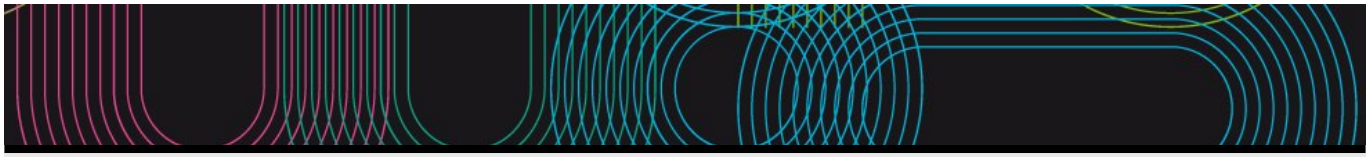

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Ciberseguridade industrial e IoT** | | | | |
| Materia | Ciberseguridade industrial e IoT | | | |
| Código | V05M175V11213 | | | |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descritores | Creditos ECTS | Sinale | Curso | Cuadrimestre |
| | 5 | OB | 1 | 2c |
| Lingua de impartición | Castelán<br>Galego | | | |
| Departamento | Dpto. Externo<br>Enxeñaría de sistemas e automática<br>Enxeñaría telemática | | | |
| Coordinador/a | Diaz-Cacho Medina, Miguel Ramón | | | |
| Profesorado | Diaz-Cacho Medina, Miguel Ramón<br>Fernández Caramés, Tiago Manuel<br>Gil Castiñeira, Felipe José | | | |
| Correo-e | mcacho@uvigo.es | | | |
| Web | http://www.moovi.gal | | | |
| Descrición xeral | Os dispositivos intelixentes están a prestarnos cada vez máis servizos case sen que nos deamos conta da súa presenza: o coche deixou de ser unha simple máquina mecánica para converterse nun sistema conectado cun enorme control electrónico; nos hoteis xa non usamos chave, senón que podemos abrir a nosa habitación cun cartón ou o noso teléfono móbil; Os nosos *termostatos domésticos pódense conectar a un servizo de prognóstico do tempo e axustarse ao clima nas próximas horas.<br><br>As contornas industriais son casos de uso particularmente importantes, xa que a conexión en rede de dispositivos que miden e controlan procesos permite a Industria 4.0.<br><br>Todos son exemplos das aplicacións habilitadas por tecnoloxías "integradas", redes de comunicacións inalámbricas e, en última instancia, "Internet das cousas" (IoT). Esta materia analiza os problemas e as mellores prácticas para facer que este tipo de sistemas sexan seguros, con especial énfase na seguridade das tecnoloxías da Industria 4.0, como os sistemas *IoT/*IioT, os sistemas *robóticos, a *computación na nube/bordo, a realidade aumentada, a cadea de bloques ou os AGV. | | | |

## Resultados de Formación e Aprendizaxe

| Código | |
|---|---|
| B9 | Identificar a arquitectura dos sistemas IoT, a súa complexidade e vulnerabilidades, así como comprender a seguridade no ámbito dos sistemas embebidos e dos sistemas de comunicación IoT. |
| C9 | Analizar as implicacións do nivel de seguridade das tecnoloxías relacionadas coa dixitalización dos sectores produtivos, así como avaliar e modelar as ameazas e executar ataques co obxectivo de deseñar sistemas de IoT seguros. |
| D2 | Demostrar autonomía e iniciativa para resolver problemas complexos que impliquen múltiples tecnoloxías no ámbito das redes ou sistemas de comunicación, e desenvolver solucións innovadoras no ámbito das comunicacións e informática distribuídas privadas. |
| D5 | Analizar a seguridade dos protocolos de comunicación na capa física; ligazón; de rede e transporte, así como avaliar nunha rede corporativa as medidas de seguridade que se deben implantar para protexer os seus bens internos e comunicacións. |
| D7 | Aplicar políticas de seguridade e implementar as diferentes técnicas de protección baseadas na comprensión dos ataques a sistemas industriais para minimizar os problemas de seguridade e os ataques ás redes de control industrial. |

## Resultados previstos na materia

| Resultados previstos na materia | Resultados de Formación e Aprendizaxe |
|---|---|
| RA01. Comprender a execución de políticas de seguridade e as súas implicacións en contornas industriais. | B9<br>C9<br>D7 |
| RA02. Comprender as diferentes técnicas de protección e ataque en sistemas industriais e saber como se poden implementar. | B9<br>C9<br>D2<br>D5<br>D7 |
| RA03. Entender as problemáticas de seguridade e os ataques a redes de control industrial e coñecer os mecanismos que permiten minimizalos. | B9<br>C9<br>D5<br>D7 |
| RA04. Coñecer e identificar a arquitectura dos sistemas IoT, a súa complexidade e as súas vulnerabilidades | B9 |
| RA05. Comprender a seguridade no ámbito dos sistemas embebidos. | B9<br>C9<br>D2<br>D5<br>D7 |
| RA06. Comprender a seguridade no ámbito dos sistemas de comunicación IoT. | B9<br>C9<br>D5 |
| RA07. Coñecer casos reais de ataques a sistemas IoT. | B9<br>D7 |
| RA08. Ser capaz de comprender as implicacións a nivel de seguridade de tecnoloxías relacionadas con conceptos como a Industria 4.0/5.0. | B9<br>C9<br>D5<br>D7 |
| RA09. Ser capaz de valorar e modelar ameazas e executar ataques sobre un sistema IoT | B9<br>C9<br>D2 |
| RA10. Ser capaz de deseñar sistemas IoT seguros | B9<br>C9<br>D2<br>D5<br>D7 |

## 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.<br><br>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.<br><br>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.<br><br>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 | B9 | C9 | D2<br>D5<br>D7 |
| Prácticas con apoio das TIC | Resolución de prácticas e realización de informes cos resultados obtidos. | 30 | B9 | C9 | D2<br>D5<br>D7 |
| Exame de preguntas obxectivas | Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso. | 30 | B9 | C9 | D2<br>D5<br>D7 |

**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.

Na realización das actividades académicas desta materia permítese o uso de intelixencia artificial xenerativa (IAX). O seu uso debe realizarse de forma ética, crítica e responsable. No caso de utilizar IAX, debe avaliarse de forma crítica calquera resultado que proporcione, e verificar de forma coidadosa calquera cita ou referencia xerada. Así mesmo, recoméndase declarar o uso das ferramentas utilizadas.

## 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**, 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


## Recomendacións