



| Guía docente          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                        |           |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|-----------|
| Datos Identificativos |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                        | 2021/22   |
| Asignatura (*)        | Ciberseguridad en Entornos Industriales                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                    | Código                 | 614530014 |
| Titulación            | Máster Universitario en Ciberseguridade                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                    |                        |           |
| Descriptorios         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                        |           |
| Ciclo                 | Periodo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Curso              | Tipo                   | Créditos  |
| Máster Oficial        | 2º cuatrimestre                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Primero            | Optativa               | 3         |
| Idioma                | CastellanoGallego                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                    |                        |           |
| Modalidad docente     | Presencial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                    |                        |           |
| Prerrequisitos        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                        |           |
| Departamento          | Electrónica e SistemasEnxeñaría de Computadores                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                        |           |
| Coordinador/a         | Fernández Caramés, Tiago Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Correo electrónico | tiago.fernandez@udc.es |           |
| Profesorado           | Fernández Caramés, Tiago Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Correo electrónico | tiago.fernandez@udc.es |           |
| Web                   | campusvirtual.udc.gal/course/view.php?id=8502                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                    |                        |           |
| Descripción general   | El concepto de la Industria 4.0 dio lugar a que cada vez sean más los dispositivos industriales conectados a la red y a procesos físicos. Esta asignatura, además de repasar los sistemas industriales tradicionales (i.e., sistemas de control industrial, control de accesos, sistemas de comunicaciones o de gestión de la información), se enfocará en la seguridad de las tecnologías de la Industria 4.0: sistemas IoT/IIoT, sistemas robotizados, cloud/edge computing, realidad aumentada, blockchain o AGVs. |                    |                        |           |



|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Plan de contingencia</b> | <p>1. Modificaciones en los contenidos</p> <ul style="list-style-type: none"><li>- No se realizarán cambios.</li></ul> <p>2. Metodologías</p> <ul style="list-style-type: none"><li>- *Metodologías docentes que se mantienen</li><li>- Trabajos tutelados, prueba mixta.</li><li>- *Metodologías docentes que se modifican</li><li>- Sesión magistral: debido a la situación excepcional, ante la imposibilidad de poder impartir la docencia de un modo completamente presencial, se utilizarán medios virtuales proporcionados por la universidad, los cuales se podrán complementar con otros medios.</li></ul> <p>Prácticas a través de las TIC: se sustituirán las prácticas que requieran de equipamiento específico por otro simulado o virtualizado. Eventualmente, se propondrán prácticas alternativas que no requieran de devandito equipamiento. Estas prácticas podrán tener un formato autónomo en previsión de problemas de conciliación e/o conectividad.</p> <p>3. Mecanismos de atención personalizada al alumnado</p> <ul style="list-style-type: none"><li>- Las sesiones de tutorización (atención al alumnado) se realizarán por medios telemáticos (e.g., correo electrónico, Teams, Moodle, FAITIC, Campus Remoto), que se podrán complementar entre si y con otras herramientas. En parte de ellas se utilizará una modalidad de concertación previa.</li></ul> <p>4. Modificaciones en la evaluación</p> <ul style="list-style-type: none"><li>- La evaluación mantendrá la misma metodología, siendo el examen una prueba mixta online utilizando los medios virtuales disponibles. No obstante, el peso de la nota pasará a ser:</li></ul> <p>Prácticas a través de las TIC: 40%;<br/>Trabajos tutelados: 40%;<br/>Prueba mixta: 20%.</p> <p>5. Modificaciones de la bibliografía o webgrafía</p> <ul style="list-style-type: none"><li>- No habrá modificaciones.</li></ul> |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Competencias del título |                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Código                  | Competencias del título                                                                                                                                                                                        |
| A1                      | CE1 - Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras                                              |
| A2                      | CE2 - Conocer en profundidad las técnicas de ciberataque y ciberdefensa                                                                                                                                        |
| A3                      | CE3 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información |
| A4                      | CE4 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información |



|     |                                                                                                                                                                                                                                                                                                                   |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A7  | CE7 - Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros                                                                                        |
| A8  | CE8 - Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad                                                                                                                                                                                                             |
| A12 | CE12 - Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura                                                                                         |
| A13 | CE13 - Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes                                                                                                                                                                    |
| A15 | CE15 - Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad   |
| B1  | CB1 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación                                                                                                                                     |
| B2  | CB2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio                                                                     |
| B3  | CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios      |
| B7  | CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones                                                                                            |
| B8  | CG3 - Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones                                                                      |
| B10 | CG5 - Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos                                                                                                       |
| B11 | CG6 - Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales |
| C4  | CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad                                                                                                                                                                                                         |

| Resultados de aprendizaje                                                                                                             |                                   |                                          |     |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------------|-----|
| Resultados de aprendizaje                                                                                                             | Competencias del título           |                                          |     |
| Conocer los conceptos fundamentales asociados con la seguridad en entornos industriales                                               | AP1<br>AP3<br>AP12<br>AP15        |                                          | CP4 |
| Comprender las diferentes técnicas de protección y ataque en sistemas industriales y saber cómo se pueden implementar                 | AP2<br>AP4<br>AP8<br>AP13         | BP2<br>BP3<br>BP7<br>BP8<br>BP10<br>BP11 |     |
| Entender las problemáticas de seguridad y los ataques a redes industriales, así como conocer los mecanismos que permiten minimizarlos | AP1<br>AP4<br>AP7<br>AP12<br>AP13 | BP3<br>BP7<br>BP8<br>BP11                |     |
| Ser capaz de comprender las implicaciones a nivel de seguridad de las diversas tecnologías de la Industria 4.0                        | AP1<br>AP3<br>AP12<br>AP15        | BP1<br>BP3                               |     |



| Contenidos                                                       |                                                                                                                                                                       |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tema                                                             | Subtema                                                                                                                                                               |
| Introducción                                                     | Políticas de seguridad industrial<br><br>Implicaciones de la ciberseguridad industrial y de infraestructuras críticas<br><br>Casos prácticos                          |
| Sistemas de control de acceso físico a dependencias industriales | Sistemas de proximidad<br><br>Sistemas de acceso remoto<br><br>Sistemas biométricos                                                                                   |
| Sistemas de control industrial                                   | Arquitecturas de comunicaciones<br><br>Sistemas tradicionales<br><br>Sistemas ciberfísicos                                                                            |
| Sistemas de la Industria 4.0                                     | Introducción a la Industria 4.0<br><br>Sistemas IoT/IIoT<br><br>Seguridad en otras tecnologías 4.0 (e.g., realidad aumentada, cloud/edge computing, blockchain, AGVs) |
| Sistemas de gestión de información en entornos industriales      | Bases de datos tradicionales<br><br>ERPs<br><br>PLMs<br><br>Sistemas MES                                                                                              |
| Sistemas de comunicaciones industriales                          | Arquitectura de comunicaciones<br><br>Tecnologías de comunicación cableadas<br><br>Tecnologías de comunicación inalámbricas                                           |

| Planificación                                                                                                                      |                                        |                    |                                          |               |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------|------------------------------------------|---------------|
| Metodologías / pruebas                                                                                                             | Competencias                           | Horas presenciales | Horas no presenciales / trabajo autónomo | Horas totales |
| Sesión magistral                                                                                                                   | A1 A2 A3 A12 A15 B1<br>B7 B8 C4        | 9                  | 9                                        | 18            |
| Prácticas a través de TIC                                                                                                          | A1 A2 A4 A7 A8 A13<br>B2 B7 B8 B10 B11 | 10                 | 10                                       | 20            |
| Trabajos tutelados                                                                                                                 | A13 B2 B3 B7 B8 B10                    | 0                  | 20                                       | 20            |
| Prueba mixta                                                                                                                       | B2 B3 B7                               | 1                  | 15                                       | 16            |
| Atención personalizada                                                                                                             |                                        | 1                  | 0                                        | 1             |
| (*) Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos |                                        |                    |                                          |               |



| Metodologías              |                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Metodologías              | Descrición                                                                                                                               |
| Sesión magistral          | Exposición por parte do profesorado de los principales contenidos teóricos relacionados con la ciberseguridad en contornos industriales. |
| Prácticas a través de TIC | Realización por parte del alumnado de prácticas guiadas y supervisadas.                                                                  |
| Trabajos tutelados        | Realización por parte del alumnado de trabajos de componente tanto teórica como práctica.                                                |
| Prueba mixta              | Prueba escrita para la evaluación de los conocimientos adquiridos en la asignatura.                                                      |

| Atención personalizada                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Metodologías                                                        | Descrición                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Trabajos tutelados<br>Sesión magistral<br>Prácticas a través de TIC | <p>Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Asimismo, los profesores orientarán y guiarán a los alumnos durante la realización de las tareas que tengan asignadas, tanto en las prácticas como en los distintos trabajos tutelados.</p> <p>Las dudas se atenderán durante las propias clases o durante el horario establecido para tutorías. Se buscará flexibilizar dicho horario para atender las dudas del alumnado con reconocimiento de dedicación a tempo parcial y dispensa académica de exención de asistencia.</p> |

| Evaluación                |                                     |                                                                                       |              |
|---------------------------|-------------------------------------|---------------------------------------------------------------------------------------|--------------|
| Metodologías              | Competencias                        | Descrición                                                                            | Calificación |
| Trabajos tutelados        | A13 B2 B3 B7 B8 B10                 | Realización de un trabajo con parte teórica y parte práctica.                         | 30           |
| Prácticas a través de TIC | A1 A2 A4 A7 A8 A13 B2 B7 B8 B10 B11 | Resolución de prácticas y realización de informes con los resultados obtenidos.       | 30           |
| Prueba mixta              | B2 B3 B7                            | Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso. | 40           |

| Observaciones evaluación |
|--------------------------|
|--------------------------|



## PRIMERA OPORTUNIDAD

Se ofrecerán dos alternativas de evaluación: continua y única.

La evaluación continua implicará la realización de las prácticas, de un trabajo tutelado y una prueba mixta que serán evaluados en los porcentajes arriba indicados (30, 30, 40) o, en caso de ser necesario, de los porcentajes indicados en el plan de contingencia, siendo necesario obtener un cinco sobre diez en la evaluación total. Igualmente, será necesario obtener un dos sobre cuatro en la prueba mixta para poder aprobar la asignatura. En caso de optar a la evaluación continua, el alumnado que realice cualquier tipo de entrega (práctica, trabajo, prueba mixta), no podrá calificarse como "no presentado".

En el caso de la evaluación única, toda la puntuación vendrá dada por una única prueba mixta que incluirá parte teórica y práctica. Dicha prueba se realizará al final del bimestre y deberá obtenerse en total al menos un cinco sobre diez para poder aprobar la asignatura.

La selección de la alternativa de evaluación deberá indicarse como muy tarde al final de la tercera semana de clase.

Para cualquiera de las dos alternativas se facilitará flexibilidad horaria para el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia.

## SEGUNDA OPORTUNIDAD Y CONVOCATORIAS EXTRAORDINARIAS

Los alumnos que hayan optado en la primera oportunidad por la evaluación continua tendrán la opción de conservar las notas de prácticas y trabajos tutelados realizados durante el curso académico. Dicho alumnado realizará una prueba mixta, estableciéndose la nota en los mismos porcentajes aplicados en la primera oportunidad. El resto de alumnos (incluido el alumnado con reconocimiento de dedicación a tiempo parcial y dispensa académica de exención de asistencia) se tratarán como alumnos de evaluación única y realizarán una prueba mixta que mezcle parte teórica y práctica.

## OTROS COMENTARIOS

No se conservará ninguna de las notas obtenidas para los cursos académicos posteriores.

En el caso de detección de plagio durante alguna de las entregas, se calificará al alumno/a con suspenso (0) y se comunicará la situación a la dirección del máster y a las autoridades universitarias correspondientes de cara a tomar las medidas oportunas.

### Fuentes de información

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Básica</b>         | <ul style="list-style-type: none"><li>- Eric Knapp, Joel Thomas Langill (2014). Industrial Network Security. Elsevier</li><li>- Junaid Ahmed Zubairi (2012). Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies. IGI Global</li><li>- Tyson Macaulay (2012). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach Publications</li><li>- Josiah Dykstra (2015). Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems. O'Reilly</li><li>- Pascal Ackerman (2017). Industrial Cybersecurity. Packt</li></ul> |
| <b>Complementaria</b> | <ul style="list-style-type: none"><li>- Peng Cheng, Heng Zhang, Jiming Chen (2016). Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop. CRC Press</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |

### Recomendaciones

#### Asignaturas que se recomienda haber cursado previamente

#### Asignaturas que se recomienda cursar simultáneamente

#### Asignaturas que continúan el temario

#### Otros comentarios

(\*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías