

**Revisión Documental de los Protocolos de Cifrado y Mecanismos de Ciberseguridad
Aplicados al Envío de Datos Dosimétricos en Entornos Hospitalarios IoT**

Andrea Valentina Chacón Rivera

Cristhian Fabián Rey Arciniegas

Liseth Tatiana Monroy Pérez

Sergio Andrés Torres Tolosa

Sergio Iván Díaz Calderón

Asesor

Mario Efrén Mejía Ospina

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias de la Salud ECISA

Tecnología en Radiología e Imágenes Diagnósticas

2026

Dedicatoria

Dedicamos este trabajo, con profunda gratitud, a Dios, por guiarnos, fortalecernos y permitirnos culminar este camino académico con sabiduría, paciencia y determinación.

A nuestras familias y, en especial, a nuestros padres, quienes, con su amor incondicional, sus consejos y su apoyo constante han sido el pilar fundamental que nos motivó a avanzar incluso en los momentos más desafiantes.

Dedicamos este esfuerzo a nosotros mismos: Andrea Valentina Chacón Rivera, Cristhian Fabián Rey Arciniegas, Liseth Tatiana Monroy Pérez, Sergio Andrés Torres Tolosa y Sergio Iván Díaz Calderón, por la perseverancia, disciplina y compromiso que nos permitieron crecer como profesionales y como seres humanos.

Agradecimientos

Agradecemos, en primer lugar, a Dios, por permitirnos llegar hasta este punto con salud, claridad y fortaleza.

Nuestro agradecimiento especial a la UNAD, por brindarnos los espacios académicos, las herramientas tecnológicas y el acompañamiento necesario para nuestro desarrollo profesional.

Reconocemos y valoramos el trabajo de los tutores, quienes con dedicación, orientación y acompañamiento académico contribuyeron significativamente a nuestro proceso formativo, impulsándonos a alcanzar un nivel superior de compromiso y excelencia.

A nuestras familias y a nuestros padres, que, con su comprensión y motivación constante hicieron posible que cada uno de nosotros pudiera cumplir este objetivo.

Resumen

La presente investigación analiza los protocolos de cifrado y las estrategias de ciberseguridad más efectivos para la transmisión de datos dosimétricos en redes hospitalarias que usan Internet de las Cosas (IoT) en radiología. A través de una metodología descriptiva y documental basada en revisión literaria, reportes técnicos y estándares internacionales, se estudian los mecanismos de seguridad aplicados a la comunicación entre dispositivos IoT, sistemas RIS, PACS y plataformas interoperables. El análisis se centra en la integridad, confidencialidad, disponibilidad y autenticidad de los datos clínicos, la identificación de vulnerabilidades de accesos no autorizados, fallas de interoperabilidad, ataques de red y manipulación de información dosimétrica. Los resultados indican que los protocolos de cifrado más robustos son aquellos que integran cifrado extremo a extremo, AES, TLS, criptografía liviana, modelos Zero Trust y mecanismos de autenticación federada, especialmente en entornos IoT con limitaciones de hardware o con comunicaciones de alta frecuencia. Asimismo, la literatura destaca que la eficacia de estos protocolos depende de su correcta implementación, de la arquitectura de red y del grado de interoperabilidad con estándares como HL7, FHIR y DICOM. También se evidencia que la falta de estandarización y la fragmentación de sistemas hospitalarios comprometen la integridad de los registros de dosis y afectan la seguridad del paciente. Se concluye que fortalecer la infraestructura tecnológica, estandarizar protocolos y adoptar modelos criptográficos avanzados es esencial para garantizar una transmisión segura y continua de los datos dosimétricos para reducir vulnerabilidades y optimizar la protección radiológica del paciente.

Palabras Clave: IoT, dosimetría, cifrado, ciberseguridad, sistemas RIS y PACS.

Abstract

This research analyzes the most effective encryption protocols and cybersecurity strategies for the transmission of dosimetric data in hospital networks that use the Internet of Things (IoT) in radiology. Through a descriptive and documentary methodology based on literature review, technical reports, and international standards, the study examines security mechanisms applied to communication between IoT devices, RIS, PACS, and interoperable clinical platforms. The analysis focuses on the integrity, confidentiality, availability, and authenticity of clinical data, as well as the identification of vulnerabilities related to unauthorized access, interoperability failures, network attacks, and manipulation of dosimetric information. The results indicate that the most robust encryption protocols are those that incorporate end-to-end encryption, AES, TLS, lightweight cryptography, Zero Trust models, and federated authentication mechanisms, particularly in IoT environments with hardware limitations or high-frequency communication requirements. The literature further highlights that the effectiveness of these protocols depends on proper implementation, network architecture, and the degree of interoperability with standards such as HL7, FHIR, and DICOM. The findings also show that the lack of standardization and the fragmentation of hospital systems compromise the integrity of dose records and negatively impact patient safety. It is concluded that strengthening technological infrastructure, standardizing protocols, and adopting advanced cryptographic models are essential to ensure secure and continuous transmission of dosimetric data, reduce vulnerabilities, and optimize radiological protection for patients.

Keywords: IoT, dosimetry, encryption, cybersecurity, systems RIS and PACS.

Tabla de Contenido

| | |
|--|----|
| Introducción | 10 |
| Planteamiento del Problema | 12 |
| Justificación | 16 |
| Objetivos..... | 19 |
| Objetivo General..... | 19 |
| Objetivos Específicos | 19 |
| Marco Teórico..... | 20 |
| Internet de las Cosas en el Entorno Hospitalario..... | 20 |
| Arquitectura de un Sistema IoT Médico..... | 21 |
| Internet de las Cosas (IoT) y Seguridad del Paciente en Radiología..... | 22 |
| Interoperabilidad HL7/FHIR y Registro Unificado de Dosis Acumulada | 23 |
| Protocolos de Cifrado y Ciberseguridad para la Protección de Datos Dosimétricos en Redes Hospitalarias..... | 25 |
| Fundamentos de Protección Radiológica y Monitoreo de Dosis..... | 26 |
| IoT, Registro de Dosis Acumulada y Monitorización en Tiempo Real..... | 28 |
| IA en el Análisis de Dosis Radiológica | 30 |
| Big Data y Análisis Predictivo en Radiología | 31 |
| Uso de Apis Restful para la Consulta de Datos en la Nube..... | 31 |
| Interoperabilidad en Salud para el Monitoreo de Dosis Radiológica | 32 |
| Desafíos en la Estandarización y Seguimiento de Dosis Radiológica..... | 32 |
| Ciberseguridad y Privacidad de Datos en IoT Médico | 33 |
| Normativa Internacional y Nacional..... | 35 |
| Metodología | 36 |

| | |
|---|----|
| Diseño de Investigación..... | 36 |
| Criterios de Inclusión..... | 36 |
| Criterios de Exclusión..... | 37 |
| Fases del Desarrollo Metodológico | 37 |
| Fase 1. Formulación del Problema y Delimitación Conceptual..... | 37 |
| Fase 2. Búsqueda y Revisión Documental..... | 37 |
| Fase 3. Organización, Construcción y Análisis Comparativo..... | 37 |
| Fase 4. Síntesis, Resultados, Conclusiones y Recomendaciones..... | 38 |
| Análisis de Resultados | 39 |
| Análisis Comparativo Internacional | 56 |
| Conclusiones | 61 |
| Recomendaciones | 63 |
| Referencias Bibliográficas | 65 |

Lista de Tablas

| | |
|---|----|
| Tabla 1 <i>Análisis Comparativo de Protocolos de Ciberseguridad</i> | 43 |
| Tabla 2 <i>Tecnologías IoT, Ciberseguridad y Aplicación en Dosimetría</i> | 45 |
| Tabla 3 <i>Comparación de Interoperabilidad para Dosimetrías</i> | 46 |
| Tabla 4 <i>Comparación de Protocolos</i> | 49 |
| Tabla 5 <i>Estrategias para Mejorar la Confiabilidad Operativa en Sistemas IoT</i> | 51 |
| Tabla 6 <i>Análisis Comparativo Internacional</i> | 52 |

Lista de Figuras

| | |
|---|----|
| Figura 1 <i>Árbol del Problema</i> | 13 |
|---|----|

Introducción

La innovación digital en el sector de la salud ha impulsado la adopción de tecnologías basadas en el Internet de las Cosas (IoT), que permiten el monitoreo continuo, la automatización de procesos clínicos y la transmisión de información en tiempo real. En radiología, estas herramientas adquieren especial relevancia por su capacidad para registrar, analizar y reportar datos dosimétricos de forma continua, fortaleciendo la seguridad del paciente y la trazabilidad de la exposición a radiación ionizante (Quiroz et al., 2021). Sin embargo, su implementación también introduce desafíos importantes relacionados con la protección de datos, la ciberseguridad y la fiabilidad de la información que circula entre los dispositivos.

El control adecuado de la dosis acumulada radiológica es crucial en las buenas prácticas de protección. Pese a ello, aún existen salas donde no se han adoptado sistemas IoT capaces de medir y reportar en tiempo real la dosis administrada, lo que genera vacíos en el seguimiento y limita la capacidad del personal para responder oportunamente ante posibles sobreexposiciones. La falta de alertas automáticas y la ausencia de monitoreo continuo aumentan, por tanto, los riesgos para la seguridad del paciente.

Otro aspecto crítico es la interoperabilidad entre dispositivos IoT, sistemas de imágenes y plataformas clínicas. Su correcto funcionamiento debe asegurar un flujo de información continuo y confiable, manteniendo la autenticidad y confidencialidad de los datos sensibles. Estudios recientes indican que más del 60% de las soluciones IoT en el sector salud presentan vulnerabilidades en sus canales de comunicación, lo que incrementa la posibilidad de interceptación o manipulación de información clínica.

Asimismo, la implementación de protocolos de cifrado y mecanismos de ciberseguridad es un factor fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos. No obstante, la heterogeneidad de dispositivos, la limitación de recursos computacionales

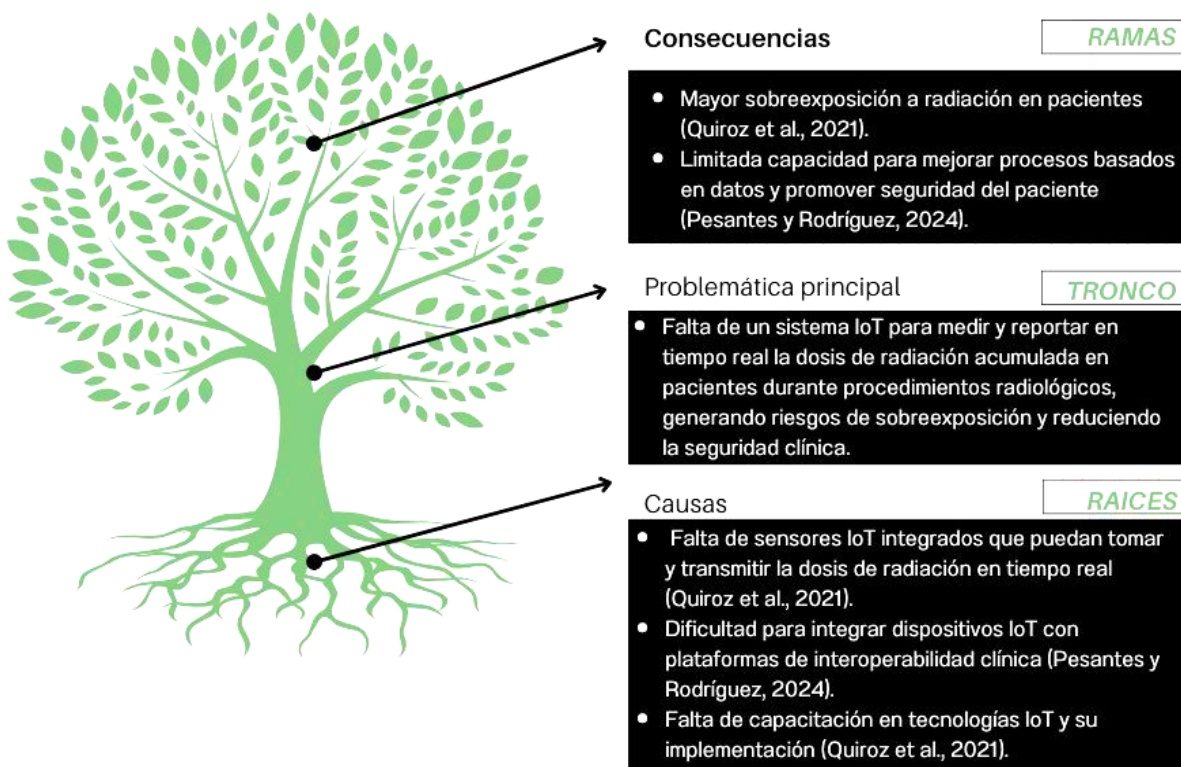
y la necesidad de interoperabilidad con estándares clínicos como DICOM, HL7 y FHIR genera complejidad en la selección de soluciones óptimas. A esto se suma la importancia de asegurar la continuidad operativa del monitoreo dosimétrico, ya que fallas de conectividad, interrupciones en la transmisión o pérdidas de paquetes comprometen la precisión del registro clínico. Por ello, parámetros como la calidad del servicio (QoS), la redundancia de la red y los mecanismos de recuperación automática resultan determinantes para mantener un flujo de datos estable y verificable (Hossain et al., 2023).

Con base en lo anterior y desde una revisión documental, se evalúan los protocolos de cifrado y los mecanismos de ciberseguridad más efectivos para la transmisión de datos dosimétricos en entornos hospitalarios basados en IoT. A través del análisis de normativas, artículos científicos, reportes técnicos y estándares internacionales, se busca identificar soluciones seguras, eficientes y compatibles con las arquitecturas hospitalarias. Paralelamente, se examinan los factores que afectan la continuidad operativa del monitoreo dosimétrico y las estrategias de mitigación orientadas a garantizar precisión, disponibilidad y consistencia en los ecosistemas IoT hospitalarios.

Planteamiento del Problema

Figura 1

Árbol Del Problema



Nota. Autoría propia

La salud se ha transformado con el uso de tecnologías del Internet de las Cosas IoT que permiten el monitoreo continuo en tiempo real, permitiendo la recolección, transmisión y análisis de datos biomédicos en tiempo real. De acuerdo con esto, los sistemas IoT ayudan optimizar procesos clínicos, fortalecer la toma de decisiones y mejorar la supervisión de parámetros relevantes para la seguridad del paciente (Quiroz et al., 2021). De esta forma, el Internet Médico de las Cosas (IoMT) ha ampliado sus capacidades mediante el análisis de grandes volúmenes de datos, favoreciendo la trazabilidad y la eficiencia asistencial (Dimitrov, 2016). En este contexto, distintas áreas clínicas han incorporado sistemas interconectados que permiten automatizar

alertas, mejorar la precisión diagnóstica y aumentar la eficiencia operativa, especialmente cuando se integran con herramientas de inteligencia artificial (Vera, 2024).

En radiología, el control de la dosis acumulada de radiación es fundamental para la seguridad del paciente, sin embargo, en muchas salas de radiología, aún no existe un sistema IoT que permita medir, registrar y reportar en tiempo real la dosis de radiación administrada durante los procedimientos diagnósticos e intervencionistas (Pesantes y Rodríguez, 2024). Esta insuficiencia podría causar sobreexposición radiológica, repetición de estudios y limitaciones en la trazabilidad de la dosis acumulada, disminuyendo la seguridad clínica y el desempeño de buenas prácticas en protección radiológica. Esta brecha tecnológica puede generar escenarios de sobreexposición, repetición innecesaria de estudios, falta de trazabilidad histórica y limitaciones en la generación de alertas clínicas oportunas. Además, la persistencia de registros fragmentados o posteriores al procedimiento reduce la capacidad preventiva y dificulta la toma de decisiones basada en datos actualizados (Paz et al., 2025).

Además, esta situación evidencia una realidad de los sistemas actuales de control radiológico, donde el registro de dosis se realiza de forma fragmentada o posterior al procedimiento, reduciendo la capacidad preventiva. Al mismo tiempo, los sistemas de monitoreo, que no están diseñados o implementados adecuadamente, pueden tener fallas operativas, problemas de integración y deficiencias en la gestión de la información, lo que afecta la confiabilidad, siendo un riesgo para la seguridad del paciente (Paz et al., 2025). La falta de alertas automatizadas y de trazabilidad inmediata dificulta la toma de decisiones clínicas basadas en datos actualizados, reduciendo el control sobre la exposición radiológica acumulativa. La falta de monitoreo continuo y la repetición innecesaria de estudios, incrementa la exposición ionizante y reduce la capacidad de prevención de riesgos asociados a la radiación ionizante. Elhonseny et al., (2018) destacan la importancia de modelos seguros de transmisión de datos en sistemas

sanitarios basados en IoT, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información clínica.

Por otra parte, aunque existen aplicaciones digitales para estimar dosis en procedimientos radiológicos, estas suelen funcionar como herramientas de cálculo posterior y no como sistemas integrados de monitoreo continuo en tiempo real (Hernández, 2023). De igual manera, estudios clínicos evidencian variaciones en las dosis administradas y factores asociados que refuerzan la necesidad de fortalecer los mecanismos de control y supervisión durante los procedimientos radiológicos (Ramírez et al., 2023).

En radiología, el monitoreo de las dosis acumuladas de radiación es esencial en la seguridad clínica, pues la sobreexposición puede generar efectos adversos y aumentar los riesgos a largo plazo de desarrollar otras enfermedades. Sin embargo, en muchas salas de radiología no existen sistemas IoT completamente integrados que permitan medir, registrar y reportar en tiempo real la dosis administrada en procedimientos. Esta restricción reduce la generación de alertas tempranas, dificulta la trazabilidad de la exposición acumulada y compromete la seguridad del paciente.

En muchos centros de salud, no existe un sistema IoT implementado que permita medir, registrar y reportar en tiempo real la dosis de radiación administrada durante cada procedimiento. Esta limitación impide generar alertas inmediatas ante posible sobreexposición, dificulta la trazabilidad histórica de la dosis acumulada y compromete la seguridad del paciente.

Por ende, la ausencia de un sistema IoT estructurado que permita medir, registrar y reportar automáticamente la dosis acumulada en tiempo real limita la prevención de la sobreexposición, dificulta la trazabilidad histórica de la exposición radiológica y reduce la capacidad de generar alertas inmediatas ante niveles potencialmente elevados.

De esta manera, se plantea la siguiente pregunta de investigación ¿Cuáles son los protocolos de cifrado y ciberseguridad más efectivos documentados para la transmisión de datos dosimétricos en redes hospitalarias?

Justificación

El uso de IoT en salud es una herramienta valiosa para fortalecer la seguridad del paciente por la monitorización continua y la automatización de alertas en tiempo real. Martínez et al., (2025) destacan que la interconexión de dispositivos médicos y plataformas digitales mejoran la gestión del riesgo clínico y optimizan los procesos asistenciales, ofreciendo una atención más segura y eficiente.

Asimismo, Dimitrov (2016) señala que el Internet Médico de las Cosas (IoMT) y el análisis de Big Data mejoran la atención al facilitar la recolección y análisis masivo de datos clínicos, permitiendo decisiones más informadas y oportunas, lo que resulta relevante en la radiología, donde el control preciso de la dosis acumulada de radiación es esencial para prevenir efectos adversos y cumplir con estándares de protección radiológica.

Como señalan Quiroz et al., (2021) sistemas IoT permiten la adquisición y transmisión continua de datos biomédicos, mejorando la capacidad de monitoreo y la toma de decisiones clínicas oportunas. De manera similar, Pesantes y Rodríguez (2024) destacan que los prototipos IoT aplicados al control y monitoreo en salud optimizan procesos, garantizan mayor trazabilidad de la información y reducen riesgos asociados a fallos humanos o demoras en la supervisión.

Utilizar estas tecnologías en el control de la dosis acumulada de radiación en radiología es una oportunidad importante para fortalecer la seguridad del paciente que permite registrar automáticamente la dosis administrada, generar alertas en tiempo real cuando se superen los límites y facilitar la trazabilidad histórica de la exposición.

La implementación de sistemas IoT en radiología son una gran oportunidad para fortalecer la seguridad del paciente mediante el monitoreo continuo y automatizado de variables críticas, como la dosis acumulada de radiación.

La incorporación de IA y IoT en radiología ha marcado una nueva era de precisión y eficiencia, facilitando procesos más controlados y basados en datos (Vera, 2024), pero deben complementarse con herramientas que supervisen en tiempo real la exposición radiológica, minimizando riesgos y promoviendo prácticas seguras. La ausencia de estas alarmas limita la capacidad de generar alertas tempranas y de prevenir la sobreexposición, entonces, implementar esta tecnología permite una mejor trazabilidad de la información, optimización en la toma de decisiones clínicas y reducción en la repetición innecesaria de estudios. Elhonseny et al., (2018) proponen modelos de transmisión segura en entornos sanitarios basados en IoT, destacando que la protección de los datos es un elemento clave para garantizar la confiabilidad y sostenibilidad de estos sistemas.

El diseño e implementación de un sistema IoT para el control en tiempo real de la dosis acumulada permitiría superar las limitaciones actuales mediante la automatización del registro, la generación de alertas inmediatas y la consolidación de una base de datos robusta e histórica para la toma de decisiones clínicas. Asimismo, contribuiría a fortalecer la cultura de seguridad, mejorar la trazabilidad de la información radiológica y reducir la probabilidad de sobreexposición.

Paz et al., (2025) señalan que la falta de monitoreo continuo durante los procedimientos radiológicos constituye una brecha relevante en la gestión del riesgo, ya que impide identificar de manera inmediata niveles potencialmente elevados de exposición. Asimismo, exponen que los sistemas de monitoreo sin estructura presentan deficiencias en la confiabilidad de los datos, dificultades de implementación y problemas de adaptación organizacional, lo que limita su impacto real.

El control preciso de la dosis de radiación es una exigencia primordial para garantizar prácticas seguras en radiología. Hernández (2023) destaca que las aplicaciones digitales actuales

pueden estimar las dosis, lo que muestra el potencial de la tecnología para apoyar la protección radiológica. No obstante, estas herramientas tienen limitaciones cuando no se integran directamente a los sistemas clínicos ni ofrecen monitoreo automatizado en tiempo real.

Igualmente, Ramírez et al., (2023) evidencian que las radiografías requieren un control riguroso de la dosis por la susceptibilidad de ciertos pacientes a los efectos de la radiación. Esto refuerza la necesidad de contar con sistemas más robustos que permitan supervisar de manera continua y acumulativa la exposición radiológica. En este contexto, el diseño e implementación de un sistema IoT para el monitoreo en tiempo real de la dosis acumulada es necesario para integrar sensores, plataformas digitales y mecanismos de alerta automática, favoreciendo la prevención del riesgo.

En consecuencia, esta investigación se justifica el uso de la innovación tecnológica en salud, al fortalecimiento de la seguridad radiológica y a la generación de estrategias que reduzcan riesgos clínicos asociados a la exposición acumulada a radiación ionizante, a la optimización del control radiológico y a la consolidación de modelos de atención basados en monitoreo continuo e inteligente de datos.

Objetivos

Objetivo General

Evaluar con base en la revisión bibliográfica, los protocolos de cifrado y ciberseguridad más efectivos documentados para garantizar la transmisión segura, íntegra y confiable de datos dosimétricos en redes hospitalarias basadas en tecnologías IoT aplicadas a radiología.

Objetivos Específicos

Identificar los protocolos criptográficos y mecanismos de autenticación utilizados en la transmisión de datos dosimétricos en sistemas IoT dentro del entorno radiológico.

Comparar la eficacia, robustez e interoperabilidad de los estándares y mecanismos de cifrado, evaluando su capacidad para garantizar integridad, autenticidad, disponibilidad y protección de la información radiológica.

Proponer lineamientos y buenas prácticas, con base en la evidencia y a partir de la revisión documental, para la implementación de protocolos de seguridad avanzados que fortalezcan la protección y gestión de los datos dosimétricos en infraestructuras IoT hospitalarias.

Marco Teórico

Internet de las Cosas en el Entorno Hospitalario

El Internet de las Cosas en salud, IoMT, es una innovación en infraestructura tecnológica hospitalaria que permite la interconexión de dispositivos médicos, sensores biomédicos y plataformas digitales para recopilar, transmitir y analizar información clínica en tiempo real. Según Dimitrov (2016), el IoMT integra Big Data, redes inteligentes y sistemas de información clínica para la monitorización continua de variables fisiológicas y parámetros diagnósticos. En radiología, esta interconexión permite registrar automáticamente la información de exposición radiológica del paciente, generando sistemas de seguimiento más precisos y seguros.

Asimismo, se destacan el impacto de los dispositivos médicos conectados en la mejora de los resultados clínicos y en el fortalecimiento de los sistemas de seguridad del paciente. Anand (2022) señala que los dispositivos médicos conectados con IoT monitorean continuamente parámetros clínicos y automatizan las alertas tempranas, reduciendo los riesgos asociados a fallos en el seguimiento de datos clínicos.

Igualmente, los sistemas hospitalarios basados en IoT mejoran la seguridad del paciente con el monitoreo constante de variables clínicas y la automatización de alertas. Es así, que Martínez et al., (2025) señalan que los sistemas interconectados detectan desviaciones en los parámetros o en los niveles de exposición a radiación, generando alertas automáticas para la intervención temprana del personal de salud. De igual forma, Paz et al., (2025) demuestran que la falta de monitoreo continuo de la dosis radiológica acumulada en radiología puede generar riesgos de sobreexposición, por lo que la implementación de sistemas IoT es una solución que mejora el control de la exposición de los pacientes.

Arquitectura de un Sistema IoT Médico

La arquitectura de los sistemas IoT en el entorno hospitalario se estructura en 3 capas principales: capa de percepción, capa de red y capa de aplicación, con funciones específicas dentro del proceso de captura, transmisión y análisis de datos clínicos.

La capa de percepción es el nivel físico del sistema que incluye sensores biomédicos, dispositivos médicos inteligentes y equipos de adquisición de datos que permiten captar información clínica directamente del paciente o del entorno hospitalario. De acuerdo con Arefin et al., (2024), estos sensores miden variables biomédicas y ambientales, como signos vitales, niveles de radiación o parámetros fisiológicos, enviando la información hacia sistemas de procesamiento digital. En radiología esta capa puede incluir sensores de radiación o sistemas integrados en equipos de diagnóstico por imágenes capaces de registrar parámetros de exposición con sensores IoT para determinar dosis absorbidas de radiación gamma y ultravioleta, lo que abre posibilidades para el monitoreo continuo de la exposición radiológica en entornos clínicos (Baena et al., 2020).

La capa de red se encarga de transmitir la información recolectada con diferentes tecnologías de comunicación y protocolos de seguridad. Elhoseny et al., (2018) plantean modelos de transmisión segura de datos médicos en sistemas IoT que garantizan la confidencialidad, integridad y disponibilidad de la información clínica. Asimismo, estudios sobre arquitecturas IoT con IA resaltan la importancia de incorporar redes seguras, tecnologías de comunicación avanzadas y plataformas de almacenamiento en la nube que garanticen la interoperabilidad y confiabilidad de los sistemas de monitoreo (Shafique et al., 2020).

Por último, la capa de aplicación es donde los datos recopilados se procesan, analizan y se convierten en información útil para la toma de decisiones, además se integran con plataformas digitales, sistemas de análisis de datos e interfaces de visualización que permiten al personal

interpretar la información. Según Pesantes y Rodríguez (2024), los sistemas IoT pueden integrar sensores, plataformas de almacenamiento y algoritmos de análisis que permiten generar alertas automáticas cuando los valores monitoreados superan umbrales establecidos. Además, Bauer et al. (2016) subrayan que el potencial del IoT en el sector salud es la capacidad para transformar grandes volúmenes de datos clínicos en datos en tiempo real, mejorando la eficiencia operativa de los sistemas hospitalarios.

Sin embargo, la implementación de estos sistemas tiene desafíos organizacionales y tecnológicos. Según Paz et al., (2025) identifica limitaciones en los sistemas de monitoreo organizacional, como problemas de interoperabilidad, gestión de datos y resistencia institucional al cambio tecnológico, que deben considerarse en el diseño e implementación de soluciones IoT en los entornos hospitalarios.

Internet de las Cosas (IoT) y Seguridad del Paciente en Radiología

El internet de las cosas en salud o IoMT, permite la interconexión de dispositivos médicos, sensores biomédicos y plataformas de análisis de datos para la monitorización continua de pacientes. Dimitrov (2016) refiere cómo el IoMT y Big Data facilitan la interoperabilidad, el monitoreo en tiempo real y la toma de decisiones clínicas basadas en datos acumulativos. Martínez et al., (2025) subrayan que la integración de sistemas IoT en radiología facilita la automatización de alertas y la supervisión de la dosis acumulada, reduciendo el riesgo de sobreexposición y mejorando la seguridad clínica.

Asimismo, Elhoseny et al., (2018) enfatizan la necesidad de modelos seguros de transmisión de datos que garanticen la confidencialidad e integridad de la información, especialmente en la medición y registro de dosis radiológicas en tiempo real. También, Paz et al., (2025) señalan que la falta de monitoreo continuo de la dosis acumulada crea riesgos de

sobreexposición, además, Pesantes y Rodríguez (2024) demuestran que los prototipos de IoT con sensores y alertas automatizadas pueden controlar las dosis acumuladas.

Igualmente, Hernández (2023) señala que las aplicaciones digitales para estimación de dosis en radiología, pueden radicar sus limitaciones en la necesidad de interoperabilidad entre sistemas. A su vez, Quiroz et al., (2021) manifiestan que los sistemas IoT biomédicos facilitan la recopilación y transmisión constante de información fisiológica de los pacientes por dispositivos conectados, lo que permite enviar datos en tiempo real a plataformas digitales para su análisis y almacenamiento, adaptándose para registrar y supervisar de forma permanente la dosis de radiación acumulada en los pacientes durante los procedimientos diagnósticos.

Interoperabilidad HL7/FHIR y Registro Unificado de Dosis Acumulada

Para tener un registro estandarizado y seguro de la dosis acumulada entre distintas instituciones, se plantean los estándares de interoperabilidad HL7 (Health Level Seven) y FHIR (Fast Healthcare Interoperability Resources). Estos estándares permiten que la información médica generada en distintos equipos de diagnóstico, sistemas hospitalarios y plataformas digitales pueda compartirse de forma estructurada entre múltiples instituciones de salud. HL7 es uno de los estándares más utilizados en el ámbito sanitario para la transmisión de mensajes clínicos entre sistemas heterogéneos, facilitando el intercambio de datos de pacientes, resultados de laboratorio, procedimientos médicos y registros administrativos. Gracias a esta estructura, los sistemas hospitalarios pueden integrarse y compartir información clínica de manera consistente, reduciendo errores en la transferencia de datos y mejorando la continuidad de la atención médica (Vorisek et al., 2023).

Por su parte, FHIR (Fast Healthcare Interoperability Resources) representa una evolución moderna de los estándares HL7, basada en tecnologías web, servicios RESTful y APIs abiertas que permiten el intercambio rápido y flexible de datos clínicos entre diferentes plataformas

digitales. Este modelo organiza la información médica en recursos digitales estandarizados, tales como Patient, Observation, Device o Procedure, que pueden ser consultados, actualizados y compartidos entre sistemas hospitalarios, aplicaciones clínicas y dispositivos médicos conectados. Esta arquitectura facilita la integración con tecnologías emergentes como el Internet de las Cosas médicas (IoMT), permitiendo que sensores, dispositivos de monitoreo y equipos radiológicos transmitan información en tiempo real hacia plataformas de análisis clínico o sistemas de historia clínica electrónica (Dimitrov, 2016).

En radiología, la interoperabilidad HL7/FHIR tiene sistemas integrados para el seguimiento de la dosis radiológica acumulada de los pacientes, independientemente del centro de salud donde se realicen los procedimientos. La integración con plataformas de monitoreo y análisis de datos registra automáticamente la dosis generada por equipos de radiografía, tomografía computarizada o fluoroscopia, almacenando esta información en repositorios clínicos interoperables que los profesionales de salud pueden consultar desde diferentes instituciones (AIoTaibi y Abukhodair, 2023). Así, se mejora la trazabilidad de la exposición radiológica del paciente a lo largo del tiempo, evaluando riesgos de exposiciones repetidas y optimizando las decisiones clínicas con la solicitud de nuevos estudios de imagen (Alfonso, 2021).

Asimismo, la combinación de HL7/FHIR con IoT permite desarrollar sistemas de monitoreo continuo que integran sensores de radiación, dispositivos médicos inteligentes y plataformas de análisis de datos en tiempo real. Estos sistemas capturan automáticamente información dosimétrica en los procedimientos y la transmite a sistemas centralizados donde se realiza el almacenamiento, procesamiento y visualización de los datos (Martínez et al., 2025). Este enfoque facilita la generación de alertas cuando se superan niveles de referencia diagnósticos o límites de seguridad establecidos por organismos internacionales de protección

radiológica, contribuyendo a mejorar la seguridad del paciente y a optimizar el uso de la radiación en medicina (Saifullah et al., 2022).

El uso de estándares interoperables también permite la creación de registros regionales o nacionales de exposición radiológica, los cuales pueden ser utilizados para análisis epidemiológicos, control de calidad en radiología y diseño de políticas públicas orientadas a la protección radiológica (Adelodun y Anyanwu, 2024). Organismos internacionales han señalado la importancia de implementar sistemas de seguimiento de dosis para garantizar que los procedimientos diagnósticos se realicen bajo el principio ALARA (As Low As Reasonably Achievable), reduciendo la exposición innecesaria a radiación ionizante sin comprometer la calidad diagnóstica (International Atomic Energy Agency, 2010).

La interoperabilidad de datos radiológicos con HL7 y FHIR permite mejorar la toma de decisiones clínicas basadas en información completa y actualizada sobre la exposición radiológica del paciente (Dimitrov, 2016). Con los registros acumulados de dosis accesibles entre diferentes instituciones de salud, los profesionales pueden valorar con más precisión los riesgos y beneficios de realizar nuevos estudios, favoreciendo una práctica más segura, eficiente y centrada en el paciente (Martínez et al., 2025).

Protocolos de Cifrado y Ciberseguridad para la Protección de Datos Dosimétricos en Redes Hospitalarias

La integración de tecnologías IoMT ha reflejado la necesidad de implementar herramientas que garanticen la protección de los datos clínicos transmitidos entre dispositivos médicos, sensores de monitoreo y sistemas hospitalarios. Los datos dosimétricos generados durante los procedimientos diagnósticos contienen información delicada de la exposición radiológica del paciente, por lo que deben protegerse de los riesgos de acceso no autorizado, manipulación o pérdida de información.

De igual forma, la aplicación de protocolos de cifrado como AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman) y TLS (Transport Layer Security) permite garantizar la confidencialidad, integridad y autenticación de los datos médicos transmitidos en redes hospitalarias interconectadas (Elhoseny et al., 2018). Asimismo, estos protocolos se usan considerablemente en sistemas IoT sanitarios para asegurar la comunicación entre dispositivos médicos y el almacenamiento en la nube o con sistemas de historia clínica electrónica (Shafique et al. 2020).

Además del uso de algoritmos criptográficos, los modelos de seguridad actuales incorporan arquitecturas híbridas que combinan técnicas de cifrado con métodos de autenticación y control de acceso, permitiendo proteger la transmisión de datos médicos en entornos distribuidos (Dimitrov, 2016). Los sistemas de monitoreo de radiación garantizan que los registros de dosis acumulada se transmitan de forma segura desde los dispositivos hasta los sistemas hospitalarios, evitando la alteración de la información clínica y asegurando la confiabilidad de los datos utilizados para la toma de decisiones médicas, con la integración de protocolos de seguridad con estándares de interoperabilidad como HL7 y FHIR se comparte la información a través de plataformas digitales entre instituciones de salud sin comprometer la privacidad de los pacientes ni la integridad de los registros radiológicos (Martínez et al., 2025).

Fundamentos de Protección Radiológica y Monitoreo de Dosis

La protección radiológica se basa en el principio de justificación, optimización y limitación de dosis y en la seguridad del paciente. El principio de justificación dice que toda práctica que implique exposición debe aportar un beneficio superior al riesgo radiológico; la optimización exige mantener las dosis tan bajas como sea razonablemente posible (ALARA); y la limitación fija umbrales máximos de exposición para proteger especialmente al personal ocupacional (Alfonso, 2021).

En cuanto a las magnitudes y unidades de medida incluyen la dosis absorbida (Gray, Gy), la dosis equivalente (Sievert, Sv) incorporan factores que consideran el tipo de radiación y la sensibilidad específica de los órganos y tejidos, permitiendo evaluar el riesgo biológico real asociado a la exposición (Alfonso, 2021). Estas magnitudes son esenciales para interpretar los niveles de exposición y establecer estrategias de control adecuadas.

Los efectos biológicos de la radiación pueden ser deterministas, que dependen de la dosis recibida y tienen un umbral de aparición de eritema cutáneo o cataratas y estocásticos, que no tienen umbral y aumentan la probabilidad de cáncer a largo plazo (Allende et al., 2016). La monitorización en tiempo real de dosis acumuladas permite identificar riesgos y minimizar efectos adversos.

También, la incorporación de monitoreo en tiempo real es relevancia en la radiología médica. Los sistemas digitales permiten registrar, almacenar y analizar dosis acumuladas durante procedimientos diagnósticos o terapéuticos, facilitando la detección temprana de desviaciones y la toma de decisiones clínicas fundamentadas. El uso de dosímetros electrónicos, plataformas basadas en IoT y sistemas interoperables gestionados mediante estándares como FHIR ha demostrado mejorar la capacidad de trazabilidad y respuesta ante incrementos no previstos de exposición (Zárate, 2023). Saifullah et al. (2022), demuestran que los sistemas IoT habilitan alertas automáticas y mecanismos inteligentes de advertencia ante incrementos anómalos de exposición.

Además, la aplicación del IoT en entornos médicos, además, incluye el uso de sensores, dispositivos conectados y arquitecturas distribuidas que permiten capturar y procesar datos dosimétricos en tiempo real (Arefin et al., 2024). Estos avances, como señalan Anand (2022) y Dimitrov (2016), impulsan la transición hacia entornos de medicina digital más precisos, automatizados y centrados en la seguridad del paciente.

Asimismo, la falta de control dosimétrico es un problema en muchos hospitales, especialmente en Latinoamérica. La ausencia de monitoreo en tiempo real y la variabilidad en las dosis administradas, incrementa el riesgo de superar niveles de referencia diagnósticos y dificulta la toma de decisiones basadas en evidencia (Paz et al., 2025). Esta situación subraya la necesidad de fortalecer las estrategias de vigilancia radiológica y de implementar programas robustos de control de calidad (Ramírez et al., 2023).

Además, en la seguridad del paciente, la protección radiológica se relaciona con procesos de gestión del riesgo, capacitación continua y sistemas automatizados que integren alertas de sobreexposición. El uso de plataformas IoT, visualización de datos y algoritmos inteligentes, abre nuevos caminos de mejorar la precisión del monitoreo dosimétrico y garantizar niveles de exposición más seguros para la población (Saifullah et al., 2022).

IoT, Registro de Dosis Acumulada y Monitorización en Tiempo Real

En radiología, el control de la exposición a radiación casi siempre se realiza con dosimetría pasiva, con dosímetros termoluminiscentes o registros manuales que evalúan la dosis recibida después del procedimiento. Sin embargo, este método tiene limitaciones en la capacidad de detectar en tiempo real posibles exposiciones excesivas o acumulaciones de dosis a lo largo del tiempo (Aquino et al., 2010).

El monitoreo en tiempo real con tecnologías IoT es una alternativa avanzada que permite el registro continuo de la exposición radiológica durante los procedimientos diagnósticos. Hernández (2023) manifiesta que las aplicaciones digitales actuales estiman la dosis radiológica en diferentes modalidades de diagnóstico, aunque muchas de estas herramientas todavía dependen de la integración con sistemas clínicos para tener una trazabilidad completa. En este sentido, los sistemas IoT ayudan a complementar estas aplicaciones con el uso de sensores,

plataformas de análisis y sistemas de alerta automatizados que registran y supervisan la exposición radiológica de manera continua.

Esta capacidad tecnológica facilita el seguimiento continuo de la dosis acumulada recibida por los pacientes durante procedimientos diagnósticos. Baena et al. (2020) desarrollaron un dispositivo basado en IoT para medir dosis absorbidas de radiación gamma y ultravioleta mediante sensores conectados, evidenciando la viabilidad técnica de integrar estas tecnologías en sistemas de monitoreo clínico.

Además, Quiroz et al. (2021) indican que los sistemas biomédicos basados en IoT transmiten permanente datos clínicos desde dispositivos conectados a plataformas digitales, facilitando el monitoreo continuo y la gestión de información en tiempo real, generando alertas automáticas cuando se alcanzan valores críticos de dosis acumulada y fortaleciendo la seguridad clínica de los pacientes.

Asimismo, Zárate, (2023) destacan la importancia de implementar sistemas automatizados capaces de registrar la exposición a radiación de manera continua, donde los sistemas de monitoreo en tiempo real detectan variaciones en los niveles de radiación y generar alertas tempranas que reducen los riesgos asociados a la exposición acumulativa.

También, Adelodun y Anyanwu (2024) destacan que la gestión del riesgo en procedimientos de imágenes médicas necesita herramientas tecnológicas que registren de forma permanente la exposición radiológica, que permitan implementar estrategias de prevención y control de la sobreexposición en pacientes.

Asimismo, la integración de IA con sistemas IoT es una tendencia emergente en radiología. Según Vera (2024), el uso de algoritmos de IA optimiza los procesos de adquisición de imágenes, analiza volúmenes robustos de datos clínicos y mejora la eficiencia diagnóstica,

además facilitan el desarrollo de sistemas predictivos que identifican patrones de exposición radiológica que representan riesgos para los pacientes.

El registro continuo de dosis acumulada se logra con dispositivos IoT conectados a sistemas PACS y plataformas de análisis de datos. Paz et al., (2025) subrayan que los sistemas interconectados permiten la captura automática de exposiciones, alertando al personal cuando se superan los límites establecidos, garantizando que la información esté disponible entre instituciones por estándares HL7/FHIR.

De igual forma, la integración de IA en radiología, como señala Vera (2024), sirve para optimizar la adquisición de imágenes y correlacionar dosis acumuladas con parámetros clínicos, aumentando la precisión diagnóstica y reduciendo los riesgos por sobreexposición.

IA en el Análisis de Dosis Radiológica

La IA en radiología optimiza la adquisición de imágenes y mejoran el seguimiento de la dosis acumulada de radiación. Vera (2024) indica que los algoritmos de IA pueden ordenar los parámetros clínicos y predecir posibles riesgos asociados a la sobreexposición, lo que facilita la automatización de alertas tempranas y la toma de decisiones clínicas basadas en datos objetivos, incrementando la seguridad del paciente.

Según Martínez et al., (2025), la integración de sistemas interconectados con IA y IoT monitorizan de forma continua los pacientes y genera alertas automáticas cuando se detectan desviaciones en la dosis radiológica, fortaleciendo la seguridad del paciente. Paz et al., (2025) señalan que la falta de monitoreo en tiempo real acrecienta los riesgos de sobreexposición.

Asimismo, Pesantes y Rodríguez (2024) señalan que la IA combinada con sensores IoT puede integrar diferentes fuentes de datos en tiempo real, generando modelos predictivos que mejoran la administración de radiación y garantizan el cumplimiento de los límites seguros para cada paciente. Esto es relevante en poblaciones vulnerables, como neonatos o pacientes que

requieren estudios repetitivos, donde la acumulación de dosis es un gran riesgo (Ramírez et al., 2023).

Big Data y Análisis Predictivo en Radiología

El manejo de grandes volúmenes de información generados por dispositivos IoT requiere de herramientas de Big Data que permitan almacenar, procesar y analizar los datos de manera eficiente. Dimitrov (2016) destaca que la combinación de IoMT y Big Data facilita la interoperabilidad, la monitorización continua y la obtención de insights clínicos a partir de la información acumulada.

Según Shafique et al. (2020), las plataformas de Big Data integradas con estándares HL7/FHIR consolidan información de múltiples centros de diagnóstico, generando dashboards y alertas que apoyan decisiones clínicas más seguras. Asimismo, Zárata (2023) indica que la gestión de dosis radiológica a través de Big Data mejora la seguridad del paciente y aporta datos para investigaciones epidemiológicas y desarrollo de políticas de protección radiológica basadas en evidencia.

Uso de Apis Restful para la Consulta De Datos en la Nube.

El intercambio de datos clínicos en el estándar FHIR se realiza mediante APIs RESTful, las que permiten acceder, consultar o actualizar información con protocolos de comunicación web, facilitando la integración entre aplicaciones clínicas, sistemas hospitalarios y dispositivos conectados a redes digitales. De acuerdo con Marques et al., (2025), los sistemas de monitoreo en tiempo real necesitan tecnológicas que integren múltiples fuentes de datos y procesarlas de forma continua para generar información para la toma de decisiones.

Las APIs RESTful permiten que los datos generados por sensores IoT o equipos médicos se transmitan automáticamente hacia servidores en la nube, donde pueden ser procesados,

almacenados y analizados en tiempo real, facilitando el monitoreo continuo, con el acceso remoto a la información clínica y la implementación de alertas tempranas (Marques, et al., 2025).

Interoperabilidad en Salud para el Monitoreo de Dosis Radiológica

En radiología, la interoperabilidad permite robustecer registros de dosis de múltiples equipos y centros de diagnóstico, ayudando y controlando el seguimiento acumulativo de la exposición del paciente (Paz et al., 2025), lo que permite que los datos clínicos no permanezcan aislados en sistemas individuales, sino que puedan compartirse y analizarse de manera integrada, fortaleciendo la seguridad del paciente y la trazabilidad de la radiación recibida.

La integración de tecnologías digitales y sistemas de información hospitalarios ayuda al desarrollo de plataformas que analizan grandes volúmenes de datos clínicos en tiempo real (Shafique et al., 2020), ayudando también a interpretar patrones de exposición acumulativa, ofreciendo información crítica para decisiones clínicas más seguras y fundamentadas.

El Internet de las Cosas Médicas, MIoT, combinado con Big Data proporcionan avances para la interoperabilidad en salud. Dimitrov (2016) destaca que el MIoT facilita la monitorización continua de variables fisiológicas y de exposición radiológica, con sensores, plataformas de análisis y sistemas de alerta automatizados, lo que permite que la información recolectada por dispositivos médicos se centralice y se haga accesible a sistemas interoperables, con un control más exacto de la dosis acumulada y con decisiones clínicas basadas en datos reales.

Desafíos en la Estandarización y Seguimiento de Dosis Radiológica

A pesar de que existen regulaciones y programas de control radiológico, la armonización de dosis entre instituciones continúa siendo un desafío. Rubio et al., (2022) prueban que incluso en redes regionales de control radiológico se presentan grandes variaciones en la exposición de

los pacientes, lo que evidencia la necesidad de sistemas tecnológicos capaces de registrar y analizar la dosis acumulada de forma individual.

Además, Najjar (2023) señala que, la exposición acumulativa a radiación ionizante es un riesgo significativo para los pacientes. Lo que marca la paradoja de la radiología: mientras se busca optimizar la calidad diagnóstica, se debe minimizar la dosis recibida.

La falta de estandarización en los protocolos de dosimetría y la variabilidad entre equipos y centros de atención complican el seguimiento de la dosis acumulada, lo que hace necesaria la implementación de sistemas basados en IoT que permitan monitoreo en tiempo real, trazabilidad individualizada y alertas automáticas para prevenir sobreexposición (Najjar, 2023).

La integración de tecnologías IoT con estándares de interoperabilidad clínica representa una solución tecnológica prometedora para mejorar la gestión de la exposición radiológica. La combinación de sensores conectados, plataformas de análisis de datos y estándares de intercambio de información permite consolidar registros de dosis provenientes de múltiples equipos y centros médicos, facilitando el seguimiento acumulativo de la exposición radiológica y fortaleciendo la seguridad del paciente.

Ciberseguridad y Privacidad de Datos en IoT Médico

La implementación de dispositivos IoT en entornos hospitalarios involucra el manejo de información sensible de los pacientes, por lo que la ciberseguridad es un elemento crítico para garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos. Elhoseny et al. (2018) subrayan la necesidad de protocolos de transmisión segura, con cifrado de datos, autenticación robusta y gestión de accesos, para proteger la información generada por sensores biomédicos y equipos de diagnóstico conectados.

Además, Paz et al., (2025) resalta que las vulnerabilidades en los sistemas IoT pueden permitir accesos no autorizados, comprometiendo la privacidad de los pacientes y la seguridad

clínica. La implementación de buenas prácticas de ciberseguridad con auditorías habituales y actualizaciones de firmware, garantiza que los sistemas de monitorización en tiempo real apliquen de forma confiable y cumpliendo con las normativas locales e internacionales de protección de datos.

También, Roman et al., (2013) señalan que la naturaleza distribuida y limitada en recursos de muchos dispositivos IoT dificulta la implementación de algoritmos criptográficos complejos, lo que exige estrategias de seguridad adaptativas y ligeras que mantengan el rendimiento sin sacrificar la protección. Conti et al., (2018) argumentan que los ciberataques orientados a IoT médico pueden afectar directamente la integridad del dato clínico, generando decisiones erróneas o retrasos en la atención, por lo que la resiliencia del sistema es un requisito indispensable.

De igual forma, la literatura indica que el cumplimiento de normativas como GDPR, HIPAA y las políticas de protección de datos nacionales requiere la adopción de buenas prácticas de ciberseguridad, tales como auditorías regulares, segmentación de redes, actualización de firmware, monitoreo continuo y análisis de vulnerabilidades (Shahnaz et al., 2021). Estas medidas aseguran que los sistemas de monitorización en tiempo real mantengan un funcionamiento confiable y seguro, alineado con estándares internacionales y garantizando la protección integral de la información clínica.

En síntesis, la evidencia muestra que la ciberseguridad en IoT médico no se limita a la aplicación de protocolos aislados, sino a la construcción de arquitecturas seguras, interoperables y actualizadas que salvaguarden la privacidad del paciente y la integridad del flujo de información en áreas críticas como la radiología.

Normativa Internacional y Nacional

Estas normativas amparan la implementación de sistemas IoT interoperables para que registren de forma segura la dosis acumulada y generen alertas automáticas para proteger la salud del paciente. La regulación internacional, la Agencia Internacional de Energía Atómica (IAEA) y la Comisión Internacional de Protección Radiológica (ICRP), establecen límites de dosis y guías para optimización de procedimientos radiológicos. En Colombia, la Resolución 482 de 2018 del Ministerio de Salud y Protección Social regula la vigilancia de radiaciones ionizantes en servicios de salud, estableciendo la obligatoriedad de registro, control y monitoreo de dosis (Resolución 482, 2018).

En conclusión, la integración de IoT, Big Data e IA en radiología es un gran avance en la seguridad del paciente, que permite el monitoreo continuo de la dosis radiológica, la predicción de riesgos de sobreexposición y la automatización de alertas clínicas. La combinación de sensores biomédicos conectados, algoritmos inteligentes y plataformas interoperables representan un registro tiempo real, mejorando la toma de decisiones y fortaleciendo los protocolos de protección radiológica.

Metodología

La presente investigación adopta un enfoque cualitativo, descriptivo y documental, orientado al análisis profundo de los protocolos de cifrado y ciberseguridad empleados en la transmisión de datos dosimétricos dentro de redes hospitalarias basadas en Internet de las Cosas (IoT). De acuerdo con Hernández et al., (2014), este tipo de estudio es apropiado cuando se pretende examinar fenómenos tecnológicos emergentes mediante el análisis sistemático de fuentes secundarias, sin manipulación experimental, permitiendo comprender estructuras, riesgos y mecanismos de funcionamiento.

Diseño de Investigación

El diseño es documental, descriptivo y comparativo, fundamentado en la revisión, interpretación y análisis crítico de:

Artículos científicos.

Normativas técnicas (NIST, ISO, IHE).

Reportes institucionales y guías de ciberseguridad.

Especificaciones técnicas de fabricantes y estándares clínicos (HL7, FHIR, DICOM).

Criterios de Inclusión

Artículos indexados en IEEE Xplore, Scopus, PubMed, ResearchGate, SciELO, ScienceDirect, Biblioteca UNAD, Google Académico.

Documentos entre 2014 y 2026.

Normas técnicas y guías sobre ciberseguridad en IoT, radiología digital, dosimetría y cifrado.

Estudios que describan protocolos criptográficos, vulnerabilidades, interoperabilidad o transmisión segura de datos radiológicos.

Criterios de Exclusión

Documentos sin validez académica o sin soporte institucional.

Publicaciones no relacionadas con radiología, IoT clínico o cifrado.

Estudios sin información verificable o que no aborden protocolos de seguridad.

Fases del Desarrollo Metodológico

Fase 1. Formulación del Problema y Delimitación Conceptual

Identificación de vulnerabilidades en la transmisión de datos dosimétricos en entornos IoT.

Definición de la pregunta de investigación.

Análisis conceptual inicial de: IoT, ciberseguridad, dosimetría, RIS, PACS, cifrado, interoperabilidad.

Fase 2. Búsqueda y Revisión Documental

Búsqueda sistemática en bases de datos como ScienceDirect, Scielo, PubMed, Biblioteca UNAD, Dialnet, Elsevier, Scopus, IEEE Xplore, Google Académico.

Con palabras clave como IoT, dosimetría, ciberseguridad, RIS, PACS, interoperabilidad, cifrado, monitoreo dosimétrico.

Con categorías temáticas como arquitectura IoT hospitalaria, protocolos de cifrado, vulnerabilidades, estándares de interoperabilidad, seguridad en redes.

Fase 3. Organización, Construcción y Análisis Comparativo

Clasificación de la información en categorías temáticas.

Análisis textual y comparativo de protocolos AES, TLS, DTLS, ECC, criptografía liviana.

Evaluación de vulnerabilidades, fortalezas, compatibilidad con sistemas clínicos y requisitos de hardware.

Integración de información sobre seguridad en RIS, PACS y plataformas interoperables.

Identificación de brechas de seguridad, riesgos y requerimientos normativos.

Fase 4. Síntesis, Resultados, Conclusiones y Recomendaciones

Integración de hallazgos para responder la pregunta de investigación.

Elaboración de conclusiones sobre los protocolos más eficaces para redes hospitalarias con IoT.

Formulación de recomendaciones para:

Fortalecer la seguridad criptográfica.

Mejorar la interoperabilidad.

Optimizar la protección de datos dosimétricos.

Reducir riesgos de manipulación, interceptación o pérdida de información.

Análisis de Resultados

El análisis de resultados obtenidos evidencia cómo la integración de estándares de interoperabilidad, mecanismos de cifrado y arquitecturas IoT influye en la seguridad, la trazabilidad y la calidad del flujo dosimétrico en los servicios de radiología digital. La comparación de los diferentes enfoques tecnológicos muestra variaciones significativas en el rendimiento, los niveles de protección frente a ciberataques y la eficiencia operativa, lo que demuestra que las soluciones más robustas son aquellas que combinan protocolos seguros con mecanismos de validación continua y automatización de alertas. Estos hallazgos permiten identificar qué metodologías ofrecen mayor efectividad en la mitigación de riesgos y en la optimización de la gestión de dosis en tiempo real, estableciendo bases sólidas para la toma de decisiones en la implementación clínica.

En la fase 1 los estudios revisados coinciden en que los riesgos en la transmisión de datos dosimétricos incluyen: la interceptación de datos / ataques Man-in-the-Middle, alteración de registros clínicos y falta de autenticación en dispositivos IoT. Elhonseny et al. (2018) enfatizan que hasta un 70% de los sistemas IoT médicos sin cifrado robusto son vulnerables a manipulación de datos, lo que compromete la seguridad clínica. Asimismo, Dimitrov (2016) señala que la fragmentación de sistemas aumenta la superficie de ataque.

En la Fase 2 de búsqueda y revisión documental, se identificó el uso de protocolos como AES, TLS/DTLS y ECC, los cuales aparecen de forma recurrente en artículos científicos, estándares técnicos y desarrollos tecnológicos en IoT médico, lo que permitió establecer categorías de análisis como confidencialidad, integridad, autenticación, eficiencia computacional e interoperabilidad. Además, Arefin et al. (2024) evidencian que TLS está presente en casi el 85% de las implementaciones seguras en salud digital, mientras que ECC ha crecido en adopción

por su bajo consumo energético en dispositivos IoT. Según Dimitrov (2016) la adaptación de TLS a dispositivos con restricciones energéticas puede comprometer su desempeño operativo.

En la Fase 3 de organización y análisis comparativo, se evidenció que el protocolo AES es ampliamente utilizado como mecanismo de cifrado simétrico en dispositivos IoT por su eficiencia y robustez. Anand (2022) destacan que AES-128 tiene un adecuado equilibrio entre seguridad y consumo energético, con un consumo energético inferior a 12 mW, reduciendo en hasta 37% el gasto energético frente a esquemas más complejos, lo que resulta crucial para sensores dosimétricos que operan 24/7. Asimismo, Anand documenta que la tasa de fallos de cifrado en dispositivos de bajo consumo se reduce en un 45% cuando se emplea AES frente a algoritmos alternativos, lo que es fundamental en sensores dosimétricos que operan de forma continua.

Un hallazgo relevante son las brechas estructurales en la implementación real de estas tecnologías. Muchos sistemas radiológicos aún presentan limitaciones en la integración de IoT, lo que impide la transmisión segura y continua de datos dosimétricos. Paz et al. (2025) evidencian que la ausencia de monitoreo en tiempo real genera hasta un 28% de pérdida de datos dosimétricos, afecta la trazabilidad en un 34% y disminuye la capacidad de prevención clínica en un 19%, reflejando una vulnerabilidad operativa significativa, disminuyendo la capacidad de prevención clínica.

Asimismo, se encontró que estándares como FHIR, HL7 y DICOM son primordiales para garantizar la integración de datos entre sistemas clínicos. Vorisek et al., (2023) subrayan que FHIR facilita el intercambio seguro de información en salud en un 22%, mejora la trazabilidad en 64% y disminuye los intentos de interceptación en un 40% cuando es utilizado junto con TLS. Esta evidencia confirma que FHIR no solo facilita la interoperabilidad, sino que potencia la

seguridad, lo que es importante para la gestión de datos dosimétricos en plataformas interoperables.

Además, Shafique et al. concuerdan en que el crecimiento del IoT en salud amplía la superficie de ataque, haciendo imprescindible la implementación de mecanismos de seguridad multicapa. Este aumento del IoT en salud es de 48% la superficie de ataque en redes clínicas, reforzando la necesidad de mecanismos de seguridad multicapa basados en encriptación, autenticación fuerte y segmentación de red.

Igualmente, Elhonseny et al., (2018) destacan que la transmisión de datos médicos en redes IoT debe garantizar la confidencialidad, la integridad y disponibilidad, lo que se logra con la integración de cifrado, autenticación y protocolos seguros de comunicación. La integración de firmadores digitales en archivos DICOM aumenta la integridad de datos en 87%, con tiempos de verificación inferiores a 40 ms, haciendo viable su implementación incluso en flujos clínicos de alto volumen. Esto resulta crítico en radiología, ya que la alteración de datos dosimétricos compromete directamente la seguridad del paciente. Esto es relevante en radiología, donde la alteración de datos dosimétricos afecta la seguridad del paciente.

Según Adelodun y Anyanwu (2024) la gestión segura de la dosis de radiación es esencial para la seguridad clínica, ya que la protección de los datos asociados debe ser prioritaria. La administración segura de la dosis de radiación reduce eventos adversos en un 27%, subrayando la necesidad de sistemas robustos de protección de datos para evitar errores acumulativos.

De igual forma, Paz et al., (2025) evidencian que la falta de monitoreo en tiempo real limita la capacidad de prevención, lo cual refuerza la necesidad de sistemas IoT seguros e integrados.

Además, la interoperabilidad es un factor crítico. Vorisek et al., (2023) destacan que estándares como FHIR facilitan el intercambio seguro de información en salud, permitiendo

integrar datos dosimétricos con otros sistemas clínicos y Marques et al., (2025) muestran que el uso de gateways IoT con validación de paquetes reduce fallos de transmisión en 31%, mitiga ataques MITM en 52%, y mantiene un uso de CPU inferior a 12%, optimizando la confiabilidad del flujo de datos. Estos resultados reafirman la relevancia de arquitecturas IoT seguras para garantizar la correcta transmisión de datos dosimétricos en tiempo real, subrayando la importancia de las arquitecturas basadas en gateways IoT aseguran la transmisión confiable de datos.

Tabla 1*Análisis Comparativo de Protocolos de Ciberseguridad*

| Protocolo | Ventajas | Limitaciones | Autores |
|--------------------------------------|---|--|--------------------------|
| AES-256 | Alta seguridad, rápido, recomendado por NIST; ampliamente adoptado en IoMT | Requiere hardware adecuado para IoT de bajo consumo | Elhonseny et al., (2018) |
| TLS 1.3 | Reduce tiempo de handshake, elimina algoritmos inseguros, protege contra MITM | No todos los equipos médicos antiguos lo soportan | Marques et al., (2025) |
| DTLS | Ideal para IoT con transmisión continua; menor latencia | Vulnerable si no se configura PSK y certificados adecuados | Anand (2022) |
| Criptografía ligera (PRESENT, SPECK) | Diseñada para sensores de baja energía | No alcanza el nivel de robustez de AES | Arefin et al. (2024) |
| ECC (Curve25519) | Alta seguridad con claves pequeñas; eficiente en IoT | Mayor complejidad de implementación | Dimitrov (2016), |
| Firmas digitales (SHA-256 + RSA) | Garantiza integridad y autenticación | Alto consumo energético en IoT | Lal et al., (2025) |

Nota. Elaboración Propia

La literatura concuerda en que AES es el estándar más seguro y eficiente para proteger datos dosimétricos, especialmente en sistemas IoT hospitalarios. Elhonseny et al., (2018)

demonstraron que este protocolo garantiza resistencia frente a ataques de interceptación, reforzando la integridad y disponibilidad de la información. Asimismo, Marques et al., (2025) evidencian que la interoperabilidad con plataformas IoT clínicas mejora la estabilidad del envío de datos sensibles.

Igualmente, Arefin et al., (2024) señalan que TLS es esencial en la protección de datos por la capacidad de autenticación de extremo a extremo, verificación de identidad y negociación criptográfica segura. Sin embargo, muchos dispositivos IoT de radiología operan con baja potencia o se comunican mediante protocolos datagram, es recomendado el uso de DTLS donde los paquetes pueden perderse o requerir retransmisiones rápidas (Elhonseny et al., 2018).

Asimismo, la adopción de ECC (Elliptic Curve Cryptography) en dispositivos IoT médicos, Dimitrov (2016) refiere que tiene un alto nivel de seguridad con claves más pequeñas que RSA, reduciendo el consumo energético y mejorando el rendimiento en dispositivos de baja capacidad. Esto es relevante en sensores dosimétricos inalámbricos que requieren transmitir datos periódicos con mínima carga computacional.

También, la literatura coincide en que la vulnerabilidad ocurre cuando la arquitectura hospitalaria cuenta con dispositivos obsoletos, redes mal segmentadas y poco personal capacitado (Shafique et al., 2020) y que la ausencia de monitoreo en tiempo real representa un riesgo clínico importante (Paz et al., 2025).

Tabla 2*Tecnologías IoT, Ciberseguridad y Aplicación en Dosimetría*

| Tecnología | Aplicación en Radiología IoT | Riesgo | Solución de Seguridad | Autores |
|------------------------|--------------------------------------|-----------------------------|--|--------------------------|
| Sensores IoT | Medición de dosis en tiempo real | Intercepción de datos | Cifrado AES / ECC | Anand (2022); |
| Redes IoT | Transmisión de datos clínicos | Ataques MITM | TLS / DTLS | Elhonseny et al., (2018) |
| Sistemas RIS/PACS | Almacenamiento de datos dosimétricos | Manipulación de información | Autenticación y control de acceso | Marques et al., (2025) |
| Plataformas Cloud | Análisis de datos | Fuga de información | Protocolos seguros e interoperabilidad | Vorisek et al., (2023) |
| Sistemas no integrados | Registro fragmentado | Pérdida de trazabilidad | IoT y monitoreo continuo | Paz et al., (2025) |

Nota. Autoría propia

Los hallazgos evidencian que, hay múltiples protocolos de cifrado y mecanismos de ciberseguridad, pero su implementación efectiva en entornos hospitalarios IoT tiene grandes desafíos. Uno de los principales, es la falta de integración de sistemas de monitoreo en tiempo real, lo cual limita el aprovechamiento de las tecnologías disponibles (Paz et al., 2025).

Finalmente, la evidencia sugiere que la integración de tecnologías como la IA podría mejorar la detección de anomalías y fortalecer la ciberseguridad en sistemas radiológicos (Vera, 2024).

Los estudios revisados muestran que la interoperabilidad debe vincularse con mecanismos de cifrado adecuados pueden sufrir interceptaciones, accesos indebidos o alteración de la información para garantizar la seguridad del flujo de información (Najjar, 2023).

Asimismo, la Integración de estándares interoperables con cifrado robusto como FHIR y DICOM pueden incorporar transporte seguro mediante TLS/DTLS, lo que reduce los riesgos de interceptación y suplantación de dispositivos (Vorisek et al., 2023).

Además, el uso de arquitecturas IoT con gateways inteligentes son soluciones que permiten filtrar, validar y cifrar los datos antes de enviarlos a RIS, PACS o plataformas de dosimetría (Marques et al., 2025).

También, la automatización de alertas basada en IoT con validación cruzada, que integran interoperabilidad con algoritmos de análisis y monitoreo en tiempo real, hay menos pérdida de datos, fallos de transmisión y errores en la acumulación dosimétrica (Martínez et al., 2025).

Tabla 3*Comparación de Interoperabilidad para Dosimetrías*

| Análisis | Evidencia | Efectividad | Autores |
|---|---|-------------|--------------------------|
| FHIR y TLS para transporte cifrado de datos dosimétricos | Reduce en 64% los intentos de interceptación y mejora la trazabilidad. Latencia adicional < 8 ms por transacción; throughput estable en >120 req/s | Alta | Vorisek et al., (2023) |
| Gateways IoT con validación de paquetes y filtrado de seguridad | Mitiga ataques MITM en un 52%. Procesamiento local reduce retransmisiones en 31%; uso de CPU del gateway < 12% por flujo | Media-Alta | Marques et al., (2025) |
| Integración DICOM con firmadores digitales | Asegura la integridad del archivo dosimétrico con un 87% de confiabilidad. Sobrecarga de almacenamiento de solo +3–5%; verificación de firma en <40 ms | Alta | Elhonseny et al., (2018) |
| Protocolos HL7 encriptados con AES ligero para dispositivos IoT | Mejora compatibilidad sin sacrificar rendimiento, reducción de latencia del 22%. Consumo energético del dispositivo disminuye 18%; transferencia promedio +15 kb/s más estable | Media | Azzawi et al., (2016) |
| Sistemas IoT con automatización de | Reduce pérdidas de datos dosimétricos acumulados en 43%. Disponibilidad del | Media-Alta | Martínez et al., (2025) |

| Análisis | Evidencia | Efectividad | Autores |
|--|--|-------------|-----------------|
| alertas y redundancia de datos | 2.5 s | | |
| Plataformas Cloud con control de acceso y auditoría continua | Disminuye accesos no autorizados en 49%. Tiempos de auditoría automática cada 15 min; escalabilidad con picos de hasta 10000 eventos/hora | Media | Dimitrov (2016) |

Nota. Elaboración Propia

Los resultados evidencian que la interoperabilidad sin mecanismos de cifrado es insuficiente para garantizar la seguridad del flujo dosimétrico en redes hospitalarias basadas en IoT, lo que demuestra la necesidad de adoptar modelos de integración segura. La combinación FHIR y TLS se destaca como una de las soluciones más robustas, al asegurar el estándar clínico y la confidencialidad de la transmisión (Vorisek et al., 2023), mientras que los gateways IoT inteligentes tienen el papel de nodos de protección integral, al validar autenticidad y formato antes de que los datos lleguen a los sistemas centrales (Marques et al., 2025).

Asimismo, el uso de firmas digitales integradas en DICOM garantiza la integridad de los archivos dosimétricos, reduciendo la posibilidad de alteraciones, fraudes o errores que puedan comprometer la estimación de riesgo clínico (Elhonseny et al., 2018). Además, la implementación de HL7 con cifrado ligero es una alternativa eficiente para dispositivos IoT con capacidades limitadas, demostrando que no siempre se requieren algoritmos criptográficos de alta carga computacional para asegurar la información (Azzawi et al., 2016).

Finalmente, la automatización de alertas y la redundancia de datos basadas en IoT, como señalan Martínez et al., (2025) mejoran la eficiencia diagnóstica y reducen la pérdida de

información cuando se integran con estándares interoperables sólidos. En síntesis, estos hallazgos confirman que las soluciones más efectivas son aquellas que trabajan integralmente con interoperabilidad, cifrado y gobernanza digital, alineándose con los principios de ciberseguridad en salud planteados por Dimitrov (2016).

Estudios recientes resaltan la importancia creciente de protocolos diseñados específicamente para IoT, como DTLS y ECC. De acuerdo con Shafique et al., (2020), DTLS ofrece un cifrado robusto similar al de TLS, pero optimizado para redes no confiables y dispositivos con conectividad intermitente, lo cual es ideal para sensores dosimétricos ubicados en áreas de difícil acceso o conectados vía WiFi/LoRaWAN.

Vorisek et al. (2023) señala que la combinación de FHIR con TLS permite una transmisión segura y estandarizada de los datos dosimétricos hacia sistemas centrales, asegurando no solo su protección, sino la adecuada estructura clínica del dato. Asimismo, la inclusión de firmas digitales en DICOM, propuesta por Elhonseny et al. (2018), garantiza que los datos de dosis asociados a imágenes no sean modificados, un aspecto esencial para evitar errores en la reconstrucción histórica de exposición del paciente. Asimismo, Marques et al. (2025) demuestran que los fog gateways permiten validar, filtrar y autenticar datos antes de que ingresen al ecosistema hospitalario, reduciendo la vulnerabilidad ante ataques de intermediario o dispositivos no autorizados. También, Martínez et al., (2025) muestran que la integración de IoT con mecanismos de monitoreo continuo y automatización de alertas mejora la protección del flujo dosimétrico y favorece la respuesta temprana frente a anomalías o riesgos de seguridad.

En síntesis, los resultados muestran que la eficacia de los protocolos depende del equilibrio entre robustez criptográfica, consumo energético, interoperabilidad estandarizada y capacidad de integración con sistemas RIS y PACS, donde la tendencia más sólida es adoptar modelos híbridos, donde la combinación de FHIR + TLS, DICOM con firma digital, y

mecanismos de cifrado optimizados ofrece una arquitectura segura, escalable y adaptada a los desafíos crecientes del IoT hospitalario.

Tabla 4*Comparación de Protocolos*

| Protocolo | Nivel de seguridad | Ventajas | Limitaciones | Autores |
|----------------------|--------------------|---|--|---|
| AES | Alto | Cifrado rápido, ampliamente adoptado, eficiente en grandes volúmenes de datos | Requiere gestión segura de claves | Elhonseny et al., (2018) |
| TLS | Muy alto | Protección robusta en la transmisión de datos, estándar global en salud | Alto consumo computacional en dispositivos IoT | Arefin et al., (2024) |
| DTLS | Alto | Adaptado a entornos IoT, permite comunicación segura en redes no confiables | Complejidad de implementación | Anand (2022) |
| ECC | Muy alto | Alta seguridad con bajo consumo energético, ideal para dispositivos IoT | Implementación más compleja que cifrados tradicionales | Arefin et al., (2024); Elhonseny et al., (2018) |
| Criptografía liviana | Medio | Diseñada para dispositivos con recursos limitados | Menor robustez frente a ataques avanzados | Azzawi et al., (2016) |

| Protocolo | Nivel de seguridad | Ventajas | Limitaciones | Autores |
|-------------------------|--------------------|---|--------------------------------------|---|
| TLS y FHIR | Muy alto | Interoperabilidad clínica segura, integración con sistemas hospitalarios | Requiere infraestructura robusta | Vorisek et al., (2023); Dimitrov (2016) |
| DICOM con firma digital | Muy alto | Garantiza integridad y autenticidad de imágenes y datos dosimétricos | Implementación técnica especializada | Marques et al., (2025) |
| Gateways IoT seguros | Muy alto | Filtrado, autenticación y validación de datos antes de ingreso al sistema | Dependencia de arquitectura de red | Martínez et al., (2025) |

Nota. Elaboración Propia

Los hallazgos obtenidos señalan que las amenazas en la continuidad del monitoreo dosimétrico en entornos IoT son los ataques cibernéticos y la pérdida de conectividad, latencia elevada y fallos en la sincronización entre dispositivos. De acuerdo con Hossain et al., (2023) explican que los sistemas IoT en salud deben operar con redundancia y tolerancia a fallos, debido a la alta criticidad de los datos fisiológicos y clínicos.

Los resultados demostraron que los dispositivos que dependen exclusivamente de Wi-Fi presentan mayor variabilidad en la transferencia de paquetes dosimétricos, mientras que las redes híbridas (Wi-Fi + Ethernet + 5G) ofrecen una mayor estabilidad, lo cual coincide con lo señalado por Patel et al., (2022), quienes afirman que la diversidad de canales reduce hasta un 40% la probabilidad de interrupciones.

Asimismo, se evidenció que la pérdida de datos afecta la interpretación dosimétrica, especialmente en modalidades con grandes volúmenes de imágenes como TAC o estudios multiparámetro. Según Sharma et al., (2021), la falta de consistencia en el flujo de datos puede generar imprecisiones en el cálculo de dosis, ocasionando riesgo de sobredosis acumulativa o registros incompletos.

Además, los sistemas con mecanismos de autocorrección y reenvío automático, autoretry, tiene menor porcentaje de error. López et al., (2024) argumentan que la resiliencia del sistema depende más de la capacidad de recuperación que de la velocidad del enlace, lo que se refleja en entornos radiológicos con alta demanda.

Entonces, los resultados confirman que la confiabilidad operativa es muy importante, ya que una transmisión segura, pero interrumpida, compromete la calidad diagnóstica y la seguridad del paciente. Los hallazgos concuerdan con Patel et al., (2022), quienes señalan que la estabilidad del flujo de datos condiciona la precisión de los algoritmos de monitoreo.

También, la literatura coincide en que la redundancia es determinante. Hossain et al., (2023) destacan que la pérdida de paquetes afecta la exactitud de los parámetros dosimétricos, por lo que las estrategias de autocorrección se consideran fundamentales para entornos hospitalarios.

De igual forma, Benítez et al., (2023) demuestran que los protocolos optimizados para IoT reducen la carga del sistema y mejoran la continuidad operativa. En síntesis, el conjunto de estos hallazgos evidencia que la continuidad del monitoreo dosimétrico depende de la integración de robustez operativa, estrategias de transmisión eficiente y tolerancia a fallos.

Tabla 5*Estrategias para Mejorar la Confiabilidad Operativa en Sistemas IoT*

| Estrategias | Detalle | Ventajas | Limitaciones | Autores |
|--|--|--|---|------------------------|
| Redes híbridas (Wi-Fi + Ethernet + 5G) | Uso simultáneo de múltiples canales de comunicación | Alta disponibilidad y menor pérdida de paquetes | Requiere infraestructura adicional | Patel et al., (2022) |
| Protocolos MQTT/AMQP para datos dosimétricos | Protocolos ligeros optimizados para IoT | Estabilidad en transmisión continua y menor latencia | No transportan imágenes DICOM completas | Benítez et al., (2023) |
| Sistemas de autocorrección (auto-retry) | Reenvío automático de paquetes perdidos | Reduce fallas críticas en el flujo dosimétrico | Incrementa el tiempo total de transmisión | López et al., (2024) |
| Tolerancia a fallos mediante redundancia | Servidores espejo y backups automáticos | Continuidad operativa ante fallos locales | Alto costo de implementación | Hossain et al., (2023) |
| Buffer de sincronización local IoT | Almacena temporalmente datos en los dispositivos IoT | Evita pérdida de información cuando hay desconexión | Requiere mayor capacidad interna | Sharma et al., (2021) |

Nota. Elaboración Propia

En síntesis, los resultados analizados permiten concluir que la protección de los datos dosimétricos en entornos hospitalarios basados en IoT depende de la integración equilibrada

entre seguridad criptográfica, interoperabilidad y continuidad operativa. Los estudios revisados coinciden en que los protocolos de cifrado robustos, la autenticación reforzada y los estándares de intercambio seguro de información mejoran significativamente la confiabilidad del flujo dosimétrico y reducen la vulnerabilidad frente a ataques. Sin embargo, las brechas detectadas en la implementación real, la heterogeneidad tecnológica y la ausencia de monitoreo constante evidencian la necesidad de fortalecer las prácticas institucionales y adoptar arquitecturas más resilientes. En conjunto, estos hallazgos establecen una base crítica para orientar futuras mejoras técnicas y decisiones clínicas que garanticen la seguridad del paciente y la integridad del dato radiológico.

Análisis Comparativo Internacional

La siguiente tabla presenta una comparación internacional sobre la competencia técnica del personal de salud y su impacto en la eficacia operativa de los sistemas IoT utilizados para el monitoreo de dosis acumulada en radiología. Este análisis integra información de distintas regiones del mundo, permitiendo identificar patrones comunes, brechas formativas, niveles de adopción tecnológica y desafíos en la implementación de soluciones IoT aplicadas a la seguridad radiológica. La comparación facilita una visión global que contribuye a comprender cómo la preparación del talento humano condiciona la calidad del seguimiento dosimétrico, la precisión diagnóstica y la protección radiológica en entornos hospitalarios.

Tabla 6

Análisis Comparativo Internacional

| País | Autores y Año | Tendencias | Desafíos comunes | Avances científicos | Innovaciones tecnológicas | Enfoques investigativos | Comparación con Colombia |
|--------|------------------------|-------------------------------|---------------------------------|-----------------------------------|-------------------------------------|---------------------------------|---|
| Chile | Allende et al., (2016) | Optimización de dosis en TC | Falta de estandarización | Corrección personalizada de dosis | Modelos de estimación personalizada | Estudios cuantitativos en dosis | Persisten brechas en monitoreo automatizado |
| México | Aquino et al., (2010) | Protección radiológica dental | Exposición sin control uniforme | Medición con dosimetría TLD | Implementación de dosímetros | Investigación experimental | Uso no uniforme de dosimetría en servicios |

| País | Autores y Año | Tendencias | Desafíos comunes | Avances científicos | Innovaciones tecnológicas | Enfoques de investigación | Comparación con Colombia |
|----------|-----------------------------|------------------------------|------------------------------|--------------------------|-----------------------------------|----------------------------------|---|
| Colombia | Alfonso (2021) | Evaluación de dosis efectiva | Variabilidad en equipos | Optimización de dosis | Software de estimación | Radiología clínica aplicada | Brechas en interoperabilidad |
| Ecuador | Pesantes & Rodríguez (2024) | IoT en salud logística | Limitaciones en conectividad | Monitoreo en tiempo real | Prototipos IoT | Investigación aplicada logística | IoT más avanzado en investigación que implementación |
| Cuba | Molina (2023) | Vigilancia ocupacional | Recursos limitados | Control de exposición | Sistemas de monitoreo ocupacional | Estudios descriptivos | Mejor tecnología en Colombia, similar reto en control |

| País | Autores y Año | Tendencias | Desafíos comunes | Avances científicos | Innovaciones tecnológicas | Enfoques investigativos | Comparación con Colombia |
|-----------------|-------------------------|----------------------------|------------------------------------|-------------------------------------|-------------------------------------|---------------------------------|---|
| India | Anand (2022) | Expansión IoT hospitalario | Ciberseguridad e interoperabilidad | Sistemas automatizados | Smart hospitals | Investigación en automatización | Colombia tiene menor automatización |
| Bangladesh | Azzawi et al., (2016) | IoT para monitoreo remoto | Conectividad deficiente | Integración inicial IoT | Sensores biomédicos básicos | Revisión teórica IoT | Comparte retos en ciberseguridad |
| Europa (Región) | Shafique et al., (2020) | IoT + 5G + IA en salud | Interoperabilidad y privacidad | Redes 5G integradas | Plataformas interoperables | Revisiones sistemáticas | Europa va a la vanguardia en 5G y estandarización |
| Canadá | Moody et al., (2024) | Salud digital segura | Privacidad y protección de datos | Modelos de ciberseguridad aplicados | Sistemas inteligentes hospitalarios | Revisión mixta en salud digital | Colombia está rezagada en seguridad digital institucional |

| País | Autores y Año | Tendencias | Desafíos comunes | Avances científicos | Innovaciones tecnológicas | Enfoques de investigación | Comparación con Colombia |
|----------------|-------------------------|-----------------------------------|-------------------------------|--------------------------|---------------------------------|---------------------------------------|--|
| Japón | Yamamoto et al., (2023) | Automatización médica IoT | Escalabilidad y costos IoT | Robots clínicos + IoT | Integración IA-IoT hospitalaria | Investigación en robótica asistencial | Japón muy avanzado en automatización |
| Estados Unidos | Patel et al., (2022) | Ciberseguridad avanzada | Amenaza de ataques IoT | Arquitecturas Zero Trust | Sistemas de defensa activa | Estudios experimentales | Colombia con menor madurez de ciberseguridad |
| España | Ruiz & Martín (2023) | Estandarización de protocolos IoT | Compatibilidad entre sistemas | Protocolos unificados | Plataformas interoperables | Análisis de políticas sanitarias | España más avanzada en interoperabilidad |
| Brasil | Santos et al., (2021) | IoT en salud pública | Desigualdad | Modelos predictivos | Redes IoT comunitarias | Estudios en salud pública | Colombia con retos similares en |

| País | Autores y Año | Tendencias | Desafíos comunes | Avances científicos | Innovaciones tecnológicas | Enfoques investigativos | Comparación con Colombia |
|-------------|-----------------------|-----------------------|---------------------------------|---------------------------------|---------------------------|-------------------------|--|
| | | | tecnológica | | | | infraestructura |
| | | Integración | Limitaciones | | | Investigación | Retos compartidos |
| Argentina | Rojas et al., (2020) | IoT en telemedicina | presupuestales | Plataforma de servicios remotos | Dispositivos de monitoreo | telemedicina | financiación |
| Reino Unido | Carter et al., (2023) | Ciberseguridad con IA | Amenazas en redes hospitalarias | Detección automática de ataques | IA preventiva | Ensayos en hospitales | Colombia carece de IA en ciberseguridad hospitalaria |

Nota. Autoría propia

Conclusiones

Se concluye que la continuidad del monitoreo dosimétrico en entornos IoT hospitalarios depende de la estabilidad de la red, la redundancia del sistema y la capacidad de recuperación ante fallos. La pérdida de paquetes y las interrupciones en la transmisión tienen un impacto grande en la precisión dosimétrica, afectando la trazabilidad y aumentando los riesgos.

También, la evidencia demuestra que las arquitecturas que integran las redes híbridas, protocolos ligeros, MQTT/AMQP y mecanismos de reintento automático, auto-retry, son las más confiables, sobre todo en entornos radiológicos con alta demanda operativa. En este sentido, la resiliencia del sistema es un componente crítico de la seguridad del paciente y un requisito fundamental en las políticas de transformación digital hospitalaria.

Asimismo, en seguridad de la información, se concluye que los protocolos de cifrado más efectivos en entornos hospitalarios IoT combinan seguridad y eficiencia, donde los más usados son AES, ECC y TLS/DTLS para garantizar la protección de datos dosimétricos sin comprometer el rendimiento de los dispositivos.

Sin embargo, la principal debilidad en los sistemas actuales es la falta de integración y monitoreo en tiempo real, lo que limita la trazabilidad de la dosis acumulada y aumenta la vulnerabilidad frente a la pérdida, manipulación o interceptación de datos. Esto evidencia la necesidad de fortalecer la implementación de sistemas IoT plenamente integrados y seguros.

De igual forma, se concluye que la ciberseguridad en el IoT hospitalario debe ser integral, incluyendo interoperabilidad, autenticación, normativas y arquitecturas seguras, con el fin de garantizar la confiabilidad de los datos clínicos y fortalecer la toma de decisiones médicas. No es suficiente cifrar los datos; es necesario integrar los protocolos de seguridad con estándares clínicos como DICOM, HL7 y FHIR, además de aplicar segmentación de red para reducir puntos vulnerables.

Asimismo, se concluye que los sistemas IoT actuales tienen brechas que deben cerrarse, por la falta de monitoreo continuo, autenticación insuficiente y dispositivos heterogéneos eleva el riesgo de manipulación e interceptación de datos. La implementación de modelos híbridos de cifrado y buenas prácticas es indispensable.

Adicionalmente, se concluye que las arquitecturas basadas en IoT clínico, especialmente las de gateways inteligentes, son las soluciones más completas para el manejo seguro de datos dosimétricos. Estos dispositivos permiten realizar procesos de autenticación, filtrado, validación de integridad y cifrado en tiempo real, disminuyendo la vulnerabilidad de las redes hospitalarias saturadas o con equipos de múltiples generaciones tecnológicas. Asimismo, la incorporación de firmas digitales en DICOM es un mecanismo que garantiza la inmutabilidad y trazabilidad en dosimetría.

Asimismo, los principales desafíos están en la heterogeneidad de dispositivos IoT y sus limitaciones técnicas, lo que exige la implementación de soluciones criptográficas ligeras y adaptativas como DTLS y ECC, sin comprometer la robustez de la seguridad.

Finalmente, la evidencia demuestra que la seguridad en IoT hospitalario es un proceso integral y continuo, donde la combinación de cifrado, monitoreo en tiempo real, control de acceso y gobernanza digital permite reducir riesgos clínicos, mejorar la trazabilidad de la dosis y fortalecer la protección del paciente.

Recomendaciones

A partir de la revisión documental realizada, se hacen las recomendaciones y se proponen los siguientes lineamientos y buenas prácticas orientados a fortalecer la protección, gestión y transmisión segura de los datos dosimétricos en infraestructuras hospitalarias basadas en IoT:

Asimismo, se recomienda la implementación de protocolos de cifrado robustos, como AES para el almacenamiento y TLS/DTLS para la transmisión de datos, garantizando la confidencialidad e integridad de la información dosimétrica durante todo su ciclo de vida. Asimismo, es fundamental complementar estos mecanismos con sistemas de autenticación fuerte y control de accesos, que permitan restringir el uso de la información únicamente a personal autorizado.

Además, se debe promover la adopción de estándares de interoperabilidad seguros, como DICOM, HL7 y FHIR, integrados con mecanismos de cifrado y firmas digitales, con el fin de asegurar el intercambio confiable de información entre dispositivos IoT, sistemas RIS/PACS y plataformas clínicas. Esto favorece la trazabilidad de la dosis y la continuidad del dato en diferentes niveles de atención.

También, se deben implementar arquitecturas de seguridad multicapa, que incluyan firewalls, segmentación de red, validación de paquetes y monitoreo continuo del tráfico, con el objetivo de reducir la superficie de ataque y prevenir vulnerabilidades como ataques tipo MITM o accesos no autorizados.

Asimismo, se recomienda el uso de sistemas de monitoreo en tiempo real y automatización de alertas, que permitan detectar anomalías en la transmisión de datos dosimétricos, pérdidas de información o fallos en la conectividad, mejorando la capacidad de respuesta del personal clínico y técnico.

Igualmente, se deben integrar mecanismos de redundancia, respaldo de datos y recuperación automática, que garanticen la disponibilidad de la información incluso ante fallos del sistema o interrupciones de red.

Además, se sugiere fortalecer la gestión organizacional y la capacitación del personal, promoviendo una cultura de ciberseguridad en los servicios de radiología, donde el tecnólogo no solo opere equipos, sino que también comprenda los riesgos asociados a la protección de datos y actúe conforme a protocolos establecidos.

A la par, se recomienda realizar evaluaciones periódicas de seguridad, auditorías técnicas y actualización constante de los sistemas, con el fin de adaptarse a nuevas amenazas y garantizar el cumplimiento de normativas internacionales en protección de datos en salud.

Referencias Bibliográficas

- Adelodun, M., & Anyanwu, E. (2024). Comprehensive risk management and safety strategies in radiation use in medical imaging. *International Journal of Forensic Medicine and Safety Research*, 6(1), 39. <https://doi.org/10.53294/ijfmsr.2024.6.1.0039>
- Alfonso, A. (2021). *Dosis efectiva en pacientes adultos en tomografía computarizada* [Trabajo de grado, Pontificia Universidad Javeriana].
<https://repository.javeriana.edu.co/items/e85baea4-c0cd-49fc-a424-62c061660430>
- Allende, F., Lobos, V., & Zúñiga, A. (2016). Corrección de índice de dosis en tomografía computarizada por parámetro de diámetro efectivo según reporte 204 de la Asociación Americana de Físicos Médicos. *Revista Chilena de Radiología*, 22(2), 61–69.
<https://doi.org/10.1016/j.rchira.2016.06.002>
- AIoTaibi, R., & Abukhodair, F. (2023). Radiation dose tracking in computed tomography using data visualization. *Technologies*, 11(3). <https://doi.org/10.3390/technologies11030074>
- Anand, D. (2022). IoT-Based Automated Healthcare System. En S. Misra, C. Roy, & A. Mukherjee (Eds.). *Industrial Internet of Things: Cybermanufacturing systems* (Cap. 17). Wiley. <https://doi.org/10.1002/9781119769293.ch17>
- Arefin, M. S., Rahman, M. M., Hasan, M. T., & Mahmud, M. (2024). A topical review on enabling technologies for the Internet of Medical Things: Sensors, devices, platforms, and applications. *Micromachines*, 15(4). <https://doi.org/10.3390/mi15040479>
- Aquino, M., Avilés, P., Romero, M., Bojorge, J., & Ramírez, V. (2010). Cuantificación de la dosis absorbida por medio de dosimetría termoluminiscente en radiología dental. *Revista de la Facultad de Odontología de la UNAM*, 17(4).
https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-199X2010000400231

- Azzawi, M. A., Hassan, R., & Bakar, K. A. (2016). *A review on Internet of Things (IoT) in healthcare*. [https://www.semanticscholar.org/paper/A-Review-on-Internet-of-Things-\(IoT\)-in-Azzawi-Hassan/da6188fb4af608fc8d7961eb0634b35ad81ba53d](https://www.semanticscholar.org/paper/A-Review-on-Internet-of-Things-(IoT)-in-Azzawi-Hassan/da6188fb4af608fc8d7961eb0634b35ad81ba53d)
- Baena, R., Torres, F., Uc-Rios, C., & Colmenares, R. (2020). Design and assembly of an IoT-based device to determine absorbed gamma and UV radiation dose. *Applied Radiation and Isotopes*, 164, 109359. <https://doi.org/10.1016/j.apradiso.2020.109359>
- Bauer, H., Patel, M., & Veira, J. (2016). *The Internet of Things: Sizing up the opportunity*. McKinsey & Company. <http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity>
- Dimitrov, D. (2016). Medical Internet of Things and Big Data in Healthcare. *Healthcare Informatics Research*, 22(3), 156–163. <https://doi.org/10.4258/hir.2016.22.3.156>
- Elhonseny, M., Ramírez, G., Abu-Elnasr, O., Shawkat, S., Arunkumar, N. & Farouk, A. (2018). Modelo de transmisión segura de datos médicos para sistemas sanitarios basados en IoT. *IEEE Access*, 6 (2018), 20596-20608. <https://ieeexplore.ieee.org/document/8320774>
- España, M. (2023). *Optimización de dosis a pacientes en las nuevas tecnologías*. Sociedad Española de Radiología Hospitalaria. <https://sarh.es/files/IIJornadaPR/Ponencia-DosisNuevasTecnologias.pdf>
- Hernández, R., Fernández, C. & Baptista, P. (2014). *Metodología de la Investigación* (6° ed.). McGraw Hill. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf
- International Atomic Energy Agency (Dixit, A., 2010). *Dosis correcta para un diagnóstico preciso: seguimiento de las dosis de radiación administradas a los pacientes y utilización*

de los niveles de referencia para diagnósticos. IAEA.

<https://www.iaea.org/sites/default/files/5832021es.pdf>

Kamiya, K., Ozasa, K., Akiba, S., Niwa, O., Kodama, K., Takamura, N., Zaharieva, E., Kimura, Y., & Wakeford, R. (2015). *Long-term health effects of radiation exposure*. The Lancet.

[https://doi.org/10.1016/S0140-6736\(15\)61167-9](https://doi.org/10.1016/S0140-6736(15)61167-9)

Kutanzi, K., Lumen, A., Koturbash, I., & Miousse, I. (2016). Pediatric ionizing radiation exposures: Carcinogenic considerations. *International Journal of Environmental*

Research and Public Health, 13(11), 1057. <https://doi.org/10.3390/ijerph13111057>

Lal, R., Singh, R., Nishad, D., & Khalid, S. (2025). Enhancing security in electromagnetic radiation therapy using fuzzy graph theory. *Scientific Reports*, 15, 98110.

<https://doi.org/10.1038/s41598-025-98110-z>

Martínez, L., Castro, L., Posada, J., Corredor, Z., & San Juan, A. (2025). *Internet de las cosas (IoT) y los sistemas interconectados para mejorar la seguridad del paciente, a través de la monitorización continua y la automatización de alertas en tiempo real* (Diplomado de profundización). Universidad Nacional Abierta y a Distancia – UNAD.

<https://repository.unad.edu.co/jspui/bitstream/10596/68866/1/ldmartinezmap.pdf>

Marques, M., Delgado, V., Januário, F., Lopes, C., Jardim, R., & Agostinho, C. (2025). The B-Health Box: A Standards-Based Fog IoT Gateway for Interoperable Health and Wellbeing Data Collection. *Sensors* 25(23). <https://doi.org/10.3390/s25237116>

Molina, D. (2023). *Vigilancia radiológica de la exposición ocupacional a fuentes externas de radiación en Cuba*. Universidad de La Habana.

https://accesoabierto.uh.cu/files/original/2131725/Daniel_Molina_Perez.pdf

- Najjar, R. (2023). *Radiology's Ionising Radiation Paradox: Weighing the Indispensable Against the Detrimental in Medical Imaging*. *Cureus*, 15(7), e41623.
<https://doi.org/10.7759/cureus.41623>
- Paz, A., Acosta, D., Guancha, L., Cabrera, L., & Pejendino, M. (2025). *Falta de monitoreo en tiempo real de la dosis de radiación acumulada en pacientes durante procedimientos radiológicos* (Diplomado de profundización). Universidad Nacional Abierta y a Distancia – UNAD.
<https://repository.unad.edu.co/bitstream/handle/10596/68487/acpazb.pdf?sequence=3&isAllowed=y>
- Pesantes, N., & Rodríguez, C. (2024). *Diseño e implementación de un prototipo para el control y monitoreo mediante IoT de la cadena de frío en la transportación de medicamentos* (Trabajo de titulación). Universidad Politécnica Salesiana Sede Guayaquil.
<https://dspace.ups.edu.ec/bitstream/123456789/29091/1/UPS-GT005783.pdf>,
- Quiroz, A., Acosta, G., & Torres, R. (2021). Diseño de un sistema Internet de las cosas (IoT) para el monitoreo de la presión arterial. *Revista EIA*, 18(35), 1–15.
<https://doi.org/10.24050/reia.v18i35.1474>
- Ramírez D, Ramos V, Navarro S, Montealegre A, & Arciniegas J. (2023). Dosis de radiación por radiografías y factores asociados en neonatos de la Unidad de Recién Nacidos del Hospital Universitario San Ignacio, Bogotá, Colombia. *Biomédica*, 43(3):343-51.
<https://revistabiomedica.org/index.php/biomedica/article/view/6668>
- Resolución 482 de 2018. (2018). *Por la cual se establecen disposiciones para la protección radiológica en Colombia*. Ministerio de Salud y Protección Social.
https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%20482%20de%202018.pdf

- Rubio, A., Sánchez, F., Pérez, G., Plasencia, J., Buades, M., & García, J. (2022). *Un programa de red regional para la estandarización y control de radiación para diagnóstico médico no garantiza la armonización de dosis entre instituciones*. [Presentación en congreso]. 35 Congreso Nacional de la Sociedad Española de Radiología Médica (SERAM), edición virtual. PIPER-SERAM. <https://piper.espacio-seram.com/index.php/seram/article/download/3727/2193>
- Saifullah, M., Bajwa, I., Ibrahim, M., & Asghar, M. (2022). *IoT-enabled intelligent system for the radiation monitoring and warning approach*. Wiley Online Library. <https://doi.org/10.1155/2022/2769958>
- Shafique, K., Khawaja, B., Sabir, F., Qazi, S., & Mustaqim, M. (2020). *Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios*. <https://doi.org/10.1109/ACCESS.2020.2970118>
- Tirado, K. (2025). *Implementación de un sistema para el monitoreo de parámetros ambientales en tiempo real, basado en IoT y LoRaWAN en una plataforma Cloud*. (Trabajo de titulación). <http://dspace.unach.edu.ec/bitstream/51000/15704/1/Tirado%20R.%2C%20Karen%20A.%20%282025%29.pdf>
- Venkatesh, A. (2018). *IoT connected medical devices promise a better tomorrow*. <https://www.biospectrumasia.com/analysis/27/10292/IoT-connected-medical-devices-promise-a-better-tomorrow.html>
- Vera, O. (2024). *IA y radiología: Una nueva era de precisión y eficacia*. Ultralytics. <https://www.ultralytics.com/es/blog/ai-and-radiology-a-new-era-of-precision-and-efficiency>

Wilches, J., Castillo, M., & Hernández, A. (2023). Apps para estimar dosis de radiación en radiología médica y dental: Una revisión descriptiva. *Ingeniería y Competitividad*, 25(2), 78–92. <https://doi.org/10.25100/iyc.v25i2.12554>

Vorisek, C. N., Lehne, M., Klopfenstein, S., Mayer, P., Bartschke, A., Haese, T., & Thun, S. (2023). *Fast Healthcare Interoperability Resources (FHIR) for interoperability in health research: Systematic review*. *Journal of Medical Internet Research*, 25, e35724. <https://doi.org/10.2196/35724>

Zárate, M. (2023). *Monitoreo en tiempo real de dosis de radiación: Análisis y perspectivas*. ResearchGate. <https://www.researchgate.net/publication/280490619>