1. OVERVIEW

Subject area	Computer Security
Degree	Bachelor's Degree in Computer Engineering
School/Faculty	School of Architecture, Engineering and Design
Year	4º
ECTS	6
Type	Elective
Language(s)	Spanish
Delivery mode	On campus / Online
Semester	S8
Year	2022/2023
Coordinating professor	Oscar Cabanillas Nuñéz

2. INTRODUCTION

Computer Security is an elective subject area, worth 6 ECTS credits, in the area of Computing, which is formed by 42 ECTS credits, 6 of which are elective. In today's digital age, where companies and individuals keep important or classified information on their digital devices, it is vitally important to be aware of the existing risks, whether that be in the form of computer attacks, espionage or criminal acts which one could fall victim to, as well as the existing tools to detect, prevent and counteract them.

The subject area summaries the perspective that one should have with regards to computer security and the handling of sensitive data. For this reason, an approach is made through the recommendations of the Data Protection Agency and the LOPD/GDD (The Organic Law on Data Protection and Guarantee of Digital Rights) on how information should be treated by an organisation.

Once the intrinsic importance of the information has been analysed, the computer security will then be looked at from a structural point of view, defining the threats and defence mechanisms in perimeter and logical security environments, with emphasis on the need to establish security policies. Finally, a more practical approach to network security and the application of cryptographic mechanisms to strengthen the use of certain applications will be made. The Computer Science student will make use of the knowledge acquired in previous subject areas to carry out the analysis of a system's vulnerabilities and propose security models and solutions.

3. SKILLS AND LEARNING OUTCOMES

Basic skills (CB, by the acronym in Spanish):

- CB4: Students can communicate information, ideas, problems and solutions to both specialist and non-specialist audiences.
- CB5: Students have developed the learning skills necessary to undertake further study in a much more independent manner.

General skills of the profession (CG, by the acronym in Spanish):

- CG3: Ability to design, develop, assess and ensure the accessibility, ergonomics, usability and security of systems, services and computer applications, as well as the information they manage.

Transversal skills (CT, by the acronym in Spanish):

- CT10: Initiative and entrepreneurial spirit: Ability to undertake difficult or risky actions with resolve. Ability to anticipate problems, propose improvements and persevere to ensure they are implemented. Willingness to take on and carry out tasks.
- CT14: Innovation/Creativity: Ability to propose and invent new, original solutions that contribute towards improving problem situations, including ideas from other contexts.
- CT16: Decision-making: Ability to choose between different options or methods to effectively solve varied situations or problems.
- CT18: Use of information and communication technology (ICT): Ability to effectively use information and communication technology, such as tools for searching, processing and storing information, and for developing communication skills.

Specific skills (CE, by the acronym in Spanish):

- CE18: Knowledge and application of the characteristics, functionalities and structures of databases, enabling their appropriate use, and the design, analysis and implementation of applications based on them.
- CE21: Knowledge and application of the fundamental principles and basic techniques of intelligent systems and their practical application.
- CE23: Ability to design and assess personal computer interfaces that guarantee the accessibility and usability of systems, services and computer applications.
- CE26: Ability to understand the theoretical foundations of programming languages and its associated lexical, syntactic and semantic processing techniques, and know how to apply them to create, design and process languages.
- CE28: Ability to learn about the fundamentals, paradigms and techniques of intelligent systems and to analyse, design and build systems, services and computer applications that use these techniques in any field of application.
- CE29: Ability to acquire, obtain, formalise and represent human knowledge in a computable form to solve problems through a computer system in any field of application, particularly those related to aspects of computing, perception and performance in intelligent environments.
- CE30: Ability to develop and evaluate interactive and complex information presentation systems and their application to solve human-computer interaction design problems.
- CE31: Ability to understand and develop computational learning techniques and design and implement applications and systems that use them, including those dedicated to automatic information extraction and knowledge from large volumes of data.

Learning outcomes (RA, by the acronym in Spanish):

- RA1: Learn the data protection regulations.
- RA2: Understand the concepts of computer security.
- RA3: Implement network security mechanisms.
- RA4: Use cryptographic techniques and mechanisms.
- RA5: Apply forensic analysis techniques.

The following table shows how the skills developed in the subject area match up with the intended learning outcomes:

Skills	Learning outcomes
CB5, CG3, CT10, CT14, CT16, CT18, CE18	RA1: Learn the data protection regulations.
CB5, CG3, CT10, CT14, CT16, CT18, CE23	RA2: Understand the concepts of computer security.
CB5, CG3, CT10, CT14, CT16, CT18, CE26, CE28, CE29, CE30, CE31	RA3: Implement network security mechanisms.
CB5, CG3, CT10, CT14, CT16, CT18, CE21, CE26, CE28, CE29, CE30, CE31	RA4: Use cryptographic techniques and mechanisms.
CB5, CG3, CT10, CT14, CT16, CT18, CE26, CE28, CE29, CE30, CE31	RA5: Apply forensic analysis techniques.

4. CONTENTS

- Data protection regulations.
  a. Personal information and their risks.
  b. Data protection regulations.
  c. LOPD (Data Protection Law)
  d. General Data Protection Regulation.
  e. Compliance Guidelines.
- Physical and Logical Security.
  - Introduction to Computer Security
  - Perimeter Security
  - Logical Security
- Network Security.
  - Introduction to Penetration Testing
  - Network Security
  - WiFi Network Security
  - Example of Man-in-the-Middle attack
- Cryptography.
  - Introduction to cryptography
  - Symmetric ciphers
  - HTTPS and SSL/TLS
- Forensic Analysis.
  - Methodology
  - Evidence acquisition
  - Case study

5. TEACHING/LEARNING METHODS

The types of teaching/learning methods are as follows:

Survey on aims and interests. This survey is used to establish the aims of the subject and gather the student's interests on the subject. We will then make reference to it throughout the year for the students to evaluate the achievement of the aims and interests.

In the online delivery mode, an initial questionnaire will be carried out with the same objective. Throughout the year, reference will be made to this survey, and a final reflective questionnaire will be carried out for the students to check their learning progress of the subject.

Lectures, subjects of study and seminars: The "lectures" taught in the on-campus delivery mode are called subjects of study and seminars in the online delivery mode, and are conducted through readings on the topic, technical notes and webinars (which are recorded for students to access).

Laboratory work: in the on-campus delivery mode, the campus laboratories will mainly be used, while in the online delivery mode, the remote desktop infrastructure will be used.

Group research and/or problem-solving.

Simulation: These will be used for the development of conditional knowledge. It is mainly used to develop practical content in the online delivery mode; however, it is also applicable in the classroom for the on-campus delivery mode.

Practical case studies: These will be used for the development of conditional knowledge. In the online delivery mode, case studies will be used to develop the practical contents of the subject through forums and seminars. This method is also applicable in the classroom for the on-campus modality.

Fieldwork, conferences, visits to companies and institutions: These will be used for the development of conditional knowledge. In the on-campus delivery mode, all learning methods may be used, while only conferences can be used in the online delivery mode, as they will be available for remote access in real time (via streaming technologies) or recorded and broadcast afterwards.

6. LEARNING ACTIVITIES

The types of learning activities, plus the amount of time spent on each activity, are as follows:

On campus:

Learning activity (AF, by the acronym in Spanish)	Number of hours
Lectures, reading on main topics and complementary materials, implementation of activities carried out independently and collectively (including participation in collaborative learning forums).	50
Integrative group work, consisting of participation in debates and seminars, and group implementation of integrative activities, mainly in the classroom.	25
Independent working	50
Tutorials, academic monitoring and assessment, both in the classroom and on the Campus Virtual.	25

Online:

Learning activity (AF, by the acronym in Spanish)	Number of hours
Independent working	50
Independent reading on complementary topics and materials and implementation of activities carried out independently. Online debates and seminars	50
Integrative group work	25
Tutorials, academic monitoring and assessment	25

7. ASSESSMENT

The assessment systems, plus their weighting in the final grade for the subject area, are as follows:

On campus:

Assessment system	Weighting
Exams and Tests	30%
Development of articles, reports and design briefs	15%-30%
Alternative assessment methods with mind maps, diaries, debates, portfolios and/or peer assessment	15%-30%
Fieldwork, conferences, visits to companies and institutions will be evaluated based on the students' participation in a discussion forum	0%-10%
Exercises, problems, case studies, designs, simulations and research. Individual Tasks.	15%

Online:

Assessment system	Weighting
Knowledge tests, exams, test	60%
Development of articles, reports or design briefs	10%-20%
Alternative assessment methods with mind maps, diaries, debates, portfolios and/or peer assessment	10%-20%
Conferences will be assessed based on the students' participation in a discussion forum.	0%-5%
Exercises, problems, case studies, designs, simulations and research. Individual Tasks.	10%-20%

On the Campus Virtual, when you open the subject area, you will find all the details of your assessable tasks and the deadlines and assessment procedures for each task.

7.1. Ordinary exam period

To pass the subject area in the ordinary exam period, you will need a final grade of at least 5.0 out of 10.0 (weighted average) for the subject area.

In any case, you will need a grade of at least 4.0 in the final test for it to be included in the weighting with the other activities.

7.2. Extraordinary exam period (resits)

To pass the subject area in the ordinary exam period, you will need a final grade of at least 5.0 out of 10.0 (weighted average) for the subject area.

In any case, you will need a grade of at least 4.0 in the final test for it to be included in the weighting with the other activities.

Activities not passed in the ordinary exam period, or those not submitted, must be submitted after receiving the relevant corrections and feedback from the lecturer.

8. TIMELINE

The timeline with submission dates for the assessable tasks in this subject area will be indicated in this section:

Assessable tasks	Date
Analysis of the Spanish data protection regulation	
Analysis of a ransomware cyber attack	
WiFi network intrusion	
Cryptographic tools	
Forensic analysis of a device	

The timeline may be subject to change for logistical reasons related to the activities. Students will be informed of any changes in due time and course.

9. BIBLIOGRAPHY

The reference material for the subject area is as follows:

-

The recommended bibliography is indicated below:

-

10. DIVERSITY AWARENESS UNIT

Students with special educational needs:

To ensure equal opportunities, curricular adaptations or adjustments for students with special educational needs will be outlined by the Diversity Awareness Unit (UAD, Spanish acronym).

As an essential requirement, students with special educational needs must obtain a report about the curricular adaptations/adjustments from the Diversity Awareness Unit by contacting unidad.diversidad@universidadeuropea.es at the beginning of each semester.

11. STUDENT SATISFACTION SURVEYS

Your opinion matters!

Universidad Europea encourages you to complete our satisfaction surveys to identify strengths and areas for improvement for staff, degrees and the learning process.

These surveys will be available in the survey area of your campus virtual or by email.

Your opinion is essential to improve the quality of the degree.

Many thanks for taking part.