**UNIVERSIDADE FEDERAL DO ABC – UFABC**

**CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO**

**BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO**

# PLANO DE ENSINO

| ANO LETIVO | QUADRIMESTRE | TURNO | CAMPUS |
|---|---|---|---|
| 2019 | Q1 | Noturno | Santo André |

| CÓDIGO | NOME | TPI |
|---|---|---|
| MCTA023-17 | Segurança de Dados | 3-1-4 |
| **TURMAS** | **RECOMENDAÇÕES** | |
| 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 (cifras DES, AES, modos de operação).

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: Criptografia de chave pública (RSA, assinatura), hash e HMAC.

Semana 5: Autenticação de usuários. Controle de acesso. Prova 1.

Semana 6: Segurança do software. Programação segura. Prática 3: Programação segura.

Semana 7: Certificados digitais de chave pública e autenticação. Framework SSL. Firewalls. Sistemas de detecção de intrusão.

Semana 8: Gestão de segurança da informação e Normas internacionais. Prática 4: Monitoração de pacotes e configuração de firewall.

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

Semana 10: Apresentações de trabalhos de pesquisa: Segurança em sistemas operacionais, Segurança em bancos de dados, Segurança na Internet.

Semana 11: Prova 2 e Prova Substitutiva.

Semana 12: Reposição de feriado e vista de provas.

Semana 13: Reposições de feriados e Mecanismo de Recuperação.

**AVALIAÇÕES**

**Avaliações do Período Letivo Regular**:

Composição: 2 provas e atividades durante o quadrimestre

30% prova 1: semana 5 (15/03/2019)
30% prova 2: semana 11 (24/04/2019)
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 11 (26/04/2019)

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 (13/05/2019), a ser realizado numa segunda-feira, dia 13/5, no laboratório (cf. calendário de reposição do feriado de 19/4)

## 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, sendo realizadas no seguinte dia, local e horário:

Quartas-feiras, das 19:00h às 21:00h, sala 533-2

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 |