INSTITUTO POLITÉCNICO DE BRAGANÇA

Course Unit	Security Management in Information Systems			Field of study	Computer Engineering		
Bachelor in	Management Informatics			School	School of Technology and Management		
Academic Year	2022/2023	Year of study	3	Level	1-3	ECTS credits	6.0
Type	Semestral	Semester	2	Code	9186-709-3202-00-22		

Workload (hours)	162	Contact hours	T -	TP 60	PL -	TC -	S -	E -	OT -	O -

T - Lectures; TP - Lectures and problem-solving; PL - Problem-solving, project or laboratory; TC - Fieldwork; S - Seminar; E - Placement; OT - Tutorial; O - Other

Name(s) of lecturer(s): Isabel Maria Lopes

Learning outcomes and competences

At the end of the course unit the learner is expected to be able to:
1. Recognise the importance of information systems security issues;
2. Understand the main security and privacy standards;
3. Identify the main types of vulnerabilities, attack vectors on networks and computer systems and solutions to minimise them;
4. Differentiate the main types of ciphers and cryptographic algorithms and their usage scenarios;
5. Use secure development methodologies.

Prerequisites

Not applicable

Course contents

Fundamentals in the area of Information Systems Security and Computer Security, with emphasis on security and privacy standards, on cryptography, on vulnerabilities and computer attacks and on secure development.

Course contents (extended version)

1. Fundamentals of security in computer systems and networks
2. Security and Privacy Guidelines
   - General concepts regarding Information Security
   - Main National and Community Standards and laws for security management
   - National and European Concepts regarding electronic administration and data protection
   - Information systems security policies
3. Introduction to Cryptography
   - Symmetric Cryptography
   - Public-key Cryptography
   - Digital Certificates
   - Digital Signatures
   - Secure Protocols
4. Information Systems Security Threats
   - Vulnerabilities
   - Attacks and Attackers
5. Secure Development
   - Security Development Lifecycle
   - Methodologies and tools to support secure development

Recommended reading

1. Duque, R. , Noivo, D, Almeida e Silva, T. (2016). Segurança Contemporânea, Editora Pactor.
2. Pfleeger, Charles P. , Pfleeger, Shari L. (2006). Security in Computing, Fourth Edition, Prentice Hall PTR.
3. Silva, P, Carvalho, H. e Torres, C. (2003). Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial, Centro Atlântico.
4. A. Zuquete (2013), "Seguranca em Redes Informaticas - 4 ed", FCA.
5. M. Correia e P. Sousa (2010), “Segurança no software”, Lidel.

Teaching and learning methods

The unit will be taught using a combination of lectures, practical classes and the execution of transversal projects for the application of the security concepts. The unit documentation will be available through e-learning facilities, with support via slack/discord.

Assessment methods

1. Final, Supplementary - (Regular, Student Worker) (Final, Supplementary)
   - Practical Work - 75% (Three Jobs, each 25%)
   - Final Written Exam - 25%
2. Special - (Regular, Student Worker) (Special)
   - Practical Work - 60% (Three Jobs, each 20%)
   - Final Written Exam - 40%

Language of instruction

Portuguese

Electronic validation

Isabel Maria Lopes	José Luís Padrão Exposto	José Carlos Rufino Amaro	Nuno Adriano Baptista Ribeiro
04-03-2023	17-03-2023	17-03-2023	27-03-2023