

**DIRETORIA DE ENSINO**  
**COORDENAÇÃO DO CURSO: TÉCNICO INTEGRADO EM TELECOMUNICAÇÕES**  
**PROGRAMA DE UNIDADE DIDÁTICA – PUD**

<b>DISCIPLINA: SEGURANCA DE REDES-</b>	
<b>Código:</b>	01.105.87
<b>Carga Horária Total: 40 HORAS</b>	<b>CH Teórica: 40      CH Prática:</b>
<b>CH - Prática como Componente Curricular do ensino:</b>	
<b>Número de Créditos:</b>	2
<b>Pré-requisitos:</b>	Não tem.
<b>Semestre:</b>	6
<b>Nível:</b>	Ensino Médio
<b>EMENTA</b>	
<p>Conceitos fundamentais de segurança cibernética.            Criptografia e certificados digitais.            Aspectos de segurança da arquitetura TCP/IP.            Ameaças e vulnerabilidades.            Conceitos básicos de política de segurança.</p>	
<b>OBJETIVO</b>	
<p>Conhecer os conceitos básicos de segurança cibernética.            Conhecer e aplicar as técnicas elementares de proteção utilizadas na internet.</p>	
<b>PROGRAMA</b>	
<p><b>Unidade I : Conceitos (4h)</b></p> <ul style="list-style-type: none"> <li>• Tríade da segurança</li> <li>• Padrões de segurança</li> <li>• Legislação</li> </ul> <p><b>Unidade II: Criptografia (6h)</b></p> <ul style="list-style-type: none"> <li>• Tipos de criptografia</li> <li>• Algoritmos e chaves</li> <li>• Funções de <i>Hash</i></li> <li>• Assinatura digital</li> <li>• Prática: Uso de criptografia em emails e arquivos. Criação de containers seguros.</li> </ul> <p><b>Unidade III: Certificados (6h)</b></p> <ul style="list-style-type: none"> <li>• Certificação digital</li> <li>• <i>Public Key Infrastructure</i> (PKI)</li> <li>• Prática: Utilizando o openSSL para criação de chaves, certificados e PKI.</li> </ul> <p><b>Unidade IV: Aplicações de Criptografia (6h).</b></p> <ul style="list-style-type: none"> <li>• SSL/TLS</li> <li>• Redes Virtuais Privadas (VPN)</li> <li>• SSH</li> <li>• Prática: Criando uma VPN.</li> </ul> <p><b>Unidade V: – Segurança em TCP/IP (10h)</b></p> <ul style="list-style-type: none"> <li>• <i>Sniffers</i></li> </ul>	

- *Denial of Service* (DoS)
- Spoofing
- SYN flood
- Ataque *fraggle*
- Ataque DRDOS
- Ataque DDOS
- Ping da morte
- *Teardrop*
- Prática: Uso do Wireshark para visualização dos ataques descritos.
- Prática: Implementando *Firewall* com IPtables

#### **Unidade VI – Política de Segurança (8h)**

- Conceitos
- Análise de risco
- Vulnerabilidades e ameaças
- Impacto
- Construindo uma política de segurança

ISO 27000

### **METODOLOGIA DE ENSINO**

As ações pedagógicas estão centradas no desenvolvimento de habilidades cognitivas. Essas habilidades incluem, entre outras, o raciocínio, a investigação e capacidade de síntese.

A metodologia de ensino conta com aulas teóricas onde os conceitos são apresentados e aulas práticas durante as quais os conceitos são implementados utilizando-se tecnologias proprietárias e abertas. As avaliações incluem atividades escritas, trabalhos e roteiros de atividade a serem executados em laboratório.

### **RECURSOS**

Material didático-pedagógico:

Livro didático;

Apostila elaborada pelo professor-regente;

Fotocópias;

Jornais virtuais ou impressos atuais.

Recursos audiovisuais:

Quadro branco e pincel adequado;

Datashow;

Projetor de mídia ou equivalente;

### **AVALIAÇÃO**

Aulas teóricas abordando os principais fundamentos de segurança cibernética, as ameaças e vulnerabilidades existentes. Aulas práticas para evidenciar os conceitos apresentados e aplicar possíveis ações mitigatórias. A avaliação da disciplina ocorrerá segundo o Regulamento da Organização Didática – ROD do IFCE, Art. 91, que determina que no IFCE a avaliação deve ter caráter diagnóstico, formativo, processual e contínuo, com a predominância dos aspectos qualitativos sobre os quantitativos e dos resultados parciais sobre os obtidos em provas finais, em conformidade com o artigo 24, inciso V, alínea a, da LDB N°. 9.394/96.

### **BIBLIOGRAFIA BÁSICA**

STALLINGS, William. **Criptografia e Segurança de Redes: princípios e práticas**. Editora: Pearson, 2008 Edição: 4ª. 512 páginas.

KUROSE, James F. **Redes de computadores e a internet: uma abordagem top-down**. Editora: Pearson, 2013 Edição: 6ª. 660 páginas

CHAHIN, Ali. Cunha, Maria Alexandra. Knight, Peter. Pinto, S. Lemos. **e-gov.br: a próxima revolução brasileira: eficiência, qualidade e democracia: o governo eletrônico no Brasil e no mundo**. Editora: Pearson, 2013 Edição: 1ª. 400 páginas

## BIBLIOGRAFIA COMPLEMENTAR

MACHADO, F.B., MAIA, L. P., **Introdução a Arquitetura de Sistemas Operacionais**, LTC - Livros Técnicos e Científicos Ed. Ltda, 5ª ed. 2013.

COMER, Douglas E. **Interligação em Rede com TCP/IP**: Volume I. Rio de Janeiro: Campus, 2006. COMER, Douglas E. **Redes de Computadores e Internet**. BOOKMAN, 2000.

SOARES, Luiz Fernando G, SOUZA, Guido Lemos de e COLCHER, Sérgio, **Redes de computadores: Das LAN'S, MAN's e WANs às redes ATM**. Editora campus, 2ª edição, Setembro 1995.

ARAÚJO, Márcio Tadeu de; FERREIRA, Fernando Nicolau Freitas. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação**. Rio de Janeiro: Ciência Moderna, 2008. MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**. Trad. São Paulo: Pearson Education do Brasil, 2003.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Invadir**. Trad. São Paulo: Pearson Education do Brasil, 2006.

Coordenador do Curso

Setor Pedagógico

