1. DATOS BÁSICOS

Asignatura	Ciberseguridad Industrial
Titulación	Máster Universitario en Industria 4.0: Transformación y estrategia digital
Escuela/ Facultad	Escuela de Arquitectura, Ingeniería y Diseño
Curso	Primero
ECTS	6 ECTS
Carácter	Obligatoria
Idioma/s	Castellano
Modalidad	Presencial / Online
Semestre	S2
Curso académico	2024/2025
Docente coordinador	

2. PRESENTACIÓN

Esta asignatura forma parte del **Módulo 3: Entornos conectados**, dónde a través de las seis unidades de aprendizaje, se adquieren los conocimientos fundamentales de la ciberseguridad OT dentro de los entornos industriales y sus diferencias y convergencias con el mundo IT.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- **CB1:** Poseer y comprender los conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- **CB2:** Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

Competencias transversales:

- **CT3:** Competencia digital. Capacidad que faculta un uso creativo y seguro de las tecnologías de la información y de la comunicación. Ayuda al desarrollo del pensamiento crítico y es una capacidad clave para la búsqueda y análisis de datos, la investigación, la comunicación, el aprendizaje y una participación inclusiva en la sociedad.
- **CT7:** Resiliencia. Capacidad de las personas para adaptarse a situaciones adversas, inesperadas, que causen estrés, ya sean personales o profesionales, superándolas e incluso convirtiéndolas en oportunidades de cambio positivo. Esta capacidad se traduce en un crecimiento profundo de la persona, haciéndoles conocer sus limitaciones, salir de su zona de confort, aprender de los

obstáculos, desarrollar su inteligencia emocional y aprender a ser perseverantes ante situaciones difíciles.

- **CT8:** Competencia ético-social. Capacidad de desenvolverse en una profesión de manera adecuada y convivir en una sociedad plural y un mundo diverso. Esta capacidad pretende desarrollar ciudadanos globales y responsables, conscientes de la desigualdad y sensibles a la diversidad en un mundo global. Con conciencia ética y compromiso social. Internacionales, multilingües, flexibles y adaptables en entornos multiculturales.

Competencias específicas:

- **CE5:** Capacidad para examinar y descomponer las características de los protocolos y comunicaciones industriales utilizados en tiempo real, reconociendo los niveles de seguridad en un entorno industrial automatizado y digitalizado.
- **CE6:** Capacidad para investigar las posibles amenazas y vulnerabilidades que se pueden dar a nivel de puesto de trabajo, de planta o proceso y de red en la transferencia de datos e información.
- **CE8:** Capacidad para implementar la metodología correcta de tratamiento de datos de múltiples fuentes para la mejora y la resolución de problemas particulares de la industria conectada, teniendo en cuenta los requerimientos de seguridad y accesibilidad.
- **CE11**: Capacidad para aplicar los conocimientos, las habilidades y las competencias adquiridas en el desarrollo del máster en entornos reales.

Resultados de aprendizaje:

- **RA1:** Determinar las actividades y requisitos de ciberseguridad industrial que debe contener un proceso industrial digitalizado.
- **RA2:** Evaluar los niveles de seguridad de los equipos de campo y sistemas, analizando las características de los protocolos de comunicaciones utilizados, dentro de un proceso industrial digitalizado.
- **RA3:** Diseñar un protocolo de seguridad operacional en los distintos sistemas de control en tiempo real y generar los informes necesarios de análisis y diagnóstico en los distintos niveles de ciberseguridad industrial.
- **RA4:** Identificar posibles vulnerabilidades en un sistema industrial a través de pruebas de penetración para evaluar y mejorar la seguridad del proceso industrial.
- **RA5:** Diseñar una estrategia de análisis forense en los sistemas de control industrial de un proceso productivo digital, utilizando las metodologías y herramientas vigentes.
- **RA6:** Evaluar escenarios de ciberseguridad industrial en procesos productivos digitales a través de casos de uso.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CB1, CB2, CT3, CT7, CT8, CE5	**RA1:** Determinar las actividades y requisitos de ciberseguridad industrial que debe contener un proceso industrial digitalizado.
CB1, CB2, CT3, CT7, CT8, CE5, CE6	**RA2:** Evaluar los niveles de seguridad de los equipos de campo y sistemas, analizando las características de los protocolos de comunicaciones utilizados, dentro de un proceso industrial digitalizado.
CB1, CB2, CT3, CT7, CT8, CE5, CE6, CE8, CE11	**RA3:** Diseñar un protocolo de seguridad operacional en los distintos sistemas de control en tiempo real y generar los informes necesarios de análisis y diagnóstico en los distintos niveles de ciberseguridad industrial.

CB1, CB2, CT3, CT7, CT8, CE5, CE6, CE8, CE11	**RA4:** Identificar posibles vulnerabilidades en un sistema industrial a través de pruebas de penetración para evaluar y mejorar la seguridad del proceso industrial.
CB1, CB2, CT3, CT7, CT8, CE5, CE6, CE8, CE11	**RA5:** Diseñar una estrategia de análisis forense en los sistemas de control industrial de un proceso productivo digital, utilizando las metodologías y herramientas vigentes.
CB1, CB2, CT3, CT7, CT8, CE5, CE6, CE8, CE11	**RA6:** Evaluar escenarios de ciberseguridad industrial en procesos productivos digitales a través de casos de uso.

4. CONTENIDOS

Unidad de aprendizaje 1: Fundamentos de la ciberseguridad industrial.

- Introducción a la ciberseguridad industrial.
- Estándares de la ciberseguridad industrial.
- Infraestructuras críticas.

Unidad de aprendizaje 2: Equipos, sistemas y redes de comunicación en la ciberseguridad industrial.

- Equipos y sistemas de automatización industrial.
- Tipos de redes y topologías.
- Configuración de dispositivos de red industrial y segmentación de red.
- Niveles de seguridad en entorno industrial. Vulnerabilidad y riesgos.

Unidad de aprendizaje 3: Procedimientos seguros en sistemas de control industrial.

- Configuración de sistemas de control industrial.
- Detección de incidentes en tiempo real en entorno industrial.
- Fundamentos de supervisión, diagnóstico y securización de ICS.

Unidad de aprendizaje 4: Análisis de riesgos: Hacking ético.

- Concepto y responsabilidad del hacking ético.
- Tipos de tecnologías hacking.
- Las 5 etapas del hacking ético.

Unidad de aprendizaje 5: Analítica forense en sistemas de control industrial.

- Introducción al análisis forense en sistemas y dispositivos industriales.
- Modelado de un ataque a un sistema de control industrial.
- Herramientas para realizar análisis forense en redes OT.

Unidad de aprendizaje 6: Casos de uso

- Segmentación y acceso seguro a célula de automatización.
- Despliegue de políticas de ciberseguridad industrial.
- Análisis forense.

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

- **MD1:** Clase magistral.
- **MD2:** Métodos del caso.
- **MD3:** Aprendizaje cooperativo.
- **MD4:** Aprendizaje basado en problemas.

- **MD6:** Aprendizaje basado en enseñanzas de taller.
- **MD10:** Entornos de simulación

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad presencial:

Actividad formativa	Número de horas
Clases magistrales	8
Clases de aplicación práctica	22
Análisis de casos	16
Resolución de problemas	21
Elaboración de informes y escritos	4
Actividades en talleres y/o laboratorios	12
Debates y coloquios	5
Trabajo autónomo	50
Tutoría	10
Prueba de conocimiento	2
TOTAL	**150**

Modalidad online:

Actividad formativa	Número de horas
Clases magistrales	8
Clases de aplicación práctica	22
Análisis de casos	16
Resolución de problemas	21
Elaboración de informes y escritos	4
Actividades en talleres y/o laboratorios	12
Debates y coloquios	5
Trabajo autónomo	50
Tutoría	10
Prueba de conocimiento	2

TOTAL	**150**

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad presencial:

Sistema de evaluación	Peso
Pruebas de conocimiento	60%
Exposiciones orales	5%
Informes y escritos	10%
Caso/problema	25%

Modalidad online:

Sistema de evaluación	Peso
Pruebas de conocimiento	60%
Exposiciones orales	5%
Informes y escritos	10%
Caso/problema	25%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Actividades evaluables	Fecha
Presentación asignatura y evaluación inicial	Semana 1-3
Realización actividades individuales o grupales	Semana 4-6
Hitos seguimiento	Semana 7-8
Realización actividades individuales o grupales	Semana 9-11
Exámenes y presentación finales	Semana 11-12

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

A continuación, se indica la bibliografía recomendada:

- PISTORIUS, Johannes. *Industrie 4.0 – Schlüsseltechnologien für die Produktion*. Berlin, Heidelberg, Springer Vieweg, 2020. ISBN 978-3-662-61579-9.
- *Ciberseguridad: la cooperación público-privada*. Ministerio de Defensa, Secretaría General Técnica. Madrid, 2017. 204 p. ISBN: 978- 84-909-1245-4.
- GUPTA Aditya. *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things.* Apress. 2019.
- STALLINGS William. *Cryptography and Network Security: Principles and Practice*. Prentice Hall. 2013.
- HERNÁNDEZ, A. *Propuestas tecnológicas de INCIBE, para la Industria 4.0. High Level Conference On Assurance.* Madrid: ISACA. 2017.
- HERRERO, M. y LÓPEZ, A. *Protocolo y seguridad de red en Infraestructuras SCI. Instituto Nacional de Ciberseguridad (INCIBE).* 2015.

10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.
Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

11. ENCUESTAS DE SATISFACCIÓN

¡Tu opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.