MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

PROGRAMA DE ENSINO

1. Identificação

Disciplina:	INE5448 - Tópicos Especiais em Aplicações Tecnológicas I
Nível:	Graduação
Carga Horária:	72 horas-aula (Teórica: 36; Prática: 36)
Vigência:	De 2025-1 até a presente data

2. Ementa

Ementa livre para assuntos relevantes na área de Aplicações Tecnológicas.

3. Cursos Relacionados

- CIÊNCIAS DA COMPUTAÇÃO (208) - Currículo: 2007-1 (Optativa)
- ENGENHARIA DE CONTROLE E AUTOMAÇÃO (220) - Currículos: 1991-1 (Optativa); 2024-1 (Optativa)

4. Objetivos

4.1 Objetivo Geral:

Desenvolver nos alunos a capacidade de compreender os princípios, desafios e oportunidades na intersecção entre Inteligência Artificial e Segurança da Informação, capacitando-os a identificar, analisar e propor soluções para os problemas emergentes nessa área.

4.2 Objetivos Específicos:

a) Compreender os fundamentos da Inteligência Artificial, seus algoritmos e aplicações;
b) Dominar os conceitos básicos de segurança da informação, incluindo criptografia, autenticação, autorização e gestão de riscos;
c) Identificar as principais ameaças e vulnerabilidades associadas à IA;
d) Conhecer as técnicas de ataque e defesa em sistemas baseados em IA;
e) Entender as implicações éticas e legais da IA na segurança.
f) Analisar a segurança de sistemas e aplicações que utilizam IA;
g) Desenvolver modelos de machine learning para detecção de intrusões e anomalias
h) Implementar técnicas de defesa contra ataques adversariais;
i) Avaliar os riscos associados a diferentes aplicações de IA;
j) Propor soluções para mitigar as ameaças à segurança em sistemas de IA.

k) Desenvolver um pensamento crítico sobre os desafios e oportunidades da IA na segurança;

l) Promover a ética e a responsabilidade na utilização da IA;

m) Estar atualizado sobre as últimas tendências e pesquisas na área.

---

5. Conteúdo Programático

1 Introdução [8 horas-aula]
- 1.1 Conceitos básicos de IA, aprendizado de máquina e deep learning.
- 1.2 Aplicações da IA em diversos setores.

2 Segurança da Informação [4 horas-aula]
- 2.1 Conceitos de segurança da informação, ameaças comuns (malware, phishing), vulnerabilidades e princípios de segurança.

3 Intersecção IA e Segurança [4 horas-aula]
- 3.1 Sinergia entre IA e segurança (detecção de intrusão, análise de malware). --Desafios da IA para a segurança (ataques adversariais, privacidade).

4 Aprendizado de Máquina e Segurança [4 horas-aula]
- 4.1 Aprendizado supervisionado, não supervisionado e por reforço aplicado à segurança.

5 Ataques Adversariais e Defesas [4 horas-aula]
- 5.1 Tipos de ataques, técnicas de defesa, casos de estudo.

6 Privacidade e Ética na IA [4 horas-aula]
- 6.1 Privacidade de dados, viés algorítmico, transparência, responsabilidade algorítmica.

7 Governança e Regulamentação [4 horas-aula]
- 7.1 Regulamentações nacionais e internacionais sobre IA.
- 7.2 Questões éticas e sociais relacionadas à IA.

8 Estudos de caso [40 horas-aula]
- 8.1 Análise de casos reais de ataques a sistemas de IA.
- 8.2 Discussão de possíveis soluções e lições aprendidas.

---

6. Bibliografia Básica

[1] Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1999.569p.

[2] RUSSELL, Stuart J.; NORVIG, Peter. Artificial intelligence: a modern approach. Pearson, 2016.

[3] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[4] STAMP, Mark; VISAGGIO, Corrado Aaron; MERCALDO, Francesco; DI TROIA, Fabio (Eds.). Artificial Intelligence for Cybersecurity: Emerging Trends and Research Applications. Cham: Springer, 2022.

---

7. Bibliografia Complementar

[1] ZHANG, Zhimin et al. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, p. 1-25, 2022.

[2] ANITHA, Cuddapah et al. Artificial Intelligence driven security model for Internet of Medical Things (IoMT). In: 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM). IEEE, 2023. p. 1-7.

[3] HOROWITZ, Michael C. et al. Artificial intelligence and international security. Center for a New American Security., 2022.

[4] OSOBA, Osonde A.; WELSER, William. The risks of artificial intelligence to security and the future of work. Santa Monica, CA: RAND, 2017.

[5] KHILAR, Rashmita et al. Artificial Intelligence?Based Security Protocols to Resist Attacks in Internet of Things. Wireless Communications and Mobile Computing, v. 2022, n. 1, p. 1440538, 2022.

[6] AL-KHASSAWNEH, Yazan Alaya. A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges. Indonesian Journal of Science and Technology, v. 8, n. 1, p. 79-96, 2023.

[7] RADULOV, Nikolay. Artificial intelligence and security. Security 4.0. Security & Future, v. 3, n. 1, p. 3-5, 2019.

[8] KAUR, Ramanpreet; GABRIJEL?I?, Du?an; KLOBU?AR, Toma?. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, v. 97, p. 101804, 2023.

[9] TRUONG, Thanh Cong et al. Artificial intelligence and cybersecurity: Past, presence, and future. In: Artificial intelligence and evolutionary computations in engineering systems. Springer Singapore, 2020. p. 351-363.

[10] MOHAMMED, Ishaq Azhar. Artificial intelligence for cybersecurity: A systematic mapping of literature. Artif. Intell, v. 7, n. 9, p. 1-5, 2020.

[11] Artigos recentes de revistas como IEEE Security & Privacy, Journal of Artificial Intelligence Research, e Nature.

[12] Materiais online

[13] Cursos online de plataformas como Coursera, edX e Udemy.

[14] Blogs e sites especializados em IA e segurança.