Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-reitoria de Ensino

DISCIPLINA: Segurança de Redes de Computadores	
Vigência: 2025/2	**Período letivo:** 6º semestre
Carga horária total: 60 h	**Código:** SUP.1132
Carga horária de extensão: 0 h	**Carga horária de pesquisa: 0 h**
Ementa: Compreensão de tópicos sobre segurança de redes, vulnerabilidades em redes, protocolos de criptografia, fundamentos de uma política de segurança. Estudo sobre algoritmos de criptografia. Compreensão sobre firewall em servidor de rede, serviço proxy-cache, redes virtuais privadas, analisadores de redes, software de varredura de portas, auditoria de segurança da informação, sistemas de detecção e prevenção de intrusos.	

Conteúdos:

UNIDADE I – Conceitos de Segurança de Redes
1.1 Princípios básicos de segurança de redes
1.2 Políticas de segurança
1.3 Vulnerabilidades em redes
1.4 Mecanismos de segurança

UNIDADE II – Criptografia
2.1 Princípio da criptografia
2.2 Algoritmos de criptografia
2.3 Protocolos de criptografia
2.4 Certificado Digital
2.5 Assinatura Digital

UNIDADE III – Analisadores de Redes
3.1 Conceitos sobre analisadores de redes
3.2 Teste com analisadores de redes

UNIDADE IV – Software de Varredura de Portas
4.1 Conceitos sobre varredura de portas
4.2 Técnicas de varredura
4.3 Teste com software de varredura de portas

UNIDADE V – Redes Virtuais Privadas
5.1 Os fundamentos da VPN
5.2 Protocolos de tunelamento

UNIDADE VI – Firewall em Servidor de Rede
6.1 Definição e função
6.2 Funcionalidade

6.3 Tipos de firewall
6.4 Testes de firewall

UNIDADE VII – Serviço Proxy-cache
7.1 Definição e função
7.2 Funcionalidade
7.3 Testes de Proxy-cache

UNIDADE VIII – Auditoria de Segurança da Informação
8.1 Definição e função
8.2 Funcionalidade
8.3 Ferramentas de auditoria

UNIDADE IX – Sistemas de Detecção e Prevenção de Intrusos
9.1 Objetivos
9.2 Características dos IDS e IPS

Bibliografia básica:

GOODRICH, Michael T.; LISBÔA, Maria Lúcia Blanck (Tradutora). **Introdução à segurança de computadores**. Porto Alegre, RS: Bookman, 2013.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. 2. ed. Rio de Janeiro, RJ: Elsevier, 2014

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 4ª ed. São Paulo, SP: Pearson, 2008.

Bibliografia complementar:

MORIMOTO, Carlos Eduardo. **Servidores linux: guia prático.** Porto Alegre: Sulina, 2010.

NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2010.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 4. ed. São Paulo, SP: Pearson, 2008.

WRIGHTSON, Tyler. **Segurança de redes sem fio: guia do iniciante.** Porto Alegre, RS: Bookman, 2014.

YAN, Song Y. **Cryptanalytic attacks on RSA**. New York: Springer, 2008.