MINISTÉRIO DA EDUCAÇÃO

# CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
## *CAMPUS* PETRÓPOLIS

CURSO SUPERIOR DE ENGENHARIA DE COMPUTAÇÃO

| DEPARTAMENTO | PLANO DE CURSO DA DISCIPLINA |
|---|---|
| **Engenharia de Computação** | **Servidores de Redes** |

| CÓDIGO | PERÍODO | ANO | SEMESTRE | PRÉ-REQUISITOS |
|---|---|---|---|---|
| GCOM6037PE | | 2017 | | Redes de Computadores II |

| CRÉDITOS | AULAS/SEMANA | | | TOTAL DE AULAS NO SEMESTRE |
|---|---|---|---|---|
| | TEÓRICA | PRÁTICA | ESTÁGIO | |
| 2 | 1 | 1 | 0 | 36 |

## EMENTA

1.Ataques e classificações de ataques.
2.Técnicas de segurança de redes.
3.IPS/IDS.
4.Firewall.
5.Redundancia.
6.Ataques de negação de serviço.
7.Ataques de força bruta.
8.Ataques de vulnerabilidade
9.Análise de risco.
10.Projetos de proteção e contenção de ataques.
11.Evolução dos ataques e defesas.

.

## BIBLIOGRAFIA


- **Básica:**
- TANENBAUM, A.S. Redes de computadores. Rio de Janeiro: Elsevier: Campus,c2003.
- KUROSE, J.F.; ROSS, K.W.Redes de computadores e a Internet: uma abordagem top-down. 6aedição. São Paulo: Pearson Education: Addison Wesley, 2013.
- FOROUZAN, B.A. Comunicação de dados e redes de computadores. Colaboração de Sophia Chung Fegan. 4a edição. S˜ao Paulo: McGraw-Hill, 2008.
- **Complementar:**
- STALLINGS, W. Criptografia e Segurança de redes: princípios e práticas. 4a edição. São Paulo: Pearson, 2008..
- STALLINGS, W. Redes e sistemas de comunicação de dados: teoria e aplicações corporativas. Rio de Janeiro: Elsevier: Campus, c2005.

- COMER, D.E. Interligação de redes com TCP/IP. Rio de Janeiro: Elsevier: Campus,c2006.
- STEVENS, W.R.; FENNER, B.; RUDOFF, A.M. Programação de rede UNIX, v.1:API para soquetes de redes. 3a edição. Porto Alegre: Bookman, 2005.
- SOARES NETO, V. Telecomunicações: sistemas de modulação: uma visão sistêmica. 3a edição revista, atualizada e ampliada. São Paulo: Erica, 2012.


## OBJETIVOS GERAIS

- Proporcionar ao aluno uma base teórica sobre segurança de redes apresentando os conceitos e politicas envolvidos no processo de segurança da informação;
- Apresentar as principais ferramentas usadas na defesa de redes de computadores;
- Utilizar práticas de laboratórios para aplicar o conhecimento adquirido nas aulas teóricas.

## METODOLOGIA

A metodologia utilizada consistiu de aulas expositivas, utilizando-se o quadro branco e o Datashow. As explicações são feitas com o intuito de proporcionar ao aluno que acompanhe de desenvolva o raciocínio nos protocolos e problemas de comunicação de redes de computadores. Para complementar e ajudar a fixar os conteúdos abordados, foram realizadas diversas aulas de exercícios teóricos e práticos. Complementam também a aula algumas videoaulas que podem ser acessadas pelos alunos.

## CRITÉRIO DE AVALIAÇÃO

Os resultados da avaliação de aproveitamento são expressos em notas, sendo que, para ser aprovado sem o exame final, o aluno deve obter média igual ou superior a 7,0 (sete). O exame final é aplicado aos alunos cuja média seja igual ou superior a 3,0 (três) e inferior a 7,0, caso contrário, o aluno está reprovado. Para a aprovação com exame final, uma prova com o valor de 10,0 (dez) pontos, faz-se uma nova média entre o grau obtido no exame e a média anterior ao exame, o resultado deve ser igual ou superior a 5,0 (cinco).

A disciplina de Redes II consiste de três avaliações, no valor de 10,0 (dez) pontos cada, sendo que a média é obtida entre estas avaliações. As avaliações são constituídas de provas e trabalhos em grupo ou individuais. Não respeitando os critérios supracitados, o aluno realiza o exame final para a conclusão da disciplina.

| CHEFE DO DEPARTAMENTO | |
|---|---|
| NOME | ASSINATURA |
| Laura Silva de Assis | |

| PROFESSOR RESPONSÁVEL PELA DISCIPLINA | |
|---|---|
| NOME | ASSINATURA |
| Dalbert Matos Mascarenhas | |

**APROVADO PELO CONSELHO DEPARTAMENTAL EM: ____/____/____**

## PROGRAMA

- Revisão dos conhecimentos adquiridos nas disciplinas de Redes;
- Descrição das políticas de segurança da informação;
- Analise do histórico de ataques;
- Tipos de ataques ativos.
- Tipos de ataques passivos;
- Exercícios;
- Evolução dos mecanismos de defesa;
- Explicação teórica e pratica de Firewall;
- Explicação teórica e pratica de IDS e IPS;
- Explicação teórica e pratica de mecanismos de redundância;
- Explicação teórica e pratica de criptografia;
- Exercícios práticos e teóricos;
- Técnicas de resposta a incidentes de segurança.
- Exercícios e trabalhos abordando os temas em problemas práticos e teóricos.