FACULDADE DE TECNOLOGIA DE TAQUARITINGA

ANO	PLANO DE ENSINO
2013	2º SEMESTRE DE 2013

CÓDIGO	DEPARTAMENTO
14	ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

CÓDIGO	DISCIPLINA
1435	SEGURANÇA DA INFORMAÇÃO

CÓDIGO	PROFESSOR RESPONSÁVEL
	MAURÍCIO MARCOS

CARGA HORÁRIA			DISTRIBUIÇÃO DAS AULAS		
SEMANAS	X AULAS/SM =	TOTAL =	TEÓRICAS +	PRÁTICAS +	AVALIAÇÃO
20	2	40	24	10	6

E M E N T A
Requisitos de segurança de aplicações, de base de dados e de comunicações. Segurança de dispositivos móveis. Políticas de segurança. Criptografia. Firewalls. Vulnerabilidades e principais tecnologias de segurança.

O B J E T I V O S
Compreender e aplicar as melhores práticas de Segurança da Informação de acordo com normas e padrões conhecidos no mercado de TI.

ANO	PLANO DE ENSINO	CÓDIGO
2013	2º SEMESTRE DE 2013	1435

PROGRAMA

Unidade	Objetivos	Conteúdo
Introdução à Segurança da Informação	Apresenta de maneira geral a segurança da informação como processo amplo e duradouro.	✓Confiabilidade, Integralidade e Disponibilidade; ✓Definição de tipos de ameaça; ✓Tipos de controle de segurança; ✓Normas e Padrões (COBIT, ISO27001 e ISO27002); ✓Estrutura Organizacional em Seg. da Informação; ✓Perfil do Profissional de Seg. Informação (Security Officer); ✓Comitê de Segurança; ✓Plano de Segurança (CID); ✓Pesquisa, treinamento e educação em segurança.
Desenvolvimento de Análise de Riscos	Ensinar como fazer uma análise de riscos sengundo definido pelo Gerenciamento de risco NIST 800-30.	✓Definição; ✓Etapa 1: Inventário; ✓Etapa 2: Análise; ✓Etapa 3: Avaliação; ✓Etapa 4: Treinamento; ✓Gerenciamento de Risco.
Gestão de Continuidade de Negócios	Apresentação de metodologias de planejamejamento e gestão da continuidade de negócios baseado na norma BS-25999 e NBR 15999-1.	✓Plano de continuidade de negócios; ✓Necessidade da operação de negócios; ✓Melhores práticas para continuidade de negócios; ✓Procedimentos de contingência; ✓Plano de recuperação de desastres.
Segurança de redes	Ensinar como proteger uma rede de ataques comuns, apresentando os principais ataques a redes cabeadas e sem fio. Apresentar as principais ferramentas de segurança contra estes ataques.	✓Topologias de redes e segurança em protocolos; ✓Ataques: Levantamento de perfil. Sniffing de rede, PortScan, Brute Force, ARP-Poison, Spoofing; ✓Proteção contra ataques contra redes e websites; ✓Firewalls e DMZ; ✓Vulmerabilidade em Wirelless; ✓Demosntração de WEP Cracking; ✓Acees Point: Filtros de IP, Filtros de MAC, WEP e WPA.
Malware	Apresentação de conceitos sobre os diferentes tipos de Malware, como eles entram em uma rede e rapidamente se espalham.	✓Principais tipos de Malware; ✓Vias de Infecção em redes de computadores; ✓Espalhamento na rede; ✓Frameword Metasplicit (construção de vírus); ✓Infeção em redes corporativas

ANO	PLANO DE ENSINO	CÓDIGO
2013	2º SEMESTRE DE 2013	1435

PROGRAMA

Unidade	Objetivos	Conteúdo
Croptografias e Assinaturas Digitais	Delineamento da historia da criptografia, sua utilização no mundo moderno com a utilização dos certificados digitas.	✓Algoitimos e Chaves; ✓Aplicações da Criptrografia; ✓Criptrografia simétrica e assimetrica; ✓Desenvolvimento de algoritmo simples de criptrografia; ✓Gerenciamento de Chaves; ✓Ataques à criptrografia: Força Bruta, Ataques Hash; ✓Assinaturas Digitais; ✓Infraestrutura de chaves públicas (PKI – ICP Brasil); ✓Futuro da Criptografia.
Controle de Acesso Lógico	Apresentar conceitos e práticas para definir controles de acesso visando o estabelecimento da segurança no acesso à redes corporativas. Apresentação de desipositivos para fatores de autenticação (tokens, biometria, entre outros).	✓Controle de acesso: conceitos, metodologias e técnicas; ✓Ameaças aos controles de acesso: identificação, avaliação, resposta e prevenção; ✓Acesso aos dados; ✓Mecadnismos de autenticação: Tokens, Smartcards e Biometria.
Controle de Acesso Físico	São abordados conceitos e metodologias de controle de acesso físico e segurança ambiental, visando a preservação de informações e recursos humanos.	✓Introdução Teórica; ✓Tipos de ameaças à segurança física; ✓Projeto de segurança física.

METODOLOGIA

O desenvolvimento do conteúdo dar-se-á por meio de aulas expositivas (giz/lousa + datashow), discussão dos aspectos teóricos, enfatizando a interdisciplinaridade do assunto no contexto da utilização prática do desenvolvimento e implantação de Segurança da Informação, foco principal da disciplina.
Também serão desenvolvidas atividades práticas em laboratório, incentivo a pesquisa e sistematização de assuntos avançados, complementares ao conteúdo da disciplina.

ANO	PLANO DE ENSINO	CÓDIGO
2013	1º SEMESTRE DE 2013	1435

CRITÉRIOS DE AVALIAÇÃO

Média final: $\frac{\left(\frac{\text{prova 1 + trabalho 1}}{2}\right) + \left(\frac{\text{prova 2 + trabalho 2}}{2}\right)}{2}$ + participação

Sendo que:

- **Prova 1:** avaliação teórica, individual e sem consulta sobre o conteúdo ministrado durante as aulas expositivas e práticas;
- **Trabalho 1:** Atividade em grupo: Desenvolvimento um plano de segurança da informação e/ou Seminário de Normas Técnicas.
- **Prova 2:** avaliação teórica, individual e sem consulta sobre o conteúdo ministrado durante as aulas expositivas e práticas;
- **Trabalho 2:** Atividade em grupo: Desenvolvimento um algoritimo de criptografia e/ou Mecanismo de Controle Ae acesso com segurança Física e Lógica.
- **Ponto por participação**: será somado 1 (um) ponto à media final aos alunos que não possuírem faltas (zero faltas). Alunos com faltas terão frações adicionadas proporcionalmente ao número de faltas.

Outras observações:

Será considerado aprovado na disciplina o aluno que obtiver média final >= 6,0 e com frequência superior a 75% das aulas lançadas em caderneta. As datas poderão ser alteradas, com prévio aviso ao corpo discente presente em sala de aula. As dispensas e abonos de faltas seguirão exclusivamente e Legislação em vigor. As faltas lançadas em caderneta são incontestáveis, excetuando-se o previsto legalmente.

E - 9,0 <=MF<=10,0
A - 8,0 <=MF<9,0
B - 6,0 <=MF<8,0
C - MF<6,0Insuficiente
F - Reprovação por faltas

ANO	PLANO DE ENSINO	CÓDIGO
2013	2º SEMESTRE DE 2013	1435

BIBLIOGRAFIA BÁSICA

FERREIRA, F N; ARAUJO, M. Política de Segurança da Informação. Ciência Moderna, 2008.

FONTES, E. Praticando a segurança da informação. Brasport, 2008.

STALLINGS, W. Criptografia e Segurança de Redes. 4 ed. São Paulo: Pearson, 2008.

BIBLIOGRAFIA COMPLEMENTAR

NBR/ISSO/IEC 17799. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas ABNT, 2002.

PEIXOTO, M C P. Engenharia Social e Segurança da Informação. Brasport, 2006.

ALVES, Gustavo Alberto. Segurança da Informação: Uma Visão Inovadora da Gestão. : Ciência Moderna, 2006. 115p.

CARNEIRO, Alberto. Auditoria de Sistemas de Informação. Coleção Sistemas de Informação. Rio de Janeiro: FCA - Editora Informática, 2004.

CARNEIRO, Alberto. Auditoria e Controle de Sistemas de Informação. Rio de Janeiro: FCA - Editora Informática, 2009.

SILVA, Pedro Tavares. TORRES, Catarina Botelho. CARVALHO, Hugo. Segurança dos Sistemas de Informação. Edições Centro Atlântico, 2003.

LEANDRO, Marcos Roberto de Lima. Segurança da Informação Métodos e Ferramentas de Segurança. 2005. 55p. • VIEIRA, Gleci Fernanda. Segurança da Informação na Web. 2004. 52p. • DAWEL, George. A Segurança da Informação nas Empresas: Ampliando Horizontes Além da Tecnologia. RIO DE JANEIRO: Ciência Moderna, 2005. 117p.

LYRA, Maurício Rocha. Segurança e Auditoria de Sistema de Informação. 1 ed. Rio de Janeiro: Ciencia Moderna, 2009. • IMONIANA, Joshua Onome. Auditoria de Sistemas de Informação. São Paulo: Atlas, 2005.