SEGURIDAD EN LA NUBE

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

ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 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 – SEGURIDAD EN LA NUBE

1. Definición

Se refiere a una serie de políticas, controles, procedimientos y tecnologías cuyo propósito es proteger los sistemas, datos e infraestructura en la nube. Aborda cuestiones como la privacidad de los datos, la gestión de identidades y accesos, el cumplimiento normativo y la resiliencia ante ciberataques derivados de la «nubización» de los datos de los pacientes en el ámbito sanitario.

2. Importancia general

La seguridad en la nube es un área de creciente preocupación a medida que el sector sanitario adopta cada vez más servicios en la nube para el almacenamiento y procesamiento de datos, lo que requiere directrices y prácticas de seguridad específicas.[1] Las ciberamenazas, las brechas de seguridad o las configuraciones incorrectas pueden exponer información confidencial sin una protección sólida en la nube. Debido a su naturaleza compartida, una falla de seguridad puede afectar a millones de usuarios simultáneamente, causando no solo daños financieros y de reputación, sino también comprometiendo el cumplimiento de los marcos legales (RGPD en Europa o HIPAA en EE. UU.).

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

La necesidad de tecnología en entornos clínicos ha aumentado recientemente; la computación en la nube, la telemedicina, la inteligencia artificial y la salud electrónica a menudo pueden ofrecer servicios superiores2. Además, el uso de la tecnología en la nube en los historiales clínicos electrónicos facilita a los pacientes un acceso amplio y sin esfuerzo a su información médica. El uso de la tecnología en la nube transforma la forma en que médicos, enfermeros, clínicas y hospitales brindan a los pacientes servicios de alta calidad y financieramente rentables3.

La computación en la nube ofrece varias ventajas, como la colaboración sencilla y cómoda entre usuarios, la reducción de costes, el aumento de la velocidad, la escalabilidad y la flexibilidad3. Sin embargo, a pesar de sus numerosos beneficios, también presenta algunos aspectos negativos y desafíos. La computación en la nube también conlleva mayores riesgos, que pueden provocar que una vulneración o una interrupción en un sistema alojado en la nube exponga información altamente sensible, retrase el tratamiento o incluso interrumpa los servicios de emergencia4.

4. ¿Qué puedo hacer como profesional sanitario?

Utilice un acceso seguro iniciando sesión a través de plataformas en la nube de hospitales autorizadas con contraseñas seguras y autenticación de dos factores.

Evite compartir archivos con información personal fuera del sistema de nube oficial.

- Esté alerta ante amenazas cibernéticas (correos electrónicos de phishing, enlaces sospechosos) e informe de inmediato cualquier irregularidad.

- Participe en la capacitación sobre ciberseguridad y manténgase al día sobre cómo responder ante incidentes y el impacto de la protección de datos de los pacientes.

5. Más información

5.1 Materiales de aprendizaje

- Cybersecurity for SMEs & self-employed (JGT-6)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- 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)
- 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)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-13)

5.2 Vídeos relevantes

Este video habla sobre el modelo de responsabilidad compartida para entornos de nube. Explica que las empresas son responsables de mantener sus aplicaciones, cargas de trabajo y datos seguros, mientras que el proveedor de la nube es responsable de la seguridad de la infraestructura que los respalda.

What is Cloud Security?
https://youtu.be/jI8IKpjiCSM?si=vXJzAbIsRoj2ltDh

El siguiente video muestra cómo se utiliza la computación en la nube en el ámbito sanitario, sopesando sus ventajas, como un mejor acceso y escalabilidad, frente a sus desventajas, como los riesgos a la privacidad de los datos y las posibles dependencias del sistema.

Cloud Computing in Healthcare: The Pros and Cons
https://youtu.be/xEl_6NZuyS4?si=cFApA9QgHFCEBzPi

5. 3 Enlaces relevantes

This article describes how a misconfiguration in the Health Service Executive's Salesforce-based vaccination portal exposed the personal and vaccination details of over one million Irish citizens, as well as internal HSE documents.

https://appomni.com/blog/saas-risks-in-healthcare-data-exposure-in-hse/

According to this article, a cloud database left publicly accessible revealed nearly 957,000 healthcare-related records, including sensitive staff and recruitment information—due to a lack of password protection.

https://www.cybersecurity-insiders.com/cloud-security-breach-leads-to-a-leak-of-957000-patient-records/

A Finnish psychotherapy company had a big data breach that made private therapy records public. The breach, which led to the clinic and its patients being extorted, cost the clinic €608,000 under GDPR for poor security and not reporting the breach in a timely manner. The fallout had a big effect on patients' trust and mental health.

https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/

6. Bibliografía

Liveri, D., Athanasios, D., & Zisi, A. (2021). ENISA Cloud Security for the Healthcare Services. Enisa.
https://doi.org/10.2824/454966

Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors, 20(18), 5392.
https://doi.org/10.3390/s20185392

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal Of Medicine And Life, 14(4), 448-461.
https://doi.org/10.25122/jml-2021-0100

Guidance on HIPAA & Cloud Computing. (2022, diciembre). U.S. Department Of Health And Human Services. Recuperado 28 de agosto de 2025, de

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

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.