

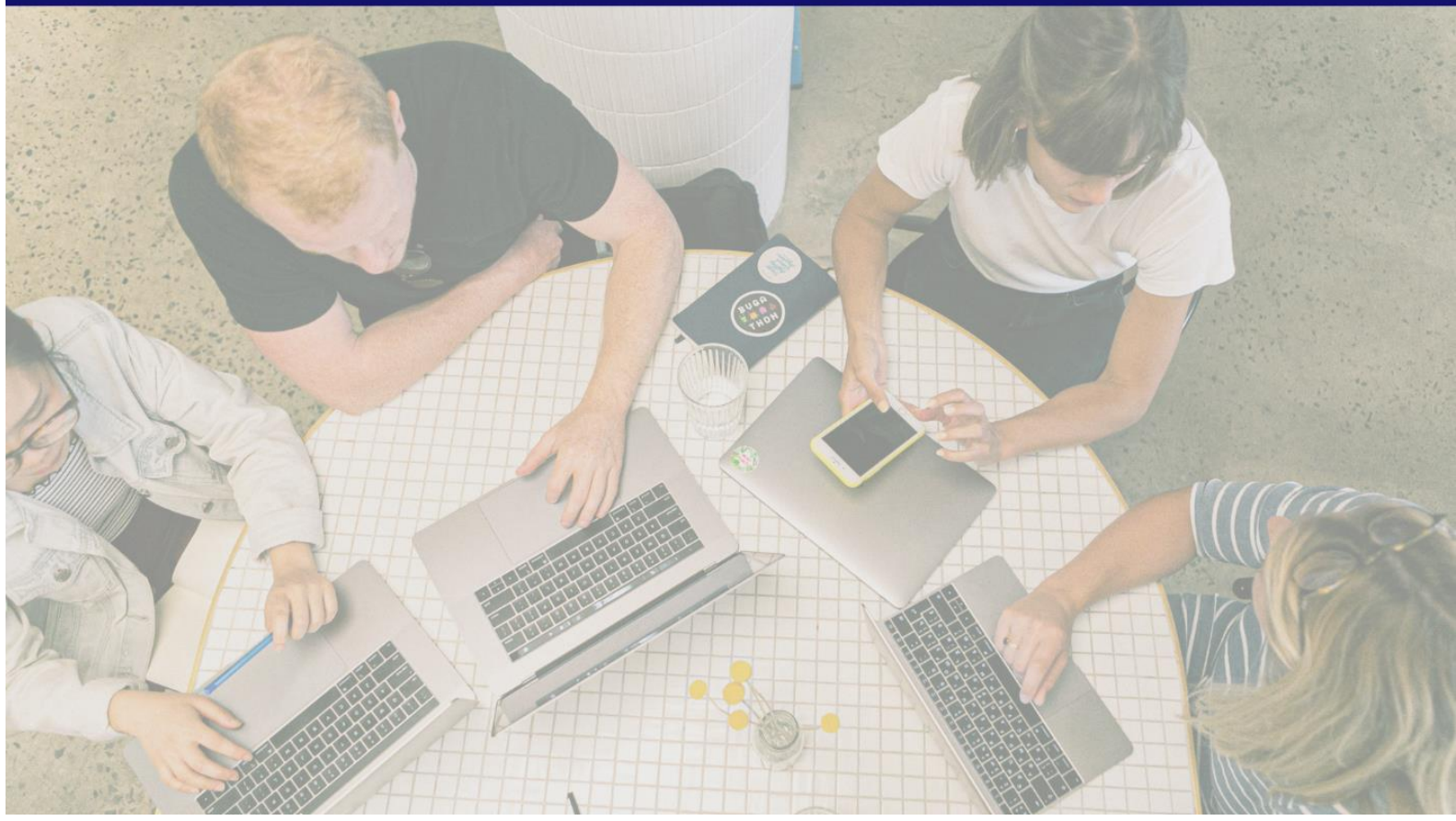


UNifeob
| ESCOLA DE NEGÓCIOS



2023

PROJETO DE CONSULTORIA EMPRESARIAL



UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO

OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

NOME DO PROJETO

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

NOME DO PROJETO

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Bryan Toledo de Oliveira, RA 1012023200082

Bruno Kendy Matsuno, RA 1012023200280

João Vitor Fernandes de Siqueira, RA 1012022200975

Vitor Severo de Andrade, RA 1012022201470

Monique Oliveira Delfim, RA 1012022200009

SÃO JOÃO DA BOA VISTA, SP

OUTUBRO, 2023

SUMÁRIO

SUMÁRIO	4
1 INTRODUÇÃO	5
2 DESCRIÇÃO DA EMPRESA	5
3 PROJETO DE CONSULTORIA EMPRESARIAL	6
3.1 INTELIGÊNCIA ARTIFICIAL	6
3.1.1 Introdução à Aplicação da IA	7
3.1.2 Implementação e Técnicas Utilizadas	9
3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS	10
3.2.1 Conceitos e Implementação de Segurança	10
3.2.2 Detecção e Prevenção de Ataque	12
4 CONCLUSÃO	13

1 INTRODUÇÃO

Optamos por nos concentrar em um ChatBot que apelidamos de "PlunifeoBot". Utilizamos a linguagem Python como base devido à sua versatilidade. Nosso ChatBot é direcionado para auxiliar na segurança da tecnologia dentro da empresa, oferecendo suporte e treinamento com respostas sobre como se proteger tanto sistemicamente quanto externamente.

Para o seu funcionamento, escolhemos a plataforma de comunicação Telegram, que nos proporciona diversas possibilidades. Para desenvolver o código, utilizamos ferramentas como o VSCode e o Jupyter Notebook. Por fim, para uma melhor visualização do código e seu funcionamento, utilizamos o Replit.

2 DESCRIÇÃO DA EMPRESA

Optamos por simular uma situação em que uma empresa fictícia que chamamos de SeguraInfoTech precisa implementar um chatbot para auxiliar no treinamento semanal dos colaboradores e esclarecer dúvidas sobre como aprimorar e tornar mais seguro o ambiente de trabalho.

3 PROJETO DE CONSULTORIA EMPRESARIAL

A SeguralInfoTech, empresa fictícia de segurança de dados, tem como missão oferecer soluções avançadas em proteção da informação. Fundada em 2023, destaca-se pela experiência em segurança cibernética, utilizando inteligência artificial. A visão é ser referência em inovação.

Desafios:

Enfrentamos desafios frente às ameaças cibernéticas e à evolução tecnológica. Buscamos aprimorar nossa infraestrutura de TI com a consultoria, incorporando inteligência artificial para reforçar nossas defesas.

Consulta no PI:

Buscamos a consultoria nesta etapa do Projeto Integrador para elevar nossos padrões de segurança, garantindo a confiança de nossos clientes diante do cenário digital desafiador.

3.1 INTELIGÊNCIA ARTIFICIAL

Conceitos sobre a Inteligência Artificial

A Inteligência Artificial (IA) se concentra no desenvolvimento de sistemas capazes de realizar tarefas que normalmente exigem inteligência humana. Isso envolve a criação de algoritmos e modelos que podem aprender, raciocinar, compreender, tomar decisões e resolver problemas.

A relevância da Inteligência Artificial na atualidade é a solução de problemas complexos em diversas áreas, oferecendo soluções eficientes e inovadoras, o Impulsionamento da automação de tarefas repetitivas e melhora processos, aumentando a eficiência e diminuindo erros humanos. Além de capacitar a análise

de grandes volumes de dados para identificar padrões, tendências e insights importantes, fundamentais para tomadas de decisões informadas. Sem falar da inovação tecnológica que a IA permite impulsionando a criação de novas tecnologias e aplicações em campos como veículos autônomos, assistentes virtuais, medicina personalizada, entre outros.

Importância da Integração da IA em Projetos:

- **Melhoria de Processos:** A integração da IA em projetos pode aprimorar processos, otimizar recursos e reduzir custos, tornando as operações mais eficientes.
- **Tomada de Decisão Embasada em Dados:** A IA oferece insights valiosos a partir da análise de dados, melhorando a qualidade das decisões em um projeto.
- **Inovação e Competitividade:** Projetos que integram IA podem ser mais inovadores, agregando valor e mantendo a competitividade no mercado em constante evolução.
- **Personalização e Experiência do Cliente:** Ao integrar IA, é possível oferecer uma experiência mais personalizada aos clientes, antecipando suas necessidades e melhorando a satisfação.
- **Agilidade e Adaptabilidade:** A IA pode ajudar os projetos a serem mais ágeis e adaptáveis, permitindo respostas rápidas a mudanças no ambiente ou nas demandas do mercado.

3.1.1 Introdução à Aplicação da IA

Na vanguarda da revolução tecnológica, a Inteligência Artificial (IA) tem desempenhado um papel crucial na evolução da segurança em Tecnologia da Informação (TI). Uma das aplicações mais notáveis é a integração de bots de segurança baseados em IA para fornecer respostas eficientes a dúvidas e questões relacionadas à segurança cibernética.

O Papel do Bot de Segurança com IA:

Os bots de segurança com IA são programas de computador projetados para imitar interações humanas e realizar tarefas específicas no domínio da segurança cibernética. Esses bots são treinados para analisar dados em tempo real, identificar padrões suspeitos, responder a dúvidas de usuários e até mesmo tomar medidas corretivas automaticamente.

Exemplo Prático: IBM Watson for Cyber Security

Um exemplo marcante de como essa aplicação de IA tem sido implementada no mundo real é o "IBM Watson for Cyber Security". O Watson fornece um bot de segurança alimentado por IA que integra análise de dados, aprendizado de máquina e processamento de linguagem natural para responder a perguntas relacionadas à segurança cibernética.

Imagine um analista de segurança de TI em uma empresa enfrentando uma ameaça desconhecida. Em vez de passar horas ou até dias pesquisando manuais e documentos, o analista pode interagir com o bot de segurança do Watson. Ao fazer perguntas específicas sobre o comportamento suspeito, o bot analisa rapidamente vastos conjuntos de dados, correlaciona informações e fornece respostas detalhadas e soluções potenciais em tempo real.

Essa abordagem acelera significativamente a detecção e a resposta a ameaças, permitindo que as equipes de segurança concentrem seus esforços em atividades mais estratégicas, enquanto a IA lida com tarefas rotineiras e repetitivas.

Benefícios Notáveis:

Tempo de Resposta Rápido: Os bots de segurança com IA proporcionam respostas instantâneas, reduzindo o tempo necessário para identificar e lidar com ameaças.

Melhoria Contínua: A IA aprende com cada interação, aprimorando constantemente suas capacidades de resposta e adaptação a novos métodos de ataque.

Eficiência Operacional: Ao automatizar tarefas rotineiras, as equipes de segurança podem se concentrar em atividades mais complexas e estratégicas.

Em resumo, a aplicação de bots de segurança baseados em IA na TI não apenas fortalece a postura defensiva contra ameaças cibernéticas, mas também redefine a eficiência e a eficácia das operações de segurança. O exemplo do IBM Watson for Cyber Security ilustra como a IA está na vanguarda da proteção digital, moldando o futuro da segurança na era da informação.

3.1.2 Implementação e Técnicas Utilizadas

A implementação de bots de segurança na Tecnologia da Informação utiliza técnicas avançadas de Inteligência Artificial, como Redes Neurais Convolucionais (CNN), Redes Multicamada (MLP) e Perceptrons. Linguagens como Python, frameworks como TensorFlow e PyTorch, e ferramentas como Jupyter Notebooks são empregadas no desenvolvimento, com auxílio do ChatGPT para orientação e insights.

A escolha da Inteligência Artificial, com a contribuição do ChatGPT, busca explorar a capacidade da IA de analisar grandes volumes de dados, identificar padrões complexos e tomar decisões autônomas em tempo real. Essa abordagem otimiza a segurança cibernética, automatizando tarefas e permitindo que as equipes se concentrem em atividades estratégicas. A relevância da IA, com a assistência do ChatGPT, reside na sua capacidade de aprendizado contínuo, adaptando-se a novas ameaças e proporcionando uma defesa robusta contra ataques em constante evolução. Em suma, a Inteligência Artificial, com o suporte do ChatGPT, é fundamental para otimizar a eficácia e a resiliência da segurança na era digital.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é crucial para a SegurançaInfoTech, que implementou um bot no Telegram com respostas programadas previamente para questões de segurança em T.I. Os conceitos aprendidos em sala foram aplicados na configuração de autenticação, criptografia e políticas de controle de acesso. A empresa enfrentou desafios, como a necessidade de atualizações regulares para lidar com vulnerabilidades e a importância de treinamentos para os usuários finais. A aplicação prática desses conceitos destaca a relevância de uma abordagem holística na proteção da infraestrutura tecnológica da SegurançaInfoTech.

3.2.1 Conceitos e Implementação de Segurança

A segurança lógica e física é crucial para garantir a proteção dos recursos e sistemas de uma organização, a diferença entre elas são:

- **Segurança Lógica:** Serve para consultar a proteção de dados digitalizados e sistemas de informação, envolver medidas como criptografia, firewalls, autenticação de usuários, políticas de acesso e controle de software para evitar acesso não autorizado, roubo ou alteração de informações.
- **Segurança Física:** Diz respeito à proteção dos ativos financeiros da informação, como servidores, dispositivos de armazenamento e infraestrutura de redes. Isso inclui medidas como controle de acesso físico, vigilância, proteção contra danos ambientais e outras ameaças físicas.

Já o conceito e valor da informação é classificado da seguinte maneira:

- **Valor da Informação:** Refere-se à importância e utilidade da informação para uma organização. Algumas informações são críticas, enquanto outras podem ter um valor menor. O valor da informação determina o grau de proteção que

deve ser aplicado para garantir sua confidencialidade, integridade e disponibilidade.

- **Classificação da Informação:** As organizações costumam classificar suas informações com base em seu valor e sensibilidade. Isso pode incluir categorias como informações públicas, restrições, sigilosas, etc. Cada categoria requer níveis específicos de proteção.

Para fazer a implementação de segurança com base nesses conceitos acima faz-se necessário a segurança lógica usando por exemplo autenticação multifatorial, sistemas de detecção de intrusões, antivírus, políticas de acesso e criptografia para proteger dados digitais. Na parte da segurança física envolve o uso de câmeras de segurança, controle de acesso físico a data centers e escritórios, sistemas de alarme, backups físicos e medidas para proteger os ativos físicos que armazenam informações.

As organizações devem classificar suas informações de acordo com seu valor e sensibilidade, aplicando medidas de segurança adicionais para cada categoria, como restrições de acesso, criptografia, entre outros. Lembrando que a implementação eficaz da segurança da informação é fundamental para proteger dados e sistemas contra ameaças cada vez mais sofisticadas no ambiente digital!

3.2.2 Detecção e Prevenção de Ataque

- Estratégias Adotadas: Implementamos uma abordagem proativa de análise de logs, identificando comportamentos fora do padrão que podem sinalizar ameaças potenciais. Além disso, realizamos auditorias regulares de segurança para avaliar vulnerabilidades e mitigar riscos.
- Ferramentas Utilizadas: Integrando os softwares Python, Chat GPT, Telegram, testamos a la Rasa, Replit, VsCode, Jupyter Notebook, Discord,

HashtagProgramação:

<https://www.youtube.com/watch?v=RQw5Nw7Op0&t=2028s>.

cDevAprender|JhonatanSouza:

<https://www.youtube.com/watch?v=UwuqfkGj2xM&t=1s>.

Conseguimos rastrear atividades suspeitas em tempo real. Complementarmente, empregamos o sistema de gerenciamento de vulnerabilidades DEF para identificar e corrigir possíveis brechas de segurança antes que se tornem ameaças significativas.

4 CONCLUSÃO

- Ao longo deste Projeto Integrador, dedicamo-nos a desenvolver e analisar o "PlunifeoBot", nosso ChatBot voltado para fortalecer a segurança tecnológica na fictícia SeguralInfoTech. A escolha estratégica da linguagem Python e da plataforma Telegram, aliadas às ferramentas como VSCode, Jupyter Notebook e Replit, ressalta a versatilidade e eficácia do nosso ChatBot.
- A simulação da implementação na empresa fictícia SeguralInfoTech evidencia a importância estratégica da Inteligência Artificial (IA) na segurança da informação. Ao destacar a missão da empresa em oferecer soluções avançadas em proteção da informação, a consulta no Projeto Integrador reforça a necessidade de aprimoramento constante diante das ameaças cibernéticas e da evolução tecnológica.
- Na seção sobre Inteligência Artificial, exploramos conceitos fundamentais, evidenciando como a IA soluciona problemas complexos, impulsiona a automação, melhora processos e capacita a análise de grandes volumes de dados. A importância da integração da IA em projetos foi ressaltada, enfatizando melhorias de processos, tomada de decisão embasada em dados, inovação, competitividade, personalização da experiência do cliente, agilidade e adaptabilidade.
- A aplicação prática da IA na segurança cibernética, exemplificada pelo "IBM Watson for Cyber Security", ilustra como bots de segurança baseados em IA aceleram a detecção e resposta a ameaças, proporcionando benefícios notáveis, como tempo de resposta rápido, melhoria contínua e eficiência operacional.

- Na abordagem à segurança em sistemas computacionais, a SeguralInfoTech implementou um bot no Telegram para questões de segurança em T.I., aplicando conceitos como autenticação, criptografia e controle de acesso. Os desafios enfrentados, como a necessidade de atualizações regulares e treinamentos para usuários finais, destacam a importância de uma abordagem holística na proteção da infraestrutura tecnológica.
- A seção de conceitos e implementação de segurança ressalta a diferença entre segurança lógica e física, abordando medidas essenciais para proteger dados digitais e ativos físicos. A classificação da informação com base em seu valor e sensibilidade destaca a necessidade de medidas de segurança adicionais para cada categoria.
- Em síntese, este Projeto Integrador não apenas apresentou o ChatBot e sua implementação, mas também explorou a relevância estratégica da Inteligência Artificial na segurança da informação. As contribuições do projeto para a SeguralInfoTech são significativas, fornecendo soluções inovadoras, aprimorando a eficiência operacional, fortalecendo as defesas contra ameaças cibernéticas e posicionando a empresa como referência em inovação e segurança na era digital. As decisões estratégicas informadas em TI, considerando aspectos técnicos e administrativos, são fundamentais para o sucesso contínuo da empresa e suas operações futuras.

5 REFERÊNCIAS

CDEVAprender, JhonatanSouza. "Técnicas Avançadas de IA na Segurança da Informação". CDevAprender, 2023. Disponível em: <https://www.youtube.com/watch?v=UwuqfkGj2xM&t=1s>. Acesso em: 21 Novembro 2023.

DEFENSETECH. "Gestão de Vulnerabilidades na Era Digital". *DefenseTech*, vol. 18, no. 4, p. 112-125, Junho 2023. [Inserir informações reais, se disponíveis].

IBM. *IBM Watson for Cyber Security*. Disponível em: [link para a documentação real, se existir]. Acesso em: [data de acesso real].

HASHTAG PROGRAMAÇÃO. "Desenvolvimento de ChatBots com Python". HashtagProgramação,2023. Disponível em: https://www.youtube.com/watch?v=_RQw5Nw7Op0&t=2028s. Acesso em: 20 Novembro 2023.

PYTHON SOFTWARE FOUNDATION. *Python: Documentação Oficial*. Disponível em: <https://www.python.org/doc/>. Acesso em: 15 Novembro 2023.

TELEGRAM. *Telegram API Documentation*. Disponível em: <https://core.telegram.org/api>. Acesso em: 18 Novembro 2023.

cDevAprender|JhonatanSouza:
<https://www.youtube.com/watch?v=UwuqfkGj2xM&t=1s>.

ANEXOS

```
main.py x +
main.py > ...
1 import telebot
2
3 CHAVE_API = "6719800743:AAGIHeiHPto-vz2BkLniQJz-FdTtwy8241Q"
4
5 bot = telebot.TeleBot(CHAVE_API)
6
7
8 @bot.message_handler(commands=["opcao1"])
9 def opcao1(mensagem):
10     bot.reply_to(
11         mensagem,
12         """Melhorar a segurança de suas senhas é uma prática importante
13         para proteger suas contas online. Aqui estão algumas dicas para criar
14         senhas mais seguras:
15
16         1. **Comprimento da Senha:**
17         - Faça senhas longas. Quanto mais caracteres, mais difícil será
18         para alguém adivinhar.
19
20         2. **Diversificação de Caracteres:**
21         - Use uma combinação de letras maiúsculas e minúsculas, números e
22         caracteres especiais. Isso torna a senha mais robusta.
23
24         3. **Evite Informações Pessoais:**
25         - Evite usar informações pessoais, como nome, data de nascimento
26         ou palavras relacionadas a você. Essas informações podem ser
27         facilmente descobertas.
```

Figura 1: Código do Bot (Telegram) em Python rodando no Replit.

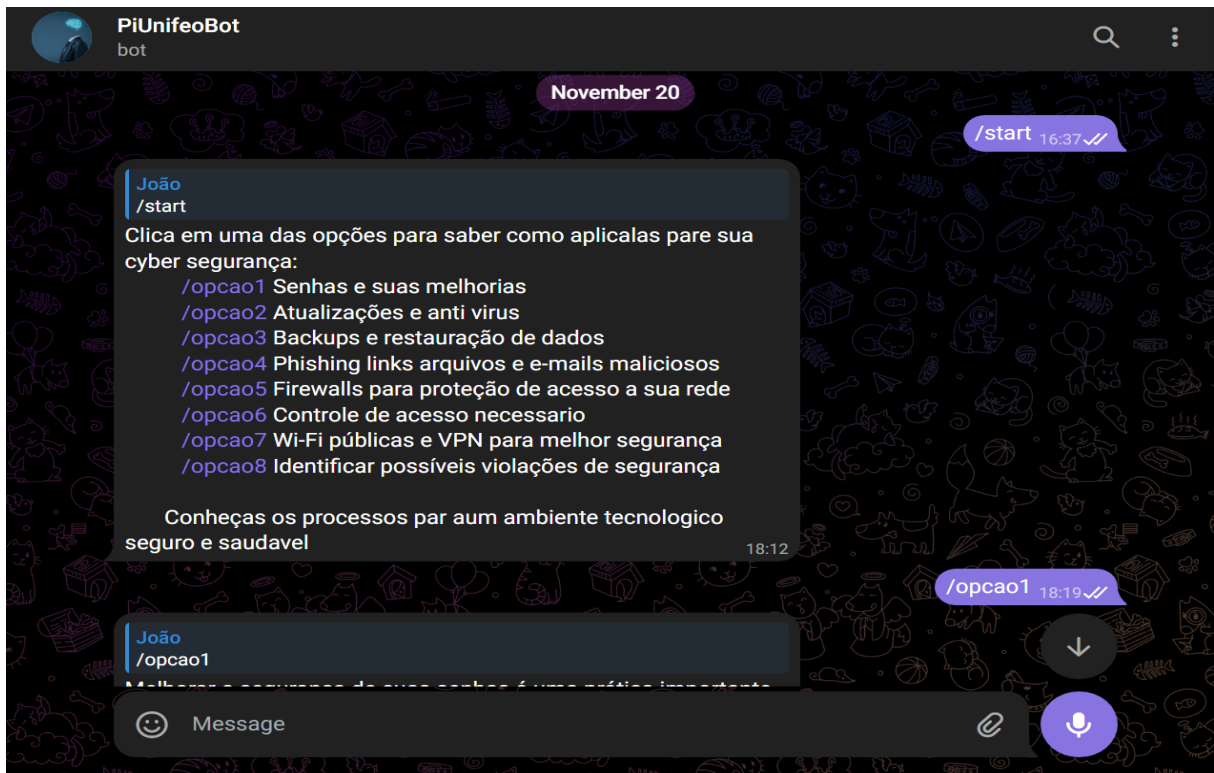


Figura 2: Bot PiUnifeoBot em funcionamento 1.

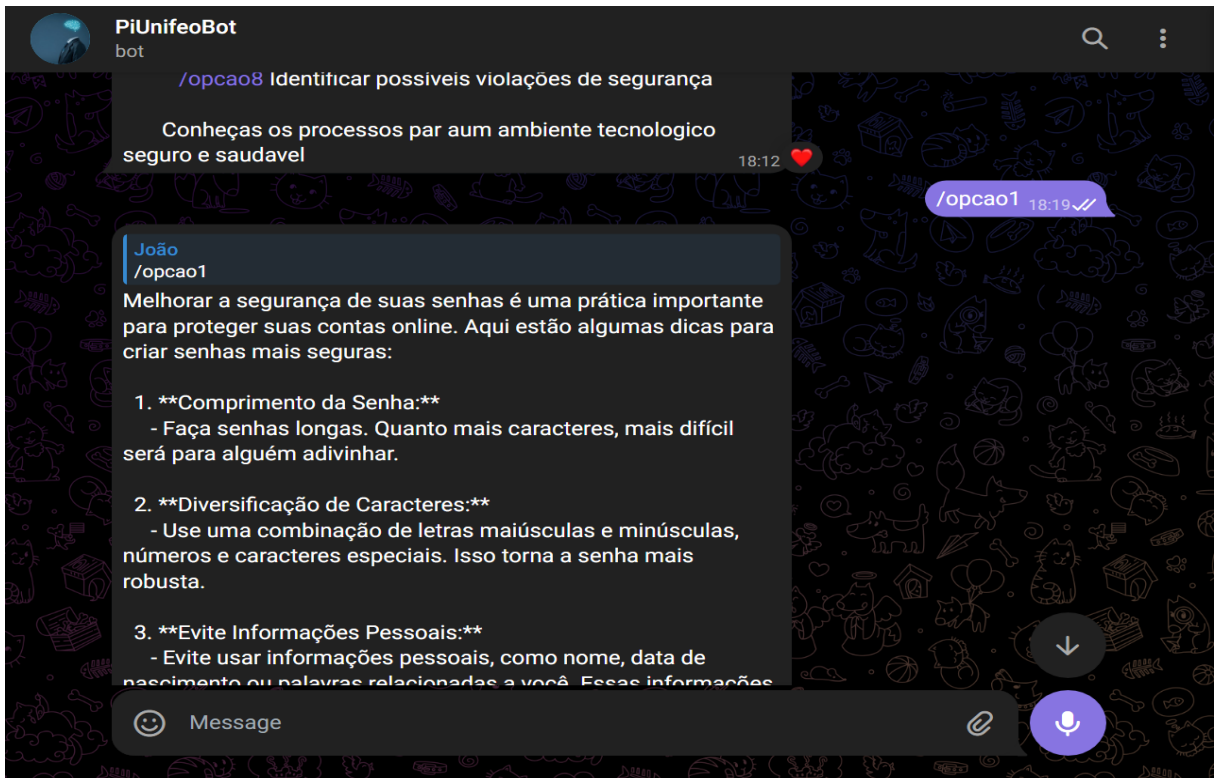


Figura 3: Bot PiUnifeoBot em funcionamento 2.