



**MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
IFPB – CAMPUS CAMPINA GRANDE
CURSO SUPERIOR DE TECNOLOGIA EM TELEMÁTICA**

PLANO DE DISCIPLINA		
IDENTIFICAÇÃO		
CURSO: Superior de Tecnologia em Telemática		
DISCIPLINA: Segurança de Redes de Computadores		CÓDIGO: TEC.1166
PRÉ-REQUISITOS: Interconexão de redes		
UNIDADE CURRICULAR: Obrigatória [X] Optativa [] Eletiva []		SEMESTRE: 5
CARGA-HORÁRIA		
TEÓRICA: 48 aulas	PRÁTICA: 32 aulas	EaD: 0 aulas
SEMANAL: 4 aulas	TOTAL: 80 aulas* (67 horas)	
DOCENTE RESPONSÁVEL:		

*1 aula = 50 min

EMENTA

Conceitos básicos sobre segurança da informação, políticas de segurança, vulnerabilidades, ameaças e ataques. Aspectos sociais da segurança de redes de computadores. Autenticação, criptografia, mecanismos de integridade de dados e assinatura digital. Configuração de segurança em rede local, controle de acesso e VPNs.

OBJETIVOS

Geral

- Adquirir habilidades teóricas e práticas sobre segurança da informação e de redes de computadores: como prevenir, defender e resolver incidentes de segurança.

Específicos

- Compreender os princípios de segurança;
- Projetar, implementar e gerenciar segurança em redes de computadores – técnicas, equipamentos, aplicações e protocolos para segurança de redes;
- Analisar e testar a segurança dos sistemas de informação;
- Projetar e implementar políticas de segurança para redes de computadores.

CONTEÚDO PROGRAMÁTICO

I. Fundamentos

1. Conceitos básicos sobre segurança da informação e segurança de redes: serviços de segurança, vulnerabilidades, ameaças, ataques, riscos, aspectos de segurança para aplicações em redes TCP/IP
2. Conceitos sobre Políticas e Normas de Segurança
3. Conceitos sobre Engenharia Social

II. Criptografia

1. Introdução à Criptografia
 - Criptografia Simétrica
 - Criptografia Assimétrica
 - Gerência de Chaves
2. Hash, Assinaturas Digitais e Certificados Digitais

III. Segurança de Dispositivos

1. Segurança de dispositivos de rede
2. Segurança de rede local
3. Conceitos e configuração de *firewalls*

IV. Soluções de Segurança

1. Soluções de segurança e tecnologias
 - Sistemas de Prevenção de Intrusão: IPS
 - Acesso remoto seguro: SSH

- Segurança em correio eletrônico: PGP e S/MIME
 - Segurança em camada de transporte: SSL/TLS
 - Segurança em camada de rede: VPN e IPSec
2. Segurança em redes sem fio

METODOLOGIA DO ENSINO

A apresentação do conteúdo dar-se-á mediante aulas teóricas e práticas, apoiadas em recursos audiovisuais e computacionais, bem como estabelecendo um ensino-aprendizagem significativo. Aplicação de trabalhos individuais, apresentações de seminários e lista de exercícios.

RECURSOS DIDÁTICOS

- [X] Quadro
- [X] Projetor
- [X] Vídeos/DVDs
- [X] Periódicos/Livros/Revistas/Links
- [] Equipamento de Som
- [X] Laboratório: Laboratório de Programação
- [X] Softwares: Wireshark, Packet Tracer, firewall (e.g., IPTables), software para certificação digital (e.g., OpenSSL), software para segurança de correio eletrônico (e.g., OpenPGP), softwares para exploração de vulnerabilidades (e.g., nmap), servidor de páginas Web com habilitação para SSL/TLS (e.g., Apache), software para acesso remoto seguro (e.g., servidor e cliente SSH).
- [X] Outros: Sala na Plataforma Moodle da Instituição.

CRITÉRIOS DE AVALIAÇÃO

- Avaliações escritas;
- Relatórios de algumas atividades práticas;
- Trabalhos individuais e em grupo (listas de exercícios, pesquisas, seminários);
- O processo de avaliação é contínuo e cumulativo;
- O aluno que não atingir 70% do desempenho esperado fará Avaliação Final.
- O resultado final será composto do desempenho geral do aluno.

BIBLIOGRAFIA

Básica

- STALLINGS, W.; BROWN, L. **Segurança de Computadores: Princípios e Práticas**. 2. ed. Rio de Janeiro: Elsevier, 2015. ISBN 9788535264500.
- FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores**. 4. ed. São Paulo: McGraw-Hill, 2008. ISBN 9788586804885.
- RUFINO, N. M. O. **Segurança em Redes Sem Fio**: aprenda a proteger suas informações em ambientes wi-fi e bluetooth. 2. ed. São Paulo: Novatec, 2007. ISBN 9788575221327.

Complementar

- STALLINGS, W. **Criptografia e Segurança de Redes**. 5. ed. São Paulo: Pearson Prentice Hall, 2008.
- SHOKRANIAN, S. **Criptografia para Iniciantes**. 2. ed. Rio de Janeiro: Ciência Moderna, 2012. ISBN 9788539902750.
- CHESWICK, . **Firewalls e Segurança na Internet**. 2. ed. Porto Alegre: Bookman, 2005. ISBN 9788536304298.
- TANENBAUM, A. S. **Redes de Computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011. ISBN 9788576059240.
- MORIMOTO, C. E. **Redes, Guia Prático**. 1. ed. São Paulo: Sul Editores, 2009.