Control de calidad y ciberseguridad en la radiología digital: evaluación documental de riesgos en la inteligencia artificial

Verónica Yulieth Cardenas Bedoya

Yeison Andrés Orozco Henao

Asesor

Edna Rocio Jamaica Guio

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias de la Salud -ECISA

Tecnología en Radiología e Imágenes Diagnosticas

2026

Dedicatoria

Este trabajo lo dedicamos a nuestras familias, que han estado con nosotros en cada momento apoyándonos y acompañándonos durante toda nuestra formación académica.

Igualmente, lo dedicamos a nosotros mismos, como un reflejo de nuestra transformación personal y profesional, gracias a la disciplina, la constancia y el compromiso que hemos demostrado durante la realización de este proyecto.

Asimismo, valoramos el recorrido conjunto en la elaboración de este proyecto, que ha posibilitado no solo el fortalecimiento de nuestras habilidades, sino también nuestro desarrollo personal y académico gracias a las responsabilidades compartidas y al trabajo colaborativo.

Por último, este resultado es una muestra de que con perseverancia y disciplina se pueden lograr las metas establecidas. Por ello, dedicamos este logro como reflejo del esfuerzo conjunto y del acompañamiento recibido.

Agradecimientos

Agradecemos a nuestra Tutora del Diplomado de Profundización en Calidad de la Imagen por su orientación, seguimiento y contribuciones académicas a lo largo de este proyecto, que fueron esenciales para alcanzar las metas propuestas.

A la Universidad Nacional Abierta y a Distancia, por brindarnos la formación académica en el programa de Radiología e Imágenes Diagnósticas y darnos los recursos necesarios para consolidar nuestro saber en este ámbito.

Asimismo, queremos agradecer a nuestras familias por su apoyo, comprensión y motivación en este proceso académico, ya que han sido un soporte fundamental para finalizar esta etapa.

Por último, agradecemos a todas las personas que, de forma directa o indirecta, ayudaron en la culminación y desarrollo de este trabajo.

De igual manera, valoramos el trabajo en equipo que se realizó durante la elaboración de este proyecto, mediante el cual fue posible combinar conocimientos, mejorar las capacidades analíticas y fomentar el aprendizaje colaborativo. La participación de los integrantes fue esencial para lograr las metas establecidas y para el avance académico y profesional a lo largo de esta etapa.

Resumen

La transformación digital en los servicios de salud ha impulsado el uso de tecnologías como la inteligencia artificial y la radiología digital, mejorando la precisión, rapidez y eficiencia en el diagnóstico médico. Sin embargo, la implementación de estos sistemas interconectados también ha generado desafíos relacionados con la seguridad de la información, la integridad de los datos y la vulnerabilidad a ciberataques, incluyendo los ataques adversariales que pueden alterar los resultados diagnósticos.

El presente documento corresponde a una revisión bibliográfica orientada a identificar las vulnerabilidades asociadas a estas tecnologías. Mediante la búsqueda de artículos científicos, se analizan las necesidades de fortalecimiento de la ciberseguridad en el campo de la radiología. Se concluye que, aunque los avances tecnológicos favorecen la toma de decisiones clínicas, aún existen importantes retos para garantizar la protección de los datos y la confiabilidad de los sistemas frente a amenazas emergentes.

Palabras Clave: Inteligencia artificial, Radiología digital, Ciberseguridad, Ciberataques, Diagnóstico médico

Abstract

Digital transformation in healthcare services has boosted the use of technologies such as artificial intelligence and digital radiology, improving precision, speed and efficiency in medical diagnosis. However, the implementation of these interconnected systems has also generated challenges related to information security, data integrity and vulnerability to cyberattacks, including adversarial attacks that can alter diagnostic results.

This document corresponds to a bibliographic review aimed at identifying vulnerabilities associated with these technologies. By searching scientific articles, the needs for strengthening cyber security in the field of radiology are analyzed. It is concluded that, even though technological advances favor clinical decision making, there are still important challenges to guarantee data protection and systems reliability in the face of emerging threats.

Keywords: Artificial intelligence, Digital radiology, Cybersecurity, Cyberattacks, Medical diagnosis

Tabla de Contenido

Lista de Tablas

Introducción

La implementación de tecnologías novedosas, como la inteligencia artificial (IA), en los procesos de diagnóstico médico, particularmente en el área de radiología digital, ha sido impulsada por el progreso de la transformación digital en el sector sanitario. Estas herramientas han hecho posible que el análisis de imágenes médicas sea más preciso, ágil y eficaz, lo que favorece la toma de decisiones clínicas y mejora la atención del paciente (Hardy & Harvey, 2020). No obstante, el uso aumentando de sistemas automatizados y su conexión con redes digitales han creado nuevos retos vinculados a la seguridad de la información, la integridad de los datos y la fiabilidad de los diagnósticos.

En este escenario, uno de los principales peligros emergentes es la susceptibilidad de los sistemas de inteligencia artificial a ataques adversariales. Estos ataques implican cambios sutiles en las imágenes médicas que tienen el potencial de modificar los resultados del análisis sin ser detectados con facilidad. Estos cambios representan un peligro importante para la calidad del diagnóstico, porque pueden generar errores clínicos y poner en riesgo la seguridad del paciente (Di Palma et al., 2025).

Además, al incorporar dispositivos médicos en entornos digitales conectados entre sí, se aumenta la vulnerabilidad a los peligros cibernéticos que pueden comprometer la confidencialidad, integridad y accesibilidad de los datos clínicos. Esto ha hecho que entidades reguladoras y organismos internacionales subrayen la importancia de reforzar la ciberseguridad en los sistemas de salud, mediante la implementación de tácticas para administrar riesgos y controlar la calidad, las cuales aseguren el uso seguro de estas tecnologías (Food and Drug Administration [FDA], 2023).

Este estudio se centra en analizar las deficiencias vinculadas con la aplicación de inteligencia artificial en la radiología digital, considerando una especial atención a los

peligros de ciberseguridad y a los ataques adversariales. Se pretende entender, mediante un análisis documental, de qué manera estas vulnerabilidades afectan la seguridad del paciente y la calidad del diagnóstico médico; además de destacar lo importante que es poner en marcha controles y medidas de protección que hagan posible aumentar la fiabilidad de los sistemas radiológicos.

Planteamiento del Problema

La implementación de la inteligencia artificial (IA) cada vez mayor en el diagnóstico médico y en la radiología digital ha revolucionado la atención sanitaria, ya que ha optimizado la exactitud, eficacia y celeridad en el análisis de imágenes médicas. Sin embargo, esta dependencia de sistemas automatizados ha creado nuevas y graves vulnerabilidades que impactan la seguridad y la fiabilidad de los procesos clínicos. Los modelos de IA que se emplean para examinar imágenes médicas son vulnerables a los ataques de manipulación, o adversarial attacks, que implican alteraciones mínimas y casi invisibles en los píxeles de las imágenes. Estos pueden generar fallos en el diagnóstico sin ser alertados por los profesionales de la salud.

Varios estudios recientes han evidenciado que los sistemas de inteligencia artificial utilizados para el análisis de imágenes médicas pueden ser vulnerables a manipulaciones digitales, las cuales cambian su proceso de detección o clasificación de enfermedades. Investigaciones en el campo de la informática médica indican que ligeras alteraciones en los datos de entrada pueden generar variaciones considerables en las predicciones del modelo, lo que supone un reto significativo para la fiabilidad clínica de estas tecnologías. Por lo tanto, la comunidad científica y las entidades internacionales han empezado a alertar acerca de la importancia de crear marcos para validar, controlar la calidad y garantizar la seguridad que aseguren que los sistemas de inteligencia artificial empleados en radiología y otras áreas del diagnóstico médico sean fiables (Organización Mundial de la Salud, 2021).

No solamente la exactitud de los diagnósticos se ve amenazada por estas debilidades, sino que también pueden poner en peligro la seguridad del paciente, generar tratamientos inapropiados y hacer que se reduzca la confianza en la tecnología médica. Asimismo, la carencia de protocolos apropiados para gestionar tecnología, controlar calidad

y asegurar la información aumenta el riesgo de que los sistemas fallen, lo que perjudica no solo la integridad de los datos médicos sino también el funcionamiento de los servicios sanitarios.

Para entender la manera en que se interconectan los problemas técnicos, normativos y organizacionales, es fundamental analizar estas vulnerabilidades. Esto queda reflejado en el árbol de problemas, donde se reconocen las causas directas e indirectas y los efectos que influyen sobre la seguridad y calidad de la atención médica.

Justificación

Para hacer más seguros, confiables y eficaces los sistemas de radiología digital, es fundamental analizar las debilidades de los sistemas de inteligencia artificial ante ataques adversariales. Este saber posibilita la creación de estrategias de control de calidad más estrictas, la implementación de medidas de ciberseguridad sólidas y la optimización del manejo tecnológico, lo cual disminuye los peligros relacionados con errores técnicos o manipulaciones perjudiciales de imágenes radiológicas (Hardy & Harvey, 2020; Di Palma et al., 2025).

Además, tratar estas debilidades ayuda a salvaguardar la privacidad, integridad y disponibilidad de los datos médicos importantes, lo cual se ajusta a las normas éticas y reglamentarias en el tratamiento de información del paciente. Fomenta la capacitación y formación continua del personal técnico y clínico, asegurando que sean capaces de reconocer, reducir y evitar potenciales ataques, así como de entender la importancia de la supervisión humana en la utilización de la IA (Food and Drug Administration [FDA], 2023).

Desde la perspectiva de la ciencia y del ámbito académico, el estudio de las debilidades de la inteligencia artificial en radiología también favorece el surgimiento de nuevas direcciones investigativas en el área de la seguridad digital en salud y la tecnología médica. Entender cómo ocurren estos cambios en los sistemas automatizados posibilita reforzar los procedimientos de validación de algoritmos, optimizar las normas de control de calidad en radiología digital e impulsar la creación de tecnologías más seguras y transparentes que ayuden con el diagnóstico clínico (Di Palma et al., 2025).

Por último, el estudio e implementación de medidas correctivas ante estas amenazas posibilitan que se aseguren diagnósticos más exactos, se fortalezca la confianza en la

tecnología médica y se garantice que la transformación digital en el sector salud sea sostenible. De esta manera, se cierra el círculo de causas y efectos propuesto en el árbol de problemas (International Organization for Standardization [ISO], 2019).

Objetivos

Objetivo General

Analizar, con base en la evidencia científica, el impacto de los ataques adversariales y amenazas de ciberseguridad en radiología digital

Objetivos Específicos

Identificar los riesgos más relevantes de ciberseguridad vinculados con la implementación de inteligencia artificial en sistemas de diagnóstico por imagen en el ámbito de la radiología digital.

Estudiar la influencia de los ataques adversariales en el desempeño de los modelos de inteligencia artificial empleados para el estudio de imágenes médicas

Analizar las normas y directrices internacionales vinculadas con la seguridad de los equipos médicos y el manejo de los riesgos tecnológicos en sistemas digitales de salud.

Determinar, a partir de la revisión documental, la relevancia de las acciones de ciberseguridad en los programas de control de calidad en radiología digital para el aseguramiento de los procesos de diagnóstico

Marco Teórico

Transformación Digital y Nuevos Riesgos en el Ámbito de la Radiología

La transformación digital de los procesos de diagnóstico ha causado un cambio importante en la radiología en los últimos diez años. Los sistemas actuales ya no operan de forma independiente; en cambio, están conectados a plataformas digitales de almacenamiento, redes hospitalarias y sistemas de información clínica. Esta interconectividad ha hecho más accesibles las imágenes, ha reducido los tiempos de respuesta y ha simplificado la toma de decisiones en el ámbito médico (Organización Mundial de la Salud, 2020).

No obstante, esta misma transformación tecnológica ha traído consigo nuevos peligros. Los equipos médicos que están conectados, como los de tomografía, resonancia magnética y radiografía digital, requieren de software y redes que tienen la posibilidad de ser vulnerables a las amenazas cibernéticas. En este escenario, la calidad en radiología digital no se puede restringir solamente a parámetros técnicos de imagen; tiene que incluir también la seguridad de la información Como establece la FDA (2023), En la actualidad, la ciberseguridad es un elemento esencial del sistema de gestión de calidad, ya que cualquier debilidad en el software puede poner en peligro la eficiencia clínica del equipo.

La digitalización de los servicios radiológicos ha promovido en este contexto la puesta en marcha de métodos avanzados para gestionar imágenes radiologicas, como los sistemas PACS (Picture Archiving and Communication System) y RIS (Radiology Information System), que posibilitan almacenar, distribuir y consultar diagnósticos por vía electrónica. Estos sistemas optimizan los procesos clínicos en las instituciones hospitalarias y favorecen la comunicación entre los diferentes profesionales. No obstante, al estar vinculados a redes institucionales y, en ciertas ocasiones a plataformas externas, tienen el

potencial de transformarse en puntos débiles ante posibles sucesos de seguridad informática.

Según varios estudios en el ámbito de la informática médica, el hecho de que las plataformas digitales sean cada vez más utilizadas en radiología ha aumentado la necesidad de poner en marcha políticas de seguridad para asegurar la protección de los datos clínicos. Como los informes radiológicos y las imágenes diagnósticas tienen datos sensibles del paciente, cualquier acceso sin autorización o modificación de esta información podría comprometer la privacidad del paciente y la fiabilidad del procedimiento diagnóstico. En esta perspectiva, la seguridad de la información se ha vuelto una parte fundamental de los programas que gestionan la calidad en los servicios de radiología.

Además, la difusión de tecnologías como la telemedicina y la teleradiología ha incrementado el intercambio de información médica entre profesionales e instituciones localizadas en distintas regiones. Si bien estas herramientas facilitan el acceso a servicios especializados, también conllevan nuevos desafíos en cuanto a la autenticación de usuarios; Por esta razón, enfatiza el American College of Radiology (ACR, 2022) la necesidad de fortalecer los protocolos de ciberseguridad y el control de acceso para disminuir los peligros relacionados con la transmisión de información fuera de las redes locales seguras.

Ciberseguridad en Dispositivos Médicos

La regulación de equipos médicos se concentró en aspectos funcionales y físicos durante un largo periodo, tales como la seguridad eléctrica junto con el rendimiento técnico. Sin embargo, el incremento de incidentes relacionados con la ciberseguridad en el ámbito sanitario forzó a las entidades reguladoras a reconsiderar sus directrices. (Food and Drug Administration, 2023).

La FDA ha sido uno de los actores con mayor impacto en esta transformación. Desde 2014, esta institución empezó a publicar guías concretas para administrar los riesgos cibernéticos en dispositivos médicos. Lo que se propuso en un principio como una recomendación, con el tiempo se ha transformado en un requisito más estructurado dentro del procedimiento de aprobación y seguimiento después de la comercialización. (Food and Drug Administration, 2023).

La evolución de las normas ha mostrado un cambio en la perspectiva: ya no es suficiente con que el dispositivo opere adecuadamente bajo condiciones ideales, sino que también debe mostrar capacidad de resistencia ante amenazas externas y tener mecanismos para actualizarse y realizar un seguimiento constante.

Dentro de las infraestructuras tecnológicas complejas del sector hospitalario actual, los dispositivos médicos son componentes que incluyen hardware, software y conectividad en red. Esta integración optimiza el rendimiento de los equipos y la eficacia de los procesos clínicos, aunque también conlleva riesgos relacionados con las vulnerabilidades tecnológicas. Por ejemplo, algunos dispositivos pueden tener vulnerabilidades en sus sistemas operativos, configuraciones de red o procedimientos de autenticación. Esto podría posibilitar el acceso no autorizado o la alteración de información clínica.

Dentro de este contexto, la ciberseguridad de los dispositivos médicos se ha vuelto un asunto crucial para las entidades reguladoras, los productores y las instituciones sanitarias. Las tácticas actuales no solamente tienen como objetivo salvaguardar los equipos contra asaltos externos, sino también asegurar la fiabilidad de la información clínica que estos producen y la continuidad en el funcionamiento de los sistemas médicos. La atención al paciente y la seguridad de los procedimientos terapéuticos o diagnósticos podrían verse

comprometidas si un incidente cibernético interrumpe el funcionamiento de un equipo médico.

Por esta razón, las guías regulatorias más actuales subrayan la importancia de establecer un enfoque integral para gestionar los riesgos. Este debe incluir acciones como poner al día el software periódicamente, examinar continuamente las vulnerabilidades, regular el acceso a los sistemas y aplicar mecanismos para supervisar la seguridad. Estas prácticas posibilitan la detección temprana de potenciales amenazas y la implementación de estrategias de mitigación para disminuir el impacto que los incidentes informáticos tienen en los ámbitos clínicos. (Food and Drug Administration, 2023).

Integración de Estándares Técnicos Internacionales

Además de la FDA entidades como la Comisión Internacional Electrotécnica (IEC) y la Organización Internacional de Normalización (ISO) han reforzado sus estándares para incluir el aspecto de ciberseguridad en el ciclo de vida del software médico y en la administración de riesgos. (International Organization for Standardization, 2019)

La actualización de normas, por ejemplo la ISO 14971, ha hecho posible que el análisis de riesgos tecnológicos se incorpore en la valoración general del dispositivo. Asimismo, los estándares vinculados al desarrollo de software médico han empezado a incorporar exigencias más rigurosas en cuanto a mantenimiento, actualizaciones de seguridad y gestión de vulnerabilidades. (International Organization for Standardization, 2019)

Este procedimiento muestra una inclinación global hacia la armonización de normas, en la que se considera la seguridad digital como un elemento básico de calidad y no como un añadido opcional. (International Organization for Standardization, 2019)

El establecimiento de marcos de referencia comunes que se han desarrollado gracias a la adopción de normas internacionales ha hecho más fácil que los fabricantes de dispositivos médicos y las entidades sanitarias se guíen por ellos para poner en marcha buenas prácticas en cuanto a seguridad tecnológica. Estos estándares no solo establecen requisitos técnicos, sino que además fomentan procedimientos sistemáticos para identificar, evaluar y controlar los riesgos vinculados con el uso de tecnologías médicas.

En este sentido, la estandarización a nivel internacional ha posibilitado que se mejore la fiabilidad de las infraestructuras digitales empleadas en el sector sanitario y que se potencie la interoperabilidad entre sistemas. En la radiología moderna, la interoperabilidad es un elemento esencial porque posibilita que los sistemas de almacenamiento de imágenes, los equipos de diagnóstico y los registros clínicos electrónicos compartan información de forma eficaz y segura. No obstante, para que esta interoperabilidad sea segura, los sistemas deben respetar criterios estrictos de gestión de vulnerabilidades y protección de datos. (International Organization for Standardization, 2019)

Asimismo, el progreso de normas universales ha beneficiado la colaboración entre entidades reguladoras, fabricantes de tecnología médica y centros dedicados a la investigación. Esta colaboración ha sido crucial para abordar los nuevos retos que la digitalización del sector salud presenta, sobre todo en lo que respecta a salvaguardar los sistemas clínicos de amenazas emergentes. Así, los estándares internacionales continúan adaptándose a las transformaciones tecnológicas y a las nuevas exigencias del entorno sanitario. (International Organization for Standardization, 2019)

Ciberseguridad y Control de Calidad en Radiología Digital

En el ámbito del control de calidad en la radiología digital, la ciberseguridad tiene una importancia estratégica. Los programas de calidad, en términos tradicionales, se centraban en corroborar parámetros tales como calibración, uniformidad, resolución espacial y dosis. Para incluir elementos asociados con los siguientes aspectos, estos controles deben expandirse teniendo en cuenta los siguientes ítems:

Integridad de las imágenes almacenadas

Rastreo de accesos y cambios

Seguridad de redes internas

Actualización de software de manera periódica

La integridad de las imágenes almacenadas significa que se debe asegurar que los archivos diagnósticos no sean alterados, arruinados o modificados en el proceso de transmisión o almacenamiento dentro de los sistemas digitales de radiología. El seguimiento de accesos y modificaciones posibilita el registro de qué usuarios realizan consultas o modificaciones en la información clínica, lo cual ayuda a identificar accesos no autorizados y mejora la trazabilidad de los datos. Además, la seguridad de las redes internas busca proteger la infraestructura tecnológica de la institución médica a través de controles de acceso, segmentación de redes y sistemas de autenticación que eviten el ingreso no autorizado. Por último, es esencial actualizar el software con regularidad, para mantener la estabilidad operacional de los sistemas médicos digitales, mejorar la protección ante nuevas amenazas y corregir las vulnerabilidades existentes.

La calidad diagnóstica no solo se basa en la precisión técnica del equipo, sino también en la confiabilidad del ambiente digital donde opera. En esta línea, la evolución de los estándares globales ha ayudado a redefinir el concepto de calidad en radiología,

incorporando la gestión del riesgo cibernético como una fase del proceso incesante de perfeccionamiento.

Incluir la ciberseguridad en los programas de control de calidad radiológica es una mejora del concepto clásico de calidad en los servicios de diagnóstico por imágenes. En el pasado, la evaluación de calidad se enfocaba sobre todo en el rendimiento técnico de los equipos; sin embargo, hoy en día también se tiene en cuenta la necesidad de asegurar que los sistemas informáticos encargados de administrar información radiológica sean seguros y confiables. Como afirma la Food and Drug Administration (FDA, 2023) en sus lineamientos de control de calidad**:** "La ciberseguridad es una parte integral de la seguridad de los dispositivos médicos y de los sistemas de gestión de calidad; una falla en la seguridad cibernética puede comprometer directamente la eficacia clínica y la seguridad del paciente".

Las entidades sanitarias han empezado a aplicar tácticas de administración de seguridad informática, que comprenden la evaluación de vulnerabilidades, auditorías periódicas de los sistemas, supervisión del estado de los datos guardados y control del acceso a los equipos médicos. Estas acciones posibilitan la disminución del peligro de modificaciones en los diagnósticos por imagen o en los reportes médicos, lo que es esencial para garantizar la validez de los resultados clínicos.

Además, la implementación de protocolos de ciberseguridad en los programas de calidad ayuda a que los expertos en salud confíen más en los sistemas digitales empleados en radiología. Es factible asegurar que la información diagnóstica se conserve intacta desde su adquisición hasta su almacenamiento y análisis clínico posterior, siempre y cuando los sistemas dispongan de mecanismos de protección apropiados.

Tendencias Actuales y Desafíos

En años recientes, se ha visto una transición hacia modelos de "seguridad desde el diseño", en los que los fabricantes tienen que verificar que la protección cibernética está integrada desde la etapa de creación del producto. Además, se requiere que haya más transparencia al comunicar las actualizaciones del software y las vulnerabilidades.

Sin embargo, existen retos significativos que persisten, sobre todo en instituciones que cuentan con infraestructura tecnológica escasa o con equipos viejos que no se desarrollaron de acuerdo con estos nuevos estándares. Esto sugiere que se deben reforzar los programas de capacitación y las políticas internas de seguridad en el sector salud.

Otra tendencia significativa en el área de la ciberseguridad aplicada a dispositivos médicos es la creación de tácticas para gestionar riesgos de manera proactiva. El American College of Radiology (ACR, 2022) destaca en sus estándares que “la protección de los datos de imagenología médica debe evolucionar de una defensa perimetral simple a una estrategia de resiliencia proactiva, dado que la interconectividad de los sistemas aumenta la superficie de ataque para actores malintencionados”. Este método tiene como objetivo prever potenciales vulnerabilidades antes de que se transformen en incidentes de seguridad, a través de la aplicación de medidas preventivas y la ejecución recurrente de evaluaciones en los sistemas. En este contexto, los modelos de gestión que se fundamentan en la evaluación permanente de riesgos tecnológicos están siendo implementados cada vez más por las organizaciones de salud.

El aumento de lo que se conoce como Internet de las Cosas Médicas (IoMT) también ha incrementado la cantidad de dispositivos conectados en los ambientes hospitalarios. Sistemas de información, equipos para diagnósticos, sensores clínicos y monitores de pacientes son componentes de redes complejas que necesitan estrategias de

seguridad cada vez más avanzadas. Este panorama presenta nuevos desafíos para los expertos responsables de la gestión tecnológica en las entidades de salud.

Finalmente, uno de los retos más importantes es la conciliación entre la seguridad informática y la innovación tecnológica. A medida que se van añadiendo nuevas funciones digitales a los dispositivos médicos, también surge la necesidad de establecer marcos regulatorios que aseguren su uso seguro. En este contexto, se vuelve esencial la actualización continua de las normas internacionales y la formación del personal sanitario para reforzar la resiliencia de los sistemas sanitarios ante las amenazas cibernéticas.

Metodología

Enfoque de la Investigación

Este estudio se realiza con una perspectiva analítica y descriptiva de tipo cualitativo, enfocada en entender las debilidades vinculadas al empleo de inteligencia artificial dentro de los sistemas de radiología digital y su conexión con los peligros cibernéticos en el sector salud. Este enfoque posibilita el análisis de datos procedentes de varias fuentes institucionales, académicas y científicas con la finalidad de interpretar las tendencias contemporáneas vinculadas a la seguridad de los dispositivos médicos y la conservación de los sistemas digitales empleados en el diagnóstico por imágenes.

Tipo de Investigación

La indagación es de carácter descriptivo y documental. Es documental porque se basa en la evaluación y el estudio de literatura científica, artículos académicos, informes de instituciones y regulaciones internacionales vinculadas con la ciberseguridad en dispositivos médicos, la inteligencia artificial para diagnóstico por imágenes y los criterios de calidad en radiología digital. Además, tiene un enfoque descriptivo porque intenta caracterizar los principales peligros tecnológicos relacionados con el empleo de estas herramientas y aclarar la manera en que pueden afectar la confiabilidad de los diagnósticos médicos y la seguridad de los sistemas clínicos.

Técnicas de recolección de información

Se utilizó el método de revisión bibliográfica para recopilar la información, que consistió en revisar y analizar distintas fuentes documentales vinculadas al tema de investigación. Se incluyen entre las fuentes empleadas documentos técnicos elaborados por

entidades internacionales, artículos científicos presentados en revistas específicas, guías regulatorias y análisis académicos que abordan la inteligencia artificial, la ciberseguridad en el área de salud y el control de calidad en radiología digital.

Estas fuentes han posibilitado el reconocimiento de los riesgos tecnológicos y las estrategias de seguridad sugeridas para mejorar la protección de los sistemas médicos digitales, así como la determinación de los conceptos teóricos más relevantes.

Los criterios de selección de la información fueron los siguientes:

Idiomas: artículos publicados en español e inglés.

Rango de Tiempo: publicaciones de los últimos 5 a 10 años, con el fin de garantizar actualidad en la información.

Criterios de Inclusión

Estudios relacionados con inteligencia artificial en radiología.

Investigaciones sobre ciberseguridad en el sector salud.

Documentos sobre control de calidad en radiología digital.

Publicaciones en revistas indexadas y fuentes oficiales.

Criterios de Exclusión

Artículos no relacionados directamente con el tema.

Publicaciones sin respaldo científico o no indexadas.

Documentos con información desactualizada o incompleta.

Estas fuentes permitieron identificar los principales riesgos tecnológicos y las estrategias de seguridad recomendadas para fortalecer la protección de los sistemas médicos digitales, así como establecer los conceptos teóricos más relevantes.

Análisis de la Información

La información se analizó a través del examen crítico y comparativo de las fuentes documentales que se consultaron. Se identificaron, a partir de este procedimiento, los aspectos comunes que aparecen en la literatura científica respecto a las vulnerabilidades de los sistemas de inteligencia artificial en el diagnóstico por imágenes. También se determinaron las sugerencias internacionales para optimizar la seguridad de los dispositivos médicos conectados a redes digitales y la gestión de riesgos.

También se examinaron las directrices regulatorias y los estándares internacionales que definen pautas para salvaguardar los sistemas tecnológicos en el sector sanitario, lo que posibilitó entender por qué es importante introducir la ciberseguridad en los programas de control de calidad de la radiología digital. Técnicas de recolección de información

Se utilizó el método de revisión bibliográfica para recopilar la información, que consistió en revisar y analizar distintas fuentes documentales vinculadas al tema de investigación. Se incluyen entre las fuentes empleadas documentos técnicos elaborados por entidades internacionales, artículos científicos presentados en revistas específicas, guías regulatorias y análisis académicos que abordan la inteligencia artificial, la ciberseguridad en el área de salud y el control de calidad en radiología digital. Las bases de datos que se revisaron fueron SciELO, OMS y ScienceDirect

Estas fuentes han permitido identificar los peligros tecnológicos y las estrategias de seguridad recomendadas para optimizar la protección de los sistemas médicos digitales, además de establecer los conceptos teóricos más significativos.

Desarrollo del Proyecto

Identificación de Riesgos y Ataques Adversariales

La revisión de la literatura evidencia que uno de los principales riesgos asociados al uso de inteligencia artificial en radiología digital son los ataques adversariales, los cuales consisten en modificaciones mínimas en las imágenes médicas que pueden alterar los resultados diagnósticos sin ser detectadas por el ojo humano.

Según Di Palma et al. (2025), estos ataques representan una amenaza significativa, ya que pueden inducir errores en los modelos de inteligencia artificial, generando falsos positivos o falsos negativos en la detección de enfermedades. En concordancia, Hardy y Harvey (2020) reconocen que, aunque la IA mejora la precisión diagnóstica, también introduce nuevas vulnerabilidades tecnológicas que pueden comprometer la seguridad del paciente.

En este sentido, se evidencia una tensión entre beneficios y riesgos: mientras algunos autores destacan el potencial de la IA, otros advierten sobre su fragilidad frente a manipulaciones externas. Esto demuestra que la implementación de estas tecnologías debe ir acompañada de estrategias de seguridad robustas.

Adicionalmente, se identificaron vulnerabilidades en sistemas como PACS y RIS, los cuales, al estar conectados a redes hospitalarias, pueden ser objeto de accesos no autorizados. Según Valencia (2026), la falta de controles de acceso y protocolos de seguridad incrementa el riesgo de alteración de imágenes y filtración de datos clínicos.

Además de destacar las vulnerabilidades, algunos autores proponen estrategias potenciales para resolver estos riesgos. Por ejemplo, Di Palma et al. (2025) proponen la implementación de tecnologías emergentes, como el blockchain, para mejorar la seguridad de los datos médicos y optimizar la trazabilidad de la información. Según Hardy y Harvey

(2020), es importante fortalecer los procesos de validación de modelos de inteligencia artificial para disminuir su vulnerabilidad a manipulaciones externas.

La FDA (2023) sugiere la incorporación de la ciberseguridad desde la etapa de diseño del equipo, por otro lado, mientras que la norma ISO 14971 (2019) hace énfasis en que es imprescindible una administración constante de riesgos durante todo el ciclo vital del sistema. Estas propuestas no se contradicen entre sí, sino que se complementan, porque enfrentan el problema desde perspectivas regulatorias, de gestión y tecnológicas; esto posibilita dar una respuesta más integral ante las amenazas detectadas.

Análisis de Normativas Internacionales

Los organismos internacionales coinciden en la necesidad de fortalecer la ciberseguridad en dispositivos médicos. La Food and Drug Administration (FDA, 2023) establece que la seguridad debe integrarse desde el diseño del dispositivo, bajo el enfoque de *"*security by design", lo que implica anticipar riesgos desde el desarrollo tecnológico.

Por su parte, la norma ISO 14971 (2019) plantea que los riesgos tecnológicos, incluyendo los cibernéticos, deben ser parte del proceso integral de gestión de riesgos en dispositivos médicos.

Ambas posturas coinciden en considerar la ciberseguridad como un elemento esencial de la calidad. Sin embargo, mientras la FDA se enfoca en la regulación y el ciclo de vida del producto, la ISO proporciona un marco metodológico para la gestión del riesgo.

Esta complementariedad demuestra que no existe contradicción entre autores, sino un enfoque integral desde distintas perspectivas

Ciberseguridad en el Control de Calidad en Radiología Digital

El análisis documental muestra que el concepto tradicional de control de calidad en radiología ha evolucionado. Antes se centraba en aspectos técnicos, como la resolución de

imagen o la dosis de radiación; sin embargo, actualmente incluye componentes de ciberseguridad.

La FDA (2023) sostiene que una falla en la seguridad digital puede afectar directamente la eficacia clínica, lo que respalda la necesidad de integrar la ciberseguridad en los programas de calidad.

En este contexto, los autores coinciden en que los nuevos programas de calidad deben incluir:

Integridad de las imágenes

Control de accesos

Seguridad de redes

Actualización de software

No se identifican discrepancias entre autores en este punto; por el contrario, existe un consenso general sobre la necesidad de ampliar el concepto de calidad hacia la seguridad digital.

Tabla 1

Cuadro Comparativo: Perspectivas Internacionales sobre Ciberseguridad e Inteligencia Artificial en Radiología Digital

País	Enfoque principal	Normativas o estrategias	Relación con la investigación	Referencia
Colombia	Fortalecimiento de la seguridad digital en los sistemas RIS/PACS y seguridad de la	Aplicación de políticas informáticas de seguridad en entidades de salud	Pretende optimizar la seguridad del paciente y la protección de las imágenes médicas frente a riesgos	Valencia (2026)

	información médica.		cibernéticos.	
Estados Unidos	Incorporación de la ciberseguridad desde el diseño de equipos médicos	Guías de la FDA acerca de "seguridad por diseño"	Fomenta la gestión de riesgos y la renovación continua del software médico.	FDA (2023)
España	Control de acceso a datos clínicos y protección de las instalaciones hospitalarias	Estrategias de ciberseguridad en la salud digital y seguridad de datos	Fortalece la confidencialidad y el seguimiento de la información radiológica.	Cervera García & Goussens (2024)
Unión Europea	Regulación detallada acerca de la protección de datos e inteligencia artificial	Normativa general sobre protección de datos (GDPR) y normas tecnológicas	Busca asegurar que las tecnologías digitales en el área de la salud se usen de manera ética y segura.	WHO/Europe (2025)

Nota. Elaboración propia con base en Valencia (2026), Food and Drug Administration (2023), Cervera García y Goussens (2024) y WHO/Europe (2025). La tabla resume las principales perspectivas internacionales sobre ciberseguridad e inteligencia artificial en radiología digital.

Tabla 2

Comparación del Control de Calidad en Radiología Digital: Enfoque Convencional y Enfoque con Ciberseguridad

Elemento de calidad	Control de calidad convencional	Control de calidad con ciberseguridad	Fuente	Descripción
Ajuste de equipos	Calibración y funcionamiento correcto del equipo	Incluye verificación del software y su seguridad	FDA (2023)	No solo se revisa el hardware, también que el sistema no tenga vulnerabilidades digitales
Integridad de las imágenes	No considerado directamente	Garantiza que las imágenes no sean alteradas o manipuladas	FDA (2023)	Evita modificaciones intencionales o accidentales en las imágenes diagnósticas
Resolución espacial	Evaluación de la calidad visual de la imagen	Se mantiene, pero se complementa con protección digital	Hardy & Harvey (2020)	La calidad ya no es solo visual, también depende de la seguridad del sistema
Monitoreo de accesos	No incluido	Registro y control de quién accede o modifica datos	Valencia (2026)	Permite detectar accesos no autorizados y mejorar la trazabilidad
Control de la dosis	Medición y optimización de radiación	Se mantiene como criterio técnico	ISO 14971 (2019)	Sigue siendo fundamental, pero ahora se integra a un enfoque más amplio
Seguridad de redes	No considerado	Protección de sistemas	ISO 14971 (2019)	Reduce riesgos de ataques informáticos

		conectados (PACS, RIS)		en redes hospitalarias
Operación técnica	Uso correcto del equipo	Uso seguro del sistema + protocolos digitales	Di Palma et al. (2025) – Blockchain & Healthcare	Se incluye la seguridad en la operación, no solo la técnica
Actualización de software	No incluida	Actualizaciones periódicas para prevenir vulnerabilidades	FDA (2023)	Mantiene los sistemas protegidos frente a nuevas amenazas
Evaluación de equipos	Revisión física y funcional	Evaluación integral (física + digital)	FDA (2023)	Se amplía el concepto de control de calidad
Protección de la información	No considerada	Seguridad de datos clínicos y privacidad del paciente	Di Palma et al. (2025)	Garantiza confidencialidad, integridad y disponibilidad de la información

Nota. Elaboración Propia con Base en Food and Drug Administration (2023), International Organization for Standardization (2019), Di Palma et al. (2025) y otros.

La comparación realizada pone en evidencia la evolución del control de calidad en radiología, pasando de un enfoque tradicional, limitado a la evaluación técnica de los equipos, a un modelo integral que incorpora la ciberseguridad y la protección de la información clínica como componentes esenciales. Este cambio responde a las nuevas dinámicas de la digitalización en salud y resulta clave para garantizar la confiabilidad de los diagnósticos y la seguridad del paciente.

Conclusiones

El análisis realizado evidencia que, aunque la inteligencia artificial ha mejorado significativamente la precisión y eficiencia del diagnóstico en radiología digital, también introduce nuevas vulnerabilidades relacionadas con la ciberseguridad.

Se identificó que los ataques adversariales representan un riesgo crítico, ya que pueden alterar los resultados diagnósticos sin ser detectados, afectando la seguridad del paciente y la confiabilidad de los sistemas.

Asimismo, se concluye que los organismos internacionales como la FDA y la ISO coinciden en la necesidad de integrar la ciberseguridad como un componente esencial en el diseño, desarrollo y gestión de dispositivos médicos, lo que fortalece los sistemas de salud frente a amenazas digitales.

En relación con el control de calidad, se evidencia una evolución del enfoque tradicional hacia un modelo integral que incluye la protección de datos, la seguridad de redes y la supervisión de accesos, lo cual garantiza la integridad de la información clínica.

Finalmente, se concluye que la implementación de estrategias de ciberseguridad, junto con la capacitación del personal sanitario y el cumplimiento de normativas internacionales, es fundamental para asegurar un uso seguro, confiable y sostenible de la inteligencia artificial en radiología digital.

Se espera que en el futuro se van a seguir fortaleciendo los procesos de actualización tecnológica y las tácticas de ciberseguridad en radiología digital, para crear sistemas de inteligencia artificial más seguros, fiables y resistentes ante riesgos cibernéticos. Además, será esencial fomentar la formación constante del personal de salud y el cumplimiento de normas internacionales que aseguren la seguridad y calidad de los diagnósticos médicos.

Referencias Bibliográficas

Arias-García, M., Soni-García, A., Santos-García, A., & Moreno-Ibarra, M. (2023). Deep learning for medical image cryptography: A comprehensive review. *Applied Sciences*, *13*(14), 8295. https://doi.org/10.3390/app13148295

Bernal Ontiveros, J. M., Palacios Reyes, M., Zorrilla Briones, F., Rosales Morales, N. R., & Cervantes Cárdenas, S. A. (2025). Ciberseguridad: Métodos de defensa ante ataques de infiltraciones. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *16*(31). https://doi.org/10.23913/ride.v16i31.2516

Cervera García, A., & Goussens, A. (2024). Cybersecurity and use of ICT in the health sector. *Atención Primaria*, *56*(3), 102854. https://doi.org/10.1016/j.aprim.2023.102854

Di Palma, G., Scendoni, R., Ferorelli, D., De Benedictis, A., Tambone, V., & De Micco, F. (2025). AI-induced cybersecurity risks in healthcare: A narrative review of blockchain-based solutions within a clinical risk management framework. *Risk Management and Healthcare Policy*, *18*, 3479–3497. https://doi.org/10.2147/RMHP.S544523

Food and Drug Administration. (2023). *Cybersecurity in medical devices*. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Hardy, M., & Harvey, H. (2020). Artificial intelligence in diagnostic imaging: Impact on the radiography profession. *The British Journal of Radiology*, *93*(1108), 20190840. https://doi.org/10.1259/bjr.20190840

International Organization for Standardization. (2019). *ISO 14971: Medical devices — Application of risk management to medical devices*. https://www.iso.org/standard/72704.html

Kriptos. (s. f.). *Informe de ciberseguridad en el sector de la salud*. https://www.kriptos.io/es/es-post/ciberseguridad-sector-salud

Namsa. (s. f.). *Ciberseguridad de dispositivos médicos previa y posterior a la comercialización de la FDA*. https://namsa.com/es/resources/blog/fda-premarket-and-postmarket-medical-device-cybersecurity/

Ojeda, S. (2025, agosto 5). *FDA updates cybersecurity guidance for medical devices: 2025 premarket recommendations*. AssurX. https://www.assurx.com

Sedgwick. (s. f.). *La FDA sigue centrándose en la ciberseguridad de los dispositivos médicos*. https://www.sedgwick.com/es/blog/fda-continues-its-focus-on-cybersecurity-in-medical-devices/

U.S. Food and Drug Administration. (2024, agosto 9). *Seguridad cibernética de dispositivos médicos: Lo que necesita saber*. https://www.fda.gov/consumers/articulos-para-el-consumidor-en-espanol/seguridad-cibernetica-de-dispositivos-medicos-lo-que-necesita-saber

Valencia, R. (2026, febrero 12). *Ciberseguridad en RIS/PACS: Cómo proteger imágenes médicas y datos de pacientes en Colombia*. NOVA Imaging. https://novaimaging.co/ciberseguridad-ris-pacs-proteccion-datos-radiologia-colombia/

World Health Organization. (2025, marzo 26). *WHO/Europe launches guide to strengthen cybersecurity in digital health*. https://www.who.int/europe/news/item/26-03-2025-who-europe-launches-guide-to-strengthen-cybersecurity-in-digital-health