

## PLANO DE ENSINO E APRENDIZAGEM

**CURSO:** Tecnologia em Redes de Computadores

<b>Disciplina:</b> Segurança de Redes	<b>Período Letivo:</b> 1º sem/2015	<b>Série:</b> 5ª Série	<b>Período:</b> <i>Não definido</i>
<b>Semestre de Ingresso:</b> 1º		<b>Ano de Ingresso:</b> 2013	
<b>C.H. Teórica:</b> 20	<b>C.H. Outras:</b> 20	<b>C.H. Total:</b> 40	

### Ementa

Conceitos de Segurança. Segurança de Dados, Informações e Sistemas. Segurança de Armazenamento. Elementos de Segurança de Redes. Tecnologias de Segurança de Redes. Fundamentos de Perímetro de Rede. Principais tipos de ataques. Vulnerabilidades dos protocolos TCP/IP. Arquitetura de software de defesa de rede. Principais mecanismos de Defesa. Criptografia. Algoritmos: DES, 3DES, RSA, PGP. Firewalls. Segurança de Roteadores. Sistemas de Detecção de Intrusão. Redes Privadas Virtuais (VPN). Política de Segurança. Projeto do Perímetro da rede. Avaliação do Projeto de Segurança da rede.

### Objetivos

Estudar e entender os principais conceitos e técnicas de segurança utilizados para proteger as informações que são armazenadas e transportadas em uma rede de computadores.

### Conteúdo Programático

Conceitos de Segurança.  
Segurança de Dados, Informações e Sistemas.  
Segurança de Armazenamento.  
Elementos de Segurança de Redes.  
Tecnologias de Segurança de Redes.  
Fundamentos de Perímetro de Rede.  
Principais tipos de ataques.  
Engenharia Social;  
Trojans;  
Sniffers;  
DoS (Denial of Service);  
DDoS (Distributed DoS);  
Spoofing;  
Spywares;  
Phishing;  
Vulnerabilidades dos protocolos TCP/IP.  
Arquitetura de software de defesa de rede.  
Principais mecanismos de Defesa.  
Esteganografia;  
Firewalls;  
Wrappers;  
Sistemas de Detecção de Intrusão;  
Certificados Digitais;  
Analisadores de Logs;  
Verificadores de Senhas;  
Ferramentas de auditoria (SATAN - Security Administrator Tool for Analyzing Networks);  
Honeypots e Honeynets;  
Sistemas Biométricos;  
Criptografia.

Introdução a Criptografia;
Cifras por substituição;
Cifras por transposição;
Algoritmos de Chave Simétrica ou de Chave Secreta;
Algoritmos de Chave Assimétrica ou de Chave Pública;
Segurança de Roteadores.
Redes Privadas Virtuais (VPN).
Características de uma VPN;
Tunelamento;
Protocolos de Tunelamento;
Funcionamento dos Túneis;
IPSec em VPNs;
Vantagens da utilização de VPNs;
Políticas de Segurança.
O que são políticas de segurança;
Como estabelecer as políticas de Segurança;
Projeto do Perímetro da rede.
Avaliação do Projeto de Segurança da rede.

Procedimentos Metodológicos Indicados
Aulas expositivas. Exercícios práticos. Estudos em grupo. Aulas laboratoriais.

Sistema de Avaliação	
1º Avaliação - PESO 4,0	2º Avaliação - PESO 6,0
Atividades Avaliativas a Critério do Professor	Prova Escrita Oficial
Práticas:	Práticas:
Teóricas:	Teóricas:
Total: 0	Total: 0

Bibliografia Básica Padrão
1) MORAES, ALEXANDRE DE. <b>SEGURANÇA EM REDES</b> : FUNDAMENTOS. 1ª ed. São Paulo: Érica, 2010.

Bibliografia Básica Unidade: Centro Universitário Anhanguera de Campo Grande (FCG)
1) THOMAS, Tom. <b>Segurança de Redes</b> : Primeiros Passos. 1ª ed. São Paulo: Ciência Moderna, 2007.
2) FOROUZAN, Behrouz A.. <b>Comunicação de dados e redes de computadores</b> . 1ª ed. São Paulo: McGraw-Hill, 2010.
3) NAKAMURA, Emilio T. (org.); GEUS, Paulo L.. <b>Segurança de redes em ambientes</b> . 1ª ed. São Paulo: Novatec, 2011.

Bibliografia Complementar: Centro Universitário Anhanguera de Campo Grande (FCG)
1) TERADA, Routo. <b>Segurança de dados : criptografia em redes de computador</b> . 2ª ed. São Paulo: Edgard Blücher, 2008.
2) STALLINGS, William. <b>Criptografia e segurança de redes : princípios e práticas</b> . 4ª ed. São Paulo: Pearson, 2010.
3) MONTEIRO, Emiliano S.. <b>Segurança no ambiente corporativo</b> . 1ª ed. Florianópolis: Visual Books, 2003.

Periódico: Centro Universitário Anhanguera de Campo Grande (FCG)
1) IEEE NETWORK MAGAZINE. New York: IEEE, 1987-2009 - Quinzenal
2) REVISTA JAVA MAGAZINE. Rio de Janeiro: DevMedia, 2004 - Mensal

Cronograma de Aulas	
Semana nº.	Tema
1	Apresentação da disciplina. Objetivos. Ementa. Bibliografia. Conceitos de Segurança.
2	Conceitos de segurança.
3	Principais tipos de ataques.
4	Principais tipos de ataques.

5	Principais tipos de ataques.
6	Vulnerabilidades dos protocolos TCP/IP.
7	Arquitetura de software de defesa de rede.
8	Principais mecanismos de defesa.
9	Exercícios e Revisão. Atividades de Avaliação.
10	Principais mecanismos de defesa.
11	Principais mecanismos de defesa.
12	Criptografia. Algoritmos de chave pública e privada.
13	Criptografia. Algoritmos de chave pública e privada.
14	Segurança de Roteadores.
15	Redes Privadas Virtuais (VPN). Política de Segurança.
16	Projeto do perímetro da rede.
17	Avaliação do projeto de segurança da rede.
18	Prova Escrita Oficial.
19	Revisão.
20	Prova Substitutiva.

<div>Coordenador do Curso</div> <div>_____</div> <div>Assinatura</div>	<div>Diretor Executivo    __/__/__</div> <div>_____</div> <div>Assinatura</div>
--	---