



**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**

AJUDA TI - CHATBOT

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**

**AJUDA TI - CHATBOT**

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Guilherme Henrique O. de Almeida, RA 1012023100740

Bruno Salim, RA 1012022100006

José Carlos Martins, RA 1012022100497

Alan Pereira, RA 1012023100411

SÃO JOÃO DA BOA VISTA, SP

OUTUBRO, 2023

# SUMÁRIO

<b>1 INTRODUÇÃO</b>	<b>6</b>
<b>2 DESCRIÇÃO DA EMPRESA</b>	<b>7</b>
<b>3 PROJETO DE CONSULTORIA EMPRESARIAL</b>	<b>8</b>
<b>3.1 INTELIGÊNCIA ARTIFICIAL</b>	<b>9</b>
<b>3.1.1 Aplicação Prática da Inteligência Artificial</b>	<b>9</b>
<b>3.1.2 Implementação e Técnicas Utilizadas</b>	<b>10</b>
<b>3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS</b>	<b>10</b>
<b>3.2.1 Conceitos e Implementação de Segurança</b>	<b>11</b>
<b>3.2.2 Detecção e Prevenção de Ataques</b>	<b>12</b>
<b>4 CONCLUSÃO</b>	<b>13</b>
<b>REFERÊNCIAS</b>	<b>14</b>
<b>ANEXOS</b>	<b>15</b>

# 1 INTRODUÇÃO

A integração de Inteligência Artificial (IA) e Segurança em Sistemas Computacionais representa uma abordagem inovadora e fundamental no mundo da tecnologia, que está moldando a forma como protegemos e fortalecemos nossos sistemas digitais em um ambiente cada vez mais complexo e ameaçador. À medida que a IA continua a se destacar como uma poderosa ferramenta para automatização, análise de dados e tomada de decisões, ela também se tornou uma aliada essencial na prevenção, detecção e resposta a ameaças cibernéticas. Esta sinergia entre IA e Segurança está revolucionando a maneira como enfrentamos os desafios de proteger informações sensíveis, redes e sistemas, permitindo a criação de soluções mais adaptáveis, eficientes e proativas para garantir a integridade, confidencialidade e disponibilidade de nossos ativos digitais. Neste contexto, exploraremos como essa abordagem inovadora está remodelando o panorama da segurança cibernética e como as tecnologias de IA estão sendo aplicadas para melhorar a resiliência e a eficácia dos sistemas computacionais. Vale ressaltar de acordo com estudos da IBM security, o Brasil está no quinto lugar de ataques cibernéticos com custo US\$5,27 milhões, esse é apenas uma estimativa que pode não refletir o verdadeiro custo dos ataques cibernéticos. pode variar dependendo de diversos fatores, incluindo o tamanho da empresa, o setor em que atua, a eficácia das medidas de segurança cibernética e a natureza do ataque.

## 2 DESCRIÇÃO DA EMPRESA

Nesse projeto não buscamos auxiliar somente uma empresa, e sim, auxiliar várias que têm dúvidas relacionadas na área de TI como por exemplo na segurança e em configurações de depósitos.

Sendo assim, desenvolvemos um ChatBot integrado com uma Inteligência Artificial (IA), para ajudar empresas que ainda tem dúvidas sobre como melhorar e prevenir a segurança de suas informações.

Em nossas pesquisas vimos que muitas empresas de pequeno e grande porte falharam no armazenamento de suas informações e de sua rede de serviços como falta de antivírus, senhas fracas e sem criptografia, aparelhos antigos e sem atualizações. A proteção das informações de uma empresa é primordial para sua sobrevivência já que em caso de invasão pode ocasionar em várias consequências.

## 3 PROJETO DE CONSULTORIA EMPRESARIAL

A princípio tivemos a ideia de ajudar uma empresa do ramo alimentício que tinha muitas dúvidas sobre sua área de TI , mas logo percebemos que muitas empresas ainda têm dificuldade com as novas tecnologias e de como se proteger de invasores em sua rede.

Logo percebemos que se criássemos um Chatbot teríamos um alcance maior e muitas outras empresas iriam tirar suas dúvidas, a ligação do Chat com a Inteligência Artificial (IA) irá trazer respostas que os auxiliam de tarefas simples como saber o melhor antivírus ou na configuração de um roteador e também tarefas mais complexas trazendo meios de como ajudar e dar um caminho para que possa melhorar sua segurança de dados e rede.

A criação do Chatbot com uma Inteligência Artificial foi um meio de darmos aos usuários respostas mais precisas e satisfatórias, para muitos a IA é desconhecida mas ela está sendo implementada em muitas áreas e beneficiando a população.

### 3.1 INTELIGÊNCIA ARTIFICIAL

Podemos considerar inteligência artificial (IA) como uma tecnologia das máquinas com capacidade de aprender com a coleta de dados, uma ferramenta valiosa no desenvolvimento de software.

A aplicação da IA oferece uma notável performance na produtividade, manutenção e traz automatização do processo.

Seu primeiro conceito e criação foi desenvolvido por Alan Turing também conhecido como Pai da Inteligência Artificial e deixou um grande legado na área da tecnologia.

### 3.1.1 Introdução à Aplicação da IA

A Inteligência Artificial (IA) é, de fato, uma tecnologia poderosa que permite que as máquinas aprendam com dados e melhorem suas capacidades ao longo do tempo. No contexto do desenvolvimento de software, a IA desempenha um papel fundamental, proporcionando benefícios significativos. Aqui estão algumas maneiras pelas quais a IA pode melhorar a produtividade, a manutenção e automatizar processos 8 h

**Aprendizado de Máquina (Machine Learning):** A IA, especificamente o Aprendizado de Máquina, permite que os algoritmos analisem dados para identificar padrões e tendências. Isso é extremamente valioso para aprimorar o desenvolvimento de software, pois pode ajudar a prever bugs, otimizar o desempenho e aprimorar a usabilidade.

No desenvolvimento de Testes e Qualidade com a IA, pode ser usada para automatizar testes de software, identificando problemas e garantindo que o código seja robusto e seguro. Isso economiza tempo e recursos, melhorando a qualidade do software.

A IA desenvolve a escrita de código mais eficiente, sugerindo soluções, correções de erros e até mesmo gerando código em algumas situações, pode prever falhas em sistemas e aplicativos, permitindo a manutenção proativa antes que ocorram problemas graves. Isso reduz o tempo de inatividade e os custos de manutenção.

Automatização de Processos pode automatizar tarefas repetitivas, como compilação, implantação e monitoramento, permitindo que os desenvolvedores se concentrem em atividades mais criativas e estratégicas.

Portanto, a aplicação da IA no desenvolvimento de software não apenas aumenta a eficiência e a produtividade, mas também contribui para a melhoria da qualidade e a redução de erros, tornando-a uma ferramenta valiosa e inovadora no campo da tecnologia.



### 3.1.2 Implementação e Técnicas Utilizadas

O projeto concentra na subárea da IA, o aprendizado de Máquina ML, a implementação foi configurado nesse modelo, treinado para capacitar os sistema de aprendizado com dados . em vez de programar explicitamente um algoritmo para executar uma tarefa, os modelos supervisionado, não supervisionado e reforço usam dados para melhorar o desempenho ao longo do tempo. A IA é um campo amplo da ciência da computação que se concentra em criar sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana. Por trás da lógica do algoritmo está todo método de multicamada e as funções de sigmóide, backpropagation e modelo perceptron de entrada e saída.

## 3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é fundamental diante do cenário digital em constante evolução. À medida que avança a tecnologia com evolução da IA, a segurança cibernética torna - se crucial por diversas razões. Sistemas computacionais armazenam muitas informações significativas , dados sensíveis, informações pessoais e corporativas. A importância do planejamento na gestão da segurança, enfatizando a necessidade de definir requisitos, utilizar tecnologia para identificar e avaliar problemas, desenvolver planos de contingência e implementar medidas corretivas. O objetivo principal é assegurar a confidencialidade, integridade e disponibilidade das informações.

Anexo 01 \_ O planejamento é de suma importância e, para ser eficaz, ele precisa ser testado e atualizado constantemente (FONTES, 2008). Outro ponto muito importante a ser destacado é que a segurança da informação é um dever de todos, e não somente da área de tecnologia da informação (TI). Portanto, o plano de segurança da informação, bem como o seu plano de contingência, deve ser conhecido por todos em uma empresa.

Esse conceitos aprendidos em sala de aula foram aplicados e os desafios enfrentados durante a implementação destes conceitos na empresa.

### 3.2.1 Conceitos e Implementação de Segurança

- A segurança lógica e física tem uma dimensão fundamental no que se refere a medidas relacionadas a hardware, instalações e recursos tangíveis. Objetivo é proteger contra ataques, ameaças físicas, engenharia social, roubos, acesso não autorizado às instalações. O controle de acesso físico, por vigilância de vídeo, sistema de alarme, salas de serviço seguras, backup de dados em local externo seguro e política de acesso físico restrito.

Ao combinar medidas de segurança lógica e física, as organizações podem criar uma abordagem abrangente para proteger ativos de informação. Por exemplo, um servidor seguro em uma sala com controle de acesso físico restrito (segurança física) pode ser complementado por firewalls e criptografia de dados (segurança lógica) para garantir uma proteção mais completa contra ameaças.

- O ataque de password spraying é explorar a probabilidade de que alguns usuários tenham senhas fracas, como "123456" ou "password", e, assim, obter acesso a contas comprometidas. Esse método é menos intrusivo e, portanto, mais difícil de detectar em comparação com ataques de força bruta, que tentam todas as combinações possíveis. Para se proteger contra ataques de password spraying, é importante implementar práticas de segurança, como o uso de senhas fortes e exclusivas, a ativação de autenticação de dois fatores (2FA) sempre que possível e o monitoramento de tentativas de login suspeitas. Além disso, é recomendável bloquear temporariamente contas após várias tentativas de login malsucedidas para evitar que os atacantes continuem tentando adivinhar senhas. Ataque de Força Bruta a Senhas, Ataque de Força Bruta a Chave de Criptografia, Ataque de Força Bruta a Números de Cartão de Crédito, Ataque de Força Bruta a PINs (Números de Identificação Pessoal), Ataque de Força Bruta a Endereços de Email. esses são apenas alguns exemplos de ataques de força bruta, e eles podem ser usados em várias situações para obter acesso não autorizado ou informações confidenciais. A proteção contra esses ataques geralmente

envolve o uso de senhas fortes, autenticação de dois fatores e outras medidas de segurança robustas.

### 3.2.2 Detecção e Prevenção de Ataques

- Estratégias Adotadas:

Utilizamos o painel do django para controlar a segurança da aplicação, criando usuários e grupos de usuários com permissões específicas na aplicação.

Utilizamos a biblioteca python-honeypot para fazer a segurança e rastreamento das tentativas de login sem sucesso no painel do django.

- Ferramentas Utilizadas:

Usamos o Python juntamente com o Django para desenvolver uma aplicação web e backend para implementar um chatbot com uma integração com a API da OpenAI, integrar essas funcionalidades ao Django, criar rotas, controladores e modelos para requisitos específicos do aplicativo.

## 4 CONCLUSÃO

Nesse desenvolvimento do projeto abordou dois temas extremamente importantes, a Inteligência Artificial (IA) é um dos assuntos mais abordado na área da tecnologia, desde de sua criação observamos uma grande evolução que fez muitas pessoas a utilizá-la para melhor processos nos seu cotidianos desde de pessoas simples até empresas de grande porte e tudos isso foi iniciado por Alan Turing que foi o desenvolvedor da base da computação moderna. Abordamos também a segurança em sistemas computacionais que é um temas extremamente importante nos dias atuais já que a base de dados de uma empresa e ou qualquer informações de uma pessoa tem o poder de afetar suas vidas de uma maneira sem precedentes se for vazadas por cracks ou pessoas maliciosas que buscam alguma vantagem em cima desses dados.

Hoje a área de TI é a parte mais importante de uma empresa e deve ter um bom investimento para sempre se manter atualizado com as melhores ferramentas, pois o banco de dados de uma empresa é seu bem mais valioso onde se concentra todas as informações de clientes, projetos, dados de funcionários e etc. Muitas pessoas maliciosas e também conhecidas com cracker tentam roubar essas informações e tentam tirar vantagem com ela, podendo pedir dinheiro em troca delas ou vender no submundo da internet(Deep Web). Assim as empresas devem investir em meios de segurança para evitar esses ataques, temos muitos antivírus corporativos que auxiliam no bloqueio de arquivos maliciosos e spam( termo usado para referir-se aos e-mails não solicitados), também temos como bloquear acessos não autorizados em nossa rede por meio de ferramentas com senhas e permissões. Também temos ferramentas de monitoração de acesso como Wireshark(captura o tráfego de rede na rede local e armazena esses dados para análise offline). Também temos sistemas de proteções integrando do a IA que podem ser mais eficientes para pessoas que tem site e apps criando barreiras para ataque,um exemplo seria o ataque de força bruta que consiste em tentar acessar um conta de um usuário tentando vários senhas até que descubra elas, com a IA podemos criar um certa quantidade de tentativas e se passar de quantidade o usuário é bloqueado.

Nossa equipe pensou em desenvolver um ChatBot com inteligência artificial para auxiliar pessoas que não têm muito conhecimento na área de TI e até profissionais de empresas que estão com dúvidas de algum processo de segurança. Basta apenas fazer uma pergunta que o Chat mostrar uma resposta muito precisa, assim auxiliando na melhor maneira de de prosseguir, podemos evitar acesso não autorizados apenas mudando a senha do login do wifi e para monitoria sua máquinas de PC podemos instalar um antivírus para monitoramentos, são simples processos que podem evitar um grande problema.

# REFERÊNCIAS

<https://www.djangoproject.com/>

<https://github.com/OWASP/Python-Honeypot>

[https://pt.wikipedia.org/wiki/Intelig%C3%A2ncia\\_artificial](https://pt.wikipedia.org/wiki/Intelig%C3%A2ncia_artificial)

<https://openai.com/blog/openai-api>