

Level of qualification:

First cycle (EQF level 6) - Bachelor

Study cycle:

Computer Science Engineering

Course Unit: 9119123 – Communication Networks Security

Year 3

Semester 1

ISCED Code: 612

ECTS: 6,0

Type of Course Unit: Compulsory Delivery Mode: Face-to-face

Language of Instruction: Portuguese

COURSE COORDINATOR: Rui Miguel Soares Silva

HOURS OF WORK

TOTAL HOURS	Contact Hours								Hours in autonomous work
	Theory	Theory and practice	Practical and laboratory work	Field work	Seminar	Internship	Tutorial guidance	Other	
150		15	45						60

Prerequisites (if applicable): Not applicable

LEARNING OUTCOMES (knowledge, skills and competence)

- (i) Understand the importance and transversality of Cybersecurity.
- (ii) Understand and know how to apply, within the scope of Computer Engineering, the scientific foundations of cryptography, namely services and security mechanisms, the main algorithms and protocols.
- (iii) Understand and know how to use Cybersecurity classification systems, languages and notations, and their interrelationships, namely in the areas of Vulnerability Management and Configuration Management.
- (iv) Have a comprehensive knowledge, at a theoretical and scientific level, and, at a practical and applicational level, of Cybersecurity technologies, namely in the design and configuration of solutions for network architectures and network communication systems.
- (v) Understand the role and interrelationship of the Cyber Security and Cyber Defence organizational structures, such as SOCs, CSIRTs, National Cyber Security Centres, Criminal Investigation Police, Cyber Defence Centres.

CONTENTS

1. Introduction to Cybersecurity
2. Notions of Cryptography
3. Cybersecurity Classification Systems
4. Cybersecurity Technologies
5. Firewalls
6. Intrusion Detection\Prevention Systems
7. Virtual Private Networks
8. Integrated Cybersecurity Solutions
9. Cooperation Structures for Cybersecurity
10. Security Operations centres (SOCs)

DEMONSTRATION OF THE CONTENTS COHERENCE WITH THE COURSE UNIT'S LEARNING OUTCOMES

There is a direct mapping between the Syllabus and the defined Objectives, specifically: the objective (i) with syllabus 1; the objective (ii) with the syllabus 2, 4, 7 and 8; the objective (iii) with the syllabus 3, 9 and 10; the objective (iv) with the syllabus 4,

5, 6, 7 and 8; the objective (v) with syllabus 9 and 10.

TEACHING METHODOLOGIES

1. Subject exposition classes: presentation and development of syllabus, using digital educational technologies, such as "Power Point" presentations or similar.
2. Practical demonstration classes: presentation and demonstration of practical applications of the program contents already exposed to the students, always relating to real world situations, using preferably open source software, virtualized systems and physical equipment of several brand technology.
3. Laboratory classes: presentation of laboratory exercises for individual or group performance by students, monitoring by the teacher.
4. Use of virtualization systems to enable hands-on learning, equivalent to real world situations, using pedagogically prepared scenarios.
5. Use of content management platforms to provide support material in multimedia format, such as texts, exercises, presentations, tutorials, video.

DEMONSTRATION OF THE COHERENCE BETWEEN THE TEACHING METHODOLOGIES AND THE LEARNING OUTCOMES

Learning objectives include understanding the technical and scientific foundations and the ability to apply it in practice, both in terms of use, and in terms of design and configuration of solutions, according to the essence of each of the objectives. In the teaching methodologies, use is made of exposition classes of the subject and practical demonstration classes to allow the understanding of the technical and scientific foundations in a pedagogical and interactive way with the students; laboratory classes and virtualization systems are used to enable students to learn their practical applicability. Virtualization systems are also used in demonstration classes by teachers. The content management platform makes it possible to provide students with all multimedia support materials, both for the autonomous study of the syllabus contents, and for carrying out exercises, also allowing the possibility of discussion in a forum environment, of topics related to the curricular unit.

EVALUATION METHODS

Assessment can be carried out by continuous assessment or alternative assessment. Continuous assessment includes a written test (Frequency) with a weighting of 60% in the final grade and a group work with a weighting of 40% in the final grade. The alternative assessment consists only of an exam, which includes a theoretical part and a practical part, with a weighting of 100% in the final grade.

MAIN BIBLIOGRAPHY

- Stallings, William, "Cryptography and Network Security – Principles and Practice", 8th Edition, Pearson Education Inc., 2020.
- Zuquete, André, "Segurança em Redes Informáticas", 5ª Edição, FCA, 2018.
- Muniz, Joseph, "The Modern Security Operations Center", Pearson Education Inc., 2021.
- Murdoch, Don, "Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases", Independently Published, 2019.
- Schneier, Bruce, "Applied Cryptography", 2nd Edition, Wiley, 1996.
- Singh, Simon, "O Livro dos Códigos", Temas e Debates, 1999.

Year of implementation: 2021/2022 | Date of approval by the Technical-Scientific Board: 2021-09-24