

CRIOGRAFIA E SEGURANÇA INFORMÁTICA

Curso Técnico Superior Profissional em Redes e Segurança Informática

Código: 322027

Área Científica Predominante: Sistemas e Tecnologias de Informação

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S1

Carga Letiva: 60h Carga Trabalho: 108h

ECTS: 6,0

Objetivos

Os objetivos desta disciplina é dotar os alunos com competências na área de segurança de informação 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.

Resultados da Aprendizagem

Os alunos, que conclua 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

Conteúdos Programáticos

1. Conceitos básicos de segurança dos sistemas de informação
2. Normas de segurança de informação ISO 27001
3. Organizações relacionadas com Segurança da informação
4. Políticas de Segurança
5. Análise de Risco
6. Auditoria à Segurança dos Sistemas de Informação
7. Criptografia

Bibliografia Recomendada

- Whitman, M. E., Mattord, H. J. (2012). Principles of information security (4th ed.). Boston, MA: Course Technology.
- Carneiro, Alberto. (2009). Auditoria e Controlo de Sistemas de Informação, FCA.
- Silva, Pedro et al. (2003). Segurança dos Sistemas de Informação, Centro Atlântico, 2003
- Shoemaker, D., Conklin, W. A. (2011). Cybersecurity: The Essential Body of Knowledge: Cengage Learning.
- Ferguson, N., Schneier, B., Kohno, T. (2012). Cryptography Engineering: Design Principles and Practical Applications: Wiley

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.

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 Pesquisa (TP) em grupo, com o objetivo de aprofundar conhecimentos em temas de segurança da Informação
- Duas Provas Escritas (PE) individual, com perguntas de desenvolvimento e exercícios práticos;
- Um Trabalho de Grupo com aplicação de ferramentas de (TG), realizado em grupo, com o objetivo de avaliar a aplicação das principais competências adquiridas na resolução de problemas reais.
- Avaliação Contínua (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: $NF = PE1 * 40\% + TP * 25\% + TG * 25\% + AC * 10\%$