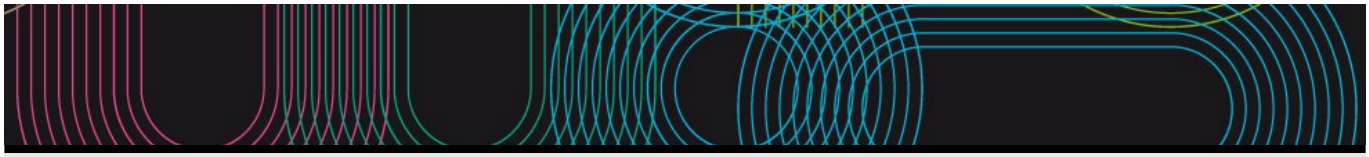

DATOS IDENTIFICATIVOS				
Ciberseguridade industrial e IoT				
Asignatura	Ciberseguridade industrial e IoT			
Código	V05M175V11213			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano Gallego			
Departamento	Dpto. Externo Ingeniería de sistemas y automática Ingeniería telemática			
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel Gil Castiñeira, Felipe José			
Correo-e	mcacho@uvigo.es			
Web	http://www.moovi.gal			
Descripción general	Los dispositivos inteligentes nos están prestando cada vez más servicios casi sin que nos demos cuenta de su presencia: el coche ha dejado de ser una simple máquina mecánica para convertirse en un sistema conectado con un enorme control electrónico; en los hoteles ya no usamos llave, sino que podemos abrir nuestra habitación con una tarjeta o nuestro teléfono móvil; Nuestros termostatos domésticos se pueden conectar a un servicio de pronóstico del tiempo y ajustarse al clima en las próximas horas. Los entornos industriales son casos de uso particularmente importantes, ya que la conexión en red de dispositivos que miden y controlan procesos permite la Industria 4.0. Todos son ejemplos de las aplicaciones habilitadas por tecnologías "integradas", redes de comunicaciones inalámbricas y, en última instancia, "Internet de las cosas" (IoT). Esta asignatura analiza los problemas y las mejores prácticas para hacer que este tipo de sistemas sean seguros, con especial énfasis en la seguridad de las tecnologías de la Industria 4.0, como los sistemas IoT/IioT, los sistemas robóticos, la computación en la nube/borde, la realidad aumentada, la cadena de bloques o los AGV.			

Resultados de Formación y Aprendizaje	
Código	
B9	Identificar la arquitectura de los sistemas IoT, su complejidad y sus vulnerabilidades, así como comprender la seguridad en el ámbito los sistemas empotrados y los sistemas de comunicación IoT.
C9	Analizar las implicaciones del nivel de seguridad de tecnologías relacionadas con la digitalización de los sectores de producción, así como valorar y modelar amenazas y ejecutar ataques con el objetivo de diseñar sistemas IoT seguros.
D2	Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
D5	Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones.
D7	Aplicar políticas de seguridad e implementar las diferentes técnicas de protección en base a la comprensión de los ataques en sistemas industriales para minimizar las problemáticas de seguridad y los ataques a redes de control industrial.

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

RA01. Comprender la ejecución de políticas de seguridad y sus implicaciones en entornos industriales.	B9 C9 D7
RA02. Comprender las diferentes técnicas de protección y ataque en sistemas industriales y saber cómo se pueden implementar.	B9 C9 D2 D5 D7
RA03. Entender las problemáticas de seguridad y los ataques a redes de control industrial y conocer los mecanismos que permiten minimizarlos.	B9 C9 D5 D7
RA04. Conocer e identificar la arquitectura de los sistemas IoT, su complejidad y sus vulnerabilidades	B9
RA05. Comprender la seguridad en el ámbito de los sistemas empotrados	B9 C9 D2 D5 D7
RA06. Comprender la seguridad en el ámbito de los sistemas de comunicación IoT.	B9 C9 D5
RA07. Conocer casos reales de ataques a sistemas IoT.	B9 D7
RA08. Ser capaz de comprender las implicaciones a nivel de seguridad de tecnologías relacionadas con conceptos como la Industria 4.0/5.0.	B9 C9 D5 D7
RA09. Ser capaz de valorar y modelar amenazas y ejecutar ataques sobre un sistema IoT	B9 C9 D2
RA10. Ser capaz de diseñar sistemas IoT seguros	B9 C9 D2 D5 D7

Contenidos

Tema	
Introducción a la ciberseguridad industrial.	Introducción a la ciberseguridad industrial.
Introducción a los sistemas ciberfísicos e IoT: hardware, firmware, comunicaciones y cloud	Introducción a los sistemas ciberfísicos e IoT: hardware, firmware, comunicaciones y cloud
Ciberseguridad de sistemas de control y comunicaciones industriales.	Ciberseguridad de sistemas de control y comunicaciones industriales.
Ciberseguridad de tecnologías de la Industria 4.0/5.0.	Ciberseguridad de tecnologías de la Industria 4.0/5.0.
Ciberseguridad de dispositivos IoT/IIoT: hardware, firmware y middleware.	Ciberseguridad de dispositivos IoT/IIoT: hardware, firmware y middleware.
Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.	Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.
Ciberseguridad en comunicaciones inalámbricas para dispositivos IoT/IioT.	Ciberseguridad en comunicaciones inalámbricas para dispositivos IoT/IioT.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Aprendizaje basado en proyectos	5	45	50
Lección magistral	14	20	34
Prácticas con apoyo de las TIC	15	25	40
Examen de preguntas objetivas	1	0	1

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Aprendizaje basado en proyectos	Implementación grupal del diseño, implementación y pruebas de un sistema IoT, con especial énfasis en la seguridad. Realizar ataques grupales a la seguridad de los sistemas implementados por otros compañeros o terceros.

Lección magistral	Presentación, por parte del profesorado, de los principales contenidos teóricos relacionados con la seguridad industrial e IoT (seguridad embebida, en comunicaciones y backends, con especial foco en entornos industriales)
Prácticas con apoyo de las TIC	Realización por parte de los alumnos de prácticas guiadas y supervisadas.

Atención personalizada

Metodologías	Descripción
Aprendizaje basado en proyectos	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Asimismo, el profesorado orientará al alumnado durante la realización del proyecto. Las dudas se resolverán durante las tutorías en grupo, o en el horario establecido para las tutorías. El horario de tutorías se establecerá al inicio del curso y se publicará en la web de la asignatura.
Lección magistral	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Las dudas se resolverán durante la propia sesión magistral, o en el horario establecido para las tutorías. El horario de tutorías se establecerá al inicio del curso y se publicará en la web de la asignatura.
Prácticas con apoyo de las TIC	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Asimismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que les hayan sido asignadas, tanto en las prácticas. Las dudas se resolverán bien durante las propias clases o bien en el horario establecido para las tutorías.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje		
Aprendizaje basado en proyectos	El alumnado se dividirá en grupos para la realización del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad y/o realizará ataques a la seguridad de los sistemas implementados por otros compañeros/as o por terceros. El proyecto realizado, y el informe que contiene el resultado de los ataques completados (en cuanto a su calidad y a su éxito) serán evaluados después de su entrega valorando aspectos como la corrección, la calidad, las prestaciones y las funcionalidades. Se deberá entregar el código, prototipos y documentación realizados. Asimismo, será necesario realizar una presentación de los resultados. Durante la realización del proyecto se realizará un seguimiento continuo del diseño y de la evolución de la implementación. Si los resultados intermedios no son satisfactorios, se podrá aplicar una penalización de hasta el 20% de la nota. El seguimiento será grupal e individual: cada uno de lo miembros del grupo debe documentar las tareas desarrolladas dentro de su equipo y responder sobre ellas.	40	B9	C9	D2 D5 D7
Prácticas con apoyo de las TIC	Resolución de prácticas y realización de informes con los resultados obtenidos.	30	B9	C9	D2 D5 D7
Examen de preguntas objetivas	Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso.	30	B9	C9	D2 D5 D7

Otros comentarios sobre la Evaluación

Para superar la asignatura es necesario completar las distintas partes en las que se divide (examen o exámenes acerca de los contenidos expuestos en la sesión magistral y el proyecto). La nota final será el resultado de aplicar la **media geométrica ponderada** de la nota de cada una de las partes.

Así, si la nota de las sesiones magistrales es NT, la nota del proyecto es NP y la nota de las prácticas es NL, la nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante el primer mes, el estudiantado deberá indicar explícitamente y por escrito su deseo de cursar la materia siguiendo

la evaluación global. En otro caso se considerará que siguen la evaluación continua. Quienes sigan la evaluación continua no se podrán considerar "no presentados" así que hayan realizado la entrega del primer cuestionario o tarea.

El alumnado que opte por la evaluación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, y muy especialmente el proyecto. En el caso de seguir la evaluación global, los alumnos/as deberán realizar el trabajo de forma individual, salvo que el profesorado les comunique explícitamente la autorización para realizarlo en grupo.

Evaluación extraordinaria

Solo podrán optar a la evaluación extraordinaria quien no supere la primera oportunidad (al finalizar el cuatrimestre). La evaluación será la descrita en los apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las

distintas tareas, muy especialmente el proyecto.

Quien hubiese seguido la evaluación continua puede optar por mantener las notas obtenidas en la primera oportunidad para las distintas partes de la asignatura o descartarlas.

Otros comentarios

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor. Aunque el proyecto se desarrollará (en la medida de lo posible) en grupos, el alumnado debe guardar evidencias de su trabajo individual dentro del grupo. En el caso en el que el rendimiento de un alumno o alumna no sea acorde al de sus compañeros de grupo, se considerará su expulsión del mismo y/o podrá ser evaluado/a de forma completamente individual en esta parte.

El uso de cualquiera material durante la realización de los exámenes tendrá que ser autorizado explícitamente por el profesorado.

En caso de detección de plagio o de comportamiento no ético en alguno de los trabajos/pruebas realizadas, la calificación de la materia será de "suspenso (0)" y los profesores comunicarán el asunto a las autoridades académicas para que tomen las medidas oportunas.

En la realización de las actividades académicas de esta materia se permite el uso de inteligencia artificial generativa (IAG). Su uso debe realizarse de forma ética, crítica y responsable. En el caso de utilizar IAG, debe evaluarse de forma crítica cualquier resultado que proporcione, y verificar de forma cuidadosa cualquier cita o referencia generada. Asimismo, se recomienda declarar el uso de las herramientas utilizadas.

Fuentes de información

Bibliografía Básica

Brian Russell, Drew Van Duren,, **Practical Internet of Things Security**, 978-1788625821, 2, Packt Publishing, 2018

Eric Knapp, Joel Thomas Langill, **Industrial Network Security**, 978-0-12-420114-9, 2, Elsevier, 2015

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, 978-1609608514, GI Global, 2012

Tyson Macaulay,, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.,**, 978-1439801963, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems**, 978-1491920947, O'Reilly, 2016

Pascal Ackerman, **Industrial Cybersecurity,**, 978-1788395151, Packt, 2017

Bibliografía Complementaria

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1-119-22604-8, 1, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security**, 978-1118809990, 1, Wiley, 2014

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, 978-1498734738, CRC Press, 2016

Recomendaciones