



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	
NA2MCTA023-17SA	Redes de Computadores e 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

Estudar os aspectos relacionados com a segurança de dados em um sistema computacional, permitindo ao aluno o desenvolvimento de novos conhecimentos, habilidades e competências na área de Ciência da Computação.

PLANEJAMENTO PRELIMINAR DE AULAS

Semana 1: Plano de Ensino; Conceitos e Fundamentos; Criptografia Simétrica.

Semana 2: Criptografia Simétrica e Autenticação de Mensagens.

Semana 3: Criptografia Assimétrica, Assinatura Digital, e Gerenciamento de Chaves.

Semana 4: Autenticação de Usuário e Controle de Acesso.

Semana 5: Autenticação de Usuário e Controle de Acesso; 1ª avaliação (prova escrita)

Semana 6: Computação Confiável e Segurança em Software

Semana 7: Segurança Operacional

Semana 8: Gerência da Segurança.

Semana 9: 2ª avaliação (prova escrita); 3ª avaliação: Apresentação de trabalhos de pesquisa.

Semana 10: 3ª avaliação: Apresentação de trabalho de pesquisa.

Semana 11: 3ª avaliação: Apresentação de trabalho de pesquisa; prova substitutiva.

Semana 12: Revista de avaliação.

Semana 13: Reposição de feriado (em 09/05/2019; prova de recuperação).

Semana 14: Reposições dos feriados (em 13/05/2019 e 14/05/2019).

AVALIAÇÕES E PROCEDIMENTOS

1) A disciplina possui no total 03 (três) avaliações parciais obrigatórias. As avaliações possuem o mesmo peso e são pontuadas no intervalo de [0,0; 10,0], considerando:

- 1ª. Avaliação (A1): prova escrita prevista para semana 5 (15/03/2019);
- 2ª. Avaliação (A2): prova escrita prevista para semana 9 (10/04/2019);
- 3ª. Avaliação (A3): trabalho de pesquisa em grupo (70%) e atividades individuais de laboratório (30%). As apresentações dos trabalhos de pesquisa em grupo são previstas para ocorrer nas semanas 9, 10 e 11 (12/04, 17/04 e 24/04/2019).

Obs: uma pontuação menor ou igual a 4,0 na **A3** implica nota final conceitual (NFC) igual a F, independentemente das pontuações obtidas nas demais avaliações.

2) A nota final numérica (NFN) é calculada pela fórmula a seguir:

$$\text{NFN} = \left(\frac{A_1 + A_2 + A_3}{3,0} \right)$$

No caso da realização da Prova de Recuperação (PR), a NFN é calculada pela fórmula a seguir:

$$\text{NFN} = 0,65 \times \left(\frac{A_1 + A_2 + A_3}{3,0} \right) + 0,35 \times \text{PR}$$

3) A nota final conceitual (NFC) tem a seguinte equivalência em relação a NFN:

- NFC = **A**: se $9,0 \leq \text{NFN} \leq 10,0$
- NFC = **B**: se $7,5 \leq \text{NFN} < 9,0$
- NFC = **C**: se $6,5 \leq \text{NFN} < 7,5$
- NFC = **D**: se $5,0 \leq \text{NFN} < 6,5$
- NFC = **F**: se $0,0 \leq \text{NFN} < 5,0$

4) Prova Substitutiva:

Estarão habilitados para a prova substitutiva, a qual engloba todo o conteúdo do quadrimestre, os alunos que se ausentarem a uma das provas escritas do período regular e estejam contemplados pelo benefício de acordo com a Resolução ConsEPE nº. 227, de 23 de abril de 2018.

Caso o aluno se ausente de mais de uma prova escrita do período regular, o conceito da avaliação substitutiva será concedido para uma única das provas escritas faltantes, privilegiando, quando for o caso, a de maior peso ponderado.

Alunos que fizeram todas as provas escritas do período regular não terão direito à avaliação substitutiva.

Data da prova substitutiva: prevista para semana 11 (26/04/2019).

5) Avaliação de Recuperação:

Estarão habilitados para a prova de recuperação (PR), a qual engloba todo o conteúdo do quadrimestre, os alunos que obtiverem conceito final **D** ou **F** na nota final conceitual (NFC), obedecendo as regras indicadas na Resolução ConsEPE nº 182, de 23 de outubro de 2014.

Data da prova de recuperação: prevista para semana 13 (09/05/19).

6) Procedimentos no decorrer das aulas

Excetuando-se a situação em que haja autorização expressa do professor para o contrário, o aluno deverá manter seu aparelho de telefone celular desligado, durante as aulas, exceto nos casos em que esteja aguardando alguma ligação de extrema importância, deixando nesse caso o aparelho no modo de vibração (vibra call), quando então deverá retirar-se da sala para atender a eventual ligação. Todos os demais aparelhos eletrônicos (computadores, laptops, ipads, smartphones, etc) deverão permanecer desligados durante toda a aula, excetuando-se também a situação em que haja autorização expressa do professor para o contrário.

O aluno deverá respeitar professores, demais funcionários da UFABC e os outros alunos. Em caso de desrespeito e/ou atos de indisciplina serão impostas as sanções disciplinares cabíveis. Tampouco é permitido ao aluno utilizar-se de palavrões bem como fumar e/ou ingerir bebidas alcoólicas e/ou alimentar-se dentro da sala de aula.

7) Casos omissos deverão ser levados ao professor da disciplina desta turma.

ATIVIDADES DE APOIO

Esta disciplina prevê horário de atendimento extraclasse para atividades de apoio aos estudantes regulares desta turma, conforme disposto na Resolução CONSUNI nº 183, de 31 de outubro de 2017. Os horários de atendimento semanal terão carga horária total de 2 horas, sendo realizadas nos seguintes dias, locais e horários:

- Quartas-feiras, das 20:00h às 21:00h, sala 546-2, Bloco A.
- Sextas-feiras, das 18:00 h às 19:00 h, sala 546-2, Bloco A.

BIBLIOGRAFIA RECOMENDADA

Bibliografia Básica

- GOODRICH, Michael T.; TAMASSIA, Roberto. Introdução à segurança de computadores. Porto Alegre: Bookman, 2013. 550 p. ISBN 978-85-407-0192-2.
- FERREIRA, Fernando Nicolau Freitas. Segurança da informação. Rio de Janeiro: Editora Ciência Moderna, 2003. 162 p. ISBN 8573932902.

- STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. Prentice Hall, 2008. ISBN 9788576051190.

Bibliografia Complementar

- TANENBAUM, Andrew S. Sistema operacionais modernos. 3 ed. São Paulo: Pearson Prentice Hall, 2009. 653 p. ISBN 978857605371.
- COMER, Douglas. Redes de computadores e internet: abrange transmissão de dados, ligação interredes, Web e aplicações. 4 ed. Porto Alegre: Bookman, 2007. x, 632p p. Bibliografia: p. 617-623. ISBN 9788560031368.
- KONHEIM, Alan G. Computer security and cryptography. Hoboken, N.J: Wiley-Interscience, c2007. xvii, 521 p. Includes bibliographical references and index. ISBN 9780471947837.
- KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet: uma abordagem top-down. 5.ed. São Paulo: Pearson, 2010. 640 p. ISBN 9788588639973.
- SCHNEIER, Bruce. Applied cryptography: protocols, algorithms, and source code in C. 2 ed. New York: Wiley, c1996. xxiii, 758 p. Includes bibliographical references (p. 675-741). ISBN 9780471117094.
- STALLINGS, William. Criptografia e segurança de redes. 4 ed. São Paulo: Pearson Prentice Hall, 2008. 492 p. ISBN 9788576051190.
- STAMP, Mark. Information security: principles and practice. Hoboken, N.J: Wiley-Interscience, 2 ed, 2011. 606 p. ISBN 978-0470626399.
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet, 2 ed. Comitê Gestor da Internet no Brasil, 2012. 140 p. ISBN 978-85-60062-54-6. Disponível em <http://cartilha.cert.br/livro/>.

PROFESSOR(ES) RESPONSÁVEL(IS)

Prof. Dr. Carlo Kleber da Silva Rodrigues e Prof. Dr. Nunzio Marco Torrisi