

DATOS IDENTIFICATIVOS				
Ciberseguridad en entornos industriales				
Asignatura	Ciberseguridad en entornos industriales			
Código	V05M175V01209			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel			
Correo-e	mcacho@uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530014&any_academic=2021_22			
Descripción general	El concepto de la Industria 4.0 dio lugar a que cada vez sean más los dispositivos industriales conectados a la rede y a procesos físicos. Esta asignatura, además de repasar los sistemas industriales tradicionales (i.e., sistemas de control industrial, control de accesos, sistemas de comunicaciones o de gestión de la información), se enfocará en la seguridad de las tecnologías de la Industria 4.0: sistemas IoT/IIoT, sistemas robotizados, cloud/edge computing, realidad aumentada, blockchain o AGVs.			

Competencias
Código

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Introducción	Políticas de seguridad industrial Implicaciones de la ciberseguridad industrial y de infraestructuras críticas Casos prácticos
Sistemas de control de acceso físico a dependencias industriales	Sistemas de proximidad Sistemas de acceso remoto Sistemas biométricos
Sistemas de control industrial	Arquitecturas de comunicaciones Sistemas tradicionales Sistemas ciberfísicos

Sistemas de la Industria 4.0	Introducción a la Industria 4.0 Sistemas IoT/IIoT Seguridade en otras tecnologías 4.0 (e.g., realidad aumentada, cloud/edge computing, blockchain, AGVs)
Sistemas de gestión de información en entornos industriales	Bases de datos tradicionales ERPs PLMs Sistemas MES
Sistemas de comunicaciones industriales	Arquitectura de comunicaciones Tecnologías de comunicación cableadas Tecnologías de comunicación inalámbricas

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Prácticas con apoio de las TIC (Repetida, non usar)	10	10	20
Trabajo tutelado	0	20	20
Lección magistral	9	9	18
Examen de preguntas objetivas	1	15	16
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías	
	Descripción
Prácticas con apoio de las TIC (Repetida, non usar)	Realización por parte del alumnado de prácticas guiadas y supervisadas.
Trabajo tutelado	Realización por parte del alumnado de trabajos de componente tanto teórica como práctica.
Lección magistral	Exposición por parte del profesorado de los principales contenidos teóricos relacionados con la ciberseguridad en contornos industriales.

Atención personalizada	
Metodologías	**Descripción**
Prácticas con apoio de las TIC (Repetida, non usar)	Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Asimismo, los profesores orientarán y guiarán a los alumnos durante la realización de las tareas que tengan asignadas, tanto en las prácticas como en los distintos trabajos tutelados. Las dudas se atenderán ya sea durante las propias clases o durante el horario establecido para tutorías. Se buscará flexibilizar dicho horario para atender las dudas del alumnado con reconocimiento de dedicación a tempo parcial y dispensa académica de exención de asistencia.

Evaluación			
	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas con apoio de las TIC (Repetida, non usar)	Resolución de prácticas y realización de informes con los resultados obtenidos.	30	
Trabajo tutelado	Realización de un trabajo con parte teórica y parte práctica.	30	
Examen de preguntas objetivas	Examen escrito sobre los contidos teóricos y prácticos impartidos durante el curso.	40	

Otros comentarios sobre la Evaluación

PRIMERA OPORTUNIDAD

Se ofrecerán dos alternativas de evaluación: continua y única.

La evaluación contínua implicará la realización de las prácticas, de un trabajo tutelado y una prueba mixta que serán evaluados en los porcentajes arriba indicados (30, 30, 40), siendo necesario obtener un cinco sobre diez en la evaluación

total. Igualmente, será necesario obtener un dos sobre cuatro en la prueba mixta para poder aprobar la asignatura. En caso de optar a la evaluación continua, el alumnado que realice cualquier tipo de entrega (práctica, trabajo, prueba mixta), no podrá calificarse como "no presentado".

En el caso de la evaluación única, toda la puntuación vendrá dada por una única prueba mixta que incluirá parte teórica y práctica. Dicha prueba se realizará al final del bimestre y deberá obterse en total al menos un cinco sobre diez para poder aprobar la asignatura.

La selección de la alternativa de evaluación deberá indicarse como muy tarde al final de la segunda semana de clase.

Para cualquiera de las dos alternativas se facilitará flexibilidad horaria para el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia.

SEGUNDA OPORTUNIDAD Y CONVOCATORIAS EXTRAORDINARIAS

Los alumnos que hayan optado en la primera oportunidad por la evaluación continua tendrán la opción de conservar las notas de prácticas y trabajos tutelados realizados durante el curso académico. Dicho alumnado realizará una prueba mixta, estableciéndose la nota en los porcentajes indicados arriba (30, 30, 40). El resto de alumnos (incluido el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia) se tratarán como alumnos de evaluación única y realizarán una prueba mixta que mezcle parte teórica y práctica.

OTROS COMENTARIOS

No se conservará ninguna de las notas obtenidas para los cursos académicos posteriores.

En el caso de detección de plagio durante alguna de las entregas, se calificará al alumno/a con suspenso (0) y se comunicará la situación a la dirección del máster y a las autoridades universitarias correspondientes de cara a tomar las medidas oportunas.

Fuentes de información

Bibliografía Básica

Eric Knapp, Joel Thomas Langill, **Industrial Network Security.**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, IGI Global, 2012

Tyson Macaulay, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity**, Packt, 2017

Bibliografía Complementaria

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, CRC Press, 2016

Recomendaciones

Plan de Contingencias

Descripción

=== MEDIDAS EXCEPCIONALES PLANIFICADAS ===

ESCENARIO 1: DOCENCIA MIXTA

Debido a la situación excepcional, ante la imposibilidad de poder impartir la docencia de un modo completamente presencial, se utilizarán medios virtuales para la impartición de las clases no presenciales.

Para la parte no presencial se utilizarán los medios proporcionados por la Universidad, actualmente el "Campus Remoto" y FAITIC. No obstante se podrá complementar con otros medios.

ESCENARIO 2: DOCENCIA NO PRESENCIAL

Debido a la situación excepcional, ante la imposibilidad de poder impartir la docencia de un modo presencial, se utilizarán medios virtuales para la impartición de las clases.

Se utilizarán los medios proporcionados por la Universidad, actualmente el "Campus Remoto" y FAITIC. No obstante se podrá complementar con otros medios.

=== ADAPTACIÓN DE LAS METODOLOGÍAS ===

Para las prácticas de laboratorio, se sustituirán las prácticas que requieran de equipamiento específico por otro simulado o virtualizado. Eventualmente se propondrán prácticas alternativas que no requieran de dicho equipamiento. Estas prácticas podrán tener un formato autónomo en previsión de problemas de conciliación y/o conectividad.

Las sesiones de tutorización (atención al alumnado) se realizarán por medios telemáticos (Correo electrónico, Foros de FAITIC, Campus Remoto), que se podrán complementar entre sí y con otras herramientas. En algunas de ellas se utilizará una modalidad de concertación previa.

=== ADAPTACIÓN DE LA EVALUACIÓN ===

La evaluación mantendrá la misma metodología, siendo el examen una prueba online utilizando Campus Remoto y FAITIC.