RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Ciberseguridad en IoMT: Retos y Amenazas

Noviembre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IOT PARA ENTORNOS DE SMART CITIES Y SALUD” (CONTR 2024 829153).

Esta guía forma parte de la colección Guías de Ciberseguridad en IoT para las Smart Cities y el sector Salud creada por la Agencia Digital de Andalucía como parte del Proyecto Red Argos, perteneciente al programa RETECH, de Redes Inteligentes de Especialización Tecnológica, en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-NextGenerationEU, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 28/11/2025

Fecha de última actualización: 28/11/2025

ÍNDICE DE CONTENIDOS

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. Introducción

El avance del Internet de los Objetos Médicos (IoMT) se ha convertido en uno de los desarrollos tecnológicos más transformadores dentro del sector salud en los últimos años. La incorporación de dispositivos médicos conectados, sensores biométricos y plataformas digitales en hospitales, clínicas y hogares ha permitido mejorar la calidad asistencial, optimizar la gestión de recursos sanitarios y reducir los costes operativos, al mismo tiempo que se impulsa una atención más personalizada, continua y basada en datos. Desde los sistemas de monitoreo remoto de pacientes y la telemedicina, hasta los equipos hospitalarios inteligentes y los dispositivos portátiles de diagnóstico, el IoMT se está consolidando como un elemento clave de la transformación digital en salud.

No obstante, esta creciente conectividad también ha incrementado de forma notable la exposición a ciberamenazas. Cada equipo médico, sensor o aplicación conectada representa un potencial punto de acceso para ataques capaces de comprometer información clínica confidencial, alterar el funcionamiento de dispositivos críticos o incluso afectar la seguridad física de los pacientes. Los entornos sanitarios, cada vez más dependientes de sistemas digitales interconectados, enfrentan riesgos que trascienden lo tecnológico, con impactos directos en la privacidad, la seguridad operativa y la continuidad de los servicios asistenciales.

En este escenario, la ciberseguridad del IoMT se ha convertido en un componente esencial para mantener la confianza en los sistemas de salud digital, garantizar la disponibilidad de los servicios médicos y proteger tanto los datos como la integridad de los pacientes. La gestión de estos desafíos demanda un enfoque integral que combine innovación tecnológica segura, marcos regulatorios sólidos, formación continua del personal sanitario y una colaboración estrecha entre instituciones públicas, privadas y organismos normativos.

2. Objetivo y alcance

2.1. Objetivo

La presente guía tiene como finalidad ofrecer una visión estructurada, actual y práctica sobre los retos, amenazas y tendencias en materia de ciberseguridad del IoMT (Internet of Medical Things) en el ámbito sanitario. Además, busca servir como base para el diseño y la actualización de políticas, estrategias y procedimientos orientados a fortalecer la seguridad digital en entornos clínicos y hospitalarios.

A través del estudio de las superficies de ataque, los riesgos técnicos y operativos, así como del análisis de los marcos regulatorios y normativos aplicables al sector salud, esta guía se propone:

- Identificar las principales vulnerabilidades y amenazas en los ecosistemas IoMT.
- Analizar los desafíos de interoperabilidad, gobernanza y responsabilidad compartida entre los diferentes actores del entorno sanitario.
- Revisar los estándares internacionales, normativas y buenas prácticas relacionadas con la seguridad de dispositivos médicos conectados.
- Ofrecer recomendaciones orientadas a mejorar la protección, resiliencia y confianza en los sistemas de salud digital.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

De este modo, la guía pretende constituirse como una herramienta de apoyo para profesionales de ciberseguridad, responsables de tecnología médica, directivos hospitalarios, organismos reguladores y empresas del sector biomédico involucradas en el diseño, implementación y mantenimiento de infraestructuras médicas conectadas.

2.2. Alcance

El documento aborda los aspectos clave de la ciberseguridad asociados al uso, despliegue e integración de tecnologías IoMT en distintos entornos de atención médica, incluyendo hospitales, clínicas, laboratorios y dispositivos domésticos de monitoreo remoto.

Incluye el análisis de:

- Arquitecturas y componentes del ecosistema IoMT en entornos clínicos.
- Superficies de ataque y riesgos específicos de los sistemas médicos conectados.
- Amenazas técnicas, físicas y de privacidad que afectan a pacientes y personal sanitario.
- Retos de interoperabilidad, estandarización y cumplimiento regulatorio.
- Tendencias emergentes relacionadas con la inteligencia artificial, Edge computing y nuevas regulaciones internacionales en el ámbito sanitario.

2.3. Metodología

La elaboración de esta guía se fundamenta en una revisión exhaustiva de marcos regulatorios, estándares internacionales y documentos de referencia en materia de ciberseguridad, salud digital y dispositivos médicos conectados.

Asimismo, el trabajo se complementa con el análisis de casos reales, estudios de incidentes relevantes y revisiones de estrategias de ciberseguridad sanitaria desarrolladas por organismos públicos, instituciones médicas y agencias reguladoras en diferentes regiones.

El enfoque metodológico combina la identificación y evaluación de riesgos del IoMT con una perspectiva estratégica orientada a la resiliencia, la protección del paciente y la gobernanza sanitaria, buscando alinear los principios de seguridad digital con los objetivos de calidad asistencial, innovación y sostenibilidad del sistema de salud moderno.

3. Referencias normativas

El presente documento se sustenta en un marco regulador y técnico integral, que combina normativas legales, estándares internacionales y guías de buenas prácticas, con el objetivo de garantizar la alineación con las exigencias del sector sanitario, la protección de los datos de salud y la resiliencia de los entornos IoMT en hospitales, clínicas y servicios médicos conectados.

Estas referencias constituyen la base metodológica y conceptual sobre la cual se estructura la guía, asegurando su coherencia con las políticas europeas, nacionales e internacionales en materia de ciberseguridad, privacidad de datos médicos y seguridad de dispositivos sanitarios conectados.

- **Normativas**:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
- Reglamento (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a las medidas para asegurar un alto nivel común de ciberseguridad en la UE (en adelante, NIS2).
- Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro (en adelante, IVDR).
- Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios (en adelante, MDR).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD).
- Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).
- NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
- NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.

- **Estándares**:
  - IEC 60601-1, Requisitos generales para la seguridad básica y el rendimiento esencial de equipos electromédicos.
  - IEC 80001-1, Gestión de riesgos para redes TI que incorporan dispositivos médicos.
  - IEC 82304-1:2016, Requisitos para la seguridad y calidad de software de salud independiente
  - ISO 13485:2016, Sistemas de gestión de calidad para dispositivos médicos
  - ISO 14971:2019, Aplicación de una metodología de riesgos para dispositivos médicos.
  - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
  - ISO/IEC 27001, Gestión de la seguridad de la información.
  - ISO 27799, Seguridad de la información en salud.
  - ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
  - ISO 22301, Gestión de la continuidad de negocio.
  - ISO 81001, Normas relacionadas con la ingeniería de software para dispositivos médicos.

- **Guías**:
  - BSI TR-03161, Requerimientos de seguridad para aplicaciones de eHealth.
  - Cloud Security Alliance (CSA), Matriz de controles Cloud (CCM).
  - ENISA - Ciberseguridad y resiliencia para hospitales inteligentes.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
  - IMDRF-Principios y prácticas de ciberseguridad para la contratación de software y materiales de dispositivos médicos.
  - OWASP IoT y OWASP, Guías de auditorías técnicas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

4. Definiciones

Acrónimos	Definición
Ataque Man-In-The Middle	Técnica de interceptación en la que un atacante se sitúa entre dos partes que se comunican, capturando, modificando o redirigiendo la información sin que lo detecten.
API	Conjunto de reglas que permiten que programas se comuniquen entre sí (del inglés, Application Programming Interface).
Blockchain	Tecnología de registro distribuido que garantiza la integridad y trazabilidad de los datos sin necesidad de intermediarios.
Botnet	Red de dispositivos infectados con programas maliciosos que son controlados de forma remota por un atacante, sin que los usuarios lo sepan
Cloud Computing	Modelo de prestación de servicios que permite acceder a recursos a través de internet, sin necesidad de infraestructura física local.
Edge Computing	Modelo de procesamiento de datos que se realiza cerca del lugar donde se generan, en lugar de depender exclusivamente de centros de datos remotos.
EMI	Información médica digitalizada que puede incluir datos clínicos, diagnósticos y tratamientos (del inglés, Electronic Medical Information).
Dashboard	Interfaz visual que muestra datos clave de forma resumida y organizada para facilitar el análisis y la toma de decisiones
Data Poisoning	Ataque que manipula datos de entrenamiento de sistemas de IA para alterar su comportamiento.
DDoS	Intento malicioso de interrumpir el funcionamiento normal de un servidor sobrecargándolo con tráfico desde múltiples fuentes (del inglés, Distributed Denial of Service).
Device Spoofing	Técnica maliciosa en la que un atacante falsifica la identidad de un dispositivo para acceder a sistemas protegidos.
DICOM	Estándar para el manejo, almacenamiento y transmisión de imágenes médicas (del inglés, Digital Imaging and Communications in Medicine).
FHIR	Estándar moderno de HL7 para facilitar el intercambio de datos clínicos mediante APIs (del inglés, Fast Healthcare Interoperability Resources).
Firmware	Programa que está integrado directamente en el equipo físico de un dispositivo, controlando sus funciones básicas.
HCE	Registro electrónico completo de la historia clínica de un paciente, accesible por múltiples profesionales de salud (Historia Clínica Electrónica).
HIS	Sistema integral para gestionar aspectos administrativos, clínicos y financieros de un hospital (del inglés, Hospital Information System),
HL7	Conjunto de estándares para el intercambio electrónico de información clínica entre sistemas de salud (del inglés, Health Level Seven).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Acrónimos	Definición
JTAG	Estándar usado para probar, programar y depurar circuitos integrados directamente desde sus pines (del inglés, Joint Test Action Group).
PACS	Sistema para almacenar, recuperar y compartir imágenes médicas como radiografías y resonancias (del inglés, Picture Archiving and Communication System).
LIMS	Sistema para gestionar muestras, datos y procesos en laboratorios clínicos (del inglés, Laboratory Information Management System).
LPWAN	Tecnología de comunicación inalámbrica de largo alcance entre dispositivos con bajo consumo energético (del inglés, Low Power Wide Area Network).
Ransomware	Programa malicioso que bloquea el acceso a sistemas o archivos y exige un pago para restaurarlo.
RIS	Sistema para gestionar datos e imágenes en departamentos de radiología (del inglés, Radiology Information System).
Smart Contracts	Programas autoejecutables en blockchain que cumplen automáticamente los términos de un contrato.
SOC	Centro especializado en monitorear, prevenir y responder a incidentes de ciberseguridad (del inglés, Security Operations Center).
UART	Protocolo de comunicación que transmite datos bit a bit sin necesidad de una señal de reloj (del inglés, Universal Asynchronous Receiver-Transmitter).
USB	Tipo de conexión física que permite transferir daros entre dispositivos (del inglés, Universal Serial Bus).
Zero Trust	Modelo de seguridad que no confía en ningún usuario o dispositivo por defecto, incluso dentro de la red interna.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Ecosistema de Salud Digital y el IoMT

El concepto de entornos de salud inteligente se basa en la integración de tecnologías digitales, dispositivos médicos conectados, sistemas de comunicación y análisis de datos para optimizar la atención clínica, mejorar la eficiencia operativa de los centros sanitarios y garantizar una atención más personalizada y segura para los pacientes.

En este contexto, el Internet de las Cosas Médicas (IoMT) actúa como el sistema nervioso de la salud digital, proporcionando la infraestructura necesaria para la recolección, transmisión y procesamiento continuo de información procedente de dispositivos médicos, sensores biométricos y plataformas de telemedicina. La combinación de IoMT, inteligencia artificial, computación en la nube y edge computing permite la creación de ecosistemas sanitarios más autónomos, predictivos y conectados, capaces de anticipar riesgos clínicos, optimizar recursos y mejorar la experiencia del paciente.

No obstante, esta interdependencia tecnológica genera nuevos vectores de riesgo y exposición, que requieren un enfoque de ciberseguridad integral, adaptativo y centrado en la gestión de riesgos clínicos y de privacidad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

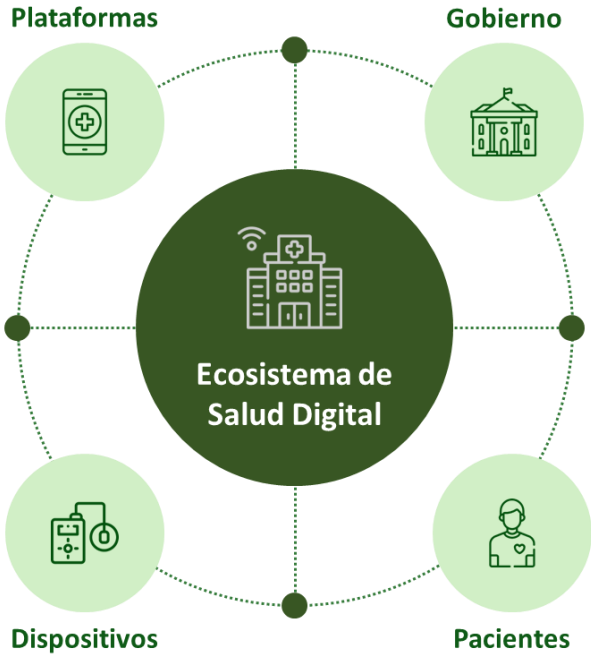

ILUSTRACIÓN 1: ECOSISTEMA DE SALUD DIGITAL

5.1. Entornos de salud inteligente

Los entornos de salud inteligente incluyen hospitales, clínicas, laboratorios y dispositivos portátiles de monitoreo remoto. Se caracterizan por la integración de tecnología digital en áreas como:

- Gestión hospitalaria y logística clínica.
- Monitoreo remoto de pacientes y telemedicina.
- Seguridad del paciente y control de dispositivos médicos conectados.
- Administración de datos clínicos y soporte a la toma de decisiones.
- Optimización de recursos energéticos y sostenibilidad en instalaciones sanitarias.

El éxito de estos entornos no depende únicamente de la tecnología, sino también de la gobernanza clínica, la coordinación entre departamentos y niveles administrativos, y la confianza en la infraestructura tecnológica que soporta la atención médica.

5.2. IoT en el ámbito sanitario (IoMT)

El IoMT constituye la base tecnológica que permite conectar dispositivos médicos físicos, sensores biométricos, equipos de diagnóstico y aplicaciones de salud móvil a redes de comunicación seguras, posibilitando la recolección y análisis de datos clínicos en tiempo real.

Entre las aplicaciones más relevantes del IoMT en entornos sanitarios destacan:

- Monitorización de pacientes: dispositivos portátiles y sensores de signos vitales conectados para seguimiento continuo.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Equipos médicos inteligentes: bombas de infusión, ventiladores y otros dispositivos conectados con sistemas de supervisión centralizada.
- Gestión hospitalaria: control de inventario, trazabilidad de medicamentos y optimización de recursos.
- Telemedicina y atención remota: consultas virtuales, análisis de datos a distancia y plataformas de soporte a la decisión clínica.
- Seguridad y alertas clínicas: sistemas de detección temprana de eventos adversos, alarmas automatizadas y análisis predictivo de riesgos para pacientes.

La presencia de dispositivos heterogéneos y distribuidos plantea desafíos importantes en ciberseguridad, interoperabilidad y mantenimiento, especialmente cuando estos sistemas manejan información sensible o forman parte de infraestructuras críticas de atención médica.

5.3. Interconectividad y dependencias entre sistemas sanitarios

El ecosistema IoMT funciona como una red compleja e interdependiente, donde la información fluye entre distintos sistemas clínicos, administrativos y tecnológicos. Entre las principales capas y dependencias destacan:

- Infraestructura de comunicaciones: redes 5G, Wi-Fi, LPWAN y conexiones seguras para telemedicina.
- Capas de procesamiento de datos: Edge computing y cloud computing para el análisis de información distribuida.
- Plataformas de integración sanitaria: sistemas que recopilan y correlacionan datos de múltiples dispositivos y aplicaciones clínicas.
- Sistemas de análisis y decisión clínica: inteligencia artificial, aprendizaje automático y modelos predictivos para soporte al diagnóstico y prevención de riesgos.
- Capas de gestión y supervisión: dashboards y herramientas de control remoto para la operación y seguridad de los servicios sanitarios.

Esta interconexión, aunque clave para la eficiencia y la innovación clínica, aumenta la superficie de ataque y la propagación de incidentes. Un fallo o vulnerabilidad en un subsistema puede afectar a otros servicios clínicos, lo que resalta la necesidad de arquitecturas seguras, segmentadas y resilientes desde la fase de diseño.

6. Superficie de ataques y riesgos asociados

Este apartado describe la arquitectura del IoMT en entornos sanitarios, identifica los puntos críticos de exposición que amplían la superficie de ataque y analiza los principales riesgos asociados a la interconexión de los sistemas médicos conectados.

El objetivo es ofrecer una visión integral de cómo la complejidad, heterogeneidad y dependencia tecnológica influyen directamente en la seguridad de la información clínica y en la capacidad de respuesta ante incidentes en hospitales, clínicas y dispositivos de atención remota.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

6.1. Arquitectura del IoMT

La arquitectura del IoMT puede representarse como una estructura de capas funcionales, que van desde los dispositivos médicos hasta las plataformas centralizadas de gestión y análisis clínico. Cada capa cumple un rol específico y presenta vulnerabilidades particulares, que deben abordarse siguiendo el principio de seguridad desde el diseño.

A continuación, se presentan cinco capas funcionales del IoMT, que interactúan entre sí: percepción, red o comunicación, procesamiento y análisis, aplicación, y gobierno y gestión.

Cada una contribuye al funcionamiento integral del ecosistema sanitario conectado, pero también introduce riesgos específicos que requieren medidas de seguridad adaptadas a entornos médicos.

ILUSTRACIÓN 2: ARQUITECTURA IOMT

6.1.1. Capa de percepción

Esta capa está formada por los dispositivos físicos que captan datos del entorno o del propio paciente, actuando como punto de conexión entre el mundo real y los sistemas digitales del IoMT.

Incluye diferentes tipologías de dispositivos:

- Sensores portátiles como monitores de frecuencia cardíaca o medidores de glucosa en sangre.
- Dispositivos implantables, tales como marcapasos o implantes cocleares, utilizados para la supervisión de parámetros fisiológicos.
- Equipos médicos en sitio, como resonadores magnéticos, tomógrafos, máquinas de rayos X, ventiladores o equipos de diálisis.
- Dispositivos actuadores, como las bombas de insulina. Encargadas de administrar medicamentos de manera automatizada.

Algunos dispositivos tienen únicamente funciones de medición, mientras que otros combinan sensorización y actuación. La interoperabilidad entre ellos permite que un mismo paciente utilice varios sensores y actuadores que trabajan de forma coordinada para cumplir una función específica.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Estos dispositivos son los más cercanos al entorno físico del paciente y, a la vez, constituyen el frente de exposición más amplio, dada su gran cantidad y diversidad.

Riesgos: manipulación física, suplantación de identidad, firmware inseguro, falta de actualizaciones, contraseñas por defecto, fallos en calibración que comprometan la seguridad clínica.

En particular, la suplantación de identidad puede manifestarse mediante spoofing de datos biométricos o imitación de sensores para que el sistema interprete lecturas falsas como reales. Esto podría derivar en la asignación incorrecta de datos clínicos, activación de alarmas erróneas o decisiones terapéuticas equivocadas. Asimismo, se podrían dar escenarios en los que un sensor legítimo se coloca en otra persona, comprometiendo la autenticidad de la información clínica del paciente.

6.1.2. Capa de red o comunicación

Los datos recopilados por los sensores se envían a esta capa mediante protocolos de comunicación inalámbrica, como Bluetooth Low Energy, ZigBee o Wi-Fi, o protocolos cableados como Ethernet.

Esta capa actúa como intermediario entre los dispositivos y los sistemas de procesamiento, que pueden encontrarse tanto en infraestructuras locales (estaciones clínicas o pasarelas médicas) como en plataformas en la nube, especialmente en el caso de dispositivos implantables o de monitorización remota. Para ello, utiliza equipos con mayor capacidad de procesamiento, tales como teléfonos inteligentes, unidades de control corporal (BCU) o puntos de acceso dedicados.

Sus funciones principales incluyen la conversión de protocolos, el filtrado y agregación de datos, así como la aplicación de medidas de seguridad, tales como encriptación y desencriptación, antes de transmitir la información.

Riesgos: intercepción de datos clínicos, ataques Man-in-the-Middle (MitM), denegación de servicio (DDoS), explotación de protocolos inseguros o configuraciones erróneas.

6.1.3. Capa de procesamiento y análisis

La información procesada en la capa de pasarela se transmite a infraestructuras locales, como servidores hospitalarios o sistemas de gestión clínica, o bien a plataformas en la nube, mediante tecnologías de comunicación móvil como redes 4G o 5G.

Cabe señalar que esta capa no necesariamente debe operar en una nube pública, ya que también puede implementarse como una nube privada o un servidor local dentro de la infraestructura sanitaria.

Esta capa está compuesta por servidores y sistemas de procesamiento administrados por los proveedores de servicios de salud o por proveedores especializados, los cuales constituyen el núcleo del IoMT. Su función principal es almacenar, proteger y analizar grandes volúmenes de datos biomédicos.

Además, permite el acceso remoto y seguro a la información tanto para los profesionales de la salud como para los pacientes.

Entre sus tareas clave destacan:

- Gestión segura de los datos, mediante cifrado y autenticación, para proteger los registros médicos electrónicos (HCE).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Análisis avanzado, que puede incluir técnicas de aprendizaje automático, análisis predictivo o minería de datos, orientadas a detectar tendencias, anomalías o patrones relevantes en la salud del paciente.

Riesgos: brechas de datos de pacientes, configuraciones inseguras en la nube, exposición de APIs, acceso no autorizado a plataformas de análisis clínico.

6.1.4. Capa de aplicación

Esta capa alberga las aplicaciones e interfaces de usuario. Su propósito es presentar los datos analizados de manera comprensible y útil para facilitar la toma de decisiones clínicas.

Los médicos pueden acceder a paneles de control con métricas de salud, tendencias y alertas, mientras que los pacientes reciben informes simplificados o notificaciones a través de aplicaciones móviles.

Por ejemplo, una aplicación de telemedicina puede mostrar un resumen diario de los signos vitales de un paciente junto con las recomendaciones médicas correspondientes.

Riesgos: explotación de vulnerabilidades de software, inyección de código, escalada de privilegios, errores en la autenticación o control de acceso, fallos en la integración de datos entre plataformas médicas.

6.1.5. Capa de gobierno y gestión

Comprende las políticas de seguridad de la información clínica, modelos de interoperabilidad, auditorías y responsabilidades compartidas entre centros sanitarios, proveedores, personal sanitario y organismos reguladores.

Riesgos: ausencia de segregación de responsabilidades, deficiencias de coordinación en la respuesta a incidentes, debilidades en la gestión del ciclo de vida de los dispositivos, incumplimiento de normativas de protección de datos.

6.2. Flujo de trabajo extremo a extremo del IoMT en un entorno hospitalario

Para ilustrar el funcionamiento integral del IoMT, se presenta a continuación un ejemplo práctico dentro de un entorno hospitalario. Consideremos el caso de un paciente en tratamiento por diabetes y problemas cardíacos, cuya atención médica se apoya en distintos dispositivos, sistemas y capas del IoMT.

- **Capa de percepción**

En esta primera capa, diversos dispositivos IoMT recopilan en tiempo real los datos fisiológicos del paciente. Un monitor continuo de glucosa, mide el nivel de glucosa en sangre cada cinco minutos y transmite los resultados a una aplicación móvil.

Simultáneamente, un marcapasos controla y regula el ritmo cardíaco, enviando periódicamente la información al sistema del hospital.

Otros equipos, como una máquina de resonancia magnética, se utilizan para evaluar posibles daños cardíacos derivados de complicaciones diabéticas, mientras que un equipo de rayos X puede emplearse para examinar el estado pulmonar u otras afecciones torácicas relacionadas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- **Capa de red o comunicación**

Los datos recopilados por los distintos dispositivos portátiles, implantables y de diagnóstico se envían a sus respectivas pasarelas para un procesamiento intermedio.

El monitor de glucosa transmite la información mediante Bluetooth al teléfono del paciente, que actúa como nodo central, agregando los datos y enviándolos a través de la red móvil al servidor del fabricante del dispositivo.

El marcapasos, por su parte, se conecta a una unidad de control corporal dedicada, que transmite de manera segura la información cardíaca a la red del hospital.

Los equipos de resonancia magnética y rayos X transfieren imágenes de gran tamaño mediante Ethernet hacia el servidor PACS (del inglés, Picture Archiving and Communication System) del hospital.

- **Capa de procesamiento y análisis**

Los datos del paciente pueden gestionarse dentro de la infraestructura privada del hospital o en un servidor en la nube.

Las imágenes de alta resolución se almacenan en el servidor PACS utilizando el formato DICOM (del inglés, Digital Imaging and Communications in Medicine).

El sistema de registros médicos electrónicos (HCE) integra toda la información del paciente, como imágenes, datos de sensores portátiles e implantables, en un expediente médico unificado.

El análisis de estos datos puede realizarse tanto por profesionales médicos como mediante herramientas de software especializadas, y, en algunos casos, con algoritmos de inteligencia artificial. Estos algoritmos permiten, por ejemplo, apoyar a los profesionales detectando anomalías en los tejidos cardíacos o identificando posibles signos de cardiomiopatía diabética a partir de las imágenes médicas

- **Capa de aplicación**

Los resultados procesados se presentan en formatos comprensibles y útiles para los distintos usuarios del sistema.

El personal médico accede a un panel de control integrado con los sistemas EHR y PACS, donde se visualizan tendencias de frecuencia cardíaca, niveles de glucosa y alertas por irregularidades.

El servidor PACS muestra imágenes de alta resolución con anotaciones generadas por IA, como zonas con daño tisular.

El sistema también puede predecir eventos de riesgo, como hiperglucemias o arritmias inminentes, facilitando ajustes tempranos en el tratamiento.

El paciente visualiza reportes simplificados desde su aplicación móvil, con resúmenes diarios de glucosa, recomendaciones dietéticas, notificaciones sobre alteraciones cardíacas y sugerencias de seguimiento médico.

Finalmente, los administradores del hospital utilizan paneles de supervisión para gestionar el estado de los dispositivos médicos, monitorizar pacientes y optimizar el uso de recursos.

- **Capa de gobierno y gestión**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

El hospital aplica políticas de seguridad y privacidad, basadas en estándares como ISO/IEC 27001 o ISO/IEC 80001, y define roles y responsabilidades entre el personal médico, los técnicos de TI y los fabricantes de dispositivos.

Por ejemplo, el departamento de TI se encarga de la auditoría de los accesos al servidor PACS, mientras que el equipo clínico valida la veracidad de los datos en el EHR.

Los proveedores externos deben cumplir acuerdos de nivel de servicio que aseguren la disponibilidad de las plataformas en la nube y la respuesta ante incidentes de ciberseguridad.

Asimismo, los organismos reguladores pueden acceder a los registros de trazabilidad del sistema para verificar el cumplimiento de las normativas sanitarias y la gestión del ciclo de vida de los dispositivos.

6.3. Diferencias de IoMT con un dispositivo médico

Antes de clasificar los diversos dispositivos IoMT, resulta relevante diferenciar el propio concepto de IoMT del de dispositivo médico, dado que suelen confundirse. Aclarar esta distinción permite comprender mejor el alcance del IoMT dentro del ecosistema sanitario conectado.

El IoMT se refiere a un ecosistema de dispositivos médicos interconectados, sistemas clínicos y plataformas digitales que permiten el intercambio de datos de salud entre sistemas, la monitorización remota de pacientes y la coordinación de múltiples servicios clínicos, incluyendo el soporte a la telemedicina y la atención a distancia. Su principal objetivo es integrar información y servicios para optimizar la atención sanitaria de manera conectada y eficiente.

En cambio, un dispositivo médico es un equipo individual diseñado para cumplir funciones clínicas concretas, como medir, monitorizar, diagnosticar o tratar a un paciente. Aunque algunos dispositivos médicos incorporan algoritmos de control o funciones digitales avanzadas, su propósito principal sigue siendo prestar directamente una función sanitaria específica. Un dispositivo médico solo forma parte del IoMT cuando está conectado a otros sistemas y participa dentro de un ecosistema interoperable de atención médica.

Un ejemplo típico en un entorno hospitalario, como el descrito anteriormente, es una bomba de infusión, la cual sigue siendo un dispositivo médico por su función de administrar insulina según las necesidades del paciente. Sin embargo, cuando esta bomba se conecta a un sistema central o a plataformas de monitorización remota, pasa a formar parte del IoMT, integrándose en un conjunto de dispositivos que permiten la supervisión y gestión de la atención a distancia. De este modo, aunque ambos conceptos pueden superponerse en ciertas circunstancias, IoMT se refiere al ecosistema conectado, mientras que el dispositivo médico es el equipo individual con una función clínica definida

La diferencia fundamental entre IoMT y un dispositivo médico radica, por tanto, en el alcance y la conectividad. Mientras un dispositivo médico opera de forma individual y cumple una función sanitaria específica, el IoMT integra múltiples dispositivos y sistemas para facilitar el flujo de información, la coordinación de servicios y la atención remota dentro de un ecosistema sanitario más amplio.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Aspectos	Dispositivos médicos	IoMT
Arquitectura	Equipos clínicos individuales	Ecosistema conectado de dispositivos y sistemas independientes
Objetivo principal	Control y monitorización en tiempo real de una tarea específica	Gestión y coordinación de múltiples servicios y datos de salud
Ejemplo práctico	Bomba de infusión	Red de salud inteligente con monitores de glucosa, marcapasos y telemedicina

TABLA 2: DIFERENCIAS ENTRE IOMT Y DISPOSITIVOS MÉDICOS.

6.4. Clasificación de los dispositivos médicos conectados

El ecosistema IoMT abarca una amplia variedad de dispositivos médicos conectados, con distintos niveles de complejidad, interacción con el paciente y criticidad clínica. Para establecer un marco coherente de gestión del riesgo y priorización de medidas de ciberseguridad, resulta fundamental considerar la clasificación establecida por el Reglamento (UE) 2017/745 sobre los productos sanitarios (MDR).

Esta clasificación define las obligaciones del fabricante, el grado de evaluación de conformidad y las medidas de seguridad que deben implementarse según el nivel de riesgo que el dispositivo representa para la salud del paciente. En el caso de los dispositivos conectados, esta categorización tiene una correlación directa con la exposición a ataques, ya que los equipos de mayor riesgo clínico suelen depender de sistemas de software, conectividad remota o integración en redes hospitalarias críticas.

El MDR clasifica los dispositivos médicos en cuatro categorías principales:

- **Clase I – Dispositivos de bajo riesgo**

Dispositivos médicos que no entran en contacto con el paciente o que lo hacen únicamente con la piel intacta, así como aquellos que penetran en el cuerpo a través de un orificio durante menos de 60 minutos. Se trata, por tanto, de dispositivos no invasivos o de contacto superficial, orientados principalmente al seguimiento general de parámetros fisiológicos o al bienestar del paciente. En el ámbito del IoMT, esta categoría abarca monitores portátiles, termómetros digitales o básculas inteligentes conectadas

Aunque el impacto clínico directo es bajo, su volumen de uso y conectividad con aplicaciones móviles o plataformas en la nube los convierten en vectores potenciales de exposición de datos personales y credenciales. La principal prioridad de ciberseguridad se centra en la protección de la privacidad, la autenticación de usuarios y el control de actualizaciones seguras.

- **Clase IIa – Dispositivos de riesgo moderado**

Dispositivos que se introducen en el cuerpo a través de un orificio corporal o mediante procedimientos quirúrgicos, sin estar destinados a permanecer en él, así como aquellos que suministran energía o sustancias al organismo o modifican procesos fisiológicos, siempre que dicha acción no se realice de forma potencialmente peligrosa. Al mantener una interacción más directa con el paciente, un fallo en su

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

funcionamiento podría provocar lesiones leves o moderadas. Ejemplos comunes son monitores de glucosa conectados, tensiómetros inteligentes, sistemas de diagnóstico remoto o equipos de fisioterapia digitalizados.

En esta categoría, la ciberseguridad adquiere mayor relevancia debido a la integración de software médico y la transmisión de datos clínicos sensibles.

- **Clase IIb – Dispositivos de riesgo alto**

Equipos que se introducen de forma invasiva, ya sea de manera temporal o permanente, con una clara aplicación sanitaria, incluidos aquellos que administran sustancias o energía de manera potencialmente peligrosa. Por este motivo, al asistir o sostener funciones fisiológicas vitales, su mal funcionamiento podría causar daños graves. Ejemplos son bombas de infusión inteligentes, ventiladores conectados, equipos de monitorización intensiva o implantes activos con comunicación inalámbrica.

Estos sistemas suelen operar en entornos clínicos críticos y están expuestos a redes hospitalarias heterogéneas o plataformas de gestión centralizadas. Por su relevancia operativa, requieren un enfoque de seguridad desde el diseño, mecanismos de segregación de red, autenticación de dispositivos, integridad del firmware y capas redundantes de seguridad para garantizar la continuidad asistencial.

- **Clase III – Dispositivos de riesgo crítico**

Productos destinados a entrar en contacto con el sistema nervioso central o el sistema circulatorio central, ya sea para administrar una terapia o establecer un diagnóstico, así como aquellos que contienen sustancias medicinales, se absorben completamente o incorporan materiales de origen animal.

Estos dispositivos representan el nivel más alto de riesgo clínico, al tener una función terapéutica directa o requerir implantación en el cuerpo humano. En el ámbito del IoMT, se incluyen marcapasos y desfibriladores implantables conectados, sistemas de asistencia ventricular, neuroestimuladores o implantes ortopédicos inteligentes. Por este motivo, combinan riesgos clínicos y de seguridad extremos, ya que una intrusión o manipulación podría comprometer directamente la salud o la vida del paciente, lo cual exige protocolos de ciberseguridad y pruebas de penetración específicas.

En resumen, la siguiente tabla sintetiza la clasificación de los dispositivos médicos conectados conforme al MDR, indicando su nivel de riesgo, descripción general y ejemplos prácticos.

Clase	Riesgo	Descripción	Ejemplos prácticos
I	Bajo	No invasivos o contacto superficial, penetran <60 min o sólo piel intacta	Monitores de actividad física portátiles, termómetros digitales, básculas inteligentes conectadas

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Clase	Riesgo	Descripción	Ejemplos prácticos
IIa	Medio	Introducción temporal en el cuerpo o modificación de procesos fisiológicos no peligrosa	Monitores de glucosa conectados, tensiómetros inteligentes, sistemas de diagnóstico remoto de bajo riesgo, equipos de fisioterapia digital
IIb	Alto	Invasivos temporales o permanentes, administran energía o sustancias potencialmente peligrosas o sostienen funciones vitales	Bombas de insulina implantables, ventiladores conectados de soporte, sensores implantables de monitorización continua de parámetros vitales no críticos, catéteres o stents inteligentes con comunicación inalámbrica
III	Crítico	Contacto con sistema nervioso o circulatorio central, terapéutico directo, implantación	Marcapasos, desfibriladores automáticos implantables, sistemas de asistencia ventricular, neuroestimuladores, implantes ortopédicos inteligentes con función terapéutica crítica

TABLA 3: CLASIFICACIÓN DISPOSITIVO MÉDICOS SEGÚN MDR

6.5. Puntos críticos de exposición

La superficie de ataque en los entornos IoMT es especialmente amplia y heterogénea, la coexistencia de dispositivos clínicos conectados, redes hospitalarias complejas y plataformas distribuidas de procesamiento genera múltiples puntos de exposición que pueden ser aprovechados por agentes maliciosos o incidentes no intencionados.

Estos puntos críticos no se limitan a los equipos médicos, sino que abarcan todo el ciclo de vida del dispositivo y los sistemas que lo soportan, desde su desarrollo y despliegue hasta su operación y retirada.

A continuación, se identifican las principales áreas de exposición que deben considerarse en el diseño y gestión de entornos IoMT seguros:

- **Dispositivos médicos conectados**

Muchos dispositivos clínicos conectados fueron concebidos con prioridad en su funcionalidad terapéutica o diagnóstica, sin incorporar medidas de seguridad desde el diseño.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

La presencia de firmware desactualizado, credenciales por defecto o ausencia de cifrado en las comunicaciones los convierte en un vector de entrada crítico. Asimismo, su accesibilidad física en entornos hospitalarios o domiciliarios incrementa la posibilidad de manipulación o acceso no autorizado.

- **Gestión del ciclo de vida**

La ausencia de políticas de gestión integral del ciclo de vida de los dispositivos médicos conectados es una de las causas más frecuentes de exposición. En muchos centros sanitarios, los equipos permanecen operativos durante años sin un inventario actualizado, sin registro de firmware ni procedimientos de retirada segura.

Esto genera entornos donde coexisten dispositivos antiguos, sin soporte de seguridad, junto a nuevos sistemas conectados, aumentando el riesgo de explotación y dificultando la trazabilidad de los mismos.

Una gestión adecuada del ciclo de vida debe contemplar la incorporación, mantenimiento, actualización, auditoría y retirada controlada de cada dispositivo, garantizando la seguridad en todas las etapas de su vida útil.

- **Integración con sistemas heredados**

El entorno sanitario es uno de los más propensos a mantener dispositivos y sistemas operativos obsoletos por razones de compatibilidad clínica o coste operativo. Muchos equipos críticos siguen dependiendo de versiones antiguas de software o protocolos sin soporte, lo que impide aplicar parches de seguridad.

La integración de estos sistemas heredados con nuevas plataformas IoMT amplía la superficie de ataque, pudiendo facilitar movimientos laterales dentro de la red hospitalaria. Este escenario exige aplicar medidas compensatorias, como la segmentación de red, la virtualización o el aislamiento de servicios obsoletos.

- **Cadena de suministro**

El ecosistema IoMT involucra una red compleja de fabricantes, integradores, proveedores de software, servicios en la nube y personal técnico de mantenimiento. Esta diversidad de actores genera una cadena de suministro extensa y difícil de controlar.

Las vulnerabilidades pueden introducirse durante el desarrollo, distribución o actualización de los dispositivos, especialmente si no existen controles de verificación de integridad o validación de firmware. Asimismo, el uso de bibliotecas de software de terceros sin validación o de componentes sin trazabilidad puede comprometer la seguridad del sistema global.

Por ello, es esencial establecer mecanismos de auditoría y certificación continua de proveedores, implementar listas de materiales de software (SBOM) y exigir transparencia sobre las actualizaciones y el soporte de ciberseguridad.

- **Redes clínicas y conectividad entre sistemas**

Las redes hospitalarias integran dispositivos médicos, sistemas clínicos y servicios administrativos en entornos donde coexisten múltiples tecnologías, como Wi-Fi, Bluetooth, ZigBee y 5G, con distintos niveles de seguridad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

La falta de segmentación, cifrado o control de acceso adecuado puede facilitar interceptaciones de datos, suplantaciones de identidad o interrupciones en servicios críticos.

Además, los sistemas sanitarios, como laboratorio, radiología o historia clínica electrónica, se comunican mediante estándares de interoperabilidad, como HL7, DICOM o FHIR, que no incluyen seguridad nativa, lo que puede permitir accesos indebidos o propagación de incidentes entre plataformas.

El diseño de redes clínicas debe apoyarse en modelos de arquitectura segura, con segmentación lógica, monitorización continua y políticas de acceso mínimo.

- **Plataformas de gestión y procesamiento**

Las plataformas de procesamiento, tanto en la nube como de integración clínica, constituyen el núcleo operativo de los servicios IoMT al permitir el almacenamiento, análisis y correlación de grandes volúmenes de datos médicos. No obstante, su complejidad y exposición las convierten en un objetivo prioritario para los ciberatacantes.

Errores de configuración en servidores, contenedores o APIs pueden provocar accesos no autorizados o la exposición pública de datos sensibles. Asimismo, la falta de cifrado extremo a extremo o de autenticación fuerte en las conexiones entre dispositivos y plataformas incrementa la vulnerabilidad.

Es indispensable aplicar principios de Zero Trust, segmentar entornos de desarrollo y producción, y reforzar la supervisión de integraciones con sistemas hospitalarios, como HIS, PACS o EHR.

- **Entornos de telemedicina y monitorización remota**

El despliegue de servicios de teleasistencia y monitorización de pacientes fuera del entorno hospitalario amplía notablemente el perímetro del IoMT. Los dispositivos domésticos o portátiles suelen conectarse mediante redes Wi-Fi inseguras o mediante aplicaciones móviles que no siempre cumplen con las normativas sanitarias.

La falta de control sobre el entorno de conexión y la veracidad de los datos transmitidos puede afectar tanto la calidad asistencial como la privacidad del paciente. Es esencial garantizar que las soluciones de telemedicina utilicen canales cifrados, autenticación de dispositivos y aplicaciones verificadas, además de políticas de concienciación para pacientes y cuidadores.

- **Estaciones clínicas y terminales de acceso**

Las estaciones clínicas, terminales de diagnóstico y consolas de control suelen ser compartidas por múltiples profesionales en turnos continuos. La ausencia de control sobre las sesiones activas o de autenticación multifactor puede dar lugar a accesos indebidos o a la exposición de información sensible.

Es fundamental establecer políticas de cierre automático de sesión, registro de actividad y autenticación reforzada, garantizando que el acceso a los datos clínicos se limite estrictamente a usuarios autorizados y en contextos legítimos.

- **Datos clínicos y privacidad del paciente**

Los entornos IoMT procesan datos altamente sensibles, como historiales clínicos, constantes vitales, imágenes médicas y registros de tratamientos. Cualquier filtración, alteración o pérdida de esta información puede tener consecuencias legales, reputacionales y, en casos graves, clínicas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

El cumplimiento de las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales (LOPDGDD), requiere aplicar medidas de cifrado, anonimización y control estricto de acceso. La trazabilidad y la gestión del consentimiento deben ser principios centrales en todo tratamiento de información sanitaria.

- **Factor humano**

El personal sanitario y técnico desempeña un papel esencial en la seguridad del entorno IoMT. Sin embargo, la presión asistencial y la prioridad de la atención clínica sobre la seguridad pueden derivar en comportamientos que comprometan la seguridad del paciente, como el uso de credenciales compartidas, la conexión de dispositivos personales o la desactivación de controles de seguridad.

Fomentar una cultura de seguridad centrada en el paciente, ofrecer formación continua y establecer políticas claras de uso tecnológico son medidas fundamentales para fortalecer la resiliencia organizativa.

6.6. Riesgos asociados

Los riesgos derivados de la exposición de los sistemas IoMT se manifiestan en múltiples dimensiones, que abarcan desde vulnerabilidades técnicas hasta impactos organizativos y estratégicos sobre la calidad asistencial, la privacidad de los pacientes y la resiliencia del sistema sanitario.

Debido a la naturaleza crítica de los dispositivos médicos conectados, cualquier incidente puede tener consecuencias no solo digitales, sino también clínicas y humanas.

A continuación, se presentan las principales categorías de riesgo que afectan a los entornos IoMT, clasificadas en tres dimensiones: técnica, operativa y estratégica.

ILUSTRACIÓN 3: RIESGOS DE CIBERSEGURIDAD EN IOMT

6.6.1. Riesgos técnicos

Los riesgos técnicos en el entorno IoMT se derivan principalmente de vulnerabilidades en los componentes físicos, lógicos y de comunicación que conforman los dispositivos médicos conectados. Su explotación puede comprometer la disponibilidad, integridad y confidencialidad de los datos clínicos, además de afectar directamente la seguridad del paciente.

Entre los más relevantes se incluyen:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Vulnerabilidades en firmware y software médico: muchos dispositivos operan con sistemas embebidos propietarios o versiones antiguas que no admiten actualizaciones, prolongando la exposición a fallos conocidos y limitando la aplicación de parches de seguridad.
- Protocolos de comunicación inseguros: el uso de estándares sin cifrado o autenticación robusta, como HL7 v2, Bluetooth clásico o Wi-Fi abierto, facilita la interceptación o manipulación de datos médicos en tránsito.
- Autenticación débil y gestión deficiente de credenciales: el uso de contraseñas por defecto, ausencia de autenticación multifactor o cuentas compartidas permite accesos no autorizados a consolas clínicas y equipos críticos.
- Infección por malware o ransomware: el software malicioso diseñado para entornos hospitalarios puede cifrar datos, alterar parámetros de tratamiento o dejar inoperativos sistemas esenciales, afectando la atención directa al paciente.
- Compromiso en la cadena de suministro: actualizaciones de firmware adulteradas, bibliotecas externas vulnerables o componentes falsificados pueden introducir puertas traseras en equipos médicos certificados.
- Manipulación o suplantación de dispositivos (device spoofing): la falsificación o sustitución de sensores, actuadores o módulos de comunicación permite inyectar datos clínicos falsos o alterar el comportamiento del dispositivo, con el consiguiente riesgo de diagnósticos erróneos o terapias inadecuadas.

6.6.2. Riesgos operativos

Los riesgos operativos en el ecosistema IoMT afectan directamente la continuidad asistencial, la interoperabilidad de los sistemas clínicos y la fiabilidad de la información médica. En entornos hospitalarios, donde la disponibilidad y precisión pueden determinar la vida del paciente, estos riesgos adquieren una criticidad especial.

Entre los más frecuentes destacan:

- Interrupción de servicios clínicos esenciales: fallos técnicos o ciberataques sobre dispositivos conectados, como respiradores, bombas de infusión o monitores de signos vitales, pueden paralizar la actividad asistencial y obligar a recurrir a procedimientos manuales de emergencia.
- Alteración o pérdida de datos clínicos: la corrupción, eliminación o manipulación de historiales médicos y registros terapéuticos puede generar diagnósticos erróneos, retrasos en tratamientos y riesgos directos para el paciente.
- Falta de interoperabilidad segura: la coexistencia de equipos de distintos fabricantes y generaciones puede provocar incompatibilidades y vulnerabilidades derivadas del uso de protocolos inseguros o no estandarizados.
- Propagación de incidentes en redes no segmentadas: la ausencia de aislamiento entre redes médicas, administrativas y de telemedicina facilita la expansión de malware o ataques DDoS hacia sistemas críticos.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Dependencia de servicios externos o en la nube: la externalización de funciones clínicas, como almacenamiento de imágenes, diagnóstico remoto, telemonitorización, incrementa la exposición ante fallos de proveedores o interrupciones de conectividad.
- Errores humanos y gestión inadecuada del ciclo de vida: la falta de protocolos claros para la instalación, mantenimiento o retirada de dispositivos conectados puede derivar en configuraciones inseguras o en la permanencia de equipos vulnerables en red.
- Ausencia de monitorización y respuesta ante incidentes: muchos hospitales carecen de sistemas SOC especializados o de capacidades de detección de anomalías en redes clínicas, lo que dificulta la detección y respuesta frente a ataques.

6.6.3. Riesgos estratégicos

Los riesgos estratégicos en el entorno IoMT trascienden el plano técnico y operativo, afectando a la gobernanza sanitaria, la confianza institucional y la sostenibilidad del sistema de salud digital. Aunque su impacto suele manifestarse a largo plazo, sus consecuencias pueden ser críticas para la continuidad asistencial y la credibilidad del sector.

Entre los más relevantes destacan:

- Compromiso de la seguridad del paciente: cualquier manipulación, indisponibilidad o fallo en un dispositivo médico conectado puede derivar en consecuencias clínicas directas, desde la alteración de tratamientos hasta daños físicos. Este riesgo requiere una coordinación estrecha entre ingeniería clínica y ciberseguridad.
- Pérdida de confianza del personal sanitario y los pacientes: los incidentes de seguridad o filtraciones de datos clínicos pueden erosionar la confianza en la digitalización hospitalaria y ralentizar la adopción de tecnologías conectadas y servicios de telemedicina.
- Impacto reputacional e institucional: una brecha en sistemas IoMT puede afectar gravemente la imagen de hospitales, fabricantes y organismos públicos, generando consecuencias legales, económicas y sociales de gran alcance.
- Incertidumbre jurídica y responsabilidades compartidas: la compleja relación entre hospitales, fabricantes, proveedores tecnológicos y reguladores puede generar vacíos legales ante incidentes. La ausencia de acuerdos de responsabilidad o cumplimiento de normativas como el RGPD, MDR o NIS2 agrava el riesgo.
- Uso indebido de datos clínicos: la explotación de información clínica para fines no autorizados, como el entrenamiento de modelos de inteligencia artificial o estudios comerciales, supone un riesgo ético y de cumplimiento normativo significativo.
- Dependencia tecnológica y ausencia de soberanía digital: la concentración de infraestructuras y servicios en plataformas externas o nubes fuera de la Unión Europea puede comprometer la soberanía de los datos sanitarios y la continuidad operativa ante crisis geopolíticas o regulatorias.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

7. Amenazas de ciberseguridad en IoMT

La Internet de las Cosas Médicas (IoMT) ha transformado el ecosistema sanitario al conectar dispositivos, sistemas clínicos y aplicaciones de diagnóstico o tratamiento en tiempo real. Esta conectividad permite mejorar la atención al paciente, optimizar los procesos hospitalarios y favorecer la medicina preventiva mediante el análisis continuo de datos clínicos.

Sin embargo, esta interconexión también amplía la superficie de ataque del entorno sanitario. Los dispositivos médicos suelen estar limitados en recursos de procesamiento, utilizan sistemas operativos propietarios o versiones antiguas de software, y dependen de redes heterogéneas donde la interoperabilidad prima sobre la seguridad.

Además, su ciclo de vida prolongado y la necesidad de certificación regulatoria dificultan la actualización o sustitución de equipos comprometidos.

Las amenazas en el IoMT pueden clasificarse en tres grandes categorías, técnicas, físicas y de privacidad clínica, todas ellas interrelacionadas y con un impacto directo no solo sobre la infraestructura tecnológica, sino también sobre la seguridad del paciente y la confidencialidad de los datos clínicos.

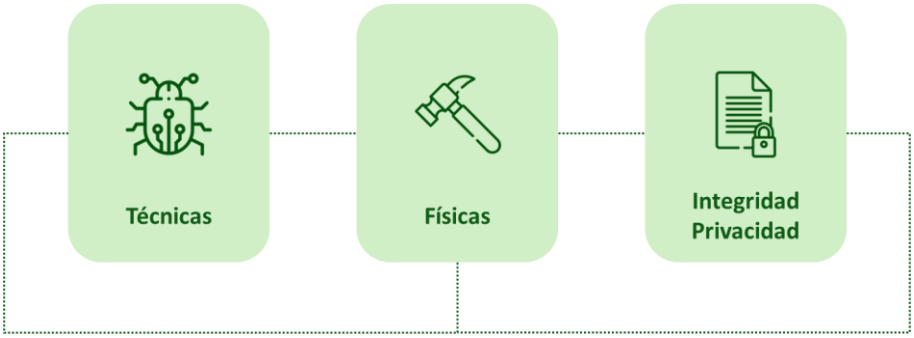

ILUSTRACIÓN 4: CATEGORÍAS DE AMENAZAS IOMT

7.1. Amenazas técnicas

Las amenazas técnicas constituyen el núcleo de los riesgos en el entorno IoMT, ya que afectan directamente al funcionamiento de los dispositivos médicos conectados, sistemas de información hospitalarios y plataformas clínicas en la nube.

Un ciberataque exitoso puede provocar la alteración de datos médicos, el mal funcionamiento de un equipo terapéutico o el acceso no autorizado a información sensible del paciente.

7.1.1. Amenazas relacionadas con el software médico

El software es el elemento más crítico de los dispositivos IoMT, por ello pueden ser objeto de ataques que comprometan su funcionamiento, la integridad de los datos clínicos o la seguridad del paciente. Estas amenazas se materializan cuando un atacante logra explotar debilidades en el software de los dispositivos, sistemas hospitalarios o plataformas clínicas

Las limitaciones en desarrollo seguro, la dependencia de software heredado y la dificultad de actualización por requisitos regulatorios crean un entorno propenso a fallos.

Entre las condiciones que facilitan la materialización de estas amenazas destacan:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Sistemas operativos desactualizados: Muchos dispositivos operan con versiones antiguas de sistemas embebidos, sin soporte ni parches de seguridad.
- Firmware no validado: La ausencia de firma digital permite la suplantación o manipulación de dispositivos.
- Credenciales por defecto o gestión insegura de usuarios: Facilitan accesos no autorizados y privilegios indebidos.
- Errores de validación de datos: Fallos en la gestión de parámetros clínicos pueden alterar tratamientos o alarmas.
- Integración insegura con sistemas hospitalarios: APIs de HIS, PACS o EHR sin autenticación robusta exponen datos clínicos críticos.

Un fallo en un dispositivo IoMT no solo compromete la información médica, sino que puede afectar directamente a la efectividad terapéutica o poner en riesgo la vida del paciente.

7.1.2. Ataque sobre credenciales o autenticación clínica

La autenticación débil en dispositivos o plataformas médicas es uno de los vectores más explotados.

Muchos equipos permiten acceso remoto sin control multifactor, contraseñas por defecto o mecanismos inseguros de gestión de usuarios.

Entre los ataques más comunes:

- Fuerza bruta o diccionario sobre ~~sobre~~ cuentas administrativas.
- Ingeniería social o phishing clínico, suplantando a personal sanitario o soporte técnico.
- Reutilización de credenciales entre equipos médicos y sistemas administrativos.

El compromiso de una cuenta privilegiada puede permitir la modificación de parámetros terapéuticos, la desactivación de alarmas o la manipulación de historiales clínicos.

7.1.3. Amenazas derivadas de la exposición a redes hospitalarias o Internet

Muchos dispositivos IoMT permanecen conectados permanentemente a redes hospitalarias o incluso a Internet para mantenimiento o monitorización remota.

La exposición de estos equipos sin medidas de segmentación ni cifrado los convierte en objetivos potenciales para los ciberatacantes.

Potenciales amenazas:

- Acceso no autorizado a monitores, bombas de infusión o sistemas de telemedicina.
- Integración de dispositivos en botnets médicas.
- Robo o filtración de datos clínicos sensibles.
- Alteración de parámetros críticos en tiempo real, afectando la atención clínica.

La exposición no controlada puede permitir la integración de estos equipos en botnets médicas, el robo de datos clínicos o la alteración de parámetros críticos en tiempo real.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

7.1.4. Ataques de denegación de servicio (DDoS)

Un ataque de denegación de servicio contra un sistema médico conectado puede tener consecuencias graves, impidiendo el acceso a historiales electrónicos, retrasando diagnósticos o bloqueando la comunicación entre equipos vitales.

Ejemplos de impacto:

- Bloqueo de comunicación entre dispositivos vitales y plataformas de control.
- Interrupción de sistemas de monitorización en UCI o quirófanos conectados.
- Saturación de redes médicas por tráfico malicioso procedente de equipos comprometidos.

La interrupción de servicios puede afectar directamente a la atención clínica y poner en riesgo al paciente.

7.1.5. Integración con otras redes y sistemas clínicos

Los entornos IoMT se comunican con numerosos sistemas hospitalarios, como HIS, RIS, PACS, EHR o LIMS, lo que amplía los vectores de ataque.

Entre las condiciones que facilitan la materialización de estas amenazas destacan:

- Protocolos médicos sin cifrar, como DICOM, HL7 o MQTT en versiones insegura.
- Falta de segmentación entre redes médicas y redes administrativas.
- Pasarelas o servidores intermedios con configuraciones inseguras.
- Ataques de repetición o manipulación de datos clínicos en tránsito.

Una brecha en cualquiera de estos sistemas puede propagarse rápidamente, afectando a la totalidad de la infraestructura clínica y la atención al paciente.

7.2. Amenazas físicas

Las amenazas físicas se refieren a cualquier ataque o manipulación que comprometa un dispositivo IoMT a nivel de hardware o entorno físico. A diferencia de las amenazas técnicas, que se dirigen al software, credenciales o redes, las amenazas físicas aprovechan el acceso directo o indirecto al dispositivo para alterar su funcionamiento, extraer información sensible o causar daño al paciente.

Estos riesgos son especialmente relevantes en entornos sanitarios, donde los dispositivos médicos conectados suelen estar expuestos o bajo un control físico limitado. Equipos como monitores de signos vitales, bombas de infusión, marcapasos, desfibriladores implantables, respiradores o sistemas de gestión hospitalaria en red pueden ser vulnerables a ataques o manipulaciones indebidas.

La seguridad física adquiere así un papel esencial dentro de la ciberseguridad en IoMT, ya que un atacante con acceso directo a un dispositivo médico puede eludir las medidas de protección, alterar el firmware, clonar dispositivos o incluso comprometer la seguridad del paciente y la continuidad de los servicios clínicos críticos.

7.2.1. Acceso físico o manipulación directa

Muchos dispositivos IoMT se encuentran en entornos de fácil acceso, como habitaciones de hospital, ambulancias o domicilios.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Un atacante podría:

- Conectarse a puertos de mantenimiento, como USB, UART o JTAG, para extraer firmware o datos clínicos.
- Alterar calibraciones o parámetros de tratamiento.
- Sustituir dispositivos legítimos por clones maliciosos.

La manipulación directa puede provocar fallos clínicos, exposición de datos o riesgos para la salud del paciente.

7.2.2. Ataques a nivel de hardware

Incluyen la manipulación o sustitución de componentes, chips o módulos de comunicación:

- Inserción de firmware malicioso en procesos de mantenimiento o reparación.
- Clonación o sustitución de sensores biomédicos.
- Ataques de canal lateral, como medición de consumo energético o radiación, para extraer claves criptográficas).
- Interferencia electromagnética (EMI) sobre equipos de diagnóstico o implantes.

Estos ataques permiten comprometer dispositivos sin necesidad de acceso remoto, afectando tanto la funcionalidad como la seguridad del paciente.

7.2.3. Manipulación durante la cadena de suministro

Los dispositivos IoMT pueden verse comprometidos antes de su despliegue:

- Introducción de puertas traseras o componentes falsificados en la fabricación o transporte.
- Riesgo crítico en implantes conectados o sistemas de soporte vital, donde la detección de modificaciones no autorizadas es muy compleja.

La integridad de la cadena de suministro es esencial para garantizar la confiabilidad y seguridad de los dispositivos médicos desde su origen.

7.3. Amenazas a la integridad y privacidad de los datos clínicos

La privacidad de los datos generados, transmitidos y almacenados por los dispositivos IoMT constituye uno de los retos más críticos en el ámbito de la ciberseguridad. Estos dispositivos operan constantemente en contacto con el entorno físico y con los pacientes, recopilando información clínica.

Un fallo de seguridad puede exponer información de salud personal, comprometer diagnósticos o facilitar la manipulación de tratamientos.

7.3.1. Robo y filtración de datos clínicos

Los historiales médicos electrónicos, imágenes diagnósticas o parámetros fisiológicos son altamente valiosos.

Los atacantes pueden:

- Acceder a bases de datos de pacientes.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Filtrar o exponer información médica en el mercado negro.
- Utilizarla para chantaje, fraude o suplantación de identidad.

Una brecha de privacidad puede generar consecuencias legales, reputacionales y clínicas graves.

7.3.2. Intercepción o alteración de datos biomédicos

Los ataques Man-in-the-Middle sobre comunicaciones entre sensores, monitores o plataformas pueden permitir:

- Espionaje de datos en tiempo real, como signos vitales o tratamientos.
- Inyección de valores falsos o alterados, como ritmo cardíaco o nivel de glucosa.
- Desincronización de sistemas clínicos, afectando a diagnósticos automáticos o alarmas médicas.

La alteración de la información en tránsito puede comprometer decisiones clínicas y poner en riesgo la salud del paciente.

7.3.3. Manipulación o pérdida de integridad de la información

La integridad de los datos médicos es fundamental para garantizar decisiones clínicas seguras. La manipulación o corrupción de registros, dosis de medicación, resultados de pruebas o parámetros fisiológicos puede provocar diagnósticos incorrectos, tratamientos inapropiados y riesgos directos para la salud del paciente.

Esta amenaza afecta tanto a la seguridad del paciente como a la confiabilidad general del sistema de atención médica.

7.3.4. Amenazas en la nube médica y plataformas de telemedicina

El uso de soluciones en la nube y aplicaciones móviles amplía la superficie de ataque de los sistemas IoMT.

Condiciones que facilitan la materialización de amenazas:

- Configuraciones inseguras de bases de datos públicas.
- Aplicaciones móviles sin cifrado de datos locales o en tránsito.
- Dependencia de proveedores externos sin auditoría de cumplimiento.

La protección de entornos en la nube y de telemedicina es clave para mantener confidencialidad, integridad y disponibilidad de la información clínica.

8. Retos de ciberseguridad IoMT

Aunque el IoMT comparte principios tecnológicos con los dispositivos médicos, su naturaleza interconectada, su capacidad de procesar información de manera distribuida en tiempo real y su estrecha vinculación con la seguridad del paciente plantean retos únicos en materia de ciberseguridad y privacidad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

A diferencia de un dispositivo médico individual, que opera de forma autónoma y cumple funciones clínicas específicas, los dispositivos IoMT funcionan dentro de redes heterogéneas y descentralizadas, donde conviven equipos clínicamente certificados, como resonancias magnéticas o marcapasos, con dispositivos de consumo, como relojes inteligentes o monitores personales. En hospitales de gran tamaño, se estima que existen miles de dispositivos IoMT activos simultáneamente, lo que amplía de forma significativa la superficie de ataque y convierte tanto los dispositivos médicos conectados como los datos de los pacientes en objetivos de alto valor para los atacantes.

Garantizar una ciberseguridad sólida en entornos IoMT resulta mucho más complejo que en sistemas informáticos convencionales. Las medidas de seguridad no solo deben proteger la confidencialidad de la información médica, sino también mantener la disponibilidad y funcionalidad de los dispositivos que sostienen la vida del paciente. La interoperabilidad entre equipos clínicos certificados y dispositivos de consumo introduce vulnerabilidades adicionales, como por ejemplo, una brecha en un dispositivo doméstico puede traducirse en un riesgo directo sobre un equipo médico conectado al mismo entorno.

A continuación se resumen los principales retos de ciberseguridad específicos del IoMT, que reflejan el equilibrio necesario entre seguridad, usabilidad y seguridad clínica:

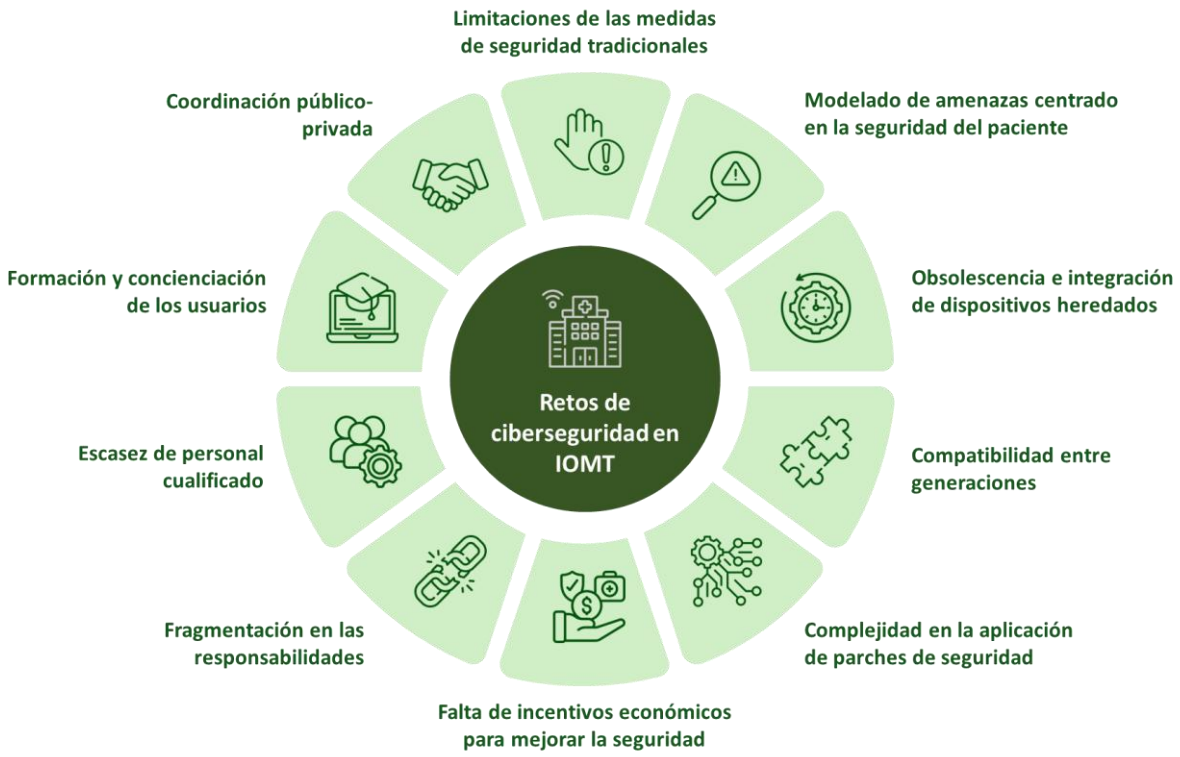

ILUSTRACIÓN 5: RETOS DE CIBERSEGURIDAD EN IOMT

8.1. Limitaciones de las medidas de seguridad tradicionales

Los mecanismos de autenticación convencionales, como contraseñas o biometría, pueden resultar ineficaces o incluso peligrosos en entornos clínicos debido a que exigir contraseñas en un respirador durante una emergencia puede retrasar una intervención crítica, los sistemas biométricos fallan en quirófanos por el uso de guantes y mascarillas, y muchos pacientes con limitaciones motrices o visuales encuentran difícil introducir credenciales complejas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

La ciberseguridad en el IoMT debe, por tanto, integrarse de forma natural en los flujos clínicos, priorizando la inmediatez de la atención sin comprometer la protección de los sistemas.

8.2. Modelado de amenazas centrado en la seguridad del paciente

El análisis de riesgos en el IoMT difiere sustancialmente del aplicado a fallos mecánicos o eléctricos. Mientras que un error físico suele ser inmediato y fácilmente detectable, una amenaza de ciberseguridad puede generar efectos diferidos, difíciles de identificar o incluso invisibles para los sistemas de monitoreo. Por ejemplo, un ataque de ransomware en un ventilador podría bloquear sus controles sin emitir alertas, o un actor malicioso podría manipular imágenes de resonancia magnética, conduciendo a diagnósticos clínicos erróneos.

Estas particularidades hacen necesario un enfoque de modelado de amenazas centrado en la seguridad del paciente, que contemple tanto los riesgos técnicos como sus implicaciones clínicas, y que fomente la colaboración activa entre fabricantes, hospitales y especialistas en ciberseguridad.

8.3. Obsolescencia e integración de dispositivos heredados

Numerosos dispositivos médicos continúan en uso durante décadas, incluso después de haber superado su periodo oficial de soporte por parte del fabricante. El alto coste de sustitución, junto con los complejos procesos de certificación regulatoria, lleva a muchos hospitales a prolongar su vida útil mediante servicios de mantenimiento externos. Sin embargo, estos proveedores suelen carecer de acceso a actualizaciones de firmware, parches de seguridad o soporte técnico oficial, lo que deja a los equipos expuestos a vulnerabilidades conocidas.

Además, algunos de estos dispositivos fueron concebidos originalmente para operar de forma local o en entornos aislados, sin capacidades nativas de conexión ni medidas de protección digital. Su incorporación posterior a redes hospitalarias mediante módulos inalámbricos o adaptadores externos amplía significativamente los vectores de ataque, ya que dichos equipos no disponen de recursos para gestionar claves criptográficas, autenticar conexiones o ejecutar cifrados modernos.

La combinación de obsolescencia tecnológica y conectividad convierte a estos dispositivos heredados en uno de los puntos más débiles del ecosistema IoMT. Para mitigar estos riesgos, es esencial implementar estrategias de gestión del ciclo de vida, segmentación de red y aislamiento por hardware, donde módulos específicos controlen la seguridad de las comunicaciones de forma independiente a las funciones clínicas.

De lo contrario, la dependencia de equipos obsoletos seguirá representando un riesgo estructural para la continuidad asistencial y la seguridad del paciente.

8.4. Compatibilidad entre generaciones

Los fabricantes de tecnología médica se enfrentan al desafío de mantener la compatibilidad entre los nuevos dispositivos y los modelos anteriores que continúan en uso clínico.

Esta necesidad de interoperabilidad, motivada por razones de continuidad asistencial y optimización de recursos, puede obligar a conservar canales de comunicación no cifrados o protocolos obsoletos para garantizar la conexión con equipos antiguos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Sin embargo, esta práctica debilita la seguridad global del ecosistema sanitario, ya que un único dispositivo legado con vulnerabilidades conocidas puede comprometer la integridad de toda la red hospitalaria.

El dilema entre seguridad y compatibilidad se convierte así en un problema estructural ya que endurecer las medidas de protección puede impedir la interoperabilidad entre generaciones de dispositivos, mientras que mantener compatibilidad con tecnologías heredadas implica aceptar niveles de riesgo elevados.

Además, la coexistencia de múltiples versiones de hardware y software dificulta la gestión de parches, la verificación de integridad y la aplicación uniforme de políticas de ciberseguridad.

Como resultado, los fabricantes y los hospitales deben coordinar estrategias conjuntas de actualización y segmentación de red, estableciendo mecanismos que permitan una transición segura hacia dispositivos modernos, sin comprometer la operatividad clínica ni la seguridad del paciente.

8.5. Complejidad en la aplicación de parches de seguridad

A diferencia de los sistemas informáticos tradicionales, la actualización de un dispositivo médico no puede realizarse sin una evaluación clínica y técnica previa, ya que cualquier modificación del software o del firmware puede afectar directamente a la seguridad del paciente o a la eficacia terapéutica y diagnóstica del equipo.

Por esta razón, los parches de seguridad deben someterse a exhaustivas pruebas de validación y certificación antes de su implementación, lo que genera demoras significativas en su despliegue y prolonga la ventana de exposición frente a posibles ataques.

Asimismo, muchos dispositivos médicos, especialmente los de generaciones anteriores, no disponen de conexión directa a Internet ni de mecanismos para verificar la autenticidad e integridad de las actualizaciones, como firmas digitales o validación criptográfica. Esto obliga a que las actualizaciones se realicen mediante procedimientos manuales o semiautomáticos, a menudo con la intervención de personal técnico especializado y en horarios fuera del servicio clínico, para no interrumpir tratamientos en curso.

El proceso resulta, por tanto, lento, costoso y altamente dependiente de la coordinación entre fabricantes, hospitales y servicios de mantenimiento, lo que dificulta la aplicación oportuna de medidas de protección.

8.6. Falta de incentivos económicos para mejorar la seguridad

El mercado sanitario rara vez incentiva mejoras que aporten únicamente un refuerzo en la seguridad sin ofrecer beneficios clínicos tangibles.

Tanto los fabricantes como los centros hospitalarios tienden a priorizar las funcionalidades terapéuticas y diagnósticas frente a las inversiones en componentes o actualizaciones destinadas exclusivamente a la protección de seguridad.

Esta falta de incentivos económicos ralentiza la adopción de estándares avanzados de ciberseguridad y perpetúa la dependencia de infraestructuras obsoletas o vulnerables.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Además, el alto coste de certificación y validación regulatoria de los dispositivos médicos hace que la inclusión de mejoras de seguridad, como módulos criptográficos, autenticación reforzada o firmware seguro, se perciba como una carga económica adicional sin retorno inmediato.

Como consecuencia, la ciberseguridad se aborda a menudo de forma reactiva, tras la detección de incidentes o la aparición de nuevas normativas, en lugar de integrarse desde la fase de diseño bajo un enfoque de seguridad desde el diseño y por defecto.

8.7. Fragmentación en las responsabilidades

La responsabilidad sobre la ciberseguridad en entornos IoMT suele repartirse entre fabricantes, hospitales y proveedores externos, sin una delimitación clara de competencias.

Mientras los fabricantes se centran en el diseño y desarrollo de los dispositivos, los hospitales asumen su uso, mantenimiento y gestión operativa.

Esta falta de coordinación genera vacíos de seguridad y zonas grises de responsabilidad, donde un fallo, por ejemplo, en el control de accesos o la configuración de red, puede atribuirse indistintamente a cualquiera de las partes, dificultando una respuesta eficaz ante incidentes.

Resulta imprescindible establecer acuerdos y protocolos claros de gobernanza y comunicación que definan responsabilidades y garanticen una actuación conjunta y coherente frente a amenazas de ciberseguridad.

8.8. Escasez de personal cualificado

La rápida expansión de los entornos IoMT y la proliferación de dispositivos conectados han generado una demanda creciente de profesionales con competencias específicas en seguridad digital, redes, análisis de vulnerabilidades y gestión de incidentes. Sin embargo, la oferta de personal cualificado no crece al mismo ritmo que las necesidades del sector.

Esta brecha de talento se traduce en una dependencia excesiva de proveedores externos, retrasos en la detección de incidentes y dificultades para mantener actualizadas las infraestructuras críticas. En muchos casos, el personal médico o técnicos responsables de la gestión carecen del conocimiento necesario para aplicar políticas de ciberseguridad coherentes, supervisar contratos tecnológicos o evaluar el cumplimiento de normativas.

Para afrontar este desafío, resulta indispensable impulsar programas de formación especializada, incentivos a la contratación de expertos y alianzas con universidades, centros tecnológicos y organismos públicos. La creación de perfiles híbridos, capaces de comprender tanto los sistemas médicos como las implicaciones de ciberseguridad, será clave para garantizar la resiliencia de los hospitales inteligentes.

8.9. Formación y concienciación de los usuarios

La ciberseguridad en entornos IoMT no depende únicamente de la tecnología, sino también del comportamiento de las personas que interactúan con ella. La falta de concienciación y formación entre el personal médico, técnicos, empresas colaboradoras y los pacientes en general constituye un factor de riesgo crítico.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Los errores humanos, como el uso de contraseñas débiles, la falta de actualización de dispositivos o la conexión de equipos no autorizados, pueden comprometer la integridad de sistemas enteros. En este sentido, la formación continua y la educación digital son esenciales para fortalecer la primera línea de defensa frente a las amenazas.

Las administraciones deben promover campañas de sensibilización adaptadas a distintos públicos, como personal médico, proveedores y usuarios, combinadas con ejercicios de simulación y certificaciones profesionales. Fomentar una cultura de ciberseguridad sólida, donde la protección de los datos y la privacidad se perciban como una responsabilidad compartida, permitirá avanzar hacia un entorno IoMT más seguro y confiable.

8.10. Coordinación público-privada

La cooperación entre el sector público y el privado es un pilar esencial para la seguridad del IoMT. La ciberseguridad requiere un enfoque compartido, donde se facilite el intercambio de información sobre amenazas, vulnerabilidades e incidentes.

Además, deben definirse mecanismos de colaboración que incluyan protocolos conjuntos de respuesta, planes de contingencia y desarrollo de estándares comunes.

La falta de coordinación puede generar duplicidades, vacíos de protección o respuestas descoordinadas ante incidentes graves, afectando a la confianza y la resiliencia de los servicios médicos.

8.11. Consecuencias de no abordar los retos de ciberseguridad en IoMT

Si los retos identificados en entornos IoMT no se abordan de manera efectiva, las consecuencias pueden ser graves y de amplio alcance. En primer lugar, los pacientes pueden verse directamente afectados, ya que la manipulación, interrupción o inaccesibilidad de dispositivos médicos conectados puede conducir a diagnósticos erróneos, tratamientos inapropiados o incluso eventos críticos que comprometan su vida.

A nivel institucional, los centros sanitarios pueden enfrentar interrupciones en los servicios, pérdida de datos clínicos, exposición de información sensible y daños reputacionales significativos. La dependencia de sistemas obsoletos, la falta de formación del personal y la fragmentación de responsabilidades incrementan la probabilidad de incidentes y dificultan una respuesta rápida y coordinada ante ataques. Asimismo, la ausencia de medidas de seguridad adecuadas expone a los sistemas a ataques financieros, legales y regulatorios.

En conjunto, la falta de mitigación de estos retos incrementa de manera exponencial la superficie de ataque del ecosistema IoMT, afectando tanto la continuidad de los servicios de atención sanitaria como la confianza de los pacientes y de la sociedad en la capacidad del sistema de salud para operar de manera segura y confiable. Este panorama evidencia que abordar los retos de ciberseguridad no es únicamente una cuestión tecnológica, sino una prioridad estratégica para garantizar la seguridad clínica, la integridad de los datos y la resiliencia de la atención sanitaria.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

9. Casos reales

Tras haber detallado las amenazas y retos asociados a los sistemas IoMT, resulta fundamental analizar incidentes reales que ejemplifiquen cómo estas vulnerabilidades y desafíos se traducen en impactos concretos sobre los servicios médicos. El estudio de casos permite comprender mejor la naturaleza de los riesgos, identificar patrones de ataque y extraer lecciones útiles para fortalecer las estrategias de ciberseguridad.

En esta sección, los incidentes se presentan clasificados en tres categorías de impacto. Para cada categoría se incluyen dos casos reales en formato de tabla, lo que permite una visualización clara y comparativa de la fecha, ubicación, tipo de incidente, sistema afectado y consecuencias principales.

9.1. Filtración de datos

Los ataques de filtración de datos se producen cuando la información sensible generada o gestionada por los sistemas IoMT es expuesta de manera no autorizada. Esto puede incluir datos clínicos de ciudadanos, información de sensores o registros de operación de servicios críticos. Las filtraciones suelen originarse por vulnerabilidades en plataformas cloud, APIs inseguras, configuraciones incorrectas o falta de cifrado en la transmisión y almacenamiento de datos.

El impacto de este tipo de incidentes puede variar desde la pérdida de privacidad hasta riesgos legales, pérdida de confianza ciudadana y consecuencias económicas para la administración pública.

Filtración de datos en el Hospital Clínic de Barcelona	
Fecha	Marzo de 2023
Víctima	Hospital Clinic de Barcelona
Activo comprometido	Máquinas virtuales y sistemas críticos (laboratorios, farmacia, radiología, PACS, LIS)
Tipo de Amenaza	Ransomware y exfiltración de datos
Vector del ataque	Acceso remoto no autorizado
Origen del ataque	Atacantes desconocidos (publicación de datos en dark web y foros)
Impacto	Exposición de información de pacientes, profesionales y proveedores, filtración de archivos clínicos y administrativos, desvío masivo de pacientes a otros centros

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Filtración de datos en el Hospital Clínic de Barcelona	
Descripción	En marzo de 2023, el Hospital Clínic de Barcelona sufrió un ataque de ransomware que comprometió máquinas virtuales y sistemas críticos, incluidos laboratorios, farmacia y radiología. Los atacantes exfiltraron grandes volúmenes de datos, incluyendo información de pacientes, profesionales y proveedores, así como archivos clínicos y administrativos, y los publicaron posteriormente en foros delictivos. La exposición afectó directamente la confidencialidad y disponibilidad de información sensible, incluyendo historiales clínicos, resultados de laboratorio y registros de radiología vinculados al ecosistema IoMT (PACS, LIS). Esto generó un riesgo elevado para la seguridad de los pacientes y la continuidad de la atención médica, al impedir el acceso oportuno a datos críticos para el diagnóstico y tratamiento. El incidente también provocó el desvío masivo de pacientes a otros centros sanitarios, incluyendo pacientes oncológicos con tratamientos personalizados. En muchos casos, estos pacientes tuvieron que repetir pruebas diagnósticas para recalcular sus dosis, lo que incrementó los retrasos asistenciales y el riesgo clínico. La autoridad catalana de protección de datos (APDCAT) concluyó en 2024 que el hospital no aplicó medidas mínimas de seguridad, lo que llevó a la obligación de implementar acciones correctivas y reforzar la ciberseguridad en sus sistemas hospitalarios.

Servidores PACS/DICOM expuestos en varios países de la UE	
Fecha	Noviembre de 2019
Víctima	Hospitales y clínicas en Bulgaria, Francia, Hungría, Italia, España y Suiza (47 sistemas PACS identificados)
Activo comprometido	Servidores PACS/DICOM expuestos públicamente (sin autenticación ni cifrado)
Tipo de Amenaza	Exposición de datos clínicos
Vector del ataque	Acceso directo vía Internet a puertos DICOM y web viewers debido a configuraciones inseguras y ausencia de controles de acceso
Origen del ataque	Atacantes externos que explotan la exposición pública de servidores PACS/DICOM
Impacto	Exposición de más de 35 millones de imágenes médicas y 500.000 estudios con datos personales y de salud, riesgo de violación del RGPD y uso indebido de información médica

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Servidores PACS/DICOM expuestos en varios países de la UE	
Descripción	En septiembre de 2019, la empresa alemana Greenbone Networks realizó un análisis a gran escala de sistemas PACS (Picture Archiving and Communication Systems) y detectó cientos de servidores DICOM accesibles sin protección, muchos en hospitales europeos. El estudio identificó 47 sistemas en la Unión Europea, entre ellos en España, Francia, Hungría, Italia, Bulgaria y Suiza, que permitían listar, visualizar e incluso descargar imágenes médicas sin requerir autenticación. Estas imágenes incluían metadatos identificativos de pacientes y personal médico, lo que representa una grave infracción del RGPD. A pesar de las advertencias a las autoridades y centros implicados, en noviembre de 2019 aún 22 servidores seguían abiertos, exponiendo más de 16 millones de imágenes. Este incidente se considera uno de los primeros casos documentados a nivel europeo de exposición masiva de sistemas IoMT (DICOM/PACS), evidenciando vulnerabilidades estructurales en la gestión de infraestructura médica y la falta de medidas de seguridad básicas como segmentación de red, cifrado de comunicaciones y autenticación de usuarios.

9.2. Manipulación de sistemas

La manipulación de sistemas en el ámbito del IoMT se produce cuando un atacante altera el funcionamiento de dispositivos médicos conectados, comprometiendo no solo la prestación de los servicios asistenciales, sino también la seguridad del paciente y la integridad de los datos clínicos. Esto puede implicar modificaciones no autorizadas en monitores de constantes vitales, bombas de infusión, sistemas de telemetría o plataformas de teleasistencia.

Estos ataques suelen explotar contraseñas por defecto, vulnerabilidades en firmware o software y accesos remotos inseguros. Sus consecuencias incluyen errores clínicos, riesgo físico para los pacientes, pérdida de confianza y posibles interrupciones en la atención sanitaria.

Riesgo de manipulación remota en de bombas de insulina	
Fecha	Julio 2019
Víctima	Pacientes con bombas de insulina Medtronic MiniMed 508 y Minimed Paradigm
Activo comprometido	Bombas de insulina implantables o portátiles
Tipo de Amenaza	Vulnerabilidad de dispositivo y manipulación de terapia
Vector del ataque	Conexión inalámbrica RF cercana al dispositivo

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Riesgo de manipulación remota en de bombas de insulina	
Origen del ataque	Terceros no autorizados
Impacto potencial	Alteración de la dosis de insulina, con riesgo de hipoglucemia o hiperglucemia, consecuencias graves para la salud y posible riesgo vital en caso de explotación
Descripción	En julio de 2019, la agencia española de medicamentos y productos sanitarios (AEMPS) alertó sobre vulnerabilidades en las bombas de insulina Medtronic MiniMed 508 y MiniMed Paradigm. La causa del riesgo se debe a fallos en la comunicación inalámbrica RF que permitían a un atacante cercano conectarse al dispositivo y modificar parámetros o controlar la administración de insulina sin pasar por servidores hospitalarios ni redes clínicas. En este sentido, un tercero no autorizado podría alterar la terapia de un paciente, provocando hipoglucemia, hiperglucemia o consecuencias graves para la salud, incluso riesgos vitales en casos críticos. La exposición afectaba directamente a los pacientes y pone de relieve la vulnerabilidad de dispositivos IoMT que no dependen únicamente de redes centralizadas para su operación. Las autoridades recomendaron medidas de mitigación inmediatas como no emparejar las bombas con dispositivos de terceros, vigilar cualquier cambio no iniciado y contactar al proveedor si se sospecha manipulación.

Riesgo de manipulación de monitores y sistemas de telemetría	
Fecha	Enero 2020
Víctima	Hospitales y centros sanitarios a nivel global, incluido España, los cuales usan equipos GE HealthCare
Activo comprometido	Monitores y sistemas de telemetría central (ApexPro, CARESCAPE, CIC, Central Stations, B450/B650/B850)
Tipo de Amenaza	Manipulación de la monitorización del dispositivo
Vector del ataque	Explotación de vulnerabilidades (CVE 2020-6961 a 6966) en dispositivos y servidores
Origen del ataque	Atacantes remotos que acceden a la red hospitalaria
Impacto potencial	Manipulación de alarmas, cambios en el comportamiento de monitorización, parada de dispositivos y riesgo inmediato para la seguridad del paciente en caso de explotación

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Riesgo de manipulación de monitores y sistemas de telemetría	
Descripción	En 2020, el INCIBE emitió un aviso oficial sobre vulnerabilidades en productos de GE HealthCare utilizados para telemetría y monitorización central de pacientes en España y la Unión Europea. Los sistemas afectados incluían ApexPro, CARESCAPE, CIC, Central Stations y monitores B450/B650/B850. La causa del riesgo se relacionaba con fallos que permitían ejecución de código no autorizado, desactivación o modificación de alarmas y parada de los dispositivos de seguimiento. El impacto potencial era crítico, ya que un atacante que explotara estas vulnerabilidades podría manipular directamente los monitores de cabecera y los sistemas de telemetría, alterando alarmas o el comportamiento de monitorización, lo que podría comprometer la seguridad de los pacientes y retrasar la respuesta clínica ante eventos críticos. Inicialmente, no existían parches para todos los componentes, aumentando la exposición a riesgos en entornos hospitalarios. Como medidas de mitigación, se recomendaron segmentación de red, listas de control de acceso y reducción de la exposición a sistemas vulnerables, además de la publicación posterior de boletines de seguridad por parte del fabricante. Este incidente ilustra la importancia de la seguridad proactiva en dispositivos IoMT de cabecera y sus servidores, donde cualquier manipulación directa puede tener consecuencias inmediatas para la atención y seguridad del paciente.

9.3. Interrupción de servicios

Los ataques de interrupción de servicios en el ámbito del IoMT tienen como objetivo degradar o paralizar el funcionamiento de sistemas y dispositivos médicos conectados, afectando no solo la disponibilidad de los servicios asistenciales, sino también la continuidad operativa y la seguridad del entorno clínico. Pueden manifestarse mediante ataques DDoS, ransomware o fallos provocados por la interdependencia entre plataformas y sistemas hospitalarios.

Sus efectos incluyen la interrupción de servicios críticos, como la monitorización de pacientes o los sistemas de emergencia, así como riesgos para la seguridad de los pacientes y consecuencias operativas, económicas y reputacionales para las organizaciones sanitarias.

Ataque dirigido al Hospital Universitario de Düsseldorf	
Fecha	Septiembre 2020
Víctima	Hospital universitario de Düsseldorf (Alemania)
Activo comprometido	Sistemas TI hospitalarios e historiales médicos electrónicos

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Ataque dirigido al Hospital Universitario de Düsseldorf	
Tipo de Amenaza	Ransomware
Vector del ataque	Phishing
Origen del ataque	Cibercriminales (ransomware)
Impacto	Desvío de pacientes a otros hospitales, retraso en atención crítica y posible muerte de un paciente
Descripción	En septiembre de 2020, el hospital universitario de Düsseldorf sufrió un ataque de ransomware que paralizó sus sistemas informáticos y bloqueó el acceso a los historiales médicos electrónicos. La causa del incidente fue la infección de los sistemas hospitalarios por un ransomware, que cifró datos críticos y dejó inaccesibles los registros de pacientes, paralizando operaciones esenciales en el hospital. La interrupción obligó a desviar pacientes a otros centros hospitalarios y afectó la capacidad de los médicos para brindar atención de emergencia de manera oportuna. Entre los pacientes desplazados se encontraba una mujer en estado crítico que falleció antes de poder recibir tratamiento, lo que evidencia las graves consecuencias clínicas del ataque. La propagación del malware impactó múltiples áreas del hospital, incluidos departamentos de emergencia y quirófanos, generando retrasos en procedimientos y decisiones médicas. Este caso se considera un ejemplo significativo del riesgo que representan los ataques de ransomware en entornos IoMT, donde la indisponibilidad de sistemas críticos puede tener efectos directos sobre la seguridad y la vida de los pacientes.

Ransomware masivo a sistemas hospitalarios	
Fecha	Mayo de 2017
Víctima	National Health Service (Reino Unido) y otros proveedores de salud globales
Activo comprometido	Sistemas TI, registros médicos electrónicos y equipos médicos críticos
Tipo de Amenaza	Ransomware
Vector del ataque	Explotación de vulnerabilidad en el protocolo SMB

Ransomware masivo a sistemas hospitalarios	
Origen del ataque	Cibercriminales (WannaCry ransomware)
Impacto	Bloqueo de accesos a registros médicos, equipos médicos críticos inoperativos, cierre de unidades de emergencia e interrupción de atención médica
Descripción	En mayo de 2017, el National Health Service (NHS) del Reino Unido y numerosos proveedores de salud a nivel global se vieron gravemente afectados por el ataque de ransomware WannaCry. La amenaza se propagó rápidamente a través de vulnerabilidades en el protocolo SMB (del inglés, Server Message Block), afectando tanto sistemas informáticos como equipos médicos conectados, incluyendo máquinas críticas como resonancias magnéticas. El ataque bloqueó el acceso a los registros médicos electrónicos, lo que impidió a los médicos administrar tratamientos y medicamentos a los pacientes de manera adecuada. La presencia de dispositivos conectados y puertos abiertos en las redes hospitalarias amplificó la vulnerabilidad, permitiendo que el ransomware se propagara con rapidez por múltiples centros sanitarios. Como resultado, varias unidades de emergencia se vieron obligadas a cerrar temporalmente y se interrumpieron servicios clínicos esenciales, generando un impacto directo en la atención a pacientes. La combinación de sistemas antiguos, falta de parches y exposición a redes públicas contribuyó a la magnitud del incidente. Este ataque evidenció la fragilidad de los sistemas IoMT frente a amenazas y la necesidad de adoptar medidas de seguridad proactivas, como segmentación de red, actualización o parcheo regular de dispositivos, cifrado de comunicaciones y políticas de respuesta ante incidentes. WannaCry se convirtió en un ejemplo de cómo la interconexión de sistemas clínicos críticos y la falta de mantenimiento adecuado pueden derivar en consecuencias graves para la seguridad del paciente y la continuidad asistencial.

10. Marco regulatorio actual y necesidades futuras

El desarrollo IoMT está redefiniendo el modelo de atención sanitaria mediante la conexión de dispositivos médicos, sensores biométricos, relojes conectados y sistemas hospitalarios inteligentes. Esta red interconectada mejora la eficiencia clínica, facilita el diagnóstico remoto y potencia la medicina personalizada; sin embargo, también amplía la superficie de exposición a riesgos de seguridad y vulnerabilidades que pueden afectar directamente a la seguridad del paciente y a la confidencialidad de los datos médicos.

Por ello, la ciberseguridad se ha consolidado como un eje estratégico dentro de las políticas de salud digital y de las estrategias de transformación tecnológica del sector sanitario. La protección de los dispositivos médicos conectados requiere un marco regulatorio robusto que combine aspectos técnicos,

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

normativos y organizativos, garantizando tanto la fiabilidad operativa como el cumplimiento ético y legal de la gestión de la información clínica.

En este apartado se examinan las principales regulaciones, estándares internacionales y estrategias de ciberseguridad aplicables al IoMT, junto con las líneas de evolución normativa que buscan reforzar la confianza en la tecnología médica conectada y asegurar la continuidad asistencial frente a amenazas digitales emergentes.

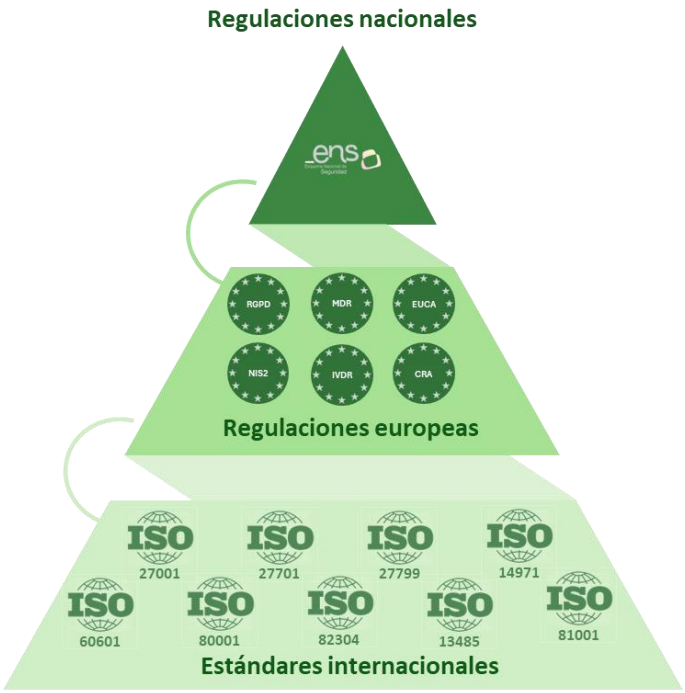

ILUSTRACIÓN 6: MARCO REGULATORIO IOMT

10.1. Estándares internacionales de ciberseguridad aplicables al IoMT

El marco normativo de la ciberseguridad en IoMT se apoya en un conjunto de estándares internacionales que establecen metodologías y requisitos para proteger la información clínica, los dispositivos médicos conectados y las infraestructuras sanitarias digitales.

Entre los principales estándares y guías de referencia destacan:

- IEC 60601-1: establece los requisitos esenciales de seguridad eléctrica y funcionamiento básico para los dispositivos electromédicos. Aunque su foco es la seguridad física, constituye el punto de partida para el cumplimiento integral en materia de seguridad del paciente y fiabilidad técnica.
- IEC 80001-1: establece las directrices para la gestión de riesgos en redes que integran dispositivos médicos, garantizando que la conectividad no comprometa la seguridad del paciente ni el rendimiento clínico.
- IEC 82304-1:2016: define requisitos de seguridad, calidad y fiabilidad para el software sanitario independiente, abarcando ciclo de vida, interoperabilidad y gestión de riesgos asociados a fallos o vulnerabilidades.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- ISO 13485:2016: define los requisitos para sistemas de gestión de calidad en la fabricación de dispositivos médicos, incluyendo procesos de diseño, producción, distribución y soporte postventa, con implicaciones directas sobre la seguridad y trazabilidad de los dispositivos conectados
- ISO 14971:2019: proporciona la metodología de referencia para la gestión de riesgos en dispositivos médicos, incorporando la identificación, evaluación y control de riesgos, incluidos aquellos asociados a amenazas de seguridad.
- ISO/IEC 27001: define los principios para la gestión de la seguridad de la información en todo tipo de organizaciones, incluidas las sanitarias, promoviendo un enfoque basado en la gestión del riesgo y la mejora continua.
- ISO/IEC 27701: extensión del estándar anterior, centrada en la privacidad y la protección de datos personales de pacientes, en conformidad con el RGPD y las normativas nacionales de protección de datos en salud.
- ISO 27799: complementa la norma ISO/IEC 27001 aplicando sus principios al ámbito sanitario. Define medidas de protección para la información médica, garantizando la confidencialidad, integridad y disponibilidad de los datos de salud frente a accesos no autorizados o pérdidas.
- ISO 81001: aborda de manera específica la ciberseguridad en el software sanitario y en los sistemas de información de salud, proporcionando requisitos de diseño seguro y de gestión del riesgo durante todo el ciclo de vida del producto.

No obstante, la mayor parte de las normas de carácter vinculante y de impacto directo sobre el ecosistema IoMT proceden del ámbito europeo, donde la Unión Europea y los Estados Miembros, incluido España, han impulsado reglamentos y directivas específicas que buscan unificar criterios, elevar el nivel de protección y definir responsabilidades claras entre fabricantes, operadores, administraciones públicas y proveedores tecnológicos.

10.2. Iniciativas europeas y nacionales sobre ciberseguridad en IoMT

Partiendo de los estándares internacionales descritos anteriormente, tanto la Unión Europea como los Estados miembros, incluido España, han desarrollado un conjunto de regulaciones destinadas a reforzar la ciberseguridad, la resiliencia y la confianza en los sistemas médicos conectados.

En el contexto de IoMT estas políticas adquieren una importancia crítica, ya que los dispositivos médicos, las plataformas de monitorización remota y los sistemas de historia clínica gestionan información altamente sensible y están directamente vinculados con la seguridad del paciente. La complejidad del ecosistema sanitario digital exige, por tanto, un marco normativo coordinado que abarque desde la fabricación y certificación de dispositivos hasta la protección de los datos personales y la gestión de incidentes.

10.2.1. Iniciativas Europeas

La Unión Europea ha desempeñado un papel determinante en la creación de un marco regulador común de ciberseguridad sanitaria, estableciendo normas y reglamentos orientados a proteger tanto los productos médicos conectados como las infraestructuras tecnológicas que los soportan.

- **Reglamento General de Protección de Datos (2016)**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

El Reglamento General de Protección de Datos de la Unión Europea (RGPD) regula el tratamiento y la protección de datos personales en todos los Estados miembros, asegurando que la información sensible sea procesada de manera legal, transparente y segura, protegiendo la privacidad y los derechos individuales.

En el contexto del IoMT, el RGPD adquiere especial relevancia, ya que los dispositivos médicos conectados recopilan grandes volúmenes de datos clínicos, biométricos e historiales médicos de pacientes, siendo de obligado cumplimiento para cualquier sistema sanitario conectado que gestione datos de ciudadanos europeos.

La aplicación del RGPD refuerza la confianza de los pacientes, la responsabilidad de los operadores y la resiliencia de las infraestructuras sanitarias digitales, constituyendo un pilar central en la gobernanza del ecosistema IoMT.

- **Reglamento sobre Dispositivos Médicos (2017)**

El Reglamento sobre Dispositivos Médicos (MDR) constituye la base regulatoria europea para los dispositivos médicos, incorporando obligaciones específicas en materia de seguridad, evaluación del riesgo y gestión del ciclo de vida del software sanitario. Asimismo clasifica los dispositivos según el riesgo (clases I, IIa, IIb y III), definiendo requisitos ~~los~~ técnicos y clínicos que deben cumplir para obtener el marcado CE, el cual no solo certifica sino que asigna obligaciones legales.

Concretamente sobre los fabricantes recae la responsabilidad de:

- Garantizar la protección del paciente frente a amenazas de seguridad.
- Asegurar la integridad y fiabilidad de los datos generados o transmitidos.
- Mantener documentación técnica que demuestre la integración de medidas de ciberseguridad durante todo el ciclo de vida del dispositivo, incluyendo la gestión de actualizaciones y vulnerabilidades.

- **Reglamento sobre Dispositivos Médicos de Diagnóstico In Vitro (2017)**

El Reglamento sobre Dispositivos Médicos de Diagnóstico In Vitro (IVDR) complementa al MDR, ampliando los requisitos de seguridad a los sistemas de diagnóstico in vitro conectado, los cuales también forman parte del ecosistema IoMT. Este reglamento exige a los fabricantes establecer procedimientos de gestión de riesgos, protección de datos y trazabilidad del software para asegurar la integridad de los resultados clínicos y la confidencialidad de la información.

- **EU Cybersecurity Act (2019)**

El EU Cybersecurity Act (EUCA), en vigor desde 2019, establece un marco europeo de certificación de ciberseguridad para productos, servicios y procesos digitales. Su objetivo es crear un sistema común y reconocido en toda la UE que garantice un nivel mínimo de seguridad y confianza en los productos conectados.

La norma también refuerza el papel de ENISA, otorgándole un mandato permanente y mayores competencias para coordinar políticas de ciberseguridad, fomentar la cooperación entre los Estados miembros y liderar la respuesta europea ante incidentes.

- **Directiva NIS2 (2022)**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

La Directiva NIS2 (del inglés, Network and Information Systems Directive), aprobada en 2022, actualiza la normativa europea sobre ciberseguridad y amplía su alcance respecto a la versión anterior.

Su propósito es reforzar la resiliencia de las infraestructuras críticas y los servicios esenciales frente a incidentes, imponiendo obligaciones de seguridad y notificación de incidentes tanto a entidades públicas como privadas.

Entre sus principales novedades destacan:

- Ampliación del ámbito de aplicación a sectores clave como energía, transporte, sanidad, agua, administración pública y servicios digitales.
- Obligación de gestión de riesgos, formación en ciberseguridad y comunicación temprana de incidentes graves.
- Refuerzo de la cooperación entre los Estados miembros y creación de un mecanismo europeo de respuesta coordinada ante incidentes.

La transposición de NIS2 a la legislación española está en curso, y su cumplimiento será esencial para el ecosistema IoMT, al involucrar tanto infraestructuras sanitarias como operadores tecnológicos.

- **EU Cyber Resilience Act (2024)**

El CRA de la Unión Europea (del inglés, EU Cyber Resilience Act) constituye uno de los avances normativos más importantes en materia de seguridad digital. Su objetivo es garantizar que todos los productos con elementos digitales, incluidos los dispositivos IoT, incorporen medidas de ciberseguridad desde su diseño y durante todo su ciclo de vida.

Entre sus principales objetivos se encuentran:

- Reducir la cantidad de vulnerabilidades presentes en los productos comercializados dentro de la UE.
- Asegurar que los fabricantes mantengan la responsabilidad de la seguridad de sus productos durante todo su ciclo de vida.
- Mejorar la transparencia sobre las características de ciberseguridad, permitiendo a los consumidores tomar decisiones informadas.
- Reforzar la trazabilidad en la cadena de suministro, exigiendo la documentación del software incorporado.
- Obligar a informar a la European Union Agency for Cybersecurity (ENISA) de los incidentes que afecten a la seguridad de los productos.

El CRA será de aplicación obligatoria a partir del 10 de diciembre de 2024 para todos los productos digitales comercializados en el mercado europeo.

10.2.2. Iniciativas nacionales

A nivel nacional, España ha consolidado en la última década un marco estratégico y normativo cada vez más robusto en materia de ciberseguridad, con el objetivo de alinear su política digital con las directrices europeas y las necesidades del ecosistema IoMT. Estas iniciativas buscan no solo proteger las

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

infraestructuras críticas, sino también fomentar una cultura de seguridad que abarque a ciudadanos, empresas y administraciones públicas.

- **Ley Protección de Infraestructuras Críticas (2011)**

La Ley 8/2011 para la Protección de Infraestructuras Críticas (LPIC), junto con su desarrollo reglamentario mediante el Real Decreto 704/2011, constituye el pilar de la protección de las infraestructuras críticas nacionales.

Esta norma establece los mecanismos de coordinación entre el sector público y privado para proteger los servicios esenciales frente a ataques o incidentes graves.

Con la proliferación del IoT y la interconexión de los sistemas urbanos, los servicios sanitarios se consideran operadores críticos o esenciales, por lo que deben alinearse con las obligaciones de la Ley PIC, incluyendo la elaboración de Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE).

- **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (2018)**

La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), adapta y desarrolla en España los principios del RGPD, incluyendo obligaciones concretas para administraciones públicas, empresas y operadores de servicios digitales. Esta ley define responsabilidades, derechos de los ciudadanos y medidas de seguridad, relevantes en el contexto de IoMT donde dispositivos médicos recopilan datos personales y clínicos.

- **Estrategia Nacional de Ciberseguridad (2019)**

La Estrategia Nacional de Ciberseguridad de España, revisada en 2019 en sustitución de la versión de 2013, constituye el marco de referencia fundamental para la protección del ciberespacio nacional. Promueve una visión integral que abarca desde la protección de infraestructuras críticas hasta la capacitación y concienciación ciudadana.

Entre sus líneas de acción destacan:

- Fortalecer la resiliencia nacional ante amenazas de ciberseguridad.
- Impulsar la cooperación público-privada en la gestión de incidentes.
- Fomentar la investigación y la innovación tecnológica en materia de ciberseguridad.
- Integrar la ciberseguridad como un componente esencial en el desarrollo de las Smart Cities y la administración digital.

La estrategia se implementa mediante el Consejo Nacional de Ciberseguridad, órgano dependiente del Consejo de Seguridad Nacional, que coordina la actuación de organismos como el INCIBE, el CCN-CERT, la Guardia Civil o la Policía Nacional.

Asimismo, el Consejo de Seguridad Nacional, el 24 de abril de 2025, aprobó el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad, con el objetivo de actualizar el marco estratégico ante la evolución del panorama de amenazas y las nuevas prioridades nacionales.

- **Esquema Nacional de Seguridad (2022)**

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece los principios básicos y los requisitos mínimos que deben cumplir las administraciones públicas y los proveedores de servicios tecnológicos para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información.

El ENS define tres categorías de seguridad (básica, media y alta) y actúa como una referencia obligada para el diseño de infraestructuras digitales seguras, especialmente en los sistemas sanitarios.

Su adaptación al contexto IoMT resulta esencial para reforzar la seguridad en los entornos sanitarios conectados y para cumplir con los nuevos requisitos de resiliencia digital europeos.

- **Plan Nacional de Ciberseguridad (2022)**

Aprobado como desarrollo operativo de la Estrategia Nacional, este plan incluye más de 100 actuaciones concretas dirigidas a reforzar la seguridad digital del país. Entre sus líneas prioritarias destacan la protección del IoT y de las infraestructuras sanitarias inteligentes, la creación de capacidades de detección temprana y la cooperación internacional.

El plan también fomenta la formación de especialistas en ciberseguridad IoT y la implantación de un marco nacional de certificación, en consonancia con el Cybersecurity Act europeo.

10.3. Necesidades regulatorias

A pesar de los avances descritos, aún existen vacíos normativos que deben abordarse para consolidar un ecosistema IoMT seguro, resiliente e interoperable. Entre las principales necesidades destacan:

- Unificación de criterios normativos entre los distintos marcos europeos y nacionales, evitando solapamientos o contradicciones.
- Actualización continua de las regulaciones, dada la rápida evolución tecnológica y la aparición de nuevos tipos de amenazas.
- Desarrollo de certificaciones específicas para dispositivos IoMT, que garanticen un nivel mínimo de seguridad y privacidad.
- Definición clara de responsabilidades entre fabricantes, operadores, administraciones y proveedores tecnológicos.
- Refuerzo de la cooperación internacional y público-privada, esencial para gestionar incidentes globales y compartir inteligencia sobre amenazas.

El futuro de la ciberseguridad en IoMT dependerá de la capacidad de los reguladores para crear un marco normativo coherente, dinámico y centrado en la protección de los pacientes, sin frenar la innovación tecnológica que impulsa la transformación digital.

11. Tendencias futuras y riesgos emergentes

El ecosistema IoMT continúa evolucionando rápidamente, impulsado por la innovación tecnológica y la creciente digitalización del sector sanitario. Esta transformación ofrece importantes oportunidades para mejorar la atención al paciente, optimizar la eficiencia hospitalaria y facilitar la medicina preventiva y

personalizada. Sin embargo, también introduce riesgos emergentes que pueden comprometer la seguridad, la privacidad y la resiliencia de los sistemas sanitarios.

11.1. Expansión de dispositivos conectados y telemedicina

El número de dispositivos médicos conectados sigue creciendo de manera exponencial, desde sensores portátiles hasta equipos clínicos críticos. Además, la telemedicina y los servicios de monitorización remota están expandiendo el perímetro del IoMT más allá de los hospitales hacia los hogares y comunidades.

Riesgos emergentes:

- Mayor superficie de ataque debido a la diversidad y heterogeneidad de los dispositivos, redes y sistemas operativos.
- Exposición de datos clínicos en redes domésticas o móviles con menor control de seguridad.
- Riesgos asociados a dispositivos personales o relojes inteligentes, que pueden ser manipulados o configurados de manera insegura.
- Dificultad para mantener inventarios precisos y gestionar el ciclo de vida de dispositivos dispersos geográficamente.

11.2. Inteligencia artificial y análisis avanzado de datos

La adopción de inteligencia artificial y aprendizaje automático en el diagnóstico, pronóstico y planificación terapéutica está transformando la toma de decisiones clínicas. Estas tecnologías permiten el análisis predictivo, la detección temprana de enfermedades y el ajuste automático de tratamientos personalizados.

Riesgos emergentes:

- Manipulación de modelos de IA mediante ataques de “data poisoning” o entradas maliciosas que induzcan errores diagnósticos.
- Falta de transparencia de los algoritmos que dificulta la identificación de errores o ciberataques que afecten a decisiones clínicas.
- Dependencia de proveedores externos de análisis y almacenamiento, con riesgos de fuga de datos o incumplimiento de normativas.
- Vulnerabilidades en la integración de sistemas de IA con dispositivos IoMT, que podrían permitir accesos no autorizados o alteraciones de información clínica.

11.3. Convergencia con tecnologías emergentes

La combinación de IoMT con tecnologías como 5G, edge computing, blockchain y realidad aumentada está redefiniendo los modelos de atención sanitaria. Estas innovaciones facilitan procesamiento en tiempo real, interoperabilidad avanzada y trazabilidad de datos, pero también introducen nuevos vectores de riesgo.

Riesgos emergentes:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Superficie de ataque ampliada en nodos de edge y dispositivos conectados a redes de alta velocidad.
- Vulnerabilidades en la implementación de blockchain, como errores en smart contracts o problemas de interoperabilidad entre plataformas.
- Dependencia de infraestructuras externas y complejas que requieren gestión avanzada de seguridad y monitorización continua.
- Posibles ataques dirigidos a tecnologías de realidad aumentada o telecirugía remota, con implicaciones directas sobre la seguridad del paciente.

11.4. Amenazas avanzadas y ciberdelincuencia organizada

Los ciberataques a entornos sanitarios están evolucionando hacia técnicas sofisticadas y coordinadas, con implicaciones directas sobre la salud y la seguridad del paciente.

Riesgos emergentes:

- Ransomware dirigido a hospitales, clínicas o dispositivos IoMT críticos, afectando a la continuidad asistencial.
- Ataques combinados que integran manipulación de datos, denegación de servicio y explotación de dispositivos IoMT.
- Potencial impacto físico sobre pacientes debido a la interrupción de dispositivos de soporte vital.
- Evolución de amenazas internas, como errores humanos o negligencia en la gestión de credenciales y accesos.

12. Conclusiones

La expansión del Internet de las Cosas Médicas (IoMT) ha transformado de manera significativa el ecosistema sanitario, permitiendo una atención más eficiente, monitorización continua de los pacientes y optimización de los procesos clínicos. Sin embargo, esta interconexión también amplía la superficie de ataque, exponiendo dispositivos, sistemas y datos clínicos a amenazas técnicas, físicas y de privacidad que pueden afectar tanto a la seguridad del paciente como a la integridad de la información.

El análisis realizado evidencia que los riesgos en entornos IoMT son multidimensionales, abarcando aspectos técnicos, operativos y estratégicos. Las vulnerabilidades en software, la autenticación débil, la exposición a redes abiertas y la manipulación física de dispositivos destacan como vectores críticos que requieren atención inmediata. Además, la gestión de datos clínicos y la seguridad en plataformas de telemedicina y soluciones en la nube son elementos clave para garantizar la confidencialidad, integridad y disponibilidad de la información médica.

Como conclusión general, la ciberseguridad en IoMT debe abordarse de manera integral, combinando medidas tecnológicas, procesos operativos robustos y una gobernanza clara que involucre a fabricantes, hospitales y autoridades reguladoras. Es fundamental mantener la actualización constante de software y firmware, implementar políticas de segmentación de redes y control de accesos, y reforzar la formación

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

y concienciación del personal sanitario frente a ataques de ingeniería social. Asimismo, la coordinación con proveedores y reguladores, así como la vigilancia de tendencias emergentes como inteligencia artificial, Edge Computing y telemedicina, resulta imprescindible para anticipar y mitigar riesgos futuros.

En definitiva, garantizar la seguridad de los entornos IoMT no solo protege la infraestructura tecnológica y la información clínica, sino que también asegura la confianza de los pacientes y la continuidad de la atención médica en un ecosistema sanitario cada vez más digitalizado.

12.1. Recomendaciones

A continuación, se recogen algunas recomendaciones prácticas para fortalecer la seguridad de los dispositivos IoMT y las redes hospitalarias o médicas a las que se conectan, tanto en entornos clínicos como en el hogar del paciente:

- **Mantener los dispositivos y el software actualizados**

Los dispositivos IoMT suelen carecer de soluciones tradicionales de protección, como antivirus o cortafuegos, por lo que las actualizaciones periódicas de firmware y software son la principal defensa frente a vulnerabilidades.

Es fundamental asegurarse de que el fabricante proporcione actualizaciones de seguridad y aplicarlas de forma inmediata, ya sea automática o manualmente desde fuentes oficiales. En el caso de entidades sanitarias, los dispositivos IoMT deben integrarse en la política general de gestión de parches y mantenimiento, garantizando su revisión continua y la planificación de actualizaciones programadas.

- **Conocer las amenazas y evaluar los riesgos**

Comprender los posibles vectores de ataque y realizar evaluaciones periódicas de riesgo permite priorizar las medidas de protección. Se recomienda identificar los dispositivos más críticos para la atención al paciente, analizar las consecuencias clínicas y operativas de un incidente, así como clasificar los riesgos según su impacto en la seguridad del paciente y la continuidad asistencial.

Este proceso debe complementarse con formación y simulacros de ciberincidentes clínicos, tanto para el personal sanitario como para los equipos técnicos. Además, debe mantenerse un inventario actualizado de activos IoMT y un sistema de monitorización continua de su comportamiento.

- **Cambiar las contraseñas por defecto**

El uso de credenciales por defecto o repetidas sigue siendo una de las principales causas de brechas de seguridad en entornos médicos. Es imprescindible modificar los nombres de usuario y contraseñas de fábrica en todos los dispositivos IoMT y asignar credenciales únicas y seguras.

Asimismo, se recomienda verificar que los dispositivos admitan autenticación robusta y gestión de accesos basada en roles, limitando las credenciales de administrador a personal técnico autorizado.

- **Utilizar contraseñas seguras**

Las contraseñas deben ser robustas y complejas, combinando letras mayúsculas, minúsculas, números y símbolos, con una longitud mínima de 12 caracteres.

Para facilitar su gestión, puede recurrirse a administradores de contraseñas que almacenen de forma segura las credenciales y eviten su reutilización. También es esencial proteger las redes Wi-Fi

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

hospitalarias o domésticas utilizadas por los dispositivos médicos, aplicando contraseñas fuertes y protocolos seguros.

- **Revisar los ajustes de privacidad y seguridad**

Los dispositivos IoMT pueden transmitir o almacenar datos personales y clínicos, por lo que es esencial revisar las configuraciones predeterminadas antes de su puesta en servicio. Se deben ajustar los parámetros de privacidad y cifrado, activar los registros de auditoría (logs) y asegurarse de que las políticas de tratamiento de datos cumplan con la normativa sanitaria y de protección de datos (como el RGPD o la HIPAA).

- **Activar y desactivar funciones en base a su uso**

Cada funcionalidad activa (Bluetooth, Wi-Fi, NFC, geolocalización, voz, etc.) amplía la superficie de ataque. Se recomienda deshabilitar las funciones no necesarias en cada dispositivo médico para minimizar los riesgos y reducir el consumo de recursos.

- **Implementar autenticación multifactor (MFA)**

Siempre que sea posible, debe activarse la autenticación multifactor para acceder a sistemas IoMT, especialmente en consolas administrativas, servidores de datos clínicos o plataformas de monitorización remota. Esta medida añade una capa adicional de protección frente al acceso no autorizado.

- **Proteger el hardware**

En entornos clínicos o domiciliarios, los dispositivos médicos deben protegerse físicamente frente a manipulaciones o accesos no autorizados. Esto incluye bloquear puertos físicos, cifrar los datos locales, asegurar las conexiones mediante redes privadas virtuales (VPN) y, si es necesario, utilizar conexiones móviles seguras en lugar de Wi-Fi público o no controlado.

- **Fomentar la formación y concienciación**

La concienciación del personal sanitario y técnico es la primera línea de defensa. Promover una cultura de ciberseguridad implica formar a médicos, enfermeros y pacientes sobre el uso seguro de los dispositivos, la gestión de credenciales, la detección de correos fraudulentos y la importancia de las buenas prácticas digitales.

Solo mediante una cultura proactiva y coordinada será posible reducir los riesgos y consolidar un entorno IoMT seguro, resiliente y centrado en la seguridad del paciente.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

13. Anexos

Este apartado incluye información complementaria que respalda y amplía el contenido principal del documento.

13.1. Anexo I: Listado de amenazas

A continuación, se presenta un listado de amenazas en entornos IoMT, organizadas por categoría, con una breve descripción de cada una y los activos afectados. Este esquema permite tener una visión estructurada de los riesgos técnicos, físicos y de privacidad, facilitando la evaluación, gestión y mitigación dentro del ecosistema IoMT.

Antes de detallar las amenazas, se definen los activos considerados en el análisis, que representan los elementos clave del entorno tecnológico que pueden verse comprometidos ante un incidente:

- Dispositivos IoMT: Sensores, actuadores, bombas de infusión, monitores y otros equipos médicos conectados.
- Plataformas de gestión: Consolas y sistemas centralizados de administración, configuración y monitorización de dispositivos IoMT.
- Sistemas Backend: Servidores, bases de datos y servicios donde se almacenan y procesan datos clínicos.
- Aplicaciones y servicios: Interfaces web, móviles o APIs que interactúan con los sistemas IoMT y presentan información al personal sanitario.
- Infraestructura: Redes, routers, switches y centros de datos que soportan la conectividad IoMT.
- Comunicaciones: Protocolos y enlaces de transmisión de datos entre dispositivos, servidores y plataformas.
- Otros dispositivos integrados: Equipos conectados indirectamente o que pueden actuar como vectores de ataque lateral.

Con base en estos activos, el siguiente cuadro recoge las principales amenazas identificadas, clasificadas según su naturaleza y su posible impacto sobre el entorno IoMT.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Descripción	Activos afectados
Amenazas Técnicas	Amenazas relacionadas con el software médico	Fallos en firmware, librerías desactualizadas o errores de validación que permiten ejecución de código no autorizado, acceso a datos o interrupción de servicios.	– Dispositivos IoMT, – Plataformas de gestión – Sistemas Backend
	Ataque sobre credenciales o autenticación clínica	Uso de contraseñas por defecto, débiles o ataques de phishing que comprometen la autenticación y control de los dispositivos.	– Dispositivos IoMT – Plataformas de gestión – Aplicaciones y servicios – Sistemas Backend
	Amenazas derivadas de la exposición a redes hospitalarias o Internet	Dispositivos o servicios accesibles públicamente sin control adecuado, detectables mediante exploración de red.	– Dispositivos IoMT – Infraestructura – Comunicaciones
	Ataques de denegación de servicio (DDoS)	Saturación de sistemas críticos mediante dispositivos comprometidos, afectando la disponibilidad de equipos médicos esenciales.	– Infraestructura – Comunicaciones, – Plataformas de gestión – Aplicaciones y servicios
	Integración con otras redes y sistemas clínicos	Amenazas que se aprovechan de conexiones inseguras entre redes hospitalarias y externas, permitiendo movimientos laterales del atacante dentro de la infraestructura.	– Infraestructura – Comunicaciones – Otros dispositivos de la red IoMT
Amenazas Físicas	Acceso físico o manipulación directa	Manipulación directa de sensores o nodos IoMT en hospitales, ambulancias o domicilios.	– Dispositivos IoMT – Infraestructura

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Descripción	Activos afectados
	Ataques a nivel de hardware	Ingeniería inversa, explotación de interfaces físicas (JTAG, UART, USB) o manipulación de componentes.	– Dispositivos IoMT – Otros dispositivos de la red IoMT
	Manipulación durante la cadena de suministro	Inserción de componentes falsificados o firmware comprometido durante la fabricación o distribución del dispositivo.	– Dispositivos IoMT – Plataformas de gestión – Sistemas Backend
Amenazas a la integridad y privacidad	Robo y filtración de datos clínicos	Infección de dispositivos mediante software malicioso que roba información o bloquea el funcionamiento de los sistemas inteligentes.	– Dispositivos IoMT – Plataformas de gestión – Sistemas Backend – Aplicaciones y servicios
	Intercepción o alteración de datos biomédicos	Captura o alteración de datos en tránsito entre dispositivos y servidores mediante ataques Man-in-the-Middle o replay, afectando decisiones clínicas.	– Dispositivos IoMT – Comunicaciones – Plataformas de gestión – Sistemas Backend
	Manipulación o pérdida de integridad de la información	Alteración de registros clínicos, dosis de medicación, resultados de pruebas o parámetros biomédicos, comprometiendo decisiones terapéuticas y la seguridad del paciente.	– Dispositivos IoMT – Plataformas de gestión – Sistemas Backend – Aplicaciones y servicios
	Amenazas en la nube médica y plataformas de telemedicina	Amenazas que explotan configuraciones inseguras, falta de cifrado o dependencia de proveedores externos sin auditoría, exponiendo datos clínicos críticos y la continuidad de servicios.	– Dispositivos IoMT – Plataformas de gestión – Sistemas Backend – Aplicaciones y servicios

TABLA 4: LISTADO DE AMENAZAS IOMT

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

14. Referencias

1. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain. (2020). *"Recent advances in the internet-of-medical-things (IoMT) systems security.* https://doi.org/10.1109/JIOT.2020.3045653

2. Arnab Ray. (2021). *Cybersecurity for Connected Medical Devices.* https://doi.org/10.1016/C2018-0-03213-2

3. Boletín Oficial del Estado (BOE). (2023). *Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios*. https://www.boe.es/eli/es/rd/2023/03/21/192

4. Boletín Oficial del Estado (BOE). (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

5. European Commission. (2025). *Procurement ecosystem factsheet (for medical devices)*. https://data.europa.eu/doi/10.2875/6879484

6. European Commission. (2021). *Guidance on qualification and classification of software in Regulation (EU)*. https://ec.europa.eu/docsroom/documents/37581

7. European Union. (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

8. European Union. (2017). *Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices*. https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng

9. European Union. (2017). *Regulation (EU) 2017/746 of the European Parliament and of the Council on in vitro diagnostic medical devices*. https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng

10. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025#contentList

11. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Cybersecurity Threat Landscape Methodology.* https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

12. European Union Agency for Cybersecurity (ENISA). (2023). *Health Threat Landscape.* https://www.enisa.europa.eu/publications/health-threat-landscape

13. European Union Agency for Cybersecurity (ENISA). (2020). *Procurement Guidelines for Cybersecurity in Hospitals*. https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

14. European Union Agency for Cybersecurity (ENISA). (2017). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

15. Federal Communications Commission (FCC). (2017). *Medical Device Radiocommunications Service (MedRadio)*. https://www.fcc.gov/medical-device-radiocommunications-service-medradio

16. Food and Drug Administration (FDA). (2025). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. https://www.fda.gov/media/119933/download

17. Instituto Nacional de Ciberseguridad (INCIBE). (2024). *Ciberseguridad en el sector salud: características, amenazas y recomendaciones.* https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

18. Instituto Nacional de Ciberseguridad (INCIBE). (2019). *La importancia de la seguridad en IoT. Principales amenazas.* https://www.incibe.es/incibe-cert/blog/importancia-seguridad-iot-principales-amenazas

19. Instituto Nacional de Ciberseguridad (INCIBE). (2017). *Riesgos y retos de ciberseguridad y privacidad en IoT*. https://www.incibe.es/incibe-cert/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

20. 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

21. International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

22. Medical Device Coordination Group Document (MDCG). (2019). *Guidance on Cybersecurity for medical devices*. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

23. MITRE Corporation. (2022). *Playbook for threat modeling medical devices*. https://www.mitre.org/publications/technical-papers/playbook-for-threat-modeling-medical-devices

15. Otras referencias de interés

El presente apartado recoge un resumen de los principales temas abordados en la guía, así como la relación de productos y servicios mencionados en ella. Su finalidad es ofrecer una visión global de los ámbitos tratados y facilitar la identificación de posibles referencias o elementos relevantes para futuras consultas o ampliaciones documentales.

15.1. Lista de materias tratadas en la guía

- Concepto y características de la Internet de las Cosas Médicas (IoMT).
- Aplicaciones y beneficios de IoMT en entornos sanitarios.
- Arquitectura IoMT: capas funcionales y componentes críticos.
- Clasificación de dispositivos médicos.
- Puntos críticos de exposición y superficie de ataque en sistemas médicos conectados.
- Riesgos asociados a IoMT: técnicos, operativos y estratégicos.
- Amenazas de ciberseguridad: técnicas, físicas y relacionadas con la privacidad de datos clínicos.
- Retos de ciberseguridad: estándares, escalabilidad, gobernanza, gestión de proveedores y coordinación clínica.
- Casos reales: filtración de datos, manipulación de sistemas e interrupción de servicios.
- Marco regulatorio actual y necesidades futuras en ciberseguridad para entornos IoMT.
- Tendencias futuras y riesgos emergentes, incluyendo inteligencia artificial, telemedicina, Edge Computing y evolución de ataques sofisticados.

15.2. Lista de productos mencionados en la guía

No se mencionan servicios específicos en la guía.

15.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Ciberseguridad en IoMT: Retos y Amenazas

Noviembre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía