UNIVERSIDAD DE MURCIA

1. Identification

1.1. About the course

Academic Term	2025/2026
Degree	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD / MASTER IN CYBERSECURITY
Course	TÉCNICAS DE GESTIÓN DE LA CIBERSEGURIDAD
Code	7813
Year	PRIMERO
Course type	OBLIGATORIA
Number of groups	1
ECTS	6.0
Estimation of workload	150.0
Timeline	1º Cuatrimestre
Languages	English

1.2. Teaching staff

GIL PEREZ, MANUEL

Professor: **GRUPO 1**

Group coordination: **GRUPO 1**

Course coordinator

Category
PROFESORES TITULARES DE UNIVERSIDAD

Area
CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL

Department
INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Email / Personal web page / Online tutoring sessions
mgilperez@um.es http://webs.um.es/mgilperez Online tutoring sessions: **Sí**

Phone number and office hours

Duration:	Day:	Hours:	Place:
A	Martes	17:00-18:30	868887645, Facultad de Informática B1.1.025

Remarks:
Despacho 1.14.

Duration:	Day:	Hours:	Place:
A	Lunes	11:30-13:00	868887645, Facultad de Informática B1.1.025

Remarks:
Despacho 1.14.

2. Presentation

This subject covers aspects related to security governance in cybersecurity scenarios to comply with current regulations and legislation, in addition to identifying, measuring and safeguarding security risks in organizations The main objectives of this subject are:

- Cover aspects related to organisational security governance, as well as security project management.
- Identify vulnerabilities, threats and risks in the organisation, as well as possible countermeasures to be applied.
- To accommodate two major interconnected blocks with (i) the management of information security systems and (ii) the identification, analysis and management of security risks.

3. Conditions of access to the course

3.1. Incompatibilities

There are no records

3.2. Requirements

There are no records

3.3. Recommendations

No existen recomendaciones para esta asignatura.

4. Competencies

4.1. Basic competencies

- CB7: Students should know how to apply the knowledge acquired and their problem-solving abilities in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their field of study.
- CB8: Students should be able of integrating knowledge and dealing with the complexity of formulating judgments based on information that, although incomplete or limited, includes reflections on the social and ethical responsibilities linked to the application of their knowledge and judgments.
- CB10: Students should acquire the learning skills that enable them to continue studying in a manner that will largely be self-directed or autonomous.

4.2. Degree competencies

- CG3: Students should be able to identify the applicable regulations and legislation in the field of cybersecurity.
- CE1: Students should be able to manage processes associated with vulnerabilities, threats, and risks within an organization.
- CE2: Students should be able to project, design, and implement intelligent products, processes, services, and infrastructures in the field of cybersecurity.
- CE5: Identify and understand new trends, best practices, standards, regulations, and human aspects related to cybersecurity.

4.3. Transversal and course competencies

There are no records

5. Contents

5.1. Theoretical contents

Block 1: Information security management systems

Theme 1: Cybersecurity and National Security (ENS) in Spain: Objectives and scope, ENS requirements, security measures

- The context: eGovernment services
- Introduction to eGovernment LAW 11/2017
- The National Security Framework (NSF)
- Key Players in Cybersecurity in Spain: CCN CERT, INCIBE, CNPIC, MCCE

Theme 2: Information Security Management Systems (ISMS). ISO 27000 series

- Components of an ISMS
- The ISMS family of standards (ISO 27k)
- ISO 27001 ISMS Requirements
- ISO 27002 Information Security controls
- ISO 27003 ISMS Guidance

- ISO 27005 Guidance on managing IS risks
- ISO 27701 Extension for privacy information management
- ISMS Implementation phases

Theme 3: Security and business continuity plans. ISO 22300 series

- BCP main procedures
- Presentation of ISO 22301
- Clauses for ISO 22301 implementation
- Business Impact Analysis (BIA)
- Presentation of ISO/TS 22317
- Impact, criteria and types

Theme 4: Implementation and auditing of ISMS according to the stages of the Deming cycle: PLAN, DO, CHECK, ACT

- Application of the Deming Cycle in cybersecurity
- Deming cycle in ISO 27001 standard
- Main components of the PDCA cycle

Block 2: Identification, analysis and security risks management

Theme 1: Risk analysis and management: Vulnerabilities, threats, malware

- The (cyber)security cycle
- Risk management life cycle
- Assets identification
- Vulnerability scanning and scoring
- Risk calculations and treatment

Theme 2: Risk identification and analysis methodologies

- NIST and ENISA methodologies
- NIST vs ENISA comparison
- Main risk analysis methodologies
- MAGERIT and PILAR

Theme 3: Security risk management case studies: Controls and safeguards for risk reduction

- Analysis of realistic cybersecurity incidents
- Simulations and cyber exercises
- Discussion and feedback sessions on the exercises conducted

5.2. Practical contents

- ### Practical activity 1: Analysis and compliance with the 27000 series in ISMS

  The objective of this practice is to introduce the student to the knowledge of the ISO 27K family of standards. The activity will be carried out on the implementation of the standard in a medium-sized private or public company, which may vary in difficulty depending on the development of the course.

  Related to:

  - Theme 1: Cybersecurity and National Security (ENS) in Spain: Objectives and scope, ENS requirements, security measures
  - Theme 2: Information Security Management Systems (ISMS). ISO 27000 series

- ### Practical activity 2: ISO 22300 series for business continuity

  The objective of this lab is twofold. Firstly, to produce a report to map the controls established by ISO 27001 with the objectives and tasks of each of the contingency plans articulated in ISO 22301. On the other hand, a study will be also carried out on the generation of a Recovery Time Objective (RTO) plan according to the devices encountered in a practical scenario, in which the impact on timeframes can be clearly seen according to the impact criteria reviewed in class.

  Related to:

  - Theme 3: Security and business continuity plans. ISO 22300 series

- ### Practical activity 3: Implementation of a Security Master Plan

  The objective of this lab is to study and develop a Security Master Plan (SMP) for a small and medium-sized company set as an example in class, with a given set of vulnerable assets to be studied. This plan should include a first risk analysis with the identification of critical assets, as well as the protection measures and security policies to be followed in case of having to deploy responses (potential countermeasures) to possible incidents that could occur.

  Related to:

  - Theme 4: Implementation and auditing of ISMS according to the stages of the Deming cycle: PLAN, DO, CHECK, ACT
  - Theme 1: Risk analysis and management: Vulnerabilities, threats, malware

- ### Practical activity 4: Security risk analysis, MAGERIT/PILAR

  Using the same small and medium-sized company used as an example in the previous lab exercise, the objective of this last lab is to conduct a comprehensive risk management analysis for the sample company, where the potential threats facing the critical assets identified in the previous exercise, including hardware, software, data and key personnel, will be identified and described, as well as to determine the existing vulnerabilities in the company's systems and processes that could be exploited by the identified threats. This vulnerability identification process will make use of repositories such as CVE for manual analysis, as well as the use of automated tools such as OpenVAS.

  Finally, the potential impact of each threat on critical assets will be analyzed, making a risk matrix to prioritize threats according to their probability of occurrence and potential impact. Finally, possible measures to mitigate the identified risks will also be associated, ensuring that they are practical and appropriate to the limited resources of the sample company. The calculation of risks will be performed both following the OWASP methodology and using PILAR tools.

  Related to:

  - Theme 2: Risk identification and analysis methodologies
  - Theme 3: Security risk management case studies: Controls and safeguards for risk reduction

6. Training activities

Training Activity	Methodology	Hours	In-person
A10: Evaluation Activities: Includes any type of evaluation necessary for the course, such as theoretical or practical partial exams, etc.		4.0	0.0
AF1: Synchronous Online Theory Sessions: These are live theoretical sessions conducted by teachers through the Virtual Classroom (real-time classes) where, depending on the teaching methodology, the instructor explains content, conducts group debate activities, resolves and discusses any questions students may have thanks to real-time interaction, etc.		9.0	0.0
AF2: Synchronous Online Laboratory Sessions: These are live practical sessions conducted by teachers through the Virtual Classroom (real-time classes) where, depending on the methodology, the instructor covers aspects related to the practice, answers students' questions, and monitors the practices carried out by the students (individually or in groups).		9.0	0.0
AF3: Asynchronous Theory Sessions: Theoretical educational content is provided by specialists in their field. This content is offered to students as material and can be developed in different environments, presenting various formats: lectures, interviews, analysis of examples and/or real cases, multimedia animations, etc. They are permanently accessible to students in the degree's document repository and can be supplied as the course progresses.		9.0	0.0
AF4: Asynchronous Laboratory Sessions: Practical educational content is provided by specialists in their field. This content is offered to students as material and can be developed in different environments, presenting various formats: lectures, interviews, analysis of examples and/or real cases, multimedia animations, etc. They are permanently accessible to students in the degree's document repository and can be supplied as the course progresses.		9.0	0.0
AF6: Tutorials: Individual or group tutorials where the teacher resolves specific doubts, guides, supports, and helps students in their work development and competency acquisition.		4.0	0.0
AF8: Seminars: These are conducted virtually to address more complex issues that arise in the completion of assignments, with common elements that serve as guidance for most students. They can also consist of specific training seminars such as data analysis or bibliography management, to name a few examples.		4.0	0.0
AF9: Autonomous Work: Students time to reviewing and studying the theoretical /practical content of the course, searching for bibliographic information, carrying out readings, etc.		102.0	0.0
	Total	150.00	

This is a subject without teaching activities as it is included in a curriculum to be extinguished. Therefore, the Training Activities shown in this section may not correspond to those carried out during the course and may be redefined in the remarks section.

7. Course schedule

https://www.um.es/en/web/estudios/masteres/ciberseguridad/2025-26#horarios

8. Assessment systems

Identifier	Name of the assessment tool	Assessment criteria	Weighting
IE1	Continuous Assessment: The grade for each course is obtained by taking into account various types of assessments throughout the semester (see section 5.1).	* For the regular/ordinary evaluation call (35%): This evaluation instrument will be measured through various controls following a continuous evaluation approach throughout the development of the course; controls that aim to evaluate the knowledge acquired on, mainly, the theoretical part of the course through exercises, multiple-choice questions, etc. * Note that for the resit evaluation call (0%): CA does not apply, so the 35% of evaluation grade is moved to LR (+10%) and TR (+25%).	35.0
IE2	Theory Report: Evaluation of reports or papers related to the theoretical content of the course.		0.0
IE3	Practical Laboratory Report: Evaluation of reports or papers related to the practical laboratory content of the course.	* For the regular/ordinary evaluation call (50%): This evaluation instrument will be measured through various laboratory reports by means of the delivery of practical material (documents, software, etc.) with the solutions obtained during the laboratory sessions. * Note that for the resit evaluation call the Laboratory Report (LR) grade can reach 60%.	50.0
IE4	Personal or Group Interview: Evaluation of individual or group interviews regarding theory or laboratory work.	* For the regular/ordinary evaluation call (15%): This evaluation instrument will be measured through group or personal interviews for the evaluation of theoretical or practical laboratory work. * Note that for the resit evaluation call the Personal Interview (PI) grade can reach 40%.	15.0

This is a subject without teaching activities as it is included in a curriculum to be extinguished. Therefore, the Evaluation Systems shown in this section may not correspond to those used during the course and may be redefined in the remarks section.

9. Exam dates

https://www.um.es/en/web/estudios/masteres/ciberseguridad/2025-26#examenes

10. Learning outcomes

- Holistically identify the issues related to a particular area of cybersecurity.
- Identify different multidisciplinary aspects (legal, social, ethical) to take into account when tackling a problem related to a particular cybersecurity scenario.
- Identify, organize and plan the technologies to be studied and/or the bibliographic resources to be analyzed in order to tackle a given problem within the field of cybersecurity.
- Identify the regulations and legislation applicable to cybersecurity.
- Plan autonomous work and self-learning processes to be executed as planned.
- List and identify the different types of vulnerabilities, threats and risks within the organization, as well as possible solutions to be applied.
- Describe the principles of risk management, how to apply them and possible tools to be used.
- Describe the main elements and functions that are part of the intelligent services, products and infrastructures in cybersecurity domains.
- Explain the different aspects related to organizational security governance, security project management, design and implementation of products, services and facilities in cybersecurity scenarios.
- Differentiate the most relevant aspects of new trends, best practices, standards, laws and human aspects with respect to existing ones.

11. Bibliography

Group: GRUPO 1

Basic bibliography

There are no records

Further reading

- Tiller, J.S., O'Hanley, R. (2008). Information Security Management Handbook (6th Ed.). Auerbach Publications; ISBN: 1-4200-6708-7.
- Gibson, D., Igonor, A. (2020). Managing Risk in Information Systems (Information Systems Security & Assurance). Jones and Bartlett Publishers, Inc.; ISBN: 978-1284183719.
- Ministry of economic and Digital Transformation Secretariat-General for administration Digital (2014). MAGERIT V.3: Methodology for Information Systems Risk Analysis and Management. Edita.
- Ministry of economic and Digital Transformation Secretariat-General for administration Digital (2022). National Security (ENS).

12. Remarks

If the student does not present some of the evidences that give a grade (IE1 or IE3), the final grade will be "Not Presented".

ADDITIONAL NOTE: This subject is not directly relatedto the Sustainable Development Goals (SDGs).

OBSERVATIONS ON STUDENTS WITH DISABILITIES OR SPECIAL EDUCATIONAL NEEDS

Students with disabilities or special educational needs can contact the Diversity and Volunteering Service (ADYV; https://wwwumes/web/adyv) to receive guidance on how to make better use of their training process and, where appropriate, the adoption of equalisation and improvement measures for inclusion, by virtue of Rectoral Resolution R358/2016 The treatment of information about these students, in compliance with the LOPD, is strictly confidential.

SPECIAL EDUCATIONAL NEEDS

Those students with disabilities or special educational needs may contact the Service of Attention to Diversity and Volunteering (ADYV - https://www.um.es/adyv) to receive guidance on better use of their training process and, where appropriate, the adoption of measures of equalization and improvement for inclusion, under the Rectoral Resolution R-358/2016. The treatment of information about this student body, in compliance with the LOPD, is strictly confidential.

STUDENT EVALUATION REGULATIONS

Article 8.6 of the Student Evaluation Regulation (REVA) provides that "except in the case of activities defined as compulsory in the teaching guide, if the student is unable to follow the continuous evaluation process due to duly justified supervening circumstances, he/she shall be entitled to take a global test".

It is also recalled that Article 22.1 of the Student Evaluation Regulations (REVA) stipulates that "the student who uses fraudulent conduct, including the improper attribution of identity or authorship, or is in possession of means or instruments that facilitate such conduct, will obtain a grade of zero in the evaluation procedure and, where appropriate, may be subject to sanction, after opening disciplinary proceedings".