CIBERRESILIENCIA

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 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

Co-funded by the European Union

FACTSHEET – CIBERRESILIENCIA

1. Definición

Consiste en la capacidad de una organización para prepararse, responder y recuperarse de un ciberataque, garantizando, a su vez, la atención al paciente y la continuidad operativa. El enfoque se centra en minimizar las interrupciones causadas por los ciberataques y asegurar la privacidad de los datos más sensibles1.

Este concepto aúna la continuidad de la empresa, la seguridad de los sistemas de información y la resiliencia organizacional. Además, describe la capacidad de seguir ofreciendo los resultados previstos a pesar de los eventos cibernéticos adversos2.

2. Relevancia general

La ciberresiliencia adquiere una importancia significativa en el contexto de la creciente dependencia digital de la sociedad contemporánea. EEn la actualidad, los gobiernos, las empresas y los usuarios emplean sistemas digitales para llevar a cabo operaciones, facilitar comunicaciones y almacenar datos.Esta dependencia ha supuesto numerosos beneficios, tales como el acceso inmediato a información, la mejora en la coordinación de la atención y la optimización de recursos, entre otros. No obstante, se ha observado un incremento en las amenazas y ciberataques, tanto en términos de escala como de sofisticación. Esta situación ha llevado a que la prevención en ciberseguridad se convierta en una prioridad creciente.
Otro aspecto que enfatiza la importancia de la ciberresiliencia es su asunción de que las brechas son inevitables, y se centra no únicamente en la prevención, sino también en el modo de adaptarse, recuperarse y crecer tras los incidentes3.
Algunos beneficios de adoptar una perspectiva ciberresiliente3:

- **Continuidad del trabajo**: garantiza la persistencia de operaciones críticas durante ciberincidentes mediante la reducción de las interrupciones aun cuando las defensas convencionales se ven comprometidas.
- **Periodo de inactividad reducido**: reduce el tiempo y los recursos que se hubieran perdido durante interrupciones prolongadas, lo cual permite a las organizaciones recuperarse rápidamente de los ataques.
- **Protección financiera**: reduce los costes asociados a errores del sistema, filtraciones de datos y consecuencias legales potenciales que suelen acompañar a incidentes de seguridad graves.
- **Gestión de la reputación**: genera y mantiene la confianza de las partes interesadas demostrando la fiabilidad y capacidad de la organización para afrontar problemas de seguridad imprevistos.
- **Cumplimiento de la normativa**: garantiza que las prácticas organizacionales se ajusten a las leyes más estrictas. La ciberresiliencia enfatiza la creciente atención regulatoria que se presta a este tema.
- **Ventaja competitiva en el mercado**: al exhibir protocolos de seguridad robustos que distinguen a la compañía de competidores con menor preparación, se capta la atención de los clientes y socios interesados en la seguridad.

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

La sanidad moderna recurre en sistemas estrechamente conectados. Debido a la ingente cantidad de información sensible de pacientes que maneja y a la criticidad de sus operaciones, la industria sanitaria es un objetivo principal de los ciberdelincuentes4.

La resiliencia es crucial a la hora de prevenir interrupciones extensas de los servicios de salud, ya que basta con que uno de los componentes falle para que las consecuencias se extiendan por toda la infraestructura sanitaria. Tanto es así que las vidas de los pacientes pueden verse en peligro si afectan a sistemas sanitarios vitales, tales como historiales clínicos electrónicos o dispositivos médicos. Para proteger la seguridad y la privacidad del paciente, la ciberresiliencia se asegura de la continuidad en la atención al paciente incluso frente a los ataques.

Asimismo, la ciberresiliencia influye en el mantenimiento de la confianza de los pacientes, socios y el público general. Dado que los datos de los pacientes contienen información sumamente sensible, sus interrupciones o vulneraciones pueden dañar la reputación de las organizaciones sanitarias.

4. ¿Qué puedo hacer como profesional sanitario?

- Mantener una buena ciberhigiene. Aplicando medidas tales como contraseñas seguras, habilitar la autentificación en dos pasos y actualizar el software de manera regular.
- Proteger la información del paciente. Informa de cualquier actividad sospechosa y gestiona con cuidado la información en tu día a día.
- Participa en formación sobre ciberseguridad. Realiza formaciones en las que traten la prevención de filtraciones de datos, cómo detectarlas y mecanismos de respuesta.

5. Más información

5.1 Materiales de aprendizaje

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- Online workshop on how to set-up our device. (JGT-5)
- Cybersecurity for SMEs & self-employed (JGT-6)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An article on security strategies applicable to electronic patient records (IST-37)

5.2 Vídeos Relacionados

Este vídeo explica el concepto de ciberresiliencia, mostrando cómo las organizaciones deben no solo prevenir ataques, sino también estar preparadas para adaptarse, recuperarse y mantener sus operaciones críticas incluso ante incidentes cibernéticos.

¿Qué es ciberresiliencia?
https://youtu.be/xp9Onz0U8lg?si=7cnRFw-79ezjSwUM

El siguiente vídeo muestra una ponencia donde se realiza una sesión de preguntas y respuestas sobre ciberseguridad y ciberresiliencia aplicadas al ámbito sanitario. Se discuten desafíos reales, experiencias del sector salud y aprendizajes prácticos.

e+salud Día 2- Q&A Ciberseguridad y ciber-resiliencia en el sector salud. Lecciones aprendidas
https://www.youtube.com/watch?v=okukM3SpeG8

5. 3 Enlaces Relevantes

Este artículo analiza cómo las organizaciones de atención médica deben planificar cortes de red, posibles tiempos de inactividad de los registros médicos electrónicos e interrupciones de los sistemas médicos vitales en caso de un ataque sorpresa de ransomware.
https://health-isac.org/es/Ciberresiliencia-en-el-sector-sanitario%3A-mitigaci%C3%B3n-del-tiempo-de-inactividad-en-los-hospitales/

Se destaca la importancia de reforzar la ciberresiliencia en hospitales y centros de salud mediante medidas técnicas y organizativas, como el uso de sistemas de detección de comportamientos anómalos y la adopción de un sistema de operaciones de seguridad (SOC).
https://digitalinside.es/la-ciberresiliencia-la-mejor-aliada-del-sector-sanitario-ante-los-ciberataques/

Se presentan casos de empresas como Maersk, Sony Pictures y Target, que han enfrentado ciberataques significativos y han implementado estrategias de ciberresiliencia para superar las crisis y fortalecer su seguridad a largo plazo.
https://circulotne.com/empresas-que-han-superado-ciberataques-con-exito-revista-tne.html

6. Bibliografía

Susnjara, S., & Smalley, I. (2025, 13 agosto). Cyber Resilience. IBM. Recuperado 18 de agosto de 2025, de https://www.ibm.com/think/topics/cyber-resilience

Tashi, K., & Beato, F. (2024, 1 febrero). Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key. World Economic Forum. Recuperado 18 de agosto de 2025, de https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/?utm_source=chatgpt.com

What is Cyber Resilience and Why Does it Matter? | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cyber-resilience?utm_source=chatgpt.com

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.