores de almacenamiento dentro de la infraestructura hospitalaria (Galiano, 2022).

La implementación de estos servicios permite la interoperabilidad entre equipos médicos dentro de una red de imágenes médicas, intercambiando información clínica entre dispositivos y sistemas de almacenamiento. Sin embargo, cuando estos servicios no tienen herramientas de seguridad robustas, son puntos vulnerables para las instituciones de salud, permitiendo accesos no autorizados a información médica sensible (ACIS, 2022).

Protocolos de Comunicación - Funcionamiento sobre TCP/IP

La transmisión de imágenes médicas por medio del sistema DICOM se efectúa mediante redes basadas en el protocolo Transmission Control Protocol/Internet Protocol (TCP/IP), que es un conjunto de protocolos esenciales para la comunicación en redes informáticas modernas y que establece conexiones confiables entre dispositivos médicos, garantizando que los datos transmitidos lleguen de forma íntegra entre los sistemas que intercambian información clínica (Cortés, 2023).

El uso de TCP/IP en los sistemas de información hospitalarios permite integrar diversas plataformas tecnológicas digitales. Con este modelo de comunicación, los sistemas

de diagnóstico por imagen pueden transmitir estudios médicos a servidores de almacenamiento, estaciones de visualización o plataformas de telemedicina. Sin embargo, la interconexión también genera nuevos retos en cuanto a la seguridad de la información clínica y la protección de los datos de los pacientes (Cervera y Goussens, 2024).

Relación entre RIS, PACS y DICOM

La gestión de imágenes funciona con la relación entre varios sistemas como son RIS, PACS y DICOM, donde el RIS se encarga de administrar la información administrativa, los datos del paciente y de los estudios; el PACS almacena, organiza y distribuye las imágenes, con acceso desde estaciones de trabajo dentro de la red hospitalaria (Magdy et al., 2022).

El sistema DICOM produce la interoperabilidad entre los equipos y los PACS, done las imágenes adquiridas en TC, RM o radiografía se transmiten y almacenan en los sistemas hospitalarios. Gracias a este estándar, las imágenes obtenidas mediante tomografía computarizada (TC), resonancia magnética (RM), radiografía digital y otras modalidades diagnósticas pueden compartirse de manera uniforme entre diferentes dispositivos y plataformas, independientemente del fabricante del equipo (García, 2014). Además, DICOM integra las imágenes y los metadatos clínicos asociados al paciente, al estudio y a los parámetros técnicos del examen, permitiendo una gestión más eficiente de la información radiológica. Esta interoperabilidad favorece la continuidad asistencial, optimiza los flujos de trabajo en radiología y mejora el acceso oportuno a la información diagnóstica dentro de los sistemas hospitalarios digitales.

En radiología, el sistema RIS gestiona la solicitud del estudio y registra los datos del paciente, luego los equipos generan las imágenes en formato DICOM, que se transmiten al PACS para su almacenamiento y gestión. De ahí, el personal de salud accede a las

imágenes para su visualización, análisis e interpretación, mientras que en el RIS hacen parte del informe clínico, esta interoperabilidad garantiza el acceso en tiempo real a las imágenes (Rai et al., 2025).

Redes Públicas vs. Redes Privadas y los Riesgos en la Transmisión de Datos Médicos

El avance de la telemedicina y los sistemas digitales en la salud depende de las redes de comunicación para el intercambio de información entre instituciones. No obstante, el uso de redes públicas como internet para la transmisión de datos médicos expone a los sistemas hospitalarios a riesgos como ataques cibernéticos, interceptación de datos o accesos no autorizados a información sensible (Cervera y Goussens, 2024).

En Colombia, la interoperabilidad entre los sistemas de información de las instituciones de salud necesita de grandes mecanismos de protección de datos. Es decir, que, la necesidad de incorporar procesos de seguridad que garanticen la integridad, confidencialidad y disponibilidad de la información médica entre plataformas digitales de salud (Cortés, 2023).

De acuerdo con el Ministerio de Salud y Protección Social de Colombia, los sistemas de información en salud deben contar con mecanismos seguros de redes privadas virtuales (VPN), autenticación segura y certificados criptográficos para la protección de datos clínicos durante la transmisión en sistema digitales de atención médica (Ministerio de Salud de Colombia, 2023).

Además, Zambrano y Mora, (2024) han resaltado la importancia de adoptar buenas prácticas de seguridad informática en las instituciones hospitalarias, incluyendo la protección de aplicaciones clínicas, el monitoreo de redes y la gestión de vulnerabilidades tecnológicas que puedan alterar la privacidad de la información médica.

En conclusión, los sistemas de teleradiología, que transmiten imágenes entre instituciones y servidores, deben garantizar infraestructuras seguras. Entonces, se deben implementar protocolos cifrados y redes privadas virtuales que protejan la información clínica en la transmisión y así evitar posibles ingresos no autorizados a las imágenes radiológicas (Mathur et al., 2025).

Archivos DICOM y los Sistemas PACS y RIS

Las imágenes médicas generadas en TC, RM, radiografías, se guardan y gestionan en plataformas como Picture Archiving and Communication System (PACS) y el Radiology Information System (RIS). El PACS almacena, organiza y distribuye las imágenes en la infraestructura hospitalaria, y el RIS tramita la información administrativa y clínica de los estudios, como los datos del paciente, la programación de exámenes y los reportes diagnósticos. La interoperabilidad entre ambos relaciona las imágenes médicas con la información clínica del paciente, facilitando la gestión de los estudios radiológicos en el flujo de trabajo hospitalario (Magdy et al., 2022).

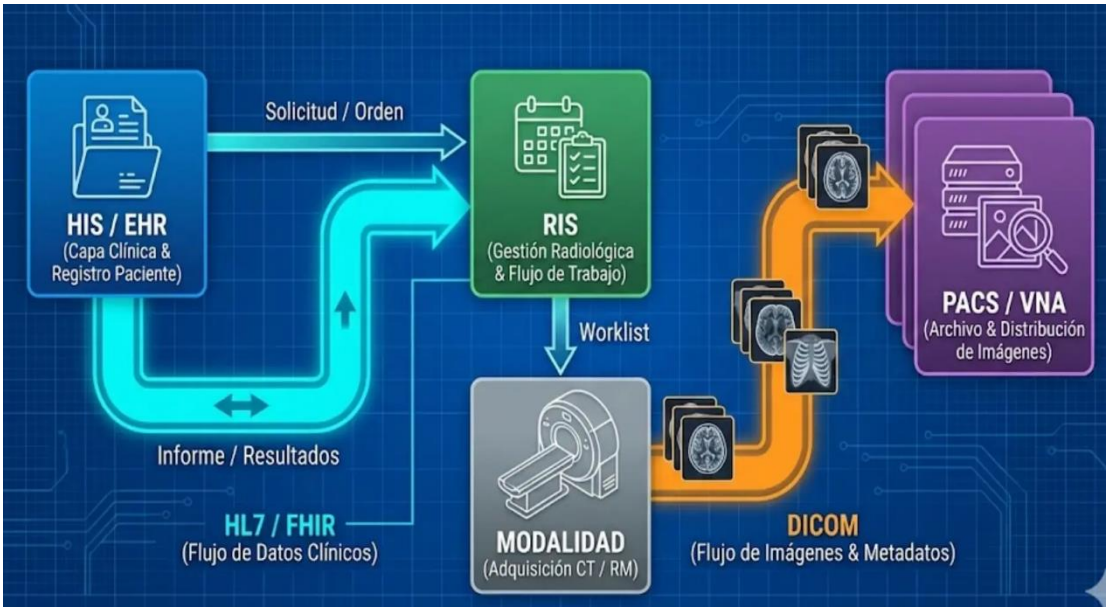
Además, las imágenes digitales tienen pros y contras con impacto directo en la calidad y eficacia en el diagnóstico médico. Entre las ventajas, está el procesamiento computarizado de imágenes que ajusta el contraste, arrojando diagnósticos más precisos, esto es por la integración del Sistema Digital de Almacenamiento y Comunicación (PACS), el Radiology Information System (RIS) y el Digital Imaging and Communications in Medicine (DICOM) (MV,2016).

Asimismo, el funcionamiento de PACS y RIS depende de la transmisión segura de archivos DICOM por las redes hospitalarias. Es decir que, las imágenes generadas por equipos de diagnóstico se envían al servidor PACS, para almacenarlas y que estén

disponibles para visualización y análisis de los profesionales de la salud, desde diferentes lugares dentro de la red clínica (Mathur et al., 2025).

Figura 1

Sistemas RIS, PACS, DICOM



Nota. Imagen tomada de https://radiologialatam.com/siglas-ris-pacs-dicom-his-ehr-informatica-radiologica/

Nodos y Gateways en Imágenes Médicas

En la infraestructura tecnológica de los sistemas de imágenes médicas hay puntos de interconexión llamados nodos y gateways, que comunican entre si a los dispositivos, servidores y redes externas, como mediadores en el flujo de información entre equipos de adquisición, servidores de almacenamiento y estaciones de visualización. Por esta razón, pueden convertirse en zonas críticas de la infraestructura tecnológica siendo vulnerables a ataques informáticos y accesos no autorizados si no se efectúan los controles de seguridad apropiados (Rai et al., 2025).

De igual forma, la exposición de los nodos en redes abiertas o malas configuraciones facilita la identificación de dispositivos conectados a internet por actores maliciosos, permitiendo el acceso a imágenes médicas o metadatos clínicos. Por esta razón, es importante aplicar prácticas robustas de seguridad en los sistemas de comunicación de imágenes médicas, con autenticación, cifrado de datos y segmentación de redes hospitalarias (Mathur et al., 2025).

Identificación de Brechas de Seguridad en la Transmisión de Imágenes DICOM

El avance de la digitalización de los sistemas de salud ha aumentado las vulnerabilidades en la seguridad de la información clínica. Sobre todo, en los sistemas de gestión de imágenes médicas que deben garantizar la protección de datos sensibles, como la información personal y clínica de los pacientes.

En Colombia, la Ley que regula la protección de la información es la 1581 de 2012, que ordena que las instituciones deben implementar las medidas adecuadas para garantizar la confidencialidad y seguridad de los datos personales, incluyendo las relacionadas con la información médica (Congreso de la República de Colombia, 2012).

En cuanto a los sistemas de radiología digital, se identifican diversas vulnerabilidades relacionadas con la implementación del protocolo DICOM, incluyendo configuraciones inseguras, exposición de servicios en redes públicas y ausencia de mecanismos de protección de datos durante la transmisión de imágenes médicas. Estas brechas pueden comprometer la integridad, confidencialidad y disponibilidad de la información clínica si no se aplican medidas de seguridad adecuadas dentro de la infraestructura tecnológica hospitalaria (Rai et al., 2025).

Falta de Cifrado (Cleartext) en la Transmisión de Imágenes Médicas

El problema más frecuente de seguridad en la transmisión de imágenes médicas es el envío de datos en texto claro o cleartext, sin mecanismos de cifrado que resguarden la información en la transmisión. Cuando las imágenes se transmiten sin protocolos de seguridad TLS o SSL, hay riesgo de que los datos sean interceptados por terceros maliciosos durante su tránsito en la red, comprometiendo la confidencialidad de los datos clínicos (Zhang et al., 2007).

Por lo tanto, la implementación de protocolos criptográficos como Transport Layer Security (TLS) o Internet Protocol Security (IPsec) establece canales seguros para la transmisión de imágenes en las redes hospitalarias o infraestructuras de teleradiología, garantizando que la información comunicada entre dispositivos médicos y servidores de sea protegida ante amenazas, interceptaciones o manipulaciones durante el proceso de comunicación (Lugo et al., 2011).

Igualmente, el uso de infraestructuras de red seguras como las Virtual Private Network (VPN) es una alternativa de protección para la transmisión de datos médicos a través de redes públicas, creando canales seguros cifrados de comunicación entre instituciones, garantizando la confidencialidad y la integridad de los datos clínicos transmitidos en servicios de telemedicina y teleradiología (Roo, 2004).

En conclusión, las mejores prácticas de ciberseguridad en los sistemas es implementar mecanismos de cifrado, autenticación y monitoreo continuo de la red para proteger la información médica transmitida entre instituciones de salud. Estas estrategias son esenciales para garantizar la seguridad de las imágenes médicas e impedir posibles vulnerabilidades en la privacidad de los pacientes o los sistemas clínicos digitales (Mathur et al., 2025).

Servidores PACS expuestos en Redes Públicas

Otro riesgo en la seguridad de los sistemas de imágenes es la exposición de servidores PACS a redes públicas sin adecuada protección, lo que permite que terceros no autorizados accedan a imágenes, puedan descargar archivos DICOM o alteren los estudios, comprometiendo la confiabilidad de la información y la integridad de los procesos (Marco et al., 2020).

Estas vulnerabilidades demuestran la necesidad de controles de seguridad más robustos y precisos, tales como autenticación segura, segmentación de redes y mecanismos de cifrado que protejan los sistemas (Rai et al., 2025).

Vulnerabilidades en la Transmisión, Fugas de Metadatos y PHI en DICOM

Los archivos DICOM contienen las imágenes médicas y los metadatos de los estudios. Los metadatos contienen información del paciente, como nombre, fecha de nacimiento, número de identificación o información del estudio realizado. Este tipo de información pertenece al PHI, cuya exposición puede comprometer la privacidad del paciente si los archivos son transmitidos o almacenados sin adecuada protección (Savón y Blanco, 2021).

Para el DICOM, los metadatos son cruciales para la óptima identificación de los estudios en los sistemas hospitalarios, para relacionar la imagen con el paciente real y el procedimiento realizado. Pero, cuando estos datos se comparten entre instituciones o se transmiten por redes inseguras, se pueden producir fugas de información sensible, siendo un riesgo significativo para la confidencialidad de los pacientes (Monzón, 2022).

Vulnerabilidades DICOM

El DICOM sirve para facilitar la interoperabilidad entre equipos y sistemas de almacenamiento de imágenes, para el intercambio de información entre diferentes

dispositivos en una infraestructura hospitalaria. No obstante, al inicio no tenía mecanismos robustos de seguridad, generando variadas vulnerabilidades en el intercambio de mensajes entre sistemas (Castañeda et al., 2024).

Una de estas es la comunicación entre dispositivos, Association Request, por el que dos sistemas DICOM de comunican antes de la transferencia de datos, si no se cuenta con mecanismos de autenticación o cifrado adecuados, un atacante malicioso puede manipular la comunicación entre los dispositivos o interceptar los datos transmitidos (Monzón, 2022).

Ataques Man in the Middle (MitM)

Uno de los ataques más significativos es el Man in the Middle attack, que consisten en que un atacante se posiciona entre dos sistemas de intercambio de información, interceptando, modificando o suplantando los datos transmitidos entre los dispositivos sin que los sistemas originales detecten la intrusión (Huraca, 2025).

En los sistemas de imágenes médicas, este ataque tiene graves consecuencias, puesto que la alteración de una imagen puede cambiar la interpretación diagnóstica del especialista, modificar los píxeles para una interpretación errónea o provocar retrasos en el diagnóstico, comprometiendo la seguridad del paciente (Abdullaeva et al., 2024).

Ataques Adversariales

Dentro de los riesgos emergentes de la ciberseguridad en radiología, están los ataques adversariales, que son las manipulaciones a las imágenes para alterar los píxeles y que sean desapercibidos por el ojo humano, en las imágenes almacenadas o transmitidas por DICOM, afectando los diagnósticos (Abdullaeva et al., 2024). Sin embargo, el principal riesgo no es engañar al observador humano, sino afectar directamente los algoritmos de inteligencia artificial utilizados para el análisis radiológico. Aunque la imagen aparentemente conserve un aspecto normal para el profesional de salud, la IA puede

interpretar erróneamente la información alterada, generando falsos positivos, falsos negativos o clasificaciones diagnósticas incorrectas. En consecuencia, estos ataques representan una amenaza crítica para la integridad y confiabilidad de los sistemas de apoyo diagnóstico basados en inteligencia artificial, ya que comprometen la toma de decisiones clínicas incluso cuando la manipulación no es detectable visualmente por el personal médico.

Asimismo, estos ataques son la introducción de perturbaciones mínimas en los píxeles de las imágenes médicas, que pueden pasar desapercibidas en la visualización, pero, inducen cambios significativos en la interpretación humana o en los algoritmos de inteligencia artificial empleados en radiología (Goodfellow et al., 2015). Las consecuencias son significativas ya que un ataque adversarial puede simular lesiones inexistentes, ocultar tumores o generar patrones patológicos falsos, afectando directamente el proceso diagnóstico. Magdy et al., (2022) indican que la manipulación malintencionada de imágenes diagnósticas puede derivar en errores médicos, retrasos en el tratamiento e incluso eventos adversos graves para el paciente.

Frente a este panorama, las estrategias de mitigación incluyen el entrenamiento adversarial de modelos de IA, la validación robusta de algoritmos, la implementación de sistemas de detección de anomalías y el uso de inteligencia artificial explicable para identificar comportamientos inusuales en las imágenes médicas (OMS, 2021). Además, investigaciones recientes proponen el uso de sistemas de IA de seguridad o meta-IA capaces de detectar patrones de manipulación adversarial antes de que las imágenes sean interpretadas clínicamente. Este enfoque genera un modelo de defensa basado en inteligencia artificial contra ataques dirigidos a otros sistemas de IA, fortaleciendo la confiabilidad y la seguridad diagnóstica en entornos radiológicos digitales.

Inyección de Malware en Archivos DICOM

Otra vulnerabilidad tiene relación con la posibilidad de utilizar archivos DICOM como contenedores para códigos maliciosos, incluyendo estructuras complejas de datos y metadatos, ocultando códigos maliciosos con técnicas como esteganografía o ejecutando softwares maliciosos en los sistemas (Monzón, 2022).

Este tipo de ataques afectan las redes de las infraestructuras hospitalarias y, en consecuencia, cuando se introducción un malware en el sistema, se podrían comprometer la integridad de los datos médicos o afectar el funcionamiento de los sistemas (Figueredo et al., 2025).

Configuraciones Incorrectas y Exposición de Puertos

Otro factor es la vulnerabilidad de los sistemas de imágenes con la mala configuración de los servicios de red usados para la transmisión de archivos DICOM, en el puerto 104, cuando queda expuesto en redes públicas sin control de acceso o autenticación, actores maliciosos identifican los servidores, los que acrecienta el riesgo de accesos no autorizados a imágenes médicas o a información clínica guardada en los sistemas hospitalarios (Castañeda et al., 2024).

La innovación de la digitalización de los sistemas de salud ha aumentado la superficie de ataque de las infraestructuras hospitalarias, donde la prioridad es establecer estrategias de ciberseguridad para proteger los sistemas de información clínica y garantizar la confidencialidad de los datos de los pacientes para reducir los riesgos asociados a los ciberataques en el sector salud (González, 2023).

Marco Normativo y Ético

En la teleradiología y el intercambio de imágenes con el estándar DICOM, la protección de los datos del paciente es fundamental por la sensibilidad de los datos

contenidos en los archivos y sus metadatos. En el contexto internacional, la Health Insurance Portability and Accountability Act (HIPAA) establece los estándares de protección de la información médica identificable, PHI, para regular el almacenamiento, transmisión y acceso a los datos de salud, exigiendo a las instituciones la implementación de controles de seguridad que no permitan el acceso no autorizado y la divulgación indebida de información (Monzón, 2022).

De igual forma, el Reglamento General de Protección de Datos (RGPD) en Europa dicta las directrices para el tratamiento de datos personales, incluyendo los datos biomédicos que son de alta sensibilidad, exigiendo a las instituciones, medidas técnicas y organizativas adecuadas para proteger la información personal durante su procesamiento y transmisión, esencialmente cuando se usan sistemas digitales para la gestión de datos médicos (González, 2023).

En Colombia, el desarrollo de telemedicina y teleradiología tiene marcos regulatorios que garantizan la seguridad de la información clínica. La Resolución 2160 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones instaura los requisitos mínimos de seguridad para los sistemas de información, el uso de protocolos de cifrado, redes privadas virtuales (VPN) y mecanismos de autenticación que permitan proteger los datos transmitidos a través de redes públicas (Ministerio TIC, 2020).

Asimismo, el desarrollo de proyectos de teleradiología en el país ha demostrado la importancia de implementar estándares técnicos y protocolos de seguridad adecuados para garantizar la transmisión segura de imágenes médicas entre instituciones de salud, especialmente en regiones donde el acceso a especialistas es limitado (Vidal, 2020).

Estrategias de Mitigación y Ciberseguridad en la Gestión de Imágenes

Los sistemas RIS y PACS necesitan estrategias de ciberseguridad robusta que permitan garantizar la integridad, confidencialidad y disponibilidad de los datos clínicos de los pacientes.

Una de las principales estrategias es la de anonimización y desidentificación de datos, para eliminar o modificar la información sensible contenida en los metadatos de DICOM antes de la transmisión, así se reduce el riesgo de exposición de los datos personales del paciente (Henao y Moscoso, 2013).

Otra medida es el uso de redes privadas virtuales (VPN) y túneles seguros para la transmisión de información, donde crean canales cifrados de comunicación sobre redes públicas, garantizando que los datos enviados entre instituciones de salud no puedan ser interceptados por terceros durante su tránsito (Lugo et al., 2011).

También, se deben fortalecer estrategias de ciberseguridad en los sistemas RIS/PACS, por medio de controles de acceso, cifrado de datos y monitoreo de redes, para prevenir vulnerabilidades que comprometan la privacidad de los pacientes y la integridad de la información médica (NOVA Imaging, 2026).

Además, con mecanismos de seguridad de Transport Layer Security (TLS), definidos en la Parte 15 del estándar DICOM, que protegen la comunicación entre dispositivos médicos mediante cifrado, autenticación y control de acceso, su implementación es crucial para la prevención de ataques como la interceptación de datos o el acceso no autorizado a servidores (Velandia y Rivera 2025).

De igual forma, el uso de firmas digitales, que verifican que un archivo no ha sido modificado desde el momento en que fue generado por el dispositivo médico, otorgando

autenticidad y trazabilidad en la transmisión de imágenes diagnósticas, que es primordial en la preservación de la confiabilidad de los procesos clínicos (Velandia y Rivera, 2025).

Igualmente, la implementación de protocolos como IPsec y SSL/TLS permite crear túneles seguros para proteger la comunicación entre dispositivos y servidores de imágenes médicas, reduciendo significativamente los riesgos de ataques o interceptaciones durante el proceso de transferencia (Lugo et al., 2011). Además, la adopción de protocolos de seguridad robustos permite prevenir accesos no autorizados y proteger los datos sensibles de los pacientes durante su transmisión entre diferentes sistemas (Velandia y Rivera, 2025).

Firmas Digitales

Las firmas digitales son un mecanismo básico para garantizar la integridad y autenticidad de las imágenes médicas transmitidas mediante el sistema DICOM, que permite verificar que el archivo no ha sido modificado desde su generación por el dispositivo o almacenamiento en el PACS, asegurando que la información mantenga su estado original en los diferentes procesos de los sistemas de información.

Por medio de las técnicas criptográficas, las firmas digitales identifican al emisor del archivo y manifiestan cualquier alteración, esto ayuda a preservar la confiabilidad de los diagnósticos clínicos y evita manipulaciones que comprometen la interpretación de las imágenes médicas (Henao y Moscoso, 2013). Por lo tanto, la implementación de firmas digitales en los sistemas de imágenes es una práctica que fortalece la ciberseguridad en la gestión de estudios radiológicos, favoreciendo la integridad de los datos clínicos, protegiendo la autenticidad de las imágenes médicas y garantizando la confiabilidad de los diagnósticos.

En conclusión, los avances tecnológicos han mejorado la gestión, almacenamiento y transmisión de imágenes diagnósticas con estándares como DICOM. Sin embargo, han

generado nuevos desafíos de ciberseguridad y protección de datos, con brechas como la falta de cifrado en la comunicación, configuraciones inseguras en servidores PACS, exposición de metadatos con información sensible y ausencia de mecanismos robustos de autenticación y control de acceso.

Por esta razón, es importante conocer la estructura DICOM, las vulnerabilidades, los pros y contras y las prácticas de mitigación. Esta investigación responde a la pregunta de investigación planteada, orientada a determinar cuáles son las principales vulnerabilidades que afectan la transmisión segura de imágenes DICOM en los sistemas digitales de salud.

Metodología

El presente estudio se desarrolló mediante un diseño no experimental y documental, con un tipo de análisis cualitativo, orientado al análisis de las brechas de seguridad presentes en la transmisión de imágenes DICOM a través de redes públicas. De acuerdo con Hernández et al., (2014), los estudios documentales permiten examinar fenómenos complejos sin manipulación de variables, a partir de la interpretación sistemática de información previamente publicada en fuentes científicas, técnicas y normativas.

Tipo y Diseño de Investigación

La investigación es no experimental, con un diseño documental, analítico y descriptivo, ya que se fundamenta en la revisión, comparación y síntesis de literatura especializada sobre vulnerabilidades del protocolo DICOM, ciberseguridad, transmisión de datos médicos e infraestructura hospitalaria digital.

Enfoque del Estudio

El estudio adopta un enfoque cualitativo con orientación descriptiva y analítica, adecuado para comprender cómo emergen las vulnerabilidades en la transmisión de imágenes médicas, su contexto operativo, tecnológico y organizacional, así como las implicaciones clínicas, éticas y de seguridad asociadas. Como afirman Hernández et al., (2014), el enfoque cualitativo permite interpretar la realidad desde perspectivas y hallazgos de distintos autores, sin el uso de instrumentos estandarizados.

Método

Se empleó un método de revisión literaria sistemática, exhaustiva y narrativa, orientado a: identificar vulnerabilidades en redes y protocolos de transmisión, analizar riesgos en sistemas DICOM, PACS y flujos de radiología, sintetizar tendencias y

recomendaciones presentes en la literatura científica y técnica y reconocer patrones de fallo, configuraciones inseguras y brechas técnicas.

Criterios de Inclusión

Para la selección del material bibliográfico se establecieron criterios de inclusión que permitieran garantizar la pertinencia, actualidad y rigor científico de las fuentes consultadas. Se incluyeron artículos publicados entre los últimos diez años, documentos científicos y técnicos relacionados directamente con la transmisión de imágenes médicas en formato DICOM, ciberseguridad en sistemas hospitalarios, vulnerabilidades en redes públicas, exposición de metadatos, fallos de autenticación, configuraciones de servidores PACS/RIS y protocolos de comunicación. También se consideraron normativas internacionales, reportes técnicos especializados y revisiones sistemáticas provenientes de bases de datos reconocidas como Scopus, PubMed, IEEE Xplore, ScienceDirect, SpringerLink, PubMed, Google Académico, Biblioteca virtual UNAD, Researchgate.

Criterios de Exclusión

Se excluyeron documentos con información redundante o irrelevante para la pregunta de investigación, publicaciones anteriores al año establecido, artículos sin respaldo metodológico, documentos con sesgos evidentes, textos orientados únicamente a aspectos clínicos sin relación con la seguridad digital, así como estudios que no abordaran específicamente la transmisión de imágenes DICOM o que carecieran de fundamento técnico para el análisis de vulnerabilidades. Estos criterios permitieron consolidar un corpus documental coherente, confiable y adecuado para el desarrollo de la revisión.

Fases Metodológicas

Tabla 1

Fases Metodológicas de la Investigación

Fase	Descripción	Actividades
Fase 1. Delimitación Temática y Formulación del Problema	Definición del objeto de estudio, pregunta problema.	Definición del problema y alcance. Identificación de conceptos clave: DICOM, ciberseguridad, redes públicas. Diseño de la estrategia de búsqueda con palabras clave, operadores booleanos y filtros.
Fase 2. Búsqueda y Selección Sistemática de Información	Recolección de literatura científica, técnica y normativa.	Búsqueda en bases de datos como Scopus, ScienceDirect, PubMed, Google Académico, Biblioteca virtual UNAD, Researchgate. Palabras clave: DICOM, PACS, vulnerabilidades, metadatos. Aplicación de criterios de inclusión/exclusión. Selección de estudios, normas y reportes relevantes.
Fase 3. Análisis Crítico y Clasificación Temática	Categorización de la información y organización de los hallazgos.	Lectura crítica y extracción de datos relevantes. Artículos encontrados inicialmente 147, con el filtro preliminar de pertinencia temática se seleccionaron 62 documentos relacionados con DICOM, PACS, RIS y ciberseguridad radiológica. Después de la lectura y evaluación metodológica, se incluyeron finalmente 38 referencias que cumplen con los criterios de actualidad y relación con la problemática estudiada. Se excluyeron documentos por duplicidad, poca relación con la temática, falta de contenido técnico sobre ciberseguridad

Fase	Descripción	Actividades
		radiológica o de respaldo académico verificable. Clasificación por categorías: metadatos, servidores, redes públicas, vulnerabilidades y brechas en DICOM, PHI, fallos de autenticación y cifrado, Configuraciones inseguras de servidores PACS y RIS. Identificación de patrones, tendencias y principales riesgos asociados a la seguridad de imágenes médicas en entornos hospitalarios y de teleradiología.
Fase 4. Interpretación, Conclusiones, Recomendaciones y propuesta	Integración de la información, conclusiones, recomendaciones y propuesta.	Síntesis de hallazgos y evaluación de implicaciones. Elaboración de conclusiones. Recomendaciones y propuesta.

Nota. Autoría propia

Análisis de Resultados

A partir de la revisión documental, se identificaron patrones recurrentes de vulnerabilidad en la transmisión de imágenes DICOM. En la fase 3 se clasificaron los hallazgos en categorías clave, evidenciando que las brechas de seguridad no solo son tecnológicas, sino también operativas y organizacionales.

Los hallazgos del estudio concuerdan con Cervera y Goussens (2024), que señalan que la transformación digital en salud ha incrementado la superficie de ataque de los sistemas clínicos, sobre todo cuando se emplean redes públicas sin controles robustos de seguridad.

La mayoría de las vulnerabilidades analizadas se originan en la herencia tecnológica del estándar DICOM, desarrollado en los años 80 y 90 para operar en redes hospitalarias cerradas (NEMA, 2023). Esta arquitectura inicial no contemplaba amenazas modernas como ataques MITM, inyección de malware o manipulación adversarial de imágenes, lo que genera una deuda de seguridad difícil de corregir sin rediseñar completamente componentes del protocolo.

Tabla 2

Brechas de seguridad identificadas en la literatura

Vulnerabilidad	Causas / deuda tecnológica	Impacto clínico, legal y económico	Estrategias de mitigación	Frecuencia / Severidad o Tendencia	Autores
Falta de cifrado (cleartext)	DICOM fue diseñado para redes cerradas y no incorporó cifrado nativo; dependencia de protocolos antiguos; ausencia de integración con TLS/SSL; configuraciones inseguras por defecto.	Interceptación de datos, exposición de PHI, sanciones legales (Ley 1581, RGPD), pérdida reputacional y alteración diagnóstica.	Implementación de TLS/SSL y VPN IPSec; requiere compatibilidad entre equipos; limitación en dispositivos antiguos.	Alta / Creciente por el aumento de la teleradiología y transmisión remota de imágenes.	Lugo et al. (2011); Zhang et al. (2007); U.S. HHS (2013).
Exposición de servidores PACS	Falta de endurecimiento del servidor; puertos abiertos (104/11112); acceso desde Internet sin autenticación; configuraciones heredadas inseguras.	Acceso no autorizado a imágenes médicas, fuga masiva de PHI, costos forenses y pérdida de confianza institucional.	Firewalls, Zero Trust Network Access y segmentación de red; requiere monitoreo continuo.	Alta / Creciente por el incremento de servidores expuestos en redes públicas.	Marco et al. (2020); Rapid7 (2026); TXOne Networks (2025).
Fugas de metadatos (PHI)	DICOM contiene metadatos extensos; deficiente anonimización; errores de configuración en teleradiología.	Violación de confidencialidad, sanciones legales, riesgo de reidentificación y fraude.	Anonimización DICOM y automatización de eliminación de PHI; requiere capacitación técnica.	Alta / Estable por el uso constante de intercambio de imágenes médicas.	Monzón (2022); Parlamento Europeo (2016); Ley 1581 (2012).

Vulnerabilidad	Causas / deuda tecnológica	Impacto clínico, legal y económico	Estrategias de mitigación	Frecuencia / Severidad o Tendencia	Autores
Configuración insegura de puertos	Uso del puerto 104 por defecto; ausencia de endurecimiento; conexiones externas sin supervisión; limitaciones en equipos heredados.	Escaneo de servidores, ataques DDoS, fuerza bruta y exfiltración de datos.	Cambio de puertos, autenticación mutua TLS y segmentación; bajo costo y alta efectividad.	Media / Creciente por el aumento de conexiones remotas hospitalarias.	Castañeda et al. (2024).
Ataques Man-in-the-Middle (MITM)	Falta de cifrado nativo y autenticación; uso de redes públicas; routers externos no administrados.	Alteración de imágenes diagnósticas, pérdida de confiabilidad clínica y responsabilidades legales.	TLS/SSL, IPSec, certificados digitales y blockchain; requiere administración especializada.	Alta / Creciente por la expansión de teleradiología y servicios remotos.	Huraca (2025); Rai et al. (2025).
Ataques adversariales a IA radiológica	Modelos de IA vulnerables a manipulación de píxeles; falta de validación robusta y estándares de seguridad.	Diagnósticos erróneos, falsos positivos/negativos y pérdida de integridad diagnóstica.	Entrenamiento adversarial, IA explicable y detección de perturbaciones; alto costo técnico.	Media / Creciente por el incremento del uso de IA en radiología.	Goodfellow et al. (2015); OMS (2021).
Malware embebido en archivos DICOM	Posibilidad de insertar payloads maliciosos; ausencia de inspección especializada; herramientas PACS vulnerables.	Compromiso total del sistema, interrupción de servicios y altos costos de recuperación.	Antivirus forense, sandboxing y validación DICOM; requiere actualización constante.	Alta / Creciente por la sofisticación de ciberataques en salud.	Figueredo et al. (2025); ACIS (2022).

Nota. Autoría propia

Según Zhang et al., (2007) la transmisión de imágenes en texto claro es una de las principales debilidades del estándar DICOM, lo que facilita ataques de interceptación. Este resultado se alinea con el presente estudio, donde esta vulnerabilidad aparece como la más recurrente. La responsabilidad por las brechas de seguridad en la transmisión y gestión de imágenes DICOM no recae únicamente sobre las limitaciones históricas del estándar, sino que constituye un problema de corresponsabilidad entre proveedores de tecnología y administradores de TI dentro de las instituciones de salud.

La literatura muestra que muchos fabricantes siguen distribuyendo equipos y servidores con configuraciones por defecto, puertos abiertos, protocolos inseguros como el puerto 104 sin cifrado, autenticación mínima y ciclos de actualización limitados, lo que deja a los PACS y VIS expuestos a ataques externos (Marco et al., 2020). Sin embargo, estas vulnerabilidades se amplifican por prácticas institucionales deficientes, donde los administradores de TI no aplican parches de seguridad oportunos, ni segmentan las redes internas, permitiendo el uso de credenciales débiles y además carecen de capacitación en ciberseguridad clínica, situación evidenciada en estudios nacionales y guías técnicas para el sector salud colombiano (Zambrano y Mora, 2024). Esto provoca un desbalance estructural entre la utilidad clínica del ecosistema radiológico y el imperativo ético y legal de proteger la información sanitaria sensible (PHI), siendo un eje crítico para la ciberseguridad radiológica, obligando a repensar los modelos de gobernanza, las responsabilidades de cada actor y la necesidad de sistemas más seguros desde el diseño.

Asimismo, los riesgos asociados a la manipulación de imágenes mediante ataques adversariales coinciden con Goodfellow et al., (2015)**,** quienes advierten que estas alteraciones pueden pasar desapercibidas por el ojo humano, pero afectan los diagnósticos médicos, lo que representa un riesgo clínico crítico. En Colombia, el Ministerio de Salud

(2023) subraya la necesidad de implementar mecanismos como VPN, cifrado y autenticación robusta para garantizar la seguridad de la información en sistemas de telemedicina. Además, las tecnologías emergentes son la nueva perspectiva para la protección de imágenes y la gestión segura del ecosistema DICOM, con alternativas que superan las limitaciones de los mecanismos tradicionales de cifrado y control de acceso. Asimismo, el uso de blockchain es una solución robusta para garantizar la trazabilidad, la integridad y la inmutabilidad de los registros radiológicos, permitiendo auditorías transparentes y reduciendo el riesgo de alteraciones maliciosas en la cadena de custodia de la información (Cortés, 2023).

También, la criptografía post-cuántica avanza hacia la creación de esquemas criptográficos resistentes a ataques de futuros computadores cuánticos, lo que representa un componente estratégico para proteger la transmisión de imágenes diagnósticas a largo plazo y responder a amenazas que los sistemas actuales basados en curvas elípticas o RSA no podrían mitigar (Abdullaeva et al., 2024). En conjunto, estas tecnologías emergentes no solo contribuyen a cerrar brechas históricas en la seguridad del estándar DICOM, sino que también establecen las bases para modelos de protección más resilientes, automatizados y alineados con el futuro de la radiología digital, además, la investigación evidencia que las brechas de seguridad en DICOM no solo derivan de limitaciones del protocolo, sino también de la falta de implementación de buenas prácticas de ciberseguridad, lo que requiere un enfoque integral que combine tecnología, gestión y regulación.

La literatura coincide en que el estándar DICOM fue diseñado primero para la interoperabilidad. Por esta razón, carece de cifrado nativo, siendo un riesgo cuando se emplean redes públicas de internet (Zhang et al., 2007). Esta debilidad estructural se confirma con los hallazgos donde aparece el cleartext como la vulnerabilidad más habitual.

Para sintetizar la información encontrada en la literatura, se categorizan las principales brechas de seguridad reportadas en la transmisión de archivos DICOM a través de redes públicas. Las brechas se agrupan según su origen tecnológico, estrategias de mitigación y el impacto sobre la información clínica.

Tabla 3

Causas, consecuencias y estrategias de mitigación de brechas de seguridad DICOM

Causas	Brecha de seguridad	Consecuencias	Estrategias de mitigación	Autores
Falta de implementación de protocolos seguros	Transmisión en texto plano (cleartext)	Interceptación de imágenes y datos del paciente	Implementación de TLS/IPsec y VPN	Lugo et al., (2011)
Deficiente configuración de infraestructura TI	Exposición de servidores PACS	Acceso no autorizado y fuga de información	Uso de firewalls, segmentación de red	Marco et al., (2020)
Ausencia de anonimización de datos	Fugas de metadatos (PHI)	Violación de privacidad del paciente	Desidentificación de datos DICOM	Monzón (2022)
Falta de autenticación en comunicación DICOM	Ataques de suplantación (SCU/SCP)	Manipulación de estudios médicos	Implementación de autenticación fuerte	ACIS (2022)
Uso de redes públicas sin protección	Ataques Man-in-the-Middle	Alteración de imágenes diagnósticas	Uso de túneles seguros (VPN)	Huraca (2025)
Baja cultura de ciberseguridad organizacional	Configuraciones inseguras persistentes	Incremento de vulnerabilidades sistémicas	Capacitación y políticas de seguridad	Bernal (2024)
Falta de validación de archivos	Inserción de malware en DICOM	Daño a sistemas PACS/RIS	Sistemas de detección y análisis de archivos	Figueredo et al., (2025)
Avances en IA sin control de seguridad	Ataques adversariales	Diagnósticos erróneos o manipulados	Validación de integridad y firmas digitales	Goodfellow et al., (2015)

Nota. Autoría propia

Asimismo, los estudios revisados reportan que muchos servidores PACS continúan operando con puertos abiertos y configuraciones predeterminadas, haciéndolos detectables mediante escaneos automatizados (Rapid7, 2026). Lo que se relaciona con la falta de conocimiento del personal técnico y de auditorías de seguridad. Marco et al. (2020) señalan que más de 80% de los incidentes en PACS se basan en configuraciones incorrectas.

En la transmisión, la ausencia de TLS permite ataques de interceptación Man-in-the-Middle, como refieren Lugo et al., (2011). Estos ataques pueden modificar píxeles y alterar diagnósticos, como documentan Abdullaeva et al., (2024) en casos de manipulación adversarial.

De igual forma, los resultados muestran que la digitalización de la radiología ha desarrollado más exposición de los sistemas. Si bien la conectividad entre modalidades, PACS y RIS garantiza eficiencia diagnóstica, también genera puntos críticos en la transmisión, especialmente en gateways y nodos que funcionan como intermediarios (Rai et al., 2025). Esta situación se agrava cuando la transmisión se realiza a través de redes públicas, donde la institución no tiene control sobre la infraestructura subyacente, lo que amplifica las vulnerabilidades inherentes.

En Colombia, donde la interoperabilidad está en expansión, las brechas de seguridad se aumentan cuando no existen políticas robustas de cifrado y autenticación (Ministerio de Salud, 2023). En síntesis, la evidencia muestra que la protección de imágenes DICOM depende del estándar técnico y del ecosistema que las gestiona, como PACS, RIS, servidores, redes y personal. Las brechas de seguridad identificadas tienen consecuencias graves como la exposición de PHI, alteración de diagnósticos e incluso ataques que comprometen toda la infraestructura hospitalaria.

Finalmente, el fortalecimiento de la ciberseguridad en radiología requiere un enfoque multidimensional que considere tecnologías, procesos y cultura organizacional. El uso de TLS, VPN, firewalls, anonimización y monitoreo continuo se presentan como estrategias efectivas para reducir riesgos, tal como señalan Mathur et al. (2025).

A partir de la revisión literaria y de las fases metodológicas con categorías de impacto relacionadas con incidentes de seguridad en la transmisión de archivos DICOM por redes públicas. Para analizarlos se empleó una clasificación por categorías de impacto CIAA, Confidencialidad, Integridad, Disponibilidad, Autenticidad.

Tabla 4

Categorías de brechas de seguridad en la transmisión DICOM

Categoría	Impacto	Brechas	Autores
Confidencialidad	Exposición de datos personales, PHI y metadatos sensibles durante la transmisión en redes públicas	Cleartext, fuga de metadatos, PACS expuestos, puertos abiertos	Monzón (2022); Lugo et al. (2011)
Integridad	Alteración de píxeles, manipulación de imágenes o modificación de cabeceras DICOM	Ataques MitM, ataques adversariales, manipulación SCU/SCP	Goodfellow et al., (2015); Huraca (2025)
Disponibilidad	Interrupción de servicios, bloqueo de PACS, corrupción de archivos DICOM	Inyección de malware, ransomware, denegación de servicio	Figueredo et al., (2025); Bernal (2024)
Autenticidad	Suplantación de dispositivos DICOM y falsificación de origen de estudios	Falsificación de UIDs, alteración de tags, spoofing DICOM	ACIS (2022); Castañeda et al. (2024)

Nota. Autoría propia

La literatura evidencia que la mayoría de brechas se causan por transmisiones sin cifrado, exposición de servidores PACS y fallos de configuración, como señalan Lugo et al., (2011). La presencia de cleartext en archivos DICOM enviados por redes públicas manifiesta la debilidad estructural del estándar en su versión original (Monzón, 2022).

Asimismo, los puertos abiertos, la autenticación débil y uso de protocolos TCP/IP sin encapsulación generan un entorno de alto riesgo, en especial en instituciones con poca madurez digital (Bernal, 2024). Algunos estudios validan la vulnerabilidad del puerto DICOM 104, capaz de ser detectado mediante escaneo público (Rapid7, 2026). Asimismo, los ataques adversariales descritos por Goodfellow et al., (2015) y Abdullaeva et al., (2024) representan una amenaza emergente debido al incremento del uso de IA en radiología.

El análisis confirma que las brechas de seguridad tienen impacto tecnológico y clínico-administrativo. La exposición de imágenes médicas afecta la confianza del paciente, la legalidad del proceso diagnóstico y la continuidad del servicio. Las instituciones deben adoptar acciones como cifrado TLS/Ipsec, segmentación de red, anonimización de metadatos, VPN para transmisión externa y monitoreo continuo (Mathur et al., 2025).

Aunque existen medidas de mitigación como TLS/IPsec, segmentación de red, VPN y anonimización de datos, su implementación en entornos hospitalarios tiene desafíos como TLS/IPsec ha demostrado ser una solución efectiva para proteger la confidencialidad e integridad de la información durante la transmisión. Lugo et al. (2011) evidencian que mejoran bastante la seguridad en entornos de teleradiología; sin embargo, su implementación puede verse limitada por la incompatibilidad con sistemas PACS antiguos, generando interoperabilidad y aumento en la complejidad de configuración en infraestructuras clínicas heredadas. De manera similar, Mathur et al. (2025) señalan que la coexistencia de sistemas modernos con tecnologías legacy dificulta la adopción uniforme de estándares de cifrado.

Asimismo, la segmentación de red reduce la superficie de ataque al aislar sistemas en la infraestructura hospitalaria. No obstante, su implementación requiere una arquitectura de red avanzada y personal capacitado, lo cual no siempre está disponible en instituciones

de salud con limitaciones técnicas o presupuestales. Zambrano y Mora (2024) destacan que la falta de madurez en ciberseguridad institucional en el sector salud colombiano limita la aplicación efectiva de este tipo de controles.

Además, la infraestructura hospitalaria tiene un desafío estructural importante. Cervera y Goussens (2024) coinciden en que los hospitales operan con sistemas heterogéneos, dispositivos médicos de diferentes generaciones y múltiples proveedores tecnológicos, lo que dificulta la estandarización de políticas de seguridad y la integración de soluciones avanzadas de protección.

También, el factor humano es esencial en la efectividad de las medidas de seguridad. Bernal (2024) señala que la falta de capacitación en gestión de incidentes y seguridad de la información en el personal sanitario contribuye a configuraciones incorrectas y al uso inadecuado de sistemas. Asimismo, Zambrano y Mora (2024) resaltan que la resistencia al cambio y la baja cultura en ciberseguridad en entornos clínicos limitan la adopción sostenida de buenas prácticas.

Igualmente, la literatura muestra que la seguridad en entornos DICOM no puede abordarse solo desde la perspectiva tecnológica. Según ISO/IEC 27001 (2022), la protección de la información debe basarse en un sistema de gestión integral que combine controles técnicos, administrativos y organizacionales. Mathur et al. (2025) enfatizan que la efectividad de las soluciones depende de la integración entre tecnología, formación del personal y gobernanza institucional.

En resumen, aunque existen soluciones tecnológicas robustas para la protección de imágenes médicas, su implementación en entornos hospitalarios se ve limitada por factores de compatibilidad tecnológica, falta de recursos especializados, heterogeneidad de sistemas y debilidades en la cultura organizacional. Por ello, se requiere un enfoque integral que

incluya la infraestructura tecnológica, capacitación continua y políticas institucionales de ciberseguridad para garantizar una protección efectiva de la información. Profundizar en la interconexión de estos factores resulta fundamental para comprender la complejidad de las vulnerabilidades en los sistemas de información utilizados en radiología.

A la par, la capacitación del personal influye directamente en la adecuada gestión de la infraestructura tecnológica y en la correcta implementación de procesos seguros, lo cual reduce los riesgos asociados a fallas operativas y errores humanos, considerados uno de los vectores más frecuentes según la literatura reciente. El componente humano es crucial en la aparición de brechas. La falta de capacitación del personal de salud y de los administradores de sistemas facilita errores como el uso indebido de credenciales, acceso a redes inseguras y apertura de archivos maliciosos.

Según Mejía et al. (2023), los errores humanos continúan siendo una de las principales causas de incidentes de seguridad en el sector salud. La capacitación del personal influye directamente en la adecuada gestión de la infraestructura tecnológica y en la correcta implementación de procesos seguros, reduciendo los riesgos derivados de fallas operativas. En este sentido, la literatura coincide en que el fortalecimiento de las competencias digitales y la formación continua son elementos esenciales para mitigar vulnerabilidades y garantizar un entorno seguro en radiología.

Asimismo, es necesario considerar el impacto de las regulaciones nacionales e internacionales diseñadas para mitigar estas vulnerabilidades, como las normas de protección de datos, los lineamientos de telesalud, la normativa sobre historia clínica y los estándares de seguridad de la información. Estas directrices establecen marcos de actuación que buscan fortalecer la protección de los datos clínicos; sin embargo, su eficacia depende

de la articulación real entre infraestructura tecnológica, talento humano capacitado y políticas institucionales sólidas.

El análisis evidencia que, aunque DICOM garantiza interoperabilidad, no fue diseñado originalmente con un enfoque de seguridad, presenta debilidades como mensajes en plaintext, metadatos visibles, autenticación ausente en solicitudes y vulnerabilidad en comandos C-STORE y C-MOVE, carece de mecanismos de cifrados nativos, dejando la protección en la infraestructura de red (Castañeda et al., 2024).

Asimismo, la literatura muestra que miles de servidores PACS han sido indexados por buscadores como Shodan, exponiendo imágenes y metadatos sin autenticación. Según Marco et al., (2020)**,** esta exposición permite que actores no autorizados descarguen estudios completos.

Según Rapid7 (2026) muchos hospitales mantienen puertos abiertos directamente a internet, facilitando ataques basados en escaneo automatizado. Y que los ataques adversariales y MITM representa amenazas como los ataques adversariales definidos por Goodfellow et al., (2015) que alteran pixeles sin ser detectados y los ataques MITM descritos por Huraca (2025) que permiten modificar estudios en tránsito, afectando la integridad del diagnóstico, donde estos ataques pueden modificar lesiones, borrar tumores o simular patologías, lo que compromete la seguridad del paciente.

El análisis de la literatura también permitió identificar que las brechas de seguridad no son producto de un único fallo, sino del efecto acumulativo de múltiples factores interrelacionados. Los sistemas DICOM, PACS y la infraestructura de red son el centro del problema. La falta de cifrado en la transmisión de datos, como lo indican Lugo et al., (2011), facilita ataques de interceptación.

Asimismo, la exposición de puertos y el uso de software desactualizado incrementan significativamente la superficie de ataque. No obstante, estas fallas son el resultado de una gestión deficiente de la infraestructura tecnológica, donde la actualización y el mantenimiento no siguen estándares uniformes.

Tabla 5

Brechas de seguridad y tipos de vulnerabilidad

Categoría	Brechas	Descripción	Consecuencias	Autores
Fallos de comunicación	Falta de autenticación mutua	Conexiones DICOM sin validación SCU–SCP	Riesgo de suplantación y acceso ilegítimo	Roo (2004)
Estructural DICOM	Manipulación de comandos C-STORE	Alteración de solicitudes de almacenamiento	Corrupción de estudios o pérdida parcial de imágenes	Castañeda et al. (2024)
Exposición operativa	PACS accesibles por Shodan	Detectables por escaneo automático de internet	Descarga no autorizada de imágenes	Marco et al. (2020)
Fallos humanos	Configuraciones por defecto	Servidores con contraseñas débiles o públicas	Acceso externo y fuga de PHI	Zambrano & Mora (2024)
Ataques emergentes	Perturbaciones adversariales	Manipulación de píxeles imperceptible	Diagnósticos alterados o eliminación de lesiones	Goodfellow et al. (2015)
Infraestructura	Uso de puertos estándar expuestos	Puerto DICOM 104 sin filtrado	Identificación y ataque directo a nodos	Rapid7 (2026)
Seguridad lógica	Metadatos sin anonimización	Datos personales visibles en tránsito	Violación de confidencialidad del paciente	Monzón (2022)

Nota. Autoría propia

Los procesos operativos son los puntos débiles en la seguridad. Configuraciones por defecto, mala gestión de accesos y ausencia de controles de autenticación robusta permiten el acceso a usuarios no autorizados. Zambrano y Mora (2024) destacan que muchas brechas se originan por errores básicos de configuración, lo que evidencia la falta de protocolos

operativos estandarizados y la carencia de auditorías continuas que aseguren la correcta implementación de las medidas. Profundizar en la interconexión de estos factores es crucial para entender la complejidad de las vulnerabilidades, pues cuando los protocolos no se actualizan o se aplican de forma correcta, la infraestructura tecnológica se expone a fallas operativas que se amplifican entre sí.

Además, la ausencia de políticas claras de seguridad y la baja inversión en ciberseguridad generan entornos vulnerables. Bernal (2024) señala que muchas instituciones de salud en Colombia presentan baja capacidad de respuesta ante incidentes, lo que agrava el impacto de los ataques. esto se agrega la necesidad de considerar el impacto de regulaciones nacionales e internacionales, como las normativas de protección de datos, los lineamientos de telesalud, la normativa sobre historia clínica y los estándares de seguridad de la información, que, aunque buscan fortalecer la protección de la información clínica, requieren una articulación real entre infraestructura tecnológica, talento humano capacitado y políticas institucionales sólidas para ser verdaderamente efectivas.

El análisis de los factores tecnológicos, operativos, organizacionales y humanos revela que las brechas de seguridad en la transmisión y gestión de imágenes DICOM no se originan en un único punto, sino en la interacción entre múltiples componentes del ecosistema digital radiológico. Los hallazgos muestran que las vulnerabilidades más críticas emergen cuando los servidores DICOM, PACS y RIS son implementados sin controles de seguridad integrales, lo cual coincide con lo planteado por Marco et al., (2020) evidencian que incluso instituciones con infraestructura moderna presentan fallos derivados de configuraciones débiles.

Tabla 6

Factores que favorecen las brechas de seguridad en DICOM, PACS y RIS

Factores	Sistema	Riesgo	Brecha de seguridad	Autores
Tecnológico	Servidores DICOM	Falta de cifrado TLS/SSL en la comunicación	Permite interceptación de datos en tránsito (ataques MITM)	Lugo et al., (2011)
Tecnológico	PACS	Sistemas desactualizados o sin parches de seguridad	Explotación de vulnerabilidades conocidas	Marco et al., (2020)
Tecnológico	Infraestructura de red	Puertos abiertos, 104, sin firewall	Facilita escaneo e intrusión externa	Rapid7 (2026)
Operativo	Configuración de sistemas	Uso de configuraciones por defecto	Acceso no autorizado a servidores clínicos	Zambrano y Mora (2024)
Operativo	Gestión de accesos	Falta de control de usuarios y privilegios	Uso indebido de información clínica	ACIS (2022)
Organizacional	Políticas de seguridad	Ausencia de protocolos de ciberseguridad institucional	Falta de prevención y respuesta ante incidentes	Bernal (2024)
Organizacional	Cultura institucional	Baja inversión en seguridad informática	Infraestructura vulnerable y sin monitoreo	Figueredo et al., (2025)
Humano	Personal de salud	Falta de capacitación	Errores humanos (phishing, uso indebido de sistemas)	Mejía et al. (2023)
Humano	Administradores TI	Configuración incorrecta de servidores y de redes	Exposición de datos sensibles	Galiano (2022)

Nota. Autoría propia

Igualmente, se identifica la ausencia de políticas formales de gestión de riesgos y la falta de integración entre áreas de TI y los servicios clínicos. Esto genera escenarios en los que las decisiones de configuración se toman sin considerar los principios de seguridad por

diseño, exacerbando la exposición a ataques de ransomware, fuga de metadatos o manipulación de imágenes (Mejía et al., 2023).

Asimismo, la literatura muestra que los errores de configuración, desconocimiento del protocolo DICOM, uso indebido de credenciales y deficiencias en la administración de accesos constituyen un porcentaje significativo de los incidentes. Zambrano y Mora (2024) señalan que la falta de capacitación continua convierte al personal en un vector crítico para la explotación de vulnerabilidades.

Conclusiones

La transmisión de imágenes DICOM por redes públicas representa un riesgo grande por la ausencia de cifrado nativo del estándar, lo que deja expuestos los datos clínicos a interceptación, manipulación o robo. El crecimiento acelerado de la teleradiología, la interoperabilidad entre sistemas PACS/RIS, la digitalización de la historia clínica electrónica y la integración de inteligencia artificial en el diagnóstico han incrementado considerablemente la exposición de los entornos clínicos a amenazas informáticas. En este contexto, la presente investigación permitió identificar que las brechas de seguridad asociadas a la transmisión de imágenes DICOM no representan únicamente un problema tecnológico, sino también un riesgo clínico, ético, legal y organizacional que puede afectar directamente la seguridad del paciente y la continuidad asistencial.

Los hallazgos evidencian que una de las principales vulnerabilidades continúa siendo la ausencia de cifrado nativo en el estándar DICOM, debido a que este protocolo fue diseñado originalmente para funcionar en redes hospitalarias cerradas y no en entornos abiertos o interconectados a internet. Esta herencia tecnológica facilita la transmisión de imágenes en cleartext, permitiendo la interceptación, manipulación o robo de datos clínicos sensibles durante su intercambio entre modalidades diagnósticas, servidores PACS y estaciones de trabajo. Asimismo, se identificó que la exposición de servidores PACS a redes públicas, el uso de puertos abiertos por defecto, la ausencia de autenticación robusta y las configuraciones inseguras incrementan significativamente la superficie de ataque de los sistemas radiológicos.

De igual forma, la revisión permitió concluir que las brechas de seguridad no se originan exclusivamente en las limitaciones técnicas del estándar DICOM, sino principalmente en factores operativos, administrativos y humanos. Las configuraciones

deficientes de servidores, la falta de segmentación de redes, el uso de credenciales débiles, la ausencia de auditorías periódicas y la insuficiente capacitación del personal sanitario y tecnológico facilitan la explotación de vulnerabilidades críticas. En consecuencia, la seguridad del ecosistema radiológico depende tanto de la infraestructura tecnológica como de las prácticas institucionales y del nivel de cultura organizacional en ciberseguridad.

Otro hallazgo relevante corresponde a las fugas de metadatos y PHI (Protected Health Information), las cuales representan una amenaza constante para la confidencialidad de la información médica. Los archivos DICOM contienen datos sensibles del paciente que, si no son anonimizados correctamente, pueden facilitar procesos de reidentificación, fraude o acceso no autorizado a historias clínicas. Estas situaciones generan importantes implicaciones legales relacionadas con normativas nacionales e internacionales como la Ley 1581 de 2012, HIPAA y el Reglamento General de Protección de Datos (RGPD), exponiendo a las instituciones sanitarias a sanciones económicas, pérdida de reputación y responsabilidades éticas derivadas de la vulneración de la privacidad del paciente.

Asimismo, el estudio permitió identificar amenazas emergentes que amplían el panorama tradicional de la ciberseguridad radiológica, especialmente los ataques Man-in-the-Middle (MITM), el malware embebido en archivos DICOM y los ataques adversariales dirigidos a sistemas de inteligencia artificial. Estos últimos representan un riesgo particularmente crítico, ya que las manipulaciones sobre los píxeles de una imagen pueden pasar desapercibidas para el ojo humano, pero inducir errores en los algoritmos de IA utilizados para el apoyo diagnóstico. Esto demuestra que las amenazas actuales no solo buscan comprometer la confidencialidad de los datos, sino también alterar la integridad diagnóstica y afectar directamente la toma de decisiones clínicas, pudiendo ocasionar falsos positivos, falsos negativos, retrasos terapéuticos o eventos adversos en el paciente.

En este sentido, se concluye que la protección efectiva de las imágenes médicas requiere un enfoque integral y multidisciplinario que involucre no solo a profesionales de tecnología e ingeniería, sino también a radiólogos, tecnólogos en imágenes diagnósticas, administradores hospitalarios, expertos en protección de datos y responsables de políticas públicas. La ciberseguridad en radiología no puede abordarse únicamente desde el componente técnico, ya que las decisiones administrativas, los protocolos clínicos, la formación del talento humano y la gestión institucional tienen un papel determinante en la reducción de riesgos.

La literatura revisada demuestra que las estrategias de mitigación más efectivas incluyen la implementación de protocolos de cifrado como TLS/SSL e IPSec, el uso de VPN seguras, la segmentación de redes, el endurecimiento de servidores PACS, la autenticación robusta entre entidades SCU-SCP, la anonimización automática de metadatos y el monitoreo continuo de eventos de seguridad. Sin embargo, también se evidencia que estas medidas requieren actualización constante, inversión tecnológica y capacitación permanente del personal, especialmente en instituciones con infraestructura heterogénea o limitaciones presupuestales.

También, la investigación evidencia que la evolución de las amenazas cibernéticas en salud continuará incrementándose debido a la expansión de la telemedicina, el almacenamiento en la nube, la interoperabilidad hospitalaria y el uso creciente de inteligencia artificial en los procesos diagnósticos. Esto implica que las instituciones sanitarias deberán adaptarse continuamente a nuevos escenarios de riesgo, fortaleciendo sus modelos de gobernanza digital, sus políticas de seguridad y sus capacidades de respuesta ante incidentes informáticos. Del mismo modo, se hace necesario promover investigaciones futuras orientadas al desarrollo de sistemas inteligentes de detección de anomalías, IA

defensiva, blockchain para trazabilidad clínica y mecanismos automatizados de protección de imágenes médicas.

Finalmente, la evidencia demuestra que las brechas de seguridad identificadas tienen un impacto significativo sobre la confidencialidad, integridad y disponibilidad de la información clínica, siendo estas las dimensiones más vulnerables durante la transmisión de imágenes DICOM por redes públicas. Por ello, se concluye que la protección del ecosistema radiológico requiere un enfoque verdaderamente integral que incluya infraestructura tecnológica segura, talento humano capacitado, políticas institucionales sólidas y mecanismos avanzados de protección y monitoreo continuo. Solo a través de la articulación coherente de estos factores será posible garantizar un entorno radiológico resiliente, confiable y preparado para los desafíos presentes y emergentes de la ciberseguridad en salud.

Referencias Bibliográficas

Abdullaeva, M., Turaeva, N., Yadgarova, S., Khalimova, D., Eshonkulova, E., Yomatova, M., & Nazarov, Q. (2024). *Multimedia data processing in an intelligent medical system featuring embedded elliptic curve cryptography*. *E3S Web of Conferences, 538*, 05026. https://dialnet.unirioja.es/servlet/articulo?codigo=10035702

ACIS – Asociación Colombiana de Ingenieros de Sistemas. (2022). Seguridad y ciberseguridad en los dispositivos médicos. *Revista Sistemas*. https://sistemas.acis.org.co/index.php/sistemas/article/view/22/20

Álzate, A. (2009). *Diseño e implementación de un sistema telemático para equipos médicos usando el protocolo de comunicaciones DICOM*. Universidad del Valle, [Trabajo de grado]. https://bibliotecadigital.univalle.edu.co/server/api/core/bitstreams/e3e83db5-f1d8-4abd-8200-e86014bc2858/content

Arias, N. (2019). *Análisis de seguridad de vulnerabilidades y ataques* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/bitstream/handle/10596/33326/naariass.pdf

Bernal, I. (2024). *Panorama de la respuesta a incidentes de seguridad de la información en el sector salud en Colombia* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/bitstream/handle/10596/65204/irbernaln.pdf

Bohórquez, Y. (2025). *Innovaciones tecnológicas en la farmacovigilancia: uso de aplicaciones digitales en la seguridad del paciente* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/bitstream/handle/10596/68339/ybohorquezu.pdf

Castañeda, K., López, J., & Rodríguez, M. (2024). *Fallas de almacenamiento en sistemas PACS* [Proyecto de investigación, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/53752

Cervera, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el sector salud. *Atención Primaria*. *56*(3), 102854. https://www.sciencedirect.com/science/article/pii/S0212656723002871

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial 48587 de octubre 18 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2010). *Ley 1419 de 2010 por la cual se establecen los lineamientos para el desarrollo de la telesalud en Colombia*. Diario Oficial 47922 de diciembre 13 de 2010. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=38741

Congreso de la República de Colombia. (1981). *Ley 23 de 1981: Normas en materia de ética médica*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=286

Cortés, J. (2023). *Modelo de seguridad basado en blockchain para la interoperabilidad de datos clínicos entre sistemas de información de IPS en Colombia* [Tesis de maestría, Instituto Tecnológico Metropolitano]. https://repositorio.itm.edu.co/server/api/core/bitstreams/c42fa2f7-73cb-4fb5-80fe-800af04a6e44/content

Figueredo, F., Rodrigues, S., & Campos, N. (2025). *Saúde sob ataque: Da avaliação de riscos ao desenvolvimento de estratégias de investimentos em cibersegurança na*

área da saúde. [Capítulo de conferencia]. https://figueredofranco.com/static/files/Cap1-SBCAS2025.pdf

Galiano, M. (2022, marzo 29). DICOM como se hackea: el estándar de los hospitales. *Security Artwork*. https://www.securityartwork.es/2022/03/29/dicomo-se-hackea-el-estandar-de-los-hospitales/

García, M. (2014). Implementación de estándares DICOM SR y HL7 CDA para la interoperabilidad de imágenes médicas. *Revista Cubana de Informática Médica, 6*(1), 71–82. https://www.medigraphic.com/pdfs/revcubinfmed/cim-2014/cim141g.pdf

González, M. (2023). *Evolución de la historia clínica digital, retos y dificultades: Avances y desafíos en la seguridad de la historia clínica y el acceso a los datos de salud*. [Repositorio institucional]. http://hdl.handle.net/10835/14572

Goodfellow, I., Shlens, J., & Szegedy, C. (2015). *Explaining and harnessing adversarial examples*. *International Conference on Learning Representations (ICLR 2015).* https://www.researchgate.net/publication/269935591_Explaining_and_Harnessing_Adversarial_Examples

Henao, C., & Moscoso, F. (2013). *Protocolo DICOM en telemedicina* [Trabajo de grado]. Universidad CES. http://hdl.handle.net/10819/1317

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw Hill. https://dialnet.unirioja.es/servlet/libro?codigo=775008

Huraca, J. (2025). *Desarrollo de un sistema de comunicación segura para la transmisión de datos médicos sensibles* [Trabajo de grado, Escuela Superior Politécnica del Litoral]. http://www.dspace.espol.edu.ec/handle/123456789/67400

Lugo, J., Pérez, O., & García, N. (2011). Evaluación de los protocolos IPsec y SSL en la transmisión segura de imágenes diagnósticas en teleradiología utilizando el estándar DICOM. *Revista REDES*. https://revistas.udistrital.edu.co/index.php/REDES/article/view/7184?utm

ISO/IEC. (2022). ISO/IEC 27001: *Information security management systems. International Organization for Standardization.* https://www.iso.org/standard/27001

Lugo, J., Pérez, O., & García, Y. (2011). Evaluación de los protocolos IPSec y SSL en la transmisión segura de imágenes DICOM en teleradiología. *Revista Redes de Ingeniería , 2*(2), 58–67. https://revistas.udistrital.edu.co/index.php/REDES/article/view/7184

Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: A systematic review. *Healthcare 10*(4), 697. https://pmc.ncbi.nlm.nih.gov/articles/PMC8938747/

Marco, E., Klaus, K., & Marc, K. (2020). Cybersecurity in PACS and Medical Imaging: an Overview. *Journal of Digital Imaging 33*, 1527–1542. https://doi.org/10.1007/s10278-020-00393-3

Mathur, N., Seralathan, S., & Kalyanpur, A. (2025). Implementation of cybersecurity systems in teleradiology services - Best practices. *European Society of Medicine.* https://esmed.org/cybersecurity-best-practices-in-teleradiology-services/

Mejía, C., Fernández, J., Carrillo, J., & García J. (2023). Security vulnerabilities in healthcare: an anlysis of medical devices and software. *Med Bil Eng Comput 62,*(1) https://pmc.ncbi.nlm.nih.gov/articles/PMC10758361/

MV informática Nordeste Ltda.. (2016). *Radiografía digital o convencional: entienda las ventajas y desventajas*. https://mv.com.br/es/blog/radiografia-digital-o-convencional--entienda-las-ventajas-y-desventajas

Ministerio de Salud y Protección Social. (2023). *Lineamiento técnico para la operación del resumen digital de atención en salud*. https://www.minsalud.gov.co/Anexos_Normatividad_Nuevo/Lineamiento_tecnico_para_la_operacioon-31-10-2023.pdf

Ministerio de Salud de Colombia. (1999). *Resolución 1995 de 1999 por la cual se establecen normas para el manejo de la historia clínica*. https://www.minsalud.gov.co

Ministerio de Tecnologías de la Información y las Comunicaciones (Resolución 2160/2020). (2020). *Requisitos de seguridad para tecnologías de la información (incluye TLS/SSL, IPSec, VPN)*. https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/resolucion_mintic_2160_2020

Monzón, R. (2022). *Ciberseguridad en infraestructura y dispositivos sanitarios*. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/server/api/core/bitstreams/7b6bc539-31ac-4c2e-9d45-a9d102329f8e/content

National Electrical Manufacturers Association. (2023). *Digital Imaging and Communications in Medicine (DICOM) standard*. https://www.dicomstandard.org/current

National Electrical Manufacturers Association. (s. f.). *History of the DICOM standard*. https://www.dicomstandard.org/history

NOVA Imaging. (2026). Ciberseguridad en RIS/PACS: Cómo proteger imágenes en Colombia. https://novaimaging.co/ciberseguridad-ris-pacs-proteccion-datos-radiologia-colombia/?utm

Organización Mundial de la Salud. (2021). *Ethics and governance of artificial intelligence for health. OMS.*

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Rai. M., Singh, P., Jain, A., Rai, P., Diwakar, S., Yadav, H., Kumar, M., & Rai, J. (2025). Ensuring Data Security in Radiology: Challenges, Standards, and Emerging Solutions. *J Neonatal Surg [Internet], 14*(9S):1107-26. https://www.jneonatalsurg.com/index.php/jns/article/view/9178

Rapid7. (2026 febrero 25). *The hidden risks of exposed DICOM servers in UK healthcare*. https://www.rapid7.com/blog/post/tr-mri-hidden-risks-exposed-dicom-servers-uk-healthcare/

Roo, A. (2004). Red privada virtual como alternativa para el acceso remoto. *Revista Electrónica de Estudios Telemáticos.* Universidad Rafael Belloso Chacín. Venezuela. https://www.redalyc.org/pdf/784/78430103.pdf

Savón, A., & Blanco, H. (2021). Sistema de transmisión interhospitalaria de imágenes médicas. *Orange Journal, 3*(1), 45–52. https://mail.orangejournal.info/index.php/orange/article/view/36/52

TXOne Networks. (2025 mayo 12). *Protecting Medical Data:* Uncovering new vulnerabilities in PACS servers and DICOM viewers.

https://www.txone.com/blog/uncovering-new-vulnerabilities-in-pacs-servers-and-dicom-viewers/

U.S. Department of Health & Human Services. (2013). *Summary of the HIPAA Security Rule*. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Varma, D. (2012). Managing DICOM images: Tips and tricks for the radiologist. *Indian Journal of Radiology and Imaging, 22*(1), 4–13. https://doi.org/10.4103/0971-3026.95396

Velandia, L., & Rivera, S. (2025). *Sistema de cifrado para seguridad en el manejo de imágenes médicas tipo DICOM.* [Tesis de pregrado, Universidad Distrital Francisco José de Caldas]. Repositorio Institucional Universidad Distrital. https://repository.udistrital.edu.co/items/dc46f26c-a24b-489a-9628-4f8477194d1d

Vidal, S. (2020). *La teleradiología como alternativa para el mejoramiento de servicios de salud en Colombia* [Trabajo de grado, UNAD]. https://repository.unad.edu.co/jspui/handle/10596/40259

Zambrano, S., & Mora, D. (2024). *Guía de buenas prácticas de ciberseguridad para entidades de salud en Colombia*. Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/server/api/core/bitstreams/faa7b57e-4268-4c5a-839e-4f4185a3ebf5/content

Zhang, J., Yu, F., Sun, J., Yang, Y., & Liang, C. (2007). DICOM image secure communications with Internet protocols IPv6 and IPv4. https://pubmed.ncbi.nlm.nih.gov/17249405/