ENSEÑANZAS PROPIAS DE POSTGRADO
GUÍA DOCENTE

Destinatario:	Servicio de Ordenación Académica

Denominación del Módulo (o Materia/Asignatura)	**Carácter**
Módulo 4: Ciberseguridad en el Sector Sanitario (2 créditos)	X Obligatorio ☐Optativo

Responsable del Módulo (o Materia/Asignatura) (nombre, filiación y datos de contacto profesional)

Enrique Rando González. Director del Centro de Ciberseguridad de Andalucía.

Duración y fecha inicial y final de realización	Desde 26 de noviembre hasta 20 de diciembre. Duración: 4 semanas.

Requisitos previos (en su caso)

Licenciados o graduados universitarios en la rama sanitaria.

Modalidad de enseñanza

☐Presencial	☐Semipresencial	X Virtual

Objetivos, competencias y resultado del aprendizaje

Objetivos:

- Identificar los desafíos y riesgos de ciberseguridad específicos para el sector sanitario.
- Desarrollar estrategias de protección y respuesta ante incidentes de ciberseguridad.

Competencias

- Identificación de Amenazas y Vulnerabilidades: Comprensión de las principales amenazas y vulnerabilidades que enfrentan los sistemas de información en salud, incluyendo ataques de malware, phishing, ransomware y otras formas de ciberataques específicos del sector sanitario.
- Estrategias de Protección en Ciberseguridad: Conocimiento de las estrategias y herramientas fundamentales para proteger los sistemas de salud, incluyendo el cifrado de datos, la autenticación fuerte y la seguridad en dispositivos médicos conectados.
- Gestión de Respuesta y Recuperación ante Incidentes: Habilidad para diseñar, implementar y gestionar planes de respuesta a incidentes cibernéticos y de recuperación de desastres, asegurando la resiliencia de los sistemas de salud frente a ataques.
- Cumplimiento Normativo y Mejores Prácticas: Conocimiento de las regulaciones y normativas relevantes para la ciberseguridad en el sector sanitario (como HIPAA, GDPR en el contexto europeo, y otras normativas locales), así como las mejores prácticas en el ámbito.
- Conciencia y Formación en Ciberseguridad: Capacidad para promover la conciencia y formación en ciberseguridad entre el personal de salud, reconociendo el papel crítico que juegan en la prevención de incidentes cibernéticos.

Resultados

- Capacidad para Proteger Sistemas de Salud: Los estudiantes estarán preparados para implementar medidas de seguridad efectivas, protegiendo contra amenazas y mitigando vulnerabilidades en los sistemas de información de salud.

- Desarrollo de Planes de Respuesta a Incidentes: Los participantes podrán desarrollar y ejecutar planes de respuesta a incidentes cibernéticos, minimizando el impacto de los ataques y restableciendo rápidamente los servicios críticos.
- Gestión de la Recuperación de Desastres: Los alumnos estarán equipados para diseñar e implementar estrategias de recuperación de desastres, asegurando la continuidad de las operaciones sanitarias incluso después de incidentes de seguridad significativos.
- Promoción del Cumplimiento Normativo: Los estudiantes comprenderán y aplicarán las regulaciones y normativas relevantes para la ciberseguridad en el sector sanitario, promoviendo el cumplimiento y la protección de los datos de pacientes.
- Fomento de una Cultura de Seguridad: Los participantes serán capaces de fomentar una cultura de seguridad entre el personal de salud, educando sobre prácticas seguras y la importancia de la ciberseguridad en la protección de la información del paciente.

Contenidos y bibliografía

Módulo 4: Ciberseguridad en el Sector Sanitario (2 créditos)

- Amenazas y vulnerabilidades en sistemas de salud.
- Estrategias de protección: cifrado, autenticación, seguridad de dispositivos médicos.
- Respuesta y recuperación ante incidentes: planes de respuesta a incidentes, recuperación de desastres.

Bibliografía:

1. **Digital technologies: shaping the future of primary health care. World Health Organization. URL: https://www.who.int/ docs/default-source/primary-health-care-conference/digital-technologies.pdf [accessed 2022-12-01]**
2. **Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res 2018 May 28;20(5):e10059 [FREE Full text] [doi: 10.2196/10059] [Medline: 29807882]**
3. **Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, Baskerville RL. How can organizations develop situation awareness for incident response: a case study of management practice. Comput Security 2021 Feb;101:102122 [FREE Full text] [doi: 10.1016/j.cose.2020.102122]**
4. **Alami H, Gagnon MP, Ag Ahmed MA, Fortin JP. Digital health: cybersecurity is a value creation lever, not only a source of expenditure. Health Policy technol 2019 Dec;8(4):319-321 [doi: 10.1016/j.hlpt.2019.09.002]**
5. **Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018 Jul;113:48-52 [FREE Full text] [doi: 10.1016/j.maturitas.2018.04.008] [Medline: 29903648]**
6. **Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. 2020. URL: https:/ /cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects% 20global%20cybercrime,%243%20trillion%20USD%20in%202015 [accessed 2021-09-12]**
7. **Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity risks in a pandemic. J Med Internet Res 2020 Sep 17;22(9):e23692 [FREE Full text] [doi: 10.2196/23692] [Medline: 32897869]**
8. **Ireland's health service executive ransomware attack (2021). Creative Commons Attribution-ShareAlike 4.0 International. 2021. URL: https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s_Health_Service_Executive_ransomware_attack_(2021) [accessed 2022-02-02]**
9. **Hackers shut down system for booking COVID-19 shots in Italy's Lazio region. euronews. 2021. URL: https://www. euronews.com/2021/08/02/us-health-coronavirus-italy [accessed 2022-02-04]**

10. **Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR Mhealth Uhealth 2020 Jun 18;8(6):e18175 [FREE Full text] [doi: 10.2196/18175] [Medline: 32554388]**
11. **Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Factors influencing the decision to proceed to firmware upgrades**
12. **to implanted pacemakers for cybersecurity risk mitigation. Circulation 2018 Sep 18;138(12):1274-1276 [doi:**
13. **10.1161/circulationaha.118.034781]**
14. **Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber**
15. **security within healthcare organisations: a systematic review. Sensors (Basel) 2021 Jul 28;21(15):5119 [FREE Full text]**
16. **[doi: 10.3390/s21155119] [Medline: 34372354]**

Número de créditos ECTS

- Créditos teóricos:2
- Créditos prácticos: 0
- Distribución de horas de trabajo del estudiante:
  - Nº total de horas: 50

☐Clases Teóricas: 20 ☐Clases Prácticas: 0

☐Tutorías Especializadas (virtuales):
- Colectivas: 5
- Individuales: 0

☐Realización de Actividades Académicas Dirigidas:
- Con presencia del profesor: 0
- Sin presencia del profesor: 5

☐Otras actividades (especificar):
- Intervención en foros: 2
- Atención de correos y chats: 2
- Preparación de clases: 15
- Realización de ejercicios prácticos: 0
- Exámenes: 1

Cronograma de desarrollo docente

Módulo 4, Ciberseguridad en el Sector Sanitario

Materia/Asignatura: Amenazas y vulnerabilidades en sistemas de salud

Profesor	Nº ECTS presenciales	Nº ECTS virtuales	Fecha inicio	Fecha final	Horarios
Dr. Rando		**0,5**	**26/11/24**	**30/11/24**	

Materia/Asignatura: Estrategias de protección: cifrado, autenticación, seguridad de dispositivos médicos

Profesor	Nº ECTS presenciales	Nº ECTS virtuales	Fecha inicio	Fecha final	Horarios
Dr. Rando		**1**	**01/12/24**	**05/12/24**	

Materia/Asignatura: Respuesta y recuperación ante incidentes: planes de respuesta a incidentes, recuperación de desastres

Profesor	Nº ECTS presenciales	Nº ECTS virtuales	Fecha inicio	Fecha final	Horarios

Dr. Rando		**0,5**	**10/12/14**	**15/12/24**	
CUESTIONARIO FINAL DE EVALUACIÓN		**0**	**26/11/24**	**15/12/24**	
CUESTIONARIO FINAL DE EVALUACIÓN DE LOS 4 MÓDULOS		**0**	**15/12/2024**	**20/12/2024**	

Sistema de evaluación

Existirá una evaluación final a través de un cuestionario tipo test de 20 preguntas autoevaluables que deberá ser superado por los alumnos para obtener la certificación oficial. Además, el cuestionario final que engloba los 4 módulos se realizará a través de la metodología de un test autoevaluable de 50 preguntas que deberá ser superado por los alumnos para obtener la certificación oficial.

Observaciones

En __Málaga_____, a__14___de _febrero_____ de _____2024___.

Fdo.: Dr. José Antonio Trujillo Ruíz. Vicepresidente Colegio de Médicos de Málaga.

Deberá cumplimentarse una Guía por cada módulo (o materia/asignatura, en el caso de que el programa de estudios no esté estructurado en módulos).

ENSEÑANZAS PROPIAS DE POSTGRADO
GUÍA DOCENTE

Deberá cumplimentarse una Guía por cada módulo (o materia/asignatura, en el caso de que el programa de estudios no esté estructurado en módulos).