CIBERSEGURANÇA

Licenciatura em Engenharia de Sistemas Informáticos

Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)

Código: 10711

Área Cientifica Predominante: Arquitetura de Computadores, Sistemas Distribuidos e Cibersegurança

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 60h Carga Trabalho: 100h

ECTS: 6,0

Objetivos

O objetivo desta disciplina é dotar os alunos com competências na área da cibersegurança num contexto organizacional; compreender e reconhecer o valor da informação como um dos ativos mais importantes da organização; identificar as ameaças e riscos de um sistema Informático; promover políticas de segurança que assegurem a continuidade de negócio; conhecimento de técnicas/ferramentas a usar para garantir confidencialidade, disponibilidade e integridade da informação. Saber identificar e explorar as principais vulnerabilidades de um Sistema de Informação e desenvolver as medidas adequadas para a sua proteção.

Resultados da Aprendizagem

Os alunos, que concluam com sucesso a disciplina deverão ser capazes:

Conhecer aspetos básicos de segurança da informação

Reconhecer o valor da informação para as organizações

Planear e implementar políticas de segurança

Desenvolver planos de continuidade de negócio

Identificar e implementar ferramentas que promovam a confidencialidade, disponibilidade e integridade da informação

Implementar protocolos seguros nas organizações

Efetuar uma auditoria básica à segurança de informação

Reconhecer os principais algoritmos de criptografia e saber como os utilizar

Explorar as vulnerabilidades de um Sistema de Informação

Desenvolver as medidas necessárias para minorar as vulnerabilidades de um SI

Conteúdos Programáticos

1. Fundamentos de segurança dos sistemas de informação: Ameaças, vulnerabilidades e consequências,

2. Padrões e organizações de segurança da informação;

3. Políticas de segurança: Políticas de segurança; Políticas de confidencialidade; Políticas de Integridade; Políticas de disponibilidade; Políticas híbridas;

4. Gestão de Risco: Tipos de risco; Estratégias de risco; Modelos de Gestão de Risco.

5. Auditoria de Segurança de Sistemas de Informação;

6. Criptografia: Criptografia básica; Gestão de chaves; Técnicas de cifragem e principais algoritmos; Autenticação; Assinaturas Digitais; BlockChains. Algoritmos de Hashing

7. Exploração de sistemas: vulnerabilidade de software, ferramentas e técnicas de hacking; testes de penetração em aplicações web; Hacking ético;

8. Informática forense

Bibliografia Recomendada

A. H., Regalado, D., Linn, R., Sims, S., Spasojevic, B., Martinez, L., … Harris, S. (2018). Gray Hat Hacking - The Ethical Hacker's Handbook (5th ed.). McGraw - Hill Education

Brooks, C. J., Grow, C., Craig, P., Short, D. (2018). Cybersecurity essentials. John Wiley Sons, Inc.Kohnke, A., Sigler, K., Shoemaker, D. (2017). Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework. CRC Press.

Métodos de Ensino e de Aprendizagem

O aluno ao longo da unidade curricular deverá adquirir conhecimentos na área de segurança em redes de forma a serem capazes de garantir a confidencialidade, disponibilidade e integridade da informação nas organizações recorrendo a aplicação de um conjunto de procedimentos, técnicas e ferramentas de segurança.

Hoje a informação é vital para o sucesso das organizações, as ameaças e riscos são mais complexas e sempre presentes, faz com seja fundamental para os alunos através das competências adquiridas em sala de aula e de forma autónoma projetem soluções tecnológicas que assegurem a continuidade de negócio da organização.Os alunos deverão reunir competências para exploração de sistemas, de forma a identificar vulnerabilidades e desenvolverem soluções para essas vulnerabilidades.

Métodos de Avaliação

O processo de avaliação visa aferir os conhecimentos e competências adquiridos, e a capacidade do aluno na sua aplicação prática. Assim, a avaliação deverá incluir três componentes:

- Um Trabalho de Projeto (TP) em grupo, com o objetivo de aprofundar conhecimentos em temas de segurança da Informação

- Uma Prova Escrita (PE) individual, com perguntas de desenvolvimento e exercícios práticos;

- Avaliação Continua (AC)

A Nota Final (NF) da unidade curricular irá resultar a partir da média ponderada da pontuação dos componentes, aplicando a seguinte fórmula de cálculo:NF = PE* 50% + TP * 35% + AC * 15%