RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Análisis de Riesgos en IoMT

Febrero de 2026

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: 09/02/2026

Fecha de última actualización: 09/02/2026

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

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

1. Introducción

La transformación digital del sector sanitario español ha experimentado un crecimiento exponencial en los últimos años, impulsado en gran medida por la incorporación del Internet de los Dispositivos Médicos (IoMT) en hospitales y centros sanitarios. Esta evolución tecnológica ha permitido avances significativos en la monitorización continua de personas pacientes, la precisión diagnóstica, la personalización de tratamientos y la optimización de recursos asistenciales. Dispositivos como bombas de infusión inteligentes, monitores de constantes vitales conectados, sistemas de imagen médica digital y plataformas de telemedicina se han convertido en elementos esenciales para una atención eficiente y centrada en las personas pacientes.

Sin embargo, la interconexión masiva de dispositivos médicos con las redes sanitarias y sistemas de información clínica ha generado una superficie de exposición a amenazas de ciberseguridad sin precedentes. Cada dispositivo IoMT conectado representa no solo una oportunidad para mejorar la atención sanitaria, sino también un potencial vector de ataque que puede comprometer la confidencialidad de datos sensibles de personas pacientes, alterar la integridad de información clínica crítica, interrumpir la disponibilidad de servicios esenciales o, en el peor de los casos, poner en peligro directo la seguridad y vida de las personas pacientes.

Los incidentes de ciberseguridad en el ámbito sanitario han demostrado que las amenazas no son solo teóricas, desde ataques de ransomware que paralizan hospitales completos, pasando por vulnerabilidades en dispositivos médicos que permiten accesos no autorizados, hasta errores de configuración que provocan fallos en equipos críticos. Estos eventos evidencian que la gestión de riesgos en dispositivos IoMT no puede abordarse como una preocupación exclusivamente técnica, sino que requiere un enfoque integral, sistemático y alineado con los estándares internacionales reconocidos en el ámbito.

2. Objetivo y alcance

2.1. Objetivo

El objetivo principal de esta guía es proporcionar una metodología práctica, estructurada y alineada con las normativas y estándares aplicables para realizar análisis de riesgos en dispositivos IoMT conectados a redes sanitarias, dentro del marco regulatorio vigente en España.

De manera específica, la guía pretende:

- Promover la implementación de procesos de gestión de riesgos que permitan a hospitales y centros sanitarios identificar, analizar, evaluar y tratar de forma sistemática los riesgos asociados a la integración de dispositivos médicos conectados.
- Proporcionar un marco metodológico claro que guíe al personal de los centros sanitarios a través de todas las fases del análisis de riesgos, desde la identificación de activos y amenazas hasta la estimación del riesgo residual.

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

- Facilitar la comprensión de los conceptos fundamentales de gestión de riesgos, permitiendo la participación activa de personas usuarias con distintos niveles de conocimiento técnico en todas las fases.

En conjunto, esta guía aspira a convertirse en un recurso de referencia para que los centros sanitarios españoles puedan desarrollar, implementar y mantener sistemas de gestión de riesgos en IoMT que sean eficientes y alineados con la normativa aplicable y, orientados, ante todo, a garantizar la seguridad de las personas pacientes, la protección de los datos y la continuidad de los servicios asistenciales esenciales.

2.2. Alcance

Esta guía aplica a los siguientes tipos de dispositivos IoMT utilizados en entornos sanitarios que se conecten a las redes sanitarias, sistemas de información o infraestructura:

- Dispositivos de monitoreo y diagnóstico conectados, como monitores de signos vitales, bombas de infusión inteligentes, ventiladores, oxímetros y sensores portátiles integrados con sistemas clínicos.
- Dispositivos implantables con conectividad, incluyendo marcapasos, bombas de insulina inteligentes y otros dispositivos que requieren supervisión remota o conexión a sistemas hospitalarios.
- Equipos médicos integrados con redes y aplicaciones, como sistemas de telemetría, CPAP conectados, monitores de constantes vitales y cualquier dispositivo que interactúe con plataformas de gestión hospitalaria o servicios en la nube.
- Infraestructura de soporte asociada, incluyendo aplicaciones móviles internas, plataformas de telemedicina, servicios en la nube y redes hospitalarias utilizadas para el funcionamiento y monitoreo de los dispositivos IoMT.

Los contenidos de esta guía están dirigidos a cualquier profesional del entorno sanitario que interactúe, gestione o tome decisiones relacionadas con dispositivos IoMT, incluyendo, entre otros:

- Personal médico, que utiliza dispositivos IoMT para el seguimiento, diagnóstico o tratamiento de personas pacientes.
- Personal de ingeniería clínica, encargado de la instalación, calibración, mantenimiento y actualización de dispositivos IoMT.
- Personal de TI, responsable de la gestión de redes, control de accesos y seguridad de la información generada por los dispositivos.

2.3. Metodología

La elaboración de esta guía se ha basado en un enfoque estructurado que combina el análisis de las normativas y estándares aplicables, la revisión de casos reales y la incorporación de conocimiento experto, con el objetivo de ofrecer un documento completo y comprensible para cualquier persona del entorno sanitario que interactúe con dispositivos IoMT.

Los principales elementos de la metodología son:

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

- Revisión normativa y documental: Se han analizado las normativas y estándares internacionales, guías de buenas prácticas y recomendaciones de organismos especializados en ciberseguridad y salud, como ENISA, INCIBE, NIST, AEMPS, ISO, y otras entidades de referencia del sector salud. Este análisis asegura que las recomendaciones estén alineadas con la legislación vigente y con las mejores prácticas reconocidas a nivel global.
- Estructuración del proceso de análisis de riesgos en fases progresivas y secuenciales: Se ha organizado el análisis en una serie de fases que permiten realizar un análisis de riesgos completo, ordenado y reproducible:
    - Inventario de activos: identificación de dispositivos IoMT, sus funciones, dependencias y entorno operativo.
    - Identificación de amenazas: análisis de posibles eventos que puedan afectar a la seguridad de la información, la continuidad asistencial o la seguridad de las personas pacientes.
    - Análisis de vulnerabilidades: valoración de debilidades técnicas, operativas u organizativas que puedan facilitar la materialización de amenazas.
    - Cálculo y evaluación del riesgo: estimación de probabilidades e impactos, clasificación según las dimensiones CIDAT del ENS y uso de matrices para determinar niveles de riesgo.
    - Definición de estrategias de mitigación y cálculo del riesgo residual, orientando la toma de decisiones y priorización de medidas.
- Adaptación del contenido a un lenguaje accesible: Se ha priorizado la claridad y comprensión para todos los perfiles de personas usuarias finales, asegurando que las recomendaciones puedan aplicarse de manera práctica sin necesidad de conocimientos técnicos avanzados.

Esta metodología asegura que la guía proporcione un marco estructurado que permite a las organizaciones sanitarias identificar, evaluar y gestionar los riesgos asociados a su ecosistema IoMT de manera sistemática y reproducible.

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 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

- 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).

- **Estándares**:
  - IEC 80001-1, Gestión de riesgos para redes TI que incorporan dispositivos médicos.
  - IEC/ISO 81001, Normas relacionadas con la ingeniería de software para dispositivos médicos.
  - ISO 14971:2019, Aplicación de una metodología de riesgos para dispositivos médicos.
  - ISO/TR 24971:2020, Guía para la aplicación de la ISO 14971.
  - ISO 31000:2018, Gestión de riesgos.
  - ISO/IEC 27001:2022, Gestión de la seguridad de la información.
  - ISO/IEC 27005:2022, Gestión de los riesgos TI.
  - ISO/IEC 27035-1:2023, Gestión de incidentes TI.
  - ISO/IEC 27701:2025, Gestión de la privacidad de la información.
  - ISO 22301:2019, Gestión de la continuidad de negocio.

- **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).
  - NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
  - NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.
  - NIST SP 800-30, Guía para la realización de análisis de riesgos.
  - NIST SP 800-37, Metodología de gestión de riesgos.
  - NIST SP 800-53 y SP 800-115, Guía de controles y pruebas técnicas de seguridad.
  - IMDRF-Principios y prácticas de ciberseguridad para la contratación de software y materiales de dispositivos médicos.

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

- OWASP IoT y OWASP, Guías de auditorías técnicas.

4. Definiciones

Acrónimos	Definición
AEMPS	Autoridad reguladora española de medicamentos y productos sanitarios (Agencia Española de Medicamento y Productos Sanitarios).
APIs	Interfaces para que sistemas o aplicaciones intercambien datos y funciones de forma controlada (del inglés, Application Programming Interfaces).
BIA	Análisis para determinar funciones críticas y el impacto de su interrupción (del inglés, Business Impact Analysis).
Botnets	Red de equipos comprometidos controlados por un atacante para acciones coordinadas
DDoS	Intento malicioso de interrumpir el funcionamiento normal de un servidor sobrecargándolo con tráfico desde múltiples fuentes (del inglés, Distributed Denial of Service).
DICOM	Estándar internacional para la transmisión, almacenamiento y visualización de imágenes médicas digitales (del inglés, Digital Imaging and Communications in Medicine).
EHR	Sistema digital que almacena la información clínica completa de una persona (del inglés, Electronic Health Record).
EMI	Perturbaciones en el funcionamiento de un dispositivo causadas por campos electromagnéticos externos (del inglés, Electromagnetic Interference)
FTP	Protocolo usado para transferir archivos entre sistemas, generalmente sin cifrado (del inglés, File Transfer Protocol)
HL7/FHIR	Conjunto de estándares para el intercambio electrónico de información sanitaria (del inglés, Health Level Seven / Fast Healthcare Interoperability Resources).
IDS	Herramienta que monitoriza redes o sistemas para identificar actividad sospechosa o no autorizada (del inglés, Intrusion Detection System).
JTAG	Interfaz de prueba y depuración de hardware (del inglés, Joint Test Action Group).
LIMS	Software para gestionar procesos, muestras y datos en laboratorios clínicos (del inglés, Laboratory Information Management System).
MFA	Mecanismo de seguridad que requiere más de un factor de verificación para acceder a un sistema (del inglés, Multi-Factor Authentication).
MQTT	Protocolo ligero de mensajería utilizado en IoT (del inglés, Message Queuing Telemetry Transport).

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

Acrónimos	Definición
PACS	Sistema que permite almacenar y visualizar imágenes médicas (del inglés, Picture Archiving and Communication System).
PILAR	Herramienta española para análisis y gestión de riesgos basada en la metodología MAGERIT
RIS	Sistema que gestiona flujos de trabajo, agendas, informes y datos administrativos de servicios de radiología (del inglés, Radiology Information System).
SAI	Dispositivo que proporciona energía temporal ante fallos eléctricos (Sistema de Alimentación Ininterrumpida).
SMB	Protocolo de compartición de archivos y recursos en red (del inglés, Server Message Block).
TAC	Técnica de diagnóstico por imagen que utiliza rayos X para generar imágenes transversales detalladas del cuerpo (Tomografía Axial Computarizada).
Telnet	Protocolo de administración remota que permite a una persona usuaria conectarse a otro sistema ubicado en la misma red.
UART	Interfaz hardware para comunicación serie directa entre dispositivo (del inglés, Universal Asynchronous Receiver-Transmitter).
UCI	Área hospitalaria destinada a la atención de personas pacientes críticas (Unidad de Cuidados Intensivos).
USB	Interfaz común para conexión de periféricos y transferencia de datos (del inglés, Universal Serial Bus).

TABLA 1: DEFINICIONES EMPLEADAS.

5. Contexto general del análisis de riesgos IoMT

El Internet de las Cosas Médicas (IoMT) se refiere a la incorporación de dispositivos médicos al entorno digital de los centros sanitarios, de modo que pueden comunicarse e intercambiar datos con otros dispositivos, con los sistemas de información clínica y con plataformas digitales internas o externas. Esta conectividad convierte equipos tradicionalmente aislados en componentes activos de un ecosistema sanitario interconectado, habilitando capacidades como la monitorización remota, el intercambio de información en tiempo real y la automatización de procesos clínicos.

La integración de dispositivos médicos en redes TI hospitalarias aporta beneficios relevantes para la calidad asistencial y la seguridad de la persona paciente, ya que mejora la continuidad de la información, agiliza flujos clínicos y permite decisiones más rápidas y fundamentadas. Sin embargo, esta digitalización también amplía la superficie de exposición y genera nuevos escenarios de riesgo que deben gestionarse mediante un enfoque específico. En este contexto, incidentes como fallos técnicos, acciones no autorizadas, compromisos de funciones o información, actos deliberados o deficiencias organizativas pueden traducirse en impactos clínicos, operativos y legales.

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

Por ello, la gestión de riesgos en IoMT no debe entenderse como una actividad opcional, sino como una necesidad estratégica para sostener tres pilares fundamentales:

- **Seguridad de la información**, protegiendo los datos clínicos frente a accesos no autorizados y garantizando su integridad.
- **Continuidad y eficacia operativa**, asegurando que los sistemas y dispositivos estén disponibles cuando se necesitan.
- **Seguridad de la persona paciente**, evitando que fallos tecnológicos o manipulaciones comprometan diagnósticos, tratamientos o monitorización.

Para abordar estos retos, resulta especialmente relevante la ISO/IEC 80001-1:2021, que establece un marco internacional para la gestión de riesgos en redes TI que incorporan dispositivos médicos, definiendo principios, roles, responsabilidades y actividades necesarias para mantener un entorno seguro y efectivo.

En España, la digitalización del sistema sanitario ha avanzado de forma notable en los últimos años, acelerándose especialmente tras la pandemia de COVID-19. Como consecuencia, los hospitales gestionan un volumen creciente de dispositivos conectados: desde equipos de diagnóstico por imagen y sistemas de monitorización de personas pacientes, hasta bombas de infusión inteligentes, soluciones de telemonitorización y otros activos del ecosistema IoMT. Este crecimiento incrementa la necesidad de disponer de inventarios completos y actualizados, así como de una visión clara de las dependencias técnicas y clínicas.

Un aspecto crítico en la gestión del IoMT es que los dispositivos conectados deben estar registrados y documentados, y la organización debe mantener una descripción completa y actualizada de la red en la que operan. No obstante, en la práctica, muchos entornos sanitarios todavía presentan desafíos para implantar procedimientos sistemáticos de gestión de riesgos alineados con los principales estándares y metodologías de referencia, lo que puede traducirse en brechas de control, falta de trazabilidad y exposición a vulnerabilidades operativas o técnicas.

A este contexto se suma un marco normativo exigente, alineado con las disposiciones europeas y nacionales, que establece obligaciones específicas relacionadas con dispositivos y datos clínicos, entre ellas:

- Reglamento (UE) 2017/745 (MDR), que exige a los fabricantes abordar la ciberseguridad a lo largo del ciclo de vida del producto sanitario.
- Esquema Nacional de Seguridad (ENS), aplicable a entornos del sector público y, por tanto, relevante para centros sanitarios públicos, estableciendo principios y requisitos para proteger la información y los servicios.
- RGPD y LOPDGDD, que regulan el tratamiento de datos personales de salud, considerados especialmente sensibles, e imponen obligaciones estrictas en materia de confidencialidad, integridad, disponibilidad y trazabilidad.
- Normativa de historia clínica digital, como el Real Decreto 1093/2010, que establece requisitos asociados a interoperabilidad, normalización y gestión segura de la información clínica.

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

Finalmente, la gestión de riesgos en IoMT requiere una coordinación efectiva entre todas las áreas implicadas: TI, ingeniería clínica, ciberseguridad, legal y personal sanitario. Por ello, la adquisición y despliegue de nuevos dispositivos debe planificarse de forma conjunta desde el inicio, definiendo claramente responsabilidades y requisitos de conectividad, mantenimiento, seguridad y cumplimiento normativo. Solo mediante un enfoque integral y una gobernanza compartida es posible reducir los riesgos sin comprometer la operativa clínica ni la seguridad de la persona paciente.

5.1. Tendencias y desafíos específicos

El ecosistema IoMT constituye uno de los ámbitos de mayor crecimiento dentro de la tecnología sanitaria global. Las proyecciones del sector estiman que el número de dispositivos médicos conectados superará los cincuenta mil millones en los próximos años, impulsado por la transición desde un modelo asistencial basado en episodios puntuales hacia otro centrado en la monitorización continua, la medicina preventiva y la personalización del tratamiento.

Esta evolución viene acompañada de una ampliación del perímetro digital sanitario y de nuevas dependencias tecnológicas que condicionan la gestión del riesgo en las organizaciones.

❖ Telemedicina y monitorización remota

La telemedicina y la monitorización remota se han consolidado tras la pandemia de COVID-19 y hoy constituyen un componente estructural de la atención sanitaria. La transmisión de datos clínicos en tiempo real desde el domicilio de la persona paciente permite anticipar incidentes, reducir hospitalizaciones en determinadas patologías y optimizar recursos asistenciales.

Sin embargo, este modelo desplaza la superficie de explotación más allá del recinto sanitario y exige garantizar la protección extremo a extremo, desde el dispositivo y sus aplicaciones asociadas, hasta las plataformas de integración y la historia clínica electrónica. La gestión de identidades y la disponibilidad del servicio pasan a ser elementos críticos para sostener el nuevo modelo de asistencia sanitaria.

❖ Inteligencia artificial aplicada al diagnóstico

La integración de inteligencia artificial (IA) y aprendizaje automático en dispositivos médicos está transformando el diagnóstico y el apoyo a la decisión clínica. Los algoritmos procesan grandes volúmenes de datos para identificar patrones, priorizar casos o alertar sobre deterioros clínicos.

El uso de IA aporta eficiencia y precisión clínica, pero introduce nuevas categorías de riesgo relacionadas con los datos procesados y los resultados obtenidos.

❖ Interoperabilidad y sistemas conectados

La interoperabilidad es un requisito creciente en los entornos sanitarios modernos. Estándares como HL7-FHIR o DICOM facilitan el intercambio de información clínica y la coordinación entre dispositivos de diferentes fabricantes. Sin embargo, la mayoría de estos estándares no cuentan con mecanismos robustos de cifrado, multiplicando así los puntos de entrada potenciales para ataques y dificultando la gestión del riesgo.

❖ Persistencia de dispositivos heredados (legacy)

Pese al avance tecnológico, la mayoría de los sistemas sanitarios mantienen una proporción significativa de dispositivos heredados que continúan en uso por razones presupuestarias o porque desempeñan un

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

rol crítico en la actividad asistencial que no puede ser reemplazado por otro dispositivo. Estos equipos fueron diseñados en un contexto de menor exposición digital y suelen incorporar capacidades de seguridad limitadas o inexistentes.

5.1.1. Tendencias específicas en el contexto español

El panorama del IoMT en España reproduce las tendencias globales, pero presenta particularidades derivadas de la propia estructura del Sistema Nacional de Salud y de su marco regulatorio. La organización territorial, con diecisiete servicios autonómicos de salud que ejercen competencias plenas en materia tecnológica, asistencial y presupuestaria, genera enfoques diversos en la adquisición, implantación, integración y explotación de dispositivos médicos conectados. Esta diversidad aporta flexibilidad e innovación, pero dificulta la estandarización de prácticas de seguridad, la reutilización de soluciones y la adopción homogénea de modelos de análisis de riesgos a escala estatal.

- **Fragmentación autonómica**

Cada comunidad autónoma establece políticas propias para la adquisición de dispositivos, define requisitos técnicos específicos y opera ecosistemas de información con arquitecturas, proveedores y niveles de madurez dispares. Para los fabricantes, esto implica adaptar productos, configuraciones de seguridad e integraciones a múltiples contextos, y para los servicios de salud significa que los servicios de un territorio no siempre son transferibles sin ajustes a otros.

La coexistencia de distintas historias clínicas electrónicas, plataformas de receta e infraestructuras de imagen (PACS/RIS) intensifica los retos de interoperabilidad y, por extensión, eleva la complejidad de la gestión del riesgo en los puntos de integración y en las pasarelas entre sistemas.

- **Complejidad del marco normativo**

En España, el IoMT se rige por un marco que integra normativa europea, como el RGPD, el MDR y el IVDR, y normativa nacional, como el ENS y la LOPDGDD, complementado por guías técnicas emitidas por organismos de referencia como la AEMPS, el CCN-CERT e INCIBE.

Este conjunto normativo es robusto pero exigente y requiere coordinación efectiva entre las distintas áreas de las organizaciones sanitarias para armonizar los requisitos de las normativas y aplicar controles de seguridad a lo largo de todo el ciclo de vida del dispositivo.

- **Oportunidades del contexto español**

Pese a estos retos, el contexto español ofrece palancas significativas para fortalecer la gestión del riesgo en IoMT. La existencia de marcos como el ENS y de organismos de referencia con publicaciones técnicas, como INCIBE, junto con la disponibilidad de fondos europeos para la transformación digital y la creciente priorización institucional de la ciberseguridad como garante de la continuidad asistencial y la seguridad de la persona paciente, conforman una base favorable.

Aprovechar estas palancas, mediante iniciativas colaborativas entre comunidades autónomas, la adopción de estándares abiertos, la definición de catálogos comunes y métricas compartidas puede mejorar la madurez y favorecer una evolución más homogénea y robusta del ecosistema IoMT en España.

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

5.2. Retos del análisis de riesgos en entornos IoMT

Más allá de las tendencias tecnológicas y de las particularidades del sistema sanitario español, las organizaciones deben afrontar una serie de retos prácticos que dificultan la implantación efectiva de procesos de análisis y gestión de riesgos en dispositivos médicos conectados. Comprender estas dificultades es esencial para diseñar aproximaciones realistas y estrategias adecuadas que permitan gestionar los riesgos de manera eficiente.

❖ Escasez de profesionales especializados

La gestión de riesgos en entornos IoMT requiere una combinación de competencias poco frecuente: conocimientos de ciberseguridad, comprensión técnica de dispositivos médicos, familiaridad con procesos clínicos y dominio del marco regulatorio sanitario. Esta convergencia de capacidades es difícil de encontrar, y el mercado profesional español dispone de un número limitado de perfiles que la cumplan.

A ello se suma que las estructuras retributivas de las organizaciones sanitarias suelen ser menos competitivas que las del sector tecnológico privado, dificultando la captación y retención de talento especializado.

❖ Ausencia de metodologías adaptadas

Aunque existen marcos generales de gestión de riesgos, su aplicación directa a dispositivos médicos conectados resulta insuficiente sin realizar adaptaciones específicas. Aspectos como la criticidad de la disponibilidad en equipos de soporte vital, las limitaciones derivadas de la certificación de productos sanitarios a la hora de aplicar actualizaciones o la necesidad de coordinar medidas de seguridad con los fabricantes no suelen estar contemplados en metodologías genéricas.

Como consecuencia, muchas organizaciones encuentran dificultades para valorar impactos clínicos, incorporar requisitos regulatorios o definir criterios de aceptabilidad del riesgo en un contexto asistencial.

❖ Inventarios incompletos o desactualizados

La eficacia del análisis de riesgos depende de disponer de un inventario preciso de los dispositivos IoMT, sus características, ubicaciones y conexiones. Sin embargo, es habitual que los centros sanitarios carezcan de una visión completa de su parque tecnológico debido al crecimiento orgánico de la infraestructura, la incorporación de equipos sin coordinación previa con TI o la existencia de dispositivos legacy con documentación insuficiente.

Esta falta de visibilidad dificulta la clasificación de los activos, la planificación de mitigaciones y la respuesta ante incidentes.

❖ Falta de concienciación en ciberseguridad

La concienciación del personal sanitario es un elemento imprescindible para la correcta ejecución del análisis de riesgos. Cuando los profesionales no comprenden la relevancia de identificar amenazas, reportar incidentes o aportar información sobre el uso real de los dispositivos, el proceso de análisis de riesgos se puede ver afectado, reduciendo así su eficacia.

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

En entornos asistenciales con elevada carga de trabajo, los controles de seguridad pueden percibirse como una interferencia, lo que dificulta la obtención de datos fiables sobre vulnerabilidades operativas o prácticas inseguras asociadas al uso cotidiano de los equipos. A nivel directivo, la falta de sensibilización puede traducirse en una limitada asignación de recursos para actividades de análisis, mantenimiento de inventarios o seguimiento de planes de tratamiento, comprometiendo la continuidad del proceso.

- **Discontinuidad en el seguimiento de planes de acción**

Incluso cuando los análisis de riesgos se realizan siguiendo las buenas prácticas establecidas en el sector, pueden perder efectividad si los planes de tratamiento no se implementan o no se realiza un seguimiento adecuado. La rotación de personal, los cambios de prioridades, las limitaciones presupuestarias y la ausencia de mecanismos de control sistemático provocan que muchas medidas queden aplazadas indefinidamente o se ejecuten solo parcialmente, dificultando la reducción real del riesgo.

- **Dependencia de fabricantes**

Los aspectos críticos de la seguridad de los dispositivos IoMT suelen depender de los fabricantes, cuyas decisiones, tiempos de actualización y prioridades comerciales no siempre coinciden con las necesidades asistenciales. La disponibilidad de parches, el soporte especializado o la posibilidad de aplicar medidas adicionales de protección pueden quedar fuera del control directo de la organización sanitaria.

Abordar eficazmente estos desafíos requiere un compromiso continuado orientado al fortalecimiento de capacidades internas, la colaboración entre organizaciones del sector, y una mayor exigencia a fabricantes y proveedores en materia de transparencia, seguridad y soporte.

El análisis de riesgos debe entenderse como un proceso continuo, integrado en la cultura de la organización sanitaria y en la gestión operativa del ciclo de vida completo de los dispositivos IoMT, y no como un ejercicio puntual centrado únicamente en el cumplimiento normativo.

5.3. Marcos de referencia para la gestión de riesgos

La gestión de riesgos en entornos IoMT se apoya en múltiples marcos metodológicos consolidados que proporcionan estructuras probadas y reconocidas internacionalmente. Estos marcos no son excluyentes entre sí, sino que se complementan ofreciendo perspectivas y herramientas que, combinadas adecuadamente, permiten construir un enfoque robusto adaptado a las particularidades del contexto sanitario español.

5.3.1. Estándares ISO

En el ámbito internacional, la familia de normas ISO/IEC proporciona los pilares para estructurar la gestión de riesgos de forma sistemática y coherente con las mejores prácticas. Estas normas crean un lenguaje común que facilita la comunicación entre organizaciones, la interoperabilidad con otros marcos y la alineación con requisitos regulatorios.

- **IEC/ISO 80001-1:2021- Application of risk management for IT-networks incorporating medical devices**

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

Establece los principios y requisitos para la aplicación de la gestión de riesgos cuando dispositivos médicos y/o software sanitario se conectan a redes TI sanitarias. Define roles, responsabilidades y actividades necesarias para preservar la seguridad de la persona paciente, la eficacia clínica y la ciberseguridad a lo largo de todo el ciclo de vida de la conexión. Se alinea con la ISO 31000 y constituye la norma central para la gestión del riesgo organizativo en entornos IoMT.

- **IEC/ISO 81001-1 - Health software and health IT systems (safety, effectiveness, security)**

Proporciona un marco de gobernanza específico para el software sanitario y los sistemas TI clínicos, estableciendo una terminología común y requisitos relacionados la seguridad de la información. Complementa a la ISO 80001-1 cuando el software clínico forma parte de ecosistemas conectados que incluyen dispositivos médicos.

- **ISO 14971- Application of risk management to medical devices**

Norma de referencia para la identificación, evaluación, control y seguimiento de los riesgos asociados a productos sanitarios a lo largo de su ciclo de vida, incluyendo dispositivos que operan en modelos SaaS. En contexto IoMT, se aplica al riesgo inherente al dispositivo, el cual debe integrarse tras la gestión del riesgo definida en la ISO 80001-1.

- **ISO/TR 24971 - Guidance on the application of ISO 14971**

Guía que detalla la implementación práctica de la ISO 14971, proporcionando criterios sobre estimación de probabilidad, selección de medidas de control, evaluación beneficio-riesgo y generación de evidencias. Resulta especialmente útil para homogeneizar los análisis de riesgos de dispositivos IoMT antes de su integración en redes clínicas.

- **ISO 31000 - Risk management — Guidelines**

Marco transversal para establecer, implementar y mejorar la gestión del riesgo a nivel corporativo, definiendo principios, estructura organizativa y procesos. En entornos IoMT garantiza la coherencia organizativa y sirve como base conceptual para la estructura de gestión del riesgo definida en la ISO 80001-1.

- **ISO/IEC 27001 - Information Security Management Systems (ISMS)**

Define los requisitos para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a proteger la confidencialidad, integridad y disponibilidad de la información. En IoMT enmarca políticas y controles sobre datos clínicos, servicios de telemetría y plataformas de soporte, así como los procesos de auditoría y mejora continua.

- **ISO/IEC 27005 - Information security risk management**

Proporciona una guía metodológica para la gestión de riesgos de seguridad de la información, abordando activos, amenazas, vulnerabilidades e impacto. En IoMT facilita la identificación, cuantificación y priorización de riesgos técnicos asociados a pasarelas, APIs, sistemas PACS/EHR y redes clínicas.

- **ISO/IEC 27035 - Information security incident management**

Establece un marco para la gestión de incidentes de seguridad de la información, cubriendo las fases de preparación, detección, análisis, respuesta y lecciones aprendidas. En IoMT vincula el riesgo residual con

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

la capacidad de respuesta ante incidentes que puedan afectar a dispositivos médicos conectados o a servicios asistenciales críticos.

- **ISO/IEC 27701 - Privacy Information Management (PIMS)**

Extiende las normas ISO/IEC 27001 y 27002 para la gestión de la privacidad de la información, definiendo roles de responsable y encargado del tratamiento, así como controles específicos. En IoMT orienta la gobernanza de los datos de salud en los flujos entre dispositivos y plataformas, alineando de forma coherente los requisitos de seguridad y protección de datos personales.

- **ISO/IEC 22301 - Business continuity management systems**

Define los requisitos para un Sistema de Gestión de Continuidad de Negocio (SGCN), incluyendo análisis de impacto en el negocio (BIA), estrategias y planes de continuidad, así como pruebas periódicas. En IoMT garantiza la disponibilidad asistencial frente a fallos de dispositivos críticos, interrupciones de conectividad o indisponibilidad de repositorios clínicos causadas por incidentes o actividades de mantenimiento.

5.3.2. Marco de ciberseguridad del NIST

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha desarrollado un conjunto de marcos y guías ampliamente adoptados en el ámbito sanitario internacional para la gestión y el análisis de riesgos de ciberseguridad, incluidos aquellos asociados a entornos IoMT. Estos marcos permiten abordar el riesgo de forma sistemática, integrando aspectos técnicos, organizativos y clínicos, y son especialmente relevantes en organizaciones sanitarias con infraestructuras digitales complejas y dispositivos médicos conectados.

- **NIST Cybersecurity Framework (CSF)**

El NIST Cybersecurity Framework establece un marco de referencia de alto nivel para la gestión del riesgo de ciberseguridad a nivel organizativo. Su estructura, articulada en las funciones de identificar, proteger, detectar, responder y recuperar, facilita una visión integral del ciclo de vida de la seguridad y permite evaluar el grado de madurez de una organización frente a amenazas que afectan a sistemas, redes y dispositivos IoMT.

En el contexto IoMT, el CSF se utiliza como marco de gobernanza, alineando la gestión de riesgos de ciberseguridad con la seguridad de la persona paciente, la continuidad asistencial y la resiliencia operativa. Asimismo, sirve como estructura para integrar normas y guías más específicas, como la ISO 80001-1, la ISO/IEC 27001 o la ISO 14971.

- **NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments**

La NIST Special Publication 800-30 proporciona una metodología detallada para la realización de análisis de riesgos de ciberseguridad, basada en la identificación de activos, amenazas, vulnerabilidades, así como la probabilidad e impacto asociado. A diferencia del CSF, que opera a un nivel estratégico, la SP 800-30 se centra en el análisis técnico y operativo del riesgo.

Aplicada a entornos IoMT, esta guía permite evaluar de forma sistemática los riesgos asociados a dispositivos médicos conectados y su integración con sistemas clínicos como EHR o PACS.

- **NIST SP 800-37 Rev. 2 – Risk Management Framework (RMF)**

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

La NIST SP 800-37 define el Risk Management Framework (RMF), un marco que integra la gestión del riesgo de ciberseguridad en todas las fases del ciclo de vida de los sistemas de información. En entornos IoMT, el RMF facilita la asignación de responsabilidades, la gestión de sistemas en base al riesgo y la supervisión continua de dispositivos conectados.

Este enfoque resulta especialmente útil para organizaciones sanitarias con infraestructuras IoMT complejas, ya que permite gestionar de forma coherente los riesgos desde la adquisición del dispositivo médico hasta su operación y retirada.

5.3.3. MAGERIT v3

En el ámbito nacional, MAGERIT v3 constituye la metodología de referencia para el análisis y gestión de riesgos de los sistemas de información en las administraciones públicas. Desarrollada por el Consejo Superior de Administración Electrónica (CSAE), ofrece un enfoque sistemático alineado con el ENS y adaptado al marco normativo español. Su aplicación en el ámbito sanitario público facilita el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información y protección de datos.

Los principales elementos que aporta MAGERIT v3 son:

- Metodología detallada para la valoración de activos: Permite identificar y evaluar los activos de información considerando las dimensiones del ENS, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Catálogo de amenazas: Incluye un repertorio extenso de amenazas que pueden afectar a los sistemas de información, clasificadas según su origen y naturaleza, lo que facilita su análisis sistemático.
- Criterios de probabilidad e impacto: Proporciona criterios para estimar la probabilidad de materialización de cada amenaza y el impacto potencial sobre los activos, permitiendo priorizar los riesgos.
- Catálogo de salvaguardas: Incluye medidas de seguridad y controles que se pueden seleccionar de forma proporcionada al nivel de riesgo identificado, favoreciendo un enfoque basado en mitigación proporcional.
- Guías de aplicación: Facilita la implementación práctica de la metodología en diferentes contextos organizativos, adaptándose a la complejidad de cada sistema.
- Herramientas de soporte: Incluye aplicaciones como PILAR, que permiten automatizar parcialmente el proceso de análisis de riesgos siguiendo los pasos definidos por MAGERIT.

En conjunto, MAGERIT v3 proporciona un marco robusto y sistemático que integra valoración de activos, análisis de amenazas y selección de controles, constituyéndose en una herramienta clave para la gestión de riesgos de los sistemas de información en el sector público español, incluyendo el ámbito sanitario.

5.3.4. Recursos del Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN), como organismo responsable de la seguridad de los sistemas de información del sector público español, ofrece recursos complementarios que facilitan la aplicación

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

práctica de marcos como MAGERIT y el ENS, adaptándolos a contextos específicos, incluido el sector sanitario.

Entre los recursos más relevantes se encuentran:

- Guías CCN-STIC: Publicaciones que desarrollan aspectos específicos de seguridad, algunas de ellas orientadas a la protección de sistemas críticos del ámbito sanitario, como:
    - CCN-STIC 800: Guía de gestión de riesgos de los sistemas de información.
    - CCN-STIC 801: Guía de gestión de riesgos aplicable a entornos con datos sanitarios
- Herramienta PILAR: Permite realizar análisis y gestión de riesgos de manera automatizada siguiendo MAGERIT y el ENS, facilitando la identificación de activos, amenazas y controles.
- Servicios de alerta temprana: Proporciona información sobre vulnerabilidades y amenazas que afectan a sistemas de información, permitiendo una gestión proactiva de riesgos.
- Capacidades de respuesta ante incidentes: A través del CCN-CERT, ofrece asistencia a entidades del sector público en la detección, contención y mitigación de incidentes de seguridad.

La elección de un marco concreto o de una combinación de varios dependerá de las características de la organización, sus obligaciones normativas y su nivel de madurez en gestión de riesgos. No obstante, lo fundamental no es adoptar un marco único, sino aplicar de forma consistente un enfoque estructurado de gestión de riesgos que permita tomar decisiones informadas sobre la protección de dispositivos médicos conectados y los datos de salud que estos procesan.

6. Instrucciones de uso de la guía

El presente documento establece un procedimiento estructurado para llevar a cabo un análisis de riesgos en entornos IoMT, definiendo las actividades, criterios y decisiones necesarias en cada fase del proceso. Su objetivo es proporcionar una metodología homogénea a alto nivel que permita a las organizaciones sanitarias identificar, evaluar y tratar los riesgos asociados a los dispositivos médicos conectados.

Asimismo, la guía está diseñada para facilitar su aplicación práctica, permitiendo que cada organización adapte las fases a su propio contexto tecnológico, asistencial y operativo. Aunque cada etapa incorpora criterios claros, escalas concretas y decisiones bien definidas, estos pueden ajustarse para reflejar las características específicas y las necesidades particulares de cada entidad sanitaria.

A continuación, se presentan de forma ilustrativa las instrucciones de uso de la guía, resumidas en un diagrama que muestra la secuencia completa del análisis de riesgos IoMT, desde la identificación de activos hasta el tratamiento del riesgo y su revisión continua:

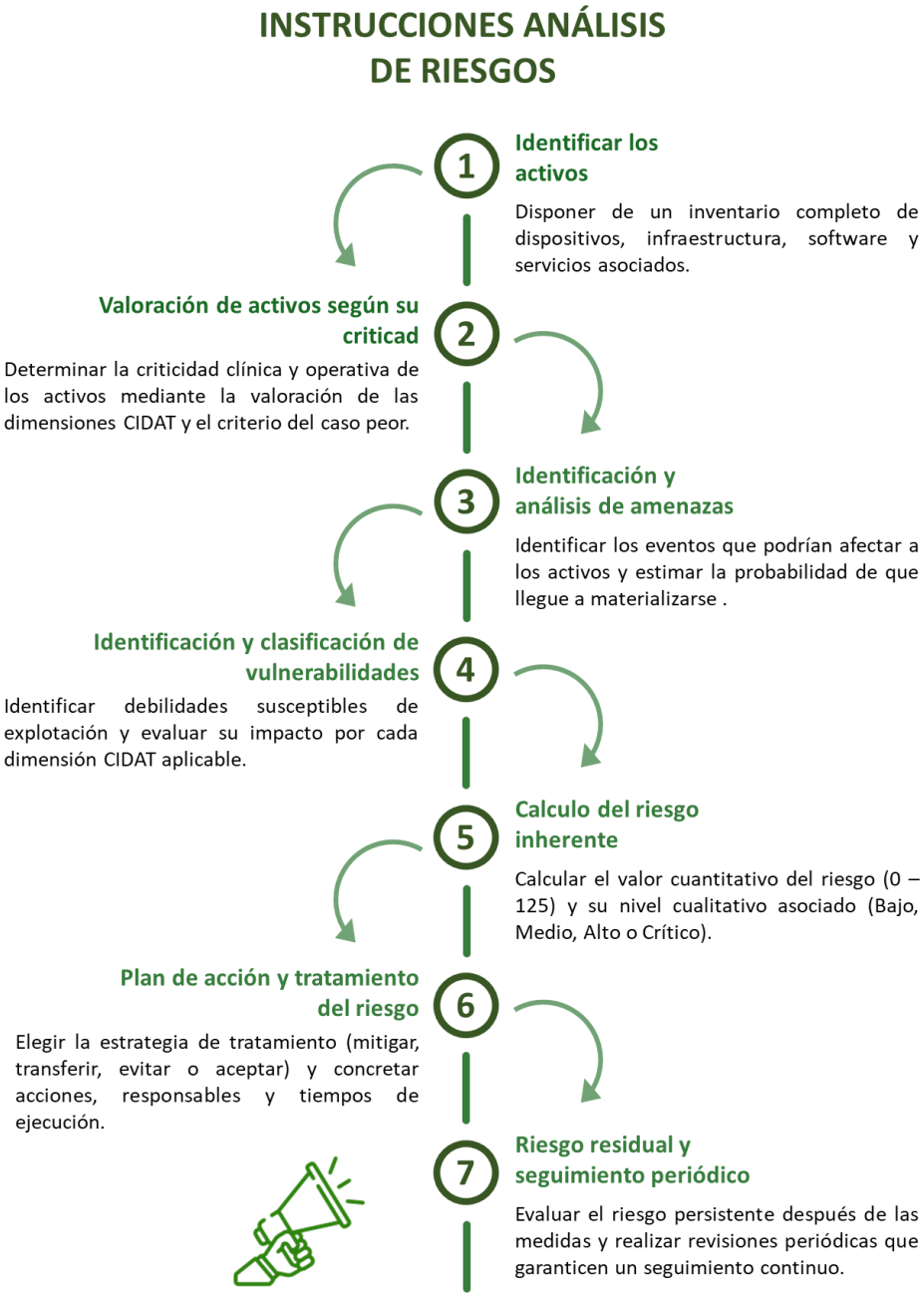

ILUSTRACIÓN 1: INSTRUCCIONES DE USO GUÍA.

7. Identificación de activos

La protección de los dispositivos médicos conectados comienza por conocer con exactitud qué dispositivos existen dentro de la organización. Aunque esta premisa pueda parecer evidente, constituye uno de los retos más significativos para muchas organizaciones sanitarias españolas, donde la evolución orgánica de la infraestructura tecnológica ha provocado la existencia de inventarios incompletos, fragmentados o desactualizados.

7.1. Activos en el contexto IoMT

Se considera activo a cualquier elemento que aporta valor a la organización y que, por ello, requiere protección. En el ámbito del IoMT, esta definición abarca un conjunto de dispositivos amplio y heterogéneo que va más allá del equipamiento informático tradicional.

La identificación de activos en el entorno IoMT implica reconocer todos los elementos, tanto tangibles como intangibles, que participan en la prestación de servicios clínicos conectados. Este ecosistema combina equipos médicos, infraestructura de red, software especializado, servicios externos y datos clínicos altamente sensibles, conformando un entorno complejo y dinámico.

Comprender qué activos existen, cómo interactúan entre sí y de qué recursos dependen es un requisito indispensable para evaluar riesgos, aplicar medidas de seguridad adecuadas y garantizar la continuidad asistencial. A partir de esta perspectiva integral, es posible estructurar y clasificar los activos del IoMT para facilitar su gestión, priorizar su protección y asegurar que cada uno reciba el nivel de control que requiere.

A continuación, se describen las principales categorías de activos que conforman un entorno IoMT típico, comenzando por los dispositivos médicos y extendiéndose posteriormente a la infraestructura técnica, los datos, el software y los servicios asociados.

❖ Dispositivos médicos

Los dispositivos médicos constituyen el primer grupo fundamental de activos dentro del entorno IoMT. Este conjunto incluye:

- Equipos de diagnóstico por imagen, como resonancias magnéticas (RM), tomografía computarizada (TAC), radiología digital o ecógrafos.
- Dispositivos de monitorización de constantes vitales.
- Equipos de soporte vital, como bombas de infusión programables, ventiladores mecánicos o sistemas de anestesia.
- Dispositivos implantables con capacidades de comunicación, entre ellos marcapasos, desfibriladores implantables y bombas de insulina.

Cada uno de estos dispositivos presenta ciclos de vida específicos, distintos requisitos de mantenimiento y perfiles de riesgo particulares que deben documentarse de forma exhaustiva.

❖ Infraestructura de comunicaciones

La conectividad de los dispositivos IoMT se sustenta en la infraestructura de red clínica, considerada un activo crítico para la continuidad y seguridad operativa. Esta infraestructura incluye:

- Redes hospitalarias cableadas e inalámbricas.
- Equipamiento de comunicaciones como switches, routers y puntos de acceso.
- Pasarelas y sistemas de integración que permiten la conexión de los dispositivos con la historia clínica electrónica y otros sistemas asistenciales.

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

En el caso de dispositivos instalados en el domicilio de la persona paciente, la infraestructura comprende también las conexiones con el entorno doméstico.

❖ **Datos**

Los datos generados, tratados o transmitidos por los dispositivos IoMT representan uno de los activos más sensibles y valiosos. Entre ellos se incluyen:

- Información clínica de personas pacientes.
- Registros operacionales de los dispositivos.
- Parámetros de configuración.
- Credenciales y autorizaciones.

La pérdida, modificación o divulgación no autorizada de estos datos puede generar consecuencias graves tanto para la organización sanitaria como para las personas pacientes.

❖ **Software y firmware**

Este grupo engloba los sistemas operativos, firmware, aplicaciones clínicas y algoritmos embebidos que permiten el funcionamiento de cada dispositivo. La integridad y actualización adecuada de estos componentes es esencial para garantizar la seguridad de la persona paciente y la estabilidad operativa de los equipos.

❖ **Servicios externos**

Aunque frecuentemente no se incluyen en los inventarios tradicionales, los servicios externos forman parte esencial del ecosistema IoMT. Entre ellos destacan:

- Servicios de actualización y soporte proporcionados por los fabricantes.
- Plataformas en la nube utilizadas para almacenamiento, análisis o procesamiento de datos.
- Servicios de mantenimiento remoto y monitorización técnica.

Todos estos servicios constituyen dependencias críticas que deben identificarse y evaluarse adecuadamente al gestionar riesgos y proteger el entorno clínico conectado.

7.2. Cómo realizar un inventario efectivo

La elaboración de un inventario de activos IoMT requiere un enfoque multidisciplinar que combine información procedente de varias áreas de la organización. Los servicios de ingeniería clínica mantienen habitualmente los registros de los equipos médicos bajo su responsabilidad, mientras que los departamentos de tecnologías de la información gestionan los inventarios de la infraestructura de red y de los sistemas de información. La integración de estas fuentes, junto con la aportación de los servicios clínicos que utilizan los dispositivos, permite obtener una visión completa y precisa del ecosistema tecnológico asistencial.

Para cada activo identificado, es recomendable documentar un conjunto mínimo de atributos que facilitarán las fases posteriores del análisis de riesgos y la definición de controles de seguridad. Entre estos atributos destacan la denominación del activo, su ubicación física y lógica dentro de la red, el

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

fabricante y modelo, la versión del software o firmware instalado, la fecha de adquisición y la prevista de fin de vida útil, así como la persona responsable asignada y las dependencias con otros sistemas.

El inventario debe concebirse como un proceso dinámico, no como una actividad puntual. Los procedimientos de gestión del cambio deben garantizar que cualquier alta, baja o cambio de activos quede reflejada de forma oportuna y consistente.

7.2.1. Clasificación por tipología

Para facilitar la gestión y la aplicación de políticas de seguridad diferenciadas, se propone clasificar los dispositivos IoMT según sus características técnicas y funcionales. Esta organización permite identificar patrones de riesgo comunes y priorizar medidas de protección. Las tipologías recomendadas incluyen:

- **Dispositivos de diagnóstico por imagen**: resonancias magnéticas, tomógrafos, equipos de radiología digital o ecógrafos, que generan grandes volúmenes de información y requieren conectividad con sistemas de archivo de imágenes.
- **Dispositivos de monitorización de personas pacientes**: monitores de constantes vitales, telemetrías y sistemas de vigilancia en tiempo real, cuya disponibilidad es crítica en unidades asistenciales como UCI.
- **Dispositivos de soporte vital y tratamiento**: ventiladores mecánicos, bombas de infusión, equipos de diálisis o sistemas de anestesia, donde la integridad de los parámetros operativos afecta directamente a la seguridad de la persona paciente.
- **Dispositivos implantables con comunicación**: marcapasos, desfibriladores implantables o bombas de insulina, que presentan superficies de ataque particulares y requieren consideraciones específicas de seguridad.
- **Dispositivos de laboratorio y diagnóstico in vitro**: analizadores automáticos, equipos de microbiología o sistemas de anatomía patológica, que procesan muestras y generan resultados clínicos.
- **Dispositivos de monitorización domiciliaria**: pulsioxímetros conectados, tensiómetros inteligentes o glucómetros con transmisión de datos, que operan fuera del perímetro controlado de la organización sanitaria.
- **Infraestructura de soporte**: pasarelas de comunicación, concentradores de datos, servidores de integración y equipamiento de red específico del entorno clínico.

7.2.2. Clasificación por criticidad clínica

Cada activo debe valorarse según su criticidad clínica, considerando el impacto que tendría su compromiso o indisponibilidad. Cuando aplique, esta valoración debe alinearse con las categorías de riesgo definidas en el MDR y el IVDR, que clasifican los dispositivos en función del riesgo inherente y de las posibles consecuencias para la persona paciente en caso de fallo.

A partir de esta perspectiva, los activos IoMT pueden clasificarse según su criticidad clínica en los siguientes niveles:

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

- **Criticidad muy alta (MDR-Clase III, IVDR-Clase D)**: dispositivos cuyo fallo puede causar daño grave o irreversible a la persona paciente, como equipos de soporte vital activos, sistemas de administración de medicamentos de alto riesgo o dispositivos implantables.
- **Criticidad alta (MDR-Clase IIb, IVDR-Clase C)**: dispositivos esenciales para la continuidad asistencial en áreas críticas, cuya indisponibilidad prolongada obligaría a derivar personas pacientes o suspender procedimientos (p. ej., tomógrafos en urgencias o monitores en UCI).
- **Criticidad media (MDR-Clase IIa, IVDR-Clase B)**: dispositivos que apoyan procesos relevantes pero con alternativas disponibles o cuyo impacto es limitado ante una indisponibilidad temporal, como equipos de diagnóstico en consultas programadas.
- **Criticidad baja (MDR-Clase I, IVDR-Clase A)**: equipos auxiliares o de impacto reducido, con alternativas simples o rápida recuperación, como dispositivos administrativos en entornos clínicos o equipos redundantes disponibles.

7.2.3. Registro de activos

Para cada activo inventariado, se recomienda documentar al menos los siguientes elementos, con el fin de asegurar su identificación precisa y disponer de la información necesaria para su gestión y análisis posterior:

- **Identificación**: identificador único, número de serie o cualquier otro dato que permita localizar el activo de forma inequívoca.
- **Información del fabricante**: nombre, modelo, versión de hardware y datos de soporte técnico.
- **Información de software**: sistema operativo, versión de firmware, aplicaciones clínicas y fecha de la última actualización aplicada.
- **Ubicación física**: edificio, planta, servicio y sala, además de si el dispositivo es fijo o portátil.
- **Ubicación lógica**: dirección IP, segmento de red, VLAN asignada y puertos de comunicación.
- **Ciclo de vida**: fecha de adquisición, puesta en servicio, fin de vida útil previsto y estado actual del soporte del fabricante.
- **Personas responsables**: persona propietaria funcional, servicio clínico responsable y personal técnico de mantenimiento.
- **Dependencias**: conexiones con otros sistemas, servicios externos asociados y activos que dependen del dispositivo.
- **Clasificación de seguridad**: tipología asignada, nivel de criticidad y valoración según las dimensiones CIDAT.
- **Protocolos de comunicación**: descripción de los protocolos empleados por el dispositivo, tanto estándar como propietarios, incluyendo los puertos y servicios utilizados, los flujos de comunicación habituales y cualquier patrón relevante de intercambio de datos.

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

8. Valoración de activos según CIDAT

Una vez identificados los activos, el siguiente paso consiste en determinar su valor para la organización. Esta valoración se fundamenta principalmente en el impacto que tendría, tanto para la organización como para las personas pacientes, la pérdida de cualquiera de las propiedades de seguridad asociadas al activo.

8.1. Dimensiones de seguridad ENS

El modelo CIDAT del ENS ofrece un marco para analizar la seguridad de la información a través de cinco dimensiones de seguridad complementarias. Cada una de ellas representa una propiedad que debe preservarse a lo largo del ciclo de vida del activo.

❖ Confidencialidad

La confidencialidad garantiza que la información únicamente sea accesible a personas, entidades o procesos autorizados. En el ámbito sanitario, esta dimensión es especialmente crítica por el carácter sensible de los datos clínicos, protegidos específicamente por el RGPD y la LOPDGDD.

Un incidente de confidencialidad puede manifestarse, por ejemplo, mediante el acceso no autorizado a registros de monitorización o la interceptación de comunicaciones entre un dispositivo implantable y su programador externo.

❖ Integridad

La integridad se refiere a la exactitud y completitud de la información y de los métodos de procesamiento. En dispositivos médicos, esta propiedad resulta crítica no solo para los datos gestionados, sino también para la propia configuración y funcionamiento del equipo.

Alteraciones en los parámetros de una bomba de infusión o manipulaciones en los valores mostrados por un monitor de constantes vitales pueden derivar en riesgos directos para la seguridad de la persona paciente, convirtiendo un fallo de integridad en un incidente potencialmente grave.

❖ Disponibilidad

La disponibilidad garantiza que la información y los sistemas estén accesibles y operativos cuando se necesiten. En entornos asistenciales, los dispositivos médicos forman parte de procesos críticos de diagnóstico y tratamiento, por lo que la pérdida de disponibilidad puede provocar retrasos, necesidad de recurrir a métodos alternativos o incluso imposibilidad de prestar asistencia vital.

Los ataques de ransomware que han afectado a instituciones sanitarias en los últimos años ilustran el impacto severo que puede derivarse de la indisponibilidad de sistemas esenciales.

❖ Autenticidad

La autenticidad asegura que un activo es quien dice ser o que la información procede de la fuente legítima. En un ecosistema IoMT, esta propiedad permite verificar que un dispositivo que se conecta a la red es legítimo, que las instrucciones enviadas a un equipo proceden de un sistema autorizado o que los datos almacenados corresponden realmente a la persona paciente identificado.

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

La falta de autenticidad abre la puerta a suplantaciones, inyecciones de comandos y alteraciones de datos clínicos.

- **Trazabilidad**

También denominada responsabilidad o no repudio, la trazabilidad permite conocer quién realizó una acción, cuándo y sobre qué activo. Esta dimensión es esencial para investigar incidentes de seguridad, auditar actividades y cumplir con las obligaciones legales de registro de accesos a datos sanitarios establecidas por la normativa de protección de datos.

Una trazabilidad adecuada facilita la detección de usos indebidos, el análisis forense y la atribución de responsabilidades.

8.2. Proceso de valoración

La valoración de cada activo debe realizarse evaluando de forma independiente cada una de las cinco dimensiones de seguridad del modelo CIDAT, dado que el impacto de un fallo puede variar significativamente según la propiedad comprometida. Así, un mismo dispositivo puede requerir niveles muy elevados de integridad y disponibilidad, mientras que su confidencialidad puede ser menos crítica si no almacena datos clínicos identificables.

Para garantizar un análisis coherente y comparable entre activos, se utiliza una escala homogénea de niveles de impacto. Esta escala suele abarcar desde un nivel mínimo, asociado a activos cuya afectación tendría un impacto despreciable, hasta un nivel máximo reservado para aquellos cuyo compromiso podría provocar daños muy graves o irreversibles. El número de niveles puede adaptarse a las necesidades de la organización, no obstante, son habituales las escalas de tres, cuatro o cinco niveles.

En este caso, se ha empleado la escala utilizada por el ENS definida en la guía CCN-STIC 803, la cual establece 4 niveles para cada una de las dimensiones. Su elección se debe a que es ampliamente conocida y utilizada para la realización de análisis de riesgos en las entidades públicas.

El proceso de asignación requiere la participación de perfiles profesionales complementarios, como personal clínico, capaz de evaluar las implicaciones asistenciales, especialistas en ingeniería clínica, que conocen las características técnicas y operativas de los dispositivos, y personas responsables de protección de datos, que aportan la perspectiva normativa y de cumplimiento.

Una vez asignado el nivel correspondiente en cada dimensión, se obtiene una caracterización completa del activo en términos de requisitos de seguridad.

Finalmente, la criticidad global del activo se determina aplicando el criterio del caso peor, es decir, la criticidad final del activo será el nivel más alto que presente en cualquiera de las cinco dimensiones.

Este valor será utilizado en las fases posteriores del análisis de riesgos para calcular el riesgo asociado y establecer las medidas de seguridad necesarias para su mitigación.

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

Nivel	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
1	**No aplicable**	**No aplicable**	**No aplicable**	**No aplicable**	**No aplicable**
	Información que puede ser de dominio público sin restricciones. No contiene datos de personas pacientes ni información sensible	La pérdida de exactitud no tendría repercusión asistencial. El esfuerzo de corrección es mínimo	El dispositivo puede estar inoperativo durante días o semanas sin afectar a la atención sanitaria. Existen alternativas inmediatas	No es necesario verificar el origen de la información o la identidad del dispositivo	No existe obligación legal ni necesidad operativa de registrar accesos o acciones realizadas
2	**Bajo**	**Bajo**	**Bajo**	**Bajo**	**Bajo**
	Información de uso interno compartible con proveedores autorizados. No incluye datos clínicos identificable	La información errónea no afecta decisiones clínicas y pueden corregirse en menos de una jornada sin consecuencias	Puede tolerarse la indisponibilidad del dispositivo durante varios días mediante procedimientos alternativos	Se requiere una verificación básica de identidad. El impacto de una suplantación es limitado y fácilmente reversible	Se requiere un registro básico, sin obligación legal estricta. Los registros pueden conservarse durante períodos cortos
3	**Medio**	**Medio**	**Medio**	**Medio**	**Medio**
	Información que debe permanecer dentro de la organización. Puede incluir datos pseudonimizados o datos operativos sensibles	Un error en la información puede afectar a la calidad asistencial pero no de forma crítica. Requieren esfuerzo de corrección	Debe recuperarse en <24 horas. Su caída afecta a la eficiencia de los servicios pero no compromete la atención sanitaria urgente	Es necesario verificar la identidad de personas usuarias y dispositivos. Una suplantación podría requerir una investigación y acciones correctivas	Existe obligación legal de mantener registros de acceso a datos sanitarios. Deben conservarse según los plazos establecidos por la normativa de protección de datos.
4	**Alto**	**Alto**	**Alto**	**Alto**	**Alto**
	Información cuya divulgación podría en riesgo la integridad de personas, como datos de	La información es crítica para la seguridad del paciente. Un error podría causar daño grave o	El dispositivo debe tener disponibilidad continua 24x7 los 365 días. Cualquier interrupción	La autenticación debe ser inequívoca y resistente a cualquier intento de suplantación.	Se requiere registro exhaustivo e inalterable de toda actividad, con garantías de integridad

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

Nivel	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	personas pacientes protegidas o información genética sensible. Su compromiso tendría consecuencias irreversibles.	irreversible, como parámetros incorrectos en dispositivos de soporte vital o dosis erróneas en sistemas de infusión. No existe margen para el error.	puede poner en riesgo inmediato la vida de personas pacientes.	Un fallo podría permitir el control no autorizado de dispositivos de soporte vital o el acceso a información cuya divulgación pondría en riesgo la vida de personas.	que permitan su uso como evidencia legal. Incluye sellado de tiempo y protección contra manipulación de los propios registros.

TABLA 2: CLASIFICACIÓN DE ACTIVOS.

9. Identificación y análisis de amenazas

Una vez identificados y valorados los activos IoMT, el siguiente paso del proceso de análisis de riesgos consiste en identificar y analizar las amenazas que podrían comprometer las dimensiones de seguridad de estos activos.

Las amenazas representan eventos, acciones o condiciones que, de materializarse, pueden causar un daño directo sobre los dispositivos médicos conectados, la infraestructura clínica o los datos que gestionan.

En el ámbito IoMT, estas amenazas pueden originarse dentro o fuera del perímetro de la organización sanitaria, y abarcan tanto ataques deliberados como fallos accidentales o condiciones físicas del entorno. Para facilitar su análisis, se clasifican en tres grandes categorías: amenazas técnicas, amenazas físicas y amenazas relativas a la privacidad e integridad de los datos clínicos.

9.1. Tipología de amenazas relevantes para IoMT

El catálogo de amenazas que afecta a dispositivos IoMT es amplio y evoluciona de forma constante. Sin embargo, todas ellas pueden agruparse en tres familias que permiten estructurar el análisis y guiar al lector en la identificación de los riesgos que deben considerarse.

Estas categorías son:

- **Amenazas técnicas**, relacionadas con software, redes, autenticación, comunicaciones o la integración con otros sistemas.
- **Amenazas físicas**, derivadas de la manipulación, acceso físico o condiciones ambientales que afectan al hardware.
- **Amenazas a la privacidad e integridad de los datos clínicos**, que comprometen la confidencialidad, autenticidad o veracidad de la información.

A continuación se detallan cada una de ellas.

9.1.1. Amenazas técnicas

Las amenazas técnicas son las más frecuentes y constituyen el núcleo de los riesgos en el ecosistema IoMT. Afectan directamente al software, a los sistemas, a las comunicaciones de red y a las plataformas clínicas conectadas.

Un ciberataque exitoso puede provocar alteración de datos médicos, mal funcionamiento de equipos diagnósticos o terapéuticos, e incluso acceso no autorizado a información clínica sensible, con consecuencias directas sobre la seguridad de la persona paciente.

Entre las amenazas técnicas se incluyen:

❖ **Amenazas relacionadas con el software médico**

El software es uno de los elementos más críticos en los dispositivos IoMT. La explotación de vulnerabilidades en firmware, sistemas operativos o aplicaciones clínicas puede comprometer la integridad de los datos, la correcta ejecución del tratamiento o la seguridad de la persona paciente. Estas

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

amenazas se materializan cuando un atacante logra explotar debilidades en el software de los dispositivos, sistemas sanitarios o plataformas clínicas.

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

- 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 cuentas de usuario: 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 de software en un dispositivo IoMT no solo afecta a la información procesada, sino que puede traducirse en errores terapéuticos, lecturas erróneas o incluso riesgo vital para la persona paciente.

❖ Ataque sobre credenciales o autenticación clínica

La autenticación débil en dispositivos, consolas de gestión o plataformas clínicas es uno de los vectores más explotados en entornos sanitarios. Muchos equipos permiten accesos administrativos sin mecanismos de autenticación multifactor, con contraseñas por defecto o con mecanismos pobres de control de cuentas de usuario.

Entre los ataques más comunes:

- Fuerza bruta o diccionario 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.

❖ Amenazas derivadas de la exposición a redes hospitalarias o Internet

Muchos dispositivos IoMT permanecen conectados de forma permanente a redes sanitarias o incluso a Internet para actualizaciones, telemetría o mantenimiento remoto.

Sin medidas adecuadas de segmentación o cifrado, se convierten en objetivos directos para atacantes.

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.

❖ **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.

En entornos clínicos, la pérdida de disponibilidad puede traducirse en retrasos diagnósticos, interrupciones terapéuticas o riesgo vital para la persona paciente.

❖ **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 a la persona paciente.

9.1.2. 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 a la persona 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

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

firmware, clonar dispositivos o incluso comprometer la seguridad de la persona paciente y la continuidad de los servicios clínicos críticos.

Entre las amenazas físicas se incluyen:

❖ **Acceso físico o manipulación directa**

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

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 de la persona paciente.

❖ **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 de la persona paciente.

❖ **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.

9.1.3. 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 las personas pacientes, recopilando información clínica.

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

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

Entre las amenazas a la integridad y privacidad se incluyen:

❖ 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 personas pacientes.
- 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.

❖ 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 de la persona paciente.

❖ 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 de la persona paciente.

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

❖ 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.

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

9.2. Estimación de probabilidad

Una vez identificada la amenaza aplicable a un activo, el siguiente paso consiste en estimar su probabilidad de materialización. Esta valoración indica la frecuencia esperada con la que la amenaza podría llegar a ocurrir dentro del contexto de la organización, teniendo en cuenta tanto el entorno operativo como el nivel de protección del activo.

Con el fin de garantizar un criterio homogéneo entre distintos evaluadores y mantener la coherencia metodológica, la probabilidad se estima utilizando la escala cualitativa de cinco niveles definida por MAGERIT v3.0. Esta escala se basa en la frecuencia temporal del acontecimiento y permite obtener una clasificación coherente, comparable y justificable, que facilite la priorización de riesgos y la toma de decisiones informadas.

❖ Como asignar el nivel de probabilidad

Para seleccionar el nivel adecuado, el evaluador debe determinar, de manera razonada, la frecuencia con la que la amenaza podría materializarse en el contexto del activo. En este sentido, se deben analizar los factores que influyen directamente en dicha probabilidad, entre los que se incluyen:

- Exposición del activo (conectividad, accesibilidad física, presencia en Internet, uso en domicilios).
- Vulnerabilidades conocidas (software sin parches, credenciales débiles, protocolos sin cifrar).
- Eficacia de los controles existentes (segmentación, autenticación robusta, monitorización, hardening).
- Historial de incidentes de la organización o el sector sanitario.
- Información externa procedente de organismos como INCIBE o ENISA.

A partir de este análisis, el evaluador debe identificar cuál de los cinco niveles de la tabla describe de forma más fiel la frecuencia esperable del acontecimiento en el entorno evaluado. Es importante que la elección esté justificada, incorporando una breve explicación que permita entender por qué se ha seleccionado un nivel concreto.

El objetivo no es alcanzar una precisión matemática, sino asegurar una clasificación coherente y razonada, que permita priorizar riesgos y adoptar decisiones consistentes.

Probabilidad	Definición
Muy Baja (1)	Acontecimiento poco probable, que podría experimentarse cada varios siglos
Baja (2)	Acontecimiento poco probable, que podría experimentarse cada varios años
Media (3)	Acontecimiento que se experimenta con una frecuencia anual

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

Probabilidad	Definición
Alta (4)	Acontecimiento que se experimenta con una frecuencia mensual
Muy Alta (5)	Acontecimiento que se experimenta frecuentemente, al menos diariamente

TABLA 3: ESTIMACIÓN PROBABILIDAD.

Es importante reconocer que esta estimación puede estar sujeta a cierto grado de incertidumbre, por lo que debe revisarse periódicamente y actualizarse cuando se detecten nuevas amenazas, cambios en los controles de seguridad o modificaciones en el entorno técnico o clínico.

El análisis debe considerar que la probabilidad de una amenaza puede variar significativamente según el activo considerado. Un dispositivo expuesto directamente a Internet presenta una probabilidad mucho mayor de sufrir intentos de intrusión que un equipo situado en un segmento de red aislado y sin conectividad externa. De igual modo, los dispositivos que almacenan grandes volúmenes de datos de personas pacientes resultan objetivos más atractivos para atacantes motivados por el robo de información que aquellos que procesan datos agregados o anonimizados.

10. Identificación y clasificación de vulnerabilidades

Tras identificar las amenazas relevantes para cada activo IoMT, el siguiente paso consiste en identificar las vulnerabilidades asociadas. Una vulnerabilidad es una debilidad, técnica, organizativa, humana o física, que puede ser explotada por una amenaza y que, por tanto, incrementa la probabilidad de que esta se materialice.

A diferencia de las amenazas, que describen qué podría ocurrir, las vulnerabilidades describen por dónde podría ocurrir. En el contexto IoMT, estas debilidades pueden encontrarse tanto en el propio dispositivo médico (software, firmware, configuración), como en la infraestructura de soporte (red, pasarelas, sistemas clínicos), en procesos operativos (mantenimiento, gestión de cambios) o en el entorno físico (acceso al equipo, custodia, puertos expuestos).

El objetivo de esta fase es doble:

- Determinar qué vulnerabilidades existen realmente en relación con las amenazas identificadas.
- Documentarlas de forma estructurada, para facilitar su valoración posterior y la definición de medidas de mitigación.

❖ Enfoque metodológico

La identificación de vulnerabilidades debe realizarse de manera sistemática, vinculándola a las amenazas previamente definidas. Para cada combinación activo–amenaza relevante, se debe averiguar que debilidades permitirían que esta amenaza afecte a este activo.

Este planteamiento asegura que la identificación de vulnerabilidades sea trazable, esté contextualizada y contribuya directamente al análisis de riesgos.

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

Además, permite distinguir entre vulnerabilidades realmente relevantes y aquellas que, aun siendo técnicamente posibles, no tienen impacto en el escenario evaluado.

❖ **Métodos para la identificación de vulnerabilidades**

La identificación de vulnerabilidades debe basarse en evidencias verificables y en múltiples fuentes de información que permitan comprender con precisión el estado real de los activos IoMT. Para ello, resulta necesario combinar distintos métodos que aportan perspectivas complementarias:

- **Inventario de activos**: información detallada sobre modelo, versión de firmware, sistema operativo, capacidades de conectividad, ubicación física y lógica, e integraciones con otros sistemas clínicos. Esta información permite detectar incompatibilidades, versiones obsoletas o configuraciones que podrían suponer debilidades.
- **Documentación del fabricante**: manuales técnicos, notas de seguridad, guías de configuración segura, ciclos de actualización y políticas de fin de soporte. Muchos fabricantes publican alertas de vulnerabilidades y requisitos específicos de hardening que deben revisarse periódicamente.
- **Observación y revisión de configuración**: análisis del dispositivo en funcionamiento, revisión de parámetros configurados, servicios habilitados, cuentas locales o remotas, reglas de red y controles de acceso. Este método permite detectar desviaciones respecto a las configuraciones recomendadas y descubrir riesgos que no aparecen en la documentación formal.
- **Procesos operativos**: evaluación de cómo se gestionan en la práctica el mantenimiento remoto, el soporte de terceros, la administración de credenciales, el control de cambios, y los procedimientos de altas y bajas. Una gestión operativa deficiente puede introducir vulnerabilidades no visibles mediante análisis técnicos.
- **Auditorías internas y revisiones previas**: resultados de pruebas de segmentación, controles de seguridad implantados, revisiones de cumplimiento y auditorías de hardening. Estos informes permiten identificar vulnerabilidades que ya han sido detectadas con anterioridad y evaluar si persisten por ausencia de medidas correctoras.
- **Información externa y fuentes especializadas**: boletines de seguridad publicados por fabricantes, alertas de organismos oficiales, como el CCN-CERT, INCIBE o ENISA, notificaciones de la AEMPS para dispositivos médicos, y bases de datos públicas de vulnerabilidades, como CVE, NVD o CERT/CC. Toda esta información debe contrastarse con el entorno real de la organización para determinar su aplicabilidad.

10.1. Naturaleza de las vulnerabilidades en entornos IoMT

Para facilitar su identificación, las vulnerabilidades se agrupan en cuatro categorías principales, siguiendo un enfoque metodológico coherente con ISO 27005 y MAGERIT, pero complementado con ejemplos específicos del entorno IoMT:

- **Vulnerabilidades técnicas**: debilidades en software, firmware, configuración, comunicaciones, integración e infraestructura de red.
- **Vulnerabilidades organizativas**: carencias en procesos, políticas, roles, gestión del cambio, mantenimiento y respuesta ante incidentes.

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

- **Vulnerabilidades humanas**: debilidades asociadas al comportamiento, formación y prácticas de personas usuarias y operadores.
- **Vulnerabilidades físicas**: debilidades derivadas del acceso físico al dispositivo, custodia, entorno ambiental y cadena de suministro.

A continuación, se detallan cada una de ellas:

❖ Vulnerabilidades técnicas

Las vulnerabilidades técnicas residen en los propios sistemas y configuraciones que soportan IoMT. Suelen deberse a defectos de diseño, errores de implementación, configuraciones inseguras o limitaciones de mantenimiento, muy comunes en dispositivos médicos debido a sus ciclos de vida y restricciones regulatorias.

Ejemplos:

- Firmware o sistemas operativos desactualizados, sin soporte ni parches.
- Servicios innecesarios habilitados (Telnet, FTP, SMB legacy, etc.).
- Comunicación sin cifrado o autenticación (DICOM, HL7 v2, MQTT inseguros).
- Contraseñas por defecto o sin políticas de complejidad.
- Puertos abiertos o configuraciones laxas en firewalls.
- Ausencia de validación criptográfica en actualizaciones de firmware.
- Integraciones con HIS, PACS, EHR o LIMS sin controles robustos.

❖ Vulnerabilidades organizativas

Las vulnerabilidades organizativas no se encuentran en un equipo concreto, sino en la forma en que la organización sanitaria gestiona y opera el ecosistema IoMT. Son especialmente relevantes en hospitales porque los equipos de ingeniería clínica, TI y sanitaria comparten responsabilidades, y cualquier vacío en procesos puede generar exposición.

Ejemplos:

- Ausencia de procedimientos de gestión de actualizaciones IoMT.
- Falta de segregación de funciones en ingeniería clínica o TI.
- Gestión deficiente de altas/bajas de cuentas en consolas de dispositivos.
- No disponer de un plan formal de respuesta ante incidentes IoMT.
- Registro y trazabilidad insuficientes en mantenimiento remoto.

❖ Vulnerabilidades humanas

Las vulnerabilidades humanas se relacionan con el comportamiento y prácticas de las personas que interactúan con IoMT: personal sanitario, ingeniería clínica, TI, ciberseguridad, proveedores o soporte. En entornos sanitarios, el factor humano es crítico porque la prioridad asistencial puede llevar a atajos operativos.

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

Ejemplos:

- Susceptibilidad a ingeniería social o phishing clínico.
- Uso de contraseñas débiles o compartidas entre turnos.
- Desconocimiento de políticas de seguridad o de procedimientos de acceso.
- Manipulación incorrecta de dispositivos sensibles o puertos.

❖ **Vulnerabilidades físicas**

Las vulnerabilidades físicas afectan a la protección material del dispositivo, su accesibilidad y su entorno. En IoMT son especialmente importantes porque muchos equipos están en zonas accesibles, son portátiles o se usan en domicilios, y pueden tener puertos de mantenimiento o componentes manipulables.

Ejemplos:

- Dispositivos en zonas abiertas o sin supervisión.
- Puertos USB/UART/JTAG accesibles.
- Ausencia de SAI o protección eléctrica en equipos críticos.
- Riesgos ambientales (temperatura, humedad, EMI).
- Equipos portátiles sin medidas de custodia.

10.2. Clasificación de vulnerabilidades según su impacto

Una vez identificadas las vulnerabilidades asociadas a cada activo, concretamente solo se valorarán las vulnerabilidades técnicas, el siguiente paso consiste en clasificarlas según el impacto que tendría su explotación. En este contexto, el impacto refleja el grado de daño que podría sufrir el dispositivo o el servicio si la vulnerabilidad fuera aprovechada con éxito por un atacante.

Para garantizar criterios homogéneos, comparables y acordes con estándares internacionales, se adopta la escala de impacto definida por el sistema CVSS (Common Vulnerability Scoring System). En este modelo, el impacto se expresa mediante una puntuación numérica entre 0.0 y 10.0, que se agrupa en cinco niveles cualitativos. Esta valoración permite determinar la severidad de la vulnerabilidad y establecer prioridades de mitigación.

La tabla siguiente recoge la descripción de los niveles de impacto basados en CVSS y debe emplearse como referencia para asignar la severidad correspondiente a cada vulnerabilidad.

Puntuación	Impacto	Definición
0.0	**Ninguno (0)**	No hay impacto en seguridad. La vulnerabilidad no afecta a la confidencialidad, integridad ni disponibilidad del dispositivo.
0.1 – 3.9	**Bajo (1-2)**	La vulnerabilidad tiene un impacto limitado en el dispositivo. El riesgo o la probabilidad de explotación es reducido.

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

Puntuación	Impacto	Definición
4.0 – 6.9	**Medio (3)**	La vulnerabilidad tiene un impacto moderado. Los ataques son posibles, pero requieren de condiciones específicas o cierto nivel de interacción de la persona usuaria.
7.0 – 8.9	**Alto (4)**	La vulnerabilidad tiene un impacto significativo. Su explotación es factible y puede afectar de forma severa a la confidencialidad, integridad o disponibilidad.
9.0 – 10.0	**Crítico (5)**	La vulnerabilidad es extremadamente grave. Generalmente, es fácil de explotar y puede comprometer por completo la seguridad o la operatividad del dispositivo afectado.

TABLA 4: CALCULO IMPACTO.

11. Cálculo del riesgo

Una vez completadas las fases anteriores, identificación y valoración de activos, identificación de amenazas con su probabilidad estimada y determinación de vulnerabilidades con su impacto, se dispone de los elementos necesarios para calcular el nivel de riesgo. Este cálculo representa el punto de convergencia del análisis y permite priorizar de forma objetiva las actuaciones de seguridad, orientando recursos y medidas hacia los escenarios con mayor relevancia para la organización y la seguridad de la persona paciente.

11.1. Fórmula básica del riesgo

De forma general, el riesgo se expresa como la combinación entre la probabilidad de materialización de un escenario y el impacto que dicho escenario produciría:

Riesgo = Probabilidad × Impacto

Esta fórmula responde a una lógica intuitiva, un evento muy probable pero con consecuencias limitadas genera un riesgo bajo, del mismo modo que un evento de consecuencias extremas pero altamente improbable puede no justificar, por sí solo, medidas desproporcionadas. Es la combinación de ambos factores lo que determina la magnitud del riesgo y, en consecuencia, la atención que debe recibir.

11.1. Fórmula del riesgo propuesta

No obstante, en entornos IoMT resulta conveniente descomponer el análisis para reflejar adecuadamente los elementos que intervienen en la materialización del riesgo. En particular, el daño no depende únicamente de la ocurrencia de una amenaza, sino también de la capacidad real de esa amenaza para explotar una vulnerabilidad y del valor/criticidad del activo afectado en el contexto clínico.

Por este motivo, en esta guía se propone una formulación ampliada:

Riesgo = Probabilidad amenaza × Impacto potencial vulnerabilidad × Criticidad activo

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

En esta expresión:

- Probabilidad de la amenaza representa la frecuencia estimada con la que la amenaza puede presentarse en el contexto de la organización, según la escala definida en el documento, considerando factores como exposición, tendencias del sector y capacidades del adversario.
- Impacto potencial de la vulnerabilidad refleja las consecuencias que tendría la explotación de la vulnerabilidad sobre las dimensiones CIDAT, valoradas según la tabla de impacto establecida.
- Criticidad del activo incorpora la importancia del activo para la organización y para la seguridad de la persona paciente, de acuerdo con la valoración previa realizada. Este factor permite diferenciar, por ejemplo, entre una misma vulnerabilidad aplicada a un dispositivo auxiliar frente a un equipo crítico de soporte vital.

Esta fórmula permite integrar de forma explícita los tres componentes que explican el riesgo en IoMT, la probabilidad de la amenaza, la severidad del daño que posibilita la vulnerabilidad, y la relevancia clínica/operativa del activo afectado. El resultado final facilita la priorización de medidas, centrando los esfuerzos en aquellos escenarios donde la combinación de factores produce un riesgo más elevado.

11.2. Interpretación del resultado

La aplicación de la fórmula definida en esta guía permite obtener un valor cuantitativo de riesgo inherente para cada escenario evaluado (activo–amenaza–vulnerabilidad). Dado que los componentes se expresan en escalas numéricas, el resultado es un valor comprendido entre 0 y 100, lo que facilita la comparación objetiva entre escenarios y permite ordenarlos de mayor a menor para priorizar actuaciones.

En concreto, el rango máximo se obtiene cuando todos los factores toman su valor más alto:

- Probabilidad: 5 (Muy alta)
- Impacto potencial de la vulnerabilidad: 5 (Crítico)
- Criticidad del activo: 4 (Alta)

Por tanto, aunque el valor cuantitativo es útil para comparar y ordenar riesgos, para facilitar la toma de decisiones y la comunicación con perfiles no técnicos resulta conveniente traducirlo a una categoría cualitativa. Para ello, el valor obtenido se convierte en un nivel de riesgo Bajo, Medio, Alto o Crítico aplicando la tabla de rangos definida a continuación.

Riesgo	Valores
Bajo	0 – 14
Medio	15 – 29
Alto	30 – 49
Crítico	50 – 100

TABLA 5: RIESGO CUALITATIVO.

Esta conversión permite:

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

- Establecer prioridades de tratamiento del riesgo.
- Determinar umbrales de aceptación o tolerancia.
- Unificar el criterio de evaluación entre distintos equipos y evaluadores.

En consecuencia, el proceso de evaluación produce dos salidas complementarias:

- Un valor numérico (0–100), que permite comparar y ordenar riesgos
- Una clasificación cualitativa, que simplifica la interpretación y la decisión.

11.3. Aclaración metodológica sobre la interpretación del resultado

Conviene aclarar un aspecto clave para interpretar correctamente los resultados del análisis. Aunque el cálculo del riesgo se exprese mediante una fórmula, en ciberseguridad, y especialmente en entornos IoMT, no se opera con magnitudes físicas directamente medibles, sino con estimaciones fundamentadas y juicios expertos representados mediante escalas ordinales.

En este contexto, cuando se asigna, por ejemplo, una probabilidad 4 en una escala de 1 a 5, no se está afirmando que la probabilidad sea exactamente del 80%, sino que, conforme a los criterios definidos, el evento se considera altamente probable. En consecuencia, el valor numérico obtenido permite comparar y priorizar escenarios, pero no debe interpretarse como una magnitud absoluta.

Desde esta perspectiva, lo verdaderamente valioso del cálculo no es el número en sí, sino el proceso estructurado que conduce a él y la capacidad de ordenar riesgos de forma consistente. Escenarios con puntuaciones similares suelen requerir niveles de atención comparables, mientras que aquellos con valores claramente superiores deben priorizarse en el tratamiento. Por el contrario, sería incorrecto concluir que un riesgo con puntuación 20 es “exactamente el doble” de grave que otro con puntuación 10.

Por último, conviene tener presente que la valoración del riesgo puede verse afectada por sesgos de percepción, debido a que las personas tienden a sobrevalorar eventos llamativos pero infrecuentes, como ataques dirigidos, y a infravalorar incidentes más cotidianos, como errores de configuración o fallos operativos durante tareas rutinarias. La aplicación de una metodología sistemática, la participación de perfiles complementarios, como clínicos, ingeniería clínica, TI y ciberseguridad, y la revisión crítica de las estimaciones ayudan a mitigar estos sesgos y a mejorar la consistencia del análisis.

12. Plan de acción y tratamiento del riesgo

La identificación, valoración y cálculo del riesgo solo aportan valor si se traducen en decisiones y actuaciones concretas. Por ello, una vez obtenida la clasificación de riesgos, tanto cuantitativa como cualitativa, la organización debe definir un plan de acción que establezca cómo se gestionará cada riesgo identificado, asignando prioridades, personas responsables, plazos y recursos para su implementación.

Este plan permite transformar el resultado del análisis en un conjunto ordenado de medidas orientadas a reducir el riesgo hasta niveles aceptables, garantizando la continuidad asistencial, la seguridad de la persona paciente y el cumplimiento normativo

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

12.1. Estrategias de tratamiento del riesgo

Ante cada riesgo identificado, la organización dispone de cuatro estrategias fundamentales de tratamiento. La elección de una u otra dependerá del nivel de riesgo, la criticidad del activo, los recursos disponibles y la tolerancia al riesgo definido por la Dirección.

❖ Mitigación

Consiste en implantar controles que reduzcan la probabilidad de materialización del escenario, el impacto en caso de ocurrencia, o ambos. Es la estrategia más frecuente en entornos IoMT y puede materializarse mediante medidas técnicas, organizativas y de capacitación.

Ejemplos: segmentación de red para aislar equipos críticos, hardening y gestión de actualizaciones, monitorización e IDS/IPS, control de accesos y MFA, o formación del personal frente a phishing.

❖ Transferencia

Implica trasladar total o parcialmente las consecuencias del riesgo a un tercero, normalmente mediante seguros de ciberriesgo o mediante acuerdos contractuales que asignen obligaciones específicas de seguridad a proveedores, como el mantenimiento remoto, servicios cloud o integradores.

Debe tenerse en cuenta que la transferencia no elimina la responsabilidad total de la organización, especialmente en materia de protección de datos y seguridad de la persona paciente.

❖ Evitación

Supone eliminar el riesgo renunciando a la actividad que lo origina. Se aplica cuando el riesgo supera claramente los beneficios o no existen medidas razonables para reducirlo.

Ejemplos: no conectar a la red determinados dispositivos cuando la exposición resulta inasumible, o retirar de servicio equipos heredados que no pueden protegerse adecuadamente.

❖ Aceptación

Consiste en asumir conscientemente el riesgo sin aplicar medidas adicionales, normalmente cuando su nivel es bajo o cuando el coste de mitigación es desproporcionado respecto al beneficio. También puede aplicarse al riesgo residual tras haber implantado controles.

La aceptación debe ser siempre una decisión informada, documentada y aprobada, y no el resultado de desconocimiento o falta de acción.

En la práctica, el tratamiento de un riesgo suele combinar varias estrategias. Por ejemplo, puede mitigarse mediante controles técnicos, transferirse parcialmente el impacto mediante un seguro y aceptar el riesgo residual resultante. La combinación seleccionada debe reflejar un equilibrio razonable entre el nivel de protección requerido, los recursos disponibles y las obligaciones legales y asistenciales aplicables.

12.2. Elaboración del plan de acción

Una vez seleccionada la estrategia de tratamiento adecuada para cada riesgo, es necesario documentar un plan de acción detallado que permita gestionar, supervisar y verificar la implantación de las medidas

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

previstas. El plan debe ofrecer la información suficiente para garantizar su ejecución efectiva y su seguimiento en el tiempo.

Para cada riesgo que vaya a ser tratado mediante mitigación o transferencia, el plan de acción debe incluir, como mínimo, los siguientes elementos:

1. **Descripción precisa de la medida**:

   La medida debe formularse de manera concreta, evitando ambigüedades sobre las actuaciones esperadas. Por ejemplo, una expresión genérica como “mejorar la seguridad de la red” resulta insuficiente, mientras que “implementar segmentación de red mediante VLAN para aislar los dispositivos de monitorización de personas pacientes del resto de la infraestructura hospitalaria” proporciona una orientación clara y verificable.

2. **Asignación de responsabilidades**:

   Debe identificarse la persona, rol o unidad organizativa responsable de ejecutar la medida. La responsabilidad debe recaer en quien disponga de la autoridad y los recursos necesarios. En organizaciones sanitarias, las medidas sobre dispositivos médicos suelen requerir coordinación entre ingeniería clínica, medicina y TI, por lo que puede ser necesario especificar responsabilidades diferenciadas. Por ejemplo, quién configura el dispositivo y quién aplica los cambios de red.

3. **Plazos de ejecución:**

   Los plazos establecen el marco temporal para la implantación. Los riesgos de mayor criticidad deben abordarse con urgencia, mientras que los de nivel moderado pueden planificarse en horizontes más amplios. Los plazos deben ser realistas, considerando la complejidad, la disponibilidad de recursos y las dependencias con otras actividades.

4. **Recursos necesarios:**

   Deben identificarse de forma explícita los recursos económicos, humanos y técnicos requeridos. Esto facilita la planificación presupuestaria, reduce bloqueos operativos y permite detectar conflictos de capacidad entre acciones concurrentes.

5. **Indicadores de seguimiento y rendimiento:**

   Se deben definir indicadores que permitan medir el progreso y la efectividad de la medida. Por ejemplo, para una segmentación de red, un indicador de avance podría ser el porcentaje de dispositivos migrados al nuevo segmento, y un indicador de eficacia podría ser la reducción del tráfico no autorizado hacia dichos dispositivos tras la implementación.

Para facilitar la gestión y trazabilidad, la siguiente tabla puede utilizarse como plantilla estándar para registrar cada acción del plan, de modo que todas las medidas queden documentadas de forma homogénea.

AC01	

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

Prioridad		**Persona responsable**	
Estado actual			
Recomendación			

TABLA 6: PLAN DE ACCIÓN.

12.3. El concepto de riesgo residual

En la gestión de riesgos es esencial comprender que ninguna medida de tratamiento elimina por completo el riesgo. Incluso después de aplicar los controles seleccionados, siempre persiste un nivel de exposición denominado riesgo residual, que representa el riesgo que la organización sigue asumiendo una vez implantadas las medidas de mitigación.

El riesgo residual puede entenderse como la diferencia entre el riesgo inicial o inherente y la reducción conseguida mediante los controles implementados. Así, si un escenario de riesgo presentaba inicialmente un nivel elevado y las medidas adoptadas reducen de forma significativa su probabilidad o su impacto, el riesgo residual puede situarse dentro de los límites que la organización considera aceptables. Por el contrario, si la reducción lograda es insuficiente, podría mantenerse en niveles excesivos y requerir nuevas acciones o una reconsideración de la estrategia de tratamiento.

La aceptación del riesgo residual debe ser siempre una decisión consciente y formal, adoptada por el nivel de responsabilidad que tenga la autoridad para asumir riesgos en nombre de la organización. Los marcos de referencia en gestión de riesgos establecen la necesidad de definir claramente quién puede aceptar riesgos y bajo qué condiciones. En el ámbito sanitario, esta decisión exige especial precaución, ya que un riesgo residual elevado puede afectar directamente a la seguridad de la persona paciente, lo que obliga a considerar criterios éticos y asistenciales además de los puramente técnicos.

Asimismo, es fundamental documentar los riesgos residuales aceptados y el razonamiento que justifica dicha aceptación. Esta documentación cumple una doble función:

- Proporciona evidencia del deber de diligencia en la gestión del riesgo.
- Facilita su revisión periódica, especialmente cuando cambian las circunstancias, se introducen nuevos controles o se dispone de información adicional que pueda afectar a la valoración.

En definitiva, gestionar el riesgo residual no consiste únicamente en calcular el riesgo restante tras las medidas aplicadas, sino en garantizar que ese nivel de riesgo es conocido, aceptado, justificado y revisado regularmente para mantener la seguridad de la persona paciente y la continuidad asistencial.

12.4. Seguimiento y revisión continua

El plan de acción no debe entenderse como un documento estático, sino como un instrumento dinámico que requiere un seguimiento y una actualización periódica. La gestión del riesgo en entornos IoMT es un

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

proceso continuo, ya que tanto las amenazas como las vulnerabilidades y los activos evolucionan con el tiempo.

El ciclo de revisión debe permitir:

- Verificar el avance en la implantación de las medidas planificadas.
- Evaluar la eficacia real de los controles desplegados.
- Identificar nuevos riesgos surgidos desde el análisis anterior.
- Revisar las valoraciones cuando cambie el contexto tecnológico, clínico o normativo.

La frecuencia de estas revisiones debe adaptarse a la criticidad de los activos y al entorno. Para dispositivos que cumplen funciones vitales o procesan datos altamente sensibles, pueden justificarse revisiones trimestrales o incluso más frecuentes. Para activos de menor criticidad, una revisión anual puede ser suficiente, siempre manteniendo la capacidad de realizar revisiones extraordinarias cuando las circunstancias lo requieran.

Se recomienda realizar una revisión extraordinaria del análisis de riesgos ante eventos como:

- Incorporación de nuevos dispositivos a la red, especialmente si introducen nuevas superficies de ataque o integraciones externas.
- Descubrimiento de vulnerabilidades significativas que afecten a dispositivos en operación.
- Incidentes de seguridad propios o en otras organizaciones sanitarias que revelen riesgos no contemplados.
- Cambios normativos que alteren obligaciones de protección.
- Modificaciones sustanciales en la arquitectura de red o en los procesos de gestión de dispositivos.

Estas revisiones garantizan que el análisis de riesgos y las medidas derivadas de él se mantengan alineados con la realidad tecnológica y asistencial de la organización.

12.5. Integración con el modelo de gobierno

El plan de acción derivado del análisis de riesgos debe integrarse de forma coherente con los procesos de gobierno y gestión de la organización sanitaria. Para que el tratamiento del riesgo sea efectivo, debe alinearse con la planificación estratégica, asistencial y presupuestaria de la entidad.

En particular:

- Las medidas que requieran inversiones significativas deben incorporarse en las partidas presupuestarias y proyectos de transformación digital.
- Las actuaciones que afecten a procedimientos asistenciales deben coordinarse con el personal sanitario responsable, garantizando que las medidas de seguridad no interfieran con la atención a la persona paciente ni comprometan la continuidad asistencial.

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

- Las obligaciones derivadas del plan deben reflejarse en los acuerdos de nivel de servicio, contratos de mantenimiento y relaciones con proveedores, asegurando que terceros cumplen las medidas de seguridad necesarias.

Asimismo, la Dirección de la organización debe recibir información periódica sobre:

- El estado de los riesgos identificados.
- El avance en la ejecución del plan de acción.
- Las desviaciones respecto a los plazos previstos.
- Las decisiones que requieren intervención estratégica o asignación de recursos.

La comunicación con la Dirección debe realizarse en un formato adaptado a sus necesidades y a su capacidad de decisión, resaltando los riesgos más significativos, los incidentes recientes y las medidas críticas pendientes.

13. Conclusiones

El análisis de riesgos en entornos IoMT no es un ejercicio únicamente académico ni una obligación legal que pueda realizarse de forma superficial. Es, por el contrario, una herramienta esencial para proteger simultáneamente a las personas pacientes, cuya seguridad depende del funcionamiento correcto de equipos cada vez más complejos e interconectados, y a las organizaciones sanitarias, que afrontan un panorama de amenazas en constante evolución y un marco normativo cada vez más exigente.

La guía presentada ofrece una metodología estructurada, adaptada a las particularidades del sistema sanitario español y alineada con los principales marcos de referencia nacionales e internacionales, que permite abordar esta tarea de forma sistemática y rigurosa.

No obstante, la eficacia de cualquier proceso de análisis de riesgos depende, antes que nada, del compromiso de la Dirección. Sin respaldo institucional, sin recursos adecuados y sin integrar la gestión del riesgo en la cultura organizativa, incluso una metodología perfecta se convierte en un documento irrelevante. Las organizaciones que obtienen resultados reales son aquellas que comprenden que la ciberseguridad de los dispositivos médicos no es responsabilidad exclusiva de TI, es un objetivo compartido que involucra a profesionales sanitarios, gestores, ingeniería clínica y, en última instancia, a cualquier persona que interactúe con la tecnología sanitaria.

Los retos descritos en esta guía, desde la escasez de perfiles especializados hasta la fragmentación del sistema sanitario o la coexistencia de parques tecnológicos heterogéneos, no deben interpretarse como desafíos imposibles, sino como condicionantes que deben tenerse en cuenta para diseñar estrategias realistas y sostenibles. Ninguna organización dispone de recursos ilimitados, gestionar el riesgo consiste precisamente en decidir dónde concentrar los esfuerzos para lograr la mayor reducción posible. La priorización basada en un análisis sistemático permite enfocar las inversiones en los escenarios donde la probabilidad y el impacto es mayor, evitando el exceso de precaución o el desconocimiento.

El carácter dinámico del ecosistema IoMT exige concebir el análisis de riesgos como un proceso continuo, no como un proyecto con principio y final. La incorporación de nuevos dispositivos, la aparición de vulnerabilidades previamente desconocidas, la evolución de los ataques y los cambios

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

regulatorios obligan a revisiones periódicas que mantengan actualizada la visión del riesgo. La gestión del cambio, la monitorización continua y la capacidad de responder a incidentes constituyen elementos esenciales de un ciclo de mejora continua que incrementa con el tiempo la madurez de la organización en materia de ciberseguridad.

Asimismo, la colaboración entre organizaciones sanitarias representa una oportunidad estratégica. Los retos son comunes, las amenazas afectan por igual a todo el sector y las soluciones desarrolladas por una entidad pueden resultar valiosas para muchas otras. Los eventos de intercambio de experiencias, la compartición de indicadores de compromiso y amenazas, y la creación de recursos comunes, como catálogos de vulnerabilidades IoMT específicas, multiplican la eficacia de los esfuerzos individuales. En un contexto de recursos limitados, la colaboración es una ventaja decisiva frente a adversarios que colaboran entre sí constantemente.

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. 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

2. 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

3. CCN-CERT. (2024). *CCN-STIC 891: Perfil de cumplimiento específico para el sector salud*. https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/7206-ccn-stic-891-perfil-de-cumplimiento-especifico-para-salud-prestacion-sanitaria-a-pacientes-atencion-primaria-y-atencion-especializada/file.html

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

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

6. European Commission. (2019). *Guidance on cybersecurity for medical devices*. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

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). *Cyber Hygiene in the Health Sector*. https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector

11. European Union Agency for Cybersecurity (ENISA). (2020). *BP. 05: Procurement guidelines for cybersecurity in hospitals (es)*.

https://www.enisa.europa.eu/publications/procurement-guidelines-for-cybersecurity-in-hospitals

12. 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

e

13. 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

14. International Organization for Standardization. (2025). *ISO/IEC 27701:2025: Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. https://www.iso.org/standard/27701

15. International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process*. https://www.iso.org/standard/78973.html

16. 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

17. International Organization for Standardization. (2022). *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks* https://www.iso.org/standard/80585.html

18. International Organization for Standardization. (2021). *IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices*. https://www.iso.org/standard/72026.html

19. International Organization for Standardization. (2020). *ISO/TR 24971:2020: Medical devices — Guidance on the application of ISO 14971. International Organization for Standardization*. https://www.iso.org/standard/74437.html

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

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

21. International Organization for Standardization. (2019). *ISO/IEC 27018:2019: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. https://www.iso.org/standard/76559.html

22. International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements*. https://www.iso.org/standard/75106.html

23. International Organization for Standardization. (2019). *ISO 31000:2018: Risk management — Guidelines*. https://www.iso.org/standard/65694.html

24. International Organization for Standardization. (2016). *ISO/IEC 27799:2016: Health informatics — Information security management in health using ISO/IEC 27002*. https://www.iso.org/standard/62777.html

25. International Organization for Standardization. (2015). *ISO/IEC 27017:2015: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. https://www.iso.org/standard/43757.html

26. International Society of Automation (ISA). (2020). *ISA/IEC 62443 series of standards: Application of risk management for IT-networks incorporating medical devices*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

27. National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments* https://csrc.nist.gov/pubs/sp/800/30/r1/final

28. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations* https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

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.

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

15.1. Lista de materias tratadas en la guía

- Contexto del IoMT y fundamentos del análisis de riesgos
- Identificación y valoración de activos
- Clasificación de activos por criticidad clínica
- Dimensiones CIDAT y valoración del impacto
- Identificación y análisis de amenazas
- Identificación y clasificación de vulnerabilidades
- Estimación de probabilidad e impacto
- Cálculo del riesgo y conversión a niveles cualitativos
- Riesgo residual y tratamiento del riesgo
- Plan de acción: diseño, responsabilidades e indicadores
- Seguimiento, revisión continua y gobernanza

15.2. Lista de productos mencionados en la guía

No se mencionan productos 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

RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Análisis de Riesgos en IoMT

Febrero de 2026

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