Vicerrectorado de Títulos Propios y Enseñanza a Distancia

Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación

GUÍA DOCENTE DE LA ASIGNATURA

A-42-024 (1) Seguridad en entornos inteligentes

42-MC3-013 (1) Microcredencial Universitaria en De la Internet de las Cosas a la Industria 4.0: Los Fundamentos de la Transformación Digital
42-MC3-013 (2) Microcredencial Universitaria en De la Internet de las Cosas a la Industria 4.0: Los Fundamentos de la Transformación Digital

Curso 2023/2024

1. DATOS IDENTIFICATIVOS DE LA ASIGNATURA	
Programas	42-MC3-013 (1) Microcredencial Universitaria en De la Internet de las Cosas a la Industria 4.0: Los Fundamentos de la Transformación Digital 42-MC3-013 (2) Microcredencial Universitaria en De la Internet de las Cosas a la Industria 4.0: Los Fundamentos de la Transformación Digital
Unidad organizadora	Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación
Código y denominación	A-42-024 (1) Seguridad en entornos inteligentes
Créditos ECTS	1,20
Tipo	Asignatura
Web	
Modalidad de impartición	Virtual asíncrono
Profesor responsable	JORGE LANZA CALDERON
Número de despacho	Edificio Ing. de Telecomunicación Prof. José Luis García García. Planta: - 2. DESPACHO JORGE LANZA (S227)
Email	
Otros profesores	LUIS SANCHEZ GONZALEZ

2. COMPETENCIAS DEL PROGRAMA TRABAJADAS EN LA ASIGNATURA
Competencias genéricas
G17 Resolución de problemas técnicos
G16 Seguridad
Competencias específicas
E19 Usar la tecnología de forma creativa
E16 Proteger datos personales
E15 Proteger dispositivos

3. MODALIDADES ORGANIZATIVAS	
ACTIVIDADES	HORAS
HORAS DE CLASE (A)	
Teoría	10,00
Prácticas	2,00
Seguimiento	3,00
Trabajo autónomo (TA)	15,00

HORAS TOTALES	30,00

4. ACTIVIDADES FORMATIVAS

Las actividades que se contemplan son:

- Impartición de clases magistrales en el aula en la que se introduzcan los diferentes contenidos que conforman el curso. En ellas se fomentará una aproximación creativa a la resolución de las distintas cuestiones que se vayan planteando durante la exposición de los citados contenidos.
- Desarrollo de una actividad de carácter práctico relativa al uso de las tecnologías de la información y las comunicaciones en distintos entornos. A tal fin se conformarán grupos de trabajo que deberán colaborar en el diseño de la solución, así como alternativas a la misma y motivación de su elección.

En concreto, se plantea la siguiente organización en temas:

- Tema 1: Tecnologías de protección de información (2 horas)
    - Criptología
    - Cifrado simétrico y asimétrico. Algoritmos para el cifrado
    - Mecanismos de seguridad
- Tema 2: Infraestructura de clave pública (PKI) (2.5 horas)
    - Certificados digitales
    - Gestión de certificados (PKI)
- Tema 3: Tecnología Blockchain y Distributed Ledger Technologies (1.5 horas)
    - Conceptos generales
    - Algoritmos de consenso
    - Contratos inteligentes
- Tema 4: Seguridad en redes de comunicación IIoT (4 horas)
    - Protocolos de seguridad en Internet (EAP, TLS, DTLS, VPN)
    - Seguridad en redes no convencionales (IEEE 802.15.4, LoRaWAN, …)

Asimismo, se plantea el desarrollo de una sesión práctica:

- Práctica 1: Mecanismos de seguridad en la Internet (2 horas)

5. CALENDARIO

5 de diciembre (09:30-11:30) 2 h. Jorge Lanza Calderón

12 de diciembre (09:30-11:30) 2 h. Jorge Lanza Calderón

13 de diciembre(09:30-11:30) 2 h. Jorge Lanza Calderón

14 de diciembre (16:30-18-30) 2 h. Luis Sánchez González

15 de diciembre (09:30 a 11:30) 2 h. Jorge Lanza Calderón

15 de diciembre (16:30-18:30) 2 h. Luis Sánchez González

Aunque se tratará mantener los horarios de las sesiones síncronas, éstos están sujetos a modificaciones motivadas por situaciones inesperadas o cambio en la planificación.

En cualquier caso, el alumnado será notificado con la suficiente antelación.

6. SISTEMAS DE EVALUACIÓN

Los cursos siguen el modelo de evaluación en el que se combina la evaluación continua y la evaluación final.

La **evaluación continua** consiste en un plan de actividades a realizar por el alumnado, basado en la presentación de ejercicios, tareas, problemas, resoluciones prácticas, intervención en foros, etc. En las actividades de evaluación continua se incluirán pruebas de validación orientadas a que el profesorado verifique la autoría por parte del alumnado. Las pruebas de validación pueden consistir en el seguimiento directo habitual de las actividades propuestas, en la defensa oral presencial o virtual síncrona de los documentos entregados por el alumnado, etc.

La **evaluación final** se realiza mediante una prueba presencial que se celebra tras finalizar el curso, de manera presencial y preferiblemente en sábado. La evaluación final de un estudiante puede ser reducida o completa:

- Evaluación final reducida: la calificación se obtiene mediante una prueba orientada aevaluar conocimientos o competencias que, bien no han sido evaluados mediante evaluación continua, bien han sido evaluados parcialmente mediante evaluación continua, bien han sido evaluados mediante evaluación continua, pero se deseacomprobar su desarrollo también mediante una prueba final.
- Evaluación final completa: la calificación se obtiene mediante una prueba en la que se evalúa cualquier conocimiento o competencia de la asignatura.

La evaluación continua tiene inicialmente un peso del 60% en la calificación del curso, pero si el estudiante no supera la calificación mínima establecida para este tipo de evaluación, realizará una evaluación final completa con un peso del 100%.

La evaluación final reducida tiene inicialmente un peso del 40% en la calificación del curso, pero si el estudiante no supera, bien la calificación mínima establecida para la evaluación final reducida, bien la calificación mínima establecida para superar el curso, realizará una evaluación final completa con un peso del 100%.

7. BIBLIOGRAFÍA

Además del material que se facilitará al alumnado, se proporcionarán diversos artículos científico-técnicos con contenidos de máxima actualidad a fin de ser analizados durante el desarrollo del curso.

Otra bibliografía básica:

- W. Stallings: “Cryptography and Network Security: Principles and Practices”, 8th Edition; Pearson. 2020.
- A. Tanenbaum, Nick Feamster, David J. Wetherall: “Computer Networks”; 6th Edition; Pearson. 2021.

8. INFORMACIÓN ADICIONAL