RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Uso responsable y seguro de dispositivos IoMT en entornos sanitarios

Enero 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: 27/01/2026

Fecha de última actualización: 27/01/2026

ÍNDICE DE CONTENIDOS

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

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. Introducción

El avance del Internet de los Dispositivos Médicos (IoMT) ha supuesto una de las transformaciones tecnológicas más relevantes en el ámbito sanitario en los últimos años. La integración de dispositivos médicos conectados, sensores biométricos y plataformas digitales en hospitales, centros sanitarios y entornos domiciliarios ha permitido mejorar la calidad asistencial, optimizar la gestión de recursos, reducir costes operativos y ofrecer una atención más personalizada y basada en datos. Desde sistemas de monitoreo remoto y soluciones de telemedicina hasta equipos hospitalarios inteligentes y dispositivos portátiles de diagnóstico, el IoMT se consolida como un pilar de la transformación digital en salud.

En este escenario, los dispositivos IoMT han evolucionado de simples herramientas de apoyo a componentes esenciales de los procesos clínicos, influyendo directamente en el diagnóstico, la toma de decisiones médicas y la administración de tratamientos. Esta dependencia creciente refuerza su papel estratégico en la atención sanitaria y resalta la necesidad de garantizar su fiabilidad, seguridad y correcto funcionamiento durante todo su ciclo de vida.

Al mismo tiempo, la interconexión de estos sistemas amplía la superficie de exposición a ciberamenazas. Cada dispositivo, sensor o aplicación conectada constituye un posible punto de acceso que podría comprometer la información clínica, alterar el funcionamiento de equipos críticos o poner en riesgo la seguridad del paciente. Los entornos sanitarios, cada vez más digitalizados y dependientes de sistemas interconectados, deben abordar riesgos que van más allá de lo tecnológico, afectando directamente a la privacidad, la seguridad operativa y la continuidad de los servicios asistenciales.

Por ello, la ciberseguridad en el IoMT se vuelve un elemento imprescindible para garantizar la confianza en los sistemas de salud digital, la disponibilidad de los servicios médicos y la protección de los datos e integridad de los pacientes. Su gestión requiere un enfoque integral que combine innovación tecnológica segura, cumplimiento normativo, formación continua del personal sanitario y colaboración entre entidades públicas, privadas y organismos reguladores. Esta guía tiene como objetivo ofrecer herramientas prácticas para orientar a los profesionales involucrados en la gestión de dispositivos IoMT, promoviendo buenas prácticas, minimizando riesgos y fortaleciendo la seguridad clínica en entornos cada vez más digitalizados.

2. Objetivo y alcance

2.1. Objetivo

El objetivo de esta guía es proporcionar un conjunto de buenas prácticas y recomendaciones para el uso seguro y responsable de dispositivos IoMT por parte del personal sanitario, personal de ingeniería clínica y personal de TI, quienes interactúan directamente con estos dispositivos en entornos hospitalarios y centros médicos.

La guía pretende:

- Promover un uso adecuado de los dispositivos IoMT que garantice la seguridad del paciente, la continuidad asistencial y el correcto funcionamiento de los equipos médicos conectados.

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

- Minimizar los riesgos asociados al uso de dispositivos IoMT, incluyendo vulnerabilidades de ciberseguridad, errores de configuración, fallos operativos y prácticas inseguras de manejo.
- Facilitar la comprensión de aspectos esenciales de seguridad digital y protección de datos relacionados con los dispositivos IoMT, de manera comprensible para usuarios con distintos niveles de conocimiento técnico.

En definitiva, la guía busca fortalecer la cultura de ciberseguridad en entornos clínicos, garantizando confianza, eficiencia y seguridad en la operación de dispositivos IoMT por todo el personal involucrado en la atención al paciente.

2.2. Alcance

Esta guía aplica a los siguientes tipos de dispositivos IoMT utilizados en entornos clínicos y hospitalarios:

- 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.
- Equipos médicos conectados que emplean radiaciones ionizantes o tecnologías terapéuticas avanzadas, tales como sistemas de radiodiagnóstico, equipos de radioterapia, planificación y administración de tratamientos radioterápicos, así como equipamiento quirúrgico y sistemas asistidos por tecnología digital, en la medida en que incorporen conectividad, intercambio de datos o integración con sistemas clínicos y plataformas digitales.
- Sistemas y dispositivos de laboratorio clínico y diagnóstico in vitro conectados, tales como analizadores automatizados, sistemas de microbiología, bioquímica, hematología y anatomía patológica digital, en la medida en que participen en procesos de diagnóstico, apoyo a la decisión clínica o seguimiento de tratamientos.
- 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:

- Personal sanitario, que utiliza dispositivos IoMT para el seguimiento, diagnóstico o tratamiento de pacientes.
- Personal de ingeniería clínica, encargado de la gestión, 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.

Esta guía no reemplaza las instrucciones específicas de los fabricantes ni las recomendaciones clínicas profesionales, ni aborda procedimientos técnicos avanzados exclusivos para especialistas en desarrollo

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

o mantenimiento de dispositivos. Su enfoque está en el uso seguro y responsable para los usuarios finales dentro del ámbito clínico.

Asimismo, no está dirigida a especialistas en ciberseguridad, ya que está pensada para personal sin conocimientos técnicos profundos en este ámbito.

2.3. Metodología

La elaboración de esta guía se ha basado en un enfoque estructurado, que combina el análisis de las normativas aplicables, el estudio de casos reales y la organización de las recomendaciones por áreas de seguridad, con el objetivo de generar un documento completo, comprensible por cualquier usuario y aplicable para el personal sanitario, de electromedicina y de TI.

Los principales elementos de la metodología son:

- Revisión normativa y documental: Se han analizado los 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.
- Estudio de casos y experiencias documentadas: Se han evaluado incidentes reales y experiencias reportadas en entornos clínicos, hospitales y centros médicos, así como situaciones relacionadas con el uso de dispositivos IoMT en telemedicina y monitoreo remoto. Esto ha permitido identificar riesgos comunes y proponer estrategias efectivas para mitigarlos.
- Organización por dominios de seguridad: Las recomendaciones se estructuraron en áreas clave que facilitan la comprensión y aplicación por parte del personal:
    - Gestión del dispositivo: instalación, configuración, calibración y operación segura.
    - Gestión de accesos: autenticación, permisos y control de usuarios.
    - Seguridad de la red: conexión segura, segmentación y protección ante intrusiones.
    - Protección de datos: confidencialidad, integridad y almacenamiento seguro de información clínica.
    - Mantenimiento y ciclo de vida: actualizaciones, parches, verificación y retiro seguro de dispositivos.
    - Detección básica de problemas e incidentes: identificación temprana de fallos, alertas y reporte a los responsables
- Adaptación del contenido a un lenguaje accesible: Se ha priorizado la claridad y comprensión para todos los perfiles de usuarios finales, asegurando que las recomendaciones puedan aplicarse de manera práctica sin necesidad de conocimientos técnicos avanzados.
- Enfoque práctico y escalable: La guía considera distintos niveles de interacción con la tecnología, diversidad de dispositivos IoMT y distintos entornos de uso, permitiendo que las recomendaciones sean implementables de forma flexible según las necesidades de los centros sanitarios.

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

Este enfoque asegura que la guía sea una herramienta práctica, segura y confiable para todo el personal que utiliza, mantiene o supervisa dispositivos IoMT, contribuyendo a la protección de los pacientes, la integridad de los datos y el correcto funcionamiento de los sistemas médicos conectados.

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**:
  - 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 60601-1, Requisitos generales para la seguridad básica y el rendimiento esencial de equipos electromédicos.
  - IEC 80001-1, Gestión de riesgos para redes TI que incorporan dispositivos médicos.
  - IEC 82304-1:2016, Requisitos para la seguridad y calidad de software de salud independiente
  - ISO 13485:2016, Sistemas de gestión de calidad para dispositivos médicos
  - ISO 14971:2019, Aplicación de una metodología de riesgos para dispositivos médicos.
  - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
  - ISO/IEC 27001, Gestión de la seguridad de la información.

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

- ISO 27799, Seguridad de la información en salud.
- ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
- ISO 22301, Gestión de la continuidad de negocio.
- ISO 81001, Normas relacionadas con la ingeniería de software para dispositivos médicos.

- **Guías**:
  - BSI TR-03161, Requerimientos de seguridad para aplicaciones de eHealth.
  - Cloud Security Alliance (CSA), Matriz de controles Cloud (CCM).
  - ENISA - Ciberseguridad y resiliencia para hospitales inteligentes.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
  - NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.
  - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
  - IMDRF-Principios y prácticas de ciberseguridad para la contratación de software y materiales de dispositivos médicos.
  - OWASP IoT y OWASP, Guías de auditorías técnicas.

4. Definiciones

Acrónimos	Definición
DDoS	Intento malicioso de interrumpir el funcionamiento normal de un servidor sobrecargándolo con tráfico desde múltiples fuentes (del inglés, Distributed Denial of Service).
Device Spoofing	Técnica maliciosa en la que un atacante falsifica la identidad de un dispositivo para acceder a sistemas protegidos.
Firmware	Tipología de software integrado en dispositivos electrónicos que controla el hardware y permite su funcionamiento básico.
HL7	Conjunto de estándares para el intercambio electrónico de información clínica entre sistemas de salud (del inglés, Health Level Seven).
HTTPS	Versión segura del protocolo HTTP (del inglés, Hypertext Transfer Protocol Secure) por el puerto 443.
JSON	Formato ligero de intercambio de datos legible por humanos y máquinas (del inglés, JavaScript Object Notation).
Logs	Registros que documentan eventos dentro de sistemas y aplicaciones.
MFA	Método de autenticación que combina múltiples factores (del inglés, Multi-Factor Authentication).
Mínimo privilegio	Principio que limita los accesos al mínimo necesario para realizar tareas.
Puertos	Puntos lógicos de conexión para enviar o recibir datos en una red.

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
Ransomware	Programa malicioso que bloquea el acceso a sistemas o archivos y exige un pago para restaurarlo.
Registros de auditoría	Logs utilizados para seguimiento de actividades, accesos y cambios en sistemas.
SIEM	Plataforma que centraliza y analiza eventos de seguridad (del inglés, Security Information and Event Management).
Superficie de ataque	Conjunto de puntos o vectores por donde un atacante o actor de amenazas puede intentar acceder a un sistema o entorno.
Syslog	Protocolo estándar para el envío de mensajes de registro de sistemas.
TLS	Protocolo criptográfico que proporciona seguridad en las comunicaciones (del inglés, Transport Layer Security).
VPN	Tecnología que crea una conexión segura sobre una red pública (del inglés, Virtual Private Network).
Vulnerabilidad	Debilidad en un sistema que puede ser explotada por atacantes o actores de amenazas.
XML	Lenguaje de marcado usado para almacenar y transportar datos (del inglés, eXtensible Markup Language).

TABLA 1: DEFINICIONES EMPLEADAS.

5. Contexto general del IoMT

El Internet de los Dispositivos Médicos (IoMT) hace referencia al conjunto de dispositivos médicos que incorporan capacidades de recopilación, transmisión, procesamiento y análisis de datos sanitarios a través de redes de comunicación. Estos dispositivos pueden comunicarse entre sí y con sistemas clínicos, plataformas hospitalarias o servicios en la nube, formando parte de un ecosistema tecnológico interconectado.

El IoMT representa una evolución natural de la tecnología médica tradicional, al integrar dispositivos físicos con software, redes y servicios digitales. Gracias a esta conectividad, es posible mejorar el diagnóstico, el tratamiento y el seguimiento de los pacientes, así como optimizar los procesos asistenciales y la gestión de los recursos sanitarios.

La incorporación del IoMT en hospitales, clínicas y otros entornos asistenciales ha transformado la forma en que se presta la atención médica, debido a que potencia las capacidades de monitorización continua, facilita el acceso a información clínica en tiempo real y permite una mayor integración entre dispositivos médicos y sistemas de información sanitaria. No obstante, esta interconexión también introduce nuevos retos técnicos, organizativos y de seguridad que deben ser gestionados de forma adecuada.

5.1. Evolución y adopción del IoMT en el entorno sanitario

La adopción del IoMT ha sido impulsada por la evolución simultánea de la tecnología médica, las redes de comunicaciones y la digitalización del sector sanitario. Dispositivos que anteriormente funcionaban

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

de manera independiente y aislada ahora se integran en redes internas, sistemas de información hospitalarios y plataformas digitales, permitiendo una gestión más eficiente de la información clínica.

Este proceso de evolución ha estado acompañado por la necesidad de mejorar la calidad asistencial, reducir tiempos de respuesta y optimizar el uso de los recursos sanitarios. La conectividad de los dispositivos ha facilitado el acceso remoto a datos clínicos, la automatización de procesos y la interoperabilidad entre distintos sistemas y tecnologías.

Sin embargo, la adopción del IoMT también ha incrementado la complejidad del entorno tecnológico sanitario. La coexistencia de múltiples dispositivos, fabricantes y protocolos, junto con la dependencia de infraestructuras de red y servicios digitales, plantea nuevos desafíos en términos de gestión, interoperabilidad, mantenimiento y seguridad. Estos desafíos hacen necesario contar con una visión clara del contexto IoMT y con directrices que orienten su uso responsable.

5.2. Tipos de dispositivos IoMT

El ecosistema IoMT está compuesto por una amplia variedad de dispositivos médicos conectados, utilizados en distintos escenarios asistenciales y con diferentes niveles de criticidad. Entre los principales tipos de dispositivos IoMT se incluyen:

- Dispositivos de monitoreo de constantes vitales y signos clínicos, como monitores de frecuencia cardíaca, presión arterial, saturación de oxígeno o temperatura, que permiten una vigilancia continua del estado del paciente.
- Equipos terapéuticos conectados, como bombas de infusión, ventiladores mecánicos o dispositivos de soporte respiratorio, que administran tratamientos y requieren un funcionamiento preciso y continuo.
- Dispositivos implantables con conectividad, como marcapasos o bombas de insulina inteligentes, que transmiten información clínica y permiten ajustes o supervisión remota.
- Sistemas de diagnóstico integrados con plataformas digitales, como equipos de imagen médica o dispositivos de laboratorio conectados a sistemas de información clínica.
- Dispositivos utilizados en telemedicina y monitoreo remoto, que facilitan la atención a distancia y el seguimiento continuo de pacientes fuera del entorno hospitalario tradicional.

Estos dispositivos no operan de forma aislada, sino que interactúan con aplicaciones, sistemas clínicos, redes hospitalarias y servicios externos, conformando un entorno altamente interconectado que requiere una gestión coordinada y segura.

5.3. Beneficios del IoMT en la atención sanitaria

La implementación del IoMT aporta beneficios significativos al sistema sanitario, tanto desde el punto de vista clínico como operativo. Uno de los principales beneficios es la mejora en la calidad y continuidad de la atención al paciente, al permitir una monitorización más precisa y constante de su estado de salud.

El acceso a información clínica en tiempo real facilita la toma de decisiones médicas más informadas y oportunas, reduciendo retrasos y mejorando la respuesta ante situaciones críticas. Asimismo, el IoMT

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

contribuye a la optimización de recursos y procesos asistenciales, al automatizar tareas, reducir errores manuales y mejorar la coordinación entre distintos servicios.

Otro beneficio relevante es la posibilidad de ofrecer seguimiento remoto y atención personalizada, adaptando los tratamientos a las necesidades específicas de cada paciente y reduciendo la necesidad de desplazamientos innecesarios. La integración de datos provenientes de múltiples dispositivos y sistemas permite una visión más completa del estado clínico del paciente, fortaleciendo la capacidad de análisis y planificación.

En conjunto, estos beneficios convierten al IoMT en un elemento clave de la transformación digital del sector sanitario, siempre que su uso se realice de forma segura, responsable y alineada con las necesidades asistenciales.

6. Riesgos asociados

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

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

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

ILUSTRACIÓN 1: RIESGOS DE CIBERSEGURIDAD EN IOMT

6.1.1. Riesgos técnicos

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

Entre los más relevantes se incluyen:

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

6.1.2. Riesgos operativos

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

Entre los más frecuentes destacan:

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

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · 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

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

6.1.3. Riesgos estratégicos

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

Entre los más relevantes destacan:

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

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · 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

7. Principios de Uso Responsable

El uso seguro y responsable de los dispositivos IoMT es fundamental para proteger la salud de los pacientes, garantizar la confidencialidad de los datos y mantener la integridad de los sistemas hospitalarios. Estos principios establecen las bases para un comportamiento seguro y consciente, promoviendo la colaboración entre personal sanitario, de ingeniería clínica y de TI.

7.1. Responsabilidad compartida

La responsabilidad compartida implica que la seguridad y buen uso de los dispositivos IoMT no depende de una sola persona ni de un solo departamento, sino de la colaboración activa de todos los agentes que interactúan con la tecnología. Cada acción, desde el encendido de un dispositivo hasta la transmisión de datos, puede afectar la seguridad del sistema y la atención al paciente. La adopción de prácticas responsables debe ser consciente y constante, comprendiendo que los errores individuales pueden tener consecuencias en todo el ecosistema de salud.

7.2. Seguridad centrada en el paciente

Este principio establece que todas las decisiones y acciones relacionadas con dispositivos IoMT deben priorizar el bienestar y la seguridad del paciente. La implementación de medidas de seguridad no puede interferir con la atención médica ni poner en riesgo la salud del paciente. Además, asegura que los dispositivos críticos estén disponibles y funcionen de manera fiable en todo momento, equilibrando las necesidades técnicas con las clínicas.

7.3. Confidencialidad

La confidencialidad protege la información sensible generada y almacenada por los dispositivos IoMT, garantizando que solo usuarios autorizados puedan acceder a los datos. Esto incluye registros médicos, resultados de pruebas, parámetros vitales y cualquier información clínica transmitida por los dispositivos. Mantener la confidencialidad previene la exposición indebida de información, protege la privacidad del paciente y cumple con estándares legales y regulatorios.

7.4. Integridad

La integridad se refiere a la exactitud y consistencia de los datos, así como al correcto funcionamiento de los dispositivos. Garantiza que la información no sea alterada de forma accidental o maliciosa, manteniendo la fiabilidad de los registros clínicos. La integridad también implica que los dispositivos operen según los parámetros esperados y que cualquier cambio en la información o configuración sea controlado y rastreable.

7.5. Disponibilidad

Este principio asegura que los dispositivos IoMT y los datos que generan estén accesibles cuando se necesiten, permitiendo una atención médica continua y sin interrupciones. La disponibilidad es crítica para dispositivos que monitorean pacientes en tiempo real o que intervienen directamente en

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

tratamientos. Requiere mantener sistemas operativos estables, implementar planes de respaldo y garantizar que los dispositivos funcionen correctamente ante fallos, mantenimientos o actualizaciones.

7.6. Autenticidad

La autenticidad garantiza que tanto los usuarios como los datos y dispositivos sean legítimos y confiables. Este principio asegura que la información provenga de fuentes verificadas y que los accesos al sistema sean realizados por usuarios autorizados, evitando fraudes, accesos no autorizados o manipulación de información. Mantener la autenticidad es fundamental para confiar en los resultados clínicos y en las operaciones de los dispositivos.

7.7. Trazabilidad

La trazabilidad permite registrar y seguir todas las acciones realizadas sobre los dispositivos y sus datos. Este principio facilita la auditoría de procesos, la detección de incidentes de seguridad y la identificación de posibles errores. La trazabilidad asegura que se pueda reconstruir el historial de uso, cambios y accesos, proporcionando transparencia y soporte para la mejora continua de la seguridad en el entorno IoMT.

7.8. Cumplimiento normativo

El cumplimiento normativo asegura que el uso de los dispositivos IoMT se ajuste a leyes, regulaciones, estándares internacionales y políticas institucionales. Esto protege la información clínica, garantiza la seguridad de los pacientes y evita riesgos legales para la organización. Cumplir con la normativa incluye seguir procedimientos de manejo de datos, mantener registros de auditoría y actualizar protocolos conforme cambian las regulaciones.

7.9. Cultura en ciberseguridad

Promover una cultura de ciberseguridad implica fomentar hábitos, valores y comportamientos que prioricen la protección de los dispositivos y la información clínica. Este principio busca que todos los usuarios adopten buenas prácticas de forma continua, comprendan los riesgos, participen en capacitaciones y reporten incidentes de manera proactiva. Una cultura sólida en ciberseguridad fortalece la prevención, minimiza riesgos y mejora la resiliencia de los sistemas IoMT.

8. Tipos de usuarios finales en IoMT

El uso seguro y responsable de los dispositivos IoMT requiere la participación coordinada de distintos usuarios finales dentro del ecosistema sanitario. Cada uno de ellos interactúa con los dispositivos desde un rol específico, aportando capacidades complementarias para garantizar la seguridad del paciente, la protección de la información clínica y el correcto funcionamiento de los sistemas.

Esta guía identifica y describe los siguientes tipos de usuarios finales, a los cuales van dirigidas las recomendaciones y buenas prácticas aquí presentadas.

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

8.1. Personal de ingeniería clínica

El personal de ingeniería clínica es responsable de la gestión técnica integral de los dispositivos médicos, incluyendo aquellos que incorporan conectividad y funcionalidades IoMT. Su rol abarca no solo la gestión y mantenimiento de los dispositivos, sino también fases clave previas y posteriores a su operación clínica.

Entre sus responsabilidades se encuentran la participación técnica en los procesos de evaluación y adquisición de dispositivos, colaborando con el órgano de contratación mediante la elaboración de informes técnicos, la definición de requisitos y la valoración de aspectos relacionados con la seguridad, la interoperabilidad y la compatibilidad. En este contexto, mantiene contacto directo con fabricantes y proveedores, especialmente en lo relativo a seguridad, actualizaciones, soporte técnico y cumplimiento normativo. Esta función resulta fundamental para asegurar que los dispositivos incorporados al entorno clínico cumplan con los estándares de seguridad, interoperabilidad y compatibilidad con la infraestructura existente.

Además, el personal de ingeniería clínica interviene en la instalación, configuración inicial, calibración, mantenimiento preventivo y correctivo, así como en la retirada segura de los dispositivos al final de su ciclo de vida de acuerdo con las instrucciones del fabricante y los procedimientos establecidos por la entidad sanitaria. Su actuación es clave para prevenir configuraciones inseguras, fallos técnicos y riesgos derivados de vulnerabilidades no gestionadas.

En el contexto de IoMT, este perfil actúa como un punto de enlace entre la tecnología médica, los proveedores y los sistemas de información, contribuyendo directamente a la seguridad, disponibilidad y fiabilidad de los dispositivos conectados.

8.2. Personal de TI

El personal de TI es responsable de la infraestructura tecnológica y de comunicaciones que soporta el funcionamiento de los dispositivos IoMT. Esto incluye redes, sistemas, plataformas de gestión, servicios en la nube y mecanismos de protección de la información.

Su rol se centra en garantizar que los dispositivos IoMT se integren de forma segura dentro del ecosistema digital de la organización, protegiendo los datos clínicos frente a accesos no autorizados, pérdidas de información o interrupciones del servicio.

En el ámbito de esta guía, el personal de TI es considerado usuario final porque interactúa directamente con los dispositivos IoMT desde el punto de vista de su conectividad, gestión de accesos, monitoreo de seguridad y respuesta ante incidentes. Su actuación es fundamental para mantener la confidencialidad, integridad y disponibilidad de los sistemas médicos conectados.

8.3. Personal sanitario

El personal sanitario utiliza los dispositivos IoMT como herramientas clínicas esenciales para el diagnóstico, monitoreo y tratamiento de los pacientes. Su interacción con estos dispositivos es directa y tiene un impacto inmediato en la atención sanitaria y en la toma de decisiones clínicas.

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

Además de su uso clínico, el personal sanitario desempeña un papel clave en garantizar que los pacientes utilicen correctamente los dispositivos IoMT, especialmente en contextos de seguimiento remoto, hospitalización domiciliaria o uso continuado. Esto incluye la correcta indicación del uso, la explicación de su funcionamiento básico y la supervisión de su utilización conforme a las recomendaciones clínicas y de seguridad.

Aunque no es responsable de la gestión técnica del dispositivo, el personal sanitario contribuye activamente a la seguridad al detectar comportamientos anómalos, errores de uso o fallos que puedan afectar la calidad de la atención o la seguridad del paciente. Su participación es esencial para asegurar la fiabilidad de los datos clínicos y la correcta integración del dispositivo en los procesos asistenciales.

9. Recomendaciones de uso seguro personal ingeniería clínica

El personal de ingeniería clínica desempeña un papel fundamental en la gestión técnica y operativa de los dispositivos IoMT dentro de las entidades sanitarias. Su responsabilidad abarca desde la adquisición y puesta en servicio de los equipos, hasta su mantenimiento, configuración segura y coordinación con proveedores y personal clínico. Una correcta gestión garantiza la seguridad del paciente, la disponibilidad de los dispositivos y la integridad de los datos clínicos.

Las siguientes recomendaciones buscan orientar al personal de ingeniería clínica en la aplicación de buenas prácticas para asegurar que los dispositivos IoMT se utilicen de forma segura, cumpliendo con normativas, estándares y políticas internas de la entidad sanitaria.

9.1. Gestión de dispositivos

Una gestión adecuada de los dispositivos IoMT a lo largo de todo su ciclo de vida es un elemento fundamental para garantizar su uso seguro y responsable. Desde la adquisición hasta su retirada, los dispositivos deben estar correctamente controlados, documentados y clasificados, de forma que se minimicen los riesgos técnicos, clínicos y de ciberseguridad asociados.

Las siguientes recomendaciones establecen buenas prácticas para una gestión eficaz de los dispositivos IoMT en el entorno sanitario:

- **Adquisición mediante procedimientos oficiales**:
  Garantizar que los dispositivos IoMT se adquieran exclusivamente a través de los procedimientos oficiales de la entidad sanitaria. Estos procesos deben incluir cláusulas específicas de ciberseguridad en los contratos con los proveedores, trasladando responsabilidades claras durante toda la prestación de los servicios, así como en caso de incidentes.
- **Disponibilidad y actualización de la documentación técnica**:
  Asegurar que el proveedor suministra toda la documentación técnica necesaria para el correcto funcionamiento y mantenimiento de los dispositivos, incluyendo manuales, guías de uso, recomendaciones de seguridad y procedimientos de actualización.
- **Clasificación según criticidad y exposición al riesgo**:
  Garantizar que todos los dispositivos IoMT estén clasificados conforme a criterios objetivos, teniendo en cuenta su criticidad clínica, impacto potencial sobre el paciente y su nivel de

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

exposición a amenazas de ciberseguridad. Esta clasificación permite priorizar medidas de seguridad durante el ciclo de vida del dispositivo y evitar potenciales incidentes.

- **Inventario y trazabilidad de los dispositivos**:
  Coordinar el registro de cada dispositivo en el inventario corporativo de la entidad, incluyendo como mínimo el número de serie, modelo, fabricante, fecha de recepción, ubicación, estado operativo y responsable asignado. Un inventario actualizado es esencial para la trazabilidad, la gestión de incidencias y la respuesta ante vulnerabilidades o alertas de seguridad.

9.2. Configuración inicial segura

La configuración inicial de los dispositivos IoMT es una fase crítica que condiciona su nivel de seguridad durante toda su vida operativa. Una configuración inadecuada o incompleta puede introducir vulnerabilidades desde el primer momento, aumentando el riesgo de accesos no autorizados, fallos de funcionamiento o incidentes con impacto clínico.

Las siguientes recomendaciones establecen las buenas prácticas para asegurar una puesta en servicio segura de los dispositivos IoMT:

- **Verificación de la integridad del dispositivo en su recepción**:
  Garantizar que los dispositivos no han sido alterados, manipulados o comprometidos antes de su recepción e instalación. Esto incluye la comprobación del estado físico, sellos de seguridad, firmware original y la procedencia legítima del equipo, conforme a los procedimientos internos de la entidad sanitaria.
- **Aplicación de configuraciones seguras conforme al fabricante y normativa interna**:
  Asegurar que los dispositivos se configuren siguiendo los parámetros de seguridad recomendados por el fabricante, y que dichas configuraciones estén alineadas con el marco normativo, políticas internas y estándares de ciberseguridad de la entidad sanitaria. Cualquier desviación debe estar debidamente justificada, documentada y aprobada.
- **Reducción de la superficie de ataque (hardening)**:
  Garantizar la desactivación de todos los servicios, funciones, cuentas y puertos que no sean estrictamente necesarios para el funcionamiento del dispositivo. Esta medida debe aplicarse tanto al propio dispositivo IoMT como a los sistemas y servicios asociados, asegurando que únicamente permanezcan operativos aquellos componentes indispensables para su uso clínico.
- **Cambio de credenciales por defecto**:
  Garantizar que todas las credenciales por defecto (usuarios, contraseñas, claves de acceso o tokens) sean modificadas antes de poner el dispositivo en producción. En caso de que el dispositivo no permita el cambio de credenciales, esta limitación debe ser documentada y compensada mediante controles adicionales.
- **Sincronización de fecha y hora**:
  Configurar correctamente la fecha y hora del dispositivo, preferiblemente mediante servidores de tiempo seguros, para garantizar la coherencia de los registros de eventos, la trazabilidad de acciones y el análisis posterior de incidentes.
- **Validación previa a la puesta en servicio**:

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

Realizar una verificación final de seguridad antes de la puesta en producción del dispositivo, confirmando que la configuración aplicada cumple con las políticas internas, las recomendaciones del fabricante y los requisitos regulatorios aplicables.

9.3. Gestión de accesos

La gestión de accesos es un elemento crítico para garantizar la seguridad de los dispositivos IoMT y la integridad de la información clínica. El personal de ingeniería clínica tiene la responsabilidad de administrar y mantener los dispositivos, pero únicamente dentro de las capacidades que el propio dispositivo permite. Cualquier acceso o modificación a través de sistemas de monitorización centralizada o plataformas clínicas corresponde al personal de TI o a los equipos responsables.

Para asegurar una gestión adecuada, se recomiendan las siguientes buenas prácticas:

- **Acceso autorizado**:
  Asegurar que solo el personal encargado interactúe con las funciones que el dispositivo, como ajustes de calibración, configuración inicial de parámetros o mantenimiento preventivo.
- **Gestión de credenciales**:
  Garantizar que las cuentas utilizadas para acceder a los dispositivos cumplan con las políticas de seguridad de la entidad, evitando contraseñas por defecto o compartidas, y promoviendo la renovación periódica.
- **Revisión periódica de permisos**:
  Revisar periódicamente los accesos asignados, asegurando que usuarios inactivos o que ya no tienen responsabilidades sobre los dispositivos sean deshabilitados.
- **Segregación de funciones**:
  Evitar que un mismo usuario tenga permisos que mezclen mantenimiento físico del dispositivo con gestión clínica o acceso a sistemas centralizados, minimizando riesgos de errores o accesos indebidos.

9.4. Gestión de actualizaciones

La correcta gestión de las actualizaciones de software, firmware y componentes asociados es un elemento clave para garantizar la seguridad, fiabilidad y continuidad operativa de los dispositivos IoMT. La falta de actualizaciones expone a los dispositivos a vulnerabilidades conocidas, mientras que una actualización mal planificada puede generar fallos operativos o impactos clínicos no deseados.

Para asegurar una gestión adecuada, se recomiendan las siguientes buenas prácticas:

- **Aplicación de versiones actualizadas y parches de seguridad**:
  Garantizar que los dispositivos IoMT, siempre que sea viable desde el punto de vista técnico y económico, cuenten con las versiones estables más recientes de hardware, software y firmware, incluyendo los parches de seguridad publicados por el fabricante. Este proceso debe realizarse en coordinación con el proveedor y con los equipos responsables de la entidad sanitaria, evaluando en todo momento su impacto clínico y operativo.
- **Mecanismos de reversión y recuperación segura**:

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

Disponer de procedimientos y mecanismos de reversión segura que permitan restaurar la configuración o la versión anterior del dispositivo en caso de fallo, incompatibilidad, impacto clínico o degradación del servicio tras una actualización.

- **Validación previa en entornos de prueba**:
  Antes de la instalación de cualquier actualización en el entorno productivo, estas deberán ser revisadas y probadas en un entorno de pruebas controlado, preferiblemente ubicado en las instalaciones del proveedor o en un entorno representativo del entorno real de operación.
- **Gestión documental y trazabilidad de actualizaciones**:
  Mantener una gestión documental sistemática para el seguimiento y registro de todas las actualizaciones aplicadas, incluyendo la fecha, el contenido de la actualización y los dispositivos, sistemas y servicios IoMT afectados. Esta trazabilidad es esencial para la gestión de incidencias, auditorías y cumplimiento normativo.

9.5. Gestión vulnerabilidades en dispositivos médicos

La gestión proactiva de vulnerabilidades es fundamental para mantener la seguridad de los dispositivos IoMT, evitando que fallos conocidos sean explotados y afecten al funcionamiento de los equipos o la seguridad del paciente. Un enfoque estructurado permite identificar, evaluar y corregir las vulnerabilidades de manera oportuna, reduciendo riesgos clínicos y operativos.

Las siguientes buenas prácticas establecen un marco de actuación para la gestión de vulnerabilidades:

- **Proceso continuo y proactivo de identificación de vulnerabilidades:**
  Establecer un proceso sistemático para la detección y seguimiento de vulnerabilidades, que incluya la consulta periódica de bases de datos públicas, boletines de seguridad de fabricantes, alertas de organismos especializados y fuentes de inteligencia de amenazas.
- **Análisis y pruebas periódicas**:
  Asegurar que se realizan evaluaciones regulares de vulnerabilidades mediante herramientas de escaneo y pruebas de penetración controladas y que estas pruebas se efectúen exclusivamente en entornos seguros y autorizados, como las instalaciones del proveedor o un laboratorio controlado. Todas las vulnerabilidades detectadas deben ser documentadas detalladamente, incluyendo descripción, riesgo asociado y dispositivos afectados.
- **Plan de respuesta y seguimiento**:
  Asegurar que cada vulnerabilidad identificada cuente con un plan de acción documentado, que incluya medidas correctivas, responsables asignados y plazos de resolución orientativos. Asimismo, realizar un seguimiento continuo hasta que la vulnerabilidad sea completamente mitigada o se acepte el riesgo asociado, garantizando en todo momento la trazabilidad de la gestión y el cumplimiento de los procedimientos de seguridad.
- **Registro y trazabilidad**:
  Mantener un registro centralizado de todas las vulnerabilidades identificadas, acciones realizadas, resultados de pruebas y estado final de mitigación. Esta documentación es esencial para auditorías internas, cumplimiento normativo y mejora continua de la seguridad en los dispositivos IoMT.

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

9.6. Gestión de eventos

La gestión de eventos en dispositivos IoMT es esencial para detectar de manera efectiva a incidentes que puedan afectar la seguridad del paciente, la operación de los dispositivos o la integridad de los datos. Un sistema de gestión de eventos permite monitorear el funcionamiento de los dispositivos, identificar anomalías y tomar acciones correctivas oportunas.

Las siguientes buenas prácticas se recomiendan para una gestión eficaz de eventos:

- **Registro inicial de eventos**:
  Asegurar desde su despliegue, que los dispositivos IoMT estén configurados para registrar de manera continua todos los eventos relevantes, incluyendo errores operativos, alertas de seguridad, fallos de funcionamiento y cualquier actividad que pueda afectar la integridad del dispositivo o la seguridad del paciente. Esta configuración inicial garantiza que la entidad disponga de información completa para la detección temprana de incidentes.
- **Canales de comunicación y atención a incidentes**:
  Establecer procedimientos y canales de comunicación para recibir, evaluar y atender incidentes relacionados con eventos no deseados, como vulnerabilidades detectadas, errores de operación o sospechas de incidentes de seguridad.
- **Registro de logs**:
  Asegurar que los registros se conserven siguiendo las políticas de la entidad sanitaria y que estén almacenados en formatos estructurados y estandarizados (XML, JSON o Syslog, etc.), facilitando su análisis y trazabilidad.
- **Integración con sistemas de monitoreo continuo**:
  Cuando sea posible, garantizar que los registros se integren con los sistemas de monitoreo y detección de la entidad sanitaria, como el SIEM corporativo, permitiendo identificar intrusiones, accesos no autorizados o actividades sospechosas de manera proactiva.

9.7. Gestión de incidentes

La gestión de incidentes es un elemento crítico para minimizar el impacto de cualquier evento que afecte a la seguridad, disponibilidad o integridad de los sistemas y dispositivos IoMT. Contar con procedimientos estructurados permite una respuesta rápida y coordinada, garantizando la continuidad de la atención y la protección de la información y de los pacientes.

Se recomiendan las siguientes buenas prácticas:

- **Procedimiento integral de gestión de incidentes**:
  Garantizar que existe un procedimiento formal para la gestión de todos los incidentes que ocurran en las instalaciones y que puedan afectar la seguridad de los sistemas, servicios o dispositivos IoMT. Este procedimiento debe cubrir todas las fases del ciclo de vida del incidente, desde su detección hasta la resolución y análisis posterior.
- **Roles y responsabilidades ante incidentes**:
  Asegurar que las responsabilidades estén claramente asignadas a los miembros del equipo técnico y de gestión, de modo que existan recursos y competencias suficientes para detectar, contener, erradicar, recuperar y analizar los incidentes de forma eficaz, garantizando una

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

respuesta rápida y coordinada frente a cualquier evento que afecte a los dispositivos IoMT o a los sistemas asociados.

- **Gestión de evidencias**:
  Garantizar que se disponen de procedimientos documentados para la recogida, conservación, transporte, acceso y análisis de evidencias digitales, cumpliendo con las normativas internas y requisitos legales aplicables.
- **Notificación inmediata**:
  Garantizar que todos los incidentes de seguridad se reporten de manera inmediata a los responsables de la entidad y que, cuando por su impacto o potencial riesgo paraa la seguridad del paciente puedan considerarse incidentes graves, se activen los procedimientos de vigilancia y notificación establecidos en el MDR y en el Real Decreto 192/2023.
- **Comunicación interna**:
  Emplear los canales de comunicación formales definidos por la entidad, asegurando que la información sobre el incidente llegue a todos los actores involucrados, incluyendo personal técnico, administrativo y clínico, para coordinar la respuesta y minimizar impactos.

9.8. Gestión de la obsolescencia

La gestión de la obsolescencia de los dispositivos IoMT es fundamental para garantizar la continuidad operativa, la seguridad del paciente y el cumplimiento normativo. Este proceso abarca la planificación de la retirada de equipos, la transferencia tecnológica y la correcta gestión de los datos que puedan contener.

Se recomiendan las siguientes buenas prácticas:

- **Notificación y baja de dispositivos**:
  Asegurar que la retirada o baja de cualquier dispositivo IoMT se gestione de forma controlada y se notifique a las áreas responsables de la entidad de acuerdo con los procedimientos internos de la entidad sanitaria y, cuando proceda, en coordinación con el fabricante, garantizando así la trazabilidad y el registro de la acción.
- **Planificación de transferencia y restitución tecnológica**:
  Garantizar que exista una planificación detallada para la restitución, reemplazo o transferencia tecnológica de los dispositivos obsoletos, contemplando los medios, procedimientos, acciones de contingencia y los riesgos potenciales asociados.
- **Gestión segura de datos personales**:
  En caso de que los dispositivos contengan datos personales o información clínica sensible, asegurar que se recupere o transfiera la información en el formato y los plazos establecidos por la normativa vigente, o, en su defecto, que se proceda a su destrucción segura, proporcionando evidencias certificadas de la correcta ejecución de estas acciones.

9.9. Auditorías técnicas

Las auditorías técnicas son fundamentales para verificar la seguridad, correcta configuración y funcionamiento de los dispositivos IoMT antes y después de su despliegue. Estas revisiones permiten detectar vulnerabilidades, errores operativos y riesgos de exposición de datos, asegurando que los dispositivos cumplen con los estándares de seguridad y las políticas de la entidad sanitaria.

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

Se recomiendan las siguientes buenas prácticas:

- **Pruebas previas a la puesta en producción**:
  Garantizar la realización de auditorías técnicas periódicas sobre los dispositivos IoMT antes de su despliegue, con el objetivo de identificar vulnerabilidades, errores de configuración, riesgos de exposición de información y posibles vectores de ataque que puedan comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de los datos clínicos y la operativa de la entidad.
- **Colaboración con el proveedor**:
  Ser el punto de contacto con los proveedores para la coordinación de las auditorías que se lleven a cabo en la entidad sobre los dispositivos, asegurando que todas las pruebas se realicen de manera segura y conforme a las recomendaciones del fabricante, y que se documenten los hallazgos y las acciones correctivas propuestas.
- **Pruebas post-despliegue**:
  Asegurar que se realicen auditorías técnicas tras el despliegue de los dispositivos en el entorno operativo, verificando que la configuración final, las actualizaciones aplicadas y la integración con sistemas existentes cumplen con los requisitos de seguridad y no generan nuevos riesgos.
- **Documentación y trazabilidad**:
  Garantizar que se registran los resultados de todas las auditorías, incluyendo vulnerabilidades detectadas, medidas correctivas implementadas y responsables asignados, garantizando la trazabilidad y soporte para auditorías internas o externas.

9.10. Protección de la información

La protección de la información es un pilar fundamental en el uso seguro de dispositivos IoMT. La información que generan y manejan estos dispositivos, incluyendo datos clínicos y personales, debe ser protegida frente a accesos no autorizados, modificaciones indebidas y pérdidas, garantizando la privacidad de los pacientes y la continuidad de los servicios sanitarios.

Se recomiendan las siguientes buenas prácticas:

- **Confidencialidad de los datos**:
  Asegurar que la información almacenada y transmitida por los dispositivos IoMT esté protegida mediante cifrado y mecanismos de control de acceso siguiendo las políticas de seguridad de la información de la entidad en coordinación con los responsables de protección de datos, garantizando que solo el personal autorizado pueda acceder a los datos clínicos o personales.
- **Integridad de la información**:
  Garantizar que se implementan medidas que aseguren que los datos no sean alterados de manera no autorizada, mediante registros de auditoría, firmas digitales o controles internos, garantizando la exactitud y confiabilidad de la información clínica.
- **Disponibilidad de la información**:
  Garantizar que los datos críticos generados por los dispositivos IoMT estén siempre disponibles cuando se necesiten, mediante copias de seguridad periódicas, redundancia de sistemas y procedimientos de recuperación ante fallos o 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

- **Clasificación y almacenamiento seguro**:
  Asegurar la clasificación de la información según su nivel de sensibilidad y criticidad, almacenándola de manera segura de acuerdo con las políticas de la entidad sanitaria, evitando la exposición innecesaria y cumpliendo con la normativa de protección de datos aplicable.

9.11. Formación y concienciación

La formación y concienciación del personal es un elemento fundamental para garantizar el uso seguro y responsable de los dispositivos IoMT. Los errores por desconocimiento, la falta de práctica o la escasa comprensión de las funcionalidades del dispositivo pueden derivar en incidentes operativos o de seguridad, afectando tanto a la atención clínica como a la integridad de los datos.

Se recomiendan las siguientes buenas prácticas:

- **Formación continua de los usuarios**:
  Garantizar que todos los usuarios que interactúan con los dispositivos IoMT reciban formación adecuada, incluyendo aspectos sobre funcionamiento, medidas de seguridad, procedimientos de operación y mantenimiento básico. La formación debe ser continua, actualizándose ante cambios en los dispositivos, software o procesos clínicos.
- **Campañas de concienciación**:
  Apoyar y promover la realización de campañas de concienciación en la entidad sanitaria sobre el uso seguro de dispositivos IoMT, destacando la importancia de buenas prácticas, cumplimiento normativo y reporte de incidentes.
- **Participación en sesiones de formación**:
  Fomentar la participación activa del personal en sesiones de formación impartidas por los proveedores, asegurando que los usuarios conozcan las recomendaciones del fabricante, procedimientos de actualización y cualquier requisito técnico relevante para el correcto uso del dispositivo.

10. Recomendaciones de uso seguro personal de TI

El personal de Tecnologías de la Información (TI) tiene un papel crítico en la gestión y seguridad de los dispositivos IoMT dentro de la entidad sanitaria. Su labor no solo incluye la administración técnica de los equipos, sino también la garantía de que la información clínica se gestione de forma segura, la infraestructura de red cumpla con las políticas de seguridad y la continuidad de los servicios clínicos no se vea comprometida.

Las recomendaciones que se presentan a continuación están orientadas a minimizar riesgos de ciberseguridad, garantizar la integridad, disponibilidad y confidencialidad de los sistemas y dispositivos IoMT, y asegurar que los accesos, comunicaciones e integraciones se realicen siguiendo buenas prácticas reconocidas.

10.1. Gestión de accesos a sistemas de control

El control de los dispositivos IoMT depende de sistemas que pueden incluir software de monitorización, consolas de gestión o plataformas de administración centralizada. La seguridad de estos sistemas es

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

crítica, ya que cualquier acceso indebido podría comprometer tanto la integridad del dispositivo como la información clínica asociada.

- **Cuentas individuales y privilegios mínimos**:

  Cada usuario debe disponer de una cuenta única, con permisos estrictamente limitados a las funciones necesarias para su rol. Evitar el uso de cuentas compartidas o genéricas.

- **Política de contraseñas robustas**:

  Configurar las contraseñas con longitud mínima, combinación de letras, números y caracteres especiales, así como el cambio periódico y prohibición de reutilización de contraseñas anteriores.

- **Autenticación multifactor (MFA)**:

  Implementar MFA siempre que sea posible para acceder a los sistemas de control de dispositivos.

- **Revisión periódica de accesos**:

  Auditar regularmente las cuentas activas, revocar accesos innecesarios o de personal que ya no requiere permisos, y ajustar privilegios según cambios en funciones o responsabilidades.

- **Registro y trazabilidad**:

  Mantener logs detallados de accesos y acciones realizadas en los sistemas, asegurando la trazabilidad de cualquier modificación sobre los dispositivos.

- **Segregación de sistemas críticos**:

  Garantizar que los sistemas de control de dispositivos estén aislados de otras redes corporativas o públicas, minimizando el riesgo de accesos no autorizados

10.2. Gestión de accesos remotos

Los accesos remotos a los dispositivos IoMT representan un vector crítico de riesgo si no se gestionan adecuadamente. Es fundamental que las conexiones sean controladas, autorizadas y monitorizadas, garantizando que solo el personal competente pueda administrar los dispositivos sin comprometer la seguridad clínica ni la integridad de la información.

Se recomiendan las siguientes buenas prácticas:

- **Accesos remotos controlados**:
  Asegurar que las herramientas y mecanismos de acceso remoto utilizados para administrar o dar soporte a los dispositivos IoMT estén debidamente autorizados, correctamente configurados y alineados con las políticas de seguridad de la entidad sanitaria.
- **Evaluación de nuevas herramientas**:
  Gestionar las solicitudes de nuevas soluciones de acceso remoto evaluando previamente su impacto en la seguridad, la privacidad de la información y la continuidad asistencial, garantizando que se aplican las medidas de protección necesarias.
- **Autenticación multifactor**:

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

Permitir y fomentar, siempre que sea técnicamente posible, el uso de mecanismos de autenticación multifactor (MFA) para los accesos remotos, reduciendo el riesgo de accesos no autorizados.

10.3. Comunicaciones seguras

Las comunicaciones entre dispositivos IoMT, sistemas clínicos y plataformas corporativas deben protegerse frente a accesos no autorizados, interceptaciones y manipulaciones de datos. La segmentación de red, el cifrado de la información y la monitorización continua son elementos esenciales para reducir la superficie de ataque y mantener la confidencialidad, integridad y disponibilidad de los datos clínicos.

Se recomiendan las siguientes buenas prácticas:

- **Protección de las comunicaciones**:
  Garantizar que las comunicaciones entre los dispositivos IoMT, los sistemas clínicos y las plataformas corporativas se realicen mediante protocolos seguros y cifrados, como HTTPS y TLS, evitando la transmisión de información sensible en texto claro.
- **Segmentación y control de red**:
  Asegurar que los dispositivos IoMT estén correctamente segmentados dentro de la red de la entidad, limitando sus comunicaciones únicamente a los sistemas y servicios necesarios para su funcionamiento.
- **Redes sanitarias segregadas**:
  Configurar redes específicas para dispositivos IoMT, aisladas de las redes de administración y de acceso público de la entidad sanitaria, garantizando que las comunicaciones sean seguras y controladas.
- **Seguridad de la infraestructura de red**:
  Modificar las configuraciones por defecto de routers, firewalls y otros sistemas de red, aplicando parámetros seguros para minimizar riesgos de acceso no autorizado y proteger la integridad de los dispositivos y la información clínica.
- **Supervisión del tráfico**:
  Monitorizar de forma continua las comunicaciones para detectar comportamientos anómalos, accesos no autorizados o posibles incidentes de seguridad.

10.4. Integración con terceros

La interoperabilidad de los dispositivos IoMT con sistemas externos, servicios en la nube o plataformas de proveedores debe realizarse de manera segura y controlada. Esto incluye limitar la información compartida a lo estrictamente necesario y asegurar la trazabilidad de los datos, evitando riesgos asociados a accesos externos o vulneraciones de privacidad.

Se recomiendan las siguientes buenas prácticas:

- **Conexiones seguras con sistemas externos**:
  Garantizar que las integraciones entre los dispositivos IoMT y sistemas de terceros (proveedores, plataformas externas o servicios en la nube) se establezcan de forma segura y controlada.
- **Minimización de la información compartida**:

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

Asegurar que únicamente se recopila y transmite la información estrictamente necesaria para la prestación del servicio, respetando los principios de minimización de datos y privacidad.

- **Interoperabilidad y control**:
  Garantizar que los dispositivos IoMT sean interoperables con las aplicaciones de la entidad mediante el uso de estándares reconocidos, evitando dependencias innecesarias y asegurando la trazabilidad de los intercambios de información.

10.5. Gestión vulnerabilidades en software médico

La gestión proactiva de vulnerabilidades es fundamental para mantener la seguridad de los sistemas de información y el software médico, evitando que fallos conocidos sean explotados y afecten al funcionamiento de los servicios o a la seguridad de los pacientes. Un enfoque estructurado permite identificar, evaluar y corregir vulnerabilidades de manera oportuna, reduciendo riesgos clínicos, operativos y de información.

El personal de TI deberá llevar a cabo la gestión de aquellos sistemas que se encuentren bajo su alcance, incluyendo software médico, aplicaciones clínicas y sistemas de información.

Las siguientes buenas prácticas establecen un marco de actuación para la gestión de vulnerabilidades:

- **Proceso continuo y proactivo de identificación de vulnerabilidades:**
  Establecer un proceso sistemático para la detección y seguimiento de vulnerabilidades, que incluya la consulta periódica de bases de datos públicas, boletines de seguridad de fabricantes, alertas de organismos especializados y fuentes de inteligencia de amenazas, tanto para software médico como para sistemas de información bajo responsabilidad de TI.
- **Análisis y pruebas periódicas**:
  Realizar evaluaciones regulares mediante herramientas de escaneo y pruebas de penetración controladas, asegurando que estas pruebas se efectúen únicamente en entornos seguros y autorizados, como laboratorios controlados o entornos de prueba del proveedor. Todas las vulnerabilidades detectadas deben documentarse detalladamente, incluyendo descripción, riesgo asociado y sistemas o software afectados.
- **Plan de respuesta y seguimiento**:
  Garantizar que cada vulnerabilidad identificada cuente con un plan de acción documentado, que incluya medidas correctivas, responsables asignados y plazos de resolución. Se debe realizar un seguimiento continuo hasta que la vulnerabilidad haya sido completamente mitigada o solucionada, asegurando la trazabilidad de la gestión y el cumplimiento de los procedimientos de seguridad.
- **Registro y trazabilidad**:
  Mantener un registro centralizado de todas las vulnerabilidades identificadas, acciones realizadas, resultados de pruebas y estado final de mitigación. Esta documentación es esencial para auditorías internas, cumplimiento normativo y mejora continua de la seguridad tanto en software médico como en sistemas de información gestionados por TI.

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

10.6. Continuidad de negocio

La continuidad de negocio es esencial para garantizar que los dispositivos IoMT sigan operando de manera segura y confiable, incluso ante incidentes, fallos técnicos o situaciones de contingencia. Contar con planes y procedimientos adecuados asegura la disponibilidad de los servicios clínicos y la protección de la información crítica.

Se recomiendan las siguientes buenas prácticas:

- **Procedimientos de respaldo y recuperación de la información**:
  Garantizar que los dispositivos IoMT estén correctamente integrados en los procedimientos de respaldo y recuperación de la entidad, incluyendo la definición de procesos para la realización de copias de seguridad, la restauración controlada y la recuperación de la información en caso de fallo, pérdida de datos o incidente de seguridad.
- **Integración en planes de recuperación ante contingencias**:
  Asegurar que los dispositivos IoMT estén incorporados en los planes de recuperación ante desastres y contingencias de la entidad sanitaria, de manera que su funcionamiento pueda ser restablecido rápidamente y sin afectar la atención al paciente.
- **Pruebas periódicas de planes de recuperación**:
  Apoyar y participar en la realización de pruebas de los planes de recuperación (DRP), verificando que los procedimientos de respaldo, restauración y continuidad operativa funcionan correctamente y permiten mantener la disponibilidad de los servicios clínicos y de los dispositivos IoMT.

11. Recomendaciones de uso seguro personal sanitario

El personal sanitario es un actor clave en el ecosistema IoMT, ya que interactúa de forma directa y continuada con los dispositivos conectados que apoyan el diagnóstico, el tratamiento y el seguimiento del paciente. Su papel resulta fundamental no solo desde el punto de vista clínico, sino también en la detección temprana de incidencias, el uso seguro de la tecnología y la transmisión de buenas prácticas a los pacientes.

Las siguientes recomendaciones están orientadas a reforzar la seguridad clínica, la protección de la información y la continuidad asistencial, teniendo en cuenta la complejidad tecnológica de los dispositivos IoMT y el entorno operativo en el que se utilizan.

11.1. Gestión de cuentas

El personal sanitario debe gestionar sus cuentas de acceso a dispositivos IoMT y sistemas relacionados de forma responsable, garantizando la seguridad de la información clínica y la continuidad asistencial. La correcta administración de cuentas y contraseñas reduce significativamente el riesgo de accesos no autorizados y de incidentes de seguridad.

Se recomiendan las siguientes buenas prácticas:

- **Cuentas únicas e individuales**:

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

Cada usuario debe disponer de una cuenta personal y no compartida con otros miembros del equipo. Esto permite asignar responsabilidades claras y garantizar la trazabilidad de todas las acciones realizadas en los sistemas y dispositivos.

- **Política de contraseñas seguras**:
  Las contraseñas deben cumplir con los criterios establecidos por la entidad sanitaria, incluyendo:
  - Longitud mínima recomendada según las políticas y normas de seguridad de la organización.
  - Combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
  - No reutilización de contraseñas anteriores.
  - Cambio periódico según las políticas de la entidad.
- **Confidencialidad de las credenciales**:
  Nunca compartir contraseñas ni dejar credenciales anotadas en lugares accesibles. Evitar el uso de credenciales de otro usuario para realizar tareas propias.
- **Bloqueo y desactivación de cuentas**:
  Informar inmediatamente sobre cualquier cuenta comprometida o inactiva, y asegurarse de que las cuentas de usuarios que ya no requieran acceso sean deshabilitadas o eliminadas de manera oportuna.
- **Uso responsable de accesos privilegiados**:
  Si se asignan permisos adicionales para funciones críticas, deben utilizarse únicamente para las tareas específicas autorizadas y registradas, evitando el uso para operaciones no justificadas.

11.2. Gestión de incidentes

El personal sanitario tiene un papel clave en la detección y respuesta temprana ante incidentes relacionados con dispositivos IoMT, garantizando la seguridad clínica y la continuidad del cuidado del paciente. La identificación oportuna de fallos o anomalías permite actuar de manera coordinada con los equipos de electromedicina, TI y proveedores.

- **Detección de problemas:**

Considerar que puede existir un incidente de seguridad o un fallo técnico cuando se observen algunos de los siguientes indicadores:

- Cambios inesperados en la configuración del dispositivo.
- Mensajes de error desconocidos, bloqueos frecuentes o funcionamiento errático.
- Consumo de batería anormalmente rápido, sobrecalentamiento o reinicios espontáneos.
- Notificaciones de acceso desde dispositivos o ubicaciones no reconocidas.
- Pérdida recurrente de conectividad o dificultades para sincronizar datos sin motivo aparente.

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

- Solicitudes inesperadas para instalar software o actualizaciones provenientes de fuentes no oficiales.
- Lecturas o mediciones incoherentes con el estado de salud habitual del paciente.

- **Contacto**:

Cuando se detecte un incidente:

- Priorice siempre la seguridad clínica del paciente.
- Utilice los canales oficiales facilitados por:
  - La entidad sanitaria.
  - El fabricante del dispositivo.
  - El servicio de ingeniería clínica del centro sanitario .
- Reúna y tenga disponible toda la información relevante que pueda recopilar, incluyendo:
  - Información del dispositivo: modelo, número de serie, identificador único y cualquier otro parámetro disponible.
  - Descripción del problema: explicación clara y concisa de la vulnerabilidad o incidente detectado, incluyendo las circunstancias en las que se haya identificado.
- No utilice foros, redes sociales ni instrucciones no oficiales como fuente de soluciones.

- **Procedimiento de emergencia**:

Seguir este procedimiento únicamente si detecta un fallo grave, sospecha de manipulación o un problema que pueda comprometer la salud del paciente o la seguridad del dispositivo:

1. Mantenga la calma para facilitar la toma de decisiones y evitar acciones impulsivas.
2. Evalúe el riesgo clínico:
   - Si el dispositivo es crítico para la salud (marcapasos, bomba de insulina, respirador, etc.), no lo apague ni lo desconecte.
3. Solo si se evalúa que existe un riesgo inminente para la seguridad del paciente, contacte de inmediato con los responsables de la entidad:
   - Contacte con el equipo de ingeniería clínica, quienes evaluarán el incidente y decidirán si debe escalarse a:
     - Equipo de seguridad de la información
     - Personal de TI

   En caso contrario, gestione la incidencia a través de la plataforma de mantenimiento correspondiente.
4. Siga estrictamente las indicaciones proporcionadas por el personal de ingeniería clínica de la entidad:

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

- Podrán solicitarle modificar configuraciones del dispositivo, como desactivar Wi-Fi, Bluetooth u otros métodos de comunicación, o apagar el dispositivo, siempre que estas acciones no comprometan la seguridad del paciente.

5. Documente todo lo observado:
   - Tome fotografías de mensajes de error.
   - Anote la hora, el contexto del incidente y cualquier cambio previo realizado en el dispositivo.
6. No intente repararlo por su cuenta:
   - Evite reinicios bruscos, restauraciones no autorizadas o la instalación de software externo.

11.3. Orientación al paciente sobre el uso seguro de dispositivos

El personal sanitario desempeña un papel fundamental en la correcta utilización de los dispositivos IoMT por parte de los pacientes, especialmente en aquellos casos en los que los dispositivos se emplean de forma ambulatoria, domiciliaria o con un alto grado de autonomía del usuario. Proporcionar indicaciones claras y comprensibles contribuye a reducir errores de uso, incidentes de seguridad y riesgos clínicos.

- **Información básica**:

Se debe asegurar que el paciente comprende, al menos, los siguientes aspectos:

- Finalidad del dispositivo y su función clínica.
- Uso correcto en condiciones normales de funcionamiento.
- Importancia de no modificar configuraciones ni parámetros sin indicación médica.
- Riesgos asociados a un uso inadecuado o a la manipulación no autorizada del dispositivo.

- **Recomendaciones de seguridad**:

Trasladar al paciente pautas básicas de uso seguro, tales como:

- No instalar aplicaciones, software o actualizaciones que no provengan de fuentes oficiales o indicadas por la entidad sanitaria o el fabricante.
- Evitar compartir credenciales, dispositivos de acceso o información sensible relacionada con el dispositivo.
- Mantener el dispositivo en condiciones adecuadas de higiene, carga y almacenamiento, siguiendo las instrucciones del fabricante.
- Informar de inmediato al personal sanitario ante comportamientos anómalos del dispositivo, lecturas incoherentes o mensajes de error.

- **Canales de comunicación**:

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

Indicar claramente al paciente:

- A quién debe contactar en caso de duda, incidencia o fallo del dispositivo.
- Qué información debe facilitar (síntomas, mensajes de error, momento en que ocurrió el problema).
- Qué acciones no debe realizar por su cuenta (reinicios, manipulaciones, restauraciones).

11.4. Formación y concienciación

La evolución constante de los dispositivos IoMT y de sus funcionalidades hace imprescindible que el personal sanitario mantenga un nivel de conocimiento actualizado. La participación activa en actividades formativas contribuye a un uso más seguro, eficiente y alineado con las recomendaciones del fabricante y de la entidad sanitaria.

- **Asistencia a formaciones internas**:

El personal sanitario debe:

- Asistir a las sesiones de formación organizadas por la entidad sanitaria, los equipos de electromedicina o los responsables de TI.
- Familiarizarse con los procedimientos internos relacionados con el uso, reporte de incidentes y mantenimiento básico de los dispositivos IoMT.
- Incorporar las actualizaciones de protocolos y buenas prácticas derivadas de dichas formaciones.

- **Formación impartida por fabricantes o proveedores**:

Siempre que sea posible, se recomienda:

- Participar en las sesiones de formación ofrecidas por los fabricantes o proveedores de los dispositivos.
- Conocer las limitaciones técnicas, recomendaciones de uso seguro y cambios introducidos mediante actualizaciones de software o firmware.
- Trasladar cualquier duda técnica o clínica detectada durante la práctica asistencial a los responsables correspondientes.

12. Casos prácticos

El objetivo de este apartado es ilustrar, mediante casos reales y escenarios documentados, las posibles consecuencias de no aplicar las recomendaciones de uso seguro y responsable de los dispositivos IoMT.

Estos casos no pretenden señalar responsabilidades individuales, sino concienciar sobre la importancia de la correcta configuración, uso y gestión de los dispositivos médicos conectados, así como del impacto directo que estas prácticas tienen sobre la seguridad del paciente.

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. Configuración errónea de dispositivos IoMT

Una configuración incorrecta, incompleta o no validada de los dispositivos IoMT puede derivar en fallos graves de funcionamiento, con consecuencias directas sobre la seguridad y la salud de los pacientes. Los dispositivos médicos conectados no solo procesan información crítica, sino que también intervienen directamente en la administración de tratamientos, diagnósticos y procedimientos clínicos.

Los casos que se presentan a continuación ilustran situaciones reales en Europa donde errores de configuración o exposición inadecuada de dispositivos médicos conectados provocaron daños clínicos, riesgos para la privacidad de los pacientes o vulnerabilidades críticas en sistemas sanitarios. Estos ejemplos subrayan la importancia de aplicar buenas prácticas de configuración, autenticación, cifrado y segmentación de red, así como de validar y supervisar continuamente el funcionamiento de los dispositivos IoMT.

Sobredosificación en tratamientos de radioterapia en Épinal (Francia)	
Fecha	2004 - 2007
Víctima	Hospital Jean Monnet, Épinal (Francia)
Activo comprometido	Unidad de radioterapia
Tipo de Amenaza	Mala configuración / errores de software
Impacto	Sobreexposición de pacientes y fallecimientos
Descripción	Entre 2004 y 2007, el servicio de radioterapia del Hospital Jean Monnet en Épinal administró dosis excesivas de radiación a pacientes con cáncer de próstata debido a errores en la configuración del software de planificación y falta de controles independientes. El incidente afectó a cientos de pacientes, provocando lesiones graves (rectitis, cistitis, fístulas) y varias muertes directamente relacionadas con la sobreexposición. Las investigaciones de la Autoridad de Seguridad Nuclear y de Radioprotección (ASNR) y la Inspección General de Asuntos Sociales (IGAS) de Francia revelaron deficiencias críticas: • Uso de software mal adaptado y sin validación adecuada. • Instrucciones técnicas en inglés sin traducción ni formación suficiente. • Ausencia de procedimientos de verificación y auditorías externas. El caso se considera uno de los más graves en la historia de la radioterapia francesa, con más de 5.000 pacientes afectados en diferentes periodos y hasta 12 fallecimientos atribuidos. Derivó en reformas regulatorias para reforzar la

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

Sobredosificación en tratamientos de radioterapia en Épinal (Francia)	
	seguridad en radioterapia, incluyendo controles redundantes, certificación de software y capacitación obligatoria del personal.

TABLA 2: SOBREDOSIFICACIÓN EN TRATAMIENTOS DE RADIOTERAPIA EN ÉPINAL.

Configuración incorrecta masiva de dispositivos médicos conectados en Europa	
Fecha	Agosto 2025
Víctima	Hospitales y clínicas europeas
Activo comprometido	Dispositivos IoMT (escáneres MRI, CT, rayos X, PACS, sistemas de laboratorio, bombas de infusión)
Tipo de Amenaza	Dispositivos expuestos por configuración incorrecta (sin autenticación, accesibles públicamente)
Impacto	Filtración de datos sensibles de pacientes y grave riesgo potencial para su seguridad
Descripción	En agosto de 2025, un informe de la entidad de ciberseguridad Modat reveló que, en Europa, más de 1,2 millones de dispositivos médicos conectados, incluyendo escáneres de resonancia magnética (MRI), equipos de tomografía computarizada (CT), sistemas PACS y plataformas de gestión hospitalaria, estaban mal configurados y expuestos directamente en Internet. Esta exposición permitió que terceros pudieran acceder a información médica altamente sensible, entre la que se incluyen: • Imágenes diagnósticas (resonancias, tomografías, rayos X). • Historias clínicas completas, incluyendo información de identificación personal (PII) y de salud protegida (PHI). • Resultados de laboratorio y registros de procedimientos clínicos diarios. Las causas técnicas identificadas incluyen: • Uso de credenciales por defecto o inexistentes. • Falta de cifrado en las comunicaciones entre dispositivos y sistemas. • Dispositivos conectados directamente a Internet sin cortafuegos ni segmentación de red, lo que los dejaba expuestos a accesos no autorizados.

TABLA 3: CONFIGURACIÓN INCORRECTA MASIVA DE DISPOSITIVOS MÉDICOS CONECTADOS EN EUROPA.

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

12.2. Incumplimiento de recomendaciones de seguridad en dispositivos IoMT

El uso seguro de los dispositivos IoMT depende no solo de su correcta configuración y mantenimiento, sino también del cumplimiento de las recomendaciones básicas de ciberseguridad por parte de las instituciones sanitarias y el personal responsable. Cuando estas pautas no se aplican de manera sistemática, los dispositivos y sistemas conectados quedan expuestos a riesgos que pueden derivar en interrupciones de la atención, pérdida de datos clínicos o incluso daños directos a los pacientes.

En este apartado se presentan casos reales ocurridos en Europa, donde la falta de aplicación de buenas prácticas de seguridad, como la actualización de sistemas, segmentación de redes y hardening de dispositivos IoMT, tuvo consecuencias graves para la continuidad asistencial y la seguridad clínica. Estos ejemplos muestran de manera clara la importancia de seguir las recomendaciones de seguridad de forma estricta y constante, y cómo su incumplimiento puede afectar tanto a los pacientes como a la operativa hospitalaria.

Ataque WannaCry al NHS (Reino Unido)	
Fecha	2017
Víctima	NHS (National Health Service), Reino Unido
Activo comprometido	Sistemas hospitalarios y dispositivos IoMT conectados
Tipo de Amenaza	Malware / ransomware (WannaCry)
Impacto	Cancelación masiva de citas y cirugías, y dispositivos médicos inoperativos

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

Ataque WannaCry al NHS (Reino Unido)	
Descripción	En 2017, el ataque de ransomware WannaCry afectó gravemente al Servicio Nacional de Salud del Reino Unido (NHS) debido a la falta de aplicación de medidas básicas de ciberseguridad. Entre las deficiencias identificadas se encontraban: • Sistemas críticos sin parches de seguridad aplicados, lo que permitió la explotación de vulnerabilidades conocidas. • Redes internas sin segmentación adecuada, facilitando la propagación rápida del malware entre distintos sistemas y dispositivos. • Ausencia de hardening en equipos y dispositivos IoMT, incrementando la superficie de ataque y la exposición de información y servicios clínicos. Estas vulnerabilidades permitieron que el ransomware se extendiera con gran rapidez, paralizando sistemas clínicos y dispositivos médicos conectados. Como consecuencia directa, se cancelaron más de 19.000 citas y procedimientos quirúrgicos, interrumpiendo de manera significativa la atención sanitaria y evidenciando la importancia de seguir las recomendaciones de seguridad de manera sistemática.

TABLA 4: ATAQUE WANNACRY AL NHS (REINO UNIDO).

Ataque ransomware al Hospital Universitario Düsseldorf (Alemania)	
Fecha	2020
Víctima	Hospital Universitario Düsseldorf, Alemania
Activo comprometido	Sistemas hospitalarios y dispositivos IoMT conectados
Tipo de Amenaza	Ransomware
Impacto	Parálisis de sistemas críticos y retrasos en la atención médica

Ataque ransomware al Hospital Universitario Düsseldorf (Alemania)	
Descripción	En 2020, el Hospital Universitario de Düsseldorf sufrió un ataque de ciberseguridad que paralizó sus sistemas informáticos, incluyendo dispositivos médicos conectados y servicios críticos de atención al paciente. La investigación posterior identificó que el incidente se produjo debido a vulnerabilidades en los sistemas hospitalarios, que no contaban con medidas de seguridad adecuadas ni planes de contingencia suficientemente robustos. Entre las deficiencias detectadas se encontraban: • Sistemas críticos sin actualizaciones de seguridad aplicadas, exponiéndolos a ataques conocidos. • Segmentación insuficiente de la red, lo que permitió la propagación rápida del malware a múltiples sistemas y dispositivos conectados. • Falta de protocolos de recuperación antes contingencias y redundancia, dificultando la continuidad de los servicios durante el incidente. Como consecuencia directa, la parálisis de los sistemas provocó retrasos significativos en la atención de pacientes, obligando al traslado de algunos casos a otros centros y la suspensión temporal de múltiples procedimientos médicos. Además, el hospital sufrió impactos operativos y financieros importantes, evidenciando la necesidad de implementar medidas de ciberseguridad robustas y planes de contingencia efectivos en entornos hospitalarios.

TABLA 5: ATAQUE RANSOMWARE AL HOSPITAL UNIVERSITARIO DÜSSELDORF.

12.3. Uso inadecuado por parte del personal sanitario

El factor humano es un elemento crítico en la operación segura de los dispositivos IoMT. Diversos informes sobre incidentes en entornos sanitarios europeos indican que una proporción significativa de los problemas relacionados con dispositivos conectados se debe a errores de uso por parte del personal sanitario, aunque estos incidentes suelen reportarse de forma agregada y no como casos individuales identificables.

Entre los problemas más frecuentes en el ámbito de ciberseguridad se incluyen accesos no autorizados, fallos en la actualización de software o firmware, configuraciones inseguras que puedan comprometer la integridad del dispositivo, y retrasos o fallos en la aplicación de parches de seguridad que aumenten la exposición a vulnerabilidades.

Estos incidentes son especialmente relevantes en entornos de alta complejidad, como unidades de cuidados intensivos, quirófanos o áreas de oncología radioterápica, donde la densidad de dispositivos conectados y la carga de alarmas es elevada.

El uso inadecuado de los dispositivos IoMT generalmente no es intencionado, sino consecuencia de la complejidad tecnológica, la presión asistencial y la falta de formación específica. Sin embargo, sus efectos pueden ser significativos, comprometiendo tanto la calidad de los datos clínicos como la seguridad del paciente.

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

Gestión inadecuada de alarmas en monitores de pacientes (Alemania)	
Fecha	2009–2015
Víctima	Hospitales alemanes
Activo comprometido	Monitores de pacientes conectados
Tipo de Amenaza	Error de uso / interacción incorrecta personal–dispositivo por falta de formación y comprensión del comportamiento del dispositivo.
Impacto	Posible omisión de eventos clínicos críticos debido a malinterpretación o desactivación de alarmas
Descripción	Entre enero de 2009 y diciembre de 2015, se analizaron los informes de incidentes enviados al BfArM (Instituto Federal de Medicamentos y Dispositivos Médicos de Alemania), que centraliza y evalúa los reportes sobre fallos de dispositivos médicos o errores de uso que puedan poner en riesgo a pacientes, usuarios o personal sanitario. El análisis se centró en la pérdida o fallo de la función de alarma de monitores de pacientes en hospitales alemanes, y reveló que casi la mitad de los incidentes reportados como fallos del dispositivo correspondían en realidad al funcionamiento previsto por el fabricante. Los hallazgos principales incluyen: • Percepción errónea de fallos: el personal consideró que el dispositivo estaba defectuoso, cuando su funcionamiento era conforme a las especificaciones del fabricante. • Déficits de conocimiento del personal: los errores se relacionaron con un desconocimiento de las múltiples funciones del monitor, de los distintos contextos de aplicación y de la interacción con otros dispositivos conectados en red. • Impacto en la atención clínica: aunque no se trataba de fallos técnicos, estos errores de uso pueden retrasar la identificación de cambios críticos en el estado del paciente, aumentando el riesgo de incidentes clínicos.

TABLA 6: GESTIÓN INADECUADA DE ALARMAS EN MONITORES DE PACIENTES (ALEMANIA).

12.4. Lecciones aprendidas de los casos reales

Los casos presentados demuestran que los riesgos asociados al IoMT no son hipotéticos, sino reales y documentados, con implicaciones tanto para la seguridad del paciente como para la continuidad de los servicios sanitarios. A partir de estos incidentes se pueden extraer varias lecciones clave:

- Configuración y validación adecuadas: asegurar que los dispositivos IoMT estén correctamente configurados y validados es fundamental para garantizar su funcionamiento seguro y confiable.

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

- Cumplimiento de las recomendaciones de uso seguro: ignorar pautas básicas de seguridad aumenta significativamente la probabilidad de incidentes clínicos y fallos técnicos.
- Consideración del factor humano: la formación, conocimiento y experiencia del personal que opera los dispositivos es un componente crítico de la seguridad del IoMT.
- Enfoque integral de seguridad: la protección efectiva de los dispositivos IoMT requiere una visión completa que combine tecnología, procesos y capacitación continua del personal.

Estas lecciones refuerzan la importancia de aplicar de manera sistemática los principios y buenas prácticas presentados a lo largo de esta guía, contribuyendo a un uso seguro y responsable de los dispositivos médicos conectados.

13. Conclusiones

Los casos prácticos revisados demuestran que errores de configuración, incumplimiento de recomendaciones de seguridad o un uso inadecuado por parte del personal pueden derivar en incidentes clínicos graves, filtración de datos sensibles o interrupciones en servicios sanitarios críticos. Esto pone de manifiesto la necesidad de abordar la seguridad del IoMT de manera proactiva y sistemática.

La seguridad de los dispositivos IoMT es una responsabilidad compartida entre el personal de ingeniería clínica, TI y médico. Cada perfil tiene competencias específicas y roles definidos, y solo mediante la coordinación entre ellos se puede garantizar la integridad, disponibilidad y confidencialidad de los sistemas, así como la seguridad del paciente. La correcta configuración, el mantenimiento regular y la gestión de vulnerabilidades son fundamentales para minimizar los riesgos, mientras que la falta de controles básicos o la desatención de las recomendaciones del fabricante puede incrementar significativamente la probabilidad de incidentes. Asimismo, una adecuada respuesta a incidentes permite reducir el impacto y la propagación una vez que el incidente se ha producido.

El factor humano se establece como un elemento determinante en la seguridad del IoMT. Muchos incidentes no se originan por fallos técnicos, sino por errores de manejo, desconocimiento de las funciones del dispositivo o insuficiente formación del personal. La capacitación continua, la concienciación sobre buenas prácticas y la familiarización con los procedimientos de operación y mantenimiento son esenciales para garantizar un uso seguro de los dispositivos.

Asimismo, la integración segura con sistemas externos y la protección de la información clínica son aspectos clave. Solo debe compartirse la información estrictamente necesaria, asegurando la trazabilidad, el control y el respeto por la privacidad del paciente. La adopción de procedimientos estandarizados, la monitorización de eventos e incidentes y la documentación rigurosa de cada acción contribuyen a la resiliencia de los entornos IoMT.

Finalmente, la seguridad del IoMT requiere una visión integral que combine tecnología, procesos, formación y cultura organizativa centrada en el paciente. La aplicación sistemática de las recomendaciones incluidas en esta guía permitirá reducir riesgos, proteger la información clínica y garantizar la seguridad del paciente en entornos sanitarios cada vez más conectados y dependientes de

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

dispositivos inteligentes, siempre cumpliendo con las recomendaciones del fabricante según la funcionalidad prevista del dispositivo.

14. Anexos

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

14.1. Anexo I: Responsabilidad de los perfiles por dominio

A continuación, se presenta el mapeado de aplicabilidad para cada uno de los dominios de seguridad definidos en el documento, en función de las diferentes tipologías de perfiles identificadas.

ID	Dominio	Personal de ingeniería clínica	Personal de TI	Personal sanitario
D_01	Gestión de dispositivos	Supervisión, mantenimiento y registro	-	-
D_02	Configuración inicial	Configuración inicial con parámetros seguros en coordinación con el fabricante/proveedor	-	-
D_03	Gestión de accesos	Accesos lógicos a los dispositivos	Accesos a sistemas de control y remotos	Gestión segura de cuentas y credenciales, contraseñas únicas
D_04	Gestión de actualizaciones	Coordinación con proveedores y pruebas en coordinación con el fabricante/proveedor	-	

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

ID	Dominio	Personal de ingeniería clínica	Personal de TI	Personal sanitario
D_05	Gestión de vulnerabilidades en dispositivos médicos	Detección y coordinación de parches en coordinación con el fabricante/proveedor	-	-
D_06	Gestión de vulnerabilidades en software médico	Detección y coordinación de parches	Detección y coordinación de parches	-
D_07	Gestión de eventos	Configuración y registro de eventos generados	Registro de eventos de red	-
D_08	Gestión de incidentes	Notificación y seguimiento de incidentes	Monitorización del tráfico y registro de evidencias	Notificación de incidentes
D_09	Gestión de la obsolescencia	Gestión de la baja de dispositivos	-	-
D_10	Continuidad de negocio	-	Procedimientos de restauración y soporte en pruebas DRP	-
D_11	Comunicaciones seguras	-	Cifrado de las comunicaciones y segmentación de red	-
D_12	Auditorías de seguridad	Apoyo y seguimiento de auditorías	-	-

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

ID	Dominio	Personal de ingeniería clínica	Personal de TI	Personal sanitario
D_13	Protección de la información	Implementación de controles de seguridad en dispositivos	Cifrado en de la comunicación en tránsito	-
D_14	Formación y concienciación	Capacitación del personal involucrado	-	Asistencia a formaciones técnicas y de seguridad

TABLA 7: APLICABILIDAD DOMINIOS POR TIPOLOGÍA DE PERFILES.

15. Referencias

1. Autorité de Sûreté Nucléaire et de Radioprotection (ASNR). (2013). *Les accidents de radiothérapie*. https://recherche-expertise.asnr.fr/savoir-comprendre/sante/laccident-radiotherapie-depinal

2. 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

3. 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

4. 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

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

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

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

8. 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

9. 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

10. 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

11. European Union Agency for Cybersecurity (ENISA). (2025). *Cyber Hygiene in the Health Sector.*

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

https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector

12. 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

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

14. Healthcare and Public Health Sector Coordinating Council (HSCC). (2021). *BP. 11: Health industry cybersecurity — Managing legacy technology security (HIC-MaLTS)*. https://healthsectorcouncil.org/legacy-tech-security/

15. Healthcare and Public Health Sector Coordinating Council (HSCC). (2021). *BP. 12: Principles and practices for software bill of materials for medical device cybersecurity*. https://healthsectorcouncil.org/health-industry-publishes-guide-for-medical-device-and-health-it-security/

16. Healthcare and Public Health Sector Coordinating Council (HSCC). (2020). *Cybersecurity practices for medium and large healthcare organizations*. https://405d.hhs.gov/Documents/tech-vol2-508.pdf

17. 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

18. 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

19. 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

20. 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

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

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

22. 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

23. 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

24. 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

25. Oficina de Coordinación de Ciberseguridad (OCC). (2023). *Guía sobre Seguridad en Dispositivos IoT*. https://occ.ses.mir.es/publico/occ/dam/jcr:a97a3ac9-1a92-4af0-a5c0-3ac8557244ba/Gu%C3%ADa%20sobre%20Seguridad%20en%20Dispositivos%20IoT.pdf

26. The Lyon Firm. (2025). *Misconfigured Healthcare Devices Data Breach | Patient Privacy*. https://thelyonfirm.com/blog/misconfigured-healthcare-devices-data-breach/

16. 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.

16.1. Lista de materias tratadas en la guía

- Ciberseguridad aplicada a dispositivos médicos conectados (IoMT)
- Contexto general del IoMT
- Riesgos asociados al IoMT
- Principios de uso responsable
- Tipos de usuarios finales en IoMT
- Recomendaciones de uso responsable en IoMT

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

- Gestión de dispositivos
- Gestión de identidades y accesos
- Seguridad de la red
- Protección de datos y privacidad
- Actualizaciones y mantenimiento
- Gestión de incidentes

16.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

16.3. 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

Uso responsable y seguro de dispositivos IoMT en entornos sanitarios

Enero 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