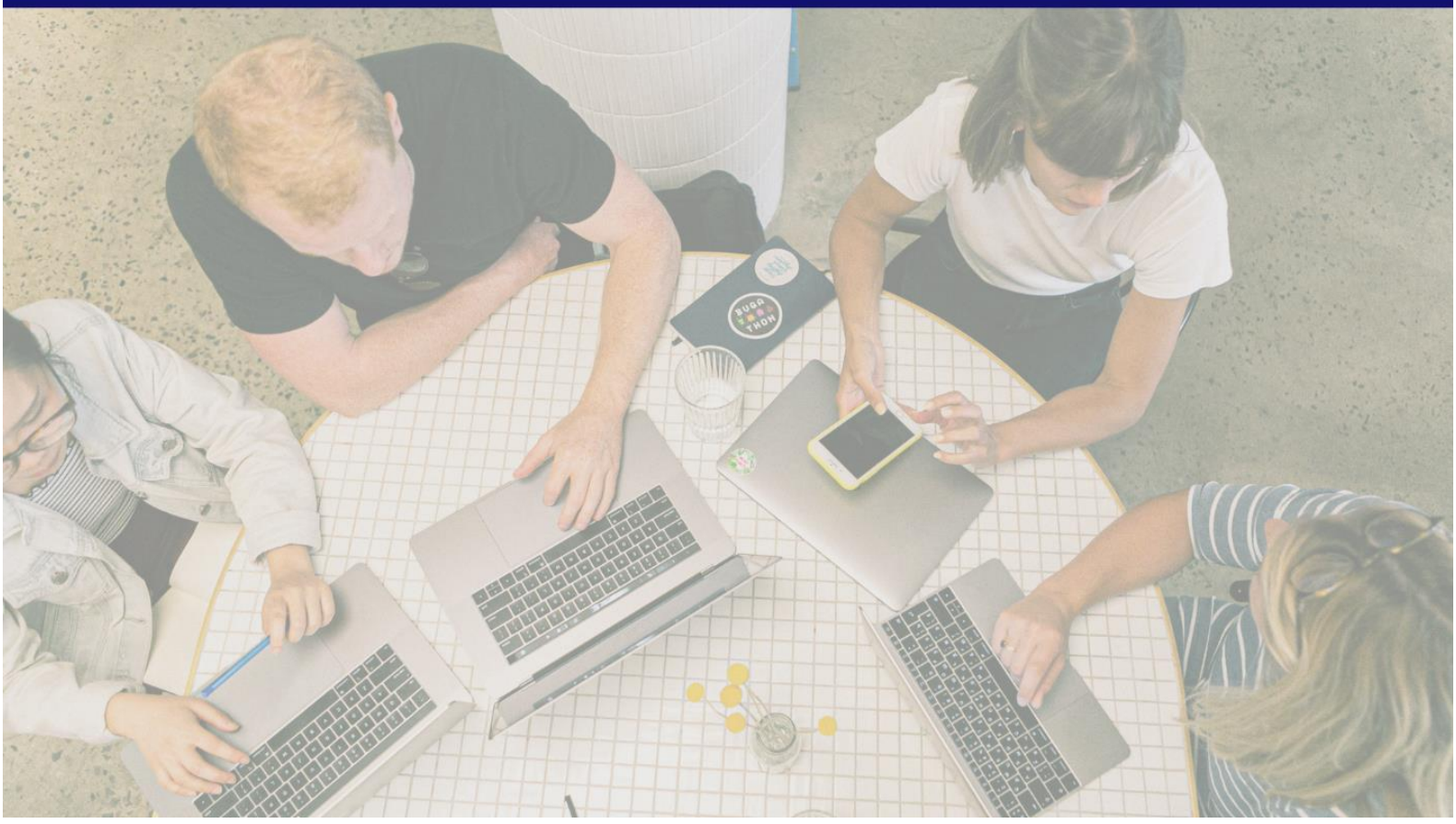
UNIFEOB
ESCOLA DE NEGÓCIOS

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 SEGURO 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 SEGURO 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:

Núbia Ferreira de Oliveira A, RA 1012022201260
Bruno Gabriel Silva, RA 1012022100896
Helena Cavalcante, RA 1012022100462
Donizeti Santana Ferreira, RA 1012023200012
Lariane Custódio de Siqueira, RA 1012022100931

SÃO JOÃO DA BOA VISTA, SP
OUTUBRO, 2023

SUMÁRIO

Sumário

INTRODUÇÃO

Na era digital em constante evolução, a Tecnologia da Informação (TI) desempenha um papel vital na sustentação e progresso das organizações. No entanto, com a expansão das fronteiras digitais, surgem desafios inerentes à segurança da informação. Nesse cenário desafiador, a implementação de soluções inovadoras torna-se imperativa. Este trabalho propõe uma investigação aprofundada sobre a integração de chatbots seguros como uma ferramenta eficaz para oferecer suporte especializado em Segurança de TI.

Os chatbots, sistemas de conversação automatizados alimentados por inteligência artificial, emergiram como uma solução proeminente para aprimorar a eficiência operacional e proporcionar respostas rápidas. No entanto, a segurança da informação é uma preocupação crítica ao incorporar essa tecnologia, especialmente em um domínio tão sensível quanto o de Tecnologia da Informação.

Este estudo concentra-se na exploração das práticas e protocolos que garantem a segurança dos chatbots utilizados para suporte em Segurança de TI. Ao compreender os desafios específicos enfrentados nesse contexto e ao desenvolver estratégias robustas para mitigar riscos, pretendemos apresentar um guia abrangente para a implementação bem-sucedida de chatbots seguros no cenário de Segurança de TI.

A segurança cibernética é um campo dinâmico que exige soluções igualmente dinâmicas. Este trabalho busca contribuir para a evolução da resposta da TI aos desafios de segurança, oferecendo uma visão detalhada sobre a integração de chatbots seguros como aliados valiosos na defesa contra ameaças digitais. Estamos prestes a mergulhar em uma jornada que une a eficácia da automação de suporte com a necessidade premente de salvaguardar dados e sistemas críticos.

2. INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) emerge como uma força transformadora na era da informação, impulsionando inovações e redefinindo paradigmas em diversas indústrias. Em sua essência, a IA refere-se à capacidade de máquinas executarem tarefas que normalmente exigiriam inteligência humana, como aprendizado, raciocínio e resolução de problemas.

Num cenário onde a complexidade dos desafios de Segurança de TI atinge novas alturas, a aplicação da IA torna-se não apenas benéfica, mas imperativa. A capacidade de análise preditiva, automação inteligente e aprendizado de máquina possibilita não apenas a identificação, mas também a prevenção proativa de ameaças cibernéticas. A IA, assim, transcende os limites da capacidade humana, agindo em tempo real para proteger ativos críticos.

A relevância da Inteligência Artificial na atualidade é inegável. Seja na otimização de processos, na personalização de experiências do usuário ou na tomada de decisões baseadas em dados, a IA permeia nosso cotidiano de maneira discreta, porém poderosa. No contexto específico de projetos de Segurança de TI, sua aplicação promete revolucionar a abordagem tradicional, proporcionando uma defesa mais eficaz e dinâmica contra ameaças digitais em constante evolução.

A integração da Inteligência Artificial neste projeto não é apenas uma escolha estratégica, mas uma necessidade estrutural. Ao capacitar sistemas com a capacidade de aprender com padrões históricos, antecipar comportamentos suspeitos e adaptar-se a cenários em tempo real, a IA eleva a eficiência operacional e fortalece as defesas contra adversários cibernéticos.

Em suma, a Inteligência Artificial é a espinha dorsal tecnológica que sustenta a visão inovadora deste projeto. Sua compreensão e aplicação cuidadosa não apenas reforçam a defesa contra ameaças digitais, mas também posicionam o projeto no epicentro da vanguarda tecnológica, onde a evolução é constante e a segurança é prioritária.

2.1. Introdução à Aplicação da IA

Na imersão no universo da Inteligência Artificial (IA) e sua integração no contexto do projeto de Segurança de TI, é crucial compreender como essa tecnologia se manifesta de maneira prática e efetiva. Uma aplicação específica que merece destaque é a utilização de chatbots inteligentes impulsionados por IA no âmbito da cibersegurança.

No mundo real, empresas líderes em segurança cibernética têm adotado chatbots impulsionados por IA para reforçar suas defesas contra ameaças digitais. Esses chatbots não são apenas interfaces de comunicação automatizadas; eles são agentes ativos que desempenham um papel crucial na detecção proativa de anomalias e na resposta rápida a incidentes.

Contextualização: Imagine uma organização que maneja grandes volumes de tráfego de dados diariamente. Um chatbot inteligente, integrado ao sistema de monitoramento de segurança, analisa padrões de comportamento de usuários, acessos a sistemas e atividades de rede em tempo real. Baseando-se em algoritmos de aprendizado de máquina, o chatbot é treinado para identificar comportamentos suspeitos, correlacionar eventos aparentemente isolados e discernir atividades potencialmente maliciosas.

Experiência no Mundo Real: Empresas financeiras, por exemplo, têm adotado essa abordagem para fortalecer suas defesas contra ataques cibernéticos. O chatbot, com sua capacidade de aprendizado contínuo, consegue detectar padrões incomuns que escapariam facilmente à percepção humana, alertando a equipe de segurança para investigação imediata.

Benefícios Observados: A implementação bem-sucedida dessa aplicação de IA resulta em uma resposta mais rápida a incidentes, minimizando potenciais danos. Além disso, a capacidade de adaptação contínua do chatbot significa que ele evolui à medida que novas ameaças surgem, mantendo as defesas sempre à frente do cenário de segurança em constante mutação.

Ao contextualizar a IA através deste exemplo prático, podemos visualizar como a integração de chatbots inteligentes se alinha não apenas com a eficiência operacional, mas também com a missão crítica de fortalecer as defesas em Segurança de TI, demonstrando a aplicabilidade tangível desta tecnologia na resolução de desafios complexos do mundo real.

2.2 Implementação e Técnicas Utilizadas

A infraestrutura foi estabelecida utilizando Python e Anaconda para configurar um servidor virtual e instalar as dependências necessárias. O front-end foi construído com React e AJAX, enquanto o back-end foi potencializado pelo RASA, responsável pela IA. A inteligência artificial foi treinada em tópicos de segurança cibernética, permitindo que ela aprendesse e armazenasse conhecimentos em seu banco de dados.

O processo foi submetido a testes rigorosos com a ferramenta POSTMAN, e um roteiro detalhado da atividade foi criado utilizando Javascript. A relevância do respeito às normas de

privacidade, conforme a Lei Geral de Proteção de Dados Brasileira, foi evidenciada, exigindo a implementação de mecanismos para excluir dados temporários a cada interação com a IA.

No segundo estágio do projeto, o controle e a segurança foram aprimorados com a utilização do Git e GitHub para persistência de dados e gerenciamento de versões. Adicionalmente, a implementação de metodologias ágeis, com sprints delegadas e monitoradas através do Notion, trouxe eficiência ao processo.

2.3 Segurança em sistemas computacionais

A segurança em sistemas computacionais emerge como um pilar fundamental no cenário empresarial moderno, onde a crescente dependência da tecnologia digital expõe organizações a uma miríade de ameaças cibernéticas. A relevância intrínseca da segurança nesse contexto é incontestável, pois influencia diretamente a integridade, confidencialidade e disponibilidade dos dados e sistemas, elementos cruciais para as operações cotidianas e a tomada de decisões estratégicas.

A rápida evolução das ameaças cibernéticas destaca a necessidade premente de estratégias de segurança robustas. A complexidade crescente dessas ameaças, que vão desde ataques de ransomware até violações de dados, exige a implementação de medidas eficazes para proteger os ativos digitais das organizações. A integridade dos dados, a confidencialidade das informações sensíveis e a continuidade dos serviços tornam-se prioridades incontestáveis, delineando a importância estratégica da segurança em sistemas computacionais.

A implementação prática dos conceitos teóricos adquire um papel crucial nesse contexto. A aplicação de firewalls, criptografia, políticas de acesso e outras medidas de segurança não apenas resguarda os sistemas contra ameaças externas, mas também assegura que a confidencialidade das informações seja mantida. A materialização desses conceitos na prática não só fortalece a resistência dos sistemas, mas também estabelece um ambiente confiável para a condução dos negócios.

Contudo, a busca pela segurança em sistemas computacionais não está isenta de desafios. A resistência organizacional à implementação de medidas de segurança, a necessidade de adaptação constante às evoluções tecnológicas e a gestão eficiente de recursos constituem obstáculos a serem superados. A discussão sobre a necessidade de equilibrar a eficácia da segurança com a usabilidade e acessibilidade, levando em conta as demandas operacionais da empresa, ressalta a complexidade inerente a esse desafio.

Em resumo, a importância da segurança em sistemas computacionais transcende a mera proteção de dados; é um componente essencial para a sustentabilidade e competitividade das

organizações na era digital. A integração de estratégias de segurança não apenas mitiga riscos, mas também promove um ambiente confiável e resiliente, permitindo que as empresas avancem com segurança em um cenário tecnológico em constante transformação.

3.1. Conceitos e Implementação de Segurança

Confidencialidade: A confidencialidade refere-se à garantia de que as informações estão acessíveis apenas a usuários autorizados. Criptografia, controle de acesso e políticas de privacidade são elementos cruciais para manter a confidencialidade dos dados.

Integridade: A integridade dos dados assegura que as informações não foram alteradas de maneira não autorizada. Mecanismos como assinaturas digitais e checksums são utilizados para verificar e garantir a integridade dos dados.

Disponibilidade: A disponibilidade diz respeito à garantia de que os recursos e informações estão disponíveis quando necessários. Estratégias de backup, redundância e planos de continuidade de negócios são essenciais para garantir a disponibilidade dos sistemas.

Autenticidade: A autenticidade verifica a identidade dos usuários e sistemas, garantindo que apenas usuários autorizados tenham acesso às informações. Senhas, autenticação de dois fatores e certificados digitais são meios comuns de garantir a autenticidade.

Firewalls e Antivírus: A implementação de firewalls ajuda a proteger redes contra acessos não autorizados, enquanto softwares antivírus identificam e removem ameaças de malware, garantindo a segurança dos sistemas.

Políticas de Segurança: Estabelecer políticas de segurança claras é fundamental. Isso inclui diretrizes para senhas, restrições de acesso e práticas recomendadas para garantir que os usuários ajam de maneira segura.

Atualizações de Software: Manter sistemas e softwares atualizados é crucial para corrigir vulnerabilidades conhecidas. Atualizações regulares ajudam a proteger contra ameaças que exploram falhas de segurança.

Treinamento de Usuários: A segurança da informação também depende da conscientização dos usuários. Treinamentos regulares sobre práticas seguras, reconhecimento de phishing e cuidados básicos ajudam a fortalecer a linha de defesa humana.

3.2. Detecção e Prevenção de Ataques

Com o crescimento exponencial das ameaças cibernéticas, a detecção e prevenção de ataques tornaram-se áreas cruciais na segurança da informação. Este trabalho explora as estratégias fundamentais para identificar e mitigar ameaças, salvaguardando organizações contra potenciais danos decorrentes de atividades maliciosas.

Monitoramento de Logs: A análise sistemática de logs permite identificar padrões incomuns ou atividades suspeitas nos sistemas. Ferramentas de análise de logs automatizadas desempenham um papel vital na detecção precoce de possíveis ataques.

Sistemas de Detecção de Intrusão (IDS): IDS monitoram o tráfego de rede em busca de comportamentos anômalos. Sistemas de detecção de intrusão podem ser baseados em assinaturas (identificando padrões conhecidos de ataques) ou em comportamentos (analisando desvios do padrão normal).

Análise de Tráfego: A análise profunda do tráfego de rede e padrões de comunicação pode revelar atividades suspeitas. Ferramentas de análise de tráfego ajudam na identificação de anomalias que podem indicar ataques em andamento.

Prevenção de Ataques:

Firewalls e Gateways de Segurança: Firewalls atuam como barreiras protetoras, controlando o tráfego de rede com base em regras predefinidas. Gateways de segurança aprimorados incorporam funcionalidades de prevenção de ameaças, bloqueando ataques conhecidos.

Sistemas de Prevenção de Intrusão (IPS): IPS complementam os IDS, não apenas identificando ameaças, mas também agindo proativamente para bloquear ou mitigar ataques em tempo real. Isso inclui a aplicação de políticas de segurança automaticamente.

Atualizações Regulares e Patch Management: Manter sistemas e softwares atualizados é fundamental para corrigir vulnerabilidades conhecidas. A implementação eficaz de um programa de gerenciamento de patches ajuda a fechar brechas de segurança que podem ser exploradas por atacantes.

Integração de Detecção e Prevenção: A eficácia na segurança cibernética muitas vezes reside na integração harmoniosa de sistemas de detecção e prevenção. A automação desempenha um papel vital, permitindo respostas rápidas a ameaças. Além disso, a colaboração entre diferentes ferramentas e a análise de dados de segurança em tempo real são cruciais para uma defesa eficaz.

CONCLUSÃO

Este trabalho proporcionou uma visão abrangente sobre a interseção crítica entre Tecnologia da Informação (TI) e decisões estratégicas empresariais. Ao resumir as principais descobertas e propostas, observamos que a integração eficiente de soluções tecnológicas não apenas otimiza os processos internos, mas também desempenha um papel crucial na formulação e execução de estratégias organizacionais. A discussão sobre a importância de tomar decisões informadas em TI revela a necessidade premente de uma abordagem holística, considerando tanto os aspectos técnicos quanto os administrativos.

A tomada de decisões estratégicas informadas não apenas aprimora a eficiência operacional, mas também fortalece a resiliência organizacional diante dos desafios em constante evolução. As contribuições destacadas por meio deste projeto não apenas refletem o êxito na implementação de soluções tecnológicas, mas também apontam para um impacto significativo nas operações e objetivos futuros da empresa selecionada.

A sinergia entre a TI e os objetivos estratégicos abre novas perspectivas para a empresa, fornecendo ferramentas e insights valiosos que podem catalisar o crescimento e a inovação contínua. Em suma, este projeto não é apenas um exercício técnico, mas sim uma demonstração tangível de como a Tecnologia da Informação pode ser alinhada estrategicamente para impulsionar o sucesso empresarial. Ao integrar decisões informadas em TI, nossa contribuição busca ser um catalisador positivo para a empresa, fortalecendo sua posição competitiva e preparando-a para um futuro dinâmico e desafiador.

Concluímos que ao trabalhar com IA é imprescindível que haja todo um preparo anterior do ambiente, instalando dependências, criando o banco, controle de dados, requisições e etc. É necessário salientar conjuntamente que devemos respeitar as regras de privacidade do usuário na lei geral da proteção de dados Brasileira, onde foi necessário criar formar de excluir dados temporário a cada interação que a IA obteve conosco, por fim, cumpre dizer que o trabalho foi satisfatório e conseguimos extrair conhecimentos necessário para nossa jornada ChatGPT Conclusão:

Ao concluir esta etapa do projeto, fica evidente que trabalhar com Inteligência Artificial (IA) exige uma preparação meticulosa do ambiente, abrangendo desde a instalação de dependências até a criação do banco de dados e o controle preciso dos dados. A complexidade intrínseca à integração de IA destaca a importância de um planejamento cuidadoso para assegurar a eficácia e segurança do sistema. A observância rigorosa das regras de privacidade

do usuário, conforme estabelecidas pela Lei Geral de Proteção de Dados Brasileira, emergiu como um princípio fundamental.

A necessidade de criar mecanismos para excluir dados temporários após cada interação com a IA reflete não apenas a conformidade legal, mas também um compromisso ético com a privacidade e segurança dos usuários. Concluindo, é gratificante afirmar que o trabalho foi satisfatório. Além do desenvolvimento técnico, a experiência proporcionou valiosos aprendizados, essenciais para nossa jornada no campo da Inteligência Artificial. O entendimento aprofundado dos desafios práticos, aliado ao compromisso ético, prepara-nos não apenas como profissionais proficientes, mas como agentes responsáveis na vanguarda da inovação tecnológica.

REFERÊNCIAS

STALLINGS, William. Criptografia e Segurança de Redes: Princípios e Práticas. 4. ed. São Paulo: Pearson, 2007. 432 p.

SCHNEIER, Bruce. Segredos e Mentiras: A Arte de Desmascarar Fraudes. São Paulo: Campus, 2001. 448 p.

ANDERSON, Ross. Segurança em Computadores e na Internet. In: **MENEZES, Nilo; FONTES, Edson.** Informática: Novas Aplicações com Microcomputadores. 3. ed. Rio de Janeiro: LTC, 2005. p. 165-196.