Ciberseguridad en dispositivos médicos conectados y su impacto en la seguridad del paciente

Cybersecurity in connected medical devices and its impact on patient safety

Carlos Alberto Rodríguez Sánchez[1], Nayibe Tatiana Sánchez Álvarez[2], Ingris Johana Hernández Martínez[3], Betsy Josefina Rodríguez Rivera[4], Carlos Andrés del Valle Pallares[5]

Universidad xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Cómo citar: xxxxxxxxxxxxxxxxxxxx

que conformaron el corpus del análisis bibliométrico de coocurrencia con VOSviewer. De ellos, tras el cribado por pares, la aplicación de los criterios de inclusión y exclusión y la evaluación de calidad, se seleccionaron 31 documentos para la síntesis cualitativa. Se identificaron vulnerabilidades relacionadas con protocolos de comunicación inseguros, autenticación débil y falta de actualizaciones de seguridad, con riesgos directos para la seguridad del paciente. El análisis bibliométrico evidenció tres clústeres temáticos: seguridad informática, seguridad del paciente y telemedicina e interoperabilidad. Se concluye que es necesario incorporar mecanismos de seguridad desde el diseño de los dispositivos médicos, fortalecer los marcos regulatorios y promover enfoques interdisciplinarios entre la ingeniería biomédica, la ciberseguridad y la gestión hospitalaria.

Palabras clave: seguridad informática; seguridad del paciente; telemedicina; equipos y suministros.

Abstract

The rise of the Internet of Medical Things (IoMT) has produced connected medical devices that enable remote monitoring and timely diagnosis, but it also introduces vulnerabilities that threaten patient safety and the integrity of clinical information. The aim of this study was to analyze the current state of cybersecurity in connected medical devices and its impact on patient safety. A narrative review of the scientific literature, complemented by a bibliometric analysis, was conducted in the PubMed and ScienceDirect databases using the DeCS/MeSH descriptors Computer Security, Patient Safety, Telemedicine and Equipment and Supplies, covering the 2016-2026 period and studies published in English and Spanish. The search retrieved 292 records (2 from PubMed and 290 from ScienceDirect), which formed the corpus for the keyword co-occurrence analysis performed with VOSviewer; from these, after peer screening, application of the inclusion and exclusion criteria and quality appraisal, 31 documents were selected for the qualitative synthesis. Vulnerabilities related to insecure communication protocols, weak authentication and lack of security updates were identified, with direct risks to patient safety, and the bibliometric analysis revealed three thematic clusters: computer security, patient safety, and telemedicine and interoperability. It is concluded that security mechanisms must be incorporated from the design stage of medical devices, regulatory frameworks must be strengthened, and interdisciplinary approaches integrating biomedical engineering, cybersecurity and hospital management must be promoted.

Keywords: computer Security; patient safety; telemedicine; equipment and supplies.

Introducción

La transformación digital del sector salud ha impulsado la incorporación de tecnologías inteligentes en los procesos de atención sanitaria y ha favorecido modelos de atención más eficientes y personalizados. En este contexto, los dispositivos médicos conectados han adquirido un papel relevante, pues permiten la recopilación, la transmisión y el análisis de datos clínicos en tiempo real. Estos sistemas incluyen marcapasos inteligentes, bombas de insulina, monitores cardíacos, sistemas de telemetría hospitalaria y dispositivos para el monitoreo remoto de pacientes (Andreadis *et al.*, 2024; Juhra, 2023).

El desarrollo y la integración de estas tecnologías han dado lugar al concepto de IoMT, que integra dispositivos biomédicos, redes de comunicación y plataformas de análisis de datos con el propósito de mejorar la calidad de la atención médica. Sin embargo, el aumento de la conectividad también ha ampliado la superficie de ataque de los sistemas de salud. Diversos estudios han demostrado que muchos dispositivos médicos presentan vulnerabilidades relacionadas con mecanismos de autenticación débiles, ausencia de cifrado en las comunicaciones y limitaciones en los procesos de actualización segura. Los actores maliciosos pueden aprovechar estas deficiencias para manipular el funcionamiento de los dispositivos, obtener acceso no

autorizado a información clínica sensible o interrumpir servicios críticos (Mbunge *et al.*, 2021; Sun *et al.*, 2019; Yaqoob *et al.*, 2019).

Por ello, la ciberseguridad de los dispositivos médicos conectados constituye un aspecto fundamental para proteger la seguridad del paciente, garantizar la continuidad de los servicios de salud y preservar la confidencialidad, la integridad y la disponibilidad de los datos médicos (Kruse *et al.*, 2017; Li *et al.*, 2025). El objetivo de este artículo es revisar el estado del arte sobre la ciberseguridad en dispositivos médicos conectados y analizar su impacto en la seguridad del paciente mediante una revisión narrativa de la literatura, complementada con un análisis bibliométrico de coocurrencia de palabras clave.

Método

Este estudio corresponde a una revisión narrativa de la literatura científica, complementada con un análisis bibliométrico de coocurrencia de palabras clave y centrada en investigaciones relacionadas con la ciberseguridad en dispositivos médicos conectados. Por tratarse de una revisión narrativa, no se siguió formalmente la declaración PRISMA 2020. No obstante, con el fin de favorecer la transparencia y la reproducibilidad del estudio, a continuación se describen la estrategia de búsqueda, los criterios de selección, el proceso de cribado, la evaluación de la calidad y los parámetros del análisis bibliométrico.

Fuentes de información y estrategia de búsqueda

La búsqueda se desarrolló en las bases de datos PubMed y ScienceDirect. Se emplearon los descriptores DeCS/MeSH *Computer Security*, *Patient Safety*, *Telemedicine* y *Equipment and Supplies* (en español: seguridad informática, seguridad del paciente, telemedicina y equipos y suministros), combinados mediante operadores booleanos. Las cadenas de búsqueda empleadas en cada base de datos fueron las siguientes:

PubMed: ("Computer Security"[MeSH Terms]) AND ("Patient Safety"[MeSH Terms]) AND ("Telemedicine"[MeSH Terms]) AND ("Equipment and Supplies"[MeSH Terms]); filtros: fecha de publicación 2016-2026; idiomas inglés y español.

ScienceDirect: ("computer security" OR "cybersecurity") AND ("patient safety") AND ("telemedicine" OR "medical devices" OR "equipment and supplies"), aplicada en los campos de título, resumen y palabras clave (*Title, abstract, keywords*); filtros: años, 2016-2026; tipo de documento, artículos de revisión y artículos de investigación.

Justificación de la diferencia en el número de registros por base de datos

La diferencia entre los registros recuperados en PubMed (2) y en ScienceDirect (290) obedece principalmente a la naturaleza de cada motor de búsqueda. En PubMed, la búsqueda se centró en los términos MeSH asignados por los indizadores. La intersección simultánea de los cuatro descriptores mediante el operador AND resulta altamente restrictiva, puesto que pocos documentos se encuentran indizados a la vez con los cuatro encabezamientos. En contraste, ScienceDirect no emplea un vocabulario controlado, por lo que la búsqueda se efectuó en texto libre en el título, el resumen y las palabras clave, lo que amplía la recuperación.

Además, ScienceDirect indiza un volumen considerable de revistas de ingeniería, informática y ciencias aplicadas, áreas en las que se concentra buena parte de la producción sobre ciberseguridad del IoMT, mientras que PubMed se orienta principalmente a la literatura biomédica. Esta asimetría se reconoce como una limitación del estudio.

Criterios de inclusión y exclusión

Se incluyeron documentos que cumplieran simultáneamente con los siguientes criterios: a) publicación entre 2016 y 2026; b) redacción en inglés o español; c) artículos de revisión, revisiones sistemáticas, metaanálisis o estudios originales publicados en revistas o actas de congresos con revisión por pares; d) abordaje explícito de la seguridad de los dispositivos médicos conectados, los ciberataques a sistemas de salud o la ciberseguridad en el IoMT, en relación con la seguridad del paciente o la protección de la información clínica, y e) acceso al texto completo. Se excluyeron: a) editoriales, cartas, notas periodísticas, artículos de opinión y literatura gris sin revisión por pares; b) registros duplicados; c) documentos centrados en el internet de las cosas en contextos ajenos al sector salud y d) documentos con información metodológica insuficiente para el análisis.

Proceso de cribado por pares

La selección se desarrolló en tres etapas: 1) eliminación de registros duplicados; 2) cribado por título y resumen y 3) lectura del texto completo para verificar la elegibilidad. Dos autores desarrollaron de manera independiente las etapas 2 y 3 y resolvieron las discrepancias por consenso o, cuando fue necesario, mediante la participación de un tercer autor. Como resultado de este proceso, se seleccionaron 31 documentos para la síntesis cualitativa.

Evaluación de la calidad metodológica

La calidad de los documentos seleccionados se valoró mediante una lista de verificación elaborada para este estudio, compuesta por cinco criterios: a) publicación en una fuente con revisión por pares; b) claridad del objetivo o de la pregunta de investigación; c) descripción suficiente del método empleado; d) coherencia entre los resultados y las conclusiones y e) pertinencia respecto al objetivo de esta revisión. Cada criterio se calificó como cumple (1) o no cumple (0). Se incluyeron en la síntesis los documentos con una puntuación igual o superior a 3 sobre 5.

Extracción y síntesis de la información

Se analizaron los 31 documentos seleccionados con el propósito de identificar los tipos de dispositivos más vulnerables, las amenazas y los ataques reportados, los impactos sobre la seguridad del paciente y las estrategias de mitigación propuestas en la literatura. La información se organizó por categorías temáticas y se sintetizó de forma narrativa, lo que permitió identificar los principales avances, tendencias y desafíos asociados con la protección de los dispositivos médicos conectados.

Análisis bibliométrico

El análisis bibliométrico se efectuó con el programa VOSviewer (versión [completar]) sobre el conjunto total de 292 registros exportados desde ambas bases de datos. Se aplicó un análisis de coocurrencia (*co-occurrence*) con la unidad de análisis "todas las palabras clave" (*all keywords*) y el método de conteo completo (*full counting*). Se estableció un umbral mínimo de [completar] ocurrencias por término, lo que dio como resultado 24 términos incluidos en la red.

Previamente, se depuraron los términos mediante un archivo de tesauro (*thesaurus file*), que permitió unificar sinónimos, variantes ortográficas, formas singulares y plurales y acrónimos (por ejemplo, "IoMT" e "Internet of Medical Things", o "cybersecurity" y "computer security"), así como excluir términos genéricos sin valor analítico (por ejemplo, "study" o "review"). En la visualización se consideraron los enlaces con un peso igual o superior a 2. La agrupación en clústeres se efectuó mediante el algoritmo de modularidad de VOSviewer con el parámetro de resolución predeterminado (1.0). Se elaboraron dos mapas de coocurrencia: uno con los registros de PubMed (figura 1) y otro con los de ScienceDirect (figura 2).

Diferencia entre el corpus bibliométrico y el corpus cualitativo

Es importante precisar que los 292 registros recuperados se emplearon exclusivamente para el mapeo general de la producción científica mediante VOSviewer, mientras que la revisión cualitativa detallada, "Vulnerabilidades identificadas en dispositivos médicos conectados", se fundamentó en los 31 documentos seleccionados tras el cribado y la evaluación de calidad.

Resultados

A partir del proceso de búsqueda bibliográfica, se recuperaron 292 registros (2 de PubMed y 290 de ScienceDirect), correspondientes al período 2016-2026, que conformaron el corpus del análisis bibliométrico. De este conjunto, tras el cribado, la aplicación de los criterios de inclusión y exclusión y la evaluación de calidad descritos en el método, se seleccionaron 31 documentos para la síntesis cualitativa, cuyos hallazgos se presentan más adelante.

Los 292 registros recuperados se importaron al programa VOSviewer con el propósito de desarrollar un análisis bibliométrico y visualizar las redes de coocurrencia de palabras clave (tabla 1).

Como se observa en la tabla 1, la mayoría de los registros proceden de la base de datos ScienceDirect (290 registros), mientras que PubMed aportó 2 registros, correspondientes a un período de publicación entre 2016 y 2026. Esta diferencia responde al carácter restrictivo de la búsqueda por descriptores MeSH en PubMed frente a la búsqueda en texto libre en ScienceDirect, tal como se explica en el método.

Tabla 1. Indicadores de la búsqueda bibliográfica

Indicador	Valor	Descripción
Total de registros	292	Suma de registros exportados de PubMed y ScienceDirect
Base de datos 1	2	PubMed
Base de datos 2	290	ScienceDirect
Período de publicación	2016-2026	Años de publicación presentes en el corpus
Fuentes únicas	156	Diferentes revistas o actas de congresos
Promedio de autores por documento	6.15	Media aritmética
Promedio de palabras clave por documento	5.85	Media aritmética
Documentos con resumen	290	Disponibilidad del resumen en el archivo exportado
Nodos de la red de coocurrencia	24	Palabras clave incluidas en la visualización
Enlaces de la red de coocurrencia	51	Coocurrencias con peso ≥ 2
Clústeres identificados	3	Comunidades identificadas mediante modularidad

Fuente: elaboración propia.

El corpus analizado incluye 156 fuentes únicas, con un promedio de 6.15 autores por documento y 5.85 palabras clave por publicación, lo que refleja un alto grado de colaboración científica y diversidad temática. Asimismo, el análisis bibliométrico permitió identificar 24 nodos y 51 enlaces en la red de coocurrencia de palabras clave, agrupados en tres clústeres principales. Estos resultados evidencian la existencia de comunidades temáticas bien definidas dentro de la investigación sobre ciberseguridad en dispositivos médicos conectados.

Vulnerabilidades identificadas en dispositivos médicos conectados

El análisis de los 31 documentos seleccionados permitió clasificar las vulnerabilidades más frecuentes de los dispositivos médicos conectados en cuatro categorías principales, según el origen y el impacto potencial sobre la seguridad del paciente y la integridad de los sistemas de salud.

Vulnerabilidades en la comunicación de datos

Diversos estudios han demostrado que algunos dispositivos médicos transmiten información clínica mediante protocolos de comunicación que carecen de mecanismos adecuados de cifrado o protección de datos. Esta situación incrementa el riesgo de interceptación, manipulación o acceso no autorizado a la información transmitida y compromete la confidencialidad y la integridad de los datos clínicos. Estas vulnerabilidades son especialmente críticas en entornos que emplean tecnologías inalámbricas, como wifi o Bluetooth, o redes hospitalarias, donde terceros pueden capturar o alterar fácilmente la información si no se implementan controles de seguridad robustos (Ghubaish *et al.*, 2021; Haleem *et al.*, 2021; Matha *et al.*, 2025).

Autenticación débil

Otra vulnerabilidad recurrente identificada en la literatura corresponde a la implementación de mecanismos de autenticación insuficientes en los dispositivos médicos conectados. Entre las prácticas más comunes se encuentran el uso de contraseñas predeterminadas, las credenciales compartidas y la ausencia de mecanismos de autenticación multifactor. Estas debilidades pueden permitir que actores maliciosos accedan a los dispositivos o a las redes hospitalarias en las que estos se integran. El fácil acceso compromete el funcionamiento de los dispositivos y las redes, la integridad de los datos clínicos y, en consecuencia, la seguridad del paciente (Knop *et al.*, 2021).

Falta de actualizaciones de seguridad

Asimismo, se identificó que numerosos dispositivos médicos presentan limitaciones en los mecanismos de actualización de programas o *firmware*, lo que dificulta la corrección oportuna de las vulnerabilidades detectadas. En muchos casos, la ausencia de actualizaciones remotas seguras o la dependencia de intervenciones manuales prolongan la exposición de los sistemas a posibles ciberataques (Burns *et al.*, 2016; Parihar *et al.*, 2024).

Riesgos para la seguridad del paciente

Las vulnerabilidades identificadas en los dispositivos médicos conectados pueden ocasionar consecuencias críticas en el entorno clínico, entre ellas, la alteración no autorizada de parámetros clínicos, la interrupción del funcionamiento de equipos médicos conectados, el acceso no autorizado a información médica sensible y la interrupción de servicios hospitalarios o sistemas clínicos (Abood *et al.*, 2025; Ghafur *et al.*, 2019). Estos riesgos pueden afectar directamente la calidad de la atención, comprometer la toma de decisiones clínicas y poner en riesgo la integridad física de los pacientes.

En consecuencia, estos riesgos demuestran que la ciberseguridad en los dispositivos médicos conectados no constituye únicamente un desafío tecnológico, sino también un problema crítico para la seguridad del paciente y la continuidad de la atención médica (Qureshi *et al.*, 2025).

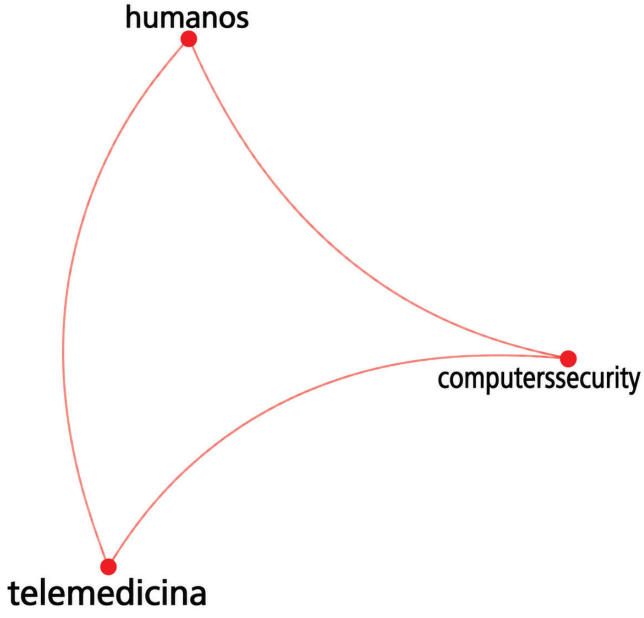
Un ejemplo representativo de estas preocupaciones se observa en los dispositivos cardíacos implantables conectados, que pueden presentar vulnerabilidades asociadas con el monitoreo remoto y el acceso a información clínica. Estas debilidades ponen de manifiesto la necesidad de integrar medidas regulatorias, técnicas y clínicas coordinadas para reducir los riesgos de ciberataques y proteger la seguridad de los pacientes (Baranchuk *et al.*, 2018; Beloualid *et al.*, 2026; Slotwiner *et al.*, 2018).

Análisis bibliométrico y de coocurrencia mediante VOSviewer

Con el propósito de identificar las relaciones temáticas entre los conceptos analizados en la literatura, se efectuó un análisis de coocurrencia de términos mediante el programa VOSviewer. Para este análisis se tomaron como base los descriptores DeCS/MeSH utilizados en la búsqueda bibliográfica en PubMed, específicamente *Computer Security, Patient Safety, Telemedicine* y *Equipment and Supplies*.

La búsqueda en PubMed, mediante estos descriptores, produjo dos resultados relevantes, que se utilizaron para elaborar un mapa de coocurrencia de términos. Este mapa permitió visualizar las relaciones conceptuales y la interrelación temática entre los principales ejes asociados con la ciberseguridad en dispositivos médicos conectados. Además, facilitó la identificación de patrones y áreas de convergencia dentro del campo de estudio (figura 1).

Figura 1. Visualización de la coocurrencia de términos en PubMed sobre ciberseguridad en dispositivos médicos



Nota. La figura se realizó mediante VOSviewer. Fuente: elaboración propia.

A continuación, se presenta el análisis de coocurrencia de términos, que permitió identificar tres grupos principales (clústeres) que representan áreas temáticas diferenciadas, pero interrelacionadas, dentro de la investigación sobre ciberseguridad en dispositivos médicos conectados:

Clúster 1: Seguridad informática y sistemas médicos conectados

Este grupo reúne términos relacionados con la *seguridad informática,* el *internet de las cosas (IoT)*, las *redes de comunicación informática*, el *diseño de programas* y la *integración de sistemas*. Estos términos evidencian la estrecha relación entre la seguridad informática y la infraestructura tecnológica que sustenta los dispositivos médicos conectados. Este clúster refleja el enfoque tecnológico predominante en la investigación, centrado en el diseño, la integración y la protección de sistemas clínicos interoperables y plataformas de IoMT (Hernandez-Jaimes *et al.*, 2023).

Clúster 2: Seguridad del paciente y dispositivos médicos

El segundo clúster comprende términos como *seguridad del paciente*, *seguridad de los equipos*, *equipos y suministros y monitoreo*, que ponen de manifiesto la relación directa entre la seguridad tecnológica de los dispositivos médicos y la protección de los pacientes en los entornos clínicos. Este grupo destaca que las vulnerabilidades presentes en los dispositivos médicos conectados pueden tener un impacto inmediato en la calidad, la continuidad y la seguridad de la atención sanitaria (Rowan, 2024).

Clúster 3: Telemedicina e interoperabilidad de los sistemas de salud

El tercer clúster se relaciona con términos como *telemedicina*, *interoperabilidad de la* i*nformación en* s*alud* e *interfaz usuario-computador*, que reflejan el crecimiento de los sistemas remotos y la integración de dispositivos médicos en las plataformas digitales de atención sanitaria. También incorpora aspectos relacionados con la seguridad, la privacidad y la confidencialidad de la información clínica, así como el uso de enfoques de inteligencia artificial y de interacción humano-computador para mejorar la experiencia del usuario y el análisis de datos clínicos en contextos de atención remota (Ndlovu *et al.*, 2023).

Interpretación de los resultados bibliométricos

El análisis de coocurrencia realizado mediante el programa VOSviewer muestra que la investigación sobre ciberseguridad en dispositivos médicos se estructura principalmente en torno a tres ejes temáticos interrelacionados: la infraestructura tecnológica y la seguridad informática; la seguridad del paciente y la confiabilidad de los dispositivos médicos y la telemedicina y la interoperabilidad de los sistemas clínicos (Hariyani *et al.*, 2025; Ni *et al.*, 2025).

Estos resultados confirman que la ciberseguridad en dispositivos médicos constituye un campo interdisciplinario en el que convergen áreas como la informática médica, la ingeniería biomédica, la seguridad informática y la gestión de la seguridad del paciente. La interrelación entre estos dominios pone de manifiesto la necesidad de desarrollar estrategias colaborativas para el diseño, la implementación y la gestión segura de las tecnologías médicas conectadas (figura 2).

Discusión

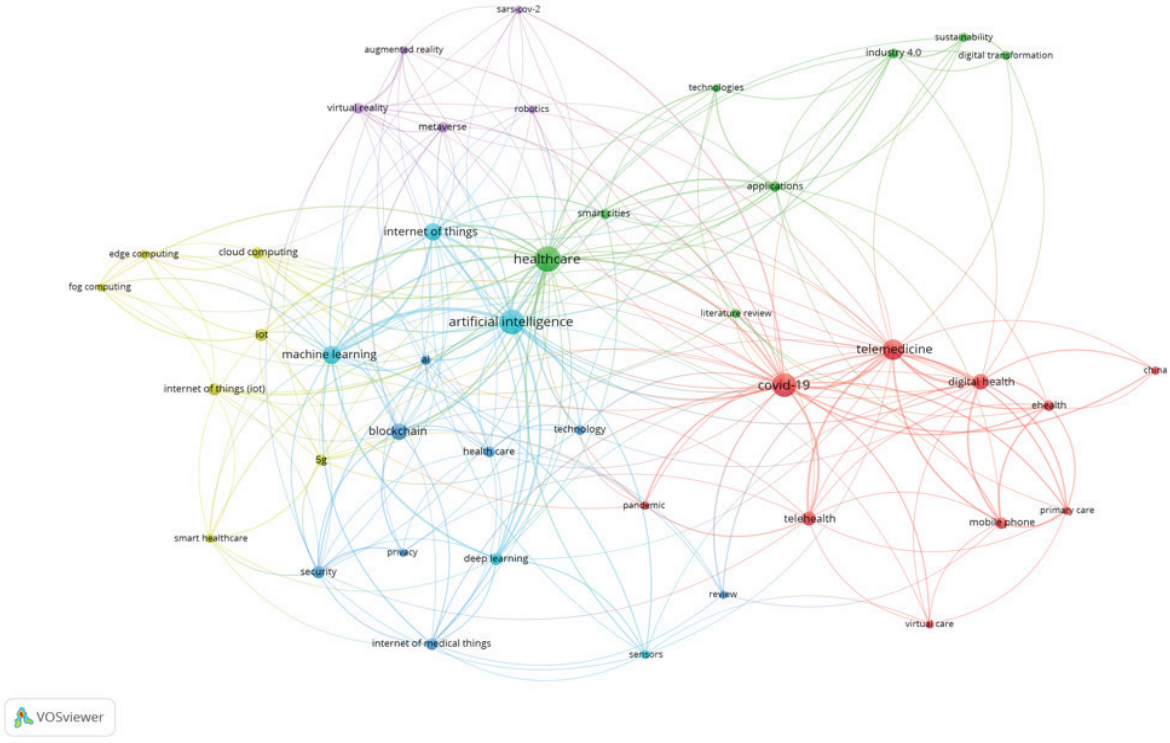
Los resultados obtenidos en este estudio concuerdan con la literatura científica reciente que analiza la creciente exposición de los sistemas de salud y de los dispositivos médicos conectados a riesgos de ciberseguridad. La integración del IoMT ha incrementado significativamente la superficie de ataque en los entornos hospitalarios debido a la interconexión de dispositivos médicos, sensores y sistemas de información clínica (Ahmad *et al.*, 2026).

Asimismo, la literatura identifica vulnerabilidades relacionadas con protocolos de comunicación inseguros, debilidades en los mecanismos de autenticación y limitaciones en la gestión de actualizaciones de seguridad, que coinciden con las identificadas en este estudio (Mejía-Granda *et al.*, 2024). Dispositivos como bombas de infusión, sistemas de monitoreo y equipos implantables pueden convertirse en puntos de entrada para ciberataques cuando no cuentan con mecanismos de seguridad robustos (Iyanda *et al.*, 2023).

Los resultados también coinciden con investigaciones que advierten sobre los riesgos para la seguridad del paciente, debido a que las vulnerabilidades en los sistemas digitales de salud pueden ocasionar la

alteración de parámetros en dispositivos médicos, la interrupción de servicios hospitalarios y la exposición de datos clínicos sensibles (Coventry y Branley, 2018). De igual manera, los ciberataques pueden afectar la disponibilidad de los sistemas clínicos, alterar registros médicos y ocasionar errores en la toma de decisiones médicas (Argaw *et al.*, 2020; Jahangir *et al.*, 2025; Jalali y Kaiser, 2018).

Figura 2. Mapa de coocurrencia de palabras clave sobre ciberseguridad en dispositivos médicos en la base de datos ScienceDirect



Nota. La figura se realizó mediante VOSviewer. **Fuente:** elaboración propia.

Limitaciones del estudio

Este estudio presenta algunas limitaciones que deben considerarse al interpretar los resultados. En primer lugar, al tratarse de una revisión narrativa, la selección de los documentos no tiene el carácter exhaustivo de una revisión sistemática y puede estar expuesta a sesgos de selección, aunque se procuró reducirlos mediante el cribado por pares y una evaluación explícita de la calidad. En segundo lugar, la búsqueda se limitó a dos bases de datos, por lo que pudieron quedar excluidos estudios relevantes indexados en fuentes como Scopus, Web of Science, IEEE Xplore o ACM Digital Library, de especial importancia en las áreas de ingeniería y ciberseguridad.

En tercer lugar, la marcada asimetría en el número de registros entre PubMed (2) y ScienceDirect (290) implica que el mapa bibliométrico refleja principalmente la producción indexada en ScienceDirect, lo que puede introducir un sesgo editorial. Asimismo, la restricción a publicaciones en inglés y español, la inclusión de 2026 como año aún en curso al momento de la búsqueda y la dependencia del análisis de coocurrencia respecto de las palabras clave asignadas por autores e indizadores, así como de las decisiones de limpieza de términos, pueden haber influido en los resultados. Finalmente, la evaluación de la calidad se efectuó con una lista de verificación propia y no con un instrumento validado, y no se efectuó una síntesis cuantitativa (metaanálisis) de la frecuencia o el impacto de los incidentes de ciberseguridad.

Líneas futuras de investigación

A partir de los hallazgos y las limitaciones identificados, se proponen las siguientes líneas futuras de investigación: a) desarrollar revisiones sistemáticas conforme a la declaración PRISMA 2020 que amplíen la búsqueda a bases de datos multidisciplinarias y técnicas e incorporen literatura gris de agencias reguladoras y de ciberseguridad; b) realizar estudios empíricos sobre la incidencia y las consecuencias clínicas de los ciberataques en instituciones de salud de América Latina y, en particular, de Colombia, donde la evidencia es aún escasa; c) evaluar la efectividad de los enfoques de seguridad desde el diseño y de los marcos regulatorios aplicables a los dispositivos médicos conectados a lo largo del ciclo de vida; d) investigar mecanismos de cifrado y autenticación ligeros adecuados para dispositivos con recursos computacionales limitados, así como sistemas de detección de intrusiones basados en inteligencia artificial (Hernandez-Jaimes *et al.*, 2023) y aplicaciones de la tecnología de cadena de bloques para la trazabilidad y la integridad de los datos clínicos (Ni *et al.*, 2025) y e) analizar el papel de los factores humanos y de la capacitación del personal sanitario en la prevención de incidentes de ciberseguridad.

Conclusiones

La ciberseguridad en los dispositivos médicos conectados constituye un problema estructural que requiere estrategias integrales y coordinadas entre fabricantes, instituciones de salud y organismos reguladores.

La creciente digitalización del sector de la salud, junto con la adopción de tecnologías como la telemedicina, las historias clínicas electrónicas y los dispositivos IoT, incrementa la dependencia de las infraestructuras digitales y los riesgos asociados a la seguridad de estas.

Por tanto, es necesario fortalecer los mecanismos de seguridad, los marcos regulatorios, las políticas institucionales de ciberseguridad y la capacitación del personal sanitario para mitigar los riesgos y proteger la seguridad del paciente y la continuidad de los servicios de salud.

Contribución de los autores. Búsqueda de información: Carlos Alberto Rodríguez Sánchez, Nayibe Tatiana Sánchez Álvarez y Carlos Andrés del Valle Pallares; análisis de la información: Carlos Alberto Rodríguez Sánchez, Nayibe Tatiana Sánchez Álvarez y Carlos Andrés del Valle Pallares; redacción del borrador original: Carlos Alberto Rodríguez Sánchez, Nayibe Tatiana Sánchez Álvarez y Carlos Andrés del Valle Pallares; adaptación al formato de la revista: Nayibe Tatiana Sánchez Álvarez e Ingris Johana Hernández Martínez. Todos los autores han leído y aceptado la versión publicada del manuscrito.

Declaración de disponibilidad de datos. Los registros analizados proceden de las bases de datos PubMed y ScienceDirect, de acuerdo con la estrategia de búsqueda descrita en el método.

Conflictos de intereses. Los autores declaran no tener conflictos de intereses.

Financiamiento. Esta investigación no recibió financiamiento externo.

Aspectos éticos. No aplicable. El estudio corresponde a una revisión de la literatura y no involucró seres humanos ni animales.

Consentimiento informado. No aplicable.

Declaración de uso de inteligencia artificial generativa (GenAI). No aplicable.

Referencias

Abood, E. W., Yassin, A. A., Abduljabbar, Z. A., Nyangaresi, V. O., Abduljaleel, I. Q., Aldarwish, A. J. Y., & Neamah, H. A. (2025). Security Challenges and Analysis Tools in Internet of Health Things: A Comprehensive Review. *Computers, Materials & Continua*, *85*(2), 2305-2345. https://doi.org/10.32604/cmc.2025.066579

Ahmad, S., Ahmed, A., Alturki, N., Hussain, S., & Abdullah, S. (2026). A formal approach towards IoT-enabled mechanism for digital polio system using Colured Petri Net. *Egyptian Informatics Journal*, *33*, 100894. https://doi.org/10.1016/j.eij.2026.100894

Andreadis, K., Muellers, K. A., Lin, J. J., Mkuu, R., Horowitz, C. R., Kaushal, R., & Ancker, J. S. (2024). Navigating Privacy and Security in Telemedicine for Primary Care. *The American Journal of Managed Care*, *30*(Spec. No. 6), SP459-SP463. https://doi.org/10.37765/ajmc.2024.89553

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D., & Lakkireddy, D. R. (2018). Cybersecurity for Cardiac Implantable Electronic Devices. *Journal of the American College of Cardiology*, *71*(11), 1284-1288. https://doi.org/10.1016/j.jacc.2018.01.023

Beloualid, S., Morino, I., Bajit, A., Benzzine, H., Sahl, S., & Essamri, H. (2026). Autonomous robotics computer-vision based framework for intelligent remote patient monitoring in health care. *Results in Engineering*, *29*, 109397. https://doi.org/10.1016/j.rineng.2026.109397

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66-72. https://doi.org/10.1145/2890488

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digital Medicine*, *2*(1), 98. https://doi.org/10.1038/s41746-019-0161-6

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet of Things Journal*, *8*(11), 8707-8718. https://doi.org/10.1109/JIOT.2020.3045653

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors International*, *2*, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Hariyani, D., Hariyani, P., Mishra, S., & Sharma, M. K. (2025). A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices. *Green Technologies and Sustainability*, *3*(3), 100169. https://doi.org/10.1016/j.grets.2025.100169

Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*, *23*, 100887. https://doi.org/10.1016/j.iot.2023.100887

Iyanda, C., Ogunwola, T., & Olalekan, Z. (2023). Cybersecurity Challenges in the Age of IoT: Safeguarding Quality and Compliance in Connected Medical Devices. *IARJSET*, *10*(10). https://doi.org/10.17148/IARJSET.2023.101003

Jahangir, Haleem, A., Javaid, M., & Jami, A. R. (2025). Understanding the causal relationships among healthcare technologies when enabled through IoT: Analysing through the MCDM Approach. *Intelligent Hospital*, *1*(2), 100028. https://doi.org/10.1016/j.inhs.2025.100028

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059

Juhra, C. (2023). Telemedizin. *Die Orthopädie*, *52*(7), 560-566. https://doi.org/10.1007/s00132-023-04396-0

Knop, M., Mueller, M., & Niehaves, B. (2021). Investigating the Use of Telemedicine for Digitally Mediated Delegation in Team-Based Primary Care: Mixed Methods Study. *Journal of Medical Internet Research*, *23*(8), e28151. https://doi.org/10.2196/28151

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263

Li, P., Fan, J., & Wu, J. (2025). Exploring the key technologies and applications of 6G wireless communication network. *iScience*, *28*(5), 112281. https://doi.org/10.1016/j.isci.2025.112281

Matha, R., Mukherjee, S., Panigrahi, R. R., & Shrivastava, A. K. (2025). A bibliometric analysis of industry 5.0 and healthcare supply chain research: Emerging opportunities and future challenges. *Supply Chain Analytics*, *10*, 100125. https://doi.org/10.1016/j.sca.2025.100125

Mbunge, E., Muchemwa, B., Jiyane, S., & Batani, J. (2021). Sensors and healthcare 5.0: Transformative shift in virtual care through emerging digital health technologies. *Global Health Journal*, *5*(4), 169-177. https://doi.org/10.1016/j.glohj.2021.11.008

Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo-de-Gea, J. M., & García-Berná, J. A. (2024). Security vulnerabilities in healthcare: An analysis of medical devices and software. *Medical & Biological Engineering & Computing*, *62*(1), 257-273. https://doi.org/10.1007/s11517-023-02912-0

Ndlovu, K., Mars, M., & Scott, R. E. (2023). Validation of an Interoperability Framework for Linking mHealth Apps to Electronic Record Systems in Botswana: Expert Survey Study. *JMIR Formative Research*, *7*, e41225. https://doi.org/10.2196/41225

Ni, E., Tang, X., Zhou, X., Lee, D., Elhussein, A., Knight, E., Gürsoy, G., & Gerstein, M. (2025). Recent advances and future prospects for blockchain in biomedicine. *Cell Reports Methods*, *5*(8), 101114. https://doi.org/10.1016/j.crmeth.2025.101114

Parihar, A., Prajapati, J. B., Prajapati, B. G., Trambadiya, B., Thakkar, A., & Engineer, P. (2024). Role of IOT in healthcare: Applications, security & privacy concerns. *Intelligent Pharmacy*, *2*(5), 707-714. https://doi.org/10.1016/j.ipha.2024.01.003

Qureshi, S. S., He, J., Zhu, N., Nazir, A., Fang, J., Ma, X., Wajahat, A., Ullah, F., Qureshi, S., Dhelim, S., & Pathan, M. S. (2025).

Enhancing IoT security and healthcare data protection in the metaverse: A Dynamic Adaptive Security Mechanism. *Egyptian Informatics Journal*, *30*, 100670. https://doi.org/10.1016/j.eij.2025.100670

Rowan, N. J. (2024). Digital technologies to unlock safe and sustainable opportunities for medical device and healthcare sectors with a focus on the combined use of digital twin and extended reality applications: A review. *Science of The Total Environment*, *926*, 171672. https://doi.org/10.1016/j.scitotenv.2024.171672

Slotwiner, D. J., Deering, T. F., Fu, K., Russo, A. M., Walsh, M. N., & Van Hare, G. F. (2018). Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit. *Heart Rhythm*, *15*(7), e61-e67. https://doi.org/10.1016/j.hrthm.2018.05.001

Sun, Y., Lo, F. P.-W., & Lo, B. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access*, *7*, 183339-183355. https://doi.org/10.1109/ACCESS.2019.2960617

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Communications Surveys & Tutorials*, *21*(4), 3723-3768. https://doi.org/10.1109/COMST.2019.2914094