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 objetivo familiarizar os alunos com os conceitos de modelos de arquitetura e desenvolvimento de software, fundamentos de seguranca no desenvolvimento de aplicacoes, identificacao de requisitos e vulnerabilidades, bem como de tecnicas, metodologias e boas praticas para uma programacao segura e confiavel atraves da implementacao e monitorizacao de controlos de seguranca.

Resultados da Aprendizagem

Os alunos que concluírem com êxito este curso devem ser capazes de:

Conhecer a arquitetura das Aplicações Modernas

Adquirir conhecimentos sobre os conceitos básicos de Segurança de Aplicações: Vulnerabilidade, Conformidade, Regulamentação, Riscos, Exploração.

Conhecer as abordagens de segurança das aplicações: SAST, DAST, IAST, SCA, SCS, APIS, IaCS

Dominar as vulnerabilidades de software e a sua correção.

Conteúdos Programáticos

Modern Application Development

Security in MAD

Introduction to App Sec

SAST, DAST, IAST

SCS, SCA and APIS

IaCS

Bibliografia Recomendada

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

Métodos de Ensino e de Aprendizagem

Os conteudos programaticos desta UC abordam os principais temas na vasta area do desenvolvimento de software seguro. Estes conceitos permitem a compreensao dos principais vetores de atuacao da area de desenvolvimento de software seguro, alavancando a capacidade dos discentes na identificacao ativa de eventuais vulnerabilidades e na construcao de um processo, adequado ao tipo de projeto e aplicacao a ser desenvolvida, que permita o desenvolvimento de aplicacoes seguras.

Métodos de Avaliação

A metodologia utilizada para avaliar os alunos consistirá num trabalho prático composto por duas partes. A primeira parte será um ensaio escrito com um máximo de 10 páginas que explorará as tendências actuais do desenvolvimento de aplicações, os riscos de segurança associados e a forma de abordar a segurança ao longo do seu SDLC. A segunda parte consistirá na seleção de uma aplicação vulnerável (por exemplo, WebGoat, kubernetesGoat) e na resolução do maior número de vulnerabilidades encontradas no seu código por uma ferramenta SAST/IaCS. No final, uma análise do código original versus o código remediado deve apresentar uma diminuição dos resultados (>2 em diferentes vulnerabilidades).