



# DISPOSITIVOS MÉDICOS



Co-funded by  
the European Union

*ESCAPE. Preparing healthcare professionals for cyberattacks  
Project No.2023-1-ES01-KA220-VET-000151536*

# Socios



Firlla

PRAMMER



ESCAPE. Preparing healthcare professionals for cyberattacks  
Project No.2023-1-ES01-KA220-VET-000151536



Co-funded by  
the European Union

*Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.*



# Tabla de Contenidos

1. Definición	1
2. Relevancia general	1
3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados	1
4. ¿Qué puedo hacer como profesional sanitario?	1
5. Más información	
1. Materiales de aprendizaje	2
2. Vídeos Relacionados	2
3. Enlaces Relevantes	3
6. Bibliografía	3



Co-funded by  
the European Union



# FACTSHEET – DISPOSITIVOS MÉDICOS

## 1. Definición

Podemos definirlos como aquellos dispositivos interconectados empleados en el ámbito sanitario. Abarcan desde herramientas de diagnóstico hasta dispositivos de soporte vital (por ejemplo, respiradores, marcapasos). Estos dispositivos representan un vector de ataque significativo debido a las posibles vulnerabilidades a las que se exponen<sup>1</sup>.

## 2. Relevancia general

Los dispositivos médicos son un área vulnerable clave y se identifican como un enfoque específico de nuevas regulaciones, como el Cyber Resilience Act, debido a su impacto directo en la atención al paciente<sup>2</sup>. Se proporcionan diagnósticos precisos, tratamientos efectivos y un monitoreo continuo de los pacientes. Además, de manera indirecta, contribuyen a una mayor esperanza de vida y a la mejora en la prestación de servicios de salud<sup>3</sup>.

Los ciberataques representan una amenaza significativa contra estos instrumentos que puede acarrear consecuencias severas, incluso poniendo en riesgo la vida de las personas. Por esta razón, es fundamental establecer regulaciones y mecanismos de vigilancia a nivel global.

## 3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

En el ámbito de la salud, los dispositivos médicos tienen un efecto directo en la seguridad y el rendimiento clínico. Las tecnologías de soporte vital son fundamentales en el ámbito de la atención crítica, y los monitores portátiles permiten a los pacientes crónicos gestionar sus problemas de salud desde sus hogares<sup>4</sup>.

Las fallas o vulnerabilidades en este tipo de dispositivos representan riesgos que abarcan desde el retraso en el tratamiento hasta incidentes que pueden poner en peligro la vida de los pacientes. La garantía de un uso seguro y efectivo de estas tecnologías contribuye a la construcción de confianza, a la reducción de daños prevenibles y a una mejora significativa en la calidad de vida.

## 4. ¿Qué puedo hacer como profesional sanitario?

- Seguir las instrucciones y protocolos del proveedor cuando manipules dispositivos médicos.
- Informar de cualquier actividad sospechosa relacionada con estos instrumentos.
- Tener una buena ciberhigiene, utilizar contraseñas seguras y habilitar la autenticación en dos pasos.
- Concienciar a los pacientes del uso seguro de dispositivos médicos en sus hogares.



## 5. Más información

### 5.1 Materiales de aprendizaje

- [Sequential videos for general topics about cybersecurity \(JGT-2\)](#)
- [An article on security strategies applicable to electronic patient records \(IST-37\)](#)
- [An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. \(IST-39\)](#)
- [A compendium on the processing of patient data on online platforms. \(IST-40\)](#)
- [Regulation of cybersecurity in healthcare \(BBS-23\)](#)
- [Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that \(PRAMMER-32\)](#)

### 5.2 Vídeos Relacionados

Este vídeo explica acciones esenciales para garantizar la seguridad del paciente en entornos sanitarios, incluyendo comunicación efectiva, cultura de seguridad y prevención de errores.

#### Dispositivos médicos

[https://youtu.be/qZStO1rWaQQ?si=\\_FwEhey9Q9KSY9zl](https://youtu.be/qZStO1rWaQQ?si=_FwEhey9Q9KSY9zl)

Este vídeo aborda la creciente preocupación por la seguridad de los dispositivos médicos conectados, como marcapasos, bombas de insulina y otros equipos IoMT (Internet de las Cosas Médicas). Estos dispositivos, al estar cada vez más integrados en redes hospitalarias, presentan riesgos significativos si no se gestionan adecuadamente.

#### Ciberseguridad en Dispositivos Médicos

<https://youtu.be/TGNcNvTRgGc?si=T8zvELa9u84qOrGB>





### 5. 3 Enlaces Relevantes

La creciente integración de dispositivos médicos conectados en los sistemas de salud presenta una amenaza significativa para la ciberseguridad, derivada de su susceptibilidad a la explotación por parte de actores maliciosos

<https://www.illumio.com/es-mx/blog/connected-medical-devices-healthcare-cybersecurity-vulnerability>

La FDA se dedica a ayudar a garantizar que los dispositivos médicos conectados estén protegidos de las amenazas de seguridad cibernética. Si se identifica una vulnerabilidad o deficiencia en el software, hardware u otro factor que pueda suponer un riesgo, la FDA puede emitir lo que se denomina una "comunicación de seguridad".

<https://www.fda.gov/consumers/articulos-para-el-consumidor-en-espanol/seguridad-cibernetica-de-dispositivos-medicos-lo-que-necesita-saber>

En este artículo, se analizan los nuevos problemas de ciberseguridad del sector, las normativas y los pasos importantes que puede dar para proteger y gestionar sus dispositivos médicos frente a las amenazas actuales y futuras.

<https://es.digi.com/blog/post/medical-device-security>

### 6. Bibliografía

Liveri, D., Drougkas, A., & Zisi, A. (2021). Cloud Security for Healthcare Services. ENISA.

<https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf>

Young, M. (2025, 22 enero). European Commission Publishes Action Plan on Cybersecurity of Hospitals and Healthcare Providers | Covington Digital Health. Covington Digital Health.

<https://www.covingtondigitalhealth.com/2025/01/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/>

Overview. (2025, 26 agosto). Public Health.

[https://health.ec.europa.eu/medical-devices-sector/overview\\_en](https://health.ec.europa.eu/medical-devices-sector/overview_en)

World Health Organization: WHO. (2020, 2 julio). Medical devices.

<https://www.who.int/health-topics/medical-devices>





ESCAPE. Preparing healthcare professionals for cyberattacks  
Project No.2023-1-ES01-KA220-VET-000151536



Co-funded by  
the European Union



Firda

PRAMMER



Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

