universidad de león

Guía Docente 2025-2026

1746014 - CIBERSEGURIDAD INDUSTRIAL I
Máster Universitario de Investigación en Ciberseguridad

Datos Generales

Curso: Primero
Semestre: Primero
Modalidad: Online
Créditos totales: 3
Idioma: CASTELLANO
English Friendly: No
Web: http://agora.unileon.es

Profesor/a responsable: MANUEL DOMÍNGUEZ GONZÁLEZ (mdomg@unileon.es)

Otro profesorado: JOSÉ RAMÓN RODRÍGUEZ OSSORIO (jrodro@unileon.es), MIGUEL ANGEL PRADA MEDRANO (mapram@unileon.es)

El profesorado que figura en esta guía docente puede ser modificado conforme a lo previsto en la normativa que regula el Procedimiento de Elaboración y Modificación de Planes Docentes de la Universidad de León.

Descripción general: Esta asignatura tiene como objetivo presentar al alumno las arquitecturas, tecnologías y protocolos de comunicación empleados en los sistemas de automatización industrial, así como los principios básicos de la ciberseguridad industrial. La asignatura se estructura en cinco temas: Peculiaridades de los sistemas de control industrial desde el punto de vista de la seguridad. Amenazas y vulnerabilidades en sistemas de control industrial e infraestructuras críticas. Iniciativas y estándares. Revisión crítica de incidentes relevantes. Introducción a los procedimientos y medidas de seguridad en el ámbito de los sistemas de control industrial.

Resultados del aprendizaje

Descripción	Tipo A	Tipo B	Tipo C
Conocimiento de las amenazas y vulnerabilidades de seguridad específicas en los entornos industriales y de infraestructuras críticas.	A18816	B5730 B5740	C4 C2
Conocimiento de las principales iniciativas, programas y procedimientos en seguridad enfocadas a sistemas, redes y aplicaciones en entornos industriales.	A18816	B5729 B5732 B5731	C2 C4 C5

Tipo	Código	Descripción
Tipo A - Competencias Específicas	A18816	Conocer las amenazas y vulnerabilidades de seguridad específicas en los entornos industriales y de infraestructuras crítucas. Conoce las principales iniciativas, programas y procedimientos en seguirdad enfocadas a sistemas, redes y aplicaciones en entornos industriales. / Knowing the specific threats ans security vulnerabilities in industrial and critical infrastructure environments. Knowing the main initiativas, programs and procedures of security focused to systems, networks and applications in industry environments.
Tipo B - Competencias Generales y Transversales	B5729	Elaborar y defender argumentos y resolver problemas dentro del área de seguridad informática y de las comunicaciones./ Developing and defending arguments and resolving problems in the field of computer and communications security.
Tipo B - Competencias Generales y Transversales	B5732	Transmitir soluciones al entorno industrial y empresarial en el campo de la ciberseguridad./ Convey solutions to the industrial and corporate environment in the field of cybersecurity.
Tipo B - Competencias Generales y Transversales	B5731	Emitir juicios sobre temas relevantes de índole social, científica o ética desde la perspectiva de la ciberseguridad./ Judging relevant subjects of social, scientific, or ethical nature from a cybersecurity perspective.
Tipo B - Competencias Generales y Transversales	B5730	Reunir e interpretar datos relevantes dentro del área de seguridad informática y de las comunicaciones/Collecting and understanding relevant data in the field of computer and communications security.
Tipo B - Competencias Generales y Transversales	B5740	Aprender de forma autónoma./Self-learning ability.

Continúa en la página siguiente

Viene de la página anterior

Tipo	Código	Descripción
Tipo C - Competencias Básicas	C2	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
Tipo C - Competencias Básicas	C4	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
Tipo C - Competencias Básicas	C5	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

Contenido

Bloque	Tema
I. Peculiaridades de los sistemas de control industrial desde el punto de vista de la seguridad	T1. Introducción y revisión de conceptos. T2. Arquitecturas y tecnologías.
II. Amenazas y vulnerabilidades en sistemas de control industrial e infraestructuras críticas	T3. Amenazas. T4. Vulnerabilidades. T5. Impacto. Riesgo.
III. Iniciativas y estándares	T6. Legislación europea y española. Entidades relevantes y fuentes de recomendaciones e información. T7. Estándares. IEC-62443.
IV. Revisión crítica de incidentes relevantes.	T8. Incidentes.
V. Introducción a los procedimientos y medidas de seguridad en el ámbito de los sistemas de control industrial.	T9. Políticas y procedimientos. Privilegios y autenticación. T10. Medidas de seguridad física. Medidas de seguridad de los equipos T11. Seguridad de red.

Metodologías

Título	Descripción	Horas en clase	Horas fuera de clase	Horas totales
Practicas con ordenadores	Aplicar, a nivel práctico, la teoría de un ámbito de conocimiento en un contexto determinado. Ejercicios prácticos a través de las TIC.	10	18	28
Tutorías	Tiempo que cada profesor tiene reservado para atender y resolver dudas del alumnado de forma individual o grupal.	1	0	1
Presentaciones/ exposiciones	Exposición oral por parte de los alumnos de un tema concreto o de un trabajo.	2	13	15
Sesión Magistral	Exposición de los contenidos de la asignatura	12	19	31

Continúa en la página siguiente

Viene de la página anterior

Título	Descripción	Horas en clase	Horas fuera de clase	Horas totales
Total		25	50	75

Tutorías

Los estudiantes pueden contar con la ayuda del profesor en tutorías individuales o grupales, previa petición por e-mail.

Evaluación

Estrategia de evaluación	Descripción	Porcentaje
Pruebas objetivas de tipo test	El examen podrá incluir preguntas relacionadas tanto con la teoría como con la práctica.	60 %
Pruebas prácticas	Evaluación de las prácticas	20 %
Trabajos	Realización y presentación de trabajo de la asignatura	20 %
Total		100 %

Otros comentarios y segunda convocatoria: Para aprobar la asignatura es necesario alcanzar un mínimo de 3,5 puntos sobre 7 en el examen escrito, un mínimo de 1,5 en la evaluación del trabajo y una nota final de al menos 5 puntos.

EVALUACIÓN EN LA SEGUNDA CONVOCATORIA:

Nota del examen escrito: 70 % Nota del trabajo: 30 %

Fuentes de información

Referencias
Autor principal/secundarios: International Society of Automation **Título:** Searchable List of ISA Standards **Fecha de publicación:** 2022 **URL:** https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order
Autor principal/secundarios: Knapp, Eric D. Samani, Raj,; Langill, Joel, **Título:** Applied cyber security and the smart grid : implementing security controls into the modern power infrastructure **Datos de publicación:** Amsterdam ;; Boston :; Waltham, MA :: Elsevier/Syngress; Syngress, 2013. **ISBN:** 1-299-40881-8; 0-12-404638-X ☆

Continúa en la página siguiente

Viene de la página anterior

Referencias

Autor principal/secundarios: Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, Michael Thompson
Título: NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security
Editorial: U.S. Department of Commerce
Fecha de publicación: 28/09/2023

Autor principal/secundarios: S2 Grupo
Fecha de publicación: 2016
Título: Informe de Amenazas CCN-CERT IA-04/16: amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS)
Título de la revista:
Páginas -

Autor principal/secundarios: Cybersecurity & Infrastructure Security Agency
Título: Cybersecurity & Infrastructure Security Agency
Fecha de publicación:
URL: https://ics-cert.us-cert.gov/

Autor principal/secundarios: National Cybersecurity and Communications Integration Center
Título: Cibersecurity & infraestructure security agency
Editorial: United States Goverment

Autor principal/secundarios: Knapp, Eric D. Langill, Joel Thomas
Título: Industrial network security : securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems
Datos de publicación: Waltham, MA :: Syngress, [2015]
ISBN: 978-0-12-420114-9

Recomendaciones

Código	Curso	Semestre	Nombre

Comentarios: Se recomienda cursar previa o simultáneamente Fundamentos de la Ciberseguridad, la Ciberdefensa y el Cibercrimen y Seguridad en Sistemas Ciberfísicos.