Caracterização da Unidade Curricular / Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Auditoria em Cibersegurança / Cybersecurity Audit

Área científica da UC / CU Scientific Area: Ciências Informáticas / 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

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

- Explicar o uso de referenciais normativos (standards) numa auditoria e verificar a conformidade em cibersegurança;
- Desenvolver, implementar e executar uma estratégia de auditoria a SGSI;
- Descrever os componentes e os requisitos básicos necessários num plano de auditoria em cibersegurança;
- Descrever os parâmetros necessários para conduzir e relatar auditorias em cibersegurança;
- Avaliar o desenho, implementação e monitorização dos controles de segurança implementados e verificar se garantem a proteção dos ativos de informação da organização;
- Realizar uma análise critica de situações legais e éticas, examinar a sua possível resolução e recomendar um conjunto de ações;
- Princípios orientadores para relatórios de auditoria em cibersegurança.

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

- Explain the use of standards and frameworks in a compliance audit of an ISMS;
- Develop, implement and execute an ISMS audit strategy in compliance with the standard ISO/IEC 27001;
- Describe the components and basic requirements for creating an audit plan;
- Describe the different parameters required to conduct and report on IT audit for organizational compliance;
- Evaluate the design, implementation and monitoring of the implemented security controls and check if they guarantee the protection of the organization's information assets;
- Critically analyze legal and ethical situations, examine their possible resolution and recommend a justifiable course of actions;
- Know the guiding principles for cybersecurity audit reports.

Conteúdos programáticos:

1. Conceitos e definições

1.1. Modelo PDCA e sua aplicação num SGSI

1.2. Normas e diretrizes para auditoria de um SGSI (por exemplo, ISACA, COBIT, ITIL)

2. Processo de auditoria

2.1. Compreender o negócio da organização

2.2. O ciclo de vida da auditoria do SGSI

2.3. Responsabilidade, autoridade e responsabilidade do auditor do SGSI

2.4. Código de ética profissional, leis e regulamentação

3. Processo de Risco de Auditoria

3.1. Elementos de uma análise de risco

3.2. Auditoria baseada na análise do risco e métodos de avaliação de risco

4. Planeamento e Gestão de Auditorias

4.1. Desenvolvimento do plano de auditoria

4.2. Classificação de auditorias e âmbito

4.3. Missão da auditoria

5. Evidência de Auditoria

5.1. Procedimento de recolha de evidências de auditoria

5.2. Conformidade

6. Relatório de Auditoria

6.1. Elaboração do relatório executivo e os resultados

6.2. Comunicação dos resultados da auditoria

Syllabus:

1. Concepts and definitions

1.1. PDCA model and its application in an ISMS

1.2. Standards and guidelines for auditing an ISMS (for example, ISACA, COBIT, ITIL)

2. Audit process

2.1. Understand the organization's business

2.2. The ISMS audit life cycle

2.3. Responsibility, authority and responsibility of the ISMS auditor

2.4. Code of professional ethics, laws and regulations

3. Audit Risk Process

3.1. Elements of a risk analysis

3.2. Audit based on risk analysis and risk assessment methods

4. Audit Planning and Management

4.1. Development of the audit plan

4.2. Classification of audits and scope

4.3. Audit mission

5. Audit Evidence

5.1. Procedure for collecting audit evidence

5.2. Compliance

6. Audit Report

6.1. Elaboration of the executive report and the results

6.2. Communication of audit results