GUÍA DOCENTE
2021 - 2022

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Ciberseguridad en la Industria e Infraestructuras Críticas
Código	DEAC-MCS-511
Impartido en	Máster Universitario en Ingeniería de Telecomunicación [Segundo Curso] Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Segundo Curso] Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	3,0 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Electrónica, Automática y Comunicaciones
Responsable	Rafael Palacios
Descriptor	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 Cibersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman • Guía de Protección de Infraestructuras Críticas, Fundación Borredá 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 cibeseguridad de l

Datos del profesorado	
Profesor	
Nombre	Juan Atanasio Carrasco Mateos
Departamento / Área	Departamento de Electrónica, Automática y Comunicaciones
Correo electrónico	jacarrasco@icai.comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Prerequisitos

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.

Competencias - Objetivos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Temario

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 Críticos y Operadores Esenciales
- Obligaciones de un Operador Crítico y obligaciones de un Operador Esencial

TEMAS 15, 16, 17 y 18: Trabajos de interés 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

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Calificaciones

Convocatoria Ordinaria

- **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 o trabajo solicitado
- **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.

Convocatoria Extraordinaria

- 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.

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Industrial Cibersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman

Guía de Protección de Infraestructuras Críticas, Fundación Borredá.