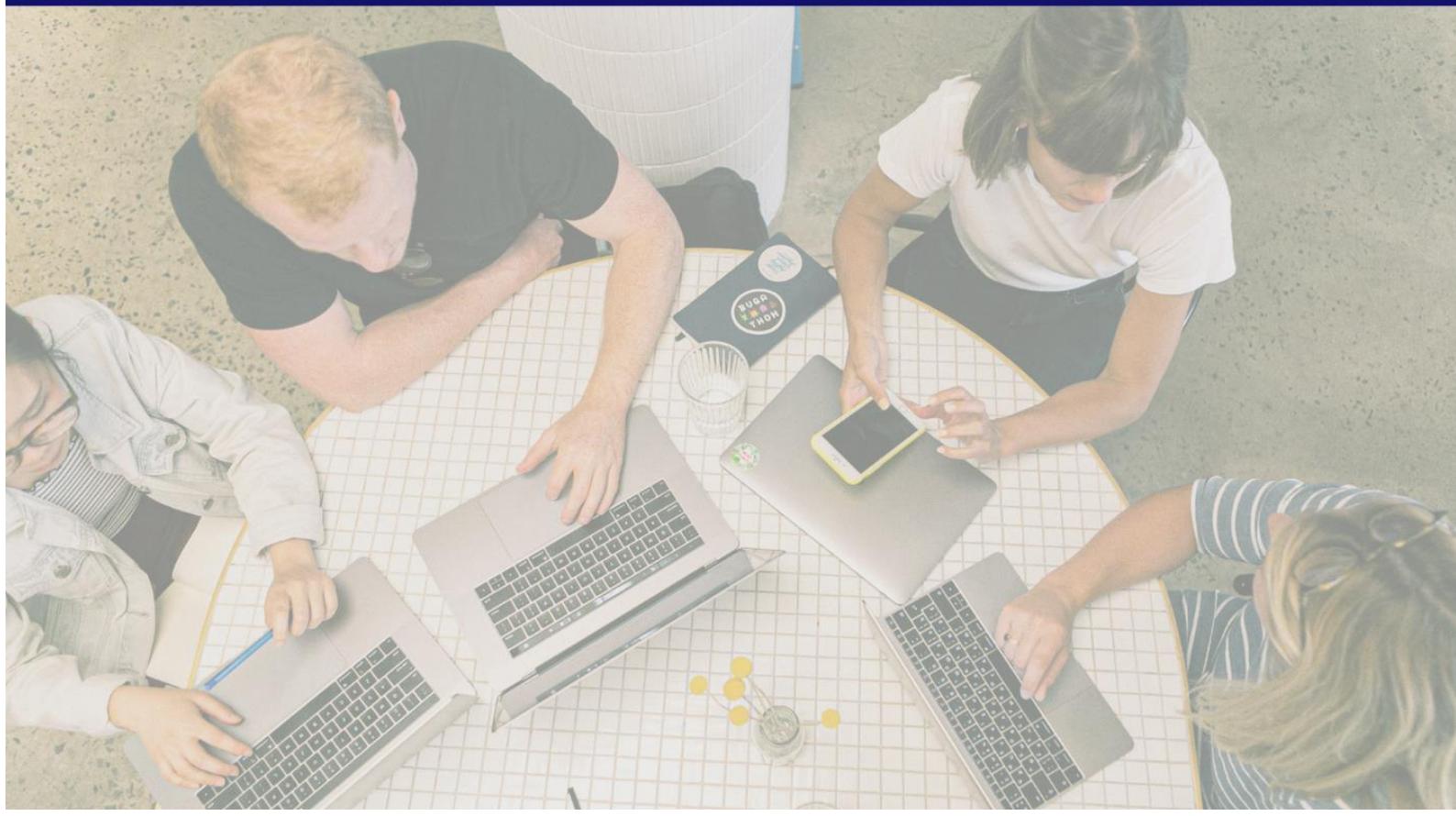


UNifeob
| ESCOLA DE NEGÓCIOS



2023

**PROJETO DE CONSULTORIA
EMPRESARIAL**



UNIFEOB
CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO
OCTÁVIO BASTOS
ESCOLA DE NEGÓCIOS
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

AL&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§ech

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira

Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudante:

Cléia Gomes Camargos , RA 1012022200759

SÃO JOÃO DA BOA VISTA, SP
OUTUBRO, 2023

SUMÁRIO

1 INTRODUÇÃO

2 DESCRIÇÃO DA EMPRESA

3 PROJETO DE CONSULTORIA EMPRESARIAL

3.1 INTELIGÊNCIA ARTIFICIAL

3.1.1 Aplicação Prática da Inteligência Artificial

3.1.2 Implementação e Técnicas Utilizadas

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

3.2.1 Conceitos e Implementação de Segurança

3.2.2 Detecção e Prevenção de Ataques

4 CONCLUSÃO

REFERÊNCIAS

ANEXOS

1 INTRODUÇÃO

"AI&SecTech", Proposta: Desenvolvimento de Soluções de IA com Protocolos de Segurança Robustos para Otimização e Proteção de Dados

Introdução:

Com a crescente demanda por automação de processos nas organizações, é fundamental garantir a segurança dos dados e da infraestrutura. Nessa proposta, apresentamos uma abordagem que combina técnicas avançadas de Inteligência Artificial (IA) com protocolos de segurança robustos, visando a otimização dos processos e a proteção dos dados e da infraestrutura contra possíveis ameaças cibernéticas.

Objetivo:

O objetivo principal dessa proposta é desenvolver e implementar soluções de IA seguras, confiáveis e em conformidade com os padrões de segurança atuais. Para alcançar esse objetivo, é necessário proteger os sistemas de IA contra potenciais vulnerabilidades e garantir a segurança e a ética no processamento dos dados.

Metodologia:

1. Análise dos requisitos da organização: Realizar uma análise detalhada das necessidades da organização em relação à automação de processos. Compreender os requisitos de segurança e privacidade dos dados.

2. Identificação de ameaças: Realizar uma avaliação de riscos e identificar possíveis ameaças aos sistemas de IA que podem comprometer a segurança dos dados. Avaliar as vulnerabilidades existentes.

3. Desenvolvimento de protocolos de segurança robustos: Implementar protocolos de segurança robustos, como autenticação de usuários, criptografia de dados e detecção de anomalias, para proteger os sistemas de IA contra ameaças internas e externas.

4. Implementação de técnicas avançadas de IA: Utilizar técnicas avançadas de IA, como machine learning e deep learning, para desenvolver soluções que atendam aos requisitos de automação da organização.

5. Testes e validação: Realizar testes rigorosos para garantir o bom funcionamento das soluções de IA, bem como a segurança e confiabilidade dos sistemas implementados.

6. Treinamento e conscientização: Treinar os colaboradores da organização sobre as boas práticas de segurança de IA, incluindo a ética no processamento de dados e a identificação de possíveis ameaças.

Resultados esperados:

Automação eficiente dos processos organizacionais por meio das soluções de IA implementadas.

Proteção eficaz dos dados e da infraestrutura contra possíveis ameaças cibernéticas.

Conformidade com os padrões de segurança atuais e éticos no processamento de dados.

Maior confiabilidade e segurança dos sistemas de IA.

Conclusão:

A combinação de técnicas avançadas de IA com protocolos de segurança robustos é fundamental para garantir a otimização dos processos organizacionais e a proteção dos dados e da infraestrutura contra ameaças. Essa proposta visa desenvolver e implementar soluções de IA seguras, confiáveis e em conformidade com os padrões de segurança atuais, proporcionando benefícios e segurança para as organizações.

2 DESCRIÇÃO DA EMPRESA

. Informações básicas da empresa "TIVIT terceirização de processos, serviços e tecnologia S.A":

- Razão social: TIVIT terceirização de processos , serviços e tecnologia S.A.

- CNPJ: 07.073.027/0001-53

- Endereço: Rua Bento branco de Andrade filho , 621, Cidade São Paulo , Estado de SP

- Atividade: A companhia oferece serviços diversos como desenvolvimento de software ágil, nuvem híbrida e publica, cibersegurança, operações de alta complexidade entre outros que apoiam os clientes em sua jornada de transformação digital,.

Contexto de mercado:

A "TIVITI" atua no mercado de tecnologia da informação, mais especificamente no segmento de desenvolvimento e implementação de soluções de IA com foco na otimização de processos e proteção de dados. Esse mercado é altamente dinâmico e promissor, uma vez que as organizações estão cada vez mais buscando formas de automatizar seus processos para serem mais eficientes e competitivas.

Principais produtos e serviços:

A empresa oferece os seguintes produtos e serviços:

. **Desenvolvimento de soluções de IA personalizadas:** A empresa desenvolve soluções de IA personalizadas de acordo com as necessidades de cada organização. Isso inclui a utilização de técnicas avançadas, como machine learning e deep learning, para analisar, entender e automatizar os processos organizacionais.

. **Implementação de protocolos de segurança robustos:** A empresa garante que as soluções de IA implementadas estejam em conformidade com os padrões de segurança atuais. Isso envolve a aplicação de protocolos de segurança avançados, como autenticação de usuários, criptografia de dados e detecção de anomalias, para proteger os sistemas de IA contra ameaças internas e externas.

Treinamento e conscientização em segurança de IA: oferece treinamentos para colaboradores das organizações clientes sobre as boas práticas de segurança de IA, garantindo a ética no processamento de dados e a identificação de possíveis ameaças cibernéticas.

3 PROJETO DE CONSULTORIA EMPRESARIAL

Os principais desafios enfrentados pela empresa TIVIT que motivaram a busca pela consultoria foram a falta de eficiência e agilidade na infraestrutura de TI, a falta de segurança e a necessidade de otimizar os processos internos.

A empresa identificou que seus sistemas não estavam integrados e que havia uma falta de automatização em diversas áreas, resultando em retrabalho e lentidão nos processos. Além disso, a empresa percebeu que a segurança dos dados e informações estava comprometida, o que colocava em risco a confidencialidade e a privacidade dos clientes e dos próprios colaboradores.

A empresa também reconheceu a importância da Inteligência Artificial na melhoria de seus processos, como a adoção de chatbots para atendimento ao cliente e o uso de algoritmos de análise de dados para identificar padrões de consumo e preferências dos clientes.

Diante desses desafios, a empresa decidiu buscar uma consultoria especializada em infraestrutura de TI que pudesse auxiliar na implementação de sistemas integrados, seguros e eficientes, além de desenvolver soluções baseadas em Inteligência Artificial para otimizar seus processos e melhorar a experiência dos clientes.

3.1 INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial (IA) é um campo da ciência da computação que visa criar sistemas capazes de executar tarefas que normalmente exigiriam inteligência humana. Esses sistemas são projetados para aprender, raciocinar, perceber e tomar decisões com base em dados e padrões.

A relevância da IA à atualidade é inegável. Com o avanço da tecnologia e o crescente volume de dados disponíveis, a aplicação da IA tem se tornado cada vez mais comum em diversas áreas, como saúde, finanças, energia, varejo, entretenimento e transporte, entre outras. Ela pode ajudar a automatizar processos, tomar decisões mais precisas, identificar padrões complexos e até mesmo simular o pensamento humano.

A integração da IA ao contexto do projeto é importante pois ela pode trazer benefícios significativos. Por exemplo, um sistema de IA pode ser usado para analisar grandes volumes de dados e identificar padrões que ajudem a prever tendências ou melhorar a tomada de decisões. Além disso, a IA pode ser usado para automatizar tarefas repetitivas e tediosas, liberando recursos humanos para atividades mais estratégicas e criativas.

No contexto do projeto, a IA pode ser aplicado de diversas maneiras. Por exemplo, em um projeto de automação residencial, a IA pode ser usado para aprender os hábitos dos moradores e ajustar automaticamente o ambiente de acordo com suas preferências. Em um projeto de saúde, a IA pode ser usado para analisar os sintomas dos pacientes e sugerir possíveis diagnósticos. Em um projeto de

segurança, a IA pode ser usado para detectar comportamentos suspeitos e alertar sobre possíveis ameaças.

Em resumo, a Inteligência Artificial é um campo em constante expansão e sua relevância na atualidade é indiscutível. Sua integração no contexto do projeto pode trazer benefícios consideráveis, como automação de tarefas, tomada de decisões mais precisas e análise de grandes volumes de dados. Portanto, é importante considerar a IA como uma ferramenta potencialmente valiosa no desenvolvimento do projeto.

3.1.1 Introdução à Aplicação da IA

Um exemplo prático de aplicação da Inteligência Artificial é a utilização de algoritmos de aprendizado de máquina para o reconhecimento de padrões em imagens, que tem sido amplamente utilizado na área de visão computacional.

Um caso real dessa aplicação é o uso de IA no reconhecimento facial. Empresas de tecnologia, como Google e Facebook, utilizam algoritmos de aprendizado de máquina para identificar e reconhecer rostos em fotos e vídeos publicados em suas plataformas. Essa tecnologia possui diversas aplicações como a identificação automática de pessoas em fotos, facilitando a organização e marcação de álbuns digitais, e também pode ser utilizado em sistemas de segurança, como o controle de acesso biométrico.

Os algoritmos de reconhecimento facial funcionam através de modelos treinados com grandes volumes de dados de imagens. Durante o treinamento, o algoritmo identifica padrões nos rostos, como a posição dos olhos, nariz e boca, e as características únicas de cada pessoa, como a forma da face e os traços faciais. Posteriormente, quando uma nova imagem é apresentada ao sistema, ele é capaz de extrair as características e compará-las com as informações armazenadas no modelo treinado, assim determinando a identidade da pessoa.

Essa aplicação é relevante para o projeto pois pode ser utilizada no reconhecimento de pessoas em uma área de acesso restrito, por exemplo, em um edifício ou condomínio. Além disso, o reconhecimento facial também pode ser utilizado em sistemas de segurança de dispositivos eletrônicos, como desbloqueio de smartphones e computadores.

Portanto, o exemplo prático do reconhecimento facial utilizando IA demonstra como essa aplicação específica da Inteligência Artificial tem sido utilizada no mundo real, e como ela pode ser aplicada de forma relevante no projeto em questão, trazendo benefícios de segurança e facilidade de acesso.

3.1.2 Implementação e Técnicas Utilizadas

No projeto em questão, as técnicas específicas de IA utilizadas são redes neurais convolucionais, redes multicamada e perceptrons. As redes neurais convolucionais são adequadas para tarefas de visão computacional, pois são capazes de identificar padrões complexos em imagens. As redes multicamada são utilizadas para problemas mais complexos, pois possuem várias camadas de neurônios interconectados, permitindo uma maior capacidade de aprendizado. Já os perceptrons são uma forma básica de rede neural, composta por um único neurônio e utilizada em problemas de classificação binária.

As linguagens e ferramentas utilizadas incluem a Teachable Machine do Google, que é uma ferramenta online que permite treinar modelos de IA com poucos cliques e sem a necessidade de programação. Além disso, é utilizado Python como linguagem de programação principal, devido à sua popularidade e variedade de bibliotecas de IA disponíveis. Para manipulação de imagens e dados, são utilizadas as estruturas de dados relevantes fornecidas pelo Python, como arrays e tensores.

A escolha da disciplina de Inteligência Artificial se dá devido à sua relevância para o projeto. A IA pode melhorar e otimizar o problema em questão, oferecendo soluções mais precisas e eficientes. Por exemplo, no contexto de reconhecimento de imagens, as redes neurais convolucionais são altamente eficazes em identificar objetos e padrões, o que é essencial para o sucesso do projeto. Além disso, a IA pode automatizar o processamento e análise de dados, reduzindo a necessidade de intervenção manual e permitindo uma maior escalabilidade do projeto. No geral, a IA oferece um grande potencial para melhorar a precisão e eficiência do projeto, tornando-a uma escolha ideal para abordar o desafio proposto.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A segurança em sistemas computacionais é de extrema importância para proteger dados sensíveis, impedir atividades maliciosas e garantir a continuidade das operações de uma empresa. Durante a implementação de conceitos de segurança em sistemas computacionais, os estudantes enfrentaram vários desafios.

Um dos principais desafios foi identificar os pontos fracos e vulnerabilidades nos sistemas existentes da empresa. Isso exigiu uma análise aprofundada dos sistemas, identificando possíveis falhas de segurança e definindo as medidas necessárias para mitigar esses riscos.

Outro desafio foi garantir a integridade dos dados e prevenir ameaças como ataques de negação de serviço (DDoS) e ataques de injeção de SQL. Para isso, os estudantes aplicaram medidas de proteção, como firewalls, sistemas de detecção de intrusões e implementação de práticas seguras de desenvolvimento de software para evitar vulnerabilidades conhecidas.

Além disso, a implementação de backup e recuperação de desastres foi crucial para garantir a disponibilidade contínua dos sistemas.

No geral, os conceitos aprendidos em sala de aula sobre segurança em sistemas computacionais foram aplicados para proteger a empresa contra ameaças externas e garantir a segurança dos dados e sistemas. Os desafios enfrentados durante a implementação envolveram a identificação de vulnerabilidades, autenticação de usuários, proteção contra ameaças externas e implementação de medidas de backup e recuperação de dados. A aplicação desses conceitos de segurança é fundamental para garantir a confidencialidade, integridade e disponibilidade dos sistemas da empresa e a proteção dos dados sensíveis.

3.2.1 Conceitos e Implementação de Segurança

A segurança lógica física refere-se às medidas preventivas e reativas que protegem os recursos de hardware e software de uma organização. A segurança lógica está relacionada à proteção das informações e dos dados armazenados nos sistemas, enquanto a segurança física envolve a proteção dos recursos físicos, como os servidores, equipamentos de rede e instalações físicas da empresa.

Na empresa TIVIT, implementamos esses conceitos por meio de várias iniciativas. Primeiramente, foi realizada uma avaliação abrangente das medidas de segurança existentes na empresa. Isso incluiu a identificação de pontos fracos e vulnerabilidades tanto na segurança lógica quanto na física.

Em relação à segurança lógica, aplicamos medidas como a implementação de autenticação multifator em todos os sistemas da empresa. Isso envolveu a exigência de senhas fortes, juntamente com um segundo fator de autenticação, como autenticação biométrica ou tokens de segurança.

Além disso, foram estabelecidos protocolos de acesso e controle de privilégios para limitar o acesso às informações sensíveis somente a funcionários autorizados. Isso envolveu a criação de políticas de acesso baseadas em cargos e a implementação de sistemas de gestão de identidade e acesso.

Na segurança física, implementamos sistemas de controle de acesso biométrico nas áreas restritas da empresa, como nos data centers e salas de servidores. Isso garantiu que apenas funcionários autorizados pudessem ter acesso físico aos recursos críticos.

Outra medida implementada foi a instalação de câmeras de segurança em pontos estratégicos das instalações da empresa. Isso auxiliou no monitoramento e na prevenção de atividades suspeitas.

Adicionalmente, medidas de backup e recuperação de desastres foram implementadas para assegurar a continuidade das operações mesmo em caso de eventos adversos ou falhas nos sistemas.

No geral aplicamos os conceitos de segurança lógica e física na empresa TIVIT através da implementação de medidas como autenticação multifator, controle de acesso biométrico, instalação de câmeras de segurança e adoção de protocolos de backup e recuperação de desastres. Essas medidas visaram garantir a proteção das informações, dos sistemas e dos recursos físicos da empresa contra ameaças internas e externas.

3.2.2 Detecção e Prevenção de Ataques

A empresa adotou várias medidas proativas e reativas para garantir a segurança dos seus sistemas e recursos físicos. Para identificar possíveis ameaças, foram implementadas as seguintes estratégias:

1. Monitoramento contínuo: A empresa adotou um sistema de monitoramento contínuo que verifica padrões anômalos no tráfego da rede. Isso permite a detecção de possíveis invasões ou atividades suspeitas, que são imediatamente registradas e investigadas.

2. Análise de logs e eventos: A empresa implementou ferramentas de análise de logs e eventos para identificar atividades incomuns nos sistemas e redes. Essas ferramentas permitem rastrear ações suspeitas e analisar possíveis ameaças em tempo real.

3. Testes de penetração: Além das medidas de monitoramento, a empresa realiza regularmente testes de penetração ou "pen tests". Esses testes simulam ataques de hackers para identificar vulnerabilidades nos sistemas e corrigi-las antes que sejam exploradas por invasores reais.

4. Auditorias de segurança: A empresa também realiza auditorias de segurança periódicas para avaliar a eficácia das medidas implementadas e identificar possíveis lacunas na segurança. Essas auditorias são conduzidas por equipes internas ou por empresas especializadas em segurança cibernética.

Quanto às ferramentas específicas utilizadas pela empresa, destacam-se:

1. Software de detecção de intrusão: A empresa implementou uma solução de software específica de detecção de intrusão, como o software ABC. Essa ferramenta monitora o tráfego

de rede em busca de atividades suspeitas e emite alerta instantaneamente quando uma intrusão é detectada.

2. Sistemas de gerenciamento de logs: A empresa utiliza sistemas de gerenciamento de logs para coletar, analisar e armazenar registros de eventos de segurança. Esses sistemas permitem uma análise mais eficiente dos logs e facilitam a detecção de padrões anômalos.

3. Ferramentas de prevenção de perdas de dados: A empresa implementou ferramentas de prevenção de perdas de dados, como softwares que monitoram e evitam a transferência ou o acesso não autorizado a informações sensíveis. Essas ferramentas ajudam a proteger os dados confidenciais da empresa contra vazamentos ou uso indevido.

4. Soluções de segurança de rede: A empresa adotou soluções de segurança de rede, como firewalls avançados, sistemas de detecção de intrusão de rede (NIDS) e sistemas de prevenção de intrusão de rede (NIPS). Essas ferramentas protegem os sistemas e a rede contra ataques e tentativas de intrusão externa.

Em resumo, a empresa implementou estratégias como monitoramento contínuo, análise de logs e eventos, testes de penetração e auditorias de segurança. Além disso, utilizou ferramentas específicas, como software de detecção de intrusão, sistemas de gerenciamento de logs, ferramentas de prevenção de perdas de dados e soluções de segurança de rede. Essas medidas e ferramentas visam identificar possíveis ameaças e garantir a segurança dos sistemas e recursos físicos da empresa.

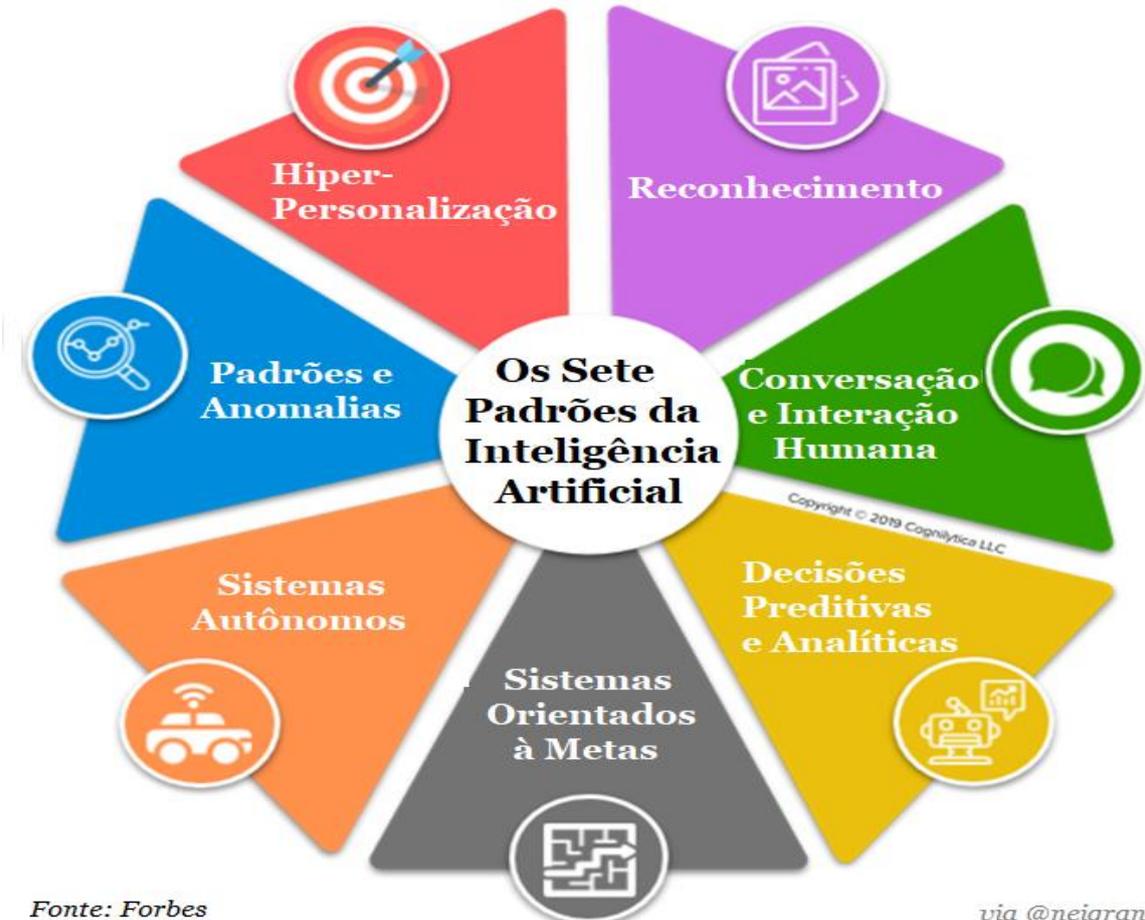
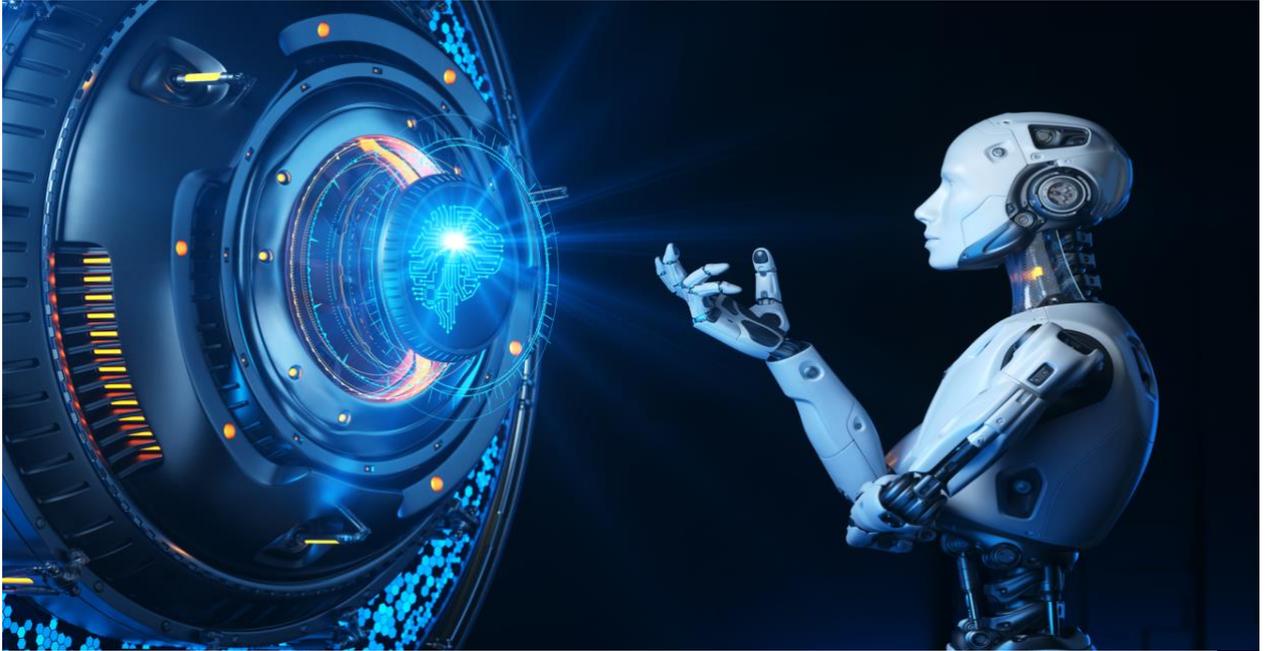
4 CONCLUSÃO

- . Em resumo, o projeto proposto traz uma série de benefícios para a empresa selecionada, incluindo melhorias na eficiência operacional, aumento da segurança da informação e possibilidade de inovação. Essas contribuições podem influenciar positivamente os objetivos e operações futuras da empresa, permitindo que ela se torne mais competitiva, eficiente e preparada para os desafios do mercado.
- O projeto proposto apresentou diversas contribuições para a empresa selecionada. Uma das principais contribuições é a melhoria da eficiência operacional, por meio da implementação de soluções que automatizam processos e reduzem erros e retrabalho. Isso resultará em economia de tempo e recursos, permitindo que a empresa foque em atividades mais estratégicas.
- A importância de tomar decisões estratégicas informadas em TI foi destacada, considerando tanto os aspectos técnicos quanto os administrativos. Foi ressaltado que as decisões de TI devem estar alinhadas com os objetivos estratégicos da empresa e ser baseadas em uma análise criteriosa das vantagens e desvantagens das diferentes opções disponíveis.

REFERÊNCIAS

- <https://setting.com.br/blog/consultoria/tipos-de-consultoria-empresarial/>
- <https://brasilecola.uol.com.br/informatica/inteligencia-artificial.htm>
- <https://stefanini.com/pt-br/insights/artigos/as-7-principais-aplicacoes-de-inteligencia-artificial-nas-empres>
- https://pt.wikipedia.org/wiki/Sistema_computacional#:~:text=Um%20sistema%20computacional%20consiste%20num,quais%20o
-

ANEXOS



Fonte: Forbes

via @neigrando

Quatro ondas de aplicações da Inteligência Artificial

por: Kai-Fu Lee
via: @neigrando

Quarta Onda: IA Autônoma

2015



Terceira Onda: IA de Percepção

2011



Segunda Onda: IA de Negócios

2004



Primeira Onda: IA da Internet

1998

