RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Privacidad y Protección de datos en IoMT

Febrero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

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

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

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 23/02/2026

Fecha de última actualización: 09/03/2026

ÍNDICE DE CONTENIDOS

Financiado por la Unión Europea NextGenerationEU

ÍNDICE DE TABLAS

1. Introducción

La digitalización del sector sanitario español ha avanzado de manera acelerada en los últimos años, impulsada en gran medida por la incorporación del Internet de los Dispositivos Médicos (IoMT) en hospitales y centros sanitarios. Esta expansión tecnológica ha permitido mejorar la monitorización remota de personas pacientes, aumentar la precisión diagnóstica y optimizar los procesos clínicos y administrativos. Dispositivos como monitores conectados, bombas de infusión inteligentes, sensores portátiles, sistemas de telemedicina y plataformas integradas con la historia clínica electrónica se han convertido en herramientas esenciales para una atención sanitaria más eficiente, preventiva y personalizada.

Sin embargo, esta transformación no solo incrementa la complejidad técnica del entorno sanitario, sino que también genera nuevos desafíos en materia de protección de datos personales, especialmente debido al tratamiento continuo de datos de salud, considerados por el Reglamento General de Protección de Datos (RGPD) como categorías especiales que requieren salvaguardas reforzadas. Cada dispositivo conectado transmite información sensible que, si no se gestiona adecuadamente, puede comprometer la intimidad de la persona paciente, alterar procesos asistenciales o exponer información crítica a usos indebidos. Además, la existencia de múltiples actores, como fabricantes, proveedores o centros sanitarios, incrementa la dificultad de garantizar el cumplimiento normativo en todo el ciclo de vida del dato.

Los incidentes relacionados con la privacidad en el sector sanitario han demostrado que la protección de datos en IoMT no puede abordarse únicamente desde una perspectiva tecnológica. Se requiere un enfoque integral que combine aspectos organizativos, legales y operativos, alineado con las exigencias del RGPD y la Ley Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y que considere tanto la complejidad técnica de los ecosistemas conectados como la necesidad de garantizar los derechos y libertades de las personas pacientes.

2. Objetivo y alcance

2.1. Objetivo

El objetivo principal de esta guía es establecer un marco práctico, estructurado y alineado con la normativa vigente en materia de protección de datos, principalmente el RGPD y la LOPDGDD, para garantizar el cumplimiento de las obligaciones de privacidad aplicables a los ecosistemas IoMT utilizados en entornos sanitarios.

De manera específica, la guía pretende:

- Proporcionar un marco metodológico claro que permita a las entidades sanitarias comprender, aplicar y documentar adecuadamente las obligaciones del RGPD y la LOPDGDD, así como otras regulaciones aplicables, en los tratamientos realizados mediante dispositivos IoMT.
- Orientar la implementación de medidas técnicas y organizativas que garanticen la privacidad y la seguridad de los datos tratados por estos dispositivos, desde su diseño e implantación hasta su operación continua y eventual retirada.

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

- Facilitar la interpretación de los principios y bases de licitud aplicables en IoMT, ayudando a identificar roles , responsabilidades y requerimientos de documentación.

En conjunto, esta guía aspira a convertirse en un documento de referencia para que las organizaciones sanitarias españolas puedan integrar adecuadamente los requisitos de privacidad en el despliegue, uso y supervisión de dispositivos IoMT, contribuyendo así a garantizar la seguridad de la persona paciente, la protección de los datos personales y la confianza en la digitalización asistencial.

2.2. Alcance

Esta guía aplica a todos aquellos dispositivos IoMT y elementos del ecosistema sanitario conectados que traten datos personales, especialmente datos relativos a la salud, y que se integren con redes, sistemas de información o infraestructuras sanitarias:

- Dispositivos médicos conectados utilizados en la monitorización, diagnóstico o tratamiento de las personas pacientes, como monitores de constantes, bombas inteligentes, ventiladores, sensores vestibles o equipos que transmiten información a sistemas clínicos.
- Dispositivos implantables con conectividad, como marcapasos, desfibriladores implantables, bombas de insulina inteligentes u otros dispositivos que permiten la supervisión remota o el intercambio continuo de datos con sistemas hospitalarios.
- Equipamiento sanitario integrado en redes asistenciales, tales como plataformas de telemetría, sistemas CPAP conectados, equipos de diagnóstico remoto o dispositivos que interactúan con servicios cloud o sistemas de historia clínica.
- Infraestructura tecnológica asociada, incluyendo aplicaciones móviles vinculadas a los dispositivos, plataformas de gestión de datos clínicos, servicios en la nube, redes hospitalarias, gateways IoMT y sistemas de interoperabilidad.

Asimismo, esta guía está dirigida a cualquier profesional o entidad involucrada en el tratamiento de datos en entornos IoMT, tales como:

- Personal clínico que utiliza los dispositivos para el seguimiento y atención de las personas pacientes.
- Personal de ingeniería clínica, encargado de la instalación, calibración, mantenimiento y actualización de dispositivos IoMT.
- Equipos de TI y seguridad, encargados de la protección de redes, la gestión de accesos, la integración tecnológica y la seguridad de la información generada o transmitida por los dispositivos.
- Proveedores tecnológicos y fabricantes, cuando actúan como encargados o subencargados del tratamiento y participan activamente en el soporte, mantenimiento o explotación de los dispositivos IoMT

2.3. Metodología

La elaboración de esta guía se ha basado en un enfoque estructurado que combina el análisis del ámbito regulatorio y el conocimiento experto en protección de datos y entornos IoMT. El objetivo es ofrecer un documento riguroso, comprensible y útil para cualquier profesional sanitario o tecnológico involucrado en el tratamiento de datos personales mediante dispositivos 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

Los principales elementos de la metodología son:

- Análisis de las principales normativas en materia de protección de datos, incluyendo el RGPD y la LOPDGDD, así como estándares, guías, informes y recomendaciones de organismos especializados como ENISA. Esta revisión garantiza que las directrices de la guía estén alineadas con el marco regulatorio vigente y con las mejores prácticas en privacidad en el contexto sanitario.
- Para facilitar la comprensión y aplicación de las obligaciones de privacidad en entornos IoMT, la guía organiza su contenido en una serie de fases estructuradas que permiten abordar de manera ordenada los aspectos esenciales del cumplimiento normativo:
    - Introducción a los aspectos de privacidad: Explicación inicial de los principios, riesgos y particularidades del tratamiento de datos en IoMT.
    - Análisis del marco normativo aplicable: Identificación y revisión de las normas que rigen el tratamiento de datos en ecosistemas IoMT.
    - Revisión de normativas y estándares complementarios: Determinación de las obligaciones adicionales que deben considerarse en entornos clínicos.
    - Definición de medidas técnicas y organizativas: Establecimiento de las medidas prácticas que deben adoptarse para garantizar la privacidad en IoMT.
- Adaptación del contenido a un lenguaje accesible, se ha priorizado la claridad y comprensión para todos los perfiles de personas usuarias finales, asegurando que las recomendaciones puedan aplicarse de manera práctica sin necesidad de conocimientos técnicos avanzados.

Esta metodología asegura que la guía proporcione un marco estructurado que permita a las organizaciones sanitarias comprender y aplicar de forma sistemática y coherente los requisitos de privacidad asociados al uso de dispositivos IoMT.

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) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud (en adelante, EHDS).
    - 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).

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

- Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización (en adelante, Data Act).
- 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).
- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.
- Ley 14/2007, de 3 de julio, de Investigación biomédica.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- **Estándares**:
  - IEC/ISO 81001, Normas relacionadas con la ingeniería de software para dispositivos médicos.
  - ISO/IEC 27001:2022, Gestión de la seguridad de la información.
  - ISO/IEC 27701:2025, Gestión de la privacidad de la información.
  - ISO 27799:2025, Gestión de la seguridad de la información en entornos sanitarios.
  - ISO 22301:2019, Gestión de la continuidad de negocio.

- **Guías**:
  - BSI TR-03161, Requerimientos de seguridad para aplicaciones de eHealth.
  - ENISA - Cyber Hygiene in the Health Sector.
  - ENISA - ENISA Threat Landscape: Health Sector.
  - ENISA - CSIRT Capabilities in Healthcare Sector.
  - ENISA - Cloud Security for Healthcare Services.
  - ENISA - Procurement Guidelines for Cybersecurity in Hospitals.
  - ENISA - Baseline Security Recommendations for IoT.
  - ENISA - Cyber security and resilience for Smart Hospitals.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - MDCG - Guidance on classification of medical devices.
  - MDCG - Guidance on Cybersecurity for medical devices.

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

- MDCG - Guidance on qualification and classification of software.
- NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
- NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.
- NIST SP 800-53 y SP 800-115, Guía de controles y pruebas técnicas de seguridad.

4. Definiciones

Acrónimos	Definición
Acceso de emergencia	Mecanismo excepcional que permite acceder a dispositivos críticos fuera de los controles habituales cuando es necesario para garantizar la continuidad asistencial.
Anonimización	Proceso que elimina cualquier posibilidad de identificar a una persona a partir de los datos.
Cadena de suministro	Conjunto de entidades, procesos y recursos implicados en el diseño, fabricación, distribución, mantenimiento y retirada de un dispositivo a lo largo de todo su ciclo de vida.
CCN-CERT	Organismo adscrito al Centro Criptológico Nacional que actúa como equipo de respuesta a incidentes de ciberseguridad para las administraciones públicas y entidades estratégicas de España.
CPAP	Terapia de presión positiva continua en la vía aérea que mantiene las vías respiratorias abiertas mediante un flujo constante de aire (del inglés, Continuous Positive Airway Pressure).
CSIRT	Equipo especializado encargado de gestionar incidentes de ciberseguridad y coordinar la respuesta.
DPIA	Evaluación de impacto en protección de datos exigida cuando un tratamiento implica un alto riesgo para los derechos de las personas (del inglés, Data Protection Impact Assessment).
EIPD	Equivalente en español de la DPIA, evaluación de impacto en la protección de datos según el RGPD.
ENISA	Agencia de la Unión Europea responsable de apoyar a los Estados miembros y a las instituciones europeas en materia de resiliencia digital (del inglés, European Union Agency for Cybersecurity).
Firewall	Dispositivo o software que controla y filtra el tráfico de red según reglas de seguridad establecidas.
IDS	Sistema que detecta posibles ataques o actividades sospechosas en la red (del inglés, Intrusion Detection System).
IPS	Sistema que detecta e impide ataques bloqueando el tráfico malicioso en tiempo real (del inglés, (Intrusion Prevention System).
LIS	Sistema de información utilizado en laboratorios clínicos para gestionar pruebas, muestras y resultados (del inglés, (Laboratory Information System).

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
MAGERIT	Metodología española para el análisis y gestión de riesgos en sistemas de información.
MDCG	Grupo de coordinación de la Comisión Europea que apoya la aplicación armonizada del reglamento europeo de productos sanitarios (MDR) y de diagnóstico in vitro (IVDR) (del inglés, Medical Device Coordination Group).
PACS	Sistema para almacenar, gestionar y visualizar imágenes médicas digitales (del inglés, Picture Archiving and Communication System).
Proxy	Servidor intermediario que gestiona las peticiones entre un cliente y un recurso externo, aplicando políticas de filtrado.
Segmentación de red	Técnica de seguridad que divide una red en segmentos aislados para limitar accesos, reducir la superficie de ataque y contener incidentes de seguridad.
Seudonimización	Técnica que transforma los datos personales de manera que no pueda identificarse a una persona concreta sin recurrir a información adicional.
SIEM	Plataforma que centraliza, correlaciona y analiza eventos de seguridad en tiempo real (del inglés, Security Information and Event Management).
SQL	Lenguaje estándar para consultar y gestionar bases de datos relacionales (del inglés, Structured Query Language).
Telemetría	Recopilación, transmisión y análisis automático de datos generados por dispositivos para supervisar su estado y comportamiento de forma remota.
UDI	Identificador único utilizado para identificar de forma estandarizada un dispositivo médico (del inglés, Unique Device Identification).
URL	Dirección utilizada para localizar recursos en Internet (del inglés, Uniform Resource Locator).
Vector de ataque	Vía o método utilizado por un atacante para explotar una vulnerabilidad y comprometer la seguridad de un sistema, red o dispositivo.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Contexto general de la privacidad y protección de datos IoMT

El Internet de los Dispositivos Médicos (IoMT) representa la convergencia equipos, sensores y aplicaciones diseñados para recopilar, transmitir, procesar y analizar datos clínicos en tiempo real. Estos dispositivos, presentes tanto en entornos sanitarios (monitores de constantes vitales, bombas de infusión inteligentes, sistemas de diagnóstico por imagen) como en el ámbito doméstico (marcapasos con conectividad remota, sistemas de monitorización de glucosa, dispositivos de telemedicina), permiten nuevos modelos asistenciales basados en la monitorización continua y en la personalización de la atención médica.

A diferencia de los dispositivos médicos tradicionales, los sistemas IoMT están conectados a redes internas, plataformas en la nube y sistemas de información clínica. Esta conectividad amplía las

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

capacidades diagnósticas y terapéuticas, pero también introduce nuevos riesgos para la privacidad y la seguridad de la persona paciente.

Los datos que manejan estos dispositivos son especialmente sensibles, como información clínica, biométrica o genética que revela aspectos íntimos de la persona paciente y, en muchos casos, enfermedades crónicas. Mientras que una filtración de datos financieros puede remediarse mediante el cambio de credenciales o la emisión de nuevas tarjetas, una filtración de datos sanitarios expone información inmutable, entre otros, un diagnóstico oncológico, una condición de salud mental o una información genética, que acompañará al individuo durante toda su vida y cuya divulgación puede provocar daños irreversibles en su esfera personal, laboral, social y familiar.

Al mismo tiempo, la expansión del IoMT ha incrementado la superficie de exposición de los sistemas sanitarios. La diversidad de dispositivos, la dificultad para mantenerlos actualizados y la interdependencia entre fabricantes, proveedores y centros sanitarios crean un entorno complejo que los actores de amenazas explotan con gran frecuencia.

En este contexto, la protección de datos personales no es solo un requisito legal, sino un elemento fundamental para preservar la confianza de la persona paciente. Una sociedad en la que los ciudadanos teman que sus datos de salud puedan ser accedidos indebidamente, utilizados para discriminarlos o expuestos públicamente, es una sociedad donde las personas ocultarán información relevante al personal médico, evitarán someterse a pruebas diagnósticas, rechazarán tecnologías beneficiosas para su salud y, en última instancia, verán deteriorada su atención sanitaria.

5.1. Amenazas a la privacidad de la información en IoMT

La creciente conectividad introducida por los dispositivos IoMT ha ampliado significativamente la superficie de exposición de los entornos sanitarios, situando al sector de la salud entre los más atractivos para los ciberdelincuentes. Esta situación no se debe únicamente por la criticidad operativa de los servicios sanitarios, sino también por el elevado valor de la información que gestionan.

Según el *IBM Cost of a Data Breach Report 2025*, el sector sanitario vuelve a posicionarse como el más costoso en términos de brechas de datos, manteniendo esta primera posición por decimocuarto año consecutivo. El coste medio de una brecha en este sector alcanza los 6 millones de euros por incidente, situándose muy por encima de otros sectores como el financiero o el industrial.

El informe también destaca que los datos sanitarios siguen siendo especialmente atractivos para actividades delictivas como la suplantación de identidad, el fraude o diversos tipos de crímenes financieros, debido a la riqueza y permanencia de la información clínica asociada a cada individuo.

Además, indica que las brechas de seguridad en el sector salud requieren un mayor tiempo para su identificación y contención, con un ciclo medio de 279 días, superando en más de cinco semanas la media global de 241 días. Este prolongado tiempo de exposición incrementa significativamente el impacto económico y operativo de los incidentes, y se explica en gran medida por la complejidad tecnológica de los entornos sanitarios y la presencia de dispositivos IoMT heterogéneos y difíciles de actualizar.

En este contexto, los entornos IoMT se enfrentan a una serie de amenazas que, debido a su estrecha integración con los sistemas clínicos y a la naturaleza sensible de los datos que gestionan, pueden

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

afectar de manera directa y significativa a la privacidad de la información sanitaria. Entre los riesgos más relevantes se encuentran los siguientes:

❖ Ataques de ransomware dirigidos

Los ataques de ransomware en el sector salud han pasado de ser incidentes centrados únicamente en el cifrado de sistemas a ser complejas operaciones de extorsión por parte de equipos especializados. En estos escenarios, los atacantes no solo bloquean el acceso a la información, sino que también exfiltran datos clínicos, amenazan con publicarlos y, en ocasiones, extorsionan simultáneamente a las personas pacientes y profesionales sanitarios. En el ámbito IoMT, esta amenaza adquiere una dimensión especialmente crítica, ya que numerosos estudios han identificado a los dispositivos conectados como vectores frecuentes de entrada en redes sanitarias, pudiendo comprometer tanto la privacidad de los datos como la seguridad física de la persona paciente.

A continuación, se presentan un ejemplo destacado que ilustra la magnitud y el impacto de esta amenaza:

Ransomware al Hospital Clínic de Barcelona	
Fecha	Marzo de 2023
Víctima	Hospital Clínic de Barcelona
Activo comprometido	Máquinas virtuales y sistemas críticos (laboratorios, farmacia, radiología, PACS, LIS)
Tipo de Amenaza	Ransomware y exfiltración de datos
Vector del ataque	Acceso remoto y cifrado de sistemas hospitalarios
Origen del ataque	Atacantes desconocidos (publicación de datos en dark web y foros)
Impacto	Exposición de información de las personas pacientes, profesionales y proveedores, filtración de archivos clínicos y administrativos, y riesgo para la seguridad y continuidad de la atención

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

Ransomware al Hospital Clínic de Barcelona	
Descripción	En marzo de 2023, el Hospital Clínic de Barcelona sufrió un ataque de ransomware que comprometió máquinas virtuales y sistemas críticos, incluidos laboratorios, farmacia y radiología. Los atacantes exfiltraron grandes volúmenes de datos, entre ellos información de las personas pacientes, profesionales y proveedores, así como archivos clínicos y administrativos, y los publicaron posteriormente en foros delictivos. La exposición afectó directamente la confidencialidad y disponibilidad de información sensible, incluyendo historiales clínicos, resultados de laboratorio y registros de radiología vinculados al ecosistema IoMT (PACS, LIS). Esto generó un riesgo elevado para la seguridad de las personas pacientes y la continuidad de la atención médica, al impedir el acceso oportuno a datos críticos para el diagnóstico y tratamiento.

TABLA 2: RANSOMWARE HOSPITAL CLÍNIC DE BARCELONA .

❖ Explotación de vulnerabilidades en dispositivos médicos

Además de los ataques de ransomware, otra de las principales amenazas para la privacidad en los entornos IoMT es la explotación de vulnerabilidades en los propios dispositivos médicos conectados. Estas vulnerabilidades, que con frecuencia pasan inadvertidas durante largos periodos de tiempo, pueden actuar como puertas traseras que permiten el acceso no autorizado a información clínica altamente sensible. Se estima que más de la mitad de los dispositivos IoMT en uso presentan vulnerabilidades críticas, lo que los convierte en un vector de riesgo significativo tanto para la privacidad como para la integridad de los sistemas sanitarios.

Estas fallas no solo exponen datos generados por el propio dispositivo, como signos vitales en tiempo real, sino que también pueden servir como punto de apoyo inicial para comprometer redes clínicas completas y facilitar la exfiltración de historiales médicos, imágenes diagnósticas o resultados de laboratorio.

A continuación, se presentan un ejemplo que ilustra la gravedad de explotar estas vulnerabilidades:

Manipulación remota de bombas de insulina	
Fecha	Enero 2023
Víctima	Personas pacientes con bombas de insulina Medtronic MiniMed 508 y Minimed Paradigm
Activo comprometido	Bombas de insulina implantables o portátiles
Tipo de Amenaza	Vulnerabilidad de dispositivo y manipulación de terapia

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

Manipulación remota de bombas de insulina	
Vector del ataque	Conexión inalámbrica RF cercana al dispositivo
Origen del ataque	Terceros no autorizados
Impacto	Alteración de dosis de insulina, riesgo de hipoglucemia o hiperglucemia, consecuencias graves para la salud y posible riesgo vital
Descripción	En enero de 2023, las agencias regulatorias ANSM (Francia) y BfArM (Alemania) alertaron sobre vulnerabilidades en las bombas de insulina Medtronic MiniMed 508 y MiniMed Paradigm. La causa del riesgo se debe a fallos en la comunicación inalámbrica RF que permitían a un atacante cercano conectarse al dispositivo y modificar parámetros o controlar la administración de insulina sin pasar por servidores hospitalarios ni redes clínicas. En este sentido, un tercero no autorizado podría alterar la terapia de un paciente, provocando hipoglucemia, hiperglucemia o consecuencias graves para la salud, incluso riesgos vitales en casos críticos. La exposición afectaba directamente a las personas pacientes y pone de relieve la vulnerabilidad de dispositivos IoMT que no dependen únicamente de redes centralizadas para su operación.

TABLA 3: VULNERABILIDADES EN BOMBAS DE INSULINA .

❖ Ataques a la cadena de suministro

Los ataques a la cadena de suministro representan una de las amenazas más complejas y de mayor alcance para la seguridad y privacidad en los entornos IoMT. A diferencia de otros vectores, su criticidad radica en que permiten comprometer simultáneamente a miles de organizaciones a través de un único proveedor de confianza. En el contexto sanitario, donde los dispositivos IoMT dependen de software de terceros, servicios gestionados y componentes embebidos, un ataque de este tipo puede otorgar a los ciberdelincuentes acceso privilegiado a la infraestructura sanitaria, facilitando tanto la exfiltración masiva de información clínica como la interceptación de datos de telemetría de las personas pacientes.

Este tipo de incidentes suele materializarse mediante la manipulación de actualizaciones de software, la inserción de código malicioso en librerías o componentes externos, o la explotación de vulnerabilidades en proveedores que forman parte del ecosistema operativo de los dispositivos médicos. Cuando estos puntos quedan comprometidos, el atacante obtiene una posición estratégica desde la cual puede infiltrarse en múltiples organizaciones sin necesidad de atacar cada instalación por separado

A continuación, se presenta uno de los casos más representativos de ataques a la cadena de suministro que ilustran el impacto en la privacidad y en la seguridad del IoMT:

Vulnerabilidad en software MOVEit Transfer	
Fecha	Junio 2023
Víctima	Entidades sanitarias a nivel internacional
Activo comprometido	Información sensible de las personas pacientes
Tipo de Amenaza	Explotación vulnerabilidad en la cadena de suministro
Vector del ataque	Software de transferencia de ficheros
Origen del ataque	Terceros no autorizados
Impacto	Acceso no autorizado a información sensible de las personas pacientes intercambiada entre dispositivos, sistemas y aplicaciones
Descripción	En enero de 2023, se identificó una vulnerabilidad de inyección SQL en la aplicación web MOVEit Transfer (CVE-2023-34362), un protocolo de transferencia de archivos. Esta vulnerabilidad permitía a un atacante acceder a la base de datos y obtener información confidencial. A través de esta falla, un atacante podría inferir detalles sobre la estructura y el contenido de la base de datos, así como ejecutar instrucciones SQL que modifiquen o eliminen registros. Aunque no se han publicado casos confirmados de explotación de esta vulnerabilidad, existen indicios de que pudo haber sido aprovechada. Cabe destacar que MOVEit Transfer ha presentado varias vulnerabilidades críticas en los últimos años, lo que resalta la importancia de mantener el sistema actualizado y protegido.

TABLA 4: VULNERABILIDADES EN SOFTWARE MOVEIT.

❖ Amenazas internas

Las amenazas internas en los entornos sanitarios constituyen un riesgo especialmente complejo de gestionar, ya que no siempre derivan de intenciones maliciosas. Con frecuencia, surgen de la presión asistencial, de la necesidad de actuar con rapidez o de la búsqueda de soluciones inmediatas ante situaciones clínicas críticas. En estos contextos, es habitual que parte del personal priorice la continuidad del servicio o la urgencia del diagnóstico por encima de los controles de seguridad establecidos, lo que genera prácticas que, aunque no son mal intencionadas, exponen la información clínica a entornos no seguros.

Este tipo de amenazas pueden comprometer gravemente a la privacidad al introducir vectores de fuga de datos desde dentro de la organización.

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

A continuación, se describen dos escenarios frecuentes en entornos IoMT que ejemplifican estas amenazas internas:

- **Uso de Mensajería Instantánea para Telemetría IoMT:** Es común que profesionales sanitarios utilicen aplicaciones como WhatsApp o Telegram para enviar capturas de pantallas de monitores de signos vitales o imágenes diagnósticas con el fin de obtener una segunda opinión de manera urgente. Aunque responde a una intención asistencial legítima, este comportamiento traslada los datos fuera del entorno controlado del hospital y los expone a servicios no autorizados que no cumplen con los requisitos normativos aplicables. Esto podría derivar en casos de divulgación accidental de información personal clínica.

  Este escenario se observa en la Resolución RPS-2024/059 del Consejo de Transparencia y Protección de Datos de Andalucía, relativa al mal uso de datos personales por parte del personal del Hospital Punta de Europa mediante la creación de un grupo de WhatsApp en el que se trataron datos de personas pacientes (nombre, DNI, historia clínica, etc.). La resolución recoge infracciones del RGPD derivadas del uso de un canal no autorizado para el tratamiento de datos de salud y concluye en la obligación de utilizar exclusivamente los canales corporativos oficiales para este tipo de comunicaciones, prohibiendo cualquier otra herramienta.

- **Credenciales Compartidas en Estaciones IoMT:** En unidades de cuidados intensivos, donde el tiempo es crítico, el personal puede recurrir a compartir contraseñas de consolas de monitorización para evitar retrasos operativos. Sin embargo, esta práctica elimina la trazabilidad de los accesos y dificulta detectar actividades indebidas.

❖ Ataques de ingeniería social

Los ataques de ingeniería social representan una de las amenazas más frecuentes y eficaces en el sector sanitario. A diferencia de otros vectores, no se apoyan en vulnerabilidades técnicas de los dispositivos IoMT, sino en errores humanos, la falta de concienciación y una higiene digital insuficiente. La presión asistencial a la hora de tomar decisiones, unida a la complejidad tecnológica del entorno clínico, convierte al factor humano en el eslabón más débil, tal y como advierte el informe "*AI-Augmented Phishing and the Threat to the Health Sector*", elaborado por el *Health Sector Cybersecurity Coordination Center* (HC3), el organismo del Departamento de Salud de EE. UU. especializado en ciberseguridad del sector sanitario.

Asimismo, este estudio subraya que el phishing sigue siendo uno de los vectores más utilizados para iniciar ciberataques en hospitales, llegando a representar casi la mitad de los incidentes en el sector salud en el país.

A continuación, se presenta uno de los casos más representativos de ataques ingeniería social sobre el sector salud:

Suplantación al Ministerio de Salud de Italia	
Fecha	Enero 2026
Víctima	Ministerio de Salud de Italia

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

Suplantación al Ministerio de Salud de Italia	
Activo comprometido	Datos personales y sanitarios de ciudadanos italianos
Tipo de Amenaza	Ataque de ingeniería social
Vector del ataque	Suplantación de identidad, phishing
Origen del ataque	Terceros desconocidos
Impacto	Exposición de información las personas pacientes y riesgo de accesos no autorizados a expedientes, con posible fraude de identidad.
Descripción	En enero de 2026, se detectó una campaña de phishing que suplantaba la identidad del Ministerio de Salud de Italia. Los atacantes enviaron correos masivos a ciudadanos con logotipos, lenguaje y diseño gráfico que imitaban las comunicaciones oficiales sobre la renovación de la tarjeta sanitaria y/o el acceso a la plataforma de historia clínica. Los mensajes incluían enlaces a páginas fraudulentas que simulaban el portal institucional para capturar datos personales y sanitarios y credenciales de acceso a servicios de salud. En los formularios alojados en dichos sitios web se solicitaba, entre otros, identificadores sanitarios, información personal y credenciales, con el objetivo de acceder a historiales médicos o reutilizar los datos en fraudes y ataques dirigidos posteriores. Tras detectar el informe, las autoridades regionales y el propio Ministerio alertaron a las personas pacientes, recomendando no pulsar enlaces, verificar dominios y acceder siempre escribiendo manualmente la URL oficial.

TABLA 5: SUPLANTACIÓN IDENTIDAD MINISTERIO DE SALUD DE ITALIA.

5.2. Datos personales

Para comprender qué es la privacidad de la información y por qué tiene una importancia tan significativa en la actualidad, resulta imprescindible partir de un del concepto de dato personal.

Los datos personales son toda información que permite identificar, de manera directa o indirecta, a una persona física y constituyen el pilar sobre el que se articula todo el marco jurídico de protección de datos. La identificación directa se produce cuando la información contiene elementos evidentes e inequívocos, como el nombre completo, el número de documento de identidad o una fotografía, que permiten reconocer inmediatamente a un individuo. La identificación indirecta, en cambio, aparece cuando diferentes fragmentos de información, que por separado podrían parecer anónimos, permiten en conjunto singularizar a una persona dentro de un grupo.

Las principales características de los datos personales son las siguientes:

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

- **Vinculación con personas físicas:** Solo las personas naturales pueden ser titulares de datos personales. Las personas jurídicas quedan excluidas de esta categoría, si bien la información relativa a profesionales sanitarios, como su número de colegiado o su firma digital, sí puede constituir un dato personal cuando identifica al individuo.
- **Amplitud del concepto de identificación:** La identificación comprende tanto la posibilidad actual como la potencial de reconocer a un individuo, teniendo en cuenta los medios disponibles para establecer esa vinculación. Por ello, incluso datos que hayan sido anonimizados, cifrados o seudonimizados pueden seguir siendo considerados datos personales si a través de procedimientos técnicos se pudiera revertir el proceso.
- **Irrelevancia del soporte:** Los datos personales pueden estar contenidos en cualquier tipo de soporte, ya sea digital, en papel, en imágenes, grabaciones de audio, señales biométricas o cualquier otro formato susceptible de tratamiento.
- **Inclusión de datos inferidos:** No solo se consideran datos personales aquellos proporcionados directamente por la parte interesada, sino también los generados, calculados o inferidos a partir de otros datos, como predicciones de riesgo clínico basadas en telemetría IoMT, siempre que permitan identificar a una persona de manera directa o indirecta.

5.2.1. Datos relativos a la salud

Concretamente, en el entorno sanitario, adquieren especial relevancia los datos relativos a la salud, entendidos como toda información vinculada al estado físico o mental de una persona, ya sea pasada, presente o futura. Esta categoría comprende no solo los diagnósticos clínicos formales, sino también cualquier dato que pueda ofrecer indicios sobre la condición fisiológica o psicológica del individuo, así como la información generada en el curso de la prestación de servicios asistenciales que permita inferir aspectos de su estado de salud.

A continuación se presentan algunas tipologías de datos de salud generados por dispositivos IoMT:

- **Datos fisiológicos directos:** Incluyen mediciones del organismo como frecuencia cardíaca, presión arterial, saturación de oxígeno, temperatura corporal, niveles de glucosa, actividad eléctrica cardíaca o cerebral y parámetros de función respiratoria. Representan información biomédica de alta sensibilidad clínica.
- **Datos de diagnóstico:** Engloban resultados procedentes de pruebas de laboratorio, imágenes médicas digitalizadas, así como informes generados por dispositivos de diagnóstico automatizado. Suelen integrarse directamente en la historia clínica electrónica.
- **Datos terapéuticos:** Recogen información relativa a la administración de tratamientos, como los registros de bombas de infusión, ajustes de dispositivos implantables, parámetros de terapia respiratoria o renal y configuraciones de sistemas de soporte vital.
- **Datos de monitorización continua:** Incluyen series temporales de parámetros vitales, alertas generadas por los dispositivos, tendencias evolutivas y datos de seguimiento longitudinal que permiten analizar la progresión de patologías o la respuesta ante intervenciones médicas.
- **Datos de adherencia y comportamiento:** Se refieren al uso real de dispositivos prescritos, cumplimiento de pautas terapéuticas, patrones de actividad y descanso, así como datos que

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

permiten evaluar conductas vinculadas a la salud, como el grado de adherencia a tratamientos o terapias.

- **Datos contextuales con relevancia clínica:** Comprenden información relacionada con el entorno y comportamiento de la persona paciente que puede influir en su estado de salud: localización durante episodios críticos, patrones de movilidad que reflejan deterioro funcional, factores ambientales que afectan a condiciones respiratorias, entre otros.

5.2.2. Categorías especiales de datos personales

Dentro de los datos personales, existen categorías especiales que requieren de una protección reforzada debido a que su tratamiento puede generar riesgos significativos para los derechos fundamentales y las libertades de las personas. Estas categorías especiales, tradicionalmente denominadas datos sensibles, están sometidas a una prohibición general de tratamiento que solo se pueden excepcionar en circunstancias específicas.

En este sentido, los datos de salud forman parte de las categorías especiales junto con otros tipos de información que comparten ciertas características que podrían generar situaciones de discriminación, vulneración de la intimidad o afectación de la dignidad personal.

Estas son las categorías especiales de datos con presencia en ecosistemas IoMT:

Categoría	Descripción	Ejemplos en el contexto IoMT
Datos de salud	Información sobre salud física o psicológica	Constantes vitales, diagnósticos, tratamientos, resultados de pruebas, historial clínico
Datos genéticos	Información sobre características genéticas heredadas o adquiridas	Secuencias genéticas, pruebas de predisposición genética, farmacogenómica
Datos biométricos	Datos obtenidos de tratamientos técnicos relativos a características físicas o fisiológicas	Patrones de ritmo cardíaco utilizados para autenticación, reconocimiento facial en sistemas de telemedicina, patrones de voz en interfaces de dispositivos, huellas dactilares para acceso a equipos
Datos sobre vida sexual y orientación sexual	Información relativa a la vida sexual o la orientación sexual de una persona física	Datos de dispositivos de salud reproductiva, información de aplicaciones de seguimiento de fertilidad

TABLA 6 6: CATEGORÍAS DATOS ESPECIALES IOMT.

5.3. Perfiles involucrados en el tratamiento

El tratamiento de datos personales en los entornos IoMT involucra a múltiples organizaciones y entidades que participan en diferentes fases del ciclo de vida del dato, desde su generación en el dispositivo hasta su almacenamiento, análisis y eventual supresión. La correcta identificación del rol que

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

cada actor desempeña en el ciclo resulta fundamental para determinar las obligaciones regulatorias aplicables, las responsabilidades ante incidentes y las relaciones contractuales que deben formalizarse.

A diferencia de escenarios más simples donde una única organización controla todo el tratamiento, los ecosistemas IoMT se caracterizan por una cadena de valor compleja donde fabricantes de dispositivos, proveedores de plataformas, prestadores sanitarios, empresas de mantenimiento y otros actores interactúan entre ellos.

5.3.1. Responsable del tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de datos personales. Esta figura ostenta la posición central en el esquema de protección de datos, recayendo sobre ella las principales obligaciones legales y la responsabilidad última de garantizar que el tratamiento se realiza conforme a los principios y requisitos aplicables.

Las principales características del responsable son:

- **Determinación de fines:** El responsable decide la finalidad del tratamiento de datos, estableciendo los objetivos que justifican el tratamiento.
- **Determinación de medios esenciales:** El responsable determina los aspectos fundamentales del tratamiento, incluyendo qué datos se recogen, durante cuánto tiempo se conservan, quién puede acceder a ellos y a quién se comunican.
- **Asunción de responsabilidad:** El responsable responde al cumplimiento de todas las obligaciones legales, incluso cuando parte del tratamiento se ejecuta a través de terceros.

5.3.2. Encargado del tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento. Esta figura actúa bajo la autoridad y las instrucciones del responsable, sin poder utilizar los datos para fines propios ni adoptar decisiones sobre el tratamiento más allá de los aspectos técnicos u organizativos que el responsable le haya delegado expresamente.

Las principales características del encargado son:

- **Actuación por cuenta ajena:** El encargado trata datos para satisfacer las finalidades determinadas por el responsable, no las suyas propias.
- **Sujeción a instrucciones:** El encargado debe seguir las instrucciones documentadas por el responsable respecto al tratamiento.
- **Autonomía técnica limitada:** Puede adoptar decisiones sobre aspectos técnicos del tratamiento pero no sobre los fines ni los medios.

5.3.3. Corresponsable del tratamiento

La figura del corresponsable del tratamiento puede surgir cuando dos o más responsables determinan conjuntamente los fines y medios del tratamiento. Esta figura representa la realidad de que en numerosos escenarios, las decisiones sobre el tratamiento no son adoptadas unilateralmente por 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

única entidad, sino que resultan convergencia de decisiones de dos o más entidades que colaboran para alcanzar objetivos compartidos o complementarios. La corresponsabilidad no exige que todos los corresponsables participen en igual medida en la determinación de fines y medios, siendo suficiente que cada uno de ellos tenga una influencia real sobre alguno de estos elementos para se considere como una situación de responsabilidad conjunta.

Las siguientes características que definen la corresponsabilidad:

- **Pluralidad de responsables:** Intervienen dos o más entidades que ostentan cada una la condición de responsable, no existiendo relación de subordinación entre ellas.
- **Determinación conjunta:** Los corresponsables participan en la definición de los fines, los medios o ambos elementos del tratamiento, aunque no necesariamente en la misma proporción o intensidad.
- **Finalidades convergentes o complementarias:** Los corresponsables pueden perseguir un mismo fin compartido o fines diferentes pero interconectados que requieren un tratamiento conjunto.
- **Autonomía decisoria de cada parte:** Cada corresponsable mantiene capacidad de decisión propia, diferenciándose así de la relación responsable-encargado donde este último actúa bajo instrucciones.

5.3.4. Identificación de roles

La distinción entre el responsable, encargado y corresponsable no siempre resulta evidente en la práctica, especialmente en ecosistemas IoMT donde múltiples actores interactúan en las diferentes fases del ciclo de vida.

Por este motivo, la identificación de estos roles debe basarse en un análisis funcional de la realidad del tratamiento, más allá de las definiciones regulatorias o de las denominaciones contractuales que las partes hayan podido adoptar.

A continuación, se describen los criterios operativos que permiten determinar cada rol en la práctica:

❖ **Identificación del responsable de tratamiento**

El responsable del tratamiento:

- Decide qué datos personales se recogen y con qué finalidad.
- Determina la base jurídica que legitima el tratamiento.
- Establece los plazos de conservación y las normas de acceso a los datos.
- Decide con quién se comparten los datos o quién puede acceder a ellos.
- Tiene obligación legal o interés propio en el tratamiento.
- Mantiene una relación directa con las partes interesadas cuyos datos se tratan.
- Ejercita control efectivo sobre el tratamiento, incluso si operaciones concretas se delegan en terceros.

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

En el ámbito sanitario, este rol suele corresponder a un hospital, un centro de salud, una clínica privada, un servicio regional de salud o un centro de investigación, entre otros.

❖ **Identificación del encargado de tratamiento**

El encargado del tratamiento:

- Actúa siguiendo instrucciones documentadas del responsable.
- No determina la finalidad del tratamiento, sino que ejecuta operaciones técnicas o de soporte.
- No persigue intereses propios con los datos más allá del servicio contratado.
- No mantiene relación directa con las partes interesadas respecto del tratamiento.
- Opera dentro del marco limitado y definido por un contrato de encargo de tratamiento.
- No puede reutilizar los datos para fines propios sin autorización expresa.
- Debe devolver o destruir los datos una vez finalizada su relación con el responsable.

En el ecosistema IoMT, este rol puede asignarse a un proveedor de una plataforma en la nube, una empresa de mantenimiento remoto de dispositivos, un integrador o un tercero que presta servicios de analítica.

❖ **Identificación de corresponsabilidad**

Existe corresponsabilidad cuando:

- Varias entidades determinan conjuntamente la finalidad del tratamiento.
- Las decisiones esenciales requieren la participación o acuerdo de múltiples partes.
- Cada entidad tiene capacidad real de influir en las decisiones clave del tratamiento.
- Las partes persiguen finalidades comunes, complementarias o mutuamente dependientes.
- El tratamiento no existiría o sería sustancialmente diferente sin la intervención conjunta de cada actor.
- Ninguna de las entidades actúa como subordinada de otra, sino que tiene autonomía para tomar decisiones.

Esta situación, dentro del entorno IoMT, puede darse cuando un centro sanitario y un proveedor colaboran para desarrollar un algoritmo u otras asociaciones entre entidades del sector salud y proveedor para gestionar o lanzar nuevas soluciones.

5.3.5. Fabricante de dispositivos IoMT

Aunque los fabricantes de dispositivos IoMT no encajan dentro de las categorías clásicas del tratamiento de datos, su papel resulta determinante para garantizar la privacidad y la seguridad del tratamiento. Su posición jurídica concreta depende del modelo de negocio, de las funcionalidades del dispositivo, y del grado de participación que tengan en el tratamiento de los datos generados por el propio equipo.

En la práctica, estos actores pueden situarse en diferentes posiciones, como simples terceros sin acceso a datos, como encargados cuando prestan servicios asociados al dispositivo, o incluso como corresponsables cuando determinan conjuntamente finalidades o medios del tratamiento. Por ello, su

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

intervención debe evaluarse desde una perspectiva funcional, atendiendo a qué decisiones adoptan realmente respecto al tratamiento de los datos y no únicamente a las descripciones contractuales.

Además, los fabricantes influyen directamente en aspectos estructurales del tratamiento, como la arquitectura de seguridad, la gestión del ciclo de vida, las actualizaciones de seguridad o la configuración por defecto, que condicionan la capacidad de los responsables sanitarios para cumplir sus obligaciones legales.

En consecuencia, para una adecuada gestión de la privacidad en entornos IoMT requiere de un modelo de colaboración que garantice que las responsabilidades de cada actor queden claramente delimitadas y definidas.

5.4. Impacto de las brechas de datos

Las brechas de datos en ecosistemas IoMT tienen un impacto especialmente elevado, ya que afectan simultáneamente a información de salud altamente sensible y a sistemas que pueden influir directamente en la seguridad y bienestar de las personas pacientes. A diferencia de otros sectores, la naturaleza clínica de los datos y la dependencia operativa de los dispositivos conectados hacen que las consecuencias de un incidente no se limiten a la privacidad, sino que puedan extenderse a la continuidad asistencial, la confianza social y la responsabilidad regulatoria.

Evaluar correctamente el impacto de una brecha es esencial tanto para la gestión de riesgos como para cumplir con las obligaciones normativas. Esta evaluación debe considerar alteraciones en los derechos de las partes interesadas, impactos operativos y económicos, repercusiones reputacionales y circunstancias propias de los entornos IoMT, donde una brecha puede implicar riesgos clínicos, exposición prolongada o propagación hacia los sistemas sanitarios.

5.4.1. Dimensiones del impacto

Las principales dimensiones sobre las que pueden afectar las brechas de datos en entornos IoMT son las siguientes:

❖ **Derechos de las partes interesadas**

La exposición de datos de salud vulnera derechos fundamentales y puede causar daños duraderos difíciles de revertir.

- **Intimidad y dignidad:** La exposición de información sobre condiciones médicas, tratamientos, hábitos de salud o predisposiciones genéticas constituye una intromisión grave en el ámbito personal, causando daño moral que puede persistir indefinidamente.
- **No discriminación:** Los datos de salud filtrados pueden utilizarse para discriminar a los afectados en ámbitos laborales, financieros o sociales, con consecuencias que pueden prolongarse durante años.
- **Autodeterminación informática:** La pérdida de control sobre los propios datos de salud socava la capacidad del individuo para decidir qué información comparte y con quién, erosionando un derecho fundamental reconocido constitucionalmente.

❖ **Seguridad de la persona 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

Cuando el dispositivo actúa o soporta decisiones clínicas, una brecha puede afectar directamente a la integridad física.

- **Manipulación de dispositivos terapéuticos:** En dispositivos IoMT con capacidad de actuación, una brecha de seguridad puede permitir modificaciones en parámetros de tratamiento con consecuencias potencialmente críticas.
- **Alteración de información clínica:** La modificación de datos de diagnósticos, resultados de pruebas o historiales puede conducir a decisiones clínicas erróneas, tratamientos inadecuados o retrasos en intervenciones necesarias.
- **Denegación de servicio en dispositivos críticos:** La indisponibilidad de dispositivos de soporte vital o monitorización puede comprometer directamente la vida de las personas pacientes dependientes de estos sistemas.

❖ Interrupción asistencial

Los incidentes pueden forzar modos degradados o paradas parciales, con impacto directo en la atención.

- **Interrupción de servicios asistenciales:** Los ataques de ransomware y otros incidentes graves pueden forzar la suspensión de consultas, intervenciones quirúrgicas, pruebas diagnósticas y otros servicios, con derivación de las personas pacientes a otros centros y deterioro de la calidad asistencial.
- **Degradación de capacidades:** Incluso sin interrupción total, la necesidad de operar en modos degradados, desconectar sistemas o recurrir a procedimientos manuales reduce significativamente la eficiencia y capacidad de respuesta.
- **Pérdida de datos clínicos:** La destrucción o corrupción de información clínica puede afectar a la continuidad de tratamientos, obligar a repetir pruebas diagnósticas y dificultar la toma de decisiones clínicas informadas.
- **Desvío de recursos:** La respuesta al incidente requiere dedicación intensiva de personal técnico, clínico y directivo, desviando recursos de otras actividades y proyectos.

❖ Costes económicos

El efecto financiero combina costes directos, pérdidas de negocio y contingencias legales.

- **Costes directos de respuesta y recuperación:** Investigación forense, contratación de servicios especializados, restauración de sistemas, sustitución de equipos comprometidos y horas extras del personal.
- **Costes de notificación y atención a afectados:** Comunicaciones individualizadas, habilitación de canales de atención, servicios de protección de identidad cuando proceda.
- **Pérdida de ingresos:** Reducción de actividad asistencial durante el incidente y período de recuperación, cancelación de servicios programados, pérdida de personas pacientes que migran a otros proveedores.
- **Incremento de primas de seguro:** Revisión al alza de las condiciones de pólizas de ciberriesgo tras incidentes significativos.

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

❖ Daño reputacional

La pérdida de confianza impacta en la adopción tecnológica y en la relación con el entorno.

- **Pérdida de confianza de personas pacientes:** La percepción de que una organización no protege adecuadamente los datos de salud puede llevar a las personas pacientes a ocultar información relevante, rechazar el uso de tecnologías beneficiosas o cambiar de proveedor sanitario.
- **Deterioro de imagen institucional:** La cobertura mediática de brechas de datos, especialmente en el sector sanitario, tiende a ser intensa y prolongada, asociando permanentemente el nombre de la organización con el incidente.
- **Afectación a relaciones con terceros:** Socios comerciales, proveedores tecnológicos, aseguradoras y otras entidades pueden revisar sus relaciones con organizaciones que han sufrido brechas significativas.
- **Impacto en la captación de talento:** La reputación en materia de seguridad afecta la capacidad de atraer y retener profesionales cualificados, tanto clínicos como tecnológicos.

❖ Consecuencias regulatorias

Los marcos europeos y nacionales exigen diligencia, notificación y medidas correctivas.

- **Sanciones administrativas:** Las infracciones del RGPD pueden conllevar multas de hasta 20 millones de euros o el 4% del volumen de negocio.
- **Litigios y reclamaciones:** Demandas de personas pacientes afectadas, acciones colectivas, reclamaciones de responsabilidad patrimonial en el sector público.

5.4.2. Cuantificación del impacto

La cuantificación del impacto de las brechas de datos resulta esencial tanto para la priorización de las inversiones en seguridad como para el dimensionamiento del riesgo residual y el alineamiento con la Dirección. Aunque la naturaleza de algunos daños, particularmente los relativos a derechos fundamentales, dificultan su expresión en términos puramente económicos, existen metodologías y marcos de referencia que permiten una aproximación objetiva a la magnitud de los impactos potenciales.

Los componentes del coste a considerar son:

- **Componentes de coste directos:** Respuesta técnica y forense, restauración de sistemas, sustitución de equipos y horas extra, así como la notificación y atención a afectados.
- **Pérdida de negocio e ineficiencias:** Interrupciones y caída de la actividad operativa, cancelaciones, reprocesos y reducción de la productividad durante la recuperación.
- **Contingencias regulatorias y legales:** Multas y sanciones potenciales, según gravedad y diligencia, y litigios o reclamaciones de personas pacientes y terceros.
- **Métodos de valoración prácticos:** Por registros (nº de registros × coste unitario ajustado por sensibilidad), por componentes (suma de categorías de coste), por escenarios (bajo/medio/alto con probabilidades) y BIA (coste por hora/día de indisponibilidad).

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

5.4.3. Factores agravantes y atenuantes

La magnitud del impacto de una brecha de datos no depende únicamente del hecho de que se produzca, sino de un conjunto de factores que pueden incrementar o reducir significativamente sus consecuencias. La consideración de estos factores resulta relevante tanto para la evaluación previa del riesgo como para la valoración del impacto real una vez producido el incidente.

Los factores que se han identificado que agravan el impacto son:

- **Agravantes típicos:** Volumen elevado de datos, alta sensibilidad, colectivos vulnerables, exposición prolongada, exfiltración confirmada o publicación en la red, intencionalidad del ataque, negligencia previa o reincidencia.
- **Atenuantes efectivos:** Detección temprana y contención rápida, cifrado robusto y seudonimización, notificación proactiva y cooperación con autoridades, medidas de apoyo a afectados, historial de cumplimiento y mejoras implementadas tras el incidente.
- **Uso en la decisión de notificación:** La combinación de factores guía si el riesgo es improbable (no se notifica a las partes interesadas), probable (la autoridad de referencia en 72h y partes interesadas si hay alto riesgo) o muy probable (la autoridad de referencia en 72h y comunicación a las partes interesadas sin dilación).
- **Documentación mínima del análisis:** Naturaleza de la brecha, categorías y volumen de datos, tipos de partes interesadas, agravantes/atenuantes presentes, nivel de riesgo razonado, decisión de notificación y medidas de mitigación aplicadas.

5.4.4. Consideraciones para la evaluación de impacto

Los dispositivos IoMT presentan características singulares que deben considerarse específicamente al evaluar el impacto de brechas de datos, complementando el análisis general con factores propios de estos entornos.

- **Criticidad clínica y capacidad de actuación:** Dispositivos que sostienen tratamientos o modifican parámetros incorporan un riesgo directo para la seguridad de la persona paciente.
- **Granularidad y continuidad de los datos:** Los dispositivos IoMT que generan flujos continuos de datos fisiológicos crean perfiles detallados cuyo compromiso tiene mayor impacto que datos puntuales.
- **Dificultad de anonimización:** Los patrones fisiológicos capturados pueden constituir identificadores únicos, limitando la eficacia de técnicas de anonimización como factor atenuante.
- **Ciclo de vida y entorno de uso del dispositivo:** Dispositivos con largos periodos de implantación o que operan en entornos fuera del perímetro de seguridad de la organización sanitaria ventanas, provocan de exposición prolongadas ante vulnerabilidades.
- **Interconexión con sistemas clínicos:** El compromiso de un dispositivo IoMT puede propagarse a sistemas de información sanitaria o redes clínicas, amplificando el alcance e impacto del incidente.

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

6. Reglamento General de Protección de Datos

El Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (RGPD), constituye el marco normativo fundamental para la protección de los datos personales en la Unión Europea y es de aplicación directa desde mayo de 2018. Su objetivo principal consiste en garantizar un nivel homogéneo de protección de los derechos y libertades de las personas físicas, asegurando al mismo tiempo la libre circulación de datos dentro del mercado interior europeo.

En el ámbito del IoMT, la relevancia del RGPD se incrementa significativamente debido al carácter sensible de los datos tratados y a la naturaleza altamente distribuida y automatizada de los ecosistemas IoMT. Los dispositivos médicos conectados procesan grandes volúmenes de datos relativos a la salud, datos biométricos o, en algunos casos, datos genéticos. Estas categorías especiales de datos están sometidas a un régimen reforzado que exige la aplicación de salvaguardas adicionales durante todo el ciclo de vida del dispositivo, desde su diseño hasta su retirada.

Además, los ecosistemas IoMT suelen implicar múltiples actores, fabricantes, proveedores de infraestructura, desarrolladores de software, profesionales del sector salud y centros sanitarios, lo que intensifica las exigencias del RGPD en materia de responsabilidad, trazabilidad, gobernanza, seguridad y rendición de cuentas. El Reglamento se basa en el principio de que los responsables del tratamiento deben poder demostrar el cumplimiento normativo, lo que implica una gestión de los riesgos, una documentación exhaustiva e implementación de controles operativos. En un entorno donde confluyen interoperabilidad clínica, monitorización remota, conectividad permanente y actualización continua, esta obligación adopta una gran complejidad.

El RGPD identifica expresamente que los tratamientos susceptibles de ocasionar daños físicos, materiales o inmateriales requieren un tratamiento reforzado. Entre ellos destacan, de forma explícita, los que involucran datos de salud, evaluaciones médicas, monitorización continua de personas pacientes y tratamientos de datos a gran escala, todos ellos presentes en la operativa diaria de los ecosistemas IoMT.

A partir de estas premisas, los requisitos centrales del RGPD que afectan a los ecosistemas IoMT pueden estructurarse del siguiente modo.

6.1. Bases de licitud y principios de tratamiento

La licitud del tratamiento en entornos IoMT exige analizar, por un lado, las bases jurídicas previstas en el artículo 6 del RGPD y, por otro, las excepciones del artículo 9 relativas a categorías especiales, dado que los datos de salud forman parte de estas. La elección de la base adecuada depende de la finalidad concreta y del rol de cada actor dentro del ecosistema IoMT.

Entre las excepciones más relevantes para el tratamiento de datos de salud se encuentran:

- Prestación de asistencia sanitaria, diagnóstico o seguimiento médico en el marco de un contrato con un profesional o institución sanitaria.
- Interés público en el ámbito de la salud pública, especialmente cuando se trate de sistemas de vigilancia epidemiológica o contención de amenazas sanitarias.

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

- Consentimiento explícito de la persona paciente, aplicable únicamente cuando no concurran otras excepciones y siempre que se realice con garantías.

Además de contar con una base de licitud válida, el RGPD exige que todos los tratamientos respeten los principios del artículo 5, que en IoMT adquieren una relevancia particular debido a la naturaleza sensible y continua del flujo de datos. Entre ellos destacan:

- Protección de datos desde el diseño y por defecto, lo que implica integrar medidas técnicas y organizativas desde la concepción del dispositivo.
- Minimización y limitación de la finalidad, asegurando que los dispositivos y plataformas procesan únicamente aquellos datos imprescindibles para la finalidad clínica o funcional definida, sin reutilizarlos posteriormente para fines incompatibles.
- Exactitud y actualización, especialmente crítica cuando los datos influyen en decisiones diagnósticas o en la monitorización del estado de la persona paciente. Los sistemas IoMT deben integrar mecanismos que garanticen la fiabilidad de las mediciones, la detección de valores anómalos y, cuando corresponda, la reconciliación con la historia clínica.

En conjunto, las bases jurídicas y los principios de tratamiento constituyen el marco que permite valorar si un tratamiento dentro del ecosistema IoMT es adecuado y conforme al RGPD.

6.2. Evaluación y gestión del riesgo

Debido al alto nivel de riesgo inherente a los ecosistemas IoMT, el RGPD exige la adopción de mecanismos de análisis, mitigación y supervisión que permitan garantizar que los tratamientos de datos personales, especialmente los relativos a la salud, se gestionan de forma segura y conforme a los principios del Reglamento.

A continuación se describen los principales elementos que deben considerarse:

❖ Evaluaciones de Impacto en Protección de Datos (EIPD)

Las EIPD constituyen una herramienta esencial en IoMT, ya que permiten analizar de forma estructurada los riesgos que pueden derivarse del tratamiento de datos sanitarios mediante dispositivos conectados. En este tipo de entornos, la realización de una EIPD no es solo recomendable, sino obligatoria, debido a factores como:

- Tratamiento de grandes volúmenes de datos sanitarios, que por su naturaleza son especialmente sensibles.
- Empleo de nuevas tecnologías.
- Monitorización continua de las personas pacientes.

Una EIPD debe identificar los riesgos específicos del tratamiento, analizar su probabilidad e impacto, determinar las medidas de mitigación adecuadas y documentar la justificación de los controles implantados. En IoMT esto incluye la evaluación de la seguridad del dispositivo, su firmware, las comunicaciones, las plataformas cloud asociadas y la cadena de suministro.

❖ Medidas de seguridad técnicas y organizativas

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

El artículo 32 del RGPD establece la obligación de aplicar medidas de seguridad apropiadas en función del nivel de riesgo. En entornos IoMT, esta obligación se intensifica debido a la sensibilidad de los datos y a la potencial incidencia en la salud de la persona paciente.

Las medidas más relevantes incluyen:

- Cifrado y seudonimización, tanto en las comunicaciones entre el dispositivo y las plataformas como en la información almacenada.
- Garantía de confidencialidad, integridad, disponibilidad y resiliencia, asegurando que los datos no sean alterados ni accesibles por terceros no autorizados y que los dispositivos puedan operar con normalidad en condiciones adversas.
- Capacidad de restauración de la disponibilidad, permitiendo recuperar datos y volver a operaciones normales en caso de incidentes, fallos del dispositivo o interrupciones del servicio.
- Procesos periódicos de verificación, auditoría y evaluación, que permitan comprobar la eficacia de los controles implantados y detectar vulnerabilidades emergentes propias del ciclo de vida IoMT.

Estas medidas deben integrarse desde el diseño del dispositivo y mantenerse actualizadas mediante una gestión adecuada de parches y actualizaciones.

❖ Registro de Actividades de Tratamiento

En IoMT resulta imprescindible mantener un registro exhaustivo y actualizado de los tratamientos realizados. Este registro debe reflejar con precisión todas las operaciones relevantes, permitiendo asegurar la trazabilidad y el cumplimiento del principio de responsabilidad proactiva.

De forma específica debe documentarse:

- Las finalidades del tratamiento, diferenciando claramente los usos clínicos, operativos y técnicos.
- Las categorías de datos tratados, destacando la presencia de datos de salud, biométricos o metadatos generados por los dispositivos.
- Los plazos de conservación, distinguiendo entre información clínica, logs técnicos, métricas de funcionamiento o datos administrativos.
- Los flujos entre dispositivos, plataformas y actores, incluyendo conexiones, integraciones con sistemas sanitarios y servicios en la nube.
- Las medidas de seguridad aplicadas y los responsables de cada fase, especialmente cuando intervienen múltiples proveedores tecnológicos.

Este registro es fundamental para asegurar la trazabilidad del ciclo de vida del dato y para demostrar la existencia de controles adecuados en entornos complejos y distribuidos como IoMT.

6.3. Relaciones con terceros

Los ecosistemas IoMT operan sobre una arquitectura distribuida en la que intervienen múltiples actores, como fabricantes, proveedores de servicios cloud, desarrolladores de software, empresas 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

mantenimiento y centros sanitarios, lo que exige un control exhaustivo de las relaciones con terceros. El RGPD establece un marco preciso para gestionar estas interacciones, asegurando que cada actor actúe conforme a las instrucciones y responsabilidades que le corresponden en el tratamiento de datos personales.

❖ Gestión de encargados de tratamiento

Los terceros que tratan datos personales por cuenta del responsable deben actuar como encargados del tratamiento conforme al artículo 28 del RGPD.

Para ello, la relación debe formalizarse mediante un contrato o acuerdo que incluya, al menos, los siguientes elementos:

- Instrucciones documentadas del responsable, que definan de manera clara los tratamientos permitidos, las finalidades y las limitaciones de uso de los datos.
- Obligaciones de seguridad y cumplimiento del RGPD, garantizando que el encargado aplica medidas técnicas y organizativas adecuadas al nivel de riesgo inherente al IoMT.
- Restricciones y control de la subcontratación, de forma que el encargado solo pueda recurrir a subencargados con autorización previa y expresa del responsable.
- Protocolos de auditoría y supervisión, que permitan verificar periódicamente la correcta ejecución de las obligaciones contractuales.
- Mecanismos de gestión de incidentes, estableciendo tiempos de notificación, canales de comunicación y responsabilidades en caso de brechas de seguridad o fallos de servicio.

❖ Régimen de subencargados

Los encargados pueden recurrir a terceros para ejecutar parte de los servicios, pero únicamente cuando cuenten con la autorización previa del responsable. En estos casos, el subencargado debe quedar jurídicamente sometido a las mismas obligaciones que el encargado principal, garantizando así que toda la cadena de suministro respeta los estándares exigidos por el RGPD.

❖ Transferencias internacionales

Cuando los datos tratados por soluciones IoMT se almacenan, procesan o acceden desde fuera del Espacio Económico Europeo, como puede darse en caso de usar plataformas cloud, es necesario aplicar las salvaguardas previstas por el RGPD para garantizar un nivel adecuado de protección.

Las principales alternativas incluyen:

- Cláusulas Contractuales Tipo (SCC) aprobadas por la Comisión Europea, que establecen obligaciones mínimas para exportadores e importadores de datos.
- Decisiones de adecuación, aplicables cuando la Comisión reconoce que un país ofrece garantías comparables a las europeas.
- Medidas adicionales cuando las salvaguardas estándar no son suficientes debido a la normativa del país de destino.

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

6.4. Derechos de las partes interesadas

En los entornos IoMT, el ejercicio de los derechos reconocidos por el RGPD debe integrarse tanto en la arquitectura técnica de los dispositivos como en la organización de los servicios asociados. La naturaleza continua, automatizada y distribuida del tratamiento obliga a diseñar mecanismos que permitan ejercer los derechos de las personas pacientes de manera efectiva, sin comprometer la seguridad clínica ni la continuidad asistencial.

Para ello, los dispositivos, plataformas y servicios IoT sanitarios deben incorporar funcionalidades específicas que permitan:

- Acceso estructurado a los datos, proporcionando a la parte interesada una visión clara de la información recopilada, su procedencia, las finalidades y los actores que intervienen. Este acceso debe ser comprensible, exportable y compatible con estándares sanitarios.
- Rectificación inmediata de datos inexactos, especialmente aquellos que influyen en diagnósticos o parámetros clínicos. Los sistemas deben prever mecanismos para corregir errores de medición, anotaciones incorrectas o discrepancias con la historia clínica.
- Supresión y limitación del tratamiento, cuando sean aplicables, equilibrando este derecho con la obligación de garantizar la continuidad asistencial y los requisitos legales de conservación de datos sanitarios. La supresión no debe comprometer la trazabilidad necesaria para la seguridad del dispositivo ni para la atención clínica.
- Oposición fundada.
- Portabilidad técnica, facilitando la transferencia de datos a otros profesionales o sistemas sanitarios mediante formatos interoperables y estandarizados, garantizando la integridad de la información.

❖ Transparencia

La transparencia constituye un elemento esencial en IoMT, debido a la complejidad de los flujos de datos y al elevado número de actores implicados. La información debe proporcionarse de manera clara, accesible y comprensible, explicando:

- Qué actores intervienen en el tratamiento, incluyendo fabricantes, proveedores cloud, desarrolladores y entidades sanitarias.
- Dónde y cómo se almacenan los datos, especificando ubicaciones, servicios cloud utilizados y, en su caso, transferencias internacionales.
- Qué decisiones automatizadas existen, especialmente cuando el dispositivo genera alertas, clasifica riesgos clínicos o activas actuaciones automáticas.
- Qué perfiles o modelos predictivos se generan, indicando su finalidad, su impacto potencial y los criterios utilizados.

❖ Decisiones automatizadas

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

Cuando los sistemas IoMT incluyen procesamientos automatizados que puedan producir efectos significativos en la persona paciente, como la evaluación del riesgo clínico, la detección automática de anomalías, la priorización de alertas o el uso de modelos de IA para apoyar decisiones médicas, deben implementarse salvaguardas reforzadas. Estas incluyen:

- Supervisión humana, con capacidad real para revisar, modificar o revertir la decisión automatizada.
- Posibilidad de expresar el punto de vista de la parte interesada, especialmente cuando las conclusiones automatizadas puedan ser cuestionables o estar afectadas por datos incorrectos.
- Derecho a impugnar la decisión, solicitando una revisión humana o la aplicación de criterios médicos adicionales.

6.5. Gestión y notificación de brechas de seguridad

La interconexión de dispositivos IoMT, servicios cloud, plataformas de análisis y redes hospitalarias aumenta de forma significativa la probabilidad e impacto de incidentes de seguridad. En este contexto, el RGPD establece obligaciones estrictas para la gestión, documentación y notificación de brechas que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos personales. La respuesta ante una brecha debe ser rápida, coordinada y documentada, ya que en entornos sanitarios un incidente puede tener tanto consecuencias sobre la privacidad como sobre la seguridad de la persona paciente.

❖ Notificación a la autoridad de control

Cuando se produce una brecha de seguridad que pueda suponer un riesgo para los derechos y libertades de las personas, el responsable del tratamiento está obligado a notificarla a la autoridad de control competente en un plazo máximo de 72 horas desde que tenga conocimiento de ella.

En España, con carácter general, dicha notificación debe realizarse ante la Agencia Española de Protección de Datos (AEPD). No obstante, en el ámbito de la administración pública de algunas comunidades autónomas, como Andalucía, Cataluña o País Vasco, la competencia corresponde a sus respectivas autoridades autonómicas de protección de datos, como la Autoridad Catalana de Protección de Datos (APDCAT), el Consejo de Transparencia y Protección de Datos de Andalucía o la Autoridad Vasca de Protección de Datos.

La notificación debe incluir, como mínimo:

- La naturaleza de la brecha, describiendo si afecta a la confidencialidad (acceso no autorizado), integridad (alteración de datos), disponibilidad (pérdida de acceso) o a varias simultáneamente.
- Las categorías y número aproximado de partes interesadas afectadas, especialmente crítico tratándose de datos de salud.
- Las posibles consecuencias o impactos previstos, tanto de privacidad como, cuando proceda, clínicos u operativos.
- Las medidas adoptadas o previstas para mitigar los efectos.

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

❖ Comunicación a las partes interesadas

Cuando la brecha suponga un alto riesgo para los derechos y libertades de las personas, el responsable deberá comunicarla sin dilación indebida a los afectados. Esta comunicación debe ser directa, clara y comprensible, evitando lenguaje técnico excesivo.

En entornos IoMT, esta obligación es especialmente relevante cuando la brecha pueda afectar a datos clínicos altamente sensibles, parámetros biométricos o alertas relacionadas con el estado de salud de la persona paciente.

❖ Documentación interna

Independientemente de si se notifica o no a la autoridad o a las partes interesadas, el responsable está obligado a documentar internamente todas las brechas de seguridad, incluyendo:

- Los hechos que la originaron, ya sean vulnerabilidades de firmware, ataques externos, errores de configuración, fallos de software o accesos no autorizados.
- El impacto real y potencial, evaluando la exposición de datos, las afectaciones a la atención sanitaria y la propagación en la cadena de suministro.
- Las medidas correctivas y preventivas adoptadas, tanto inmediatas como a medio plazo, incluyendo parches, actualizaciones, mejoras en la arquitectura de seguridad o revisión de protocolos operativo.

6.6. Infracciones y sanciones

El RGPD establece un régimen sancionador especialmente estricto en aquellos tratamientos que involucran categorías especiales de datos, como los datos de salud procesados en ecosistemas IoMT. Debido al impacto potencial que un tratamiento ilícito puede tener sobre la privacidad, la seguridad y la propia atención sanitaria de la persona paciente, el incumplimiento de las obligaciones del Reglamento puede dar lugar a sanciones económicas significativas, así como a responsabilidades civiles adicionales.

❖ Sanciones

El RGPD prevé un sistema de multas administrativas graduado en función de la gravedad de la infracción.

Para las infracciones más serias, entre ellas, el tratamiento ilícito de datos de salud, el incumplimiento de los derechos de las partes interesadas o la falta de medidas de seguridad adecuadas, las sanciones pueden alcanzar los 20 millones de euros o el 4% del volumen de negocio.

❖ Criterios de graduación

Las autoridades de control no aplican las sanciones de manera automática. Para determinar la cuantía concreta, evalúan distintos factores relacionados con la infracción y con la conducta del responsable o encargado. Entre los más relevantes se incluyen:

- Naturaleza, gravedad y duración de la infracción, analizando si afecta a datos sanitarios o si compromete la seguridad de la persona 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

- Intencionalidad o negligencia, distinguiendo entre fallos accidentales y comportamientos claramente descuidados o temerarios.
- Daños causados y medidas correctoras, valorando si el responsable actuó diligentemente para mitigar el impacto.
- Grado de cooperación con la autoridad de control, especialmente en incidentes IoMT donde se requiere coordinación con proveedores.
- Categorías de datos afectadas, siendo los datos de salud, biométricos o genéticos los que comportan mayor severidad en la graduación.

❖ **Responsabilidad civil e indemnización**

Además de las sanciones administrativas, el RGPD reconoce a las partes interesadas el derecho a ser indemnizados por los daños y perjuicios, tanto materiales como inmateriales, que hayan sufrido como consecuencia de una infracción del Reglamento.

Esto incluye tanto daños como perjuicios morales, afectación a la reputación, estrés, ansiedad o consecuencias derivadas de un uso indebido de datos clínicos.

7. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), es la norma que adapta el RGPD al ordenamiento jurídico español. Su objetivo es garantizar el derecho fundamental a la protección de datos personales, reconocido en el artículo 18.4 de la Constitución Española, que de forma pionera dispuso que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". En el contexto sanitario y, en particular, en ecosistemas IoMT, esta posición se traduce en exigencias adicionales en materia de licitud, gobernanza, seguridad y ejercicio de derechos, por la sensibilidad de los datos y la multiplicidad de actores que intervienen en el ciclo de vida del dispositivo y de la plataforma

La LOPDGDD desarrolla aspectos que el RGPD dejó a la determinación de los Estados miembros, estableciendo precisiones sobre el consentimiento de menores, el tratamiento de datos de personas fallecidas, el régimen de categorías especiales, y obligaciones específicas para determinados sectores y tratamientos. Para el ámbito sanitario, la Ley introduce disposiciones particulares que afectan directamente a los tratamientos realizados mediante dispositivos IoMT, incluyendo requisitos reforzados para el tratamiento de datos de salud con fines de interés público y condiciones específicas para la investigación biomédica.

Los requisitos fundamentales del LOPDGDD para ecosistemas IoMT son:

7.1. Disposiciones específicas para el ámbito sanitario

En el sector sanitario español, la LOPDGDD concreta aspectos clave que condicionan la base de licitud, la gobernanza y la supervisión de los tratamientos con datos de salud. En IoMT, estas reglas determinan

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

cómo justificar legalmente el tratamiento, qué figuras organizativas deben existir y cómo gestionar el consentimiento cuando intervienen menores.

- **Tratamiento de datos de salud por interés público**

La Disposición adicional decimoséptima establece que el tratamiento de datos de salud por razones de interés público debe estar respaldado por una norma con rango de ley. Esta previsión incluye tratamientos vinculados a la investigación biomédica, la evaluación y mejora de sistemas sanitarios, la vigilancia epidemiológica o el uso secundario de datos con fines de investigación o planificación.

En entornos IoMT, donde los dispositivos generan datos clínicos en tiempo real y se integran de forma directa con sistemas públicos de salud, esta exigencia condiciona las bases de licitud disponibles, obligando a identificar correctamente la cobertura legal y a documentar las salvaguardas aplicables para cada tipo de tratamiento.

- **Designación obligatoria del Delegado de Protección de Datos:**

El artículo 34 obliga a designar un Delegado de Protección de Datos (DPD) a los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de las personas pacientes, exceptuando únicamente a profesionales que ejerzan a título individual.

En la práctica, esto implica que cualquier entidad sanitaria que opere dispositivos IoMT, como hospitales, clínicas, laboratorios, unidades asistenciales o redes de telemedicina, debe contar con un DPD. Esta figura resulta esencial para supervisar la adecuación normativa de los tratamientos IoMT, incluyendo la revisión de Evaluaciones de Impacto, la gestión de proveedores tecnológicos, la aplicación de medidas de seguridad, la respuesta ante incidentes y la verificación del cumplimiento continuo.

- **Consentimiento de menores:**

La LOPDGDD fija en 14 años la edad a partir de la cual los menores pueden prestar consentimiento para el tratamiento de sus datos, aspecto especialmente relevante para dispositivos IoMT de monitorización pediátrica donde debe determinarse si el consentimiento corresponde al menor o a sus representantes legales.

7.2. Garantías y mecanismos de protección

La LOPDGDD complementa el RGPD con mecanismos operativos que ayudan a equilibrar el cumplimiento legal con la continuidad asistencial y la trazabilidad técnica propia de IoMT. Destacan el bloqueo de datos, el deber de confidencialidad reforzado y los derechos digitales, que refuerzan la protección en entornos conectados y 24/7.

- **Bloqueo de datos**

El artículo 32 regula el bloqueo de datos como alternativa a la supresión cuando exista una obligación legal que impida el borrado inmediato. Bajo este mecanismo, los datos deben identificarse y reservarse, quedando inaccesibles para cualquier uso operativo y disponibles únicamente para atender responsabilidades judiciales, administrativas o de auditoría.

- **Deber de confidencialidad reforzado**

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

La obligación de secreto se extiende a todas las personas que intervengan en cualquier fase del tratamiento de datos personales, con la particularidad de que debe mantenerse incluso tras finalizar la relación con el responsable o encargado, aspecto crítico en entornos IoMT donde personal técnico de mantenimiento, fabricantes y proveedores acceden a datos sensibles.

❖ Derechos digitales

El Título X de la LOPDGDD incorpora derechos vinculados al entorno digital, que resultan especialmente relevantes en sistemas IoMT debido a su funcionamiento constante, automatizado y altamente conectado. Entre los más significativos destacan:

- Derecho a la desconexión digital del personal sanitario, evitando que la utilización de sistemas conectados o alertas IoMT suponga disponibilidad permanente fuera de turnos o tiempos de descanso.
- Garantías frente a decisiones automatizadas, aplicable cuando dispositivos IoMT o sistemas asociados generan perfiles clínicos, estratifican riesgos, emiten alertas o ejecutan recomendaciones basadas en algoritmos. En estos casos deben habilitarse mecanismos para ofrecer explicaciones, intervención humana y la posibilidad de impugnación.
- Derecho a la educación y capacitación digital, que sirve de base para programas de formación en ciberseguridad, privacidad y uso seguro de dispositivos conectados, especialmente para personal asistencial que interactúa con sistemas IoMT.

7.3. Régimen sancionador

El régimen sancionador español tipifica con mayor detalle las infracciones que el RGPD y fija agravantes vinculados a la sensibilidad de los datos y a la vulnerabilidad de los colectivos afectados. En IoMT, donde se tratan datos sanitarios y la cadena de suministro es compleja, esta tipificación y los agravantes son especialmente relevantes.

❖ Clasificación de infracciones

Las infracciones se clasifican en muy graves, graves y leves, conforme a los artículos 72 a 74 de la LOPDGDD.

Entre las infracciones muy graves se incluyen:

- El tratamiento de datos personales vulnerando los principios del artículo 5 del RGPD.
- El tratamiento de categorías especiales sin una base jurídica válida.
- La ausencia de información a la parte interesada sobre el tratamiento.
- La desatención reiterada del ejercicio de derechos.

En el ámbito IoMT, estos supuestos pueden producirse con mayor facilidad si no existe una trazabilidad adecuada de los flujos de datos, si los consentimientos no están correctamente documentados o si los dispositivos generan información sin una base legal claramente identificada.

❖ Especial consideración a datos sensibles y colectivos vulnerables

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

La LOPDGDD establece que la naturaleza de los datos tratados y la condición de los afectados son criterios esenciales para graduar la sanción.

En particular, se agrava la infracción cuando afecta a:

- Categorías especiales de datos, como datos de salud, biométricos o genéticos.
- Menores de edad.
- Personas pacientes o personas en situación de dependencia.
- Colectivos en situación de especial vulnerabilidad clínica o social.

❖ Régimen diferenciado para Administraciones Públicas

Las entidades incluidas en el artículo 77.1, entre ellas las Administraciones Públicas sanitarias que operan dispositivos IoMT en el marco del Sistema Nacional de Salud, quedan sujetas a un régimen específico que excluye las sanciones económicas, pero mantiene las potestades correctivas, la notificación de las resoluciones y la posibilidad de proponer actuaciones disciplinarias sobre los responsables.

8. Marco Normativo Complementario

Más allá del marco regulatorio principal aplicable a la protección de datos aplicable a los dispositivos sanitarios, existe un conjunto de reglamentos, directrices y estándares técnicos que resultan esenciales para garantizar un nivel adecuado de seguridad y gobernanza en entornos IoMT. Estos marcos aportan criterios prácticos, controles específicos y metodologías reconocidas que permiten aterrizar los requisitos legales en medidas concretas y asegurar la privacidad de la información clínica.

Normativa	Ámbito	Descripción	Fecha
MDR	Dispositivos médicos	Regulación sobre la comercialización y puesta en marcha de dispositivos médicos	2017
IVDR	Dispositivos de diagnóstico in vitro	Regulación sobre la comercialización y puesta en marcha de dispositivos de diagnóstico in vitro	2017
NIS2	Ciberseguridad	Directiva que establece obligaciones de ciberseguridad para sectores esenciales, incluido el sanitario	2022
Ley 41/2002	Derechos de la persona paciente / Historia clínica	Ley española que regula los derechos de la persona paciente y la gestión de la información clínica	2002
ENS	Ciberseguridad	Marco de seguridad obligatorio para entidades públicas	2022

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

Normativa	Ámbito	Descripción	Fecha
Data Act	Acceso y portabilidad de datos	Reglamento que garantiza el acceso y uso de los datos generados por productos conectados	2023
EHDS	Datos de Salud	Marco europeo para el acceso, intercambio y reutilización de datos sanitarios electrónicos	2025
ISO/IEC 27001	Seguridad de la información	Estándar internacional de gestión de la seguridad de la información (SGSI)	2019
ISO/IEC 27701	Privacidad	Extensión de 27001 para la gestión de la privacidad y los datos personales	2025
ISO/IEC 27799	Seguridad en salud	Directrices específicas para la implementación de controles de seguridad en el sector sanitario	2016
Directrices MDCG	Productos sanitarios	Orientaciones para aplicar MDR e IVDR en dispositivos y software sanitario	2019 - 2021
Directrices ENISA	Ciberseguridad	Recomendaciones de ciberseguridad para el sector salud	2016 - 2020

TABLA 7 7: MARCO Y ESTÁNDARES DE REFERENCIA.

8.1. Reglamento de Productos Sanitarios (MDR)

El Reglamento (UE) 2017/745, conocido como MDR, constituye el marco regulatorio principal para la introducción en el mercado y puesta en servicio de productos sanitarios en la Unión Europea, siendo plenamente aplicable desde el año 2021. Un aspecto esencial del MDR es el reconocimiento expreso de que los programas informáticos constituyen productos sanitarios cuando están destinados a finalidades médicas, lo que sitúa a la práctica totalidad del software de dispositivos IoMT y las aplicaciones de salud conectadas dentro de su ámbito de aplicación.

El MDR establece un sistema de clasificación basado en el riesgo con cuatro clases (I, IIa, IIb y III). Esta clasificación determina el rigor del procedimiento de evaluación de conformidad, el nivel de supervisión por parte de los organismos notificados y, de forma indirecta, los requisitos de ciberseguridad, protección de datos y gestión de riesgos asociados al dispositivo IoMT.

En materia de protección de datos, el MDR integra la seguridad de la información como requisito esencial de seguridad del producto. El Anexo I establece que los fabricantes deben diseñar productos que protejan los datos personales almacenados, mencionando expresamente el cifrado y el control de acceso como medidas requeridas, y obliga a desarrollar los productos conforme a la gestión de riesgos.

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

El Reglamento impone además medidas de vigilancia postcomercialización que implican necesariamente el tratamiento de datos potencialmente identificativos de personas pacientes, generando una conexión directa con las obligaciones del RGPD.

Los principales requisitos del MDR en materia de privacidad y protección de datos:

- **Seguridad de datos personales desde el diseño:** Los productos deben prever la protección de los datos personales almacenados, incorporando cifrado, control de acceso y medidas contra accesos no autorizados y manipulaciones como parte de los requisitos esenciales de seguridad.
- **Gestión de riesgos integrada:** La seguridad de la información debe formar parte del proceso general de gestión de riesgos del producto conforme a la norma ISO 14971, evaluando amenazas de ciberseguridad con el mismo rigor que otros riesgos para la seguridad de la persona paciente.
- **Requisitos de infraestructura y entorno:** Los fabricantes deben definir y comunicar los requisitos mínimos de hardware, red y medidas de seguridad informática necesarios para que el producto opere de forma segura en su entorno previsto.
- **Vigilancia postcomercialización y protección de datos:** Los sistemas obligatorios de vigilancia y notificación de incidentes implican tratamientos de datos que deben realizarse conforme al RGPD, garantizando la protección de la información de personas pacientes durante el seguimiento del producto.
- **Documentación técnica y trazabilidad:** La documentación técnica completa y la asignación de identificadores únicos (UDI) deben conciliarse con los principios de minimización y proporcionalidad en el tratamiento de datos personales.

8.2. Reglamento de Productos Sanitarios para Diagnóstico In Vitro (IVDR)

El Reglamento (UE) 2017/746, conocido como IVDR, establece el marco regulatorio específico para productos destinados al diagnóstico in vitro de muestras procedentes del cuerpo humano. Aunque estos productos no implican contacto directo con de la persona paciente, muchos forman parte integral de ecosistemas IoMT, como analizadores de laboratorio conectados, sistemas de diagnóstico en el punto de atención, dispositivos de autodiagnóstico con conectividad a aplicaciones móviles y plataformas de secuenciación genética interoperables. Un aspecto diferenciador del IVDR es su especial relevancia para la medicina personalizada, dado que las pruebas diagnósticas para selección terapéutica y las pruebas genéticas implican frecuentemente el tratamiento de datos genéticos, categoría especial bajo el RGPD que exige salvaguardas reforzadas.

El IVDR comparte con el MDR el enfoque de integrar la seguridad de la información como requisito esencial, pero añade consideraciones específicas para productos de autodiagnóstico conectados, exigiendo que las obligaciones de seguridad se extiendan expresamente a la protección de las comunicaciones y los datos personales transmitidos a profesionales sanitarios. Su sistema de clasificación (clases A, B, C y D) somete a los requisitos más estrictos a los productos de clase C (pruebas genéticas, pruebas de selección terapéutica) y clase D (detección de agentes transmisibles, determinación de grupos sanguíneos), con implicaciones directas sobre el rigor de la evaluación de las medidas de protección de datos implementadas.

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

Los principales requisitos del IVDR en materia de privacidad y protección de datos:

- **Protección de datos personales almacenados:** Obligación de garantizar la seguridad de los datos almacenados en el producto, incluyendo explícitamente cifrado y control de acceso, con especial atención a datos genéticos y resultados diagnósticos sensibles.
- **Seguridad informática conforme al estado de la técnica:** El apartado 16.4 del Anexo I obliga a los fabricantes a establecer requisitos mínimos de hardware y red, desarrollar productos conforme a la gestión de riesgos y especificar medidas de protección frente a accesos no autorizados.
- **Seguridad de comunicaciones en autodiagnóstico conectado:** Los productos de autodiagnóstico con conectividad deben garantizar específicamente la seguridad de las comunicaciones y la protección de datos personales transmitidos, considerando las aptitudes y medios de la persona usuaria final.
- **Protección de datos genéticos:** Los productos que generan datos genéticos o información sobre predisposiciones a enfermedades requieren salvaguardas de privacidad reforzadas, dada la naturaleza especialmente sensible e inmutable de esta información.
- **Vigilancia postcomercialización:** Sistema de vigilancia y notificación de incidentes equivalente al del MDR, cuyos tratamientos de datos deben realizarse conforme al RGPD, con requisitos adicionales específicos para productos de diagnóstico.

8.3. Directiva NIS2

La Directiva (UE) 2022/2555, conocida como NIS2, establece medidas para alcanzar un elevado nivel común de ciberseguridad en toda la Unión Europea. Su relevancia para el sector sanitario es directa, ya que la Directiva clasifica expresamente a los prestadores de asistencia sanitaria como entidades esenciales sujetas a los requisitos más estrictos, ampliando significativamente las obligaciones respecto a la anterior Directiva de 2016. Un aspecto diferenciador de la NIS2 es la responsabilidad que atribuye a los órganos de dirección, que deben aprobar personalmente las medidas de gestión de riesgos, supervisar su aplicación, recibir formación específica en ciberseguridad y pueden ser considerados responsables de infracciones, lo que eleva la ciberseguridad al máximo nivel de gobernanza corporativa.

Para los ecosistemas IoMT, la NIS2 tiene implicaciones que trascienden la propia organización sanitaria, al exigir un enfoque integral que contemple las vulnerabilidades introducidas por terceros, incluyendo expresamente la seguridad de la cadena de suministro y la seguridad en la adquisición, desarrollo y mantenimiento de sistemas. Los dispositivos IoMT, suministrados por fabricantes externos e integrados en infraestructuras hospitalarias, quedan directamente afectados por estas exigencias.

Los principales requisitos de la Directiva NIS2 con impacto en entornos IoMT son:

- **Gestión integral de riesgos de ciberseguridad:** Adopción de medidas técnicas, operativas y organizativas proporcionadas para gestionar los riesgos de seguridad de los sistemas de información, incluyendo los dispositivos IoMT y sus comunicaciones.

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

- **Seguridad de la cadena de suministro:** Evaluación y gestión de los riesgos introducidos por fabricantes de dispositivos, proveedores de plataformas y empresas de mantenimiento, con requisitos de seguridad en la adquisición y desarrollo de sistemas.
- **Políticas de cifrado y control de acceso:** Implementación obligatoria de políticas de criptografía para proteger la confidencialidad e integridad de los datos, y de mecanismos de autenticación multifactor.
- **Notificación escalonada de incidentes:** Alerta temprana en 24 horas, notificación detallada en 72 horas e informe final en un mes al CSIRT o autoridad competente, con coordinación con las obligaciones de notificación del RGPD.
- **Formación y responsabilidad de la Dirección:** Obligación de que los órganos de dirección aprueben las medidas de seguridad, supervisen su aplicación y reciban formación específica, pudiendo ser considerados personalmente responsables.
- **Auditoría y evaluación de eficacia:** Políticas y procedimientos para evaluar periódicamente la eficacia de las medidas de ciberseguridad implementadas, incluyendo auditorías regulares.

8.4. Disposiciones sanitarias españolas

El tratamiento de datos personales en el ámbito sanitario español está sometido a un entramado de normas sectoriales que reconocen la singularidad del dato sanitario y la especial relación de confianza entre la persona paciente y las entidades sanitarias.

La **Ley 41/2002**, de autonomía del paciente, constituye la pieza central de este marco, estableciendo que la historia clínica comprende el conjunto de documentos que contienen datos, valoraciones e informaciones sobre la situación y evolución clínica de la persona paciente, lo que incluye los datos generados por dispositivos IoMT con relevancia clínica. Un aspecto diferenciador de esta legislación es la exigencia de separar los datos identificativos de los clínico-asistenciales cuando se accede con fines de investigación, epidemiología o docencia, así como el establecimiento de un periodo mínimo de conservación de 5 años que las comunidades autónomas pueden ampliar en su normativa específica.

A la Ley de autonomía del paciente se suma la **Ley 14/2007** de Investigación Biomédica, que resulta especialmente relevante para dispositivos IoMT utilizados en ensayos clínicos o investigación, estableciendo requisitos específicos de consentimiento informado, intervención de comités de ética y anonimización de datos.

Asimismo, el **Real Decreto 1093/2010** regula el conjunto mínimo de datos de los informes clínicos y la interoperabilidad de la historia clínica digital del Sistema Nacional de Salud, con implicaciones directas para la integración de datos procedentes de dispositivos IoMT.

Los principales requisitos derivados de la normativa sectorial sanitaria son:

- **Integración en la historia clínica:** Los datos generados por dispositivos IoMT con relevancia clínica deben incorporarse a la documentación clínica de la persona paciente con las mismas garantías de custodia, conservación y acceso que el resto de información 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

- **Separación de datos y anonimización:** Obligación de preservar los datos identificativos separados de los clínico-asistenciales para garantizar el anonimato en usos secundarios, con requisitos específicos de anonimización para investigación biomédica.
- **Conservación y retención:** Periodos mínimos de conservación de 5 años para la documentación clínica, ampliables por normativa autonómica, que condicionan las políticas de retención de datos generados por dispositivos IoMT.
- **Interoperabilidad y conjunto mínimo de datos:** Requisitos de formato e integración de datos en el ecosistema de información sanitaria nacional, con implicaciones para la compatibilidad de los datos generados por dispositivos IoMT.
- **Consentimiento e investigación:** Requisitos específicos de consentimiento informado, intervención de comités de ética y salvaguardas adicionales cuando los dispositivos IoMT se empleen en contextos de investigación biomédica.

8.5. Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece el marco de seguridad obligatorio para los sistemas de información del sector público español y para los proveedores privados que les prestan servicios. Su objetivo es garantizar que la información y los servicios digitales se gestionen con niveles adecuados de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, alineándose con la estrategia nacional y con el panorama europeo de ciberseguridad.

En el ámbito sanitario público, el ENS es especialmente relevante porque los sistemas clínicos tratan datos particularmente sensibles y soportan servicios asistenciales críticos. Cuando los dispositivos IoMT se integran en redes y sistemas sujetos al ENS, deben ajustarse al nivel de seguridad correspondiente a la categoría del sistema en el que operan. Dado el impacto que podría tener una brecha en datos de salud o un incidente sobre la continuidad asistencial, concretamente, estos sistemas suelen clasificarse como categoría media o alta, lo que implica que deben cumplir con un conjunto medidas de protección estrictas.

Los principales requisitos de seguridad que define el ENS y que son aplicables a entornos IoMT son:

- **Categorización de sistemas**: Clasificar a los sistemas de información según el impacto de en las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, determinando la categoría (básica, media o alta) que establece el nivel de exigencia de las medidas de seguridad.
- **Análisis y gestión de riesgos**: Disponer de un proceso formal de identificación, análisis y tratamiento de riesgos, con una metodología reconocida, como MAGERIT u otras equivalentes, incluyendo la documentación de activos, amenazas, vulnerabilidades, salvaguardas y revisión periódica.
- **Marco organizativo**: Definir una política de seguridad aprobada por la dirección, una normativa de seguridad que desarrolle la política, así como procedimientos operativos de seguridad y procesos de autorización para componentes del sistema.

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 incidentes**: Contar con un procedimiento de gestión de incidentes de seguridad que incluya la detección, análisis, contención, erradicación, recuperación y comunicación, con notificación al CCN-CERT en los plazos indicados.
- **Productos certificados**: Utilizar únicamente productos que tengan certificada la funcionalidad de seguridad para la que son empleados, conforme al Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) del CCN.
- **Adquisición de productos de seguridad**: Incluir requisitos de conformidad con el ENS en los pliegos de contratación y, para la contratación de sistemas de categoría alta, exigir la certificación de los productos.

8.6. Data Act - Reglamento de Datos

El Reglamento (UE) 2023/2854 , conocido como Data Act, establece las normas para garantizar un acceso justo y no discriminatorio a los datos generados por los productos conectados y por los servicios asociados. Su propósito es evitar que los datos queden en exclusiva bajo control del fabricante y asegurar que la persona usuaria, ya sea quien utiliza el dispositivo o contrata el servicio, pueda acceder, reutilizar y compartir esa información en formatos estándar y seguros.

En IoMT, esto es especialmente relevante debido a que los dispositivos médicos conectados generan datos clínicos y técnicos de alto valor para las personas pacientes, profesionales y organizaciones sanitarias. El Data Act aclara quién puede pedir esos datos, cómo deben entregarse y en qué condiciones pueden compartirse con terceros, cumpliendo en todo momento con las obligaciones de protección de datos personales definidas por el RGPD.

Los requisitos fundamentales que define el Data Act aplicables para ecosistemas IoMT son:

- **Acceso de la persona usuaria a los datos del dispositivo**: El fabricante debe poner a disposición del usuario los datos generados por el dispositivo, gratuitamente, de forma segura y en formato estructurado y legible por máquina.
- **Acceso directo o mediante solicitud**: Cuando sea técnicamente posible, el acceso debe ser directo desde el dispositivo o su servicio, en caso contrario, el fabricante debe facilitarlo sin demoras injustificadas tras la solicitud de la persona usuaria.
- **Derecho a compartir datos con terceros**: La persona usuaria puede designar a terceros, como profesionales sanitarios, para recibir los datos, que deben entregarse con la misma calidad y formato.
- **Prohibición de obstáculos técnicos o contractuales**: El titular de los datos no puede utilizar medidas técnicas, contractuales u organizativas que impidan u obstaculicen indebidamente el ejercicio de los derechos de acceso y portabilidad de los datos generados por el dispositivo.
- **Protección de secretos comerciales**: El titular de los datos puede exigir medidas de confidencialidad para proteger secretos comerciales, pudiendo en circunstancias excepcionales denegar el acceso a datos específicos cuando exista alta probabilidad de perjuicio económico grave, sin que esta excepción pueda utilizarse para impedir los derechos de acceso.

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

- **Acceso para organismos del sector público**: En situaciones de necesidad excepcional, incluyendo expresamente emergencias de salud pública, los organismos del sector público pueden solicitar acceso a datos, prevaleciendo el interés público sobre el interés del titular de disponer libremente de los datos.
- **Compatibilidad con el RGPD**: El Data Act se aplica sin perjuicio de la normativa de protección de datos personales, no pudiendo interpretarse de manera que reduzca o limite los derechos de protección de datos.

8.7. Reglamento del Espacio Europeo de Datos de Salud (EHDS)

El Reglamento (UE) 2025/327 sobre el Espacio Europeo de Datos de Salud, adoptado en el año 2025, representa la iniciativa más ambiciosa de la Unión Europea para transformar el acceso, uso e intercambio de datos sanitarios electrónicos. Su objetivo es establecer un marco que mejore el acceso de las personas físicas a sus datos electrónicos de salud y su control sobre los mismos en el contexto de la atención sanitaria (uso primario), así como facilitar otros usos que beneficien a la sociedad, tales como la investigación, la innovación, la salud pública, estadísticas o aspectos regulatorios (uso secundario).

Para los dispositivos IoMT, el EHDS tiene implicaciones profundas en ambas dimensiones, por un lado refuerza el acceso de las personas pacientes y profesionales sanitarios a los datos generados por estos dispositivos y, por otro, define las condiciones y controles en que dichos datos pueden utilizarse para finalidades de interés general englobadas dentro de los usos secundarios.

Requisitos del EHDS para el uso primario de datos sanitarios:

- **Acceso y portabilidad para uso asistencial**: Las personas deben poder acceder gratuitamente a categorías prioritarias de datos de salud y compartirlos con los profesionales que ellos elijan, incluidos profesionales de otros Estados miembros, mediante el MyHealth@EU.
- **Integración de datos generados por de la persona paciente**: Debe existir la posibilidad de incorporar los datos generados por los dispositivos IoMT a la historia clínica electrónica o a un historial personal de salud separado, siempre en formato que aseguren su interoperabilidad.
- **Control seguro de la persona paciente**: Se debe disponer de herramientas para restringir selectivamente el acceso a partes de su información, salvo en casos de emergencias que requieren proteger intereses vitales, y opciones de establecer un derecho de exclusión absoluto del acceso por terceros distintos del prestador original (*opt-out*) cuando lo prevea el derecho nacional.
- **Uso secundario con permisos y límites**: Todos los tratamientos destinados a la investigación, innovación o salud pública requieren el permiso de los organismos nacionales competentes, existiendo usos prohibidos, como publicidad.
- **Entornos de tratamiento seguros**: El uso secundario de los datos debe realizarse en entornos controlados que impidan la extracción de datos identificables y garanticen la confidencialidad, integridad y trazabilidad de los mismo, siempre a través del HealthData@EU.

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

- **Interoperabilidad y seguridad en HCE**: Los sistemas de historia clínica electrónica deben cumplir con los requisitos de interoperabilidad, registro de accesos y ciberseguridad, obligando que los fabricantes de IoMT aseguren la compatibilidad con los formatos europeos.

8.8. ISO/IEC 27001

La ISO/IEC 27001:2022 es el estándar internacional de referencia para implantar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos. Proporciona un marco estructurado para proteger la confidencialidad, integridad y disponibilidad de la información, estableciendo procesos, controles y un ciclo de mejora continua mediante auditorías internas y externas. La versión 2022 incorpora controles actualizados orientados a entornos cloud, amenazas emergentes y desarrollo seguro, todos especialmente relevantes en entornos con alta dependencia tecnológica.

En ecosistemas IoMT, la ISO 27001 actúa como una capa de gobernanza transversal que permite gestionar los riesgos asociados a dispositivos conectados, plataformas cloud, aplicaciones móviles y servicios externos. Muchas organizaciones sanitarias, tanto públicas como privadas, exigen la certificación a proveedores tecnológicos, incluyendo fabricantes, como garantía de madurez y cumplimiento en materia de seguridad.

Los requisitos principales que define la ISO/IEC 27001:2022 aplicables a IoMT son:

- **Definir el contexto y alcance del SGSI**: Identificar qué parte del entorno, incluidos dispositivos IoMT, apps y servicios asociados, queda dentro del SGSI, junto con las expectativas de clientes, personas pacientes y reguladores.
- **Liderazgo y compromiso de la Dirección**: Establecer una política de seguridad, asignar responsabilidades claras y garantizar recursos suficientes para la gestión de riesgos y la operación segura del IoMT.
- **Enfoque sistemático de gestión de riesgos**: Evaluar amenazas y vulnerabilidades que afectan a dispositivos, comunicaciones, plataformas cloud y procesos, seleccionando controles adecuados para mitigarlos.
- **Soporte y competencia del personal**: Asegurar recursos, formación, concienciación y documentación necesaria para operar de forma segura los componentes IoMT y sus integraciones.
- **Operación y control de cambios**: Ejecutar los planes de tratamiento de riesgos, gestionar cambios planificados o imprevistos y controlar adecuadamente los servicios externos involucrados en el IoMT.
- **Evaluación y mejora continua**: Realizar seguimiento periódico mediante auditorías internas y tratamientos de no conformidades para mejorar continuamente el SGSI y adaptarlo a nuevas amenazas.
- **Controles del Anexo A**: En el anexo se definen 93 controles de referencia organizados en cuatro categorías (organizativos, de personas, físicos y tecnológicos) que incluyen controles específicos para seguridad cloud, desarrollo seguro, gestión de vulnerabilidades y protección de datos.

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

8.9. ISO/IEC 27701

La norma ISO/IEC 27701:2019 extiende la ISO/IEC 27001 para implantar un Sistema de Gestión de la Información de Privacidad (PIMS). Aporta controles y orientación específicos para organizaciones que actúan como responsables y/o encargados del tratamiento, complementando la seguridad de la información con prácticas relacionadas con la privacidad de los datos, como licitud, derechos, minimización, transferencias, brechas, entre otras.

En IoMT, donde el tratamiento de datos de salud es intrínseco, esta norma ofrece un marco operativo de privacidad desde el diseño y por defecto, la gestión de derechos de la persona paciente y la trazabilidad de las actividades de tratamiento en dispositivos, apps y plataformas.

Adoptarla junto con la ISO 27001 permite disponer de una gobernanza integrada, juntando seguridad y privacidad, que alinea a fabricantes y proveedores de IoMT con los requisitos del RGPD y con las expectativas contractuales del sector salud. La certificación 27701 se percibe como evidencia objetiva de madurez y compromiso con la protección de datos personales en entornos clínicos conectados.

Requisitos específicos de la ISO/IEC 27701:2019:

- **Alcance y roles claros (R/ER)**: Definir el alcance del PIMS y el rol de la organización (responsable, encargado o ambos), identificando tratamientos, sistemas IoMT y flujos de datos asociados.
- **Licitud y bases jurídicas documentadas**: Asegurar que cada tratamiento tiene base legal válida, aplicando la condición del art. 9 RGPD al tratar datos de salud, con evidencia actualizada y rastreable.
- **Derechos y transparencia operables**: Establecer procesos y herramientas para informar al paciente y atender derechos (acceso, rectificación, supresión, limitación, oposición, portabilidad) de forma verificable y en plazo.
- **Privacidad desde el diseño y minimización**: Integrar privacidad desde el diseño y por defecto en dispositivos, aplicaciones y sistemas vinculados, con datos mínimos, retención limitada, configuraciones seguras y controles de acceso proporcionados.
- **Terceros y transferencias controladas**: Gestionar a los encargados y subencargados de los datos y garantizar que todas las transferencias, tanto nacionales como internacionales, cuentan con los salvaguardas adecuados.
- **Gestión de incidentes y mejora continua**: Detectar, registrar y notificar brechas de datos personales cuando proceda, realizar auditorías internas y revisiones por la dirección e impulsar la mejora continua del PIMS.

8.10. ISO/IEC 27799

La ISO/IEC 27799:2205 ofrece directrices específicas para el sector sanitario al aplicar los controles de ISO/IEC 27002 al contexto clínico. Reconoce que la información de salud es especialmente sensible y que los entornos asistenciales tienen dinámicas y riesgos propios, como el acceso por roles clínicos, las situaciones de urgencia, la interoperabilidad entre sistemas y una trazabilidad exigente de los datos. En ecosistemas IoMT, esta norma ayuda a conocer cómo proteger datos de personas pacientes cuando circulan entre dispositivos, aplicaciones, redes sanitarias y sistemas de historia clínica.

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

Como complemento sectorial de la ISO 27001, la ISO 27799 aporta un marco práctico para entidades sanitarias, servicios regionales de salud y proveedores IoMT. Aunque la edición vigente es de 2016 (en revisión), sus principios siguen siendo una base sólida para gobernanza, controles operativos y cultura de seguridad adaptados al entorno clínico.

La ISO 27799 ofrece las siguientes directrices específicas del sector salud:

- **Clasificación de información sanitaria**: Definir niveles de sensibilidad según el riesgo para la persona paciente, requisitos legales y expectativas de confidencialidad, usando esta clasificación para configurar la gestión accesos, cifrado y retención.
- **Gestión de accesos basada en roles clínicos y mínimo privilegio**: Modelar los permisos según el entorno sanitario, donde los profesionales requieren acceso a información de personas pacientes según su rol en la atención, con principios de mínimo privilegio y segregación de funciones.
- **Registro y trazabilidad clínica**: Mantener una gestión detallada de accesos y actividades sobre los datos de personas pacientes (quién, qué, cuándo, por qué), con retención de eventos de auditoría y revisión periódica según las normativas y el contexto clínico.
- **Seguridad del equipamiento médico conectado**: Integrar los dispositivos IoMT tras realizar una evaluación de riesgos, con segmentación de red, monitorización y políticas claras para la gestión de parches y actualizaciones.
- **Disponibilidad y acceso de emergencia**: Equilibrar la seguridad y continuidad asistencial con procedimientos acceso de emergencia y salvaguardas para no comprometer la privacidad.
- **Intercambio seguro entre organizaciones**: Proteger el tránsito de datos clínicos con mecanismo de autenticación y cifrado extremo a extremo, en caso de derivaciones entre entidades sanitarias.

8.11. Directrices MDCG

El Grupo de Coordinación de Productos Sanitarios (MDCG), establecido por el artículo 103 del MDR, reúne a expertos designados por los Estados miembros con el fin de asesorar a la Comisión Europea y promover una aplicación armonizada tanto del MDR como del IVDR. Aunque sus documentos no son jurídicamente vinculantes, constituyen interpretaciones autorizadas de los requisitos regulatorios y establecen indicaciones claras para fabricantes, organismos y autoridades competentes. En el ámbito de la ciberseguridad y la protección de datos, estas directrices son indispensables para comprender cómo deben aplicarse los requisitos técnicos del MDR e IVDR, proporcionando una guía práctica que complementa el texto legal.

El MDCG ha publicado numerosas guías que inciden directamente en la ciberseguridad, protección de datos y seguridad de dispositivos IoMT. Estas abarcan desde la calificación del software como producto sanitario hasta la integración de la ciberseguridad en la gestión de riesgos o la evaluación de tecnologías. La interpretación de los requisitos de seguridad del MDR e IVDR debe realizarse siguiendo estas orientaciones, que reflejan el consenso entre las autoridades de los Estados miembros.

Concretamente, los principales documentos del MDCG en materia de ciberseguridad son:

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

- **MDCG 2021-24 "Guidance on classification of medical devices"**: Clarifica la aplicación de las reglas del Anexo VIII del MDR, incluyendo la necesidad del tratamiento activo del software.
- **MDCG 2019-16 "Guidance on Cybersecurity for medical devices"**: Guía principal para abordar la ciberseguridad a lo largo del ciclo de vida del producto, desde el diseño hasta la vigilancia poscomercialización, en coherencia con la ISO 14971.
- **MDCG 2019-11 "Guidance on qualification and classification of software"**: Criterios para determinar cuándo un software es un producto sanitario y cómo clasificarlo, con especial relevancia en la interpretación de la Regla 11.

8.12. Directrices ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) publica guías y recomendaciones prácticas para reforzar la seguridad en sectores críticos, entre ellos el sector salud y los dispositivos médicos conectados. Su objetivo es ofrecer orientación técnica y organizativa que complemente la normativa europea, proporcionando buenas prácticas, marcos de evaluación y herramientas para mejorar la resiliencia de las organizaciones de estos sectores.

Las directrices ENISA abordan aspectos particularmente relevantes para la protección de datos en entornos IoMT, incluyendo la gestión de riesgos en la cadena de suministro, la seguridad en el ciclo de vida de dispositivos médicos, la respuesta a incidentes en entornos clínicos y la concienciación del personal sanitario. ENISA también ha desarrollado metodologías de evaluación de riesgos y herramientas de autoevaluación para que las organizaciones sean capaces de identificar vulnerabilidades y priorizar inversiones. Para organizaciones sanitarias españolas, las directrices ENISA proporcionan orientación valiosa para complementar los requisitos del Esquema Nacional de Seguridad y prepararse para las obligaciones de la Directiva NIS2.

Principales directrices ENISA para el sector sanitario:

- **Cyber Hygiene in the Health Sector (2025):** Guía sobre prácticas esenciales de higiene digital para entornos sanitarios con listas de verificación operativas adaptadas a hospitales y servicios de salud.
- **ENISA Threat Landscape: Health Sector (2023):** Guía que analiza las amenazas y vectores de ataque más frecuentes en el sector sanitario, incluyendo tendencias, casos concretos y recomendaciones de mitigación priorizadas.
- **CSIRT Capabilities in Healthcare Sector (2021):** Guía que proporciona directrices para definir y reforzar las capacidades de respuesta a incidentes en el sector salud.
- **Cloud Security for Healthcare Services (2021)**: Guía sobre el uso seguro de soluciones cloud, incluyendo evaluación de riesgos, selección de proveedores, protección de datos clínicos, continuidad y respuesta ante incidentes.
- **Procurement Guidelines for Cybersecurity in Hospitals (2020)**: Guía para la adquisición segura en hospitales, la cual indica qué requisitos de ciberseguridad se deben incluir en pliegos, cómo realizar evaluaciones a proveedores y productos, y cómo verificar el cumplimiento tras la adjudicación.

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

- **Baseline Security Recommendations for IoT (2017)**: Guía sobre recomendaciones mínimas de seguridad para dispositivos IoT (incluido IoMT), cubriendo la seguridad desde el diseño, capacidades básicas del dispositivo, gestión de vulnerabilidades y actualizaciones y comunicaciones seguras, entre otros.
- **Cyber security and resilience for Smart Hospitals (2016)**: Guía sobre análisis de amenazas y buenas prácticas para hospitales conectados, con recomendaciones de arquitectura y gestión de riesgos.

9. Plan de Acción y medidas necesarias en entornos IoMT

Tras analizar el marco regulatorio a nivel nacional, europeo e internacional aplicable a los entornos IoMT en materia de privacidad y protección de la información, entre los cuales se incluyen RGPD, LOPDGDD, MDR, IVDR, NIS2, ENS, así como otros estándares y regulaciones, resulta necesario transformar las obligaciones que estas regulaciones imponen, en un conjunto de medidas concretas que permitan a las entidades sanitarias garantizar un tratamiento seguro de los datos personales.

En este contexto, se debe diseñar un plan de acción estructurado en tres tipos de medidas:

- **Medidas organizativas:** Definen la gobernanza, roles, procedimientos internos y documentación necesaria para asegurar el cumplimiento normativo.
- **Medidas técnicas:** Destinadas a proteger la información mediante controles aplicables tanto a los dispositivos médicos como a la infraestructura que los soporta.
- **Medidas operativas:** Orientadas a garantizar la aplicación práctica de los controles en la operativa diaria de la entidad sanitaria.

No obstante, a diferencia de otros entornos, el ecosistema IoMT presenta un conjunto de limitaciones inherentes a las características de los dispositivos médicos, que dificultan o incluso impiden la aplicación directa de determinadas medidas de seguridad.

Por este motivo, el plan de acción debe incorporar un conjunto de medidas compensatorias, orientadas a mitigar los riesgos derivados de la falta de controles técnicos en los propios dispositivos y a reforzar la seguridad a nivel de red, infraestructura, procesos y gobernanza.

El objetivo de este apartado es aportar un marco práctico que permita a las entidades sanitarias compensar las limitaciones de los entornos IoMT, cumpliendo con las obligaciones normativas aplicables y preservando al mismo tiempo la seguridad de la persona paciente, la continuidad asistencial y la protección de los datos personales.

9.1. Medidas Organizativas

Las medidas organizativas establecen la estructura de gobernanza, los roles, los procesos y la documentación que permiten garantizar un uso seguro y conforme a la normativa de los dispositivos IoMT. Estas medidas son imprescindibles para coordinar áreas clínicas, técnicas y de cumplimiento, y constituyen el soporte sobre el que se implementan el resto de las medidas.

❖ Gobernanza y responsabilidades

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

Una gobernanza adecuada es esencial para asegurar que la organización gestiona los entornos IoMT de forma coordinada, coherente y alineada con sus obligaciones legales y asistenciales. Para ello, la entidad sanitaria debe disponer de una estructura clara que establezca quién decide, quién supervisa y cómo se gestionan los riesgos asociados a los dispositivos médicos.

- **Política de seguridad de la información**: Disponer de una política formal, aprobada por la Dirección, que establezca los principios y criterios generales de seguridad aplicables a los dispositivos IoMT y a los sistemas que los soportan.
- **Modelo de gobierno IoMT**: Definir un modelo organizativo que determine cómo se gestionan los dispositivos IoMT dentro de la organización y qué áreas participan en su supervisión.
- **Comité de seguridad**: Contar con un órgano formal donde participen la Dirección, los servicios clínicos, electromedicina, TI, seguridad y privacidad, encargado de tomar decisiones estratégicas.
- **Delegado de Protección de Datos (DPD):** Garantizar que la organización cuenta con un DPD y que este participa en las decisiones que afecten al tratamiento de datos personales derivados del uso de dispositivos IoMT.
- **Definición del apetito de riesgo**: Establecer cuál es el nivel de riesgo asumible por la organización en cuyo alcance estén los dispositivos IoMT.
- **Procedimiento de escalado**: Definir cuándo y cómo deben comunicarse incidentes, riesgos, vulnerabilidades o fallos relevantes a los niveles directivos correspondientes, asegurando que cada situación recibe la atención adecuada en función de su gravedad.
- **Roles y responsabilidades**: Dejar documentado quién se encarga de cada fase del ciclo de vida del IoMT, adquisición, configuración, mantenimiento, monitorización, retirada, evitando solapamientos entres distintos equipos.

❖ Cuerpo normativo interno

La gestión de los entornos IoMT debe integrarse en el marco general de seguridad y privacidad de la organización. Contar con políticas y procedimientos claros permite garantizar una actuación coherente ante cualquier situación y demostrar el cumplimiento normativo en las auditorías externas.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: Disponer de un SGSI que establezca el marco de control de seguridad, e incluya los activos, procesos y controles aplicables al ecosistema IoMT.
- **Sistema de Gestión de Privacidad de la Información (SGPI)**: Disponer de un SGPI que integre la gestión de privacidad y protección de datos en los entornos IoMT.
- **Procedimiento de gestión de vulnerabilidades**: Establecer cómo identificar, evaluar y tratar vulnerabilidades que afecten a los dispositivos IoMT, incluyendo casos en los que el dispositivo no pueda ser parcheado o actualizado y requiera medidas compensatorias.
- **Procedimiento de gestión de incidentes**: Definir cómo actuar ante fallos técnicos, incidentes de seguridad o brechas de datos personales asociadas a 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

- **Procedimiento de gestión de accesos**: Documentar cómo se autorizan, revisan y eliminan los accesos a los entornos IoMT, así como los accesos físicos o remotos necesarios para el mantenimiento.
- **Procedimientos de gestión de copias de seguridad**: En los casos en que existan sistemas intermedios o plataformas que gestionen datos de los dispositivos IoMT, establecer normas para realizar copias de seguridad, almacenarlas de forma segura y garantizar la recuperación ante fallos.

Los procedimientos anteriormente definidos, forman el conjunto mínimo de procedimientos recomendados que una entidad sanitaria debería disponer para cumplir con el marco regulatorio aplicable. No obstante, en función del tamaño y las características de la entidad, la organización podrá requerir procedimientos adicionales.

❖ Clasificación de activos IoMT

Una gestión adecuada de los dispositivos IoMT exige conocer con precisión qué dispositivos existen, dónde están, qué funciones cumplen y qué riesgos introducen. Sin un inventario actualizado y una clasificación clara, no es posible priorizar medidas o tomar decisiones informadas.

- **Inventario de dispositivos IoMT**: Mantener un registro centralizado que incluya todos los dispositivos médicos y sus elementos asociados. Este inventario deberá incluir:
    - **Características del dispositivo**: Información esencial como fabricante, modelo, número de serie, ubicación, servicio clínico, tipo de conectividad, versiones de firmware o software, estado, etc.
    - **Clasificación por criticidad clínica**: Impacto potencial sobre la seguridad de la persona paciente en caso de fallo, funcionamiento inadecuado o indisponibilidad.
    - **Responsables del activo**: Persona o área propietaria del dispositivo y el equipo encargado de su mantenimiento.

❖ Gestión de riesgos

La gestión de riesgos es fundamental para determinar qué medidas deben aplicarse a cada dispositivo IoMT. Dado que muchos equipos presentan limitaciones técnicas o clínicas, es imprescindible evaluar el riesgo y justificar cuándo una medida no se puede aplicar y debe sustituirse por una medida compensatoria.

- **Metodología de análisis de riesgos**: Disponer de un proceso formal que tenga en cuenta aspectos técnicos, clínicos y regulatorios asociados al uso de dispositivos IoMT.
- **Realización de DPIA/EIPD**: Llevar a cabo una evaluación de impacto en protección de datos cuando el tratamiento de información de salud o la naturaleza del dispositivo así lo requiera.
- **Gestión de excepciones**: Documentar los casos en los que un dispositivo no permite aplicar un control y justificar la necesidad de adoptar medidas compensatorias.
- **Planes de acción**: Establecer controles alternativos que reduzcan el riesgo y realizar un seguimiento de la implantación de estos.

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

- **Registro de riesgos IoMT**: Mantener un registro actualizado en el que se recojan los riesgos identificados, las medidas aplicadas, las excepciones aprobadas y las fechas de revisión.

❖ Gestión del ciclo de vida

La gestión del ciclo de vida del IoMT abarca todas las fases de un dispositivo médico conectado, desde su adquisición hasta su retirada. Para minimizar riesgos y garantizar el cumplimiento normativo, la organización debe aplicar medidas en cada una de las etapas.

- **Proceso de adquisición segura**: Definir requisitos mínimos de seguridad y privacidad en la compra de dispositivos IoMT.
- **Evaluación técnica y clínica previa**: Validar que el dispositivo cumple los requisitos funcionales, asistenciales y de seguridad antes de su despliegue, evitando la incorporación de equipos que no cumplan con las medidas de seguridad e introduzcan riesgos a la entidad.
- **Alta y puesta en servicio**: Asegurar que cada dispositivo se despliega siguiendo los procedimientos definidos, ajustando los parámetros por defecto cuando sea posible y registrándolo en el inventario de la organización.
- **Mantenimiento y actualizaciones**: Establecer procedimientos claros para gestionar las actualizaciones de firmware y software, garantizando que todas ellas se prueban y validan antes de su despliegue.
- **Gestión del cambio**: Definir cómo se autorizan y ejecutan modificaciones en los entornos de producción, asegurando que no se introducen nuevos riesgos sin evaluación previa por parte de los responsables.
- **Retirada del dispositivo**: Definir un proceso seguro para la retirada de los dispositivos, garantizando el borrado de datos, la desconexión controlada, la revocación de accesos y la gestión del hardware.

❖ Gestión de la cadena de suministro

Los dispositivos IoMT dependen en gran medida de fabricantes, proveedores y servicios externos, lo que introduce riesgos que la organización no puede controlar directamente. Por ello, es esencial establecer mecanismos claros para gestionar la cadena de suministro y proteger el entorno sanitario ante posibles riesgos externos a la entidad.

- **Evaluación de proveedores**: Analizar previamente a cada proveedor para comprobar que cumple con requisitos mínimos de seguridad y privacidad, así como asignarle un nivel de riesgo asociado a los servicios prestados.
- **Requisitos contractuales de seguridad**: Incluir en los contratos y acuerdos cláusulas específicas sobre seguridad, siguiendo las pautas definidas en la guía "*Clausulado de seguridad para la contratación pública de tecnologías IoMT*" de la Agencia Digital de Andalucía .
- **Notificación de incidentes**: Exigir al proveedor la notificación de incidentes de seguridad que afecten a los servicios prestados a 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

- **Acuerdos de nivel de servicio**: Definir tiempos máximos aceptables para la resolución de incidencias o aplicación de parches, incluyendo penalizaciones en caso de incumplimiento, especialmente cuando el fallo pueda afectar a la seguridad de la persona paciente o a la protección de datos personales.

❖ Formación y concienciación

El factor humano es determinante para garantizar la protección de la información en los entornos IoMT. Por ello, la organización debe establecer acciones formativas que garanticen un uso seguro y responsable de los dispositivos médicos conectados.

- **Formación por perfiles**: Ofrecer formación diferenciada según el rol y el nivel de responsabilidad. Esta formación debe incluir buenas prácticas y guías como la guía "*Uso Responsable y Seguro de dispositivos IoMT en entornos sanitarios*" de la Agencia Digital de Andalucía.
- **Simulacros y ejercicios prácticos**: Realizar ejercicios periódicos para evaluar la preparación del personal, como campañas de phishing y escenarios prácticos.

❖ Seguimiento y mejora continua

Para garantizar que las medidas implantadas en el entorno IoMT siguen siendo eficaces a lo largo del tiempo, la organización debe establecer mecanismos de seguimiento y mejora continua. El objetivo es detectar desviaciones, identificar nuevas necesidades y adaptar los controles a los cambios tecnológicos, regulatorios o asistenciales.

- **Seguimiento y revisión periódica**: Revisar de forma regular el inventario de dispositivos, los riesgos asociados, las medidas aplicadas y las posibles excepciones autorizadas, asegurando que la información refleja la situación real del entorno IoMT.
- **Auditorías internas**: Realizar auditorías periódicas para verificar que los controles se aplican correctamente, que las políticas se cumplen y que no existen brechas entre lo documentado y lo que realmente ocurre en la operativa diaria.
- **Actualización de políticas y procedimientos**: Adaptar la documentación interna cuando existan cambios tecnológicos, nuevas amenazas, nuevas versiones de dispositivos, actualizaciones regulatorias o modificaciones organizativas.

9.2. Medidas Técnicas

Las medidas técnicas constituyen los controles directos aplicados sobre los dispositivos IoMT, las redes y las infraestructuras que los soportan. Su implantación debe considerar las limitaciones inherentes a muchos dispositivos médicos, que en ocasiones impiden aplicar soluciones de seguridad. Estas medidas deben implementarse siempre que sea técnicamente viable y complementarse con medidas compensatorias cuando el dispositivo no permita configuraciones avanzadas.

❖ Control de acceso

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

Controlar quién puede acceder a los dispositivos IoMT y a las plataformas asociadas es esencial para reducir la superficie de ataque y prevenir usos indebidos.

- **Autenticación robusta**: Aplicar autenticación multifactor en plataformas y sistemas de gestión cuando sea posible y asegurar, como mínimo, la eliminación de todas las credenciales por defecto presentes en los dispositivos.
- **Gestión centralizada del acceso**: Disponer de un sistema centralizado para la gestión de cuentas de acceso y permisos, evitando la existencia de cuentas locales y la ejecución de tareas manuales.
- **Principio de mínimo privilegio**: Revisar periódicamente los permisos de cada cuenta de acceso, asegurando que solo tienen acceso a los entornos estrictamente necesarios para su actividad.
- **Eliminación de credenciales por defecto**: Deshabilitar servicios, cuentas o contraseñas por defecto, y aplicar políticas de gestión de contraseñas.
- **Registro de accesos**: Registrar accesos exitosos y fallidos en dispositivos o plataformas, siempre que sea técnicamente posible.

❖ Protección de datos

La protección de los datos de salud requiere garantizar su confidencialidad, integridad y disponibilidad tanto durante la transmisión como en el almacenamiento. Dado que muchos dispositivos IoMT no soportan cifrado nativo o algoritmos avanzados, las medidas deben aplicarse preferentemente en las capas y sistemas que rodean al dispositivo.

- **Cifrado de comunicaciones**: Emplear protocolos seguros para proteger la transmisión de datos entre los dispositivos IoMT y los sistemas clínicos, aplicando configuraciones reforzadas en los elementos de red o pasarelas intermedias cuando el propio dispositivo no soporte cifrado.
- **Cifrado en reposo**: Aplicar cifrado en los dispositivos o plataformas que almacenan datos de salud, teniendo en cuenta las limitaciones técnicas de cada equipo. Cuando el dispositivo no permita cifrado, aplicar medidas compensatorias en el sistema que aloja o procesa la información.
- **Seudonimización o anonimización**: Reducir la exposición de datos personales cuando la identificación directa de la persona paciente no sea necesaria para el funcionamiento del dispositivo o para los procesos asistenciales.
- **Controles de integridad**: Implementar mecanismos que permitan detectar modificaciones no autorizadas en los datos transmitidos o almacenados, especialmente en sistemas intermedios o plataformas de agregación de datos.
- **Gestión segura de claves**: Definir procedimientos claros para la generación, almacenamiento, distribución, rotación y revocación de claves criptográficas, asegurando que se utilizan prácticas actualizadas y acordes a estándares de seguridad.

❖ Seguridad de 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

La red actúa como capa de protección fundamental en entornos IoMT, especialmente en dispositivos con capacidades de seguridad limitadas.

- **Segmentación de red**: aislar los dispositivos IoMT mediante Blanes u otras tecnologías, sobre todo aquellos con riesgo crítico en la seguridad de la persona paciente, con reglas de tráfico estrictamente controladas y diferenciadas del resto de la red corporativa.
- **Filtrado de red**: Aplicar políticas de filtrado para limitar las comunicaciones entrantes y salientes únicamente a los servicios y destinos necesarios para el funcionamiento del dispositivo, mediante el uso de dispositivos como firewalls y proxys.
- **Restricción de conectividad**: Asegurar que cada dispositivo solo se comunica con los sistemas y servicios necesarios.
- **Desactivación de servicios no esenciales**: Deshabilitar puertos, protocolos y funcionalidades que no sean imprescindibles para la operativa del dispositivo.
- **Monitorización del tráfico**: Disponer de herramientas de monitorización del tráfico, como SIEM, IDS o IPS, que permitan supervisar patrones y comportamientos anómalos en los segmentos donde se alojan dispositivos IoMT.

❖ Gestión de vulnerabilidades y actualizaciones

Los dispositivos IoMT requieren un enfoque específico debido a su fuerte dependencia del fabricante, sus ciclos de vida prolongados y las limitaciones habituales para aplicar parches o realizar escaneos sin impacto clínico.

- **Identificación controlada de vulnerabilidades**: Aplicar escaneos o revisiones técnicas adaptadas al entorno clínico para evitar interrupciones.
- **Proceso formal de aplicación de parches**: Evaluar, probar y validar cada parche antes de su despliegue, asegurando que no afecta al funcionamiento clínico.
- **Seguimiento de avisos oficiales**: Monitorizar boletines de fabricantes, CCN-CERT y fuentes públicas para detectar vulnerabilidades relevantes.
- **Inventario de versiones**: Mantener un registro actualizado de firmware y software para identificar rápidamente dispositivos afectados.

9.3. Medidas Operativas

Las medidas operativas se centran en cómo se gestionan y utilizan los dispositivos IoMT en el día a día de la entidad. La operativa diaria de los entornos IoMT debe estar alineadas con los procesos clínicos, garantizando que la seguridad no obstaculiza la atención sanitaria y que los dispositivos se gestionan de forma controlada.

❖ Gestión de incidentes de seguridad

La organización debe estar preparada para detectar, contener y resolver incidentes relacionados con dispositivos IoMT, evitando impactos sobre la atención 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

- **Procedimiento de gestión de incidentes**: Definir fases claras de detección, contención, análisis, recuperación y lecciones aprendidas.
- **Clasificación de incidentes**: Establecer niveles de severidad según el impacto potencial en la seguridad de la persona paciente, la disponibilidad del dispositivo o la privacidad de los datos.
- **Equipo de respuesta a incidentes**: Designar un equipo con roles y responsabilidades definidos, incluyendo los protocolos de comunicación interna y la coordinación con el resto de los equipos del entorno sanitario.
- **Notificación de brechas**: Integrar en el procedimiento los requisitos legales de notificación a la Agencia Española de Protección de Datos (AEPD) en un máximo de 72 horas cuando se vea comprometida información personal.
- **Coordinación con organismos externos**: Activar la comunicación con el CCN-CERT u organismos equivalentes cuando la entidad forme parte del sector público o el incidente tenga impacto sobre la privacidad de los datos de las personas pacientes.

❖ Gestión de brechas de datos personales

Los dispositivos IoMT al tratar datos de salud, obliga a las organizaciones a disponer de un proceso específico para gestionar brechas conforme al RGPD y la LOPDGDD.

- **Procedimiento de brechas de datos**: Identificar, evaluar y documentar cualquier incidente que pueda tener un impacto en los datos personales.
- **Evaluación del riesgo**: Determinar si la brecha supone un riesgo para los derechos y libertades de la persona paciente, y si requiere notificación a la autoridad de control o a los afectados.
- **Registro de brechas**: Documentar todas las brechas, incluidas aquellas que no deben ser notificadas , para evidenciar diligencia y detectar patrones.
- **Protocolos de comunicación**: Disponer de mensajes y plantillas predefinidas para agilizar la comunicación cuando la brecha sea confirmada.
- **Intervención del Delegado de Protección de Datos**: Asegurar que el DPD supervisa el análisis, la decisión y el cierre de cada brecha.

❖ Continuidad de servicio

Muchos dispositivos IoMT forman parte de procesos asistenciales críticos, por lo que deben existir medidas para garantizar la continuidad de la atención incluso cuando se producen escenarios de contingencia.

- **Planes de continuidad específicos**: Identificar los dispositivos IoMT críticos y definir planes que permitan mantener la actividad asistencial ante escenarios de contingencia.
- **Procedimientos de operación alternativa**: Establecer instrucciones para que los profesionales clínicos puedan continuar prestando asistencia cuando un dispositivo conectado no esté operativo.

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

- **Copias de seguridad y restauración**: Para los sistemas o configuraciones asociados al IoMT, realizar copias periódicas y validar su integridad y capacidad de recuperación.
- **Pruebas y ejercicios de continuidad**: Llevar a cabo ejercicios que simulen escenarios de contingencia para comprobar la eficacia de los planes de continuidad y detectar áreas de mejora.
- **Compromisos con fabricantes**: Asegurar que existen tiempos de respuesta adecuados por parte de los proveedores para restaurar servicios críticos cuando sea necesario.

10. Conclusiones

La protección de datos personales en ecosistemas IoMT constituye uno de los retos más relevantes y complejos de la transformación digital del sector sanitario. Los dispositivos médicos conectados aportan nuevas oportunidades para mejorar la calidad asistencial, sin embargo, también incrementan la exposición a riesgos de privacidad y seguridad que deben gestionarse por las entidades sanitarias.

El marco normativo español, europeo e internacional, junto con estándares y directrices sectoriales, establece obligaciones en materia de protección de datos, ciberseguridad y gestión del riesgo. No obstante, el cumplimiento no se limita a conocer la norma, sino a convertir sus principios en medidas aplicables, adaptadas al contexto clínico y tecnológico de cada organización.

En IoMT, además, es imprescindible asumir que muchos dispositivos presentan limitaciones que impiden aplicar controles de seguridad de forma directa. En estos casos, la gestión del riesgo exige adoptar controles alternativos en capas externas que reduzcan la exposición y permitan mantener niveles de seguridad aceptables sin comprometer la continuidad asistencial.

En definitiva, la protección de los datos sanitarios no se alcanza mediante controles aislados, sino a través de un enfoque integral que combine gobernanza, medidas técnicas y operativas, con el objetivo de proteger la información y la seguridad de las personas pacientes.

11. Referencias

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

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

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

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

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

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

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

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

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

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

10. European Union Agency for Cybersecurity (ENISA). (2025). *Cyber Hygiene in the Health Sector.* https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector

11. European Union Agency for Cybersecurity (ENISA). (2020). *BP. 05: Procurement guidelines for cybersecurity in hospitals (es)*. https://www.enisa.europa.eu/publications/procurement-guidelines-for-cybersecurity-in-hospitals

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

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

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

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

15. 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

16. 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

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

18. 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

19. 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

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

12. 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.

12.1. Lista de materias tratadas en la guía

- Contexto del IoMT
- Tratamiento de datos personales
- Marco normativo en protección de datos
- Roles y responsabilidades del tratamiento de datos
- Principios y bases de licitud en el tratamiento de datos de salud

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

- Medidas de protección de datos en IoMT

12.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

12.3. 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

Privacidad y Protección de Datos en IoMT

Febrero de 2026

Versión 1.0

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