Pró-Reitoria de Graduação

Plano de Ensino – 1º Quadrimestre de 2023

Caracterização da disciplina									
Código da disciplina:	MCTA023-17	Nome da disciplina:	Segurança de Dados						
Créditos (T-P-I):	(3-1-4)	Carga horária total:	48 horas	Aula prática:	12 horas	Câmpus:	Santo André		
Código das turmas:	NA1MCTA023-17SA e NA2MCTA023-17SA	Turmas:	A1 e A2	Turno:	Noturno	Quadrimestre:	1	Ano:	2023
Docente(s) responsável(is):	Rodrigo Augusto Cardoso da Silva (teoria das turmas A1 e A2) Rodrigo Augusto Cardoso da Silva (prática da turma A1) Rodrigo Izidoro Tinini (prática da turma A2)								

Alocação da turma (QU1 - quinzenal 1; QU2 - quinzenal 2; SEM - semanal)						
	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
19:00 - 20:00				S-214-0(SEM)		
20:00 - 21:00				S-214-0 (SEM)		
21:00 - 22:00	S-214-0 (QU1) 404-2 (QU2 A1) 407-2 (QU2 A2)					
22:00 - 23:00	S-214-0 (QU1) 404-2 (QU1 A1) 407-2 (QU2 A2)					

Planejamento da disciplina

Objetivos

Estudar os aspectos relacionados com a segurança de dados em sistemas computacionais. Entender os principais conceitos de criptografia, segurança em redes, segurança de computadores, segurança de sistemas operacionais, e gerência de segurança de dados.

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.

Conteúdo programático		
Aula	**Conteúdo**	**Estratégias didáticas**
06/02	Introdução à disciplina	Aula expositiva
09/02	Malware	Aula expositiva
13/02	Aula prática	Atividade prática em laboratório
16/02	Criptografia simétrica - substituição e transposição	Aula expositiva
20/02	Não haverá aula (feriado)	—
23/02	Criptografia simétrica - cifras de bloco	Aula expositiva
27/02	Aula prática	Atividade prática em laboratório
02/03	Criptografia assimétrica	Aula expositiva
06/03	Funções de hash	Aula expositiva
09/03	Assinaturas digitais	Aula expositiva
13/03	Aula prática	Atividade prática em laboratório
16/03	Prova 1	Avaliação
20/03	Autenticação	Aula expositiva
23/03	Segurança de redes (camada de transporte)	Aula expositiva
27/03	Aula prática	Atividade prática em laboratório
30/03	Segurança de redes (IP)	Aula expositiva
03/04	Segurança de redes (firewalls, IDSs, negação de serviço)	Aula expositiva
06/04	Segurança em sistemas operacionais	Aula expositiva
10/04	Aula prática	Atividade prática em laboratório
13/04	Gerência de segurança	Aula expositiva
17/04	Gerência de segurança	Aula expositiva
20/04	Prova 2	Avaliação
24/04	Revisão de prova	Atendimento individual
27/04	Prova substitutiva	Avaliação
01/05	Não haverá aula (feriado)	—
03/05	Prova de recuperação	Avaliação

Observações:

- O planejamento poderá sofrer mudanças caso seja necessário durante o quadrimestre;
- As datas das provas só serão alteradas se for extremamente necessário.

Descrição dos instrumentos e critérios de avaliação qualitativa

A comunicação entre o professor e os alunos será feita durante as aulas, através da plataforma Moodle, e também pelo e-mail institucional.

A avaliação desta disciplina será feita através de duas provas e trabalhos práticos. As provas terão um conjunto de questões a serem resolvidas no tempo dado. Os trabalhos serão atividades de natureza prática e exigirão o uso de computador e software específico. O professor divulgará a forma de entrega dos trabalhos e datas de entrega juntamente com seus enunciados. As aulas práticas serão usadas para fazer os trabalhos e tirar dúvidas.

A nota será calculada da seguinte forma. Sejam P_1, P_2, T as notas da primeira prova, segunda prova, e média aritmética simples das notas dos trabalhos, respectivamente. P_1, P_2 , e T serão notas numéricas no intervalo entre 0 e 10. A média numérica final M será calculada da seguinte forma:

$M = P_1 \cdot 0,35 + P_2 \cdot 0,35 + T \cdot 0,3$

Caso o aluno não faça algum trabalho ou prova, a nota correspondente será zero. Trabalhos entregues fora do prazo não serão avaliados. Os alunos que não concordarem com a nota de alguma das avaliações deverão fazer o pedido de reconsideração por escrito no dia de divulgação da nota.

Todo aluno que tiver cumprido os requisitos de presença terá direito a fazer uma prova substitutiva. Para isso, o aluno deve avisar o professor, com 24 horas de antecedência por e-mail, que irá fazê-la. Caso decida fazê-la, a nota P_S da prova substitutiva substituirá a menor nota entre P_1 e P_2.

A nota final N será calculada como $N = M$ e mapeada para o conceito final da seguinte forma:

- Se o aluno não obtiver a presença mínima nas aulas, ele se reprovará com conceito O independentemente de sua nota N;
- Se $N < 5,0$, o aluno se reprovará com conceito F;
- Se $5,0 \leq N < 6,0$, o aluno se aprovará com conceito D;
- Se $6,0 \leq N < 7,0$, o aluno se aprovará com conceito C;
- Se $7,0 \leq N < 8,5$, o aluno se aprovará com conceito B;
- Se $8,5 \leq N \leq 10,0$, o aluno se aprovará com conceito A.

Caso o aluno tenha conceito final D ou F, ele terá direito a uma recuperação. A recuperação poderá ser composta de provas e/ou trabalhos extras. Caso o aluno faça recuperação, ele será avaliado com uma nota R da recuperação e sua nota final N será calculada como $N = (M + R)/2$. Neste caso, o conceito final será dado de acordo com o novo valor de N, usando o mapeamento de conceitos já apresentado.

Caso uma fraude seja identificada, todos alunos envolvidos se reprovaram com conceito F. Além disso, outras punições cabíveis dentro das regras vigentes da universidade e também dentro da legislação poderão ser aplicadas. Fraudes são quaisquer atos ilícitos para obter vantagens no curso, em especial aquelas envolvendo plágio.

Atendimento extra-classe

O professor oferecerá até uma hora de atendimento extra-classe por semana no campus de Santo André ou virtualmente. O horário deverá ser combinado entre o aluno e o professor por e-mail com antecedência mínima de 24 horas úteis.

Referências bibliográficas

[1] STALLINGS, W. Cryptography and Network Security: Principles and Practice. 8th edition. Pearson, 2022.
[2] GOODRICH, M. T.; TAMASSIA, R., Introduction to Computer Security: Pearson New International Edition. Pearson Education Limited, 2014
[3] GOODRICH, M. T.; TAMASSIA, R. Introdução à segurança de computadores. Porto Alegre, RS: Bookman, 2013.
[4] STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 6. ed. Pearson, 2015.
[5] WHITMAN, M. E.; MATTORD, Herbert J. Principles of Information Security. Sixth Edition. Boston, USA. Cengage Learning, 2018.