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 objective of the curriculum unit of forensic Audit networks and systems, consists:

Transmit the fundamental principles of Forensic Audit of networks and systems, focusing on the most relevant aspects;

Understand the steps and techniques required to plan and develop an audit, how to evaluate information security of

an organization;

Pass the core principles to the analysis of compliance of information security;

Transmit the fundamental principles for data recovery in file systems.

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 standards

Data protection systems

Forensic Tools

Property protection and confidential information

Encryption Practices

Online and offline forensic techniques

Course Contents

The importance of Forensic

InformaticsGeneral auditing

principlesLegal and regulatory

contextISO 27001 and CO

BIT 5 standard

Data protection systemsForensic Tools

Property protection and confidential information

Encryption Practices

Online and offline forensic techniques

Recommended Bibliography

Michael A. Caloyannides: Computer Forensics and Privacy, Artech House PublishersChris Prosise, Kevin Mandia, Matt Pepe: Incident Response and Computer Forensics, Second Edition,McGraw Hill Osborne MediaBrian Carrier: File System Forensic Analysis, Addison?Wesley ProfessionalHarlan 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%)

Practical component (40%)

Attendance + Participation (10%)

Presence at least two-thirds of the contact hours