

## NETWORK AND SYSTEMS FORENSIC AUDITING

---

Code: 322014

Main Scientific Area: Computer networks and architecture

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 organizational context 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, knowledge of techniques / tools to use to ensure confidentiality availability and integrity of information.

### **Learning Outcomes**

Students who successfully complete the course, you should be able to get an overview about the various elements that constitute the forensic Audit networks and systems and their importance in the process of auditing and its application in different scenarios;

Knowledge in the following themes, with special emphasis on:

The importance of Forensic Informatics

General auditing principles

Legal and regulatory context

ISO 27001 and COBIT 5 standards

Data protection systems

Forensic Tools

Property protection and confidential information

Encryption Practices

Online and offline forensic techniques

### **Course Contents**

The importance of Forensic Informatics

General auditing principles

Legal and regulatory context

ISO 27001 and COBIT 5 standards

Data protection systems

Forensic Tools

Property protection and confidential information

Encryption Practices

Online and offline forensic techniques

### **Recommended Bibliography**

Michael A. Caloyannides: Computer Forensics and Privacy, Artech House Publishers

Chris Prosise, Kevin Mandia, Matt Pepe: Incident Response and Computer Forensics, Second Edition,

McGraw-Hill Osborne Media

Brian Carrier: File System Forensic Analysis, Addison-Wesley Professional

Harlan Carvey: Windows Forensics and Incident Recovery, Addison-Wesley Professional

### **Learning and Teaching Methods**

To acquire the knowledge, students will be able to get an overview about the various procedures of Forensic Audit of networks and systems, their function and relationship, know various techniques and Forensic Tools on line and off line, protect data and apply encryption, meet ISO 27001 and COBIT standards and their interpretation and application, meet the legal and normative context.

They will learn to understand and implement the main techniques of protection of confidential information.

### **Assessment Methods**

The assessment consists of two theoretical components and a practical component. The theoretical components have a total weight of 50% (25% + 25%), and the practical component a 40% weight, attendance and class

Participation (+ 10%). The practical work is required. Is required to obtain 7.5 values to each of the components, the final grade must be greater than or equal to 10 values, for approval.

Continuous Evaluation:

Two Written Tests (25% + 25%)