COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2024 - 2025

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Ciberseguridad y Protección de la Información
Código	DTC-IMAT-412
Título	Grado en Ingeniería Matemática e Inteligencia Artificial
Impartido en	Grado en Ingeniería Matemática e Inteligencia Artificial [Cuarto Curso]
Nivel	Reglada Grado Europeo
Cuatrimestre	Semestral
Créditos	3,0 ECTS
Carácter	Obligatoria (Grado)
Departamento / Área	Departamento de Telemática y Computación
Responsable	Gregorio Ignacio López López

Datos del profesorado	
Profesor	
Nombre	Gregorio Ignacio López López
Departamento / Área	Departamento de Electrónica, Automática y Comunicaciones
Despacho	A303
Correo electrónico	gllopez@icai.comillas.edu
Profesor	
Nombre	Roberto Gesteira Miñarro
Departamento / Área	Instituto de Investigación Tecnológica (IIT)
Correo electrónico	rgesteira@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

Proporcionar fundamentos de ciberseguridad y protección de la información.

Prerrequisitos

No hay prerrequisitos.

Competencias - Objetivos

Competencias

GENERALES

CG08	Capacidad para identificar, analizar y definir los elementos significativos que constituyen un problema vinculado a la explotación de datos e inteligencia artificial aplicada a las actividades empresariales para resolverlo con criterio y de forma efectiva
CG15	- Capacidad para trabajar en un contexto internacional
ESPECÍFICAS	
CE09	Capacidad para analizar, diseñar y resolver problemas reales a través de técnicas algorítmicas mediante un lenguaje de programación
CE26	Capacidad para aplicar técnicas de inteligencia artificial adecuadas para la realización de trabajos y proyectos de ingeniería.
CE31	Capacidad para especificar, diseñar e implementar las técnicas de aprendizaje automático y profundo para la resolución de problemas complejos.

Resultados de Aprendizaje	
RA1	Tener una visión global de la importancia de la seguridad y la privacidad en los sistemas de información
RA2	Conocer los riesgos asociados a una mala gestión de la seguridad, en las infraestructuras, en el diseño de herramientas, en la gestión de la información, y en el almacenamiento
RA3	Conocer las funciones principales de la gestión de la seguridad: Identificar, Proteger, Detectar, Responder y Recuperar
RA4	Tener un conocimiento global de la legislación y la normativa relativa a seguridad
RA5	Conocer diferentes tipos de algoritmos criptográficos, para anonimización, cifrado, firma electrónica y blockchain
RA6	Conocer cómo aplicar técnicas de Inteligencia Artificial y de tratamiento de información para proteger y detectar ataques

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

La asignatura consta de 3 bloques temáticos:

1. Teoría
2. Prácticas de laboratorio
3. Proyecto final

Teoría

Tema 1. Introducción

1.1. Principios de la ciberseguridad

1.2. Estudio de casos

Tema 2. Privacidad

2.1. Concepto de privacidad

2.2. Normativa

2.3. Estudio de casos

Tema 3. Criptografía

3.1. Criptografía simétrica

3.2. Criptografía asimétrica

3.3. Aplicaciones

Tema 4. Gestión de riesgos

4.1. Concepto de riesgo

4.2. Frameworks y metodologías

4.3. Estudio de casos

Tema 5. Gestión de vulnerabilidades

5.1. Concepto de vulnerabilidad

5.2. Gestión de vulnerabilidades

5.3. Estudio de casos

Tema 6. Inteligencia Artificial y Seguridad

6.1. Aplicaciones de la Inteligencia Artificial a la Ciberseguridad

6.2. Seguridad en sistemas basados en Inteligencia Artificial

6.3. Estudio de casos

Prácticas de laboratorio

Práctica 1

Fundamentos de seguridad

Práctica 2

Privacidad

Práctica 3

Criptografía

Práctica 4
Vulnerabilidades
Práctica 5
Aplicaciones de la Inteligencia Artificial a la Cibserseguridad

Proyecto final
Proyecto final
Desarrollo de un proyecto final en el que el estudiante podrá integrar los conceptos vistos en teoría y en las sesiones de laboratorio y profundizar en ellos.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura
La asignatura contarás de sesiones de teoría, en la que también se aplicarán los conceptos teóricos al estudio y discusión de casos prácticos, y sesiones de laboratorio. Con el fin de conseguir la adquisición de las competencias propuestas, la materia se desarrollará teniendo en cuenta la actividad del alumno como factor prioritario. Por tanto, tanto las sesiones teóricas como las de laboratorio promoverán la implicación activa de los alumnos en las actividades de aprendizaje.

Metodología Presencial: Actividades	
Lección expósitiva: El profesor explicará los conceptos fundamentales de cada tema.	CE09, CG08, CG15, CE26, CE31
Estudio y discusión de casos: Se aplicarán los conceptos teóricos para analizar casos y aplicaciones relacionados.	CE09, CG08, CG15, CE26, CE31
Prácticas de laboratorio: Permitirán al alumno obtener experiencia práctica de primera mano con los temas estudios en teoría.	CE09, CG08, CG15, CE26, CE31

Metodología No presencial: Actividades	
Estudio de los conceptos expuestos en las lecciones presenciales.	CE09, CG08, CG15, CE26, CE31
Realización de trabajos de investigación relacionados con los conceptos expuestos en las lecciones presenciales.	CE09, CG08, CG15, CE26, CE31
Preparación de prácticas de laboratorio.	CE09, CG08, CG15, CE26, CE31

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES

Clases magistrales expositivas y participativas	Sesiones prácticas con uso de software	Tutorías para resolución de dudas	Ejercicios prácticos y resolución de problemas	Actividades de evaluación continua del rendimiento
19.00	8.00	5.00	8.00	2.00
HORAS NO PRESENCIALES				
Sesiones prácticas con uso de software	Estudio personal	Ejercicios prácticos y resolución de problemas	Trabajos	
8.00	15.00	5.00	20.00	
CRÉDITOS ECTS: 3,0 (90,00 horas)				

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	Peso
Realización de exámenes: Examen Intersemestral (15%) Examen Final (35%) Para aprobar la asignatura el alumno deberá obtener al menos 5 puntos sobre 10 en el examen final de la asignatura.	Comprensión de conceptos. Aplicación de conceptos a la resolución de problemas prácticos. Análisis e interpretación de los resultados obtenidos en la resolución de problemas. Presentación y comunicación escrita.	50 %
Proyecto final integrador en el que el estudiante aplicará los conceptos vistos en teoría así como en las sesiones prácticas realizadas.	Complejidad técnica. Calidad de la implementación. Presentación de resultados.	20 %
Prácticas de laboratorio relacionadas con los temas vistos en teoría.	Aplicación de los conceptos teóricos. Habilidad para manejo de software.	30 %

Calificaciones

La calificación variará entre la convocatoria ordinaria y extraordinaria, reduciéndose ligeramente en esta última el peso de la evaluación continua.

Convocatoria ordinaria

La teoría representará el 50% de la nota final:

- Evaluación continua: 15%
- Examen final: 35% (se exigirá nota mínima de 5)

Las practicas de laboratorio representarán el 30% de la nota final.

El proyecto final representará un 20% de la nota final.

Convocatoria extraordinaria

La teoría representará el 50% de la nota final:

- Evaluación continua: 10%
- Examen final: 40% (se exigirá nota mínima de 5)

Las practicas de laboratorio representarán el 30% de la nota final.

El proyecto final representará un 20% de la nota final.

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Transparencias de la asignatura.

Bibliografía Complementaria

- RGDP
- NIST Risk Management Framework
- MAGERIT
- AI Act
- C. Valero, J. Pérez, S. Solera-Cotanilla, M. Vega-Barbas, G. Suárez-Tangil, M. Álvarez-Campana, G. López. Analysis of security and data control in smart personal assistants from the user's perspective. *Future Generation Computer Systems*, Vol. 144, pp. 12 - 23, 2023.
- J. Fúster de la Fuente, S. Solera-Cotanilla, J. Pérez, M. Vega-Barbas, R. Palacios, M. Álvarez-Campana, G. López. Analysis of security and privacy issues in wearables for minors. *Wireless Networks*. 2023.
- J. González, et al, "Does Facebook use sensitivie data for advertising purposes?", Communications of the ACM, 64(1), Jan. 2021, Pp. 62-69
- J. Pérez, M. Castro, E. Awad, G. López. Generation of probabilistic synthetic data for serious games: A case study on cyberbullying. *Knowledge-Based Systems*, Vol. 286, 2024.
- L. Hernández Encinas. La criptografía. ¿Qué sabemos de?, 69, CSIC-Catarata., Madrid, 2016
- E. M. Hutchins, et al, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". Lockheed Martin Corporation

En cumplimiento de la normativa vigente en materia de **protección de datos de carácter personal**, le informamos y recordamos que puede consultar los aspectos relativos a privacidad y protección de datos que ha aceptado en su matrícula entrando en esta web y

pulsando “descargar”

https://servicios.upcomillas.es/sedeelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792