Atividade Domiciliar 1

INE 5448 – Inteligência Artificial e Segurança

Prof. Ricardo Custódio

2º semestre de 2025

Objetivo

Consolidar os conhecimentos iniciais sobre Inteligência Artificial (IA), Aprendizado de Máquina (Machine Learning – ML) e Aprendizado Profundo (Deep Learning – DL), conectando-os às aplicações em diferentes setores e aos riscos associados ao uso da IA na área de segurança da informação.

Instruções

O aluno deverá responder às questões abaixo e entregar o trabalho em formato **PDF**. Tamanho sugerido: entre 5 e 10 páginas. Inclua: identificação do aluno, respostas e referências utilizadas (em formato ABNT).

Parte 1 – Conceitos Fundamentais

1. Explique, com suas palavras:
   a) O que é Inteligência Artificial (Russell; Norvig (1));
   b) O que é Aprendizado de Máquina e como ele se diferencia da IA em geral;
   c) O que é Deep Learning e qual sua relação com o aprendizado de máquina tradicional (Goodfellow; Bengio; Courville (2)).
2. Dê exemplos reais de cada conceito (IA, ML e DL), indicando:
   a) Onde é aplicado;
   b) Qual o impacto para usuários ou organizações.

Parte 2 – Aplicações da IA em Diversos Setores

Escolha pelo menos **três setores**, entre saúde, segurança da informação, transporte, finanças, indústria 4.0 ou governo. Para cada setor:

a) Cite um exemplo prático de uso da IA;

b) Analise vantagens e riscos dessa aplicação (OECD (3); World Health Organization (4)).

c) Relacione os riscos com os conceitos de **ameaças, vulnerabilidades e princípios de segurança** (Stallings (5)).

Parte 3 – Reflexão Crítica

1. Quais são os maiores benefícios e riscos da IA para a sociedade?
2. No contexto da **Segurança da Informação**, explique:
   a) Um caso de uso de IA que poderia **fortalecer** a proteção de dados (Stamp et al. (6)).
   b) Um caso de uso de IA que poderia **ameaçar** a segurança.
3. Faça uma analogia simples que ajude um leigo a entender a diferença entre Machine Learning e Deep Learning.

Parte 4 – Vídeo: The Future of AI is Beyond Imagination: 100 Predictions

Assista ao vídeo disponível em: `https://youtu.be/ZII3PQ3QkIQ`.
Dica: Procure usar NotebookLM para ajudar a assisitir e entender todo o vídeo (Google (7)).

1. Escolha **uma previsão** apresentada no vídeo e comente:
   a) Qual é a previsão;
   b) Como ela poderia impactar positivamente ou negativamente a sociedade;
   c) Se ela apresenta riscos de segurança ou desafios éticos relacionados ao uso da IA.
2. Selecione **cinco previsões** do vídeo que você considera **mais prováveis de se tornarem realidade nos próximos 10 anos**. Justifique sua escolha, explicando:
   a) Por que acredita que cada previsão é plausível;
   b) Quais são os fatores tecnológicos, econômicos, sociais ou políticos que favorecem sua concretização.

Esta seção busca estimular a reflexão crítica dos alunos sobre tendências emergentes em IA e sua relação com o futuro da segurança da informação YouTube (8).

Referências

1 RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 3. ed. [S.l.]: Pearson, 2016.

2 GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. **Deep Learning**. [S.l.]: MIT Press, 2016. Disponível em: ¡https://www.deeplearningbook.org¿.

3 OECD. **Artificial Intelligence in Society**. [S.l.]: OECD Publishing, 2019. DOI: 10.1787/eedfee77-en.

4 WORLD HEALTH ORGANIZATION. **Ethics and Governance of Artificial Intelligence for Health**. [S.l.]: WHO, 2021. Disponível em: ¡https://www.who.int/publications/i/item/9789240029200¿.

5 STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. [S.l.]: Prentice Hall, 1999.

6 STAMP, Mark et al. (Ed.). **Artificial Intelligence for Cybersecurity: Emerging Trends and Research Applications**. [S.l.]: Springer, 2022.

7 GOOGLE. **NotebookLM**. Acessado em: 19 ago. 2025. 2023. Disponível em: ¡https://notebooklm.google.com/¿.

8 YOUTUBE. **The Future of AI is Beyond Imagination: 100 Predictions**. https://youtu.be/ZII3PQ3QkIQ. 2024.