DISCIPLINA:	SEGURANÇA DA INFORMAÇÃO	
Código:	SI	
Carga Horária Total: 40h	CH Teórica: 30h	CH Prática: 10h
Número de aulas: 40	**Número de Créditos:** 2	
Pré-requisitos:	-	
Ano:	3º	
Nível:	Médio	

EMENTA

Introdução à segurança da informação; criptografia; Medidas de proteção e prevenção de ataques e segurança na web..

OBJETIVO

Propiciar aos discentes conhecimentos essenciais sobre segurança da informação visando capacitá-los a projetar softwares seguros utilizando os conceitos abordados.

PROGRAMA

Unidade I - Introdução à segurança da informação

- Conceito de Segurança da Informação
- Principais vulnerabilidades
- Softwares maliciosos
- Tipos de ataques

Unidade II - Criptografia

- Noções de criptografia
- Criptografia simétrica e assimétrica
- Hash/digest
- Assinatura e certificados digitais

Unidade III - Medidas de proteção e prevenção de ataques

- Back-up e recuperação de dados
- Barreiras e medidas de segurança
- Prevenção de ataques
- Noções de proteção de dados

Unidade IV - Segurança na Web

- Cookies, rastreadores e permissões de aplicativos
- Noções básicas da LGPD
- Tor, HTTPS e VPN

METODOLOGIA DE ENSINO

Aulas teóricas:

- Ministradas em sala, ou outro ambiente que facilite o processo de ensino-aprendizagem, por meio expositivo-dialógico e com discussões com resolução de exercícios, onde a ênfase está em demonstrações conceituais e fundamentos essenciais;
- Como recursos de apoio, tem-se a utilização do quadro branco, projetor de slides e livro(s) de referência(s)

Aulas práticas:
- Ministradas em laboratório de informática, ou outro ambiente que facilite a consolidação dos conceitos fundamentais.
- Como recursos de apoio, tem-se a utilização de ferramentas para pentest, de plataformas online de ensino aprendizagem.

AVALIAÇÃO

O processo avaliativo deve ser contínuo e constante durante todo o processo de ensino-aprendizagem, com o propósito de analisar o progresso do aluno, criando indicadores capazes de apontar meios para ajudá-lo na construção do conhecimento.
Desta forma, para início do processo ensino-aprendizagem, sugere-se avaliações diagnósticas, como forma de se construir um panorama sobre as necessidades dos alunos e, a partir disso, estabelecer estratégias pedagógicas adequadas e trabalhar para desenvolvê-los, inclusive evidenciando os casos que necessitarão de métodos diferenciados em razão de suas especificidades, tais como a necessidade de inclusão. Essas avaliações deverão seguir, preferencialmente, métodos qualitativos, todavia, também seguirão métodos quantitativos quando cabíveis dentro dos contextos individuais e coletivos da turma.
Durante toda a continuidade do processo ensino-aprendizagem, sugere-se a promoção, em alta frequência, de avaliações formativas capazes de proporcionar ao docente um feedback imediato de como estão as interferências pedagógicas em sala de aula, e permitindo ao aluno uma reflexão sobre ele mesmo, exigindo autoconhecimento e controle sobre a sua responsabilidade, frente aos conteúdos já vistos em aula, privilegiando a preocupação com a satisfação pessoal do aluno e juntando informações importantes para mudanças na metodologia e intervenções decisivas na construção de conhecimento dos discentes, inclusive com subsídios para propostas de atividades de recuperação paralela na(s) reunião(ões) de colegiado de curso, coordenadoria de curso e demais setores ligados ao ensino.
Ao final de cada etapa do período letivo, pode-se realizar avaliações somativas, com o objetivo de identificar o rendimento alcançado tendo como referência os objetivos previstos para a disciplina. Há nesses momentos a oportunidade de utilizar recursos quantitativos, tais como exames objetivos ou subjetivos, inclusive com recursos de TIC, todavia, recomenda-se a busca por métodos qualitativos, baseados no planejamento de projetos práticos, práticas interdisciplinares ou atuação em experimentos de laboratório, dentre outros.

BIBLIOGRAFIA BÁSICA

STALLINGS, William. **Criptografia e segurança de redes**: princípios e prática. Tradução de Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 558 p. ISBN 9788543005898. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/22446. Acesso em: 19 jul. 2020.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. ISBN 9788574528670. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044. Acesso em: 19 jul. 2020.

MORAES, Alexandre Fernandes de. **Segurança em redes:** fundamentos. São Paulo: Érica, 2010. ISBN 9788536503257.

BIBLIOGRAFIA COMPLEMENTAR

TERADA, Routo. **Segurança de dados:** criptografia em rede de computador. 2. ed. São Paulo: Blucher, 2008. ISBN 9788521204398. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/173353. Acesso em: 19 jul. 2020.

CABRAL, Carlos; CAPRINO, WILLIAN. **Trilhas em segurança da informação:** caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. ISBN 9788574527178. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160689. Acesso em: 19 jul. 2020.

MANOEL, Sergio da Silva. **Governança de segurança da informação.** Rio de Janeiro: Brasport, 2014. ISBN 9788574526768. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160684. Acesso em: 19 jul. 2020.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva, 12 ed. Rio de Janeiro: Elsevier, 2003. ISBN 9788535211917.

THE HONEYNET PROJECT, **Conheça seu inimigo:** o projeto Honeynet - revelando as ferramentas de segurança, táticas e motivos da comunidade hacker. São Paulo: Pearson Education do Brasil, 2002. ISBN 9788534614191. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/255. Acesso em: 19 jul. 2020.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores**: princípios e práticas. Rio de Janeiro: Elsevier, 2014. ISBN 9780132775069.

Coordenador do Curso	Setor Pedagógico
_____	_____