

PLANO DE ENSINO

Campus funcionamento: Foz do Iguaçu

Centro responsável: Centro de Engenharias e Ciências Exatas

Programa: Engenharia Elétrica e Computação

Carga horária: 30

Turno: Integral

Creditos: 2

Nível: Mestrado

Data de Fechamento do PE: 02/10/2024 *Prd. Letivo:* 2024/2

Aprovação: 27/09/2024 019

Homologação (Conselho de Centro):

Disciplina

Segurança Computacional

Ementa

Resolução: N° 248/2019-CEPE

Segurança física. Criptografia simétrica e assimétrica. Ciclo de vida de chaves criptográficas. Integridade e autenticação. Assinatura digital. Funções Hash. Entidades certificadoras. Protocolos criptográficos. Vulnerabilidades de softwares, códigos maliciosos e classes de ataques. Segurança de sistemas operacionais e de redes de computadores. Segurança da web. Segurança de sistemas distribuídos. Sistemas de detecção de intrusão.

Docentes

Nome	C/H
Renato Bobsin Machado	30:00

Objetivo geral

Trabalhar conceitos sobre métodos de segurança computacional, com foco na prevenção, detecção e reação a ataques.

Objetivos Específicos

Apresentar conceitos sobre criptografia simétrica e assimétrica, algoritmos e aplicabilidade. Estudar vulnerabilidades e classes de ataques computacionais, com foco em medidas para prevenção e detecção de ameaças e ataques.

Metodologia

Aulas expositivas
Listas de exercícios
Trabalhos teóricos e práticos (com especificação prévia do tema e número de alunos envolvidos)
Seminários (com especificação prévia do tema e número de alunos envolvidos)
Avaliações teóricas e práticas em sala de aula

Atividades Práticas

Avaliação

1. Nota Final: composta pelas Notas de Provas (Equação2) e Notas de Trabalhos (Equação3) segundo a Equação1;
2. Conteúdo das avaliações (provas, trabalhos, dinâmicas em sala e exame): acumulativo;
3. Trabalhos (datas, temas e critérios de avaliação): apresentados por escrito na definição de cada trabalho;

Equação1: $NotaFinal = 0,50 * NotaProvas + 0,50 * NotaTrabalhos$

Equação2: $NotaProvas = (Prova1 + Prova2) / 2$

Equação3: $NotasTrabalhos = (Trabalho1 + Trabalho2 + Trabalho3) / 3$

As provas serão realizadas aproximadamente a cada 1/2 (um terço) da carga horária da disciplina.

Os trabalhos serão realizados aproximadamente a cada 1/3 (um terço) da carga horária da disciplina.

PLANO DE ENSINO

Conteúdo Programático

Título	C/H
Criptografia	10
a. Definições	
b. Algoritmos simétricos	
c. Algoritmos assimétricos	
d. Chaves criptográficas	
e. Funções hash	
f. Assinatura digital	
g. Entidades certificadoras	
2. Vulnerabilidades de Segurança	6
a. Conceitos	
b. Metodologias de Pentest	
c. Ferramentas de Pentest	
Segurança Computacional	6
a. Classes de ataques	
b. Segurança de sistemas operacionais	
c. Segurança na Web	
Prevenção de Detecção de Intrusão	8
a. Conceitos	
b. Classificação	
c. Métodos de prevenção de instrução	
d. Métodos de detecção de intrusão	

bibliografia básica

COULOURIS, G. Sistemas Distribuídos: conceitos e projetos. Editora Bookman. 5a. Ed. 2015.

FERREIRA, DANIEL. Segurança de Rede, Defesa Cibernética e Operações. 1ª edição. FCA, 2024.

TANENBAUM, A. S.; WETHERALL, D.; FEAMSTER, N. Redes de Computadores. 6ª edição. ed. [S.l.]: Pearson, 2021.

SANTOS, JOAS ANTÔNIO; FANCO, DEIVISON PINHEIRO; SOARES, CLEBER. Introdução à Segurança Ofensiva: Uma abordagem para pentesters e red teams. Editora Basport, 2023.

STALLINGS, WILLIAM. Cryptography and Network Security: Principles and Practices. 8ª edição. Pearson, 2022.