Caracterização da Unidade Curricular/ Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Segurança da Informação / Information Security

Área científica da UC / CU Scientific Area: Informática / Computer Science

Semestre / Semester: 2º

Número de créditos ECTS / Number of ECTS credits: 6

Carga horária por tipologia de horas / Workload by type of hours: TP: 22,5; PL: 22,5; OT: 6; O: 9

Carga letiva semanal / Weekly letive charge: 3h

Docente responsável / Responsible professor: Sérgio Francisco Sargo Ferreira Lopes, Doutor

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Os objetivos específicos pretendidos com a UC de Gestão da Segurança de Informação é que ao final da UC os alunos consigam:

- Propor, implementar e gerir processos de SI;
- Elaborar PSI e propor políticas de SI, através da utilização de metodologias e técnicas de gestão e planeamento consistentes, alicerçados por normas técnicas;
- Realizar a gestão de riscos e vulnerabilidades, aplicando normas técnicas (ISO), elaborando planos de contingência;
- Realizar o controlo de acesso lógico em sistemas/aplicações informáticas, em ambientes físicos com equipamentos informáticos;
- Realizar o planeamento e gestão da proteção ambiental dos meios físicos e digitais de fornecimento de dados e informações;
- Gerir e propor a utilização de ferramentas/aplicações informáticas para a segurança digital, principalmente em ambientes de redes de computadores.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The specific objectives intended with the Information Security Management course is that at the end of the students will be able to:

- Propose, implement and manage IS processes;
- Develop ISP and propose IS policies, through the use of consistent management and planning methodologies and techniques, based on technical standards;
- Perform risk and vulnerability management, applying technical standards (ISO), preparing contingency plans;
- Perform logical access control in computer systems/applications, in physical environments with computer equipment;

- Carry out the planning and management of environmental protection of physical and digital means of providing data and information;
- Manage and propose the use of computer tools/applications for digital security, especially in computer network environments.

Conteúdos programáticos:

1. Introdução e conceituação geral sobre Segurança da Informação (SI)

2. Normas da série ISO/IEC 27000

3. Auditoria de sistemas e organizações empresariais

4. Análise e gestão de riscos e vulnerabilidades em sistemas e organizações empresariais

4.1. Tipos de ameaças, riscos e vulnerabilidades

5. Implementação de processos de SI

5.1. Políticas de SI e planos de SI (PSI)

5.2. Controlo de acesso lógico e físico

5.3. Controlo ambiental de organizações empresariais

5.4. Segurança de aplicações/sistemas informáticos

6. Segurança física e lógica de redes de computadores

6.1. Ferramentas/aplicações de gestão de serviços/sistemas de rede de computadores

6.2. Sistemas de controlo e monitorização de redes de computadores

7. Plano de contingência e continuidade de serviços informáticos

8. Avaliação de sistemas informáticos e aspetos específicos de SI

8.1. Controlo de computadores

8.2. Controlo de sistemas

8.3. Controlo de bases de dados

8.4. Encapsulamento de códigos-fonte

8.5. Criptografia

8.6. Controlo e monitorização de sistemas em ambientes de rede cliente/servidor

8.7. Segurança em *cloud computing*

8.8. Regulamento Geral sobre a Proteção de dados (RGPD)

8.9. Cibercrime

Syllabus:

1. Introduction and the general concept of Information Security (IS)

2. ISO/IEC 27000 series

3. Audit of systems and business organizations

4. Analysis and management of risks and vulnerabilities in business systems and organizations

4.1. Types of threats, risks, and vulnerabilities

5. Implementation of IS processes

5.1. IS policies and IS plans (ISP)

5.2. Logical and physical access control

5.3. Environmental control of business organizations

5.4. Security of computer applications/systems

6. Physical and logical security of computer networks

6.1. Service management tools/applications/computer network systems

6.2. Computer network control and monitoring systems

7. Contingency plan and continuity of IT services

8. Evaluation of IT systems and specific aspects of IS

8.1. Computer control

8.2. Systems control

8.3. Database control

8.4. Encapsulation of source codes

8.5. Cryptography

8.6. Control and monitoring of systems in client/server network environments

8.7. Cloud computing security

8.8. General Data Protection Regulation (GDPR)

8.9. Cybercrime