



SEGURIDAD DEL PACIENTE



Co-funded by
the European Union

*ESCAPE. Preparando a los profesionales sanitarios para los
ciberataques.*

Proyecto n.º 2023-1-ES01-KA220-VET-000151536

Socios



Firla

PRAMMER



ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.º 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

1. Definición	1
2. Importancia general	1
3. Importancia en la salud y la atención, e impacto en la calidad de la atención	1
4. ¿Qué puedo hacer como profesional de la salud?	1
5. Más información	
a. Materiales de aprendizaje	2
b. Vídeos relevantes	2
c. Enlaces relevantes	3
6. Bibliografía	3



Co-funded by
the European Union



FACTSHEET – SEGURIDAD DEL PACIENTE

1. Definición

La principal preocupación en la atención médica se refiere a evitar daños prevenibles a los pacientes y preservar su bienestar. Los incidentes cibernéticos pueden comprometer directamente la seguridad del paciente al retrasar o interrumpir los procedimientos y tratamientos médicos.

2. Importancia general

La seguridad del paciente impacta directamente la vida y el bienestar humanos, y es una prioridad de salud pública y el objetivo final de las medidas de ciberseguridad en la atención médica. Los errores en la atención médica pueden tener consecuencias catastróficas, como un aumento de la morbilidad y la mortalidad, y costos financieros significativos.

Según la Organización Mundial de la Salud, la atención insegura es una de las diez principales causas de muerte y discapacidad a nivel mundial, lo que hace que la seguridad del paciente sea un requisito fundamental para la confianza en la atención sanitaria².

3. Importancia en la salud y la atención, e impacto en la calidad de la atención

La seguridad del paciente, como explicamos en el punto anterior, es fundamental para mantener la confianza entre pacientes y profesionales, además de garantizar resultados efectivos del tratamiento.

Las prácticas inseguras pueden provocar daños a largo plazo, retrasos en la recuperación, discapacidad o la muerte. El daño a los pacientes en la atención médica es generalizado y problemático, y puede ocurrir en todos los entornos y niveles de la atención sanitaria.

Algunos factores que conducen al daño al paciente son:

Factores organizativos del sistema: la complejidad de las intervenciones médicas, procesos y procedimientos deficientes, interrupciones en el flujo de trabajo y en la coordinación de la atención, etc.

Factores tecnológicos: problemas con los registros médicos electrónicos o los sistemas de dispensación de medicamentos.

Factores humanos: no poder comunicarse, no trabajar bien juntos, cansancio, burnout...

Factores relacionados con el paciente: historial de salud limitado, falta de compromiso y no adherencia al tratamiento.

Factores externos: regulaciones inconsistentes, presiones financieras, etc.

4. ¿Qué puedo hacer como profesional sanitario?

Siga los protocolos de seguridad que incluyen higiene cibernética, verificación doble de medicamentos y seguimiento de las pautas clínicas. Reportar errores para evitar que vuelvan a ocurrir y promover una cultura de transparencia.

- Participe en la capacitación sobre prácticas seguras.



5. Más información

5.1 Materiales de aprendizaje

- [Sequential videos for general topics about cybersecurity \(JGT-2\)](#).
- [Cibersecurity guide for healthcare sector \(EU scope\) \(JGT-7\)](#).
- [An article on security strategies applicable to electronic patient records \(IST-37\)](#).
- [An infographic on security and cybersecurity devices used in different healthcare settings. \(IST-38\)](#).
- [An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. \(IST-39\)](#).
- [Cybersecurity of hospitals and healthcare providers \(BBS-24\)](#).
- [Cybersecurity in Hospitals - Legal Accountability when Patients are harmed \(BBS-26\)](#).
- [Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that \(PRAMMER-32\)](#).
- [Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach \(PRAMMER-35\)](#).

5.2 Vídeos relevantes

Según el vídeo, la seguridad del paciente implica evitar errores y lesiones a los pacientes durante la prestación de atención médica, enfatizando el valor de una cultura de seguridad, una comunicación clara y un desarrollo continuo para garantizar un tratamiento de primera calidad.

What is Patient Safety?

https://youtu.be/6Bbsqg2UMEE?si=qy5P8J5jNHWjn_0l

Este video muestra cómo escuchar las voces de los pacientes, sus familias y cuidadores puede contribuir a una atención médica más segura para todos. Visite el sitio web de la campaña para obtener más información y formas de participar.

World Patient Safety Day 2023: Engaging Patients for Patient Safety

<https://youtu.be/8P9ABYMsTuE?si=4m5VAAKBgQXRZHYP>

El video enfatiza que la seguridad del paciente y la mejora de la calidad son esenciales para la atención médica. Su objetivo es prevenir daños, optimizar los procesos de atención y garantizar mejores resultados para los pacientes mediante el aprendizaje continuo y la mejora del sistema.

Patient Safety & Quality Improvement

https://youtu.be/oU5m5rQIHC4?si=ScTu0XWi_3uUVb70



5. 3 Relevant Links

A woman died of sepsis four days after childbirth due to delayed antibiotic treatment. The event brought attention to the need for better sepsis protocols and faster response systems.

<https://trilliumhealthpartners.ca/>

Systemic failures and wrongdoing put patients at risk, which led to unnecessary surgeries and taking advantage of waiting lists. This case demonstrated the importance of transparent processes and organizational culture for safe care.

<https://www.childrenshealthireland.ie/your-hospital-visit/our-locations/chi-at-crumlin/>

6. Bibliography

New European Commission Action Plan on the Cybersecurity of the European Healthcare System is Much Needed - Trellix, fecha de acceso: agosto 13, 2025,

<https://www.trellix.com/blogs/perspectives/eu-action-plan-cybersecurity-healthcare/>

World Health Organization: WHO. (2019, 6 noviembre). Patient safety.

<https://www.who.int/health-topics/patient-safety>

World Health Organization: WHO. (2023, 11 septiembre). Patient safety.

<https://www.who.int/news-room/fact-sheets/detail/patient-safety>





5. 3 Enlaces relevantes

A woman died of sepsis four days after childbirth due to delayed antibiotic treatment. The event brought attention to the need for better sepsis protocols and faster response systems.

<https://trilliumhealthpartners.ca/>

Systemic failures and wrongdoing put patients at risk, which led to unnecessary surgeries and taking advantage of waiting lists. This case demonstrated the importance of transparent processes and organizational culture for safe care.

<https://www.childrenshealthireland.ie/your-hospital-visit/our-locations/chi-at-crumlin/>

6. Bibliografía

New European Commission Action Plan on the Cybersecurity of the European Healthcare System is Much Needed - Trellix, fecha de acceso: agosto 13, 2025,

<https://www.trellix.com/blogs/perspectives/eu-action-plan-cybersecurity-healthcare/>

World Health Organization: WHO. (2019, 6 noviembre). Patient safety.

<https://www.who.int/health-topics/patient-safety>

World Health Organization: WHO. (2023, 11 septiembre). Patient safety.

<https://www.who.int/news-room/fact-sheets/detail/patient-safety>





ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.º 2023-1-ES01-KA220-VET-000151536



Co-funded by
the European Union



ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Ni Weser

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.

