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

CHATBOT PARA SUPORTE EM SEGURANÇA DE TI

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

CHATBOT PARA SUPORTE EM SEGURANÇA DE TI

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:

Adryelle Pereira Felippe Araujo, Ra 1012023100409

SÃO JOÃO DA BOA VISTA, SP

OUTUBRO, 2023

SUMÁRIO

1 INTRODUÇÃO

Neste projeto foi desenvolvido um Chatbot que deverá auxiliar e esclarecer dúvidas dos colaboradores da empresa Cebrace em relação a segurança de informação, o Chatbot é integrado com inteligência artificial para a máquina conseguir responder as dúvidas mesmo que questionadas de formas diferentes, além disso também foi aplicado conceitos de segurança para que o Chatbot não coletasse informações sobre os trabalhadores.

Os Chatbots são robôs desenvolvidos para o conversas com pessoas (GOMES, 2017), para o atual projeto foi a ferramenta escolhida pela praticidade ao consumidor de apenas digitar a pergunta e já ter a resposta, sem precisar passar minutos em sites de pesquisa para encontrar o que precisa sobre segurança da informação. Quando a ferramenta é unida com inteligência artificial conseguem agradar mais ainda a quem esteja conversando. A inteligência artificial é um sistema desenvolvido para ser capaz de adquirir, representar e manipular conhecimento e dados, onde a manipulação se diz a respeito da dedução e compreensão de novos conhecimentos (SILVA, 2019).

Com todo esse poder de manipular dados e conhecimento, a segurança se torna essencial para proteger dados de pessoas e empresas. A segurança da informação é indispensável para uma empresa, pois ela vem para proteger os ativos de informação (qualquer objeto, físico ou digital, que possua informações da empresa) a fim de evitar roubos de dados e informações, sequestro de dados, vazamentos de informações confidenciais de clientes etc. (BARRETO, 2018).

2 DESCRIÇÃO DA EMPRESA

O projeto foi realizado para a empresa Cebrace, localizada em Jacareí.

Nome Empresarial: Cebrace Cristal Plano LTDA.
CNPJ: 45.070.190/0001-51.
Endereço: Av. do Cristal, 540, Jardim das Indústrias, Jacareí - São Paulo**.**
CEP: 12311-900.
Atividade Principal: 23.11-7-00 - Fabricação de vidro plano e de segurança.

A empresa possui como atividade principal a produção de vidros planos, produzindo vidros para fachadas, decorações, eletrodomésticos etc.

.

3 PROJETO DE CONSULTORIA EMPRESARIAL

A empresa Cebrace atua no ramo do vidro plano, fruto de uma joint-venture que está no Brasil desde 1977, onde sua missão é “serem reconhecidos como a empresa líder do mercado de Vidro Plano, que oferece produtos, serviços e soluções inovadoras”. Os valores da empresa se baseiam em excelência operacional e tecnológica, com foco no cliente, zelando pela segurança e condições de trabalho para os colaboradores (Site da Cebrace).

Foi necessário a busca por uma ferramenta para conscientizar seus colaboradores que em sua maioria não pertencem a área de TI e não conhecem, ou sabem pouco, sobre segurança de informação, algo que a empresa vem valorizando cada dia mais por prezar o sigilo cliente-empresa.

3.1 INTELIGÊNCIA ARTIFICIAL

A inteligência artificial (IA) é um ramo da engenharia da computação que visa solucionar problemas complexos ao simular uma forma humana de aprendizado e raciocínio (SILVA, 2019). Seu sucesso é gigante nos dias de hoje, no dia-a-dia é utilizada em nossos sistema de busca e recomendação de produtos que aprendem com nossos hábitos, os sistemas financeiros utilizam de sistemas que são capazes de aprender e decidir com base no mercado, graças à inteligência artificial e seu grande avanço (SICHMAN, 2021).

No Chatbot desenvolvido no projeto a inteligência artificial é o coração para seu bom funcionamento, pois suas respostas são geradas devido ao aprendizado da máquina em cima de uma base, além da adaptação da mesma, lembrando que uma boa IA deve ser capaz de manipular dados (SILVA, 2019).

3.1.1 Introdução à Aplicação da IA

Uma das aplicações mais famosas e que se relaciona totalmente com o projeto é o ChatGPT, um Chatbot aliado à inteligência artificial criado pela OpanAI lançado em 2022, ele foi treinado com base em Aprendizagem por reforço com feedback humano - RLHF (Site OpenAI).

Nos dias atuais o ChatGPT se tornou um aliado para muitas pessoas, por ser um Chatbot que consegue pesquisar e modelar uma respostas em segundos baseado em fontes encontradas na internet. Desenvolvedores utilizam-o para ajudar a corrigir bugs, corrigir sintaxe de linguagens de programação; o sistema baseado em IA é capaz de resolver problemas matemáticos, bem como sugerir ideias para projetos ou redigir um email. Um exemplo de seu uso é o Tribunal de Justiça de Minas Gerais que utiliza um sistema baseado no ChatGPT para geração de textos para e-mails, portarias etc (CASSOL, 2023).

Vale ressaltar que, por mais que haja inúmeros benefícios para utilização de sistemas baseados em IA, é necessário redobrar a atenção em questões éticas, tais discussões aconteceram e acontecem acerca de privacidade, justiça e segurança, também é muito discutido o impacto desse tipo de sistema nos trabalhos atuais (SICHMAN, 2021).

3.1.2 Implementação e Técnicas Utilizadas

Ao decorrer dos anos e da evolução dos estudos sobre inteligência artificial, *machine learning* e *deep learning*, foram sendo criadas técnicas para desenvolvimento de tais algoritmos. Acerca disso, pode-se citar a criação dos Perceptrons na década de 1950 por Frank Rosenblatt, que são modelos de neurônios artificiais no qual possuem uma camada que recebem entradas, atribuem pesos a elas, realiza a soma das entradas ponderadas pelos seus pesos e resulta em uma única saída (SILVA, 2019).

Os perceptrons trabalham com camadas únicas, não possibilitando a resolução de tarefas não lineares, e por conta disso temos as redes multicamadas. São redes neurais compostas por uma cama de entrada, uma ou mais camada ocultas e uma camada de saída sendo capaz de receber múltiplas entradas e gerar múltiplas saídas, é muito utilizada em *deep learning* por conseguirem resolver problemas não lineares (SOUSA, 2020) e o seu aprendizado é supervisionado, um tipo de aprendizado no qual necessita de um “professor” que instrui a rede neural qual seria o tipo de resposta a uma determinada entrada, utiliza então o algoritmo *backpropagation*, que é baseado no aprendizado por correção de erros (FARIA, 2018). Uma ferramenta bastante utilizada para processos de aprendizado da máquina (ou *machine learning* - ML) é a linguagem e programação Python, por maior versatilidade para trabalhar com a linguagem além das bibliotecas que facilitam o trabalho (SOUSA, 2020).

Outro tipo importante para se comentar, são as redes neurais convolucionais, também conhecidas como CNNs. Esse tipo de rede neural possui camadas convolucionais que identificam padrões e hierarquias nas entradas, cada camada utiliza filtro de aprendizado que responde a um subconjunto da entrada, e pelo menos uma das camadas realizam convolução (que são um tipo de operação linear). As CNNs foram projetadas principalmente para tarefas de visão computacional, contudo são aplicadas em outras áreas (FARIA, 2018). A Google possui uma ferramenta que utiliza desse modelo de rede neural para treinar modelos para reconhecimento de padrões em imagens, conhecido como *Teachable Machine* foi lançado em 2017 e possibilita que pessoas treinem modelos sem conhecimentos avançados em programação (Site Oficial do Teachable Machine).

Mais especificamente nesse projeto foi utilizado o NPL - Processamento de Linguagem Natural, no qual permite que os computadores possam analisar e manipular a linguagem falada e escrita. Ela se torna importante para o nosso Chatbot por conta de possibilitar que o Bot responda na linguagem natural a partir de *machine learning* e linguística (BENIN, 2023). Com isso torna o processo de interação entre Bot e o colaborador mais humanizado, onde o colaborador pode escrever sua dúvida como se estivesse perguntando a um colega que o Bot irá compreender e conseguir responder, tornando o *user experience* (UX) mais agradável e aumentando a aderência dos funcionários ao uso do Chatbot.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança da informação é uma área que tem como fundamento a proteção, confidencialidade (os dados são protegidos contra acessos não autorizados), disponibilidade (a informação estará disponível para quem precisar) e integridade (os dados não serão editados indevidamente) dos dados, seu foco é em proteger os ativos da empresa, que são tudo aquilo que possui valor na empresa. Visando sempre a proteção de empresas contra acessos não autorizados, modificações indesejadas, interrupções de serviço, invasões etc (BARRETO, 2018).

A maior dificuldade em implementar a segurança na empresa é a conscientização e conhecimento dos colaboradores acerca do assunto, por esse motivo o projeto possui foco na construção de um Chatbot para sanar dúvidas dos mesmos e auxiliar na identificação de ataques.

3.2.1 Conceitos e Implementação de Segurança

Muito se fala sobre proteger os dados e informações, mas, afinal, por que? Primeiramente há uma separação do que são dados e informações: dados são fatos de forma bruta, enquanto as informações possuem tratamento e organização lógica desses fatos. Dentro de uma organização, as informações dizem sobre suas regras de negócios, segredos de desenvolvimento, informações de clientes e fornecedores entre outros, e é de suma importância que esse tipo de conhecimento não saia de sua bolha empresarial, podendo chegar em rivais ou até comprometer seus clientes (BARRETO, 2018).

Por esse motivo é recomendado a segurança lógica e física dos dados, onde a segurança lógica se diz a respeito da proteção dos sistemas utilizados pela empresa, por softwares e/ou controle rígido de acesso (LEITE, 2018). Enquanto a segurança física se trata do todo hardware, como os computadores fornecidos pela empresa até as salas onde se encontram os servidores, há inúmeras formas de proteção física tal como a proteção da localização e detecção de intrusão, sempre é visado manter um bom controle de acessos para evitar esses tipos de situações (GOODRICH, 2013).

Na Cebrace já é aplicado um controle rígido de segurança física, todo controle de acesso a salas é feito por cartões com tarjas magnéticas e algumas, que são consideradas mais sensíveis, são utilizadas fechaduras de pinos. Nos sistemas possui também um controle rígido de acesso, monitorando e sempre tomando com cuidado os acessos e permissões que cada usuário pode ter. Um dos pontos do Chatbot desenvolvido para a empresa, foi implementado uma tratativa em que o Bot não armazena nenhuma informação sensível dos colaboradores ou qualquer informação que possa ser vista com ativo da empresa.

3.2.2 Detecção e Prevenção de Ataques

Foi implementada um sistema de intrusão por anomalia, no qual é detectado um problema quando algo fora do perfil do usuário é feito, que performa de forma passiva, onde é gerado um log com as informações da anomalia e o administrador do sistema gera um relatório e discute com a equipe as atitudes a serem implementadas (GOODRICH, 2013).

A empresa utiliza o Nessus, uma ferramenta que torna a análise de vulnerabilidade mais simples e intuitiva, para verificação diária de vulnerabilidades na rede, onde o *pentester*

analisa e verifica os relatórios para ser possível aplicarem as medidas de correção de tais vulnerabilidades. Também faz uso de *Kali Linux*, uma distribuição do Linux, muito utilizado por auditores por oferecer amplas ferramentas para testes de invasão e auditorias de segurança (GOODRICH, 2013).

As leis LGPD são muito visadas pela a empresa e, por conta disso, é utilizado a ferramenta *OneTrust*, que auxilia no gerenciamento de todo o ciclo de vida do processamento de dados pessoais, desde a coleta até o encerramento e a exclusão de informações.

Com foco no projeto, foi identificado como um fator de risco a engenharia social, nesses casos os ataques exploram a ingenuidade do usuário a fim de obter informações privilegiadas (GOODRICH, 2013). Para combater foi recomendado a implementação e uso do Chatbot para conscientizar os colaboradores que não possuem grandes conhecimentos e os ajudar a entender o que são e reconhecer os ataques.

4 CONCLUSÃO

Em suma, o estudo mostrou que a maior vulnerabilidade encontrada na empresa de interesse era a ingenuidade dos colaboradores fora da área de TI sobre normas e procedimentos de segurança, além dos tipos de ataques comuns (como *phishing* por e-mail).

A implantação do Chatbot foi bem vista e apoiada pelo fato de se comunicar com linguagem natural, graças ao NPL, e também pelo uso corriqueiro dos funcionários com esse tipo de sistema. A maior dificuldade na implantação de projetos como esse é a aderência das áreas, mas uma vez obtendo o apoio da alta liderança isso se tornou um processo mais facilitado.

O treinamento e sanar dúvidas dos funcionários acerca de segurança traz inúmeros benefícios a empresa, pois uma empresa segura é bem vista aos olhos de clientes e investidores.

REFERÊNCIAS

BARRETO, Jeanine dos Santos. **Fundamentos de segurança da informação**. Porto Alegre: SAGAH, 2018.

BENIN, Keli Rodrigues Do Amaral. Processamento de Linguagem Natural e a Ciência da Informação: Inter-Relações e Contribuições. Londrina: **Universidade Estadual de Londrina**, 2023. Disponível em: processamentolinguagemnaturalcienciainformacao.pdf (utfpr.edu.br). Acesso em: 17 nov. 2023.

CASSOL, Daniel. Quais os impactos do ChatGPT e da Inteligência Artificial na Educação?. Santa Catarina: **IFSC**, 2023. Disponível em: Quais os impactos do ChatGPT e da Inteligência Artificial na Educação? - IFSC Verifica - Portal do IFSC. Acesso em: 16 nov. 2023.

FARIA, Elisangela Lopes de. Redes neurais convolucionais e máquinas de aprendizado extremo aplicadas ao mercado financeiro brasileiro. Rio de Janeiro: **Universidade Federal do Rio de Janeiro**, 2018. Disponível em: Pantheon: Redes neurais convolucionais e máquinas de aprendizado extremo aplicadas ao mercado financeiro brasileiro (ufrj.br). Acesso em: 17 nov. 2023.

GOMES, Caroline. Chatbot: entenda tudo sobre o assunto. São Paulo: **Simply**, 2017. Disponível em: http://blog.simply.com.br/chatbot/. Acesso em: 15 nov. 2023

.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à segurança de computadores**. Porto Alegre: Bookman, 2013.

LEITE, Luciano Monteiro. Políticas de Segurança Física e Lógica de Tecnologia da Informação em Redes de Computadores e seus Ativos. Curitiba: **Universidade Tecnológica Federal do Paraná**, 2018. Disponível em: CT_GESER_X_2018_04.pdf (utfpr.edu.br). Acesso em: 15 nov. 2023.

SILVA, Fabrício Machado da. **Inteligência artificial**. Porto Alegre: SAGAH, 2019.

Site da Cebrace:Cebrace - Sobre nós.

Site da OpenAI: https://chat.openai.com/.

Site da Teachable Machine: Teachable Machine.

SOUSA, J. R. de; ANTUNES, J. F.; OLIVEIRA, Ícaro A. de; *et al*. Python e predição de dados usando redes neurais multicamadas. Curitiba: **Brazilian Journal of Development**, 2020. Disponível em: Python e predição de dados usando redes neurais multicamadas/Python and data prediction using multi-layered neural networks | Brazilian Journal of Development (brazilianjournals.com.br). Acesso em: 17 nov. 2023.

SICHMAN, J. S. Inteligência Artificial e sociedade: avanços e riscos. São Paulo: **USP**, 2021 Disponível em: SciELO - Brasil - Inteligência Artificial e sociedade: avanços e riscos Inteligência Artificial e sociedade: avanços e riscos. Acesso em: 15 nov. 2023.