FIAP – Turma 2TDCPR [2024]

Disciplina: IA & Machine Learning

Checkpoint 1 - IA & Machine Learning

Professor: André Santos

Aluno: Ícaro Meirelles dos Santos

RM: 554027

# PARTE 1 - CONCEITOS

1. **O PAPEL DA INTELIGENCIA ARTIFICIAL (IA) NA SEGURANÇA CIBERNETICA**

Resumo: Presente na rotina na maioria das pessoas e principalmente nas organizações, a tecnologia tem sido a principal responsável para resoluções de problemas de forma inteligente, mas seu uso de forma inadequada pode abrir espaço para brechas nos sistemas da organização, ocasionando ataques mal-intencionados e vindo a causar prejuízos em larga escala. Com isso, esse trabalho tem o objetivo de apresentar o quanto a Inteligência Artificial é importante para as grandes, médias e pequenas organizações, auxiliando principalmente na identificação de ataques mal-intencionados e reforçando assim a segurança da informação ([Zequim & Ribeiro, 2022](https://revista.fatectq.edu.br/interfacetecnologica/article/view/1358/748)).

O resumo no parágrafo anterior refe-se ao artigo “O papel da IA na Segurança Cibernética” de Zequim e Ribeiro, 2022. Os autores discorrem sobre o uso de sistemas inteligentes em benefício da segurança dos dados das empresas" e abordam a importância da IA na proteção de dados corporativos. O artigo explora como a IA pode ser utilizada por organizações de diferentes portes para identificar ataques mal-intencionados e reforçar a segurança da informação.

O estudo destaca que, embora a tecnologia tenha sido crucial para a resolução de problemas de forma inteligente, o uso inadequado de sistemas pode abrir brechas para ataques cibernéticos. O artigo também descreve os benefícios e desafios do uso de IA na segurança cibernética, como sua capacidade de aprender e responder automaticamente a ameaças. Além disso, discute tipos de ataques cibernéticos comuns, como Phishing e ZeroDay, e as ferramentas que utilizam IA para proteger dados.

O artigo conclui que o uso da IA na segurança cibernética está cada vez mais em demanda devido ao aumento de ataques cibernéticos, como ransomware, levando as empresas a investirem nessa tecnologia como medida proativa de proteção. Apesar de apresentar algumas desvantagens, como custos elevados e a necessidade de profissionais qualificados, os benefícios, como monitoramento contínuo, redução de erros humanos e otimização de processos, superam os desafios, tornando a IA essencial para a segurança da informação. A IA ainda requer tempo de adaptação, pois seu aprendizado é contínuo, mas é considerada vital para enfrentar ameaças em um ambiente digital cada vez mais complexo. Além disso, a adoção de IA é estratégica para a competitividade das empresas, protegendo dados e evitando prejuízos financeiros, enquanto também auxilia na conformidade com regulamentações de proteção de dados, como a LGPD, por meio do uso de tecnologias avançadas para análise e compreensão de documentos legais e corporativos.

Dadas as considerações gerais sobre o artigo mencionado, para responder às perguntas a seguir leia o respectivo artigo de Zequim & Ribeiro, 2023; seguindo estas instruções:

1. **Indique a página da resposta:**Especifique o número da página onde a resposta pode ser encontrada.
2. **Indique a seção e subseções:**Mencione a seção e quaisquer subseções relevantes onde a resposta está localizada.
3. **Teça comentários relacionando o artigo com tópicos discutidos em sala de aula:**
   1. Identifique a página do slide da aula corrobora com o seu argumento.
   2. Estabeleça uma conexão entre o conteúdo do artigo e os tópicos abordados em sala de aula.
   3. Ao responder às perguntas, certifique-se de fornecer informações precisas e relevantes.

Perguntas sobre o artigo de Zequim & Ribeiro, 2022:

1. Qual o principal objetivo da segurança cibernética? (ítens A, B e C)

**Resposta:**

Objetivo da segurança cibernética é proteger nossos dispositivos e informações de ataques que possam roubar, manipular ou destruir dados. ela está aqui para garantir que os dados importantes e os recursos digitais de uma empresa estejam seguros, garantindo que permaneçam íntegros e autênticos.

Página: 24-25

Seção: 4 Segurança Cibernética

Subseção: Objetivo da Segurança Cibernética

Comentário:

Como dito em aula somo responsaveis pela a confidencialidade, integridade e disponibilidade dos dados.

1. O que é Phishing? (ítens A, B e C)

**Resposta:**

Phishing é um ataque que estimula os usuários a revelarem informações sigilosas, como senhas, dados bancários e números de documentos,através de e-mails falsos que direcionam para páginas idênticas às legítimas.

**Página: 26**

**Seção:4.2 Tipos de ataques cibernéticos**

**Subseção: Phishing**

Comentário:

São tentativas de roubo de dados focados em E-mails parar mandar aos alvos e induzindo o acesso do usuario relacionado ao slide 3

1. Como a inteligência artificial e a segurança cibernética trabalham juntas? (ítens A e C)

**Resposta:**

A inteligência artificial pode aprender com dados e identificar ameaças automaticamente, assim como reagir rapidamente a ataques cibernéticos.detectando e corrigindo problemas antes que causem danos significativos.

**Página: 26-27**

**Seção: 5. Como a Inteligência Artificial e a Segurança Cibernética Trabalham Juntas**

Comentário:  
A IA nos pode ajudar com modelos, para automatizar a análise como de bases para termos resultados e tomada de decisão para corrigir vulnabilidades como no slide 4

1. Qual o marco histórico relacionado ao aumento de incidentes cibernéticos? (ítens A e C)

**Resposta:**

O marco histórico significativo foi o aumento de 394% nos ataques cibernéticos em 2020 devido à adoção do regime de home office durante a pandemia da COVID-19.

**Página: 27-28**

**Seção: 6. Inteligência Artificial nas Empresas**

Comentário:

Como discutido em aula sobre o caso Front Running que busca um operaador que vai fazer uma operação de grande valor e afetar o lucro do ativo como no slide 4

1. **A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA CIBERNÉTICA**

A inteligência artificial (IA) está se tornando uma ferramenta cada vez mais valiosa na prevenção e detecção de ataques cibernéticos. Isso se deve à sua capacidade de processar e analisar enormes quantidades de dados de tráfego de rede, logs de sistema e outras fontes em tempo real. Além disso, os algoritmos de aprendizado de máquina (machine learning) permitem que a IA se adapte e melhore continuamente sua capacidade de detectar novas ameaças e táticas de ataque.

No entanto, é importante lembrar que a IA não é uma solução mágica para a segurança cibernética. Os cibercriminosos também estão usando IA para desenvolver ataques mais sofisticados. Portanto, é fundamental adotar uma abordagem de segurança em camadas que combine IA com outras ferramentas e práticas de segurança, além de investir em treinamento e conscientização dos usuários.

Assim, um dos grandes desafios que a área de segurança cibernética é **estruturar uma abordagem de segurança em camadas que utilize IA e outras técnicas e/ou práticas de segurança.** Essa abordagem multifacetada é crucial para garantir que, mesmo que uma camada seja comprometida, as demais continuem a oferecer proteção, resultando em uma defesa resiliente e adaptável contra ameaças cibernéticas.

1. Posto isso e com base nos conhecimentos adquiridos na disciplina de IA & Machine Learning, como você estruturaria uma abordagem de segurança em camadas, que utilize IA e outras técnicas e/ou práticas de segurança?

**Resposta:**

Começaria pela parte de OWASP e NIST para estar seguindo os principais Frameworks de área de segurança, e com a IA desenvolver modelos para sempre ter tomadas de dicisão relacionado a tentativas de ataques, medidas de mitigação e melhorias tanto na rede local e Web da Empresa.

# PARTE 2 - APLICAÇÃO

* 1. Criar um repositório aberto da prova “disciplina\_ia\_c1\_2024” (disponibilize o link de acesso).
* 2. Organizar o material do check-point 1 (prova, csvs, imagens) por pasta.
* 3. Desenvolver uma aplicação no Google Colab para responder/analisar os seguintes pontos:
  + Carregue a base de dados “urls\_phishing\_checkpoint1.csv” para o repositório no Github.
  + Gere uma amostra com 4000 observações (ver na tabela 1 qual semente utilizar).
  + Faça a EDA das URLs de phishing e legítimas para as variáveis “length\_url”, “depth\_url”, e “age\_domain” (ver na tabela 1 qual variável deve utilizar).
  + Analisar no dataset (base de dados) “urls\_phishing\_checkpoint1\_not\_label.csv” quais domínios (coluna “domain”) tem maiores chances de conterem as urls de phishing?
  + De acordo com as suas análises qual a sua recomendação? Caso tenha identificado um possível ataque, qual deve ser a tomada de decisão para mitigar ou previnir o problema?
* 4. Carregar o Notebook no repositório “disciplina\_ia\_c1\_2024”.
* 5. Finalizar o relatório executivo, salvar um PDF e carregar no diretório “disciplina\_ia\_c1\_2024”.

Tabela 1. Parâmetros que devem ser utilizados por cada aluno para realizar a parte 2.

|  |  |  |
| --- | --- | --- |
| **Alunos** | **“Semente” para amostra aleatória de 4000 observações** | **Variável para EDA** |
| Demétrio de Freitas Oliveira | random\_state = 42 | length\_url |
| Erik Alves da Silva | random\_state = 7 | length\_url |
| Fabio Moraes do Amaral | random\_state = 101 | length\_url |
| Gabriel de Oliveira Monteiro Batista | random\_state = 2023 | length\_url |
| Gabriel Turcatti Conforto | random\_state = 303 | length\_url |
| Higor Moura Santos | random\_state = 17 | depth\_url |
| Ícaro Meirelles dos Santos | random\_state = 85 | depth\_url |
| Mateus Rocha Pessoa | random\_state = 123456 | depth\_url |
| Matheus Oliveira da Costa | random\_state = 999 | depth\_url |
| Nícolas Miguel Bittencourt Tanajura | random\_state = 2048 | depth\_url |
| Robert Leandro Lacerda | random\_state = 31415 | depth\_url |

**Distribuição da pontuação da avaliação**

Parte 1

1. Qual o principal objetivo da segurança cibernética? (1 pt)

2. O que é Phishing? (1 pt)

3. Como a inteligência artificial e a segurança cibernética trabalham juntas? (0,5 pt)

4. Qual o marco histórico relacionado ao aumento de incidentes cibernéticos? (0,5 pt)

5. Como você estruturaria uma abordagem de segurança em camadas com IA? (2 pts)

Parte 2

1. Criar repositório (0,25 pt)

2. O organizar repositório no GitHub (0,5 pt)

3. Desenvolver Notebook (2 pts)

4. Upload Notebook no GitHub (0,25 pt)

5. Relatório Executivo (2 pts)