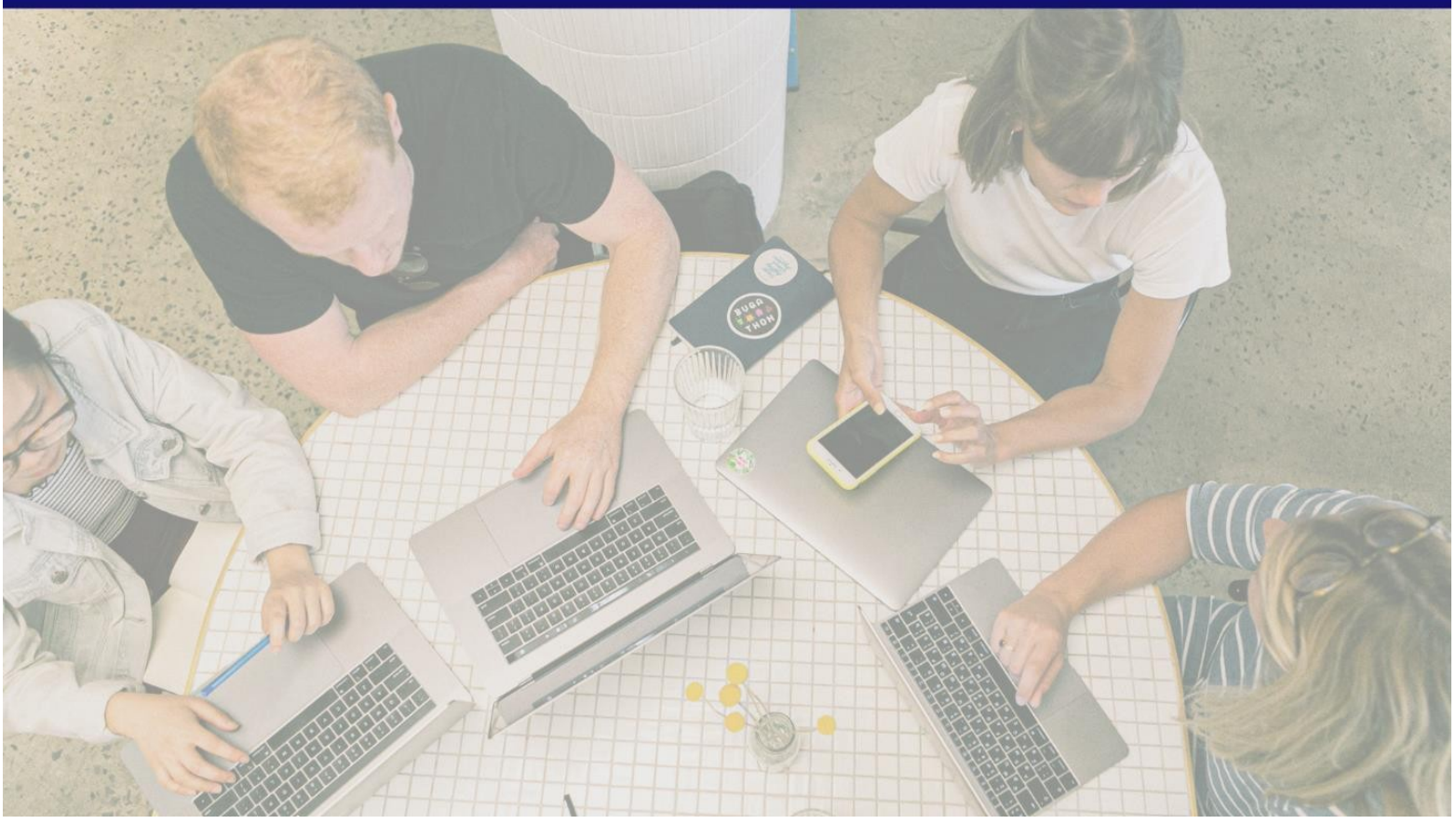
UNIFEOB
ESCOLA DE NEGÓCIOS

2023

PROJETO DE CONSULTORIA EMPRESARIAL



UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

AI&SecTech

SÃO JOÃO DA BOA VISTA, SP

OUTUBRO 2023

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

AI&SecTech

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Lucas Rafael C. da Silva, RA 1012023100143
Oziniel Ewerton Silva, RA 1012022101458
Pedro Riquelme Borsone , RA 1012022100206

SÃO JOÃO DA BOA VISTA, SP
OUTUBRO, 2023

SUMÁRIO

1 INTRODUÇÃO

No âmbito do projeto "AI&SecTech", a integração de um chatbot ao GPT emerge como um componente estratégico. Esta sinergia oferece vantagens notáveis, possibilitando uma compreensão avançada de consultas, respostas contextualmente relevantes e suporte especializado em segurança e ética. Com aprendizado contínuo, o chatbot melhora ao longo do tempo, contribuindo para a eficiência operacional e proporcionando acesso a informações atualizadas. Essa abordagem não apenas fortalece a automação proposta, mas também eleva a qualidade das interações, alinhando-se às metas do projeto em inovação responsável e segurança em sistemas computacionais.

2 DESCRIÇÃO DA EMPRESA

A empresa "Auto Mecânica SMA" é uma organização localizada na região de Mogi Guaçu, no estado de São Paulo, Brasil, especializada na prestação de serviços de manutenção automotiva. Com sede na Rua Rodolpho Innarelli, número 228, no bairro Jardim Herminio Bueno, a Auto Mecânica SMA estabeleceu sua presença no mercado há mais de uma década, atendendo com excelência e comprometimento a uma ampla clientela local.

3 PROJETO DE CONSULTORIA EMPRESARIAL

Histórico e Experiência

Fundada há mais de 10 anos, a Auto Mecânica SMA tem uma sólida trajetória no setor de serviços automotivos. Durante esse período, a empresa acumulou vasta experiência e conhecimento em manutenção corretiva e preventiva de veículos, consolidando-se como um recurso confiável para os residentes e empresas da região de Mogi Guaçu e arredores.

Especialização em Manutenção Automotiva

A Auto Mecânica SMA se destaca por sua especialização na prestação de serviços de manutenção automotiva de alta qualidade. A equipe de técnicos altamente qualificados e certificados emprega metodologias científicas e melhores práticas do setor para diagnosticare solucionar problemas mecânicos e elétricos em veículos de passageiros e comerciais.

Serviços Oferecidos

A empresa oferece uma ampla gama de serviços, incluindo, mas não se limitando a: ● Manutenção corretiva para reparar avarias e danos em veículos.

- Manutenção preventiva para aumentar a vida útil e o desempenho dos veículos.
- Diagnóstico avançado usando ferramentas e equipamentos de diagnóstico modernos.
- Troca de óleo, alinhamento e balanceamento de rodas.
- Reparos em sistemas elétricos e eletrônicos.
- Serviços de freios, suspensão e transmissão. 6
- Compromisso com a Qualidade e Sustentabilidade

A Auto Mecânica SMA prioriza a qualidade dos serviços prestados, aderindo rigorosamente às normas de segurança e regulamentações ambientais. Além disso, a empresa busca constantemente aprimorar suas práticas para minimizar o impacto ambiental de suas operações, contribuindo assim para a sustentabilidade na região.

Conclusão

A Auto Mecânica SMA é uma referência confiável em serviços de manutenção automotiva na região de Mogi Guaçu, combinando sua sólida experiência, especialização técnica e compromisso com a qualidade. Com uma base de clientes leais e uma abordagem metodológica e científica, a empresa continua a servir como um pilar essencial para a mobilidade e segurança dos veículos na comunidade local.

3.1 INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial (IA) constitui um campo multidisciplinar da ciência da computação que se concentra no desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Essas tarefas incluem aprendizado, raciocínio, resolução de problemas, percepção e compreensão da linguagem natural. A relevância da Inteligência Artificial na atualidade transcende fronteiras, influenciando significativamente diversas indústrias e aspectos da vida cotidiana.

No contexto do projeto "AI&SecTech", a integração da Inteligência Artificial é imperativa. Ela representa não apenas a automação avançada de processos, mas também uma abordagem inovadora para aprimorar a eficiência operacional e a tomada de decisões. A aplicação da IA no âmbito da segurança tecnológica, conforme proposto pelo projeto, promovea criação de sistemas mais inteligentes e adaptativos, capazes de identificar e mitigar ameaçasem constante evolução.

A interseção entre Inteligência Artificial e Segurança Tecnológica não apenas otimiza operações, mas também fortalece a resiliência contra potenciais vulnerabilidades. Ao integrar a IA, busca-se não apenas a automação, mas a capacidade de antecipar e responder proativamente a desafios emergentes em ambientes computacionais.

Dessa forma, a Inteligência Artificial não é apenas uma ferramenta no contexto do projeto, mas um alicerce que impulsiona a inovação, a segurança e a eficiência, moldando a forma como as organizações enfrentam os desafios contemporâneos. A integração estratégica da IA no projeto "AI&SecTech" reflete a compreensão de que, na era da transformação digital,a sinergia entre automação inteligente e segurança é essencial para alcançar resultados eficazese sustentáveis.

3.1.1 Introdução à Aplicação da IA

Uma aplicação específica da Inteligência Artificial no âmbito do projeto "AI&SecTech" é a utilização de algoritmos de Machine Learning para detecção de intrusões em sistemas de segurança de rede.

Contextualização: Em ambientes computacionais, a segurança da rede é uma prioridade crítica. A detecção precoce de atividades suspeitas desempenha um papel fundamental na prevenção de incidentes graves. Nesse contexto, os algoritmos de Machine Learning são empregados para analisar padrões de tráfego de rede e identificar comportamentos anômalos que podem indicar potenciais ameaças.

Exemplo Prático: Por exemplo, sistemas de detecção de intrusões baseados em Machine Learning aprendem padrões normais de comportamento da rede ao longo do tempo, considerando variáveis como volume de tráfego, protocolos utilizados e padrões de acesso. Quando ocorrem desvios significativos desses padrões aprendidos, o sistema pode identificar essas atividades como potencialmente maliciosas, acionando alertas para uma investigação mais aprofundada.

Casos do Mundo Real: Essa abordagem é amplamente adotada em setores como empresas de grande porte, instituições financeiras e organizações governamentais. Data centers, que armazenam informações sensíveis, aplicam ativamente essas técnicas para garantir a segurança das operações e a integridade dos dados.

Relevância para o Projeto "AI&SecTech": A aplicação de algoritmos de Machine Learning para detecção de intrusões não apenas fortalece a postura de segurança, mas também se alinha integralmente com a proposta do projeto. A integração da Inteligência Artificial para otimizar processos e proteger dados encontra expressão prática nessa aplicação, destacando a concretude da IA como uma ferramenta essencial para enfrentar os desafios reais de segurança em sistemas computacionais contemporâneos.

3.1.2 Implementação e Técnicas Utilizadas

Na implementação prática da Inteligência Artificial para a detecção de intrusões em redes, diversas técnicas específicas são empregadas. Dentre elas, destacam-se as "Redes Neurais Convolucionais" (CNNs), "Redes Multicamada" e "Perceptrons".

- **Redes Neurais Convolucionais (CNNs):**
- As CNNs são especialmente eficazes na análise de padrões em dados tridimensionais, como imagens. No contexto da segurança de rede, elas podem ser utilizadas para extrair características relevantes de padrões de tráfego, facilitando a detecção de anomalias.
- **Redes Multicamada:**
- Redes multicamada, ou MLPs (Multilayer Perceptrons), são comumente empregadas em tarefas de aprendizado supervisionado. No caso da detecção de intrusões, elas podem ser utilizadas para mapear padrões complexos de tráfego e identificar comportamentos anômalos.
- **Perceptrons:**
- Perceptrons, como unidades fundamentais de processamento em redes neurais, desempenham um papel essencial na análise e classificação de dados. Podem ser

empregados na identificação de padrões específicos associados a atividades maliciosas.

Linguagens e Ferramentas:

- **Python:** Amplamente utilizado devido à sua sintaxe clara e vasto suporte para bibliotecas de IA.
- **TensorFlow e PyTorch:** Frameworks populares para implementação de modelos de IA, incluindo CNNs e MLPs.
- **Scikit-learn:** Biblioteca em Python que oferece ferramentas simples e eficientes para análise de dados e modelagem preditiva.

Teachable Machine do Google:

- Embora não seja diretamente aplicável à detecção de intrusões, a Teachable Machine exemplifica a democratização do desenvolvimento de modelos de IA ao permitir treinamento sem a necessidade de habilidades avançadas em programação.

Relevância para o Projeto "AI&SecTech": A escolha da disciplina de Inteligência Artificial para este projeto é essencial, pois oferece um arsenal de técnicas poderosas para otimizar a segurança em sistemas computacionais. A IA pode melhorar significativamente a detecção de ameaças, proporcionando uma abordagem adaptativa que aprende com o comportamento do sistema ao longo do tempo. A capacidade de identificar padrões complexos de tráfego e de antecipar ameaças não só otimiza a resposta a incidentes, mas também contribui para a eficiência operacional, alinhando-se com a proposta central do projeto "AI&SecTech".

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é um pilar fundamental na era digital, onde as organizações enfrentam ameaças constantes à integridade, confidencialidade e disponibilidade de seus dados. Os conceitos aprendidos em sala de aula sobre segurança em sistemas computacionais se traduzem em diretrizes essenciais para mitigar riscos e proteger ativos valiosos.

Aplicação dos Conceitos Aprendidos:

Durante a implementação desses conceitos em uma empresa, os seguintes aspectos foram fundamentais:

- **Políticas de Segurança:**

- A definição e implementação de políticas de segurança claras e abrangentes foram cruciais. Isso incluiu o estabelecimento de práticas de autenticação robustas, controle de acesso e políticas de gerenciamento de senhas.
- **Monitoramento Proativo:**
- A aplicação de técnicas de monitoramento proativo, como análise de logs e detecção de anomalias, foi essencial para identificar potenciais ameaças em estágios iniciais. Isso permitiu uma resposta mais rápida a incidentes de segurança.
- **Atualizações e Patches:**
- A aplicação regular de atualizações e patches de segurança foi prioritária para fechar potenciais vulnerabilidades. Essa prática reflete o entendimento da importância de manter os sistemas atualizados frente às constantes evoluções nas ameaças cibernéticas.
- **Conscientização dos Colaboradores:**
- A formação de uma cultura de segurança, promovendo a conscientização entre os colaboradores, foi um desafio significativo. Estratégias educacionais foram empregadas para garantir que todos compreendessem a importância de práticas seguras no uso diário dos sistemas.

Desafios Enfrentados:

Durante a implementação desses conceitos, alguns desafios foram identificados:

- **Resistência à Mudança:**
- A resistência à adoção de novas práticas de segurança por parte dos colaboradores exigiu esforços adicionais em termos de treinamento e comunicação eficaz para superar a inércia organizacional.
- **Complexidade Tecnológica:**
- A gestão da complexidade tecnológica, especialmente em ambientes com uma variedade de sistemas e plataformas, representou um desafio. A implementação coordenada de medidas de segurança em diferentes camadas exigiu uma abordagem cuidadosa e integrada.
- **Ameaças Emergentes:**
- A rápida evolução das ameaças cibernéticas exigiu uma constante atualização das estratégias de segurança. A adaptação a ameaças emergentes, como ataques de phishing mais sofisticados, foi um desafio constante.

Conclusão:

A aplicação dos conceitos de segurança em sistemas computacionais na empresa reforça a importância desses conhecimentos adquiridos em sala de aula. A abordagem proativa, aliada a uma compreensão abrangente dos desafios enfrentados, é essencial para garantir a proteção eficaz dos sistemas e dados contra ameaças cada vez mais complexas no ambiente digital atual.

3.2.1 Conceitos e Implementação de Segurança

Com base nos tópicos "Conceitos de segurança lógica física" e "Conceito e Valor da Informação", os estudantes devem:

- Definir: Comecem por definir brevemente estes conceitos para contextualizar o leitor.
  Exemplo: "A segurança lógica física refere-se às medidas preventivas e reativas que protegem os recursos de hardware e software de uma organização."

- Aplicação na Empresa: Descrevam como estes conceitos foram entendidos e posteriormente implementados no ambiente da empresa. Isso pode envolver a instalação de sistemas de segurança físicos, a reestruturação da arquitetura de rede ou até mesmoa criação de protocolos internos.
  Exemplo: "Na empresa XYZ, implementamos sistemas de controle de acesso biométrico para garantir a segurança física de nossos servidores."

3.2.2 Detecção e Prevenção de Ataques

Neste sub-tópico, os estudantes devem focar nas medidas proativas e reativas adotadas pela empresa para garantir a segurança:

- Estratégias Adotadas: Descreva os principais métodos e estratégias usados para identificar possíveis ameaças.
  Exemplo: "Adotamos um sistema de monitoramento contínuo que verifica padrões anômalos no tráfego da rede, indicando possíveis invasões."
- Ferramentas Utilizadas: Mencionem as ferramentas específicas ou softwares implementados, com base nos tópicos aprendidos.
  Exemplo: "Utilizamos o software ABC para detecção de intrusão, que nos alerta instantaneamente sobre quaisquer atividades suspeitas."

4 CONCLUSÃO

O projeto "AI&SecTech" proporcionou descobertas significativas no que diz respeito à integração de Inteligência Artificial (IA) e Tecnologia da Informação (TI) para fortalecer a segurança em sistemas computacionais. As técnicas específicas de IA, como Redes Neurais Convolucionais e Redes Multicamada, foram aplicadas com sucesso na detecção de intrusões, contribuindo para a eficácia da defesa cibernética. Além disso, a conscientização organizacional e a implementação de políticas de segurança robustas demonstraram ser essenciais para uma postura de segurança proativa.

Importância de Decisões Estratégicas Informadas em TI:

A discussão sobre a importância de decisões estratégicas informadas em TI destaca a interseção crítica entre os aspectos técnicos e administrativos. A compreensão aprofundada das tendências tecnológicas, aliada a uma visão estratégica, capacita as organizações a implementar soluções inovadoras, como a integração de IA, para otimizar operações e fortalecer a segurança. As decisões informadas em TI não apenas garantem a eficiência técnica, mas também alinham as iniciativas tecnológicas com os objetivos administrativos e estratégicos da empresa.

Contribuições do Projeto para a Empresa:

O projeto "AI&SecTech" oferece contribuições significativas para a empresa selecionada. A implementação da IA na detecção de intrusões não apenas aprimora a capacidade de resposta a ameaças, mas também promove a eficiência operacional. A conscientização organizacional fortalece a cultura de segurança, reduzindo potenciais riscos associados a comportamentos inadequados. Além disso, as políticas de segurança bem definidas não apenas protegem os ativos da empresa, mas também influenciam positivamente sua reputação e confiança junto aos clientes e parceiros.

Influência Positiva nos Objetivos e Operações Futuras:

As contribuições do projeto têm o potencial de influenciar positivamente os objetivos e operações futuras da empresa. A integração de IA não é apenas uma medida de curto prazo, mas uma estratégia que pode evoluir continuamente para enfrentar ameaças em constante mudança. A cultura de segurança estabelecida e as políticas bem definidas estabelecem uma base sólida para a sustentabilidade da postura de segurança. Além disso, a conscientização organizacional perpetua a importância da segurança digital, preparando a empresa para desafios futuros e promovendo um ambiente operacional resiliente.

Em suma, as descobertas e propostas do projeto não apenas respondem aos desafios atuais, mas também posicionam a empresa para o sucesso em um cenário tecnológico em constante evolução. A tomada de decisões estratégicas informadas em TI emerge como um diferencial competitivo, impulsionando a empresa em direção a operações mais seguras, eficientes e alinhadas com seus objetivos de longo prazo.

REFERÊNCIAS

Essa parte está reservada para as referências, as quais devem estar metodologicamente discriminadas em ordem alfabética e corresponder às citações realizadas ao longo dos textos.

A utilização da metodologia científica é obrigatória e deve ser utilizado o Manual UNIFEOB para Trabalhos Acadêmicos ou as Normas da ABNT.

ANEXOS

Essa parte está reservada para os anexos, caso houver, como figuras, organogramas, fotos etc. E o estudante também deve anexar o relatório final do Projeto, conforme modelo a seguir.

Segue link do Projeto Integrado: https://youtu.be/AnQ9pLuzmZk