COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

Syllabus
2025 - 2026

TECHNICAL SHEET OF THE SUBJECT

Data of the subject

Subject name	Ciberseguridad/Cybersecurity
Subject code	E000014021
Involved programs	Grado en Análisis de Negocios/Bachelor in Business Analytics [Third year] Grado en Admin. y Dirección de Emp. y Grado en Análisis de Negocios/Bachelor in Business Analytics [Third year]
Level	Reglada Grado Europeo
Quarter	Semestral
Credits	3,0 ECTS
Type	Obligatoria (Grado)
Department	Department of Telematics and Computer Sciencies
Schedule	Morning
Office hours	To be agreed with the teacher

Teacher Information

Teacher

Name	Sergio Laborda Castellote
Department	Department of Telematics and Computer Sciencies
EMail	slaborda@comillas.edu

Teacher

Name	Manuel Mora de Amarillas
Department	Escuela Técnica Superior de Ingeniería (ICAI)
EMail	mmdeamarillas@comillas.edu

Teacher

Name	Roberto Gesteira Miñarro
Department	Instituto de Investigación Tecnológica (IIT)
EMail	rgesteira@comillas.edu

SPECIFIC DATA OF THE SUBJECT

Contextualization of the subject

Contribution to the professional profile of the degree

Provide cybersecurity and information protection fundamentals.

Prerequisites

There are no prerequisites

Competencies - Objectives

THEMATIC BLOCKS AND CONTENTS

Contents - Thematic Blocks

The course consists of three thematic sections:

1. Theory
2. Laboratory
3. Final Project

Theory

Topic 1. Introduction

1. Principles of Cybersecurity
2. Case Studies

Topic 2. Privacy

1. The Concept of Privacy
2. Regulations
3. Case Studies

Topic 3. Cryptography

1. Symmetric Cryptography
2. Asymmetric Cryptography
3. Applications

Topic 4. Risk Management

1. The Concept of Risk
2. Frameworks and Methodologies
3. Case Studies

Topic 5. Vulnerability Management

1. The Concept of Vulnerability
2. Vulnerability Management
3. Case Studies

Topic 6. Artificial Intelligence and Security

1. Applications of Artificial Intelligence to Cybersecurity
2. Security in Systems Based on Artificial Intelligence
3. Case Studies

Laboratory

Practice 1
Security Fundamentals

Practice 2
Privacy

Practice 3
SQL Injection

Final Project

Development of a final project in which the student will be able to integrate the concepts covered in theory and laboratory sessions and delve deeper into them.

TEACHING METHODOLOGY

General methodological aspects of the subject

The course will consist of theoretical sessions, in which theoretical concepts will also be applied to the study and discussion of practical cases, and laboratory sessions. In order to achieve the acquisition of the proposed skills, the course will be developed with student activity as a priority. Therefore, both theoretical and laboratory sessions will promote active student engagement in the learning activities.

In-class Methodology: Activities

Lecture: The instructor will explain the fundamental concepts of each topic. (CE09, CG08, CG15, CE26, CE31)
Case Study and Discussion: Theoretical concepts will be applied to analyze related cases and applications. (CE09, CG08, CG15, CE26, CE31)
Laboratory Practices: These will allow students to gain firsthand practical experience with the theoretical topics studied. (CE09, CG08, CG15, CE26, CE31)

Non-Presential Methodology: Activities

Study of the concepts presented in the in-person lessons. (CE09, CG08, CG15, CE26, CE31)
Completion of research projects related to the concepts presented in the in-person lessons. (CE09, CG08, CG15, CE26, CE31)
Preparation of laboratory exercises. (CE09, CG08, CG15, CE26, CE31)

SUMMARY STUDENT WORKING HOURS

- In-Person Hours
  - Expository and participatory master classes, → 19
  - Practical sessions using software, →8
  - Tutorials to resolve doubts → 5
  - Practical exercises and problem-solving → 8
  - Continuous performance assessment activities →2
- Out-of-Person Hours
  - Practical sessions using software → 8
  - Personal study → 15
  - Practical exercises and problem-solving → 5

- Assignments → 20

ECTS CREDITS: 3 (90 hours)

EVALUATION AND CRITERIA

Assessment Activities

- Exams:(50%)
  - Intersemester Exam (15%)
  - Final Exam (35%)
  - To pass the course, the student must obtain at least 5 points out of 10 on the final exam.
  - Evaluation criteria
    - Understanding of concepts.
    - Application of concepts to practical problem-solving.
    - Analysis and interpretation of the results obtained in problem-solving.
    - Presentation and written communication.
- Integrating final project in which the student will apply the concepts covered in theory as well as in the practical sessions. (20%)
  - Evaluation criteria
    - Technical complexity.
    - Quality of implementation.
    - Presentation of results.
- Laboratory practices related to the topics covered in theory. (30%)
  - Evaluation Criteria
    - Application of theoretical concepts.
    - Software handling skills.

Ratings

The grading will vary between the ordinary and extraordinary calls, with the weight of continuous assessment being slightly reduced in the latter.

Ordinary Call

Theory will represent 50% of the final grade:

- Continuous assessment: 15%
- Final exam: 35% (a minimum grade of 5 will be required)

Laboratory exercises will represent 30% of the final grade.

The final project will represent 20% of the final grade.

Extraordinary Call

Theory will represent 50% of the final grade:

- Continuous assessment: 10%
- Final exam: 40% (a minimum grade of 5 will be required)

Laboratory exercises will represent 30% of the final grade.

The final project will represent 20% of the final grade.

AI Policy

AI can be used for pre-assignment activities such as brainstorming, outlining, and initial research. This level focuses on the use of AI for planning, synthesizing, and generating ideas, but assessments should emphasize the ability to independently develop and refine these ideas. AI can be used to assist in completing the assignment, including idea generation, writing, feedback, and evaluation. Students should critically evaluate and modify the outcomes suggested by AI, demonstrating their understanding. In all cases, the use of AI must be cited and the sources independently verified by the student.

The use of AI is not permitted in any examination papers or performance assessment tests.

BIBLIOGRAPHY AND RESOURCES

Basic Bibliography

Subject presentations

Complementary Bibliography

- 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