# ROBO DE DATOS

Co-funded by the European Union

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

# Socios

**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 la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.*

# Tabla de contenido




Co-funded by the European Union

# FACTSHEET – ROBO DE DATOS

## 1. Definición

Constituye cualquier acción intencional o inintencional que da como resultado un acceso no autorizado, revelación o manipulación de datos sensibles, privados o protegidos, incluidos aquellos de los pacientes o sus historiales clínicos1. Las filtraciones son fruto del hacking, phishing, un error de configuración, un error interno o un robo físico.

## 2. Relevancia general

En los últimos años, ha habido un vertiginoso crecimiento en la incidencia de los robos de datos, tanto en frecuencia como en severidad. Aproximadamente el 46% de estos incidentes tiene como objetivo directo la información sensible de los pacientes y la propiedad intelectual, involucrando con frecuencia ataques de ransomware.

Las filtraciones de datos conllevan costes significativos, y pueden afectar a la reputación de las empresas, ya que exponen datos personales, financieros y confidenciales. Ante la ocurrencia de un ataque, las empresas se ven obligadas a interrumpir sus sistemas para investigar el incidente, lo que conlleva retrasos, cancelaciones y pérdidas en las ventas2.

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

Los ciberdelincuentes se encuentran particularmente interesados en el robo de datos en el sector sanitario. La razón de esto es la enorme cantidad de información privada y financiera que pueden recopilar de las personas, lo cual causa un perjuicio significativo en hospitales y pacientes. La información extraída puede emplearse para el robo de identidad, y tiene un impacto considerable en la salud y tratamiento de los pacientes3:

1. Los riesgos para la seguridad del paciente surgen cuando los atacantes modifican la información de los pacientes, como las recetas y la historia clínica. Esto puede provocar la incorrecta administración de medicación o retrasos en los tratamientos de pacientes con enfermedades crónicas.
2. De acuerdo con IBM, el coste de los robos de datos en el sector sanitario asciende a 10.98 millones de dólares. Esto incluye los gastos de medicamentos, notificar a los pacientes afectados y la conformación de un equipo para investigar el robo de datos.
3. Sanciones legales, de acuerdo con la HIPAA en Estados Unidos y el RGPD en Europa.
4. Las filtraciones de datos pueden interrumpir la atención médica. Pueden desconectar los sistemas, lo que puede generar retrasos, cancelaciones de citas y complicaciones administrativas. La restauración del funcionamiento normal puede requerir un periodo de semanas o meses, lo que conlleva que el hospital opere a una capacidad reducida.
5. Otra de las consecuencias derivadas del robo de datos es el daño reputacional, causando que los pacientes pueden mostrarse reacios a compartir información médica sensible. Fuentes estiman una caída del 4.65% en las visitas de pacientes tras la violación de datos4.

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

- Utilizar accesos seguros mediante el inicio de sesión en la plataforma en la nube del hospital, con contraseñas seguras y la autentificación en dos pasos.
- Encriptar la información sensible y emplear sistemas de almacenamiento seguro que se adhieran a las regulaciones oficiales (HIPAA y RGPD).
- El error humano es uno de los riesgos más significativos en ciberseguridad. Fomenta entre los empleados y mantente al día sobre cómo responder ante los incidentes.
- Sigue un plan de respuesta al robo de datos tan pronto como detectes un posible ataque.

## 5. Más información

### 5.1 Learning Materials

- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- Educational project on safe and responsible digital use. (IST-41)
- Regulation of cybersecurity in healthcare (BBS-23)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)

### 5.2 Vídeos Relacionados

Este vídeo trata sobre cómo los servidores pueden ser vulnerables a robos de información personal si no se protegen adecuadamente, y explica algunas buenas prácticas para asegurar los servidores y prevenir filtraciones de datos.

| **Robo de datos personales \| Seguridad en Servidores** |
|---|
| https://youtu.be/0kK902-ZvNM?si=88dPA3YzMOBh2Dip |

En el vídeo se aborda cómo los ciberdelincuentes acceden a nuestros datos personales, destacando el uso de técnicas como el phishing, la ingeniería social y el malware. Se enfatiza la importancia de proteger la información personal en la era digital.

| **Robo de identidad virtual: ¿cómo protegernos?** |
|---|
| https://youtu.be/VDrWbjgM3Ik?si=ZsGCq4znqXMylOvH |

En este vídeo se describen los desafíos y amenazas que enfrenta el sector sanitario en relación con la protección de datos personales. Se destacan riesgos como accesos no autorizados, pérdida de datos, ataques cibernéticos y la importancia de cumplir con normativas de privacidad.

| **Principales riesgos de protección de datos en el sector sanidad** |
| --- |
| https://youtu.be/kqaMIFEz15s?si=vfWlFH2uQVbr4OlO |

### 5. 3 Enlaces Relevantes

El grupo de ciberdelincuentes Ransom House publicó en la dark web datos personales de pacientes y trabajadores del Hospital Clínic de Barcelona. La policía catalana logró impedir el acceso a los datos publicados, pero el incidente evidenció vulnerabilidades en la protección de datos del hospital. https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona

En noviembre de 2024, se publicó información sobre 750.000 pacientes de varios hospitales franceses pertenecientes a la entidad Aléo Santé en foros de la dark web. El ataque fue protagonizado por el actor de amenaza 'near2tlg', quien aseguró haber conseguido los datos de un millón y medio de pacientes a través de una brecha de seguridad en Mediboard. https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/datos-de-750000-pacientes-robados-en-francia

En 2024, los ciberataques al sector sanitario se incrementaron un 47%. La pandemia y el teletrabajo fueron factores que contribuyeron al aumento de la ciberdelincuencia en este sector. https://www.elespanol.com/reportajes/20250921/expediente-sanitario-eur-dark-web-hospitales-colapsados-operan-ladrones-datos-medicos/1003743921605_0.html

## 6. Bibliografía

European action plan on the cybersecurity of hospitals and healthcare providers. (2025, 8 agosto). Public Health. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal. https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Technologies, I. (2025, 7 abril). The 5 Most Alarming Healthcare Data Breaches You Need to Know. Infosprint Technologies. https://www.infosprint.com/blogs/cybersecurity/the-5-most-alarming-healthcare-data-breaches-you-need-to-know?

Park, E., & Lim, J. H. (2025). The impact of healthcare data breaches on patient hospital visit behavior. International Journal Of Research In Marketing. https://doi.org/10.1016/j.ijresmar.2025.01.004


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

**Co-funded by the European Union**







This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.