UNIVERSIDADE FEDERAL DO ABC – UFABC

CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

PLANO DE ENSINO

ANO LETIVO	QUADRIMESTRE	TURNO	CAMPUS
2020	Q1	Noturno	Santo André

CÓDIGO	NOME	TPI
MCTA023-17	Segurança de Dados	3-1-4
TURMAS	**RECOMENDAÇÕES**	
NA1MCTA023-17SA NA2MCTA023-17SA NA3MCTA023-17SA	Redes de Computadores, Algoritmos e Estruturas de Dados I	

EMENTA

Introdução à segurança de computadores. Algoritmos e ferramentas de criptografia: algoritmos simétricos e de chave pública. Autenticação de usuários e controle de acesso. Negação de serviço (DoS). Firewalls, sistemas de prevenção de intrusão e detecção de intrusão. Computação confiável. Segurança em software: estouro de buffer e outros problemas. Problemas de gerência da segurança: infraestrutura, aspectos humanos, auditoria e avaliação de riscos. Segurança na Internet. Segurança em sistemas operacionais.

OBJETIVOS

Compreender aspectos relacionados com a segurança de dados em um sistema computacional.

PLANEJAMENTO PRELIMINAR DE AULAS

Semana 1: Introdução à segurança de computadores. Introdução a criptografia: técnicas primitivas e cifras clássicas.

Semana 2: Criptografia moderna e confidencialidade: cifras de fluxo, cifras de bloco e modos de operação. Prática 1: Algoritmos de criptografia simétrica clássica (cifra de Vigenère).

Semana 3: Criptografia moderna e integridade: hash, autenticação de mensagem MAC. Acordo de chave secreta, Diffie-Hellman. Criptografia de chave pública, Encriptação RSA e ElGamal.

Semana 4: Criptografia assimétrica e autenticidade: assinatura digital, assinaturas RSA e DSA. Prática 2: Algoritmos de criptografia simétrica clássica (cifras DES, AES, modos de operação).

Semana 5: Autenticação de usuários. Controle de acesso. Certificados digitais de chave pública e autenticação. Framework SSL.

Semana 6: Prática 3: TLS e certificados digitais. Prova 1.

Semana 7: Segurança do software. Programação segura. Firewalls. Sistemas de detecção de intrusão.

Semana 8: Prática 4: Programação segura. Apresentações de trabalhos: Gestão de segurança da informação; Normas internacionais de segurança da informação; Gestão de fatores humanos em segurança da informação.

Semana 9: Apresentações de trabalhos: Software malicioso, Negação de serviço; padrão SHA-3 em Hash criptográfico; Blockchain, segurança e aplicações; Segurança em sistemas operacionais.

Semana 10: Prática 5: Monitoração de pacotes e configuração de firewall. Apresentações de trabalhos: Segurança em bancos de dados; Padrões em desenvolvimento seguro de software; Segurança em aplicações Web.

Semana 11: Prova 2.

Semana 12: Prova Substitutiva e vista de provas.

Semana 13: Reposições de feriado: Mecanismo de Recuperação.

Semana 14: Reposição de feriado: Vista de prova de Recuperação e fechamento de conceito.

AVALIAÇÕES

Avaliações do Período Letivo Regular:

Composição: 2 provas e atividades durante o quadrimestre

30% prova 1: semana 6 (19/03/2020)
30% prova 2: semana 11 (23/04/2020)

25% trabalhos de pesquisa
15% atividades de laboratório e exercícios

Avaliação Substitutiva:

Estarão habilitados para a avaliação substitutiva os alunos que se ausentarem a uma das avaliações do período regular e contemplados pelo benefício de acordo com a Resolução CONSEPE no. 181, de 23 de outubro de 2014.

Data da prova sub: semana 12 (27/04/2020)

Caso o aluno se ausente de mais de uma avaliação do período regular, o conceito da avaliação substitutiva será concedido para UMA ÚNICA avaliação não realizada, privilegiando a de maior peso ponderado.

Avaliação de Recuperação:

Estarão habilitados para a avaliação de recuperação os alunos que obtiverem conceito final **D** ou **F** na conclusão de todas as atividades e avaliações aplicadas no período letivo regular, obedecendo as regras indicadas na Resolução CONSEPE no. 182, de 23 de outubro de 2014.

Data da prova de recuperação: semana 13 (05/05/2020), a ser realizado numa terça-feira, dia 5/5, na sala 302-2 (cf. calendário de reposição do feriado de 24/2)

ATIVIDADES DE APOIO

Esta disciplina prevê um horário de atendimento extraclasse para atividades de apoio aos estudantes regulares desta turma, conforme disposto na Resolução CONSUNI 183, de 31 de outubro de 2017.

Os horários de atendimento semanal terão carga horária total de 2 horas para conteúdos de teoria, lab e projeto, ou 1h para dúvidas específicas das turmas práticas A2 e A3, sendo realizadas nos seguintes dias, locais e horário:

Quintas-feiras, das 19:00h às 21:00h, sala 533-2, com profª Denise
Quartas-feiras, das 18:00h às 19:00h, sala 507-2, com prof. Paulo
Quintas-feiras, das 10:00h as 12:00h, no lab 6 do bloco delta SBC, com prof. Nunzio

ou em horário previamente agendado e confirmado via mensagem no Tidia

BIBLIOGRAFIA RECOMENDADA

Bibliografia Básica

GOODRICH, M. T.; TAMASSIA, R. Introdução à segurança de computadores. Porto Alegre, RS: Bookman, 2013.

FERREIRA, F. N. F. Segurança da informação. Rio de Janeiro, RJ: Editora Ciência Moderna, 2003.

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 4a edição. São Paulo, SP: Prentice Hall, 2008.

Bibliografia Complementar

TANENBAUM, A. S. Sistemas operacionais modernos. 3ª edição. São Paulo, SP: Pearson Prentice Hall, 2009.

COMER, D. Redes de computadores e internet: abrange transmissão de dados, ligação inter-redes, Web e aplicações. 4a edição. Porto Alegre, RS: Bookman, 2007.

KONHEIM, A. G. Computer security and cryptography. Hoboken, N.J: Wiley-Interscience, 2007.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet: uma abordagem top-down. 5ª edição. São Paulo, SP: Pearson, 2010.

SCHNEIER, B. Applied cryptography: protocols, algorithms and source code in C. 2aedição. New York, USA: Wiley, 1996.

STALLINGS, W. Criptografia e segurança de redes. 4ª edição. São Paulo, SP: Pearson Prentice Hall, 2008.

STAMP, M. Information security: principles and practice. 2a edição. Hoboken, NJ: Wiley-Interscience, 2011

PROFESSOR(ES) RESPONSÁVEL(IS)
Profª. Dra. Denise Hideko Goya
Prof. Dr. Paulo Henrique Pisani
Prof. Dr. Nunzio Marco Torrisi