CRYPTOGRAPHIE AND COMPUTERS SECURITY

Code: 322027

Main Scientific Area: Information and computer systems

Lecturer: Vitor Manuel Viana Manso

Language of Instruction: Portuguese

Regime: S1

Contact Hours: 60h Total Workload: 108h

ECTS: 6,0

Objectives

The objectives of this course is to equip students with skills in the area of information security in an organizationalcontext understand and recognize the value of information as one of the most important assets of the organization,identify the threats and risks of an Mainframe; promote security policies to ensure business continuity, knowledgeof techniques / tools to use to ensure confidentiality availability and integrity of information.

Learning Outcomes

Students who successfully complete the course should be able to :

Know basic aspects of information security

Recognize the value of information for organizations

Plan and implement security policies

Develop business continuity plans

Identify and implement tools that promote the confidentiality , availability and integrity of information

Implement secure protocols in organizations

Conduct a basic security audit information

Course Contents

1. Security Fundamentals of information systems

2. Information security standards ISO 27001

3. Organizations related to Information Security

4. Security Policies

5. Risk Analysis

6. Information Systems Security Audit

7. Cryptography

Recommended Bibliography

Whitman, M. E., Mattord, H. J. (2012). Principles of information security (4th ed.). Boston, MA: CourseTechnology.

Carneiro, Alberto. (2009). Auditoria e Controlo de Sistemas de Informação, FCA.

Learning and Teaching Methods

The student along the curriculum unit should acquire knowledge in the area of network security in order to be ableto ensure the confidentiality, availability and integrity of information in organizations using the application of a set ofprocedures, techniques and safety tools.

Today information is vital to the success of organizations, threats and risks are more complex and ever-present,makes it critical for students through the skills acquired in the classroom and independently room to designtechnological solutions that ensure business continuity the organization.

Assessment Methods

The evaluation process aims to assess the knowledge and skills acquired , and the student's ability in practicalapplication . Thus , the assessment should include three components :

- A Research Paper (RP) individual , in order to deepen knowledge on security issues Information

- Two Written Tests (WT) detached, essay questions and practical exercises ;

- A Working Group with application of (WG) tools , conducted in a group , with the aim of evaluating theapplication of key skills acquired in solving real problems .

- Continuous evaluation (CE)

The Final Grade(FG) of the course will result from the weighted average of the component scores by applying thefollowing calculation formula :

FG = WT * 40 % + RP* 25 % + WG * 25 % + CE*10%