TÓPICOS AVANÇADOS DE SEGURANÇA INFORMÁTICA

Master in Engenharia Informática

Code: 22700

Main Scientific Area: Computer Architecture, Distributed Systems and Cybersecurity

Lecturer: Paulo Adriano Marques Sousa Teixeira

Language of Instruction: Portuguese

Regime: S1

Contact Hours: 30h Total Workload: 130h

ECTS: 6,0

Objectives

Understand the fundamental concepts of Information Security.

Analyze the main issues in Information Security.

Implement and manage an effective security plan.

Raise awareness about the importance of Information Systems security.

Identify and mitigate vulnerabilities in information systems.

Develop secure software for web platforms and mobile devices.

Understand the security risks in Cloud Computing.

Perform security audits on information systems.

Develop secure web applications.

Learning Outcomes

Students who finish this course unit should be able to:

• Describe concepts related to information security;

• Identify the main fundamental questions on information security;

• Implement, keep and follow and security plan;

• Advocate the importance of application security within an organization;

• Identify and describe the main security vulnerabilities affecting information systems;

• Know and apply mitigation strategies on application security vulnerabilities;

• Identify the security principles in the development of web and mobile applications;

• Know security risks affecting Cloud-based architectures and their mitigation strategies;

• Know tools and techniques for auditing the security of applications.

• Draw and implement application based on secure web services;

Course Contents

1. Information Systems Security Classify organization resources Security event Security incident Security characteristics (CIA) Menaces to information systems Attacks Counter-measures 2. Security Norm ISO 27000 Security Policy Risk Analysis Auditing the security of information systems 3. Vulnerabilities, identification, and mitigation OWASP top 10 CWE - the vulnerability catalog Techniques for vulnerability mitigation - Sanitation of inputs and outputs -White and Black-lists -Data encryption/codification Tools and Techniques for security auditing - SAST, DAST e IAST 4. Security of web and mobile applications Computation architecture on Web and Mobile devices Security principles on Web Programming Authentication and session management Security on data storage 5. Security on Cloud Computing Computation architecture of cloud applications Main risks and mitigations Data protection in the cloud Cloud security as a service Security of Web Services

Recommended Bibliography

William Stallings, Lawrie Brown; Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015. Url: https://www.pearsonhighered.com/program/Stallings-Computer-Security-Principles-and-Pra ctice-3rd-Edition/PGM153489.html

Paulo J. Sousa e Miguel P. Correia, Segurança no Software, FCA, 2010 url: https://www.wook.pt/livro/seguranca-no- software-paulo-jorge-sousa/9621169

Learning and Teaching Methods

The content of this discipline was defined envisaging the learning of the main topics in application security. The concepts are gradually presented and explored. They will be consolidated, in the end, with the development of real applications with strong focus on its own security.

Assessment Methods

The evaluation will consist in one theoretical-practical test and a research work that will be reported under the appearance of a scientific article.