



DATOS IDENTIFICATIVOS

Ciberseguridade industrial e IoT

Asignatura	Ciberseguridade industrial e IoT			
Código	V05M175V11213			
Titulación	Máster Universitario en Ciberseguridade			
Descriptor	Creditos ECTS	Selección	Curso	Cuatrimestre
	5	OB	1	2c
Lingua	Impartición			
Departamento				
Coordinador/a	Díaz-Cacho Medina, Miguel Ramón			
Profesorado	Díaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel Gil Castiñeira, Felipe José			
Correo-e	mcacho@uvigo.es			
Web				

Descrición xeral Los dispositivos intelixentes nos están prestando cada vez máis servizos case sin que nos demos conta de súa presenza: o coche ha deixado de ser unha simple máquina mecánica para converterse en un sistema conectado con un enorme control electrónico; en os hoteles xa non usamos llave, sino que podemos abrir a nosa habitación con unha tarxeta ou o noso teléfono móbil; Nostros termostatos domésticos se poden conectar a un servizo de pronóstico do tempo e axustarse ao clima en as próximas horas.

Los entornos industriais 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 exemplos de las aplicaciones habilitadas por tecnoloxías "integradas", redes de comunicacións 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 tecnoloxías de la Industria 4.0, como los sistemas IoT/IIoT, los sistemas robóticos, la computación en la nube/borde, la realidade aumentada, la cadena de bloques o los AGV.

Resultados de Formación y Aprendizaje

Código

Resultados previstos en la materia

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

Contenidos

Tema	
Introducción a la ciberseguridad industrial.	Introducción a la ciberseguridad industrial.
Introducción a los sistemas ciberfísicos e IIoT: hardware, firmware, comunicacións y cloud	Introducción a los sistemas ciberfísicos e IIoT: hardware, firmware, comunicacións y cloud
Ciberseguridad de sistemas de control y comunicacións industriais.	Ciberseguridad de sistemas de control y comunicacións industriais.
Ciberseguridad de tecnoloxías de la Industria 4.0/5.0.	Ciberseguridad de tecnoloxías de la Industria 4.0/5.0.
Ciberseguridad de dispositivos IIoT: hardware, firmware y middleware.	Ciberseguridad de dispositivos IIoT: hardware, firmware y middleware.
Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.	Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.

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 los miembros del grupo debe documentar las tareas desarrolladas dentro de su equipo y responder sobre ellas.	40	

Prácticas con apoyo de las TIC	Resolución de prácticas y realización de informes con los resultados obtenidos.	30
Examen de preguntas objetivas	Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso.	30

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:

$$\text{Nota} = \text{NT}^{0.3} \times \text{NP}^{0.4} \times \text{NL}^{0.3}$$

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 "suspense (0)" y los profesores comunicarán el asunto a las autoridades académicas para que tomen las medidas oportunas.

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**, Elsevier, 2014

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

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

Recomendaciones
