Pró-Reitoria de Graduação

Plano de Ensino – 1º Quadrimestre de 2024

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:	2024
Docente responsável:	Rodrigo Augusto Cardoso da Silva								

Alocação da turma						
	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
19:00 - 20:00	A-108-0 (A1 e A2)		407-2 (A1)			
20:00 - 21:00	A-108-0 (A1 e A2)		407-2 (A1)			
21:00 - 22:00			407-2 (A2)			
22:00 - 23:00			407-2 (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**
05/02	Introdução à disciplina
07/02	Criptografia simétrica - introdução e técnicas
12 e 14/02	Não haverá aulas
19/02	Criptografia simétrica - cifras de bloco
21/02	Criptografia simétrica - operação de cifras de bloco
26/02	Criptografia assimétrica
28/02	Funções de hash
04/03	Assinaturas digitais
06/03	Segurança em redes - camada de transporte
11/03	Prova teórica 1
13/03	Aula prática
18/03	Segurança em redes - camada de rede
20/03	Aula prática
25/03	Segurança em redes - segurança de dispositivos
27/03	Aula prática
01/04	Malware
03/04	Aula prática
08/04	Não haverá aula
10/04	Prova prática
15/04	Segurança em sistemas operacionais
17/04	Segurança em sistemas operacionais
22/04	Gerência de segurança
24/04	Prova teórica 2
30/04	Prova substitutiva
03/05	Recuperação
Observação: o planejamento poderá sofrer mudanças caso seja necessário durante o quadrimestre.	

Descrição dos instrumentos e critérios de avaliação qualitativa

A comunicação entre o professor e os alunos será feita predominantemente durante as aulas. O Moodle será usado usado para disponibilizar material das aulas e divulgação de notas.

A avaliação desta disciplina será feita através de três provas, sendo duas teóricas e uma prática. As provas teóricas cobrarão assuntos apresentados nas aulas de teoria. Exercícios de listas de exercícios, assim como exercícios inéditos poderão fazer parte das provas. No caso da provas prática, a prova cobrará assuntos relacionados às atividades práticas. A menos que indicado o contrário, todas as provas serão feitas de forma individual e sem consulta.

A nota será calculada da seguinte forma. Sejam PT_1, PT_2, e PP as notas da primeira prova teórica, segunda prova teórica, e prova prática, respectivamente. PT_1, PT_2, e PP serão notas numéricas no intervalo entre 0 e 10. A média numérica final M será calculada da seguinte forma: $N = PT_1 \cdot 0,35 + PT_2 \cdot 0,35 + PP \cdot 0,3$. Se $PT_1 \geq 6,0$, $PT_2 \geq 6,0$, e $PP \geq 6,0$, então $M = N$. Caso contrário, M será o valor mínimo entre N , PT_1, PT_2, e PP.

Caso o aluno não faça alguma prova, a nota correspondente será zero. Os alunos que discordarem da avaliação poderão fazer um pedido de reconsideração por escrito no dia de divulgação da nota.

O aluno que perder uma avaliação poderá solicitar uma prova substitutiva caso tenha presença mínima e apresente um documento válido para justificar a ausência segundo a Resolução ConsEPE N° 227 de 23 de abril de 2018.

A nota M será 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 M;
- Se $M < 5,0$, o aluno se reprovará com conceito F;
- Se $5,0 \leq M < 6,0$, o aluno se aprovará com conceito D;
- Se $6,0 \leq M < 7,0$, o aluno se aprovará com conceito C;
- Se $7,0 \leq M < 8,5$, o aluno se aprovará com conceito B;
- Se $8,5 \leq M$, o aluno se aprovará com conceito A.

Caso o aluno tenha conceito final D ou F, ele terá direito a uma recuperação. A recuperação funcionará da seguinte forma: o aluno fará duas provas, uma teórica e outra prática. Seja PRT a nota da prova de recuperação teórica e PRP a nota da prova de recuperação prática. O novo conceito será calculado da seguinte forma:

- $RT_1 = máximo(PRT, PT_1)$
- $RT_2 = máximo(PRT, PT_2)$
- $RP = máximo(PRT, PP)$
- $NR = RT_1 \cdot 0,35 + RT_2 \cdot 0,35 + PP \cdot 0,3$
- Se $RT_1 \geq 6,0$, $RT_2 \geq 6,0$ e $RP \geq 6,0$, então $M = NR$. Caso contrário, M será o valor mínimo entre NR, RT_1, RT_2, e RP.
- O novo valor de M será mapeado para o conceito final da mesma forma apresentada anteriormente.

Caso uma fraude seja identificada, todos alunos envolvidos se reprovarão 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 horário e local de atendimento extra-classe serão informados no Moodle. O atendimento só ocorrerá caso seja solicitado por pelo menos um aluno com 24 horas de antecedência.

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.