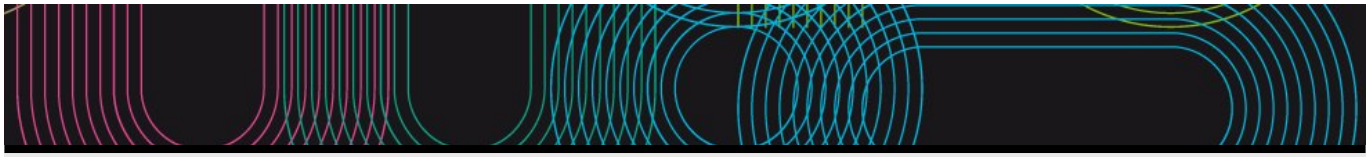

DATOS IDENTIFICATIVOS				
Ciberseguridade industrial e IoT				
Materia	Ciberseguridade industrial e IoT			
Código	V05M175V11213			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de impartición				
Departamento				
Coordinador/a	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				
Descrición xeral	(*)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 e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introdución á ciberseguridade industrial.	Introdución á ciberseguridade industrial.
Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud	Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud
Ciberseguridade de sistemas de control e comunicacións industriais.	Ciberseguridade de sistemas de control e comunicacións industriais.
Ciberseguridade de tecnoloxías da Industria 4.0/5.0.	Ciberseguridade de tecnoloxías da Industria 4.0/5.0.
Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.	Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.
Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.	Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.

Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.	Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Aprendizaxe baseado en proxectos	5	45	50
Lección maxistral	14	20	34
Prácticas con apoio das TIC	15	25	40
Exame de preguntas obxectivas	1	0	1

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Aprendizaxe baseado en proxectos	Implementación grupal do deseño, implementación e probas dun sistema IoT, con especial énfase na seguridade. Realizar ataques grupales á seguridade dos sistemas implementados por outros compañeiros ou terceiros.
Lección maxistral	Presentación, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade industrial e IoT (seguridade embebida, en comunicacións e backends, con especial foco en contornas industriais)
Prácticas con apoio das TIC	Realización por parte dos alumnos de prácticas guiadas e supervisadas.

Atención personalizada

Metodoloxías	Descrición
Aprendizaxe baseado en proxectos	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará ao alumnado durante a realización do proxecto. As dúbidas resolveranse durante as titorías en grupo, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Lección maxistral	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. As dúbidas resolveranse durante a propia sesión maxistral, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Prácticas con apoio das TIC	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que lles foron asignadas, tanto nas prácticas. As dúbidas resolveranse ben durante as propias clases ou ben no horario establecido para as titorías.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Aprendizaxe baseado en proxectos	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, pondo unha énfase especial na seguridade e/ou realizará ataques á seguridade dos sistemas implementados por outros compañeiros/as ou por terceiros. O proxecto realizado, e o informe que contén o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Si os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de até o 20% da nota. O seguimento será grupal e individual: cada un do membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	40	
Prácticas con apoio das TIC	Resolución de prácticas e realización de informes cos resultados obtidos.	30	

Exame de preguntas obxectivas	Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso.	30

Outros comentarios sobre a Avaliación

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exámenes acerca dos contidos expostos na sesión maxistral e o proxecto). A nota final será o resultado de aplicar a **media xeométrica ponderada** da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, a nota do proxecto é NP e a nota das prácticas é NL, a nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante o primeiro mes, o estudiantado deberá indicar explícitamente e por escrito o seu desexo de cursar a materia seguindo a evaluación global. Noutro caso se considerará que seguen a availiación continua. Quen sigan a avaliación continua non se podrán considerar "non presentados" así que realicen a entrega do primeiro cuestionario ou tarefa.

O alumnado que opte pola avaliación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, e moi especialmente o proxecto. No caso de seguir a avaliación global, os alumnos/as deberán realizar o traballo de forma individual, salvo que o profesorado comuníquelles explícitamente a autorización para realizalo en grupo.

Avaliación extraordinaria

Só podrán optar á avaliación extraordinaria quen non supere a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Quen seguise a avaliación continua pode optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor. Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, o alumnado debe gardar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, se considerará a súa expulsión do mesmo e/ou podrá ser avaliado/a de forma completamente individual nesta parte.

O uso de calquera material durante a realización dos exámenes tendrá que ser autorizado explícitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a calificación da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tomen as medidas oportunas.

Bibliografía. Fontes 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

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

Recomendacións