GUÍA DOCENTE

DENOMINACIÓN DE LA ASIGNATURA

Denominación: **CIBERSEGURIDAD (CS)**
Código: 634009
Plan de estudios: **MÁSTER UNIVERSITARIO EN INTELIGENCIA COMPUTACIONAL E INTERNET DE LAS COSAS** Curso: 1
Créditos ECTS: 3.0 Horas de trabajo presencial: 23
Porcentaje de presencialidad: 30.0% Horas de trabajo no presencial: 52
Plataforma virtual: https://moodegle.uco.es/moodlemap/

DATOS DEL PROFESORADO

Nombre: GÁMEZ GRANADOS, JUAN CARLOS (Coordinador)
Departamento: INGENIERÍA ELECTRÓNICA Y DE COMPUTADORES
Área: ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES
Ubicación del despacho: LV7P190 - LEONARDO DA VINCI
E-Mail: el1gagrj@uco.es Teléfono: 957 218 376
URL web: http://www.uco.es/organiza/departamentos/iec/arquitectura/profesores/jcgamez/

Nombre: HERRUZO GÓMEZ, EZEQUIEL
Departamento: INGENIERÍA ELECTRÓNICA Y DE COMPUTADORES
Área: ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES
Ubicación del despacho: LV7P060 - LEONARDO DA VINCI
E-Mail: el1hegoe@uco.es Teléfono: 957218375
URL web: http://www.uco.es/organiza/~el1hegoe/

REQUISITOS Y RECOMENDACIONES

Requisitos previos establecidos en el plan de estudios

Ninguno

Recomendaciones

Ninguna especificada

GUÍA DOCENTE

COMPETENCIAS

CG2	Manejar las fuentes de información científica y recursos útiles para el estudio y la investigación en los ámbitos de la Inteligencia Computacional y el Internet de las cosas
CG3	Realizar una correcta comunicación oral, escrita y gráfica en los ámbitos de la Inteligencia Computacional y el Internet de las cosas, tanto en niveles científicos como divulgativos
CB7	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 multidisciplinares9 relacionados con su área de conocimiento.
CB10	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
CT1	Analizar y sintetizar conocimiento y realizar un razonamiento crítico.
CT2	Integrar conocimientos y formular juicios y propuestas aplicativas complejas.
CT3	Aplicar los conocimientos adquiridos en la resolución de problemas en contextos nuevos.
CT5	Actuar conforme a un compromiso ético.
CE10	Desarrollar sistemas IoT para proporcionar flujos de información desde entornos físicos a entornos lógicos y viceversa,incorporando las técnicas avanzadas propias de los entornos IoT para la reducción de flujos de información y el manejo de dispositivos estáticos y móviles.
CE12	Establecer los requisitos de securización y/o trazabilidad de los flujos de la información y de las infraestructuras computacionales y de comunicaciones.

OBJETIVOS

Proporcionar al estudiante la capacidad de detectar amenazas, vulnerabilidades y ataques en sistemas en general y sistemas IoT en particular.
Proporcionar al estudiante la capacidad para planificar, desarrollar e implementar actuaciones sobre las amenazas y vulnerabilidades detectadas.
Proporcionar al estudiante la capacidad de establecer e implementar mecanismos para resolver los problemas derivados de los ataques en este tipo de sistemas.
Proporcionar al estudiante la capacidad de estudiar e implementar técnicas para la securización de flujos de información y trazabilidad.

CONTENIDOS

1. Contenidos teóricos

Bloque I.- Introducción a la ciberseguridad.
Bloque II.- Amenazas, vulnerabilidades y ataques a la ciberseguridad.
Bloque III.- Técnicas, herramientas y soluciones para prevenir y resolver los problemas derivados de las amenazas, vulnerabilidades y ataques en este tipo de sistemas.
Bloque IV.- Blockchain como herramienta para trazabilidad y securización de flujos de información

2. Contenidos prácticos

Actividades prácticas relacionadas con los contenidos teóricos para refuerzo de los mismos.

GUÍA DOCENTE

OBJETIVOS DE DESARROLLO SOSTENIBLE RELACIONADOS CON LOS CONTENIDOS

Industria, innovación e infraestructura
Producción y consumo responsables

METODOLOGÍA

Aclaraciones

Se empleará la exposición de contenidos mediante clases magistrales, así como clases prácticas para reforzar los conocimientos teóricos o adquirir capacidades procedimentales relativas al diseño y explotación de las redes de comunicaciones. Cada alumno llevará a cabo uno o varios trabajos de investigación sobre tecnologías emergentes en el ámbito de la ciberseguridad, que serán posteriormente expuestos. Organizados en grupos de trabajo los alumnos realizarán un proyecto de ciberseguridad. Profesorado y alumnado podrán tener una comunicación fluida mediante tutorías virtuales y reuniones periódicas individuales o en grupo.

Actividades presenciales

Actividad	Total
Actividades de evaluación	3
Laboratorio	10
Lección magistral	6
Tutorías	4
Total horas:	***23***

Actividades no presenciales

Actividad	Total
Análisis	6
Búsqueda de información	6
Consultas bibliográficas	10
Ejercicios	10
Estudio	10
Problemas	10
Total horas:	***52***

GUÍA DOCENTE

MATERIAL DE TRABAJO PARA EL ALUMNO

Casos y supuestos prácticos - *https://moodle.uco.es/moodlemap/*
Ejercicios y problemas - *https://moodle.uco.es/moodlemap/*
Presentaciones PowerPoint - *https://moodle.uco.es/moodlemap/*
Referencias Bibliográficas - *https://moodle.uco.es/moodlemap/*

Aclaraciones

El material proporcionado, tanto de contenidos teóricos, guiones de prácticas así como ejercicios y problemas se encuentran disponibles en la plataforma e-learning

EVALUACIÓN

Instrumentos	Porcentaje
Autoevaluación	25%
Exámenes	50%
Trabajos y proyectos	25%

Periodo de validez de las calificaciones parciales:

La calificación de las partes superadas se guardarán durante el curso académico.

Aclaraciones:

BIBLIOGRAFIA

1. Bibliografía básica

William Stallings. *Network Security Essentials*. Pearson
William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson
Anderson, R. J. *Security Engineering*, Wiley
Gollmann, D. *Computer Security*, Wiley

2. Bibliografía complementaria

Ninguna

Las estrategias metodológicas y el sistema de evaluación contempladas en esta Guía Docente serán adaptadas de acuerdo a las necesidades presentadas por estudiantes con discapacidad y necesidades educativas especiales en los casos que se requieran.