

Programa de Ensino

1) Identificação

Disciplina: INE5448 - Tópicos Especiais em Aplicações Tecnológicas I
Carga horária: 72 horas-aula Teóricas: 36 Práticas: 36
Período: 1º semestre de 2025 até a presente data

2) Cursos

- Ciências da Computação (208)
- Engenharia, áreas Elétrica e Mecânica, habilitação Controle e Automação (220)

3) Requisitos

- Ciências da Computação (208)
 - INE5417 - Engenharia de Software I
 - INE5608 - Análise e Projeto de Sistemas

4) Ementa

Ementa livre para assuntos relevantes na área de Aplicações Tecnológicas.

5) Objetivos

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.

Específicos:

- Compreender os fundamentos da Inteligência Artificial, seus algoritmos e aplicações;
- Dominar os conceitos básicos de segurança da informação, incluindo criptografia, autenticação, autorização e gestão de riscos;
- Identificar as principais ameaças e vulnerabilidades associadas à IA;
- Conhecer as técnicas de ataque e defesa em sistemas baseados em IA;
- Entender as implicações éticas e legais da IA na segurança.
- Analisar a segurança de sistemas e aplicações que utilizam IA;
- Desenvolver modelos de machine learning para detecção de intrusões e anomalias
- Implementar técnicas de defesa contra ataques adversariais;
- Avaliar os riscos associados a diferentes aplicações de IA;
- Propor soluções para mitigar as ameaças à segurança em sistemas de IA.
- Desenvolver um pensamento crítico sobre os desafios e oportunidades da IA na segurança;
- Promover a ética e a responsabilidade na utilização da IA;
- Estar atualizado sobre as últimas tendências e pesquisas na área.

6) Conteúdo Programático

6.1) Introdução [8 horas-aula]

- Conceitos básicos de IA, aprendizado de máquina e deep learning.
- Aplicações da IA em diversos setores.

- 6.2) Segurança da Informação [4 horas-aula]
 - Conceitos de segurança da informação, ameaças comuns (malware, phishing), vulnerabilidades e princípios de segurança.
- 6.3) Intersecção IA e Segurança [4 horas-aula]
 - Sinergia entre IA e segurança (detecção de intrusão, análise de malware). --Desafios da IA para a segurança (ataques adversariais, privacidade).
- 6.4) Aprendizado de Máquina e Segurança [4 horas-aula]
 - Aprendizado supervisionado, não supervisionado e por reforço aplicado à segurança.
- 6.5) Ataques Adversariais e Defesas [4 horas-aula]
 - Tipos de ataques, técnicas de defesa, casos de estudo.
- 6.6) Privacidade e Ética na IA [4 horas-aula]
 - Privacidade de dados, viés algorítmico, transparência, responsabilidade algorítmica.
- 6.7) Governança e Regulamentação [4 horas-aula]
 - Regulamentações nacionais e internacionais sobre IA.
 - Questões éticas e sociais relacionadas à IA.
- 6.8) Estudos de caso [40 horas-aula]
 - Análise de casos reais de ataques a sistemas de IA.
 - Discussão de possíveis soluções e lições aprendidas.

7) Bibliografia Básica

- Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1999.569p.
- RUSSELL, Stuart J.; NORVIG, Peter. Artificial intelligence: a modern approach. Pearson, 2016.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
- STAMP, Mark; VISAGGIO, Corrado Aaron; MERCALDO, Francesco; DI TROIA, Fabio (Eds.). Artificial Intelligence for Cybersecurity: Emerging Trends and Research Applications. Cham: Springer, 2022.

8) Bibliografia Complementar

- ZHANG, Zhimin et al. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, p. 1-25, 2022.
- 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.
- HOROWITZ, Michael C. et al. Artificial intelligence and international security. Center for a New American Security., 2022.
- OSOBA, Osonde A.; WELSER, William. The risks of artificial intelligence to security and the future of work. Santa Monica, CA: RAND, 2017.
- 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.
- 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.
- RADULOV, Nikolay. Artificial intelligence and security. Security 4.0. Security & Future, v. 3, n. 1, p. 3-5, 2019.
- KAUR, Ramanpreet; GABRIJELČlČ, Dušan; KLOBUČAR, Tomaž. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, v. 97, p. 101804, 2023.
- 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.

- MOHAMMED, Ishaq Azhar. Artificial intelligence for cybersecurity: A systematic mapping of literature. Artif. Intell, v. 7, n. 9, p. 1-5, 2020.
- Artigos recentes de revistas como IEEE Security & Privacy, Journal of Artificial Intelligence Research, e Nature.
- Materiais online
- Cursos online de plataformas como Coursera, edX e Udemy.
- Blogs e sites especializados em IA e segurança.