

## GENERAL INFORMATION

| Course information |                                                                                        |
|--------------------|----------------------------------------------------------------------------------------|
| Name               | Nombre de la asignatura. Ciberseguridad en la Industria y en Infraestructuras críticas |
| Code               | DTC - MCS - 511                                                                        |
| Degree             | Master en Ciberseguridad (MCS), Master en Ingeniería de Telecomunicación (MIT)         |
| Year               | 2026-2027                                                                              |
| Semester           | Primer Semestre                                                                        |
| ECTS credits       | 3.4 ECTS                                                                               |
| Type               | Obligatoria                                                                            |
| Department         | DEA – Departamento de Electrónica y Automática                                         |
| Area               |                                                                                        |
| Coordinator        | Juan Atanasio Carrasco Mateos                                                          |

| Lecturer     |                                                                                |
|--------------|--------------------------------------------------------------------------------|
| Name         | Juan Atanasio Carrasco Mateos                                                  |
| Department   | Departamento de Electrónica y Automática                                       |
| Area         |                                                                                |
| Office       | Sala de Profesores                                                             |
| e-mail       | <a href="mailto:jacarrasco@icai.comillas.edu">jacarrasco@icai.comillas.edu</a> |
| Phone        | +34 629 33 76 22                                                               |
| Office hours | Solicitud por correo o móvil                                                   |

| Lecturer     |  |
|--------------|--|
| Name         |  |
| Department   |  |
| Area         |  |
| Office       |  |
| e-mail       |  |
| Phone        |  |
| Office hours |  |

| Lecturer     |  |
|--------------|--|
| Name         |  |
| Department   |  |
| Area         |  |
| Office       |  |
| e-mail       |  |
| Phone        |  |
| Office hours |  |

## DETAILED INFORMATION

### Contextualization of the course

#### Contribution to the professional profile of the degree

El propósito de esta asignatura es proporcionar a los alumnos una visión del funcionamiento básico de los sistemas de control industriales (SCI), su posible impacto en una Infraestructura Crítica (IC) y sus servicios y cuál debe ser un adecuado planteamiento de ciberseguridad para protegerlos (SCI y servicios).

Es una mezcla de aspectos técnicos de SCI, entendimiento de la ciberseguridad y metodologías a aplicar en la defensa de un SCI y de una IC.

La asignatura está organizada en el formato tradicional de clases presenciales y usa como libros de referencia los siguientes textos:

- Industrial Cybersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman
- Guía de Protección de Infraestructuras Críticas y Guía Protección Integral de los Servicios Esenciales en España, Fundación Borredá (sólo referencia)

A la finalización de la asignatura los alumnos:

- Conocerán las funciones básicas de un sistema de control y los principales sistemas de control que hay en la actualidad.
- Conocerán las referencias legislativas aplicables a la ciberseguridad de ICs en España (y países de nuestro entorno)
- Dispondrán de un conocimiento básico de tendencias actuales en la protección de sistemas de control
- Estarán preparados para aplicar el resto de conocimientos adquiridos en el Master de Ciberseguridad en la protección de sistemas de control y de infraestructuras críticas.

#### Prerequisites

Aunque no es estrictamente necesario, ayudan a la comprensión de la asignatura el disponer de conocimientos de conceptos básicos de sistemas control y de ciberseguridad, tanto tecnológicos como normativos, que por otra parte se adquirirán a lo largo del curso.

## CONTENTS

### Contents

#### TEMA 1: Sistemas de control industrial, SCI

- Introducción a los Sistemas de Control Industrial (SCI)
- Funciones básicas y componentes de un SCI
- Diferentes tipos de SCI y posibles arquitecturas de los mismos

#### TEMAS 2 Y 3: Inseguros por Herencia y Descripción escenario de arranque

- Dificultades asociadas al diseño histórico de SCI
- Importancia de las comunicaciones en un SCI y detalle de los protocolos de comunicación más habituales en SCI
- Metodología de ataque a SCI
- Ejemplo de Ataque a un SCI

#### **TEMA 4: Análisis de Riesgos de un SCI**

- Conceptos básicos análisis de riesgos
- Ejemplo análisis de Riesgos en un SCI

#### **TEMA 5: Arquitectura de referencia de un SCI**

- Arquitectura de red global y resiliente para una empresa que tiene SCIs
- Modelo Purdue adoptado en la ISA99

#### **TEMAS 6, 7, 8, 9, 10 y 11: Defensa en profundidad y detalles de la misma**

- Concepto de defensa en profundidad y diversidad
- Seguridad física
- Seguridad de red
- Seguridad de ordenador
- Seguridad de aplicación
- Seguridad de dispositivo

#### **TEMA 12: Desarrollo de un programa de ciberseguridad**

- Proceso para la generación de un programa de ciberseguridad de una empresa industrial y una Infraestructura Crítica (IC)
- Partes del programa y metodología iterativa/continua para el desarrollo del mismo

#### **TEMAS 13 y 14: Detalles sobre infraestructuras Críticas (ICs) y su protección**

- Servicio esencial para nuestra sociedad
- Concepto de Infraestructura Crítica de España y en países de su entorno
- Normativa aplicable para la protección e infraestructuras y de servicios esenciales (apoyados en sistemas de control, redes y sistemas de información. Operadores/Entidades Críticos y Operadores/Entidades Esenciales. Directivas NIS, NIS2, PIC y RCE y su transposición en España.
- Obligaciones de Operadores/Entidades Críticos y obligaciones de Operadores/Entidades Esenciales

#### **TEMAS 15, 16, 17 y 18: Herramientas/Investigación para la defensa de ICs**

- Certificación Según Cadena de Valor ENC4V (NIST/CIP?), Borrador

- Análisis Ligero de Riesgos en Sistemas Industriales, Borrador
- Indicadores para la mejora de la Ciberresiliencia
- Guía de respuesta a incidentes

### REFLEXIÓN CONJUNTA FINAL

Reflexión conjunta sobre el futuro de Ciberseguridad OT y el impacto de la IA.

## COMPETENCES, KNOWLEDGE, SKILLS AND LEARNING OUTCOMES

### Competences and Learning Outcomes

#### Competences

##### General Competences

- CG1. Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio.
- CG2. Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto con investigadores como con profesionales altamente especializados.
- CG3. Haber adquirido la capacidad de adaptarse a las nuevas teorías, metodologías y cambios de escenarios habituales en el sector de la ciberseguridad, incluyendo la facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
- CG4. Disponer de la capacidad para la resolución de problemas de manera individual y colectiva, basados en la iniciativa y eficiencia personal, con razonamiento crítico y toma de decisiones importantes, transmitiendo conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional del Ingeniero.
- CG5. Adquirir la capacidad de realizar medidas, cálculos, diagnósticos, estudios, auditorías y la consecuente planificación de proyectos y servicios para la implantación de mejoras en los procesos empresariales.
- CG6. Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio
- CG10. Disponer de la habilidad de trabajar en un entorno multidisciplinar.

##### Basic Competences

- BC 1. Conocerán las funciones básicas de un sistema de control y los principales sistemas de control que hay en la actualidad.
- BC 2. Conocerán las referencias legislativas aplicables a la ciberseguridad de ICs en España (y países de nuestro entorno)
- BC 3. Dispondrán de un conocimiento básico de tendencias actuales en la protección de sistemas de control
- BC 4. Estarán preparados para aplicar el resto de conocimientos adquiridos en el Master de Ciberseguridad en la protección de sistemas de control y de infraestructuras críticas.

### Specific Competences

CS1. Tener una visión general de las características y requerimientos de los productos y servicios de Ciberseguridad en los principales sectores críticos y esenciales que se apoyan en el empleo de Sistemas de Control Industrial, así como el papel de las organizaciones gubernamentales de Ciberseguridad y las tendencias tecnológicas

### Knowledge / Conocimientos

CO1. Arquitecturas y componentes de sistemas ICS/SCADA.

CO2. Modelo Purdue e ISA/IEC 62443.

CO3. Normativa PIC, RCE, NIS y NIS2.

CO4. Metodologías de análisis de riesgos OT.

### Skills / Habilidades

HA1. Analizar riesgos en entornos industriales.

HA2. Diseñar arquitecturas OT seguras.

HA3. Evaluar cumplimiento regulatorio.

HA4. Metodologías de análisis de riesgos OT.

### Learning outcomes / Resultados de Aprendizaje

RA1. Identificar activos, procesos y componentes críticos de un SCI.

RA2. Aplicar metodologías de análisis de riesgos y defensa en profundidad

RA3. Diseñar una arquitectura OT alineada con buenas prácticas y requisitos regulatorios.

RA4. Interpretar obligaciones derivadas de requisitos regulatorios (NIS, NIS2, PIC y RCE).

### Indicators /Indicadores

I1. Ecología integral. ¿La guía docente de esta asignatura incorpora contenidos relacionados con la ecología integral? Sí. La asignatura incorpora contenidos relacionados con la protección de infraestructuras críticas y servicios esenciales cuya disponibilidad es imprescindible para el bienestar social y el desarrollo sostenible. Se analizan aspectos de resiliencia, gestión responsable del riesgo, cumplimiento normativo y protección de sistemas que pueden tener impacto sobre personas, sociedad y medio ambiente.

I2. Bibliografía no occidental. ¿La bibliografía de la asignatura incluye referencias académicas o científicas de perspectivas no occidentales? No. Se excluye a propósito la bibliografía no occidental por motivos de seguridad, asumiendo el posible sesgo que pueda producir la reducción de bibliografía a bibliografía europea y americana.

13. Metodologías docentes. ¿Qué metodologías docentes se incorporan en esta asignatura? Otra, varias de las citadas. La asignatura se desarrolla mediante una combinación de clases magistrales, análisis de casos reales de ciberseguridad industrial, ejemplos de resolución de problemas, laboratorios prácticos y análisis de escenarios de protección de infraestructuras críticas, fomentando un aprendizaje activo, continuo (orientado a retos de forma iterativa).
14. Pedagogía ignaciana. ¿La asignatura se diseña e imparte teniendo en cuenta elementos propios de la pedagogía ignaciana? Sí. La asignatura combina la comprensión del contexto de las infraestructuras críticas con actividades experienciales en laboratorio, análisis de casos reales, reflexión sobre las consecuencias de los incidentes de ciberseguridad y aplicación práctica de medidas de protección, en línea con los principios de la pedagogía ignaciana.
15. PAUs. ¿La asignatura está alineada con las Preferencias Apostólicas Universitarias (PAUs)? Sí. La asignatura contribuye a la formación de profesionales capaces de proteger servicios esenciales para la sociedad mediante la mejora de la resiliencia y ciberseguridad de infraestructuras críticas, alineándose con la promoción del bien común y la sostenibilidad social.
16. IA como apoyo al aprendizaje. ¿La asignatura incorpora el uso de herramientas de Inteligencia Artificial como apoyo al aprendizaje del estudiantado? Sí. La guía ya incluye explícitamente: "Se fomenta un uso responsable de la IA en todas las partes de la asignatura..."
17. Evaluación adaptada a IA. ¿El sistema de evaluación y calificación de la asignatura ha sido revisado o adaptado en relación con el uso de la Inteligencia Artificial? Se ha incorporado una política explícita de uso responsable de herramientas de IA, promoviendo la trazabilidad de su utilización, la supervisión crítica de los resultados obtenidos y el respeto a la propiedad intelectual, manteniéndose la estructura de evaluación actual. La aparición de la IA no ha cambiado pesos ni actividades, pero sí ha requerido una adaptación a la normativa del uso de IA.
18. IA como contenido del temario. ¿El sistema de evaluación y calificación de la asignatura ha sido revisado o adaptado en relación con el uso de la Inteligencia Artificial? La guía actual no contiene ningún tema específico de tamaño significativo dedicado a IA o IA aplicada a ciberseguridad industrial, pero se hacen referencias continuas a la misma y el curso finaliza con una reflexión conjunta sobre el futuro de Ciberseguridad OT y el impacto de la IA.

## TEACHING METHODOLOGY

### General methodological aspects

En cada sesión se combinará una exposición teórica de los aspectos principales del tema en cuestión, con una visión práctica utilizando casos de uso reales que sean ejemplos ilustrativos de ciberataques y servicios de ciberdefensa para prevenir, detectar y responder a los mismos.

La clase será abierta a diferentes grupos de alumnado, con tiempo tras la exposición para la discusión y participación activa entre todos los asistentes y el profesor de la asignatura.

### In-class activities

- 1. Lección expositiva. (aprox. 60% horas):** El profesor desarrolla el temario mediante la proyección de transparencias, vídeos, documentos y el uso de pizarra. Una vez desarrollados los conceptos teóricos, se exponen ejemplos prácticos y reales del día a día del profesor, aportando recomendaciones y soluciones aplicables a la resolución de la problemática identificada. Se potenciará la participación activa de los alumnos para el planteamiento de requisitos y la resolución de los mismos.
- 2. Trabajo con casos prácticos (aprox. 30% horas):** La asignatura comprende la exposición de casos prácticos contenidos en el material de referencia y ejemplos de sistemas de control reales trabajando (tanto en la sesiones teóricas en aula, como en las sesiones prácticas en laboratorio).
- 3. Debates grupales, pruebas y resolución de ejercicios.** Se podrán planificar sesiones específicas para resolver dudas planteadas por los alumnos, así como debates entre los alumnos sobre la importancia y actualidad de las mismas.
- 4. Tutorías.** Se realizarán tutorías en grupo o individualmente para resolver las dudas de los alumnos sobre la materia impartida, así como para orientar el alumno en su proceso de aprendizaje.

### Off-class activities

- 1. Estudio personal** de los contenidos expuestos por el profesor
- 2. Realización de posibles ejercicios/cuestionarios** que el profesor solicite durante la exposición del temario

## ASSESSMENT AND GRADING CRITERIA

| Assessment activities    | Grading criteria                                                                                                                                                                                                                                                                                                                                  | Share |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Examen intermedio        | <ul style="list-style-type: none"> <li>• Comprensión de conceptos relacionados con el funcionamiento de sistemas de control.</li> <li>• Importancia .</li> <li>• Análisis e interpretación crítica de los resultados obtenidos en la resolución de problemas.</li> </ul>                                                                          | 15%   |
| Examen Final             | <ul style="list-style-type: none"> <li>• Comprensión de los conceptos relacionados con el funcionamiento de sistemas control</li> <li>• Comprensión de los conceptos relacionados con la ciberseguridad de sistemas control</li> <li>• Referencias básicas sobre la legislación para protección de infraestructuras críticas en España</li> </ul> | 50%   |
| Prácticas de Laboratorio | <ul style="list-style-type: none"> <li>• Trabajo con PLCs, estaciones de interfase hombre máquina y su entorno de configuración y programación.</li> <li>• Revisión pirámide automatización y los conceptos de protección de una instalación.</li> </ul>                                                                                          | 20%   |
| Proactividad y esfuerzo  | <ul style="list-style-type: none"> <li>• Actitud y esfuerzo: Iniciativa y proactividad en el trabajo, y colaboración en el trabajo en equipo.</li> <li>• Habilidades de comunicación en la escritura y en las presentaciones verbales.</li> </ul>                                                                                                 | 15%   |

## GRADING AND COURSE RULES

### Grading

#### Regular assessment

- El 15% de la nota será por la valoración de la proactividad y actitud en clase
- El 15% de la nota será el examen intermedio
- El 20% de la nota será por las prácticas del laboratorio
- El 50 % de la nota será el examen final

Para aprobar la asignatura los alumnos tienen que alcanzar al menos 5 puntos sobre 10 en el examen final.

#### Retakes

Se mantendrán las notas de proactividad y presentaciones.

Adicionalmente se realizará un examen final extraordinario que valdrá un 65% de la nota

Para aprobar la asignatura los alumnos tienen que alcanzar al menos 5 puntos sobre 10 en el examen final extraordinario.

#### Course rules

- La asistencia a clase es obligatoria según el Artículo 93 del Reglamento General de la Universidad Pontificia Comillas, y el Artículo 6 de las Normas Académicas de la Escuela de Ingenieros del ICAI. El no cumplimiento de éste requisito tendrá las siguientes consecuencias:
  - A los alumnos que no atiendan más de un 15% de las clases, se les podrá denegar el derecho de realizar el examen final en la convocatoria ordinaria.
  - Respecto a las Prácticas de Laboratorio, la ausencia de más del 15% de las sesiones, se les podrá denegar el derecho a la realización del examen final tanto en la convocatoria ordinaria como en la extraordinaria.
- Los alumnos que cometan alguna irregularidad en las actividades académicas, recibirán una nota de cero en dicha actividad, y se iniciará un procedimiento disciplinario según el Artículo 168 del Reglamento General de la Universidad Pontificia Comillas.
- Uso IA en la asignatura: Se fomenta un uso responsable de la IA en todas las partes de la asignatura (incluidos exámenes y pruebas), recomendando referenciar su uso. Ese uso responsable obliga a realizar un adecuado tratamiento de la propiedad intelectual del material que uno usa. El alumno debe ser consciente de que es una herramienta muy útil con una adecuada supervisión, que evite errores y sesgos en sus respuestas.

## WORK PLAN AND SCHEDULE

| In and out-of-class activities                                       | Date/Periodicity               | Deadline |
|----------------------------------------------------------------------|--------------------------------|----------|
| • Examen intermedio                                                  | Mitad de Octubre               | -        |
| • Examen Final                                                       | Último día de clase            | -        |
| • Lecciones y Prácticas                                              | Semanal                        | -        |
| • Seguimiento continuo del auto-estudio y de los conceptos expuestos | Semanal                        | -        |
| • Preparación de las prácticas e informes                            | Puntual dos sesiones a definir | -        |

| STUDENT WORK TIME SUMMARY     |                               |            |                |
|-------------------------------|-------------------------------|------------|----------------|
| IN_CLASS HOURS                |                               |            |                |
| Lectures                      | Lab sessions                  | Assessment |                |
| 27h                           | 4h                            | 3h         |                |
| OFF_CLASS HOURS (recommended) |                               |            |                |
| Self-study                    | Lab preparation and reporting |            |                |
| 8h                            | 2h                            |            |                |
| ECTS credits:                 |                               |            | 3.4 (34 hours) |

## BIBLIOGRAPHY

### Basic

- Industrial Cybersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman
- Guía de Protección de Infraestructuras Críticas y Guía Protección Integral de los Servicios Esenciales en España, Fundación Borredá

### Complementary

- IEC 62443 Redes de comunicación industrial. Seguridad de la TI para redes y sistemas (Ciberseguridad para sistemas de automatización y control industrial).
- NIST CSF 2.0 NIST Cybersecurity Framework.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (PIC).
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- IMC\_01 - Metodología de evaluación de Indicadores para Mejora de la

Ciberresiliencia (IMC), INCIBE

- Esquema Nacional de Seguridad Industrial, ENSI\_C4V\_01- Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V) CERTSI (nombre previo de INCIBE-CERT), Borrador
- Esquema Nacional de Seguridad Industrial, ENSI\_ARLI-CIB\_01- Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB), CERTSI (nombre previo de INCIBE-CERT), Borrador
- Guía sobre controles de seguridad em sistemas OT de Ministerio del interior, 2021
- Directivas europeas PIC, RCE y NIS/NIS2 y sus anteproyectos y proyectos de trasposición
- La protección de Infraestructuras críticas y la Ciberseguridad Industrial, CCI
- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team September 2016, DHS
- Cyber Resilience Review from the U.S. Department of Homeland Security's National Cybersecurity and Communication Integration Center (NCCIC)