



Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Pato Branco



Informações da disciplina

Código Ofertado	Disciplina/Unidade Curricular	Modo de Avaliação	Modalidade da disciplina	Oferta
SC28CP	Segurança Computacional	Nota/Conceito E Frequência	Presencial	Semestral

Carga Horária					
AT	AP	APS	ANP	APCC	Total
3	1	4	0	0	60
<ul style="list-style-type: none"> • AT: Atividades Teóricas (aulas semanais). • AP: Atividades Práticas (aulas semanais). • ANP: Atividades não presenciais (horas no período). • APS: Atividades Práticas Supervisionadas (aulas no período). • APCC: Atividades Práticas como Componente Curricular (aulas no período, esta carga horária está incluída em AP e AT). • Total: carga horária total da disciplina em horas. 					

Objetivo		
Compreender os mecanismos de ameaças aos sistemas computacionais. Identificar e aplicar mecanismos de prevenção contra falhas e possíveis ataques. Compreender conceitos e mecanismo de segurança como: criptografia, autenticação, assinatura digital e firewall. Gerenciar a segurança em sistemas computacionais.		
Ementa		
Segurança lógica, física e ambiental; políticas de segurança; vulnerabilidade; mecanismos de segurança: autenticação, assinatura digital, firewall, criptografia; ameaças e contramedidas em um sistema computacional; aplicação de solução de segurança em estudo de caso.		
Conteúdo Programático		
Ordem	Ementa	Conteúdo
1	Segurança lógica, física e ambiental	Mecanismos de proteção baseados em software para proteção de dados, programas e sistemas, contra tentativas de acessos não autorizados. Proteção das vias de acesso ao ambiente e equipamentos, contra usuários não autorizados. Prevenção de danos por causas naturais.

Ordem	Ementa	Conteúdo
2	Políticas de segurança	Definição, planejamento e pontos importantes a serem tratados sobre política de segurança. Política para senhas, firewall e acesso remoto. Política de segurança em ambientes cooperativos.
3	Vulnerabilidade	Definição de Vulnerabilidade. Análise de vulnerabilidades em sistemas.
4	Mecanismos de segurança: criptografia, autenticação, assinatura digital, firewall;	O Papel da Criptografia, Criptografia de Chave Simétrica, Criptografia de Chave Pública e gerenciamento de Chaves. Autenticação de mensagens, funções de autenticação. Assinatura Digital e protocolos de autenticação: autenticação mútua e autenticação unidirecional. Princípios de projeto de Firewall, arquiteturas de Firewall.
5	Ameaças e contramedidas em um sistema computacional	Definição de ameaças e contramedidas. Utilização de contramedidas para diminuição de riscos e ameaças.
6	Aplicação de solução de segurança em estudo de caso.	Avaliar e aplicar ferramentas e mecanismos de segurança em sistemas de informações.

Bibliografia Básica
STALLINGS, William. Criptografia e segurança de redes : princípios e práticas . 4. ed. São Paulo, SP: Pearson Prentice Hall, 2008. xvii, 492 p. ISBN 9788576051190.
NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de redes : em ambientes cooperativos. São Paulo, SP: Novatec, 2007. 482 p. ISBN 9788575221365.
COULOURIS, George F.; DOLLIMORE, Jean; KINDBERG, Tim (Autor). Sistemas distribuídos : conceitos e projeto. 4. ed. Porto Alegre, RS: Bookman, c2007. viii, 784p. ISBN 978-85-60031-49-8.

Bibliografia Complementar
LUCCHESI, Claudio Leonardo. Introdução a criptografia computacional . Campinas: Papirus: UNICAMP, 1986. xiii, 132 p. (Informática).
TRIGO, Clodionil Honório. Projeto de segurança em software livre . Rio de Janeiro, RJ: Alta Books, 2004. 193p. : ISBN 857608026-5
BISHOP, Matt. Computer security : art and science. Boston: Addison-Wesley, 2003. xli, 1084 p. ISBN 9780201440997.
GOLLMANN, Dieter. Computer Security . 3. ed. United Kingdom, UK: John Wiley & Sons, 2011. xix, 436 p. ISBN 9780470741153.
SCHNEIER, Bruce. Segurança.com : segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro, RJ: Campus, 2001. 403 p. ISBN 8535207554.

#	Resumo da Alteração	Edição	Data	Aprovação	Data
1	ok.	Dalcimar Casanova	15/04/2016	Pablo Gauterio Cavalcanti	25/04/2016

