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	Matutino	Santo André

CÓDIGO	NOME	TPI
MCTA023-17	Segurança de Dados	3-1-4
TURMAS	**RECOMENDAÇÕES**	
DA1MCTA023-17SA	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.

Início dos Estudos Continuados Emergenciais - ECE:

Semana 6: Prática 3: TLS e certificados digitais. Projeto (Etapa 2: texto preliminar)

Semana 7: Firewalls. Sistemas de detecção de intrusão. Projeto (feedback do texto preliminar). Entrega da Questão 1 dissertativa.

Semana 8: Projeto (entrega do texto final e início da Etapa 4: elaboração de testes)

Semana 9: Projeto (feedback do texto final e Etapa 4: elaboração de testes).

Semana 10: Projeto (entrega da Etapa4). Início das leituras dos textos revisados.

Semana 11: Leituras dos textos revisados. Início dos testes (de todos os temas).

Semana 12: Realização dos testes. Fechamento de conceitos.

Retorno das aulas presenciais:

Semana 13: Mecanismo de Recuperação (prova presencial).

AVALIAÇÕES

Avaliações do Período Regular e ECE:

As avaliações serão compostas de:

1. Projeto (35%): desenvolvido em equipe, abordando os tópicos: malware; DDoS (negação de serviço distribuída); segurança no software e desenvolvimento seguro; segurança em sistemas operacionais; segurança em banco de dados; gestão da segurança; blockchain e temas específicos em criptografia (como SHA-3 e criptografia pós-quântica);
2. Questão dissertativa (15%): individual;
3. Testes (20%): individual;
4. Atividades de laboratório (30%): individual.

Observações:

- A não participação no projeto ou obter F em duas das quatro avaliações acima implica não-aprovação;

- No ECE, apenas aprovação constará no histórico escolar (se tirar F na disciplina, ela será cancelada).

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 dos Estudos Continuados Emergenciais, obedecendo às regras indicadas na Resolução CONSEPE no. 182, de 23 de outubro de 2014.

Data da prova de recuperação: após o retorno das atividades presenciais, em calendário a ser definido.

ATIVIDADES DE APOIO

Durante os Estudos Continuados Emergenciais, os atendimentos a dúvidas serão realizados por meio de mensagem via Tidia e via fórum na aba da disciplina 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