PLANO DE DISCIPLINA		
IDENTIFICAÇÃO		
CURSO: **Superior de Tecnologia em Sistemas para Internet**		
DISCIPLINA: **Segurança de Dados**	CÓDIGO DA DISCIPLINA: **47**	
PRÉ-REQUISITO: **Protocolos de Interconexão de Redes**		
UNIDADE CURRICULAR: Obrigatória [X] Optativa [ ] Eletiva [ ]		
CARGA HORÁRIA		
TEÓRICA: **42 h/r**	PRÁTICA: **13 h/r**	EaD[1]: **0 h/r**
CARGA HORÁRIA SEMANAL: **3 h/r**	CARGA HORÁRIA TOTAL: **50 h/r**	

EMENTA

Conceitos básicos sobre segurança da informação. Vulnerabilidades, ameaças e ataques. Autenticação, criptografia simétrica e assimétrica, funções de hash, assinatura digital, certificado digital. Aspectos de segurança para aplicações em redes TCP/IP, firewalls, Protocolo IPSEC, protocolo TLS. Políticas de segurança. Aspectos sociais da segurança de dados.

OBJETIVOS

Conhecer conceitos básicos relacionados à segurança de dados e segurança redes de computadores; Identificar vulnerabilidades presentes nas redes de computadores; Identificar formas de ameaças às redes de computadores; Conhecer protocolos para transferência segura de dados; Conhecer técnicas e algoritmos de criptografia;

CONTEÚDO PROGRAMÁTICO

1	Conceitos Básicos Sobre Segurança Da Informação	3
2	Tipos De Vulnerabilidades, Ameaças E Ataques	3
3	Fundamentos Sobre Criptografia E Assinatura Digital	
3.1	Funções de Hash	2
3.2	Introdução à Criptografia	2
3.3	Algoritmos De Chave Simétrica	6
3.4	Diffie-Helmman Key Exchange	3
3.5	Algoritmos De Chave Pública	5
3.6	Assinatura Digital	3
3.7	Infraestrutura de Chaves Públicas (PKI)	3
3.8	Certificados Digitais X.509	3
4	Segurança Da Comunicação	
4.1	Protocolo TLS	3
4.2	Protocolo IPSEC	3
4.3	Redes Privadas Virtuais (VPN)	1
5	Componentes De Segurança De Redes	

1 **Para a oferta de disciplinas na modalidade à distância, integral ou parcial, desde que não ultrapasse 20% (vinte por cento) da carga horária total do curso, observar o cumprimento da Portaria MEC nº 1.134, de 10 de outubro de 2016.**

Thiago José Marques Moura
Coord. do CST em Sistemas para Internet
Mat. 1550140

5.1	Firewalls	2
5.2	IDS – Sistemas De Detecção De Intrusão (Intrusion Detection Systems)	1
6	Laboratórios Práticos	
6.1	Quebra de senhas	2
6.2	Captura de pacotes (sniffing)	2
6.3	Criação de chave pública/Privada	2
6.4	Criação de uma Autoridade Certificadora	2
6.5	Firewall com Linux/NFTables	2
7	Seminários com temas emergentes	3

METODOLOGIA DE ENSINO

Aulas teóricas e práticas.

RECURSOS DIDÁTICOS

[X] Quadro
[X] Projetor
[ ] Vídeos/DVDs
[X] Periódicos/Livros/Revistas/Links
[ ] Equipamento de Som
[X] Laboratório
[X] Softwares: Linux com ferramentas open source
[ ] Outros:_____

CRITÉRIOS DE AVALIAÇÃO

Provas e seminários

BIBLIOGRAFIA

Bibliografia Básica:

Steve Suehring, Linux Firewalls: Enhancing Security with nftables and Beyond (4th Edition), Addison-Wesley Professional; 4 edition (February 8, 2015)

Andrew S. Tanenbaum, David J. Wetherall, Computer Networks (5th Edition), Pearson; (October 7, 2010)

Toxen, B. Real World Linux Security. 2nd ed., Prentice Hall PTR, 2002.

Bibliografia complementar:

T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. IETF. 2008. Disponível em https://www.ietf.org/rfc/rfc5246.txt

Garfinkel, S. and Spafford, G. Practical UNIX & Internet Security. Sebastopol, CA., O'Reilly & Associates, 1991.

“SSL/TLS in Windows Server 2003” white paper at http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=a9c6b790-050c-4ac8-b065-b166e8f7db0b.

Agathoklis Prodromou, TLS/SSL explained – a brief history of TLS/SSL, part 1, posted on january 17, 2017. Disponível em http://www.acunetix.com/blog/articles/what-is-tls-ssl-part-1/

Thiago José Marques Moura
Coord. do CST em Sistemas para Internet
Mat. 1550140

Agathoklis Prodromou, TLS/SSL explained – a brief history of TLS/SSL, part 2, posted on january 24, 2017. Disponível em https://www.acunetix.com/blog/articles/history-of-tls-ssl-part-2/

Tutorias sobre segurança em redes de computadores. Disponíveis em http://www.cert.org

OBSERVAÇÕES

Thiago José Marques Moura
Coord. do CST em Sistemas para Internet
Mat. 1550140