



| Guía Docente | | | | |
|-----------------------|---|----------|--------------------|------------------------|
| Datos Identificativos | | | | 2018/19 |
| Asignatura (*) | Ciberseguridade en Contornos Industriais | | Código | 614530014 |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descritores | | | | |
| Ciclo | Período | Curso | Tipo | Créditos |
| Mestrado Oficial | 2º cuatrimestre | Primeiro | Optativa | 3 |
| Idioma | CastelánGalegoInglés | | | |
| Modalidade docente | Presencial | | | |
| 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 | www.munics.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 asignatura, ademáis 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. | | | |

| Competencias / Resultados do título | |
|-------------------------------------|--|
| Código | Competencias / Resultados do título |
| A1 | CE1 - Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, 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, restricións e limitacións que teñen que acometerse para obter unha infraestrutura 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 máis 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 avaliación 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 infraestruturas, equipamentos 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 / Resultados do título | |
| Coñecer os conceptos fundamentais asociados coa seguridade en entornos industriais | | AP1 AP3 AP12 AP15 | CP4 |
| Comprender as diferentes técnicas de protección e ataque en sistemas industriais e saber cómo 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 |
| Introducción | 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 | <p>Introducción á Industria 4.0</p> <p>Sistemas IoT/IloT</p> <p>Seguridade noutras tecnoloxías 4.0 (e.g., realidade aumentada, cloud/edge computing, blockchain, AGVs)</p> |
| Sistemas de xestión de información en entornos industriais | <p>Bases de datos tradicionais</p> <p>ERPs</p> <p>PLMs</p> <p>Sistemas MES</p> |
| Sistemas de comunicacións industriais | <p>Arquitectura de comunicacións</p> <p>Tecnoloxías de comunicacións cableadas</p> <p>Tecnoloxías de comunicacións inarámicas</p> |

| Planificación | | | | |
|---------------------------|--|---|-------------------------|--------------|
| Metodoloxías / probas | Competencias / Resultados | Horas lectivas (presenciais e virtuais) | Horas 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 asignatura. |

| Atención personalizada | |
|------------------------|------------|
| Metodoloxías | Descrición |



| | |
|--|--|
| Traballos tutelados Sesión maxistral Prácticas a través de TIC | Os profesores da materia proporcionarán atención individual e personalizada 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 de forma presencial, xa sexa 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 / Resultados | 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 |
|---|
| <p>PRIMEIRA OPORTUNIDADE</p> <p>Ofreceranse dúas alternativas de avaliación: continúa e única.</p> <p>A avaliación continúa implicará a realización das prácticas, dun traballo tutelado e unha proba mixta que serán avaliados nas porcentaxes arriba indicadas (30, 30, 40), 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 asignatura. No caso de optar á avaliación continúa, o alumnado que realice calqueira tipo de entrega (práctica, traballo, proba mixta), non poderá calificarse como "non presentado".</p> <p>No caso da avaliación única, toda a puntuación virá dada por unha única proba mixta que incluírá 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 asignatura.</p> <p>A selección da alternativa de avaliación deberá indicarse como moi tarde ao remate da segunda semana de clase.</p> <p>Para calquera das dúas alternativas darase flexibilidade horaria para o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.</p> <p>SEGUNDA OPORTUNIDADE E CONVOCATORIAS EXTRAORDINARIAS</p> <p>Os alumnos que optaran na primeira oportunidade pola avaliación continúa, terán a opción de conservar as notas de prácticas e traballos tutelados realizados durante o curso académico. Dito alumnado realizará unha proba mixta, establéndose a nota nas porcentaxes indicadas arriba (30, 30, 40). O resto de alumnos (incluído 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.</p> <p>OUTROS COMENTARIOS</p> <p>Non se conservará ningunha das notas obtidas para os cursos académicos posteriores.</p> <p>No caso de detección de plaxio durante algunha das entregas, calificarse ao alumno/a cun suspenso (0) e comunicarse a situación á dirección do máster e ás autoridades universitarias correspondentes de cara a tomar as medidas oportunas.</p> |

| Fontes de información | |
|----------------------------|--|
| Bibliografía básica | <ul style="list-style-type: none"> - 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

(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías