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:

Gabriel gerts luiz - 1012023200184

SUMÁRIO

1 INTRODUÇÃO

No cenário digital em constante evolução, a segurança da informação tornou-se uma

preocupação fundamental para organizações e indivíduos. A rápida expansão da tecnologia trouxe consigo desafios significativos, aumentando a complexidade das ameaças cibernéticas que podem comprometer a integridade, confidencialidade e disponibilidade dos dados. Nesse contexto, surge a necessidade de uma abordagem proativa e educativa para garantir a proteção eficaz das informações.

O projeto de chatbot de segurança da informação propõe-se a oferecer uma solução inovadora e interativa para auxiliar na compreensão e implementação de práticas de segurança cibernética. Este chatbot, alimentado por inteligência artificial, visa capacitar usuários, sejam eles indivíduos ou profissionais de TI, a adotar medidas preventivas e corretivas para mitigar riscos e fortalecer a resiliência digital.

Ao integrar tecnologias avançadas de processamento de linguagem natural, o chatbot proporcionará uma experiência intuitiva e personalizada, adaptando-se ao nível de conhecimento e às necessidades específicas de cada usuário. Com uma abordagem amigável e acessível, o chatbot orientará os usuários por conceitos-chave de segurança da informação, desde noções básicas até estratégias avançadas de proteção.

Este projeto representa não apenas uma ferramenta de aprendizado, mas também um recurso dinâmico que evoluirá continuamente para se manter atualizado em relação às últimas ameaças cibernéticas e melhores práticas de segurança. Através de diálogos interativos, simulações de cenários e fornecimento de informações relevantes, o chatbot visa criar uma cultura de segurança robusta e consciente, promovendo a prevenção ativa e a prontidão diante dos desafios digitais em constante mutação.

2 DESCRIÇÃO DA EMPRESA

A segurança da informação desempenha um papel vital no setor bancário, onde a confiança e a integridade são primordiais. Bancos, responsáveis por dados sensíveis dos clientes, enfrentam constantes ameaças cibernéticas em transações digitais globais. Medidas como firewalls, detecção de intrusão e criptografia são essenciais

para proteger contra ataques, sendo a educação contínua de funcionários e clientes crucial. A conformidade com normas rigorosas é obrigatória, pois qualquer falha na segurança pode resultar em impactos financeiros, perda de confiança e danos à reputação. Em síntese, a segurança da informação é fundamental para a estabilidade bancária, exigindo abordagem proativa e investimentos contínuos em tecnologias atualizadas.

Por isso, a empresa escolhida foi o Bradesco.

Banco *Bradesco* SA

CNPJ: 60.746.948.0001-12.

Endereço: Cidade de Deus, s/nº Vila Yara Osasco | SP |

CEP: 06029-900.

3 PROJETO DE CONSULTORIA EMPRESARIAL

O Bradesco, Banco Bradesco S.A., é uma das maiores instituições financeiras do Brasil, com uma história rica e uma presença significativa no setor bancário. Fundado em 1943 na cidade de Marília, São Paulo, por Amador Aguiar, inicialmente como Banco Brasileiro de Descontos, o Bradesco cresceu ao longo das décadas por meio de fusões e aquisições estratégicas.

Ramo de Atuação: O Bradesco atua em diversos segmentos financeiros, oferecendo uma ampla gama de serviços, incluindo serviços bancários tradicionais, seguros, previdência privada, gestão de ativos, entre outros. Sua presença é marcante tanto no varejo, atendendo milhões de clientes individuais, quanto no segmento corporativo, atendendo empresas de diversos portes.

Missão: A missão do Bradesco é fornecer soluções financeiras inovadoras, contribuindo para o desenvolvimento sustentável e a satisfação de seus clientes.

Visão: A visão do banco busca ser reconhecido como a melhor e mais eficiente organização financeira, destacando-se pela excelência no relacionamento com clientes, colaboradores e na geração de valor para a sociedade.

Valores: Os valores do Bradesco incluem ética, respeito, transparência, responsabilidade socioambiental, e inovação.

Desafios e Consultoria: Dentre os desafios enfrentados pelo Bradesco ao longo de sua trajetória, destacam-se a competitividade acirrada no setor bancário, as demandas crescentes por inovação tecnológica e a necessidade de se adaptar a um ambiente financeiro dinâmico e regulamentado. A busca por consultoria muitas vezes está relacionada à otimização de processos, implementação de tecnologias avançadas, gestão de riscos e conformidade com regulamentações em constante evolução. A consultoria pode ser essencial para manter a eficiência operacional, a segurança da informação e a capacidade de inovação do Bradesco diante de um cenário financeiro em constante transformação.

3.1 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é um campo da ciência da computação que busca criar sistemas capazes de realizar tarefas que, normalmente, requerem inteligência humana. Essas tarefas incluem aprendizado, raciocínio, resolução de problemas, reconhecimento de padrões, compreensão de linguagem natural e interação com o ambiente.

Relevância Atual:

A relevância da IA na atualidade é evidente em sua aplicação em diversos setores, incluindo saúde, educação, automação industrial e, particularmente, no setor bancário. A capacidade da IA de processar grandes volumes de dados, aprender com padrões e tomar decisões rápidas a torna uma ferramenta valiosa em ambientes complexos e dinâmicos.

Integração no Contexto Bancário:

No contexto bancário, a IA desempenha um papel fundamental. Ela pode otimizar processos, detectar fraudes, personalizar experiências do cliente, prever tendências de mercado e aprimorar a segurança da informação. A capacidade de analisar dados em tempo real permite respostas rápidas a ameaças cibernéticas, enquanto algoritmos de aprendizado de máquina aprimoram a eficiência operacional e a experiência do usuário.

Importância da IA no Setor Bancário:

1. **Detecção de Fraudes:** A IA pode identificar padrões suspeitos de atividade financeira, contribuindo para a prevenção e detecção de fraudes.
2. **Atendimento ao Cliente:** Chatbots e assistentes virtuais baseados em IA oferecem suporte ao cliente 24/7, respondendo a consultas, fornecendo informações e facilitando transações.
3. **Análise Preditiva:** Algoritmos de IA analisam dados históricos para prever tendências de mercado, riscos e oportunidades de investimento.
4. **Segurança da Informação:** A IA fortalece as defesas contra ameaças cibernéticas, identificando comportamentos anômalos e protegendo dados sensíveis.
5. **Personalização de Serviços:** A IA analisa o comportamento do cliente para oferecer recomendações personalizadas, melhorando a experiência do usuário.

A integração da IA no setor bancário não apenas aumenta a eficiência operacional, mas também impulsiona a inovação, melhorando a segurança e a qualidade dos serviços oferecidos. Isso destaca a importância de abraçar a Inteligência Artificial como uma ferramenta estratégica para enfrentar os desafios e aproveitar as oportunidades na era digital.

3.1.1 Introdução à Aplicação da IA

Um exemplo prático de um chatbot que oferece informações sobre segurança da informação pode ser observado em instituições financeiras que implementam

assistentes virtuais para orientar clientes sobre práticas seguras online. Vamos considerar um cenário hipotético:

Cenário: Um banco decide integrar um chatbot especializado em segurança da informação em seu site e aplicativo móvel para oferecer orientações aos clientes sobre como proteger suas contas contra ameaças cibernéticas.

Funcionalidades do Chatbot:

1. **Educação sobre Phishing:** O chatbot explica o que é phishing, como os golpes funcionam e fornece dicas para identificar e evitar e-mails ou mensagens fraudulentas.
2. **Autenticação Segura:** Oferece informações sobre a importância da autenticação multifatorial (AMF) e orienta os clientes sobre como configurá-la para aumentar a segurança de suas contas.
3. **Atualizações de Segurança:** Informa sobre as últimas ameaças cibernéticas e fornece dicas de segurança relevantes, incentivando os clientes a manterem seus dispositivos e softwares atualizados.
4. **Configurações de Privacidade:** Orienta sobre configurações de privacidade, como ajustar as opções de visibilidade em perfis online e redes sociais para proteger informações pessoais.
5. **Dúvidas Frequentes:** Responde a perguntas comuns dos clientes relacionadas à segurança da informação, como criar senhas fortes, como identificar sites seguros, entre outros.

Experiência do Usuário: Os clientes podem interagir com o chatbot em tempo real, seja através de mensagens de texto ou comandos de voz, obtendo informações imediatas e personalizadas sobre segurança cibernética. Além disso, o chatbot pode encaminhar os usuários para recursos adicionais, como tutoriais ou links para ferramentas de verificação de segurança.

Benefícios:

1. Acesso 24/7: Os clientes têm acesso a informações de segurança a qualquer hora do dia, independentemente do horário de funcionamento do banco.
2. Personalização: O chatbot adapta as informações com base nas necessidades e nível de conhecimento do cliente, oferecendo uma experiência personalizada.
3. Prevenção de Riscos: Ao educar os clientes sobre práticas seguras, o chatbot contribui para a prevenção de fraudes e ataques cibernéticos.

4. Engajamento: A interação proativa com os clientes através do chatbot pode aumentar o engajamento e a conscientização sobre questões de segurança.

Esse exemplo demonstra como um chatbot de segurança da informação pode ser uma ferramenta eficaz para capacitar os usuários, fortalecendo a postura de segurança em um ambiente digital.

3.1.2 Implementação e Técnicas Utilizadas

Desenvolver um chatbot de segurança da informação em Python envolve a integração de técnicas específicas para processar informações, entender consultas dos usuários e fornecer respostas relevantes. Abaixo estão alguns conceitos e técnicas específicas que foram implementadas:

Processamento de Linguagem Natural
Reconhecimento de Intenções (Intent Recognition)
Interatividade e Respostas Dinâmicas

Foi escolhido essa disciplina pois um chatbot de um banco dedicado a esclarecer dúvidas sobre segurança da informação desempenha um papel crucial na proteção tanto dos clientes quanto da instituição. Sua importância reside na capacidade de fornecer informações rápidas e precisas, promovendo a conscientização dos clientes sobre práticas seguras online. Isso não apenas fortalece a segurança das transações e dados pessoais, mas também constrói a confiança do cliente ao oferecer um recurso acessível e proativo para lidar com preocupações relacionadas à segurança cibernética. Além disso, o chatbot pode contribuir para a prevenção de fraudes, educando os usuários sobre ameaças potenciais e promovendo uma cultura de segurança digital no ambiente bancário.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é crucial para proteger informações sensíveis, garantir a integridade dos dados e prevenir acessos não autorizados. Ela visa minimizar riscos de ataques cibernéticos, garantindo a confidencialidade, disponibilidade e autenticidade dos dados. A falta de segurança pode resultar em perda de dados, danos à reputação, interrupção de serviços e impactos financeiros. Portanto, a implementação de medidas de segurança é essencial para manter a confiança dos usuários e a estabilidade das operações em ambientes computacionais.

3.2.1 Conceitos e Implementação de Segurança

Segurança lógica refere-se à proteção de dados e informações por meio de controles de acesso, criptografia e políticas de segurança digital. Envolve o uso de senhas, firewalls, antivírus e outras medidas para salvaguardar sistemas e dados contra ameaças cibernéticas.

Segurança física, por outro lado, concentra-se na proteção física dos recursos de computação, como servidores e equipamentos. Isso inclui medidas como controle de acesso físico, monitoramento por câmeras, e a implementação de ambientes controlados para prevenir roubos ou danos físicos aos dispositivos e infraestrutura. Ambas são partes essenciais da segurança global em sistemas computacionais.

Já o **conceito de informação** refere-se a dados processados e organizados de maneira significativa. A informação tem valor quando é relevante, precisa e utilizável, contribuindo para a tomada de decisões ou execução de tarefas. Seu valor está intrinsecamente ligado à sua capacidade de influenciar positivamente ações ou resultados, sendo um recurso valioso para indivíduos e organizações. A proteção adequada da informação é essencial para preservar sua integridade, confidencialidade e disponibilidade, garantindo seu valor e contribuindo para o sucesso de operações e estratégias.

Segurança Lógica:

- *Aplicação:* Implementação de firewalls, sistemas de detecção de intrusões, controle rigoroso de acessos a sistemas e dados confidenciais no ambiente virtual do banco.

Segurança Física:

- *Aplicação:* Controle de acesso físico aos data centers do banco, monitoramento por câmeras, sistemas de alarme e ambientes controlados para proteger servidores e equipamentos sensíveis.

Conceito e Valor da Informação:

- *Aplicação:* A informação no contexto bancário inclui dados de clientes, transações financeiras, e estratégias de negócios. Garantir a confidencialidade dessas informações é essencial para proteger clientes contra fraudes e manter a reputação do banco. O valor da informação reside na sua capacidade de apoiar a tomada de decisões, fornecer serviços confiáveis aos clientes e cumprir regulamentações financeiras. A integridade dos dados é crucial para evitar erros em transações, enquanto a disponibilidade garante que os serviços bancários estejam sempre acessíveis, contribuindo para a confiança e fidelidade dos clientes.

3.2.2 Detecção e Prevenção de Ataques

Medidas Proativas:

- *Identificação Antecipada:* Monitoramento contínuo de redes e sistemas para detectar atividades suspeitas antes que causem danos.
- *Treinamento e Conscientização:* Educação regular dos funcionários sobre práticas seguras para prevenir ataques de engenharia social e promover a cultura de segurança.
- *Atualizações Constantes:* Manutenção de sistemas e softwares atualizados para corrigir vulnerabilidades conhecidas.

Medidas Reativas:

- *Resposta a Incidentes:* Plano de ação para lidar com incidentes de segurança, incluindo investigação forense e recuperação de dados.
- *Backup e Recuperação:* Implementação de sistemas robustos de backup para restaurar dados em caso de perda ou corrupção.
- *Colaboração com Autoridades:* Cooperação com órgãos de segurança e reguladores para investigar e resolver incidentes mais graves.

4 CONCLUSÃO

Em conclusão, a implementação de um chatbot dedicado à segurança da informação desempenha um papel crucial na promoção e conscientização das práticas seguras, especialmente em setores sensíveis como o bancário. A capacidade de fornecer informações instantâneas sobre ameaças cibernéticas, dicas de segurança e esclarecimentos relacionados à proteção de dados contribui significativamente para a construção de uma cultura organizacional voltada à segurança. Além disso, em um ambiente bancário, onde a confiança e integridade dos dados são fundamentais, a segurança da informação emerge como uma pedra angular. A proteção proativa contra ameaças cibernéticas e a resposta eficiente a incidentes não apenas salvaguardam os ativos digitais do banco, mas também fortalecem a confiança dos clientes, mantendo a reputação da instituição financeira. Portanto, a interseção entre a tecnologia dos chatbots e a segurança da informação é não apenas relevante, mas essencial para garantir a robustez e confiabilidade das operações bancárias em um mundo cada vez mais digital e interconectado.

REFERÊNCIAS

1. Wikipédia

2. Livros da matéria