Guía Docente				
Datos Identificativos				2020/21
Asignatura (*)	Ciberseguridade en Contornos Industriais		Código	614530014
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Optativa	3
Idioma	CastelánGalegoInglés			
Modalidade docente	Híbrida			
Prerrequisitos				
Departamento	Electrónica e SistemasEnxeñaría de Computadores			
Coordinación	Fernández Caramés, Tiago Manuel	Correo electrónico	tiago.fernandez@udc.es	
Profesorado	Fernández Caramés, Tiago Manuel	Correo electrónico	tiago.fernandez@udc.es	
Web	faitic.uvigo.es			
Descrición xeral	O concepto da Industria 4.0 deu lugar a que cada vez sexan máis os dispositivos industriais conectados á rede e a procesos físicos. Esta materia, ademais de repasar os sistemas industriais tradicionais (i.e., sistemas de control industrial, control de accesos, sistemas de comunicacións ou de xestión da información), enfocarase na seguridade das tecnoloxías da Industria 4.0: sistemas IoT/IIoT, sistemas robotizados, cloud/edge computing, realidade aumentada, blockchain ou AGVs.			

Plan de continxencia	1. Modificacións nos contidos - Non se realizarán cambios. 2. Metodoloxías - *Metodoloxías docentes que se manteñen - Traballos tutelados, proba mixta. - *Metodoloxías docentes que se modifican - Sesión maxistral: debido á situación excepcional, ante a imposibilidade de poder impartir a docencia dun modo completamente presencial, utilizaranse medios virtuais proporcionados pola universidade, os cales se poderán complementar con outros medios. Prácticas a través das TIC: substituiranse as prácticas que requiran de equipamento específico por outro simulado ou virtualizado. Eventualmente, proporanse prácticas alternativas que non requiran de devandito equipamento. Estas prácticas poderán ter un formato autónomo en previsión de problemas de conciliación e/ou conexión. 3. Mecanismos de atención personalizada ao alumnado - As sesións de titorización (atención ao alumnado) realizaranse por medios telemáticos (e.g., correo electrónico, Teams, Moodle, FAITIC, Campus Remoto), que se poderán complementar entre si e con outras ferramentas. En parte delas utilizarase unha modalidade de concertación previa. 4. Modificacións na avaliación - A avaliación manterá a mesma metodoloxía, sendo o exame unha proba mixta online utilizando os medios virtuais dispoñibles. Non obstante, o peso da nota pasará a ser: Prácticas a través das TIC: 40%; Traballos tutelados: 40%; Proba mixta: 20%. 5. Modificacións da bibliografía ou webgrafía - Non haberá modificacións.

Competencias do título	
Código	Competencias do título
A1	CE1 - Coñecer, comprender e aplicar os métodos de criptografía e criptoanális, os fundamentos de identidade dixital e os protocolos de comunicacións seguras
A2	CE2 - Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
A3	CE3 - Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información
A4	CE4 - Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información

A7	CE7 - Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análisis de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
A8	CE8 - Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
A12	CE12 - Coñecer o papel da ciberseguridade no deseño das novas industrias, así como as particularidades, restricciones e limitacións que teñen que acometerse para obter unha infraestructura industrial segura
A13	CE13 - Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
A15	CE15 - Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade
B1	CB1 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación
B2	CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
B3	CB3 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos
B7	CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións
B8	CG3 - Capacidade para o razonamiento crítico e a evaluación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
B10	CG5 - Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
B11	CG6 - Destreza para investigar. Capacidade para innovar e contribuir ao avance dos principios, as técnicas e os procesos referidos o seu ámbito profesional, deseñando novos algoritmos, dispositivos, técnicas ou modelos útiles para a protección dos activos dixitais públicos, privados ou comerciais
C4	CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias do título		
Coñecer os conceptos fundamentais asociados coa seguridade en contornas industriais	AP1 AP3 AP12 AP15		CP4
Comprender as diferentes técnicas de protección e ataque en sistemas industriais e saber como se poden implementar	AP2 AP4 AP8 AP13	BP2 BP3 BP7 BP8 BP10 BP11	
Entender as problemáticas de seguridade e os ataques a redes industriais, así como coñecer os mecanismos que permiten minimizalos	AP1 AP4 AP7 AP12 AP13	BP3 BP7 BP8 BP11	
Ser capaz de comprender as implicacións a nivel de seguridade das diversas tecnoloxías da industria 4.0	AP1 AP3 AP12 AP15	BP1 BP3	

Contidos	
Temas	Subtemas
Introdución	Políticas de seguridade industrial Implicacións da ciberseguridade industrial e de infraestruturas críticas Casos prácticos
Sistemas de control de acceso físico a dependencias industriais	Sistemas de proximidade Sistemas de acceso remoto Sistemas biométricos
Sistemas de control industrial	Arquitectura de comunicacións Sistemas tradicionais Sistemas ciberfísicos
Sistemas da Industria 4.0	Introducción á Industria 4.0 Sistemas IoT/IIoT Seguridade noutras tecnoloxías 4.0 (e.g., realidade aumentada, cloud/edge computing, blockchain, AGVs)
Sistemas de xestión de información en contornas industriais	Bases de datos tradicionais ERPs PLMs Sistemas MES
Sistemas de comunicacións industriais	Arquitectura de comunicacións Tecnoloxías de comunicacións por cable Tecnoloxías de comunicacións sen fío

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Sesión maxistral	A1 A2 A3 A12 A15 B1 B7 B8 C4	9	9	18
Prácticas a través de TIC	A1 A2 A4 A7 A8 A13 B2 B7 B8 B10 B11	10	10	20
Traballos tutelados	A13 B2 B3 B7 B8 B10	0	20	20
Proba mixta	B2 B3 B7	1	15	16
Atención personalizada		1	0	1
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	**Descrición**
Sesión maxistral	Exposición por parte do profesorado dos principais contidos teóricos relacionados coa ciberseguridade en contornos industriais.
Prácticas a través de TIC	Realización por parte do alumnado de prácticas guiadas e supervisadas.
Traballos tutelados	Realización por parte do alumnado de traballos de compoñente tanto teórica coma práctica.
Proba mixta	Proba escrita para a avaliación dos coñecementos adquiridos na materia.

Atención personalizada	
Metodoloxías	**Descrición**
Traballos tutelados Sesión maxistral Prácticas a través de TIC	Os profesores da materia proporcionarán atención individual e persoalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Asemade, os profesores orientarán e guiarán aos alumnos durante a realización das tarefas que teñan asignadas, tanto nas prácticas como nos distintos traballos tutelados. As dúbidas atenderanse durante as propias clases ou durante o horario establecido para titorías. Buscarase flexibilizar dito horario para atender as dúbidas do alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.

Avaliación			
Metodoloxías	**Competencias**	**Descrición**	**Cualificación**
Traballos tutelados	A13 B2 B3 B7 B8 B10	Realización dun traballo con parte teórica e parte práctica.	30
Prácticas a través de TIC	A1 A2 A4 A7 A8 A13 B2 B7 B8 B10 B11	Resolución de prácticas e realización de informes cos resultados obtidos.	30
Proba mixta	B2 B3 B7	Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso.	40

Observacións avaliación

PRIMEIRA OPORTUNIDADE

Ofreceranse dúas alternativas de avaliación: continua e única.

A avaliación continua implicará a realización das prácticas, dun traballo tutelado e unha proba mixta que serán avaliados nas porcentaxes arriba indicadas (30, 30, 40) ou, en caso de ser necesario, das porcentaxes indicadas no plan de continxencia, sendo necesario obter un cinco sobre dez na avaliación total. Igualmente, será necesario obter un dous sobre catro na proba mixta para poder aprobar a materia. No caso de optar á avaliación contínua, o alumnado que realice calqueira tipo de entrega (práctica, traballo, proba mixta), non poderá cualificarse como "non presentado".

No caso da avaliación única, toda a puntuación virá dada por unha única proba mixta que incluirá parte teórica e práctica. Dita proba realizarase ao final do bimestre e deberá obterse en total a lo menos un cinco sobre dez para poder aprobar a materia.

A selección da alternativa de avaliación deberá indicarse como moi tarde ao remate da terceira semana de clase.

Para cualquera das dúas alternativas darase flexibilidade horaria para o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.

SEGUNDA OPORTUNIDADE E CONVOCATORIAS EXTRAORDINARIAS

Os alumnos que optaran na primeira oportunidade pola avaliación contínua, terán a opción de conservar as notas de prácticas e traballos tutelados realizados durante o curso académico. Dito alumnado realizará unha proba mixta, establecéndose a nota nas mesmas porcentaxes aplicadas na primeira oportunidade. O resto de alumnos (incluido o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia) trataranse coma alumnos de avaliación única e realizarán unha proba mixta que mesture parte teórica e práctica.

OUTROS COMENTARIOS

Non se conservará ningunha das notas obtidas para os cursos académicos posteriores.

No caso de detección de plaxio durante algunha das entregas, cualificarse ao alumno/a cun suspenso (0) e comunicarase a situación á dirección do máster e ás autoridades universitarias correspondentes de cara a tomar as medidas oportunas.

Fontes de información	
Bibliografía básica	- Eric Knapp, Joel Thomas Langill (2014). Industrial Network Security. Elsevier - Junaid Ahmed Zubairi (2012). Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies. IGI Global - Tyson Macaulay (2012). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach Publications - Josiah Dykstra (2015). Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems. O'Reilly - Pascal Ackerman (2017). Industrial Cybersecurity. Packt
Bibliografía complementaria	- Peng Cheng, Heng Zhang, Jiming Chen (2016). Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop. CRC Press

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións