DESENVOLVIMENTO DE SOFTWARE SEGURO

Pós-Graduação em Cibersegurança e Informática Forense

Código: 124003

Área Cientifica Predominante: Ciências da Computação

Docente: Nuno Alberto Ferreira Lopes

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 30h Carga Trabalho: 0h

ECTS: 6,0

Objetivos

Esta unidade curricular tem como principal objectivo familiarizar os alunos com os fundamentos de desenvolvimento de software seguro, através da compreensão de técnicas, metodologias, e boas práticas utilizados na segurança de aplicações.

Resultados da Aprendizagem

Os alunos que concluírem com êxito esta unidade curricular devem ser capazes de:

• conhecer as arquiteturas de aplicações modernas e tradicionais de forma a identificar os padrões de segurança no seu desenvolvimento de forma a criar software seguro;

• compreender conceitos como: fraquezas, vulnerabilidades, riscos, regulamentação, exploração;

• compreender metodologias utilizadas no desenvolvimento de software seguro: SAST, DAST, SCA, SCS;

• compreender, identificar e mitigar as principais vulnerabilidades e riscos de software.

Conteúdos Programáticos

Desenvolvimento de Software e Desenvolvimento de Software Seguro

• Application Security

• Practical Application Security

• Web Security

• API Security

• Cloud Native Application Security – CNAS

• AI, LLMs, Security

• Known Application Security Approaches:

SAST
DAST
SCA
SCS

Bibliografia Recomendada

Miguel Pupo Correia, Paulo Jorge Sousa (2017) Segurança no Software, FCA.

Tanya Janca (2020), Alice and Bob Learn Application Security, Wiley, ISBN: 1119687357.

Code Review Guide - Eoin Keary https://owasp.org/www-project-code-review-guide/assets/OWASP_Code_Review_Guide_v2.pdf

Métodos de Ensino e de Aprendizagem

Os conteúdos programáticos desta UC abordam os principais temas na vasta área do desenvolvimento de software seguro. Estes conceitos permitem a compreensão dos principais vetores de atuação da área de desenvolvimento de software seguro, alavancando a capacidade dos discentes na identificação ativa de eventuais vulnerabilidades e na construção de um processo, adequado ao tipo de projeto e aplicação a ser desenvolvida, que permita o desenvolvimento de aplicações seguras.

Métodos de Avaliação

A metodologia utilizada para avaliar os alunos consiste em dois trabalhos:

• Ensaio escrito (máximo de 10 páginas) sobre práticas de desenvolvimento de software seguro, tendências do desenvolvimento de aplicações, riscos associados, SDLC.

• Trabalho prático focado em revisão e análise de código e remediação do mesmo.