Análisis de los estándares internacionales de ciberseguridad para dispositivos médicos establecidos por la FDA, ISO e IEC

Julián Andrés Gonzáles Valencia

Diana María Posada Builes

Valentina Ramírez Taborda

Asesor

Edna Rocío Jamaica Guio

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias de la Salud - ECISA

Tecnología en Radiología e Imágenes Diagnosticas

2026

Resumen

En el contexto de la creciente digitalización del sector salud y el aumento en el uso de dispositivos médicos conectados, se ha generado una transición progresiva de recomendaciones voluntarias hacia requisitos técnicos obligatorios en materia de ciberseguridad. Este cambio ha sido impulsado por la necesidad de garantizar la protección de los datos clínicos y la integridad de los sistemas sanitarios frente a un entorno digital cada vez más complejo.

El problema radica en la evolución de las amenazas cibernéticas, las cuales han dejado de ser consideradas únicamente fallos técnicos para convertirse en riesgos directos para la seguridad del paciente, debido a la posibilidad de afectar el funcionamiento de dispositivos médicos, alterar información clínica y comprometer procesos de diagnóstico y tratamiento.

Desde el punto de vista metodológico, la investigación se desarrolla bajo un enfoque cualitativo, mediante una revisión documental de tipo descriptivo, basada en el análisis de normas internacionales, artículos científicos y documentos técnicos publicados en la última década. Para el tratamiento de la información se emplea el análisis de contenido, permitiendo identificar patrones, cambios regulatorios y tendencias relevantes.

El propósito del estudio es analizar la evolución de los estándares internacionales de ciberseguridad aplicados a dispositivos médicos, con el fin de identificar tendencias, avances y transformaciones en las políticas de protección de datos clínicos y sistemas de salud. Los resultados evidencian un fortalecimiento de los marcos regulatorios y una mayor incorporación de estrategias de gestión de riesgos, contribuyendo a mejorar la seguridad en el entorno sanitario.

Palabras Clave: ciberseguridad, dispositivos médicos, riesgos cibernéticos, seguridad del paciente, gestión de riesgo.

Abstract

In the context of the increasing digitalization of the healthcare sector and the growing use of connected medical devices, a progressive transition from voluntary recommendations to mandatory technical requirements in cybersecurity has emerged. This shift has been driven by the need to ensure the protection of clinical data and the integrity of healthcare systems in an increasingly complex digital environment.

The problem lies in the evolution of cyber threats, which are no longer considered merely technical failures but direct risks to patient safety, as they can affect the functioning of medical devices, alter clinical information, and compromise diagnosis and treatment processes.

From a methodological perspective, this research follows a qualitative approach through a descriptive documentary review, based on the analysis of international standards, scientific articles, and technical documents published over the last decade. Content analysis is used to identify patterns, regulatory changes, and relevant trends.

The purpose of this study is to analyze the evolution of international cybersecurity standards applied to medical devices, to identify trends, advancements, and transformations in policies related to clinical data protection and healthcare systems. The findings reveal a strengthening of regulatory frameworks and the incorporation of risk management strategies, contributing to improved security in the healthcare environment.

Keywords: cybersecurity, medical devices, cyber risks, patient safety, risk management.

Tabla de Contenido

Lista de Tablas

Introducción

En la actualidad, el avance de la tecnología en el sector de la salud ha permitido el desarrollo de sistemas médicos, especialmente en el área de la radiología y las imágenes diagnosticas (ISO, 2022). La digitalización de todos los estudios radiológicos ha transformado la forma en que se obtienen estos, el almacén y compartes las imágenes diagnosticas, facilitando así el acceso a esta; esto mejora la eficiencia en los procesos de atención en salud (NIST, 2018). Los sistemas como las RIS y PACS, junto con otros estándares, han permitido integrar los equipos de diagnóstico por imágenes de redes hospitalarias, favoreciendo la comunicación entre profesionales y el análisis de los estudios médicos (ISO, 2022).

Sin embargo, esto también ha generado nuevos desafíos relacionados con la seguridad de la información. Los dispositivos médicos y los sistemas de imágenes diagnosticas pueden presentar diferentes vulnerabilidades que los hacen ser susceptibles a ataques cibernéticos, lo que podría comprometer la confidencialidad de los datos de nuestros pacientes, la integridad de las imágenes y la disponibilidad de los sistemas hospitalarios (FDA, 2023).

Por esta razón, en los últimos años diferentes organismos internacionales como la FDA, la ISO y el IMDRF han desarrollado normas y lineamientos orientados a fortalecer la ciberseguridad en los dispositivos médico y en los sistemas de información utilizados en el sector de la salud (IMDRF, 2020; ISO, 2019), en este contexto, resulta fundamental comprender como han evolucionado estos estándares y de qué manera contribuyen a garantizar la seguridad de los dispositivos médicos y de los sistemas de radiología digita

Planteamiento del Problema

Con el paso del tiempo en el sector salud las instituciones médicas han generado de manera significativa un aumento considerable en el uso de tecnología digital, especialmente en los dispositivos utilizados para el diagnóstico y tratamiento de diferentes condiciones médicas (Organización Mundial de la Salud, 2022).

Equipos como tomógrafos, resonadores magnéticos monitores multiparámetros, bombas de infusión y sistemas de almacenamiento de imágenes médicas su funcionamiento se basa en el uso de software, y sistemas informáticos que permiten almacenar información, procesar datos y conectarse a redes hospitalarias (FDA,2023). Gracias a estos avances, se ha logrado mejoras significativas en la calidad y eficiencia de los servicios de salud.

Estos avances tecnológicos han permitido mejorar la calidad en los servicios aumentar la precisión en muchos diagnósticos, agilizar procedimientos médicos. Además, la integración de sistemas digitales ha favorecido el almacenamiento y transmisión de datos clínicos en tiempo real, aportando a una atención más eficiente y organizada dentro de las instituciones hospitalarias.

Sin embargo, el incremento en el uso de dispositivos médicos con tecnología más avanzada también representa un riesgo en termino de seguridad informática, Debido a su conexión a diferentes redes, algunos de estos dispositivos presentan vulnerabilidades que pueden aprovecharse para realizar ataques informáticos, lo que podría generar fallas en los sistemas y afectar tanto la seguridad del paciente como la prestación de los servicios de salud en las diferentes instituciones.

En los últimos años se han reportado diversos incidentes de ciberseguridad en instituciones de salud a nivel internacional, evidenciando la necesidad de fortalecer las medidas

de protección radiológica, ataques como el ransomware han afectado hospitales y sistemas clínicos, generando retrasos en la atención médica, perdida de información y fallas operativas en equipos biomédicos (Kaspersky,2022).

Como antecedente durante la última década se ha evidenciado un aumento en las regulaciones y recomendaciones relacionadas con la protección de los sistemas médicos digitales. Estas normativas buscan que los fabricantes incorporen medidas de ciberseguridad desde el diseño de los dispositivos, así como mecanismos de actualización, monitoreo y gestión de vulnerabilidades que permitan responder de manera oportuna ante posibles amenazas informáticas (FDA,2023).

En este contexto, resulta importante analizar el siguiente planteamiento de investigación:

¿Cómo han evolucionado los estándares internacionales de ciberseguridad para dispositivos médicos (como los de la FDA) en la última década?

Justificación

En la actualidad, el sector salud ha experimentado un crecimiento evidente en el uso de tecnologías digitales, especialmente en el uso de dispositivos médicos usados para el diagnóstico tratamiento y monitoreo de pacientes (Organización Mundial de la Salud [OMS],2022). Gran parte de estos equipos funcionan por medio de software y sistemas informáticos por que permiten almacenar información, procesar datos clínicos y acceder a redes hospitalarias o internet, con estos avances a nivel tecnológico se ha logrado mejorar diferentes procesos en la atención medica permitiendo diagnósticos más acertados.

A su vez, a medida que los dispositivos médicos se vuelven más complejos y dependen cada vez más de la tecnología digital, surgen nuevos retos relacionados con la seguridad informática. Algunos estudios evidencian que estos dispositivos pueden presentar vulnerabilidades que podrían dar lugar a ataques informáticos o fallas en los sistemas. Esto afecta tanto la confidencialidad de la información médica del paciente como el funcionamiento adecuado de los diferentes equipos lo cual genera riesgos en la atención (FDA,2023).

Con base en diversas investigaciones sobre ciberseguridad en salud, la digitalización de los sistemas médicos he incrementado la exposición a amenazas informáticas. Esto ha generado que los hospitales y fabricantes de dispositivos médicos pongan un mayor énfasis en la protección de estos sistemas, ya que estar expuestos a estas vulnerabilidades puede traer diferentes consecuencias, como la perdida de información, interrupciones para el diagnóstico y tratamiento de diversas condiciones médicas (Kaspersky,2022). Por tal motivo, la seguridad de los sistemas tecnológicos en salud se ha convertido en un tema de gran importancia.

Debido a esta situación, diferentes organismos internacionales han desarrollado regulaciones y estándares con el objetivo de mejorar la seguridad en os dispositivos médicos.

Estas entidades han dispuesto diversas guías y recomendaciones dirigidas a los fabricantes, con el fin de fortalecer la protección de los sistemas que utilizan estos equipos. Estas medidas buscan garantizar que los dispositivos incorporen mecanismos de ciberseguridad desde su diseño, además de promover la gestión de posibles vulnerabilidades durante su uso (FDA,2023).

Teniendo en cuenta lo anterior, esta investigación se justifica porque permite analizar la manera en que han evolucionado los estándares internacionales de ciberseguridad en dispositivos médicos en la última década, lo cual es fundamental para comprender los cambios en las regulaciones y las estrategias implementadas para reducir los riesgos asociados al uso de estes tecnologías en el sector salud.

Asimismo, este estudio es importante porque aporta al fortalecimiento del conocimiento en el área de radiología e imágenes diagnosticas, permitiendo a estudiantes y profesionales identificar la relevancia de la seguridad informática en el manejo de dispositivos médicos y sistemas digitales. De igual manera, beneficia a las instituciones de salud al promover una mayor conciencia sobre la necesidad de implementar medidas de protección que garanticen la seguridad del paciente y la calidad en la prestación de los servicios.

Objetivos

Objetivo General

Analizar la evolución de los estándares internacionales de ciberseguridad aplicados a los dispositivos médicos, mediante revisión documental, y su impacto en la protección de la información clínica y la seguridad del paciente en entornos hospitalarios.

Objetivos Específicos

Describir el funcionamiento de los sistemas de radiología digital y su integración con plataformas como RIS, PACS en la gestión de imágenes diagnosticas, a partir de la revisión documental.

Identificar las principales vulnerabilidades y riesgos de ciberseguridad asociados a los dispositivos médicos, con base en la evidencia científica.

Analizar los principales estándares y regulaciones internacionales relacionados con la ciberseguridad en dispositivos médicos, como las normas ISO y las guías de la FDA mediante revisión bibliográfica.

Comprender la importancia de implementar medidas de seguridad informática en los sistemas de imágenes médicas para proteger la confidencialidad, integridad y disponibilidad de la información clínica.

Marco Teórico

Introducción a la Ciberseguridad en Dispositivos Médicos

El avance de la digitalización en el sector salud ha permitido el desarrollo de dispositivos médicos cada vez más sofisticados, capaces de conectarse a redes hospitalarias, sistemas en la nube y plataformas de inteligencia artificial (OMS,2022). Estos dispositivos incluyen desde monitores de signos vitales y equipos de diagnóstico por imágenes hasta dispositivos implantables y sistemas de radiología digital.

Sin embargo, esta interconectividad ha generado nuevas vulnerabilidades en términos de ciberseguridad, ya que los dispositivos médicos ahora pueden ser objeto de ataques informáticos que comprometan la integridad de los datos clínicos, la funcionalidad del dispositivo e incluso la seguridad del paciente (FDA,2023). Los sistemas médicos conectados contienen software y componentes digitales que pueden presentar vulnerabilidades explotables por atacantes, lo que convierte la ciberseguridad en un elemento crítico dentro del ciclo de vida de estos dispositivos.

En este contexto, diversas organizaciones regulatorias y organismos internacionales han desarrollado estándares y guías para garantizar que los dispositivos médicos cumplan con requisitos de seguridad informática desde su diseño hasta su uso clínico.

Fundamentos de la Radiología Digital

La radiología digital es un sistema de diagnóstico por imágenes en el cual la información obtenida mediante equipos de rayos X, tomografía computarizada, resonancia magnética o ultrasonido se captura en formato digital y se gestiona mediante sistemas informáticos especializados.

A diferencia de la radiología tradicional basada en películas radiográficas, la radiología digital permite almacenar las imágenes en bases de datos, visualizarlas en estaciones de trabajo

clínicas y compartirlas instantáneamente dentro de la red hospitalaria. Este cambio ha generado múltiples ventajas, entre ellas:

Reducción del uso de películas y químicos radiográficos.

Mayor rapidez en la obtención y distribución de imágenes.

Posibilidad de procesamiento digital de las imágenes.

Acceso remoto a estudios médicos.

Integración con sistemas de información hospitalaria.

Dentro de este contexto, los sistemas de información radiológica se han convertido en elementos clave para la gestión de los estudios médicos y la coordinación entre los diferentes profesionales de salud.

Ecosistema RIS/PACS y la Red de Imágenes Médicas

El funcionamiento de la radiología digital depende de la interacción entre varios sistemas informáticos que conforman el ecosistema de gestión de imágenes médicas.

RIS (Radiology Information System)

El RIS es un sistema de información diseñado para gestionar los procesos administrativos y clínicos relacionados con el servicio de radiología. Entre sus principales funciones se encuentran:

Programación de estudios radiológicos.

Registro de pacientes.

Gestión de órdenes médicas.

Generación de informes radiológicos.

Integración con sistemas hospitalarios como el HIS (Hospital Information System).

El RIS permite organizar el flujo de trabajo dentro del departamento de radiología, asegurando que los estudios se realicen de manera eficiente y que la información clínica esté disponible para los especialistas.

PACS (Picture Archiving and Communication System)

El PACS es un sistema informático encargado del almacenamiento, gestión y distribución de imágenes médicas en formato digital. Este sistema reemplaza el archivo físico de placas radiográficas y permite acceder a los estudios desde cualquier estación de trabajo conectada a la red hospitalaria.

El funcionamiento del PACS se basa en varios componentes principales:

Modalidades de adquisición: equipos de diagnóstico como rayos X, tomografía o resonancia magnética.

Servidor de almacenamiento: base de datos donde se almacenan las imágenes médicas.

Red de comunicación: infraestructura que permite la transmisión de datos entre dispositivos.

Estaciones de visualización: computadoras utilizadas por radiólogos y médicos para analizar las imágenes.

La integración entre RIS y PACS permite automatizar el flujo de información desde la solicitud del estudio hasta la entrega del informe diagnóstico.

El Estándar DICOM y su Arquitectura

El estándar DICOM (Digital Imaging and Communications in Medicine) es el protocolo internacional utilizado para el almacenamiento, transmisión e intercambio de imágenes médicas entre dispositivos de diferentes fabricantes (NEMA,2024).

DICOM define tanto el formato de los archivos de imágenes como los protocolos de comunicación que permiten el intercambio de información entre sistemas médicos.

La arquitectura del estándar DICOM se basa en varios elementos fundamentales:

Objetos de información (Information Objects): Representan los datos médicos, incluyendo la imagen y la información asociada al estudio.

Servicios de comunicación: Permiten el envío, almacenamiento y consulta de imágenes entre dispositivos dentro de la red.

Entidades de aplicación (Application Entities): Son los sistemas o dispositivos que participan en la comunicación DICOM, como equipos de imagen, servidores PACS o estaciones de trabajo.

Gracias a esta arquitectura, dispositivos de diferentes fabricantes pueden comunicarse entre sí sin problemas de compatibilidad

Vulnerabilidad en el Intercambio de Metadatos

Uno de los aspectos más sensibles del estándar DICOM es el manejo de los metadatos, que contienen información asociada a las imágenes médicas, como:

Datos del paciente

Fecha del estudio

Tipo de modalidad,

Parámetros técnicos de adquisición.

Identificadores del estudio.

Estos metadatos son fundamentales para la correcta identificación y gestión de los estudios radiológicos. Sin embargo, también representan un punto crítico de vulnerabilidad en términos de ciberseguridad.

En muchos sistemas, los metadatos pueden modificarse o interceptados durante la transmisión si no existen mecanismos adecuados de protección, lo que podría provocar:

Alteración de información clínica.

Confusión en la identificación de pacientes.

Manipulación de estudios médicos.

Exposición de datos personales sensibles.

Internet de las Cosas Médicas (IoMT)

El Internet de las Cosas Médicas (IoMT) representa la evolución de los dispositivos médicos hacia entornos completamente interconectados mediante redes digitales (IEEE,2021).

En el pasado, muchos equipos médicos funcionaban de manera aislada, almacenando la información localmente. Sin embargo, la necesidad de compartir datos clínicos en tiempo real ha impulsado la conexión de estos dispositivos a redes hospitalarias y plataformas en la nube.

El IoMT incluye una amplia variedad de dispositivos, entre ellos:

Equipos de diagnóstico por imágenes.

Monitores de signos vitales.

Dispositivos portátiles de monitoreo de pacientes.

Sistemas de telemedicina.

Equipos médicos conectados a plataformas de análisis de datos.

Esta conectividad permite mejorar la coordinación entre profesionales de salud, optimizar el seguimiento de los pacientes y facilitar el acceso remoto a la información médica.

Riesgos Asociados al IoMT

Aunque el IoMT ofrece importantes beneficios para el sistema de salud, también introduce nuevos riesgos de seguridad. La interconexión de dispositivos médicos aumenta la superficie de ataque para posibles amenazas cibernéticas, lo que puede comprometer tanto la privacidad de los datos como la integridad de los sistemas médicos.

Entre los principales riesgos se encuentran:

Acceso no autorizado a dispositivos médicos.

Manipulación de datos clínicos.

Interrupción del funcionamiento de sistemas hospitalarios.

Exposición de información sensible de pacientes.

Definición de Ciberseguridad Médica

La ciberseguridad puede definirse como el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o daños. En términos generales, la seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de los datos dentro de una organización.

Sin embargo, en el ámbito sanitario surge el concepto de ciberseguridad médica, el cual amplía este enfoque al incluir la protección de dispositivos médicos y sistemas clínicos que pueden afectar directamente la salud de los pacientes. En este contexto, una vulnerabilidad informática no solo puede provocar la pérdida de datos, sino también alterar diagnósticos, interrumpir tratamientos o comprometer el funcionamiento de equipos médicos críticos.

Por esta razón, la ciberseguridad médica integra principios de seguridad informática con estrategias de gestión de riesgos clínicos, con el objetivo de proteger tanto la información médica como la seguridad del paciente (FDA,2023).

Protección de datos clínicos y registros electrónicos de salud.

Seguridad de dispositivos médicos conectados a redes hospitalarias.

Protección de sistemas de imágenes médicas.

Prevención de manipulación de información diagnóstica.

Continuidad operativa de los sistemas hospitalarios.

Tríada de la Seguridad (CIA) Aplicada a Sistemas de Imágenes Médicas

La base conceptual de la seguridad de la información se sustenta en la tríada CIA, que representa tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad (Whitman & Mattord,2022).

Confidencialidad

La confidencialidad se refiere a la protección de la información frente a accesos no autorizados. En el entorno de radiología, esto implica garantizar que únicamente el personal autorizado pueda acceder a las imágenes médicas y a los datos del paciente almacenados en sistemas como RIS (Radiology Information System) y PACS (Picture Archiving and Communication System).

Las imágenes diagnósticas contienen información altamente sensible, por lo que su exposición podría vulnerar la privacidad del paciente y generar implicaciones legales para las instituciones de salud.

Integridad

La integridad se refiere a la garantía de que los datos no sean modificados o alterados de manera no autorizada. En radiología, la integridad es fundamental, ya que cualquier modificación en una imagen diagnóstica podría conducir a interpretaciones clínicas incorrectas.

Por ejemplo, la alteración de una imagen de tomografía o resonancia magnética podría provocar errores en el diagnóstico o afectar decisiones terapéuticas. Por ello, los sistemas PACS deben incorporar mecanismos que aseguren la autenticidad y consistencia de las imágenes almacenadas.

Disponibilidad

La disponibilidad garantiza que los sistemas y datos estén accesibles cuando los profesionales de salud los necesiten. En entornos hospitalarios, la indisponibilidad de sistemas de imágenes médicas puede retrasar diagnósticos y afectar la atención del paciente.

Ataques cibernéticos como el ransomware han demostrado que la interrupción de sistemas hospitalarios puede paralizar servicios clínicos completos. Por esta razón, asegurar la disponibilidad de los sistemas RIS/PACS es un aspecto crítico de la ciberseguridad médica.

Clasificación y Naturaleza de los Dispositivos Médicos

Los dispositivos médicos constituyen herramientas fundamentales para el diagnóstico, monitoreo y tratamiento de diversas condiciones de salud. Organismos internacionales como la Organización Mundial de la Salud (OMS) y la Food and Drug Administration (FDA) han desarrollado definiciones y marcos regulatorios para clasificar estos dispositivos según su función y nivel de riesgo.

Definición de Dispositivo Médico

Según la OMS, un dispositivo médico es cualquier instrumento, aparato, equipo, software o material utilizado con fines médicos, tales como el diagnóstico, prevención, monitoreo o tratamiento de enfermedades.

Por su parte, la FDA define los dispositivos médicos como productos destinados a uso médico que no ejercen su acción principal mediante medios farmacológicos, inmunológicos o metabólicos.

Dentro de esta categoría se encuentran los dispositivos de imagenología médica, que incluyen equipos utilizados para obtener imágenes del cuerpo humano con fines diagnósticos.

Entre los principales dispositivos de imagenología se encuentran:

Equipos de radiografía digital

Tomógrafos computarizados

Sistemas de resonancia magnética

Equipos de medicina nuclear

Sistemas de ultrasonido

Estos dispositivos generan grandes volúmenes de datos digitales que deben ser almacenados y transmitidos de forma segura dentro de las redes hospitalarias.

Ciclo de Vida de los Dispositivos Médicos

Los dispositivos médicos, al igual que cualquier sistema tecnológico, poseen un ciclo de vida que abarca diferentes etapas desde su desarrollo hasta su retiro del mercado.

Las principales fases del ciclo de vida de un dispositivo médico incluyen:

Diseño y Desarrollo

En esta etapa se definen las características técnicas del dispositivo y se desarrollan los sistemas de hardware y software que lo componen.

Fabricación y Certificación

El dispositivo es producido siguiendo estándares regulatorios y sometido a evaluaciones de seguridad y eficacia.

Implementación y Uso Clínico

El equipo es instalado en entornos hospitalarios y utilizado para la atención de pacientes.

Mantenimiento y Actualizaciones

Durante su vida útil, el dispositivo requiere mantenimiento técnico y actualizaciones de software para garantizar su funcionamiento seguro.

Fin de Vida Util (End of Life – EoL)

Cuando el fabricante deja de proporcionar soporte técnico o actualizaciones, el dispositivo entra en una fase de riesgo creciente, especialmente si utiliza sistemas operativos obsoletos.

El uso prolongado de dispositivos con sistemas operativos desactualizados puede generar vulnerabilidades críticas que pueden ser explotadas por atacantes, lo que representa un riesgo significativo para la seguridad hospitalaria.

Software Como Dispositivo Médico (SaMD)

El concepto de Software as a Medical Device (SaMD) se refiere al software diseñado para realizar funciones médicas sin formar parte de un hardware médico específico. Este tipo de software puede utilizarse para analizar datos clínicos, procesar imágenes médicas o apoyar la toma de decisiones diagnósticas.

En el campo de la radiología, el SaMD ha adquirido gran relevancia debido al desarrollo de algoritmos de inteligencia artificial (IA) capaces de analizar imágenes médicas y detectar patrones asociados a diversas patologías.

Estos sistemas pueden ayudar a los radiólogos en tareas como:

Detección temprana de tumores.

Identificación de anomalías en imágenes pulmonares.

Análisis automatizado de estudios de tomografía o resonancia magnética.

Apoyo en la priorización de estudios urgentes.

Sin embargo, debido a que estos algoritmos influyen directamente en el proceso diagnóstico, su seguridad y confiabilidad son aspectos críticos. Un ataque cibernético que manipule el funcionamiento de un algoritmo de IA podría alterar los resultados del análisis de imágenes médicas.

Por esta razón, la protección de los sistemas SaMD se ha convertido en un elemento clave dentro de la ciberseguridad médica, requiriendo mecanismos de validación, control de integridad del software y protección frente a manipulaciones maliciosas.

Regulación Internacional de la Ciberseguridad en Dispositivos Médicos

En el ámbito global, varios organismos han participado en el desarrollo de marcos regulatorios para la seguridad de dispositivos médicos digitales. Entre los principales se encuentran:

La Food and Drug Administration (FDA) en Estados Unidos

La Unión Europea mediante el Medical Device Regulation (MDR)

Organizaciones de estandarización como ISO, IEC y IMDRF (International Medical Device Regulators Forum)

Estos organismos han establecido directrices destinadas a asegurar que los dispositivos médicos incorporen medidas de seguridad que permitan prevenir, detectar y mitigar vulnerabilidades informáticas.

Entre los estándares más relevantes se encuentran:

IEC 62304 y la Integración de la Seguridad Desde el Diseño

La norma IEC 62304 establece el ciclo de vida del software utilizado en dispositivos médicos, definiendo procesos estructurados para el desarrollo, mantenimiento y gestión del software clínico. Tradicionalmente, esta norma se enfocaba principalmente en la seguridad funcional del software, es decir, en garantizar que el sistema funcionara correctamente sin causar daños al paciente.

Con el aumento de los dispositivos médicos conectados y el software clínico integrado en redes hospitalarias, la ciberseguridad comenzó a considerarse un aspecto esencial dentro del ciclo de vida del software médico. En las interpretaciones más recientes y en las guías complementarias, se ha promovido la incorporación del enfoque Security by Design, que implica integrar mecanismos de seguridad desde las primeras etapas del desarrollo del software.

Este enfoque incluye prácticas como:

Modelado de amenazas durante el diseño del sistema.

Desarrollo seguro de software.

Control de vulnerabilidades y actualizaciones de seguridad.

Verificación y validación de mecanismos de protección.

De esta manera, la norma ha evolucionado hacia una visión más integral del software médico, en la que la seguridad informática se considera un componente inseparable de la seguridad del paciente.

ISO 13485 e ISO 14971: Gestión de Riesgos Clínicos y Cibernéticos

Las normas ISO 13485 e ISO 14971 constituyen pilares fundamentales en la regulación de dispositivos médicos. La primera define los requisitos para los sistemas de gestión de calidad en fabricantes de dispositivos médicos, mientras que la segunda establece el marco para la gestión de riesgos asociados a dichos dispositivos (ISO,2019).

Tradicionalmente, la gestión de riesgos se centraba en fallos técnicos, errores de uso o problemas de diseño que pudieran afectar la seguridad del paciente. Sin embargo, con la creciente digitalización de los dispositivos médicos, se ha reconocido que los ataques cibernéticos también pueden generar riesgos clínicos.

Por ejemplo, un ataque informático que manipule datos de imágenes médicas altere parámetros de un dispositivo o interrumpa el funcionamiento de un sistema hospitalario puede provocar diagnósticos erróneos o afectar tratamientos críticos.

En respuesta a estas amenazas, los enfoques actuales de ISO 14971 promueven la integración de los riesgos cibernéticos dentro del proceso de gestión de riesgos clínicos. Esto implica:

Identificar amenazas cibernéticas potenciales.

Analizar el impacto de estas amenazas en la seguridad del paciente.

Implementar controles técnicos y organizacionales para mitigarlas.

A su vez, ISO 13485 exige que las organizaciones integren estos procesos dentro de sus sistemas de gestión de calidad, asegurando que la ciberseguridad sea considerada a lo largo de todo el ciclo de vida del dispositivo.

Evolución de las Guías de la FDA Sobre Ciberseguridad (2014 – 2025)

La Food and Drug Administration (FDA) ha desempeñado un papel fundamental en el desarrollo de lineamientos regulatorios sobre ciberseguridad en dispositivos médicos.

En 2014, la FDA publicó una de las primeras guías sobre ciberseguridad para dispositivos médicos, enfocada principalmente en la gestión de riesgos durante el diseño y el desarrollo de los dispositivos (FDA,2023). Esta guía recomendaba a los fabricantes incorporar controles básicos de seguridad, como autenticación de usuarios, protección de datos y actualizaciones de software.

Posteriormente, en 2018, la agencia amplió estas recomendaciones al ciclo de vida posterior a la comercialización, enfatizando la importancia de monitorear vulnerabilidades y aplicar parches de seguridad.

Las actualizaciones más recientes, publicadas entre 2023 y 2025, representan un avance significativo. Estas guías incluyen requisitos más estrictos, tales como:

Presentación obligatoria de documentación de ciberseguridad durante la aprobación de dispositivos.

Implementación de programas de gestión de vulnerabilidades.

Uso de SBOM (Software Bill of Materials) para identificar componentes de software.

Pruebas de penetración y evaluaciones de seguridad.

IMDRF y la Transparencia del Software Mediante SBOM

El International Medical Device Regulators Forum (IMDRF) es una organización internacional que reúne a autoridades regulatorias con el objetivo de armonizar las regulaciones sobre dispositivos médicos.

Uno de los aportes más importantes del IMDRF en materia de ciberseguridad es la promoción del concepto Software Bill of Materials (SBOM). Un SBOM es esencialmente un inventario detallado de todos los componentes de software que forman parte de un dispositivo médico, incluyendo bibliotecas, dependencias y módulos de terceros.

La adopción de SBOM permite mejorar la transparencia del software y facilita la identificación rápida de vulnerabilidades cuando se descubren fallos de seguridad en componentes específicos. De esta manera, los fabricantes y las instituciones de salud pueden evaluar rápidamente el impacto de una vulnerabilidad y aplicar las medidas correctivas necesarias.

ISO/IEC 27001 y la Seguridad de la Información en el Sector Salud

El estándar ISO/IEC 27001 es uno de los marcos más reconocidos a nivel mundial para la gestión de la seguridad de la información. Este estándar establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita proteger datos sensibles frente a accesos no autorizados, pérdida o manipulación.

En el contexto sanitario, ISO 27001 es particularmente relevante debido a la sensibilidad de los datos médicos. Su implementación en hospitales y organizaciones de salud permite establecer políticas, controles técnicos y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información clínica.

Además, este estándar se integra fácilmente con otros marcos regulatorios del sector médico, proporcionando una base sólida para la gestión de la ciberseguridad a nivel organizacional.

ISO 81001-5-1 y la Seguridad del Software de Salud

La norma ISO 81001-5-1 representa uno de los avances más recientes en la regulación de software sanitario. Este estándar se centra específicamente en la seguridad, eficacia y resiliencia del software utilizado en entornos de salud.

Su objetivo principal es garantizar que el software médico sea diseñado y desarrollado con mecanismos adecuados de seguridad, interoperabilidad y protección frente a amenazas cibernéticas. Entre los aspectos clave que aborda se encuentran:

Desarrollo seguro de software clínico.

Gestión de vulnerabilidades.

Protección de datos de pacientes.

Integración de controles de seguridad en sistemas interoperables.

Este estándar complementa normas como IEC 62304 al proporcionar requisitos adicionales orientados específicamente a la seguridad del software médico.

NIST Cybersecurity Framework en Hospitales

El NIST Cybersecurity Framework, desarrollado por el National Institute of Standards and Technology, es uno de los marcos más utilizados para la gestión de ciberseguridad en organizaciones.

Este marco se estructura en cinco funciones principales:

Identificar: reconocimiento de activos, riesgos y vulnerabilidades.

Proteger: implementación de controles de seguridad para evitar ataques.

Detectar: monitoreo continuo para identificar incidentes de seguridad.

Responder: gestión y contención de incidentes.

Recuperar: restauración de los sistemas afectados.

En el contexto hospitalario, este modelo permite estructurar programas de ciberseguridad que protejan infraestructuras críticas como sistemas de imágenes médicas, historiales clínicos electrónicos y dispositivos médicos conectados.

Evolución del Estándar DICOM Y la Seguridad en el Intercambio de Imágenes Médicas

El estándar DICOM (Digital Imaging and Communications in Medicine) es el principal protocolo utilizado para el almacenamiento y transmisión de imágenes médicas, especialmente en sistemas de radiología y diagnóstico por imágenes.

La Parte 15 de DICOM define los perfiles de seguridad utilizados para proteger el intercambio de información médica entre sistemas. Con el tiempo, estos perfiles han evolucionado para incorporar mecanismos más eficaces de protección, incluyendo:

Cifrado de datos mediante protocolos seguros.

Autenticación de usuarios y dispositivos.

Control de acceso a la información médica.

Registro de auditorías de acceso.

Estas mejoras responden a la necesidad de proteger la integridad y confidencialidad de las imágenes médicas, que constituyen un elemento crítico en los procesos de diagnóstico.

Marco Metodológico

Enfoque de la Investigación

La presente investigación se desarrolla bajo un enfoque cualitativo, ya que busca analizar la evolución de los estándares internacionales de ciberseguridad aplicados a los dispositivos médicos durante la última década. Este enfoque permite interpretar información proveniente de normativas, documentos técnicos y literatura científica con el propósito de comprender los cambios regulatorios y tecnológicos en materia de seguridad informática dentro del sector sanitario.

El enfoque cualitativo facilita el análisis detallado de documentos y regulaciones internacionales, permitiendo identificar tendencias, avances y transformaciones en las políticas de ciberseguridad que buscan garantizar la protección de los sistemas médicos y la seguridad de los pacientes.

"El enfoque cualitativo permite comprender fenómenos desde una perspectiva interpretativa, analizando significados, experiencias y contextos" (Hernández Sampieri, Fernández & Baptista, 2014).

Tipo de Investigación

El estudio corresponde a una investigación documental de tipo descriptivo.
Es documental, ya que se basa en la recopilación y análisis de información proveniente de documentos oficiales, artículos científicos, informes técnicos y normas internacionales relacionadas con la ciberseguridad en dispositivos médicos.

Asimismo, es descriptiva porque pretende explicar y detallar cómo han evolucionado los estándares internacionales de seguridad durante la última década, identificando los principales

cambios, avances tecnológicos y desafíos que enfrentan los sistemas médicos frente a amenazas cibernéticas.

Diseño de la Investigación

El diseño de la investigación es no experimental, debido a que no se manipulan variables ni se realizan experimentos. En cambio, se analizan documentos existentes y literatura especializada relacionada con el tema de estudio.

Además, El estudio se basa en un análisis de información histórica a lo largo del tiempo, ya que examina la evolución de los estándares internacionales de ciberseguridad en dispositivos médicos a lo largo de los últimos diez años, permitiendo identificar cambios regulatorios y avances en las estrategias de protección de datos y sistemas médicos.

Población y Muestra

La población de la investigación está conformada por documentos académicos, normas internacionales, informes técnicos y publicaciones científicas relacionadas con la ciberseguridad en dispositivos médicos.

La muestra estará compuesta por documentos relevantes publicados durante la última década por organismos internacionales, entidades reguladoras y centros de investigación especializados en tecnología médica y seguridad informática.

La selección de los documentos se realizará mediante muestreo no probabilístico de tipo intencional, seleccionando aquellos que aporten información significativa para el análisis de la evolución de los estándares internacionales de ciberseguridad.

Técnicas de Recolección de Información

Revisión Documental

Consiste en la búsqueda, recopilación y análisis de documentos científicos, normas internacionales, guías regulatorias e informes técnicos relacionados con la ciberseguridad en dispositivos médicos.

Análisis de Contenido

Permite examinar de manera sistemática la información contenida en los documentos seleccionados, identificando conceptos clave, cambios en las regulaciones y avances en las estrategias de protección frente a amenazas cibernéticas.

“ El análisis de contenido es una técnica que permite interpretar de manera sistemática la información contenida en documentos, identificando patrones y categorías relevantes “ (Hernández Sampieri et al., 2014).

Fuentes de Información

Fuentes Primarias

Normativas internacionales sobre dispositivos médicos

Guías regulatorias de organismos internacionales

Documentos técnicos sobre ciberseguridad

Fuentes Secundarias

Artículos científicos

Libros especializados

Informes académicos y revisiones de literatura relacionadas con la ciberseguridad en el sector salud

Técnicas de Análisis de Datos

La información recopilada se analizará mediante análisis cualitativo de contenido, lo cual permitirá identificar patrones, tendencias y cambios en los estándares internacionales de ciberseguridad.

Este análisis facilitará la comparación entre diferentes normativas y permitirá comprender cómo han evolucionado las estrategias de protección frente a amenazas informáticas en los dispositivos médicos.

Procedimiento de la Investigación

El desarrollo de la investigación se realizará mediante las siguientes etapas:

Búsqueda de Información

Recopilación de documentos científicos, normas internacionales y guías regulatorias relacionadas con la ciberseguridad en dispositivos médicos.

Selección de Documentos

Identificación y selección de las fuentes más relevantes publicadas durante la última década.

Revisión Documental

Análisis detallado de los documentos seleccionados para identificar conceptos, regulaciones y cambios en los estándares de ciberseguridad.

Organización de la Información

Clasificación de los datos obtenidos mediante fichas documentales y matrices de análisis.

Interpretación y Análisis

Evaluación de la información recopilada para identificar tendencias, avances y desafíos en la evolución de los estándares internacionales de ciberseguridad.

Tabla 1

Matriz Metodológica

Pregunta de Investigación	Objetivo	Variable	Técnica	Fuente
¿Cómo han evolucionado los estándares internacionales de ciberseguridad para dispositivos médicos en la última década?	Analizar la evolución de los estándares internacionales de ciberseguridad	Evolución de estándares	Revisión documental	Normativas y documentos oficiales
¿Qué cambios regulatorios se han implementado en los estándares de seguridad?	Identificar las principales actualizaciones en las regulaciones de ciberseguridad	Normativas internacionales	Análisis de contenido	Artículos científicos y guías regulatorias
¿Qué impacto tienen estos estándares en la seguridad de los dispositivos médicos?	Evaluar la influencia de los estándares en la protección de los sistemas médicos	Ciberseguridad en dispositivos médicos	Análisis documental	Estudios académicos e informes técnicos

Nota. Elaboración propia con base en Hernández Sampieri et al (2014)

Resultados

Los resultados obtenidos evidencian que la creciente integración de sistemas de inteligencia artificial en dispositivos médicos ha incrementado significativamente la superficie de ataque, exponiendo estos sistemas a vulnerabilidades como la manipulación de datos, accesos no autorizados y fallas en la protección de información clínica (FDA, 2023). Esto demuestra que, aunque la IA mejora la precisión diagnóstica y la eficiencia clínica, también introduce riesgos críticos en términos de ciberseguridad que deben gestionarse desde etapas tempranas del desarrollo.

De acuerdo con IMDRF (2020), la evolución de los dispositivos médicos conectados mediante tecnologías loMT ha generado nuevos desafíos para los sistemas hospitalarios, especialmente en termino de protección de datos sensibles y continuidad operativa. Asimismo, La norma ISO 14971 establece que los riesgos cibernéticos deben gestionarse como parte integral de la seguridad clínica del paciente (ISO, 2019).

En relación con los estándares internacionales analizados, se evidencio que organismos como la FDA, ISO e IEC han fortalecido progresivamente sus lineamientos regulatorios, incorporando estrategias como Security by Desing, gestión de vulnerabilidades y monitoreo continuo del Software medico (IEC, 2006). Estas medidas buscan reducir riesgos asociados a ataques cibernéticos que puedan afectar el funcionamiento de dispositivos médicos y sistemas de imágenes diagnosticas.

Estos hallazgos responden directamente al problema planteado, ya que confirman que la adopción acelerada de tecnologías basadas en IA en el ámbito médico no ha sido acompañada al mismo ritmo por mecanismos robustos de seguridad (FDA,2023). En este sentido, se valida la hipótesis de que existen brechas importantes en la protección de los sistemas frente a amenazas

cibernéticas, lo que puede comprometer tanto la información como la seguridad del paciente (IMDRF, 2020).

Sustento Teórico

Desde el marco teórico, estos resultados se sustentan en estándares internacionales como ISO 14971, que establece la gestión de riesgos en dispositivos médicos, y IEC 62304, que regula el ciclo de vida del software médico (ISO, 2019; IEC, 2026). Ambos enfoques enfatizan la identificación temprana de riesgos y su mitigación. Asimismo, organismos regulatorios han señalado la necesidad de incorporar la ciberseguridad como un componente esencial del diseño, lo cual coincide con los hallazgos obtenidos en esta investigación (NIST, 2018).

Los resultados tienen implicaciones relevantes para el sector salud, ya que evidencian la necesidad de fortalecer las estrategias de ciberseguridad en dispositivos médicos que incorporan inteligencia artificial. Esto impacta directamente la protección de datos sensibles y la seguridad clínica, dado que una vulneración podría alterar diagnósticos, tratamientos o el funcionamiento de los dispositivos (ISO, 2021).

Limitaciones del Estudio

No obstante, es importante considerar que el estudio se basa principalmente en revisión documental y análisis teórico, lo que puede limitar la generalización de los resultados a contextos clínicos específicos (Hernández Sampieri et al., 2014). Además, la rápida evolución de la tecnología y las amenazas cibernéticas implica que los riesgos identificados pueden cambiar en el corto plazo.

Aporte de la Investigación

Este estudio aporta una visión actualizada sobre la relación entre inteligencia artificial y ciberseguridad en dispositivos médicos, destacando la necesidad de integrar enfoques de

seguridad desde el diseño (security by design) (FDA, 2023). Asimismo, contribuye a la identificación de riesgos emergentes que aún no han sido completamente abordados en todos los marcos regulatorios, especialmente en contextos en desarrollo (IMDRF, 2020).

Tabla 2

Tabla Comparativa de los Criterios Analizados

Criterio	ISO	NIST	IEC
Enfoque Principal	Gestión de riesgos y calidad en dispositivos médicos	Marco de ciberseguridad y gestión de riesgos tecnológicos	Desarrollo seguro y ciclo de vida del software médico
Objetivos	Gestión de riesgos y calidad en dispositivos médicos	Proporcionar lineamientos para identificar, proteger, detectar y responder a amenazas	Asegurar que el software médico sea seguro, confiable y mantenible (IEC 62304)
Tipo De Estándar	Normas internacionales certificables	Guías y frameworks (no siempre certificables)	Normas técnicas específicas para ingeniería de software
Aplicación En Medicina-IA	Evalúa riesgos asociados al uso de IA en dispositivos	Ayuda a gestionar amenazas cibernéticas en sistemas con IA	Regula el desarrollo del software que integra IA
Enfoque De Ciberseguridad	Preventivo basado en análisis de riesgos	Integral (identificación, protección, detección, respuesta y recuperación)	Preventivo desde el diseño y desarrollo del software

Criterio	ISO	NIST	IEC
Aportes Claves	Introduce la gestión sistemática del riesgo clínico y tecnológico	Ofrece un marco estructurado para la ciberseguridad organizacional	Define buenas prácticas para el desarrollo seguro del software médico
Limitaciones	No profundiza en ciberseguridad técnica específica	No es obligatorio ni específico para dispositivos médicos	Se enfoca más en software que en amenazas externas
Relevancia En El Estudio	Permite entender cómo gestionar riesgos en dispositivos con IA	Complementa la protección frente a ataques cibernéticos	Asegura que el software médico cumpla estándares de seguridad
Enfoque Principal	Gestión de riesgos y calidad en dispositivos médicos	Marco de ciberseguridad y gestión de riesgos tecnológicos	Desarrollo seguro y ciclo de vida del software médico

*Nota***.** Elaboración propia con base a la revisión documental de estándares internacionales como ISO14971, NIST 2018 y IEC62304.

Conclusión

La integración de la inteligencia artificial en dispositivos médicos constituye un avance significativo en términos de precisión diagnóstica, eficiencia operativa y capacidad de análisis de grandes volúmenes de datos clínicos. No obstante, este progreso tecnológico también amplía considerablemente la superficie de ataque, introduciendo vulnerabilidades asociadas a la manipulación de datos, accesos no autorizados y fallos en los sistemas automatizados. En este sentido, se concluye que la adopción de IA en el ámbito sanitario debe ir acompañada de estrategias de ciberseguridad sólidas e integrales, que no solo protejan la información sensible de los pacientes, sino que también garanticen la confiabilidad y seguridad de los procesos clínicos.

A partir de los resultados obtenidos, se evidencia la existencia de una brecha significativa entre el acelerado desarrollo e implementación de tecnologías basadas en inteligencia artificial y la adecuada adopción de estándares y prácticas de ciberseguridad. Aunque existen marcos regulatorios y normativas internacionales orientadas a la gestión de riesgos y seguridad del software médico, su aplicación no siempre es homogénea ni suficientemente rigurosa en todos los contextos. Esta situación incrementa la exposición de los sistemas de salud a amenazas cibernéticas, lo que permite concluir que es necesario fortalecer la regulación, la supervisión y la cultura de seguridad en las instituciones sanitarias.

Finalmente, se concluye que la ciberseguridad debe ser concebida como un componente fundamental desde las etapas iniciales del diseño y desarrollo de dispositivos médicos con inteligencia artificial, adoptando enfoques preventivos como el “security by design” y la gestión continua de riesgos. Este enfoque proactivo permite anticipar posibles vulnerabilidades y reducir el impacto de eventuales ataques, fortaleciendo la resiliencia de los sistemas. Asimismo, su implementación no solo contribuye a mejorar la seguridad tecnológica, sino que también

refuerza la confianza de los profesionales de la salud y los pacientes en el uso de estas herramientas, favoreciendo una adopción más segura y sostenible de la innovación en el sector sanitario.

Referencias.

Bermúdez Rubio, D., Cuenca Rivera, P. E., García Murillo, P. G., Gutiérrez Gómez, G. y Portela Ramírez, A. J. (2021). *Sugerencias para escribir análisis de resultados, conclusiones y recomendaciones en tesis y trabajos de grado. CITAS,* 7(1). https://doi.org/10.15332/24224529.6608

Castro, S. (2020). *Metodología de la investigación* [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/36005

FDA. (2023). *Cybersecurity in medical devices: Quality system considerations and content of premarket submissions*. U.S. Food and Drug Administration. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket

Gallegos, C., & Lobato, P. (2024). *Cómo elaborar una conclusión*. Programa de Apoyo a la Educación Académica, Universidad de Chile, 1–8. https://comunicacionacademica.uc.cl/images/recursos/espanol/escritura/recurso_en_pdf_extenso/17_Como_elaborar_una_conclusion.pdf

Gogniéva, D., et al. (2023). *Cybersecurity vulnerabilities of medical devices in public procurement datasets*. Scientific Reports, 13, Article 45927. https://doi.org/10.1038/s41598-023-45927-1

Hernández Armas, J. Á. (2020). *Ciberseguridad en el entorno sanitario*. Hospitecnia. https://hospitecnia.com/sites/default/files/inline-files/JAHernandez-seeic-ciberseguridad-entorno-sanitario.pdf

Hernández, H. A. (2018). *Metodología de la investigación* [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/18130

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación*. Abrir este documento utilizando ReadSpeaker docReader6 (1). https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

IEC. (2006). IEC 62304*: Medical Device Software – Software Life Cycle Processes.* https://www.iso.org/standard/38421.html

International Medical Device Regulators Forum (IMDRF). (2020). *Principles and practices for medical device cybersecurity*. https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

International Medical Device Regulators Forum. (2020). *Principles and practices for medical device cybersecurity*. https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

ISO. (2016). ISO 13485: *Medical Devices – Quality Management Systems.* https://www.iso.org/standard/59752.html

ISO. (2019). ISO 14971: *Medical Devices – Application of Risk Management to Medical* Devices.https://www.iso.org/standard/72704.html.

ISO. (2022). ISO/IEC 27001: *Information Security Management Systems.* https://www.iso.org/standard/27001

Kripka, R. M., Scheller, M., & Bonotto, D. (2015*). Investigación documental: conceptos y caracterización*. Revista de Investigaciones UNAD*,* 14(2), 55–73. https://doi.org/10.22490/25391887.1455

Laverde, M. (2021). *Importancia de los resultados, análisis y conclusiones en una investigación*. https://doi.org/10.13140/RG.2.2.20558.95048

Luvezute Kripka, R. M., Scheller, M., & de Lara Bonotto, D. (2015). *La investigación documental sobre la investigación cualitativa : conceptos y caracterización*. Revista De Investigaciones UNAD, 14(2), 55-73. https://doi.org/10.22490/25391887.1455

Marroquín, E., et al. (2025). *Tips Normas APA 7 ed.* [Objeto virtual de aprendizaje OVA]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/65792

Martínez-Peña, L. M. (2020). *Enfoques y diseños de investigación* [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35836

Medina, J. (2018). *Redacción Marco teórico y Metodología.* [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/22624

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

National Democratic Institute. (2025). *Cybersecurity handbook for civil society organizations*. https://www.ndi.org/sites/default/files/%5BSpanish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf

Medina, J. (2018). *Redacción marco teórico y metodología* [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/22624

Pérez, C. E. (2016). *Uso de bases de datos y manejadores de referencias* [Objeto virtual de aprendizaje OVA]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/9102

Rodríguez, J. P. (2021). *Objetivo y metodología* [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/41649

Vidal, M. (2024). *Cómo elaborar una introducción*. Programa de Apoyo a la Educación Académica, Universidad de Chile, 1-5. https://comunicacionacademica.uc.cl/images/recursos/espanol/escritura/recurso_en_pdf_extenso/14_Como_elaborar_una_introduccion.pdf