



## FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Ciberseguridad/Cybersecurity
Código	E000014021
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
Horario	Mañana
Horario de tutorías	A acordar con el profesor

Datos del profesorado	
<b>Profesor</b>	
Nombre	Sergio Laborda Castellote
Departamento / Área	Departamento de Telemática y Computación
Correo electrónico	slaborda@comillas.edu
<b>Profesor</b>	
Nombre	Manuel Mora de Amarillas
Departamento / Área	Escuela Técnica Superior de Ingeniería (ICAI)
Correo electrónico	mmdeamarillas@comillas.edu
<b>Profesor</b>	
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	
<b>Aportación al perfil profesional de la titulación</b>	
Proporcionar fundamentos de ciberseguridad y protección de la información	
<b>Prerrequisitos</b>	
No hay prerrequisitos	



## Competencias - Objetivos

### Competencias

#### AAAGENERALES

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

#### AAAESPECÍFICAS

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

Acrónimo	Descripción
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

### 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

SQL Injection

## 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 contará 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 estudiados 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
<u>19</u>	<u>8</u>	<u>5</u>	<u>8</u>	<u>2</u>
Horas No Presenciales				
Sesiones prácticas con uso de software	Estudio personal	Ejercicios prácticos y resolución de problemas	Trabajos	
<u>8</u>	<u>15</u>	<u>5</u>	<u>20</u>	
<b>CRÉDITOS ECTS: 3 (90 horas)</b>				

## EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	Peso
Realización de exámenes: <ul style="list-style-type: none"> <li>Examen Intersemestral (15%)</li> <li>Examen Final (35%)</li> </ul> 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



Actividades de evaluación	Criterios de evaluación	Peso

## 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.

## Normas de uso de la IA

La IA puede utilizarse para actividades previas a la tarea, como la lluvia de ideas, la descripción, y la investigación inicial. Este nivel se centra en el uso de la IA para la planificación, las síntesis y la generación de ideas, pero las evaluaciones deben hacer hincapié en la capacidad de desarrollar y refinar estas ideas de forma independiente. La IA puede utilizarse para ayudar a completar la tarea, incluida la generación de ideas, la redacción, la retroalimentación y la evaluación. Los estudiantes deben evaluar y modificar críticamente los resultados sugeridos por la IA, demostrando su comprensión. En todo caso, el uso de la IA tiene que estar citado y las fuentes verificadas de forma independiente por el alumno.

No se permite el uso de la IA en ninguna de las pruebas de examen, ni en los test de evaluación del rendimiento.

## BIBLIOGRAFÍA Y RECURSOS

### Bibliografía Básica

Transparencias de la asignatura.

### Bibliografía Complementaria

- RGDP



# COMILLAS

UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

**GUÍA DOCENTE**

**2025 - 2026**

- 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 sensitive 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