CIBER-HIGIENE

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 – CIBER-HIGIENE

1. Definición

Se refiere a prácticas sencillas que todas las personas podemos adoptar para proteger nuestra información personal y nuestros dispositivos de ciberataques. Algunas de esas medidas incluyen la autentificación en dos pasos, contraseñas seguras, actualizar de manera regular el software, etc1.

2. Relevancia general

La mayoría de las brechas de seguridad se derivan del aprovechamiento de vulnerabilidades que han sido pasadas por alto por las prácticas actuales de ciberhigiene de la organización. La ciberhigiene es fundamental para garantizar la seguridad de los ordenadores, redes y datos frente a diversos riesgos de ciberseguridad, tales como el malware, el ransomware y otros tipos de ataques2.

La correcta operación de los sistemas es fundamental, ya que su eficiencia se ve directamente afectada por su adecuado funcionamiento. La ausencia de un mantenimiento adecuado puede comprometer el rendimiento general de los mismos. Así, la ciberhigiene previene las violaciones de datos y el robo de identidad, además de reducir los riesgos financieros, reputacionales y operativos2.

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

La ciberhigiene reviste de gran importancia en el cuidado de la salud debido a la sensibilidad de los datos de los pacientes y la dependencia de los sistemas digitales para el diagnóstico, tratamiento y comunicación entre profesionales. De manera similar a la higiene básica en la atención clínica, la higiene cibernética desempeña un papel fundamental en la prevención de incidentes cibernéticos. Las deficiencias en las medidas de seguridad pueden facilitar la ocurrencia de ataques de ransomware, los cuales tienen el potencial de interrumpir las operaciones de un hospital, provocar la filtración de información sensible, o poner en riesgo la seguridad del paciente si se comprometen los dispositivos médicos3.

El impacto en la calidad de la atención también implica una pérdida de confianza en las instituciones sanitarias, lo que puede disuadir a los pacientes a compartir información vital para su tratamiento. Por consiguiente, la conservación de una ciberhigiene adecuada no solo preserva la calidad de la atención, sino que también garantiza la seguridad del paciente y preserva la confianza pública.

4. ¿Qué puedo hacer como profesional sanitario?

- Emplear medidas preventivas, tales como contraseñas seguras y la autentificación en dos pasos.
- Actualizar de forma regular el software, aplicaciones y los dispositivos médicos.
- Estar alerta a posibles ciberataques (phishing emails, links sospechosos) e informar inmediatamente de cualquier irregularidad.
- Realizar formaciones sobre ciberseguridad y mantenerse al día sobre cómo se manifiestan este tipo de ataques en el trabajo diario.

5. Más información

5.1 Materiales de aprendizaje

- Cybersecurity for your sector (JGT-1)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- 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 overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- Educational project on safe and responsible digital use. (IST-41)
- IT Security Requirements and Protective Measures – Tips and Practical Examples (BBS-42)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- 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)
- This learning material highlights the growing role of media in the healthcare and welfare sector for both professional collaboration and client care, including attention to the consequences of media use among vulnerable groups (FIRDA-11)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-14)
- Digital training in cybersecurity, fun and fast questions (FIRDA-15)
- Free e-learning courses on cybersecurity in healthcare (FIRDA-17)
- Free courses to improve digital skills for health care workers (FIRDA-18)
- Online game about cybersecurity, raises awareness. (FIRDA-19)
- Online game about phishing (FIRDA-21)

5.2 Vídeos Relacionados

Este vídeo ofrece prácticas esenciales para proteger la información digital en entornos laborales, enfocándose en la importancia de contraseñas seguras, actualizaciones periódicas y precauciones frente a correos electrónicos sospechosos.

Recomendaciones de Ciberhigiene
https://youtu.be/8Z5mJXs8L4U?si=864oIyEnVM02ePia

5. 3 Enlaces Relevantes

Este artículo destaca la importancia de la formación en ciberseguridad para el personal sanitario, enfatizando que los trabajadores son los guardianes de los datos y que la concienciación es esencial para prevenir ciberataques.
https://www.metacompliance.com/es/blog/cyber-security-awareness/concienciacion-sobre-ciberseguridad-y-el-sector-sanitario

Se discuten estrategias clave para proteger los datos médicos, incluyendo la gestión segura de contraseñas y la implementación de medidas de seguridad en dispositivos médicos conectados
https://www.cipher.com/es_ES/blog/cipher/ciberseguridad-sector-salud

Este artículo ofrece una guía práctica para profesionales de la salud sobre cómo implementar medidas básicas de ciberseguridad para proteger la información digital de los pacientes.
https://www.splashtop.com/es/blog/importance-of-cybersecurity-in-healthcare

6. Bibliografía

Cyber Hygiene | ENISA. (2018, 18 enero).
https://www.enisa.europa.eu/topics/cyber-hygiene

What is Cyber Hygiene? Definition & Best Practices. (2025, 21 marzo). SecurityScorecard.
https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

World Health Organization. (2025, 26 marzo). WHO/ Europe launches guide to strengthen cybersecurity in digital health.
https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

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.