TÓPICOS AVANÇADOS DE SEGURANÇA INFORMÁTICA

Mestrado em Engenharia Informática

Código: 22700

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

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S1

Carga Letiva: 30h Carga Trabalho: 130h

ECTS: 6,0

Objetivos

Compreender os conceitos fundamentais da Segurança da Informação.

Analisar as principais questões da Segurança da Informação.

Implementar e gerir um plano de segurança eficaz.

Sensibilizar para a importância da segurança dos Sistemas de Informação.

Identificar e mitigar vulnerabilidades em sistemas de informação.

Desenvolver software seguro para plataformas web e dispositivos móveis.

Compreender os riscos de segurança em Cloud Computing.

Realizar auditorias de segurança em sistemas de informação.

Desenvolver aplicações web seguras.

Resultados da Aprendizagem

Os alunos que terminem esta Unidade Curricular deverão se capazes de:

• Descrever conceitos relativos à Segurança da Informação;

• Identificar as principais questões que fundamentam a atividade da Segurança da Informação;

• Implementar, manter, e seguir um plano de segurança;

• Sensibilizar para a importância da segurança dos Sistemas de Informação numa organização;

• Identificar e descrever as principais vulnerabilidades de segurança em sistemas de informação;

• Conhecer e aplicar os principais meios de mitigação de vulnerabilidades de segurança em sistemas de informação;

• Identificar os princípios de segurança no desenvolvimento de software para plataformas web ou dispositivos móveis;

• Conhecer os riscos de segurança presentes numa arquitetura em Cloud, identificando as principais medidas de resposta para os evitar;

• Conhecer técnicas e ferramentas de auditoria de segurança para sistemas de informação

• Desenhar e implementar aplicações baseadas em serviços web seguros;

Conteúdos Programáticos

1- Segurança dos Sistemas de Informação Classificação dos recursos de uma Organização Evento e Incidências de segurança Características de Segurança (CIA Ameaças aos Sistemas de Informação Ataques Medidas de controlo 2. Norma de Segurança ISO 27000 Política de Segurança Análise de Risco Auditoria à Segurança 3.Vulnerabilidades, Identificação e sua Mitigação O OWASP top 10 Catálogo de vulnerabilidades - CWE Técnicas de mitigação de vulnerabilidades, Sanitização de inputs e outputs, White e Black-lists, Encriptação Técnicas e Ferramentas de auditoria - SAST, DAST e IAST 4. Segurança em Aplicações Web e Móveis Arquitetura de computação na Web e Móveis Princípios de segurança na programação Web Autenticação e gestão de sessões Segurança no armazenamento dos dados 5. Segurança na Computação na Cloud Arquitetura de computação na cloud Principais riscos e medidas de resposta Proteção dos dados na Cloud A segurança da cloud como um serviço Segurança em serviços web

Bibliografia Recomendada

William Stallings, Lawrie Brown; Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015. Url: https://www.pearsonhighered.com/program/Stallings-Computer-Security-Principles-and-Pra ctice-3rd-Edition/PGM153489.html

Paulo J. Sousa e Miguel P. Correia, Segurança no Software, FCA, 2010 url: https://www.wook.pt/livro/seguranca-no- software-paulo-jorge-sousa/9621169

Métodos de Ensino e de Aprendizagem

Os conteúdos programáticos foram definidos tendo em vista a aprendizagem dos principais tópicos de segurança de aplicações. Os conceitos são apresentados e explorados de forma cumulativa e gradativa, sendo no final consolidados com o desenvolvimento de aplicações reais com forte incidência na sua própria segurança.

Métodos de Avaliação

A avaliação consistirá em 1 teste teórico-prático e um trabalho de investigação a reportar sob o aspecto de um artigo científico.