



UNIVERSIDADE FEDERAL DO ABC – UFABC  
CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO  
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

**PLANO DE ENSINO**

ANO LETIVO	QUADRIMESTRE	TURNO	CAMPUS
2025	Q1	Noturno	Santo André

CÓDIGO	NOME	TPI
MCTA023-17	Segurança de Dados	3-1-4
TURMAS	RECOMENDAÇÕES	
NA1MCTA023-17SA NA2MCTA023-17SA	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: preparo do ambiente (Seed Labs) e criptnálise de frequência.

Semana 3: Criptografia moderna e integridade: hash, autenticação de mensagem MAC. Acordo de chave secreta, Diffie-Hellman. Criptografia de chave pública, Encrytação RSA e ElGamal. Criptografia assimétrica e autenticidade: assinatura digital, assinaturas RSA e DSA.

Semana 4: Carnaval

Semana 5: Autenticação de usuários. Controle de acesso. Certificados digitais de chave pública. Framework TLS. Programação segura (SQL Injection, XSS).

Semana 6: Programação segura (buffer overflow, string de formatação). Prática: criptografia simétrica.

Semana 7: Apresentações de trabalhos de pesquisa: Gestão de segurança da informação; Normas internacionais.

Semana 8: Apresentações de trabalhos de pesquisa: Negação de serviço; padrão SHA-3 em Hash criptográfico. Prática: criptografia assimétrica.

Semana 9: Apresentações de trabalhos de pesquisa: Algoritmos criptográficos pós-quânticos; Blockchain (segurança e aplicações).

Semana 10: Apresentações de trabalhos de pesquisa: Segurança em sistemas operacionais; Segurança em bancos de dados; Segurança Web. Prática: segurança no software.

Semana 11: Apresentações de trabalhos de pesquisa: Firewall; IDS.

Semana 12: Apresentações de trabalhos de pesquisa: Software malicioso; Privacidade e proteção de dados pessoais. **Prova.**

Semana 13: Reposições de feriados: **Prova Sub.** Vista de provas e dúvidas.

Semana 14: Reposições de feriados: **Mecanismo de Recuperação.** Vista de provas e dúvidas.

## AVALIAÇÕES

### Avaliações do Período Letivo Regular:

Composição: Uma prova (P), trabalho de pesquisa (T) e atividades de laboratório (L) e exercícios durante o quadrimestre, com os pesos a seguir

40% prova (P): semana 12 (30/04/2025)

30% trabalho de pesquisa (T)

30% atividades de laboratório e exercícios (L)

Caso o aproveitamento em P, T ou L seja igual a **0%**, o conceito pré-recuperação será no máximo igual a **D**, independente do aproveitamento nos demais componentes avaliativos.

### **Avaliação Substitutiva:**

Estarão habilitados para a avaliação substitutiva os alunos que se ausentaram de uma das avaliações do período regular (P1 ou P2) e contemplados pelo benefício de acordo com a Resolução CONSEPE no. 181, de 23 de outubro de 2014.

Data da prova sub: **semana 13 (05/05/2025)**

### **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 às regras indicadas na Resolução CONSEPE no. 182, de 23 de outubro de 2014.

Data da prova de recuperação: **semana 14 (12/05/2025)**

O conceito final da disciplina será uma combinação do conceito pré-recuperação e da prova da recuperação, com igual peso.

## **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 15:00h às 17:00h, sala 533-2**

ou em horário previamente agendado e confirmado via mensagem no Moodle

## **BIBLIOGRAFIA RECOMENDADA**

### **Bibliografia Básica**

KATZ, J.; LINDELL, Y. Introduction to modern cryptography. CRC Press, 2014.

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 4a edição.

São Paulo, SP: Prentice Hall, 2008.

Stallings, W., Brown, L. Computer Security: Principles and Practice, ed. Prentice Hall, ISBN-13: 9780136004240

### **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. 2ª edição. New York, USA: Wiley, 1996.  
STAMP, M. Information security: principles and practice. 2ª edição. Hoboken, NJ: Wiley-Interscience, 2011

**PROFESSOR(ES) RESPONSÁVEL(IS)**

Profa. Dra. Denise Hideko Goya