RECA
REVISTA ELETRÔNICA DE COMPUTAÇÃO APLICADA
Vol. 4 Nro. 2 2023

RECONHECIMENTO DE IMAGEM VOLTADO À SEGURANÇA CIBERNÉTICA

Igor França Cintra
Bacharelado em Ciência da Computação – Uni-FACEF
igorfrancacintra2@gmail.com

Pietro Gonçalves Fernandes
Bacharelado em Ciência da Computação – Uni-FACEF
pietrogf@outlook.com

Fausto Gonçalves Cintra
Docente do Uni-FACEF
faustocintra@facef.br

Resumo

A segurança cibernética é um tema crucial na sociedade digital com o aumento de ataques cibernéticos sofisticados e frequentes. Nesse contexto, o reconhecimento de imagem, uma área da inteligência artificial, surge como uma solução promissora para aumentar a segurança e diminuir potenciais ataques. Este artigo tem por objetivo propor uma análise aprofundada sobre a significativa influência do reconhecimento de imagem no âmbito da segurança cibernética. Em um contexto cada vez mais digitalizado e interconectado, a segurança cibernética é uma preocupação premente. Nesse cenário, exploraremos uma gama de aplicações dessa tecnologia, destacando sua importância estratégica. Adicionalmente, examinaremos questões éticas inerentes ao uso de dados visuais, considerando preocupações relacionadas à privacidade e ao uso responsável. Além disso, abordamos o papel central da API Google Cloud Vision na funcionalidade da inteligência artificial no modelo proposto, seguindo de uma apresentação do projeto de desenvolvimento de um site que utiliza de reconhecimento de imagem em documentos pessoais como forma de autenticação de acesso para fortalecer a segurança cibernética dos usuários. São descritos desde a documentação e gerenciamento do projeto com aplicação de metodologia ágil até a implementação do protótipo e codificação. Seguimos uma abordagem metodológica de desenvolvimento ágil para garantir a entrega eficiente e de alta qualidade do produto digital. O processo inclui a criação de protótipo para visualização em processo de *wireframing* e modelo de alta fidelidade, bem como a codificação utilizando a linguagem de programação Python.

Palavras-chave: Cibersegurança. Imagem. Segurança. Tecnologia. Digital.

Abstract

Cybersecurity is a crucial topic in the digital society, given the increase in sophisticated and frequent cyberattacks. In this context, image recognition, an area of artificial intelligence, emerges as a promising solution to enhance security and reduce potential threats. This article aims to propose an in-depth analysis of the significant influence of image recognition in the realm of cybersecurity. In an increasingly digitalized and interconnected landscape, cybersecurity is a pressing concern. In this scenario, we will explore a range of applications of this technology, highlighting its strategic importance. Additionally, we will examine ethical issues inherent to the use of visual data, considering privacy and responsible use concerns. Furthermore, we address the central role of the Google Cloud Vision API in the functionality of the proposed artificial intelligence model, followed by a presentation of the development project of a website that uses image recognition in personal documents as a means of access authentication to strengthen users' cybersecurity. The article describes everything from project documentation and management with the application of agile methodology to the implementation of the prototype and coding. We follow an agile development methodology to ensure efficient and high-quality delivery of the digital product. The process includes the creation of a prototype for visualization in wireframing and high-fidelity model stages, as well as coding using the Python programming language..

Keywords*: Cybersecurity. Image. Security. Technology. Digital*

1. Introdução

À medida que os ataques cibernéticos se tornam cada vez mais sofisticados e frequentes, a proteção de sistemas e dados se torna uma prioridade. Muitos fluxos de trabalho de negócios envolvem o recebimento de informações da mídia impressa, incluindo formulários em papel, faturas, documentos legais digitalizados e contratos impressos. O armazenamento e a gestão desses documentos demandam tempo e espaço consideráveis, além de enfrentar desafios na digitalização. A conversão do conteúdo de documentos em arquivos de imagem cria um problema adicional, uma vez que o texto nas imagens não pode ser processado pelo software de processamento de texto da mesma maneira que os documentos de texto. Aqui, o Reconhecimento Óptico de Caracteres (OCR) entra em cena como uma solução.

O OCR é crucial para a segurança cibernética, pois permite a análise de documentos digitalizados em busca de informações sensíveis e, ao fazer isso, contribui para a detecção precoce de ameaças, como vazamento de dados ou tentativas de intrusão. Além disso, o OCR é utilizado para automatizar processos de segurança, economizando tempo e recursos. A tecnologia OCR converte imagens de texto em dados de texto, que podem ser analisados por outros softwares de negócios. Esses dados podem ser usados para análises, otimização de operações, automação de processos e melhoria da produtividade.

Este artigo tem como objetivo explorar o uso do OCR em reconhecimento de imagem no contexto da segurança cibernética. Abordaremos os fundamentos teóricos relacionados ao reconhecimento de imagem, destacando técnicas como processamento de imagem, extração de características e classificação de objetos.

Ao final deste artigo, espera-se fornecer uma visão abrangente e atualizada sobre o reconhecimento de imagem voltado para a segurança cibernética. As informações apresentadas serão relevantes para profissionais e pesquisadores interessados em utilizar essa abordagem para aprimorar a proteção de sistemas e dados contra ameaças cibernéticas.

2. Referencial Teórico

O Reconhecimento Óptico de Caracteres, também conhecido como OCR, é um procedimento que transforma uma imagem contendo texto em um formato de texto que um computador pode entender. Por exemplo, se você escanear um formulário ou um recibo, o seu computador irá armazenar a digitalização como uma imagem, o que significa que você não conseguirá usar um programa de edição de texto para modificar, pesquisar ou até mesmo contar as palavras no arquivo de imagem. No entanto, o OCR oferece a capacidade de converter essa imagem em um documento de texto, em que o conteúdo é transformado em dados de texto que podem ser manipulados, editados e pesquisados.

Em um cenário de segurança cibernética, a maioria das operações comerciais envolve a obtenção de informações críticas a partir de mídias impressas, como formulários em papel, faturas, documentos legais digitalizados e contratos impressos. Lidar com esses grandes volumes de documentos torna-se um desafio, especialmente quando se trata de garantir a integridade e a segurança dos dados. Embora a gestão de documentos sem papel seja uma solução mais segura, a conversão desses documentos em papel em imagens digitais é fundamental. No entanto, esse processo requer intervenção manual, tornando-o suscetível a erros humanos e ameaças cibernéticas. Portanto, é essencial que as organizações adotem tecnologias avançadas, como o Reconhecimento OCR, para digitalizar e processar esses documentos com eficiência e, ao mesmo tempo, fortalecer a segurança de seus dados sensíveis para promover uma melhor confiabilidade nesse processo.

A confiabilidade das senhas em texto como método de autenticação está em declínio à medida que a tecnologia avança. Muitos agora preferem métodos como reconhecimento facial e impressão digital. Isso reflete uma preocupação crescente com a segurança online e a busca por alternativas mais seguras e convenientes

> 78% das pessoas afirmam confiar mais na impressão digital ou no reconhecimento facial do que nas senhas em texto como método de autenticação. (Delisjulia, 2023, *online*).

Essas tecnologias de reconhecimento de imagem desempenham um papel crucial na melhoria da precisão e eficiência do reconhecimento de imagens, enquanto também desempenham um papel fundamental na segurança cibernética, ajudando a reduzir o risco de fraude e roubo de identidade.

3. Aplicações de reconhecimento de imagem na segurança cibernética

O reconhecimento de imagem pode ser aplicado em várias áreas de segurança cibernética, como autenticação de usuários, detecção de fraudes e prevenção de crimes cibernéticos. Serão apresentadas algumas das principais aplicações de reconhecimento de imagem na segurança cibernética:

- Autenticação de usuários: o reconhecimento de imagem pode ser utilizado para autenticar a identidade de usuários em um sistema, por meio de imagens de seus documentos de identificação.
- Detecção de fraudes: o reconhecimento de imagem pode ser utilizado para detectar fraudes em transações financeiras, identificando alterações em imagens de cheques ou documentos de identificação.
- Prevenção de crimes cibernéticos: o reconhecimento de imagem pode ser utilizado para identificar indivíduos que tentam acessar um sistema de forma não autorizada, por meio de imagens de seus rostos ou documentos de identificação.

No entanto, o uso do reconhecimento de imagens por meio de algoritmos também tem levantado preocupações em relação à proteção da privacidade e dos dados pessoais. A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde setembro de 2020, estabelece diretrizes claras para a coleta, armazenamento, uso e compartilhamento de dados pessoais.

> A utilização de imagens e o reconhecimento facial devem ser utilizados com finalidades muito bem definidas, específicas e limitadas, respeitando-se os direitos dos titulares dos dados pessoais, sendo possível minimizar riscos através de uma governança de dados transparente e com os mais altos níveis de segurança da informação. (Lippi, [s.d.], *online*).

Dentre as principais diretrizes da LGPD, destacam-se a necessidade de consentimento do titular dos dados para a utilização desses dados, transparência na coleta e tratamento dos dados, garantia da segurança dos dados, eliminação dos dados após a finalidade para a qual foram coletados, entre outras obrigações. É essencial que empresas e organizações que utilizam essa tecnologia respeitem as leis e adotem boas práticas de proteção dos dados pessoais.

4. Questões éticas

O reconhecimento de imagem tem sido cada vez mais utilizado em diversos setores, incluindo a segurança cibernética. Essa tecnologia tem se mostrado promissora para a detecção de ameaças cibernéticas e para a validação de identidades em sistemas de autenticação.

> A ética na análise de dados e IA é fundamental para garantir que essas tecnologias sejam usadas de maneira responsável e justa. É importante que as empresas e organizações considerem as implicações sociais, legais e morais do uso de dados e IA e adotem práticas éticas em seus processos. (Almeida, 2023, *online*).

O reconhecimento de imagem pode ser aplicado em diversos cenários da segurança cibernética, como a identificação de usuários em dispositivos móveis e a detecção de atividades suspeitas em redes de computadores. Além disso, essa tecnologia pode ser utilizada para a autenticação de documentos, como passaportes e carteiras de identidade, reduzindo a possibilidade de fraudes.

No entanto, o uso do reconhecimento de imagem na segurança cibernética apresenta desafios técnicos e éticos. Um dos principais desafios técnicos é o desenvolvimento de algoritmos que sejam capazes de reconhecer imagens com precisão e de forma rápida. Já em relação às questões éticas, é necessário garantir a privacidade dos usuários e evitar o uso indevido dos dados pessoais coletados.

O artigo destaca ainda a importância da pesquisa e desenvolvimento na área de reconhecimento de imagem para aprimorar a segurança cibernética. É necessário investir em tecnologias mais avançadas e em soluções que atendam às necessidades do mercado, sem comprometer a privacidade e os direitos dos usuários.

5. Estudos sobre APIs de reconhecimento de imagem

A Application Programming Interface (API) de reconhecimento de imagem do Google Cloud Vision é uma ferramenta avançada para análise e compreensão de conteúdo visual. Essa API permite identificar objetos, textos, logotipos, *faces* e outros elementos em imagens digitais, proporcionando uma ampla gama de aplicações.

Além do reconhecimento de imagem em geral, a API do Google Cloud Vision oferece recursos adicionais, como a detecção de emoções faciais, classificação de conteúdo inapropriado, detecção de pontos de referência e até mesmo identificação de celebridades. Essas funcionalidades adicionais ampliam as possibilidades de uso da API em diversas áreas, como análise de mídias sociais, detecção de conteúdo impróprio e criação de sistemas de recomendação personalizada.

> O *Google Cloud Vision* API é a sigla para *Application Programming* Interface. APIs ... More é uma ferramenta poderosa para o reconhecimento de imagem em aplicativos, oferecendo recursos avançados de processamento de imagem, como detecção de objetos, reconhecimento de texto, detecção facial e muito mais. Ele permite que desenvolvedores de todo o mundo adicionem recursos de análise de imagem em seus aplicativos e serviços, independentemente do setor ou caso de uso. (Como usar.., 2023, *online*).

Além da API do Google Cloud Vision, existem outras opções no mercado, como a API de reconhecimento de imagem do Microsoft Azure e a API de reconhecimento de imagem do Amazon Rekognition. Cada uma dessas APIs tem suas próprias características e recursos únicos, permitindo aos desenvolvedores escolher a melhor opção para atender às necessidades específicas de seus projetos.

A pesquisa e o estudo sobre APIs de reconhecimento de imagem têm se mostrado cada vez mais relevantes, pois permitem avanços na segurança cibernética, no processamento automático de imagens, na análise de dados visuais e em outras áreas relacionadas. Com a evolução contínua dessas tecnologias, é fundamental explorar e compreender as capacidades das APIs disponíveis, a fim de utilizar todo o potencial do reconhecimento de imagem em diversas aplicações práticas.

No geral, as APIs de OCR são ferramentas úteis para extrair informações de documentos e imagens digitalizadas, e podem ser úteis em uma ampla variedade de cenários de negócios e de uso pessoal

6. Validação de acesso em um site de reconhecimento de imagem

A validação de acesso por reconhecimento de imagem é uma técnica poderosa para reforçar a segurança cibernética em várias áreas, como serviços bancários, comércio eletrônico e serviços governamentais. Além de prevenir fraudes, esse método oferece benefícios adicionais:

- Facilidade de Uso: Ao eliminar a necessidade de inserir manualmente informações, como senhas, os usuários têm uma experiência mais conveniente e rápida. Isso pode aumentar a satisfação do cliente.
- Redução de Erros: Com a automação do processo de validação de identidade, a probabilidade de erros humanos é minimizada, o que aprimora a precisão e a confiabilidade da verificação.
- Resistência à Fraude Avançada: Os sistemas de reconhecimento de imagem empregam algoritmos avançados que podem detectar sinais de adulteração em documentos, tornando-os resistentes a fraudes sofisticadas.
- Integração Simples: Esses sistemas podem ser integrados com facilidade em plataformas existentes, minimizando o impacto nas operações em andamento.

O processo de validação de acesso em um *site* com reconhecimento de imagem geralmente ocorre em três etapas. Primeiro, o usuário deve enviar uma imagem digitalizada do seu documento de identificação para o sistema. Em seguida, o sistema utiliza técnicas avançadas de reconhecimento de imagem para verificar se a imagem é autêntica e se corresponde ao documento de identificação do usuário. Por fim, se a imagem for validada, o sistema permitirá que o usuário acesse o *site*.

Ao utilizar o reconhecimento de imagem para validar o acesso de usuários, o *site* pode tornar o processo mais seguro e eficiente, evitando a utilização de documentos falsos e prevenindo fraudes. Além disso, esse tipo de sistema pode ser facilmente integrado a plataformas existentes, proporcionando uma camada adicional de segurança para os usuários.

Em resumo, o reconhecimento de imagem na validação de acesso não apenas melhora a segurança, mas também a experiência do usuário, a precisão e a

eficiência dos processos. É uma solução versátil que se adapta a várias indústrias e cenários de segurança cibernética.

7. Documentação de requisitos

Este documento de requisitos tem como objetivo descrever os requisitos para o desenvolvimento de um sistema de reconhecimento de imagem voltado para segurança cibernética, que permitirá a validação do acesso a outro sistema por meio do reconhecimento de documentos pessoais.

O sistema a ser desenvolvido deverá ser capaz de realizar o reconhecimento de imagem de documentos pessoais, como RG, CPF, passaporte, carteira de motorista, entre outros, para validar o acesso a outro sistema que contenha informações sensíveis

O sistema deverá permitir a captura de imagens de documentos por meio de câmera ou upload de imagem, além de garantir a segurança e privacidade das informações pessoais dos usuários.

7.1. Requisitos Funcionais

Requisitos funcionais: específica brevemente os casos de uso do sistema. (Figura 1)

Figura 1 - Requisitos funcionais

[RF01] - Cadastro de dados	O sistema deverá ser capaz de solicitar dados para o usuário a fim de que ao ser feito o reconhecimento de imagem, encontre tais dados na imagem fornecida para a validação do acesso.
[RF02] - Reconhecimento de imagem	O sistema deverá ser capaz de reconhecer e ler as informações contidas nos documentos pessoais por meio de técnicas de OCR (Reconhecimento Óptico de Caracteres) e analisar as informações para validar o acesso ao outro sistema.
[RF03] - Validação de acesso	O sistema deverá ser capaz de validar o acesso ao outro sistema, conferindo se as informações contidas no documento pessoal correspondem às informações fornecidas pelo usuário no outro sistema.
[RF04] - Segurança cibernética	O sistema deverá ser desenvolvido com foco em segurança cibernética, utilizando técnicas de criptografia para garantir a privacidade das informações pessoais e impedir que dados sensíveis sejam acessados por terceiros.
[RF05] - Registro e monitoramento de atividades	O sistema deverá registrar e monitorar todas as atividades realizadas pelos usuários, garantindo a segurança e a rastreabilidade das informações pessoais.
[RF06] - Integração com outros sistemas	O sistema deverá permitir a integração com outros sistemas para validação de informações pessoais, a fim de garantir a veracidade das informações fornecidas pelo usuário.

Fonte: elaborado pelos autores

.

7.2. Requisitos não funcionais

Requisitos não funcionais: cita e explica os requisitos não funcionais do sistema (Figura 2)

Figura 2 - Requisitos não funcionais

[RN01] - Desempenho	O sistema deverá ter um desempenho rápido e eficiente, garantindo a resposta em tempo hábil para validar o acesso ao outro sistema.
[RN02] - Usabilidade	O sistema deverá ser intuitivo e fácil de usar, permitindo que usuários com diferentes níveis de habilidade possam utilizá-lo sem dificuldades.
[RN03] - Confiabilidade	O sistema deverá ser confiável e disponível para uso a qualquer momento, evitando falhas e interrupções no processo de validação do acesso.
[RN04] - Segurança da informação	O sistema deverá ser desenvolvido com base em práticas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações pessoais dos usuários.
[RN05] - Escalabilidade	O sistema deverá ser escalável, permitindo que novos usuários possam ser adicionados sem impactar no desempenho e na segurança do sistema.

Fonte: elaborado pelos autores.

Este documento de requisitos descreve as principais funcionalidades e requisitos não funcionais do sistema de reconhecimento de imagem voltado para segurança cibernética. A implementação desses requisitos garantirá a eficácia e segurança do sistema, protegendo as informações pessoais e sensíveis dos usuários. Além disso, permitirá a validação do acesso a outros

O sistema de reconhecimento de imagem de dados pessoais deve seguir as leis e regulamentações relacionadas à privacidade e proteção de dados pessoais, tais como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia.

O custo do desenvolvimento do sistema de reconhecimento de imagem de dados pessoais dependerá da complexidade do sistema e das tecnologias utilizadas. Além disso, é importante considerar os custos de manutenção e atualização do sistema, bem como os custos relacionados à segurança da informação.

O suporte ao sistema de reconhecimento de imagem de dados pessoais deverá ser oferecido aos usuários para garantir a eficácia e confiabilidade do sistema. O suporte poderá ser oferecido por meio de uma central de atendimento ou suporte *online*.

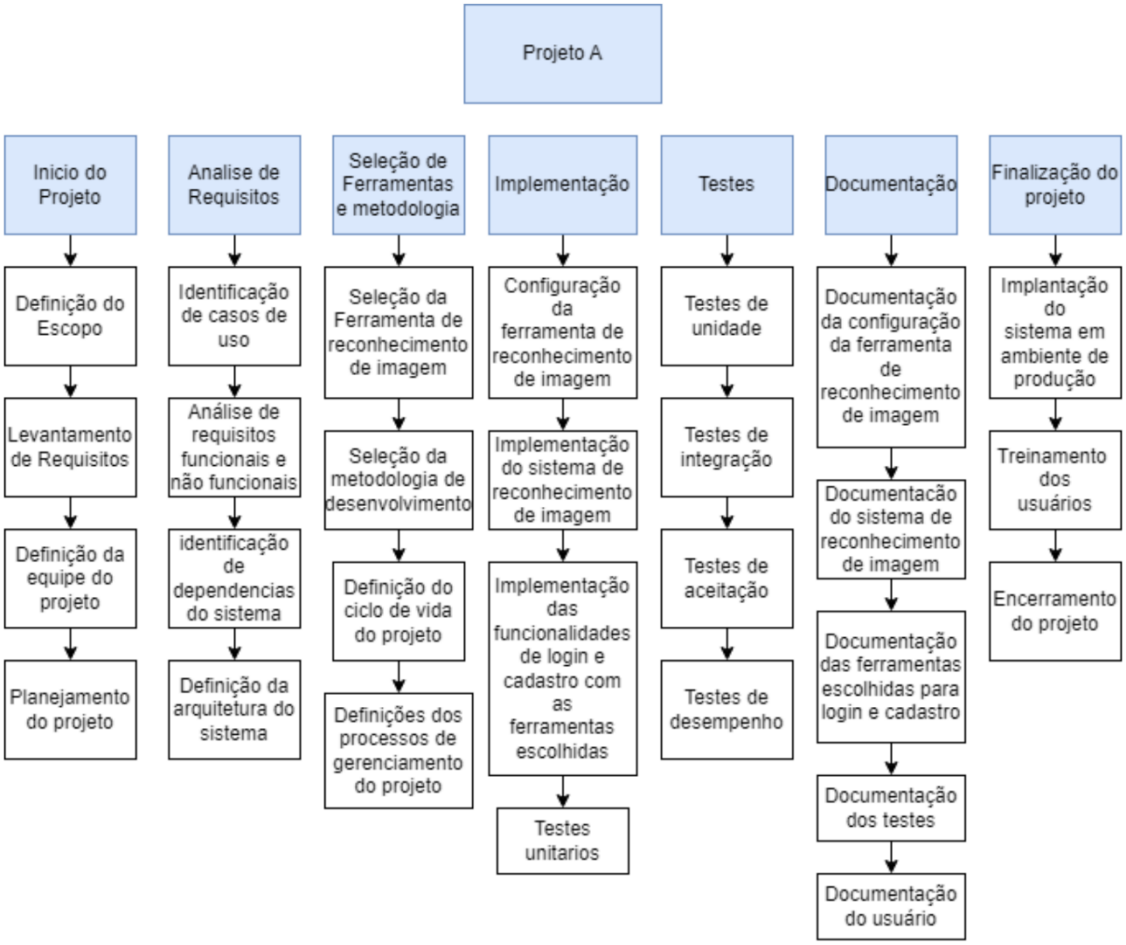
8. Metodologia e Ferramentas

Para orientar o desenvolvimento da solução proposta, foram utilizados diversos métodos e ferramentas de gerenciamento de projetos e desenvolvimento de software. As principais ferramentas utilizadas foram:

Estrutura Analítica do Projeto (EAP): a EAP é uma ferramenta de gerenciamento de projetos que permite a divisão do projeto em partes menores e mais gerenciáveis. Foi utilizada para dividir a solução proposta em componentes menores e mais específicos, o que ajudou a entender melhor o escopo e a complexidade do projeto. A EAP também permitiu que fossem identificadas as principais entregas e tarefas do projeto, facilitando o planejamento e o controle do trabalho (Figura 1).

Termo de Abertura do Projeto (TAP): o TAP é um documento que define as principais características do projeto, como descrição, justificativa, objetivos e requisitos. Foi elaborado no início do projeto e serviu como guia para o planejamento e execução do trabalho.

Figura 3 - EAP do desenvolvimento da solução



Fonte: elaborado pelos autores.

Figura 4 - Termo de Abertura do Projeto

Termo de Abertura do Projeto - Projeto de Reconhecimento de Imagem
Nome do Projeto: Projeto de Reconhecimento de Imagem
Descrição do Projeto: O Projeto de Reconhecimento de Imagem tem como objetivo desenvolver um *site* que utilize técnicas de reconhecimento de imagem para validar o acesso de usuários a outro *site*, por meio do reconhecimento de dados pessoais contidos em documentos. O *site* de reconhecimento será responsável por validar a identidade dos usuários e garantir que apenas usuários autorizados tenham acesso a ele.
Gerentes: Igor França Cintra e Pietro Gonçalves Fernandes
Justificativa: A validação de identidade dos usuários é um fator crítico de segurança para muitos *sites* e serviços *online*. O uso de técnicas de reconhecimento de imagem pode ajudar a garantir que apenas usuários autorizados tenham acesso ao *site*. O projeto também tem como objetivo oferecer uma experiência mais rápida e fácil para os usuários ao acessar o *site*, pois não será necessário digitar manualmente as informações de *login*.
Objetivos: • Desenvolver um *site* de reconhecimento de imagem preciso e confiável; • Validar a identidade dos usuários com base em dados pessoais contidos em documentos, como RG, CNH e passaporte; • Garantir a privacidade e segurança das informações dos usuários; • Disponibilizar uma interface amigável e intuitiva para os usuários.
Requisitos: • O *site* deve utilizar técnicas de reconhecimento de imagem precisas e eficientes; • O *site* deve ser compatível com diferentes tipos de documentos, como RG, CNH e passaporte; • O *site* deve garantir a privacidade e segurança dos dados dos usuários, em conformidade com a legislação de proteção de dados vigente; • O *site* deve ser desenvolvido dentro do orçamento e prazo estabelecidos; • O *site* deve ser compatível com diferentes plataformas e sistemas operacionais.

Fonte: elaborado pelos autores.

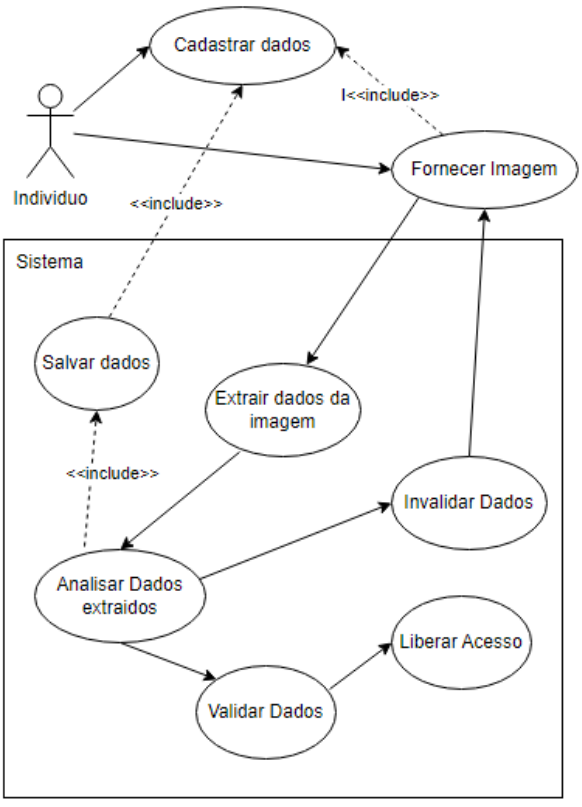
Diagrama e documentação de Casos de Uso: Diagramas de casos de uso (Figura 6) e sua documentação (Figura 5) desempenham um papel vital na engenharia de sistemas, identificando atores e funcionalidades. Os diagramas esquematizam visualmente como os atores interagem com o sistema, enquanto a documentação fornece detalhes textuais. Ambos são cruciais para entender e comunicar os requisitos e o comportamento do sistema de forma clara e abrangente. Isso ajuda a garantir que todas as funcionalidades necessárias sejam consideradas e implementadas corretamente, servindo como uma base sólida para o desenvolvimento, teste e colaboração entre equipes multidisciplinares, desde desenvolvedores até partes interessadas.

Figura 5 - Documentação de Casos de Uso

Nome do Caso de Uso	Validar Acesso
Ator Principal	Indivíduo
Resumo	Esse caso de uso visa mostrar como funciona o processo de validação de dados fornecidos de uma imagem para acesso de um sistema externo.
Pré-Condições	O indivíduo precisa previamente ter cadastrado uma imagem para ter os dados base
Fluxo Principal	
Ações do Autor	Ações do Sistema
1. Cadastrar dados	
2. Fornecer Imagem	
	3. Extrair dados
	4. Analisar dados extraídos
	5. Validar dados
	6. Invalidar dados
	7. Liberar Acesso

Fonte: elaborado pelos autores.

Figura 6 - Diagrama de Casos de Uso da solução



Fonte: elaborado pelos autores.

5W1H: A ferramenta 5W1H foi utilizada para definir as principais questões relacionadas ao projeto, tais como: *What* (o que será feito?), *Why* (por que será feito?), *Who* (quem fará?), *When* (quando será feito?), Where (onde será feito?), e *How* (como será feito?). Essas questões foram respondidas no início do projeto e ajudaram a definir o escopo e os objetivos da solução proposta (Figura 7).

Figura 7 - Plano 5W1H do desenvolvimento da solução

Fonte: elaborado pelos autores.

9. Linguagem de Programação

O projeto foi desenvolvido em Python, uma linguagem de programação de alto nível, interpretada e de propósito geral, amplamente utilizada em projetos de ciência de dados, *machine learning*, automação de tarefas, entre outros. A escolha de Python se deu por diversos motivos:

- Facilidade de aprendizado: é conhecida por ter uma sintaxe simples e intuitiva, o que torna a linguagem de fácil aprendizado para programadores iniciantes e experientes.
- Grande comunidade: possui uma grande comunidade de desenvolvedores, que contribuem com bibliotecas e ferramentas, tornando a linguagem uma das mais utilizadas em todo o mundo.
- Bibliotecas para reconhecimento de imagem: possui diversas bibliotecas e *frameworks* para processamento de imagem, como o OpenCV e o Pillow. Além disso, o Google Cloud Vision oferece uma API em Python para reconhecimento de imagem, o que torna a integração com o serviço mais fácil.
- Flexibilidade: é uma linguagem flexível e versátil, permitindo que o desenvolvedor crie soluções para uma ampla variedade de problemas.

Por esses motivos, foi a escolha ideal para o projeto de reconhecimento de imagem voltado para segurança cibernética, oferecendo uma ampla gama de recursos e facilidades para a implementação da solução.

10. Implementação do protótipo

A tecnologia de Reconhecimento Óptico de Caracteres tem desempenhado um papel crucial na extração de informações de documentos e imagens digitalizadas. Neste artigo, é apresentado o uso da API de OCR do Google Cloud Vision para extrair informações específicas de imagens.

Será mostrado o processo passo a passo, desde a configuração do ambiente de desenvolvimento até a obtenção dos resultados. De início é preciso criar um projeto no Google Cloud Platform e ativar a API do Cloud Vision. Em seguida deve-se gerar as credenciais de autenticação e instalar as bibliotecas necessárias. Também é importante habilitar a faturação do projeto, uma vez que o uso da API de OCR do Cloud Vision não é gratuito.

Foi utilizada a linguagem Python para implementar a extração de informações de imagens. Foi feito uso da biblioteca Google Cloud Vision para interagir com a API da plataforma. O código deve percorrer os arquivos de uma pasta selecionada pelo usuário, identificar as imagens presentes nela e, em seguida, enviar cada imagem para a API de OCR para extração das informações. Os resultados são armazenados em um arquivo texto, como mostrado no código da (Figura 8) que possui comentários explicativos de cada função.

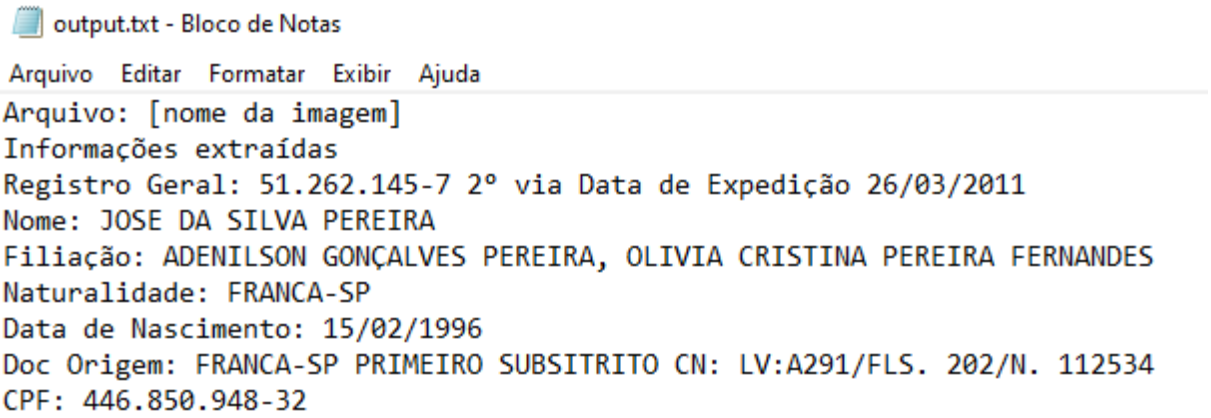
Figura 8 – Codificação de extrator de características

```python
import os
from tkinter import Tk
from tkinter.filedialog import askdirectory
from google.cloud import vision_v1

def recognize.image(image_path:)
    # Configuração de autenticação
    os.environ['GOOGLE_APPLICATION_CREDENTIALS'] = 'C:/PROJETOS/TCC/chave_apli.json'

    # Criação do cliente da API Cloud Vision
    client = vision_v1.ImageAnnotatorClient()

    # Carrega a imagem
    with open(image_path, 'rb') as image_file:
        content = image_file.read()

    #  Cria um objeto de imagem para análise
    image = vision_v1.Image(content= content)

    # Faz a chamada para a API Cloud Vision
    response + client.document_text_detection(image=image)

    # Processa os resultados
    if response.error.message:
        raise Exception(f'Erro na chamada da API Cloud Vision: {response.error.message}')

    # Extrai o texto da imagem
    extracted_text = response.full_text_annotation.text

    return extracted_text

# Cria a janela para seleção de pasta
root = Tk()
root.withdraw()

# Solicita ao usuário para selecionar a pasta
folder_path = askdirectory()

# Cria um arquivo txt para salvar as informações extraídas
output_file = open('output.txt', 'w')

# Itera sobre todos os arquivos na pasta selecionada
for filename in os.listdir(folder_path):
    # Verifica se o arquivo é uma imagem
    if filename.lower().endswith(('.png', '.jpg', '.jpeg')):
        # Caminho completo para a imagem
        image_path = os.path.join(folder_path, filename)

        # Chama a função para reconhecer a imagem
        extracted_text = recognize_image(image_path)

        # Escreve as informações extraídas no arquivo de saída
        output_file.write(f'Arquivo: {filename}\n')
        output_file.write(f'Informações extraídas: {extracted_text}\n\n')

# Fecha o arquivo de saída
output_file.close()
```

Fonte: elaborado pelos autores.

Ao enviar uma imagem para a API do Cloud Vision, ela é processada utilizando técnicas avançadas de reconhecimento de texto. Os resultados são retornados em uma estrutura hierárquica, contendo blocos, parágrafos, palavras e símbolos. No código implementado, foram processados os dados resultantes da API para extrair o texto bruto e organizá-lo em um formato legível. Ao executar o código, é feita uma chamada de faturamento na API do *Google Cloud*, que solicita a movimentação na conta para usar a função. Por isso, é apresentada uma versão hipotética de um resultado com dados fictícios criado pelo ChatGPT como prova de conceito. Com base no código obtido e nas informações mencionadas da imagem, o arquivo de saída *output.txt* deve ser preenchido como o mostrado na Figura 9.

Figura 9 – Simulação de um resultado do extrator de características



Fonte: elaborado pelos autores.

O arquivo *output.txt* tem o nome da imagem no início de cada seção, seguido das informações extraídas do texto da imagem. Cada seção começa com identificadores como: Registro Geral, Nome, Filiação, Naturalidade, Data de Nascimento, Doc Origem e CPF. As informações correspondentes são apresentadas abaixo de cada identificador.

No momento em que forem extraídas as informações da imagem, o sistema deverá filtrar as informações relevantes e verificar se estão em conformidade com os dados previamente cadastrados. Posteriormente, será concedido o acesso ao *site* de origem, caso haja concordância

11. Prototipação

Na fase inicial de um projeto, é essencial criar protótipos para visualizar e comunicar as ideias de *design* e funcionalidade antes da implementação completa.

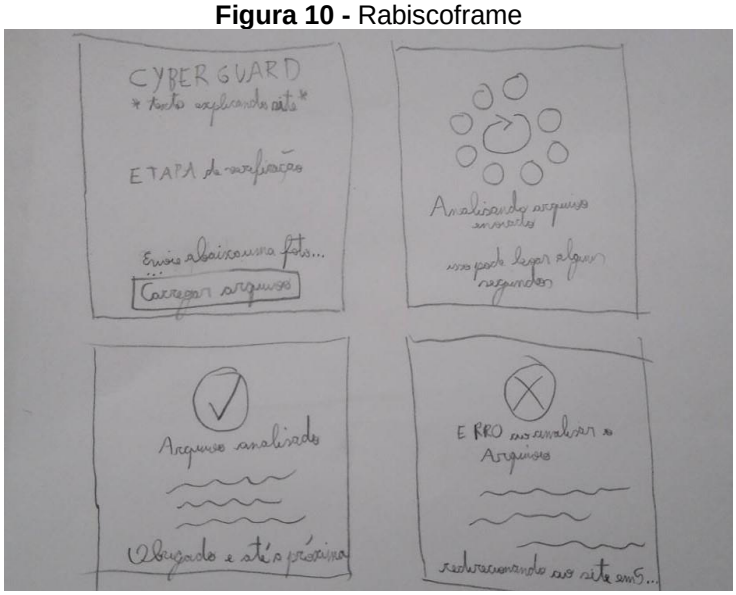
Os protótipos desempenham um papel crucial no processo de desenvolvimento, permitindo a validação de conceitos, a identificação de problemas e a obtenção de *feedback* dos usuários.

Existem diferentes tipos de protótipos utilizados no desenvolvimento de projetos, sendo três deles amplamente conhecidos: rabiscoframe, *wireframe* e protótipo de alta fidelidade.

O rabiscoframe é o tipo mais básico de protótipo, caracterizado por esboços rápidos e simples, geralmente feitos à mão ou com ferramentas digitais de desenho. Esses protótipos são úteis para visualizar rapidamente as ideias iniciais,

esboçar o fluxo de interação e testar conceitos de forma rápida e acessível. O rabiscoframe é flexível e permite iterações rápidas, mas não possui detalhes refinados ou elementos visuais completos (Figura 10).

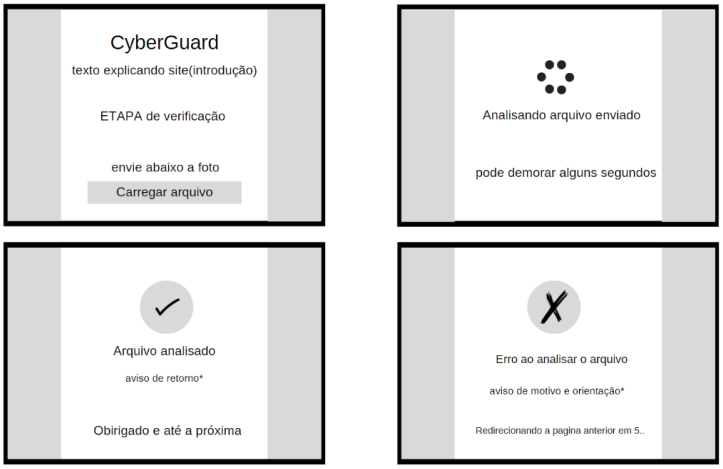
Figura 10 - Rabiscoframe



Fonte: elaborado pelos autores.

O *wireframe* é um protótipo mais elaborado e estruturado. Ele representa a estrutura e o *layout* do projeto, incluindo a disposição dos elementos de interface, como botões, menus, campos de entrada e áreas de conteúdo. Geralmente, os *wireframes* são criados com ferramentas específicas de *design*, oferecendo uma representação visual mais precisa das funcionalidades e da organização das informações. Os *wireframes* são valiosos para testar a usabilidade e a arquitetura da informação, além de servirem como base para a criação de protótipos mais avançados (Figura 11)**.**

Figura 11 - *Wireframe*



Fonte: elaborado pelos autores.

O protótipo de alta fidelidade é o estágio mais avançado dos protótipos, buscando uma representação fiel do produto final. Nesse tipo de protótipo, os detalhes

visuais, as interações e as funcionalidades são desenvolvidas com maior precisão, aproximando-se do produto real. Geralmente são utilizadas ferramentas de *design* e desenvolvimento para criar protótipos de alta fidelidade permitindo simular o comportamento do produto de forma mais realista. Esses protótipos são úteis para execução de testes de usabilidade e experiência do usuário, obter *feedback* detalhado e realizar demonstrações mais próximas do produto.

Na Figura 12, consegue-se ver um protótipo de uma tela de cadastro dos dados pessoais e da imagem que será fornecida pelo usuário.

Figura 12 - Protótipo de Alta Fidelidade – Página Cadastro

Fonte: elaborado pelos autores.

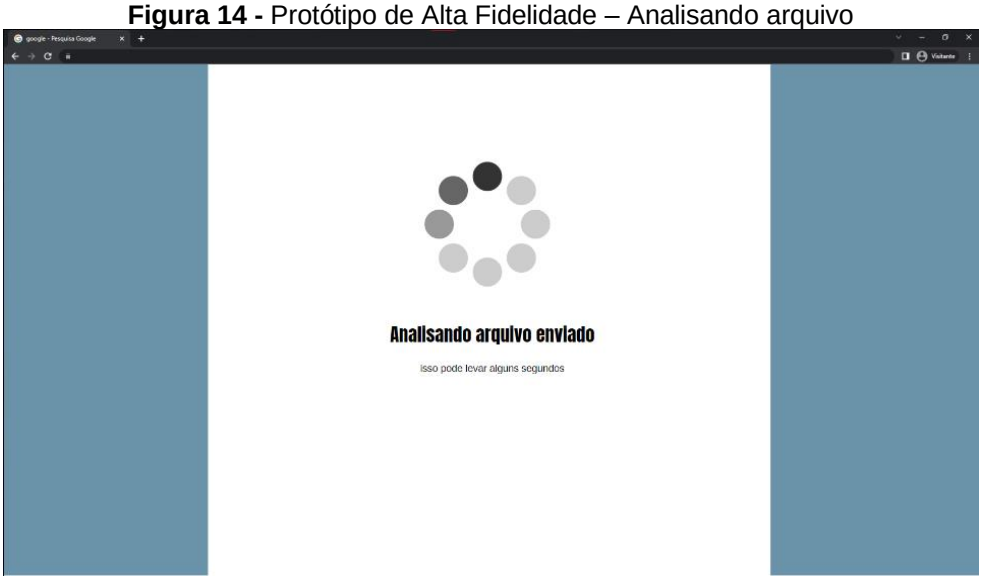
Na Figura 13, mostra uma tela semelhante a do cadastro, porém é quando o usuário tem acesso ao sistema, após ja ter feito o processo de cadastro, no qual ele precisa apenas fornecer a imagem para dar seguimento no processo de reconhecimento de imagem.

Figura 13 - Protótipo de Alta Fidelidade – Página inicial

Fonte: elaborado pelos autores.

Na Figura 14, temos umas tela informando que o sistema está analisando a imagem enviadas para extração dos dados e liberação do acesso caso esteja tudo correto

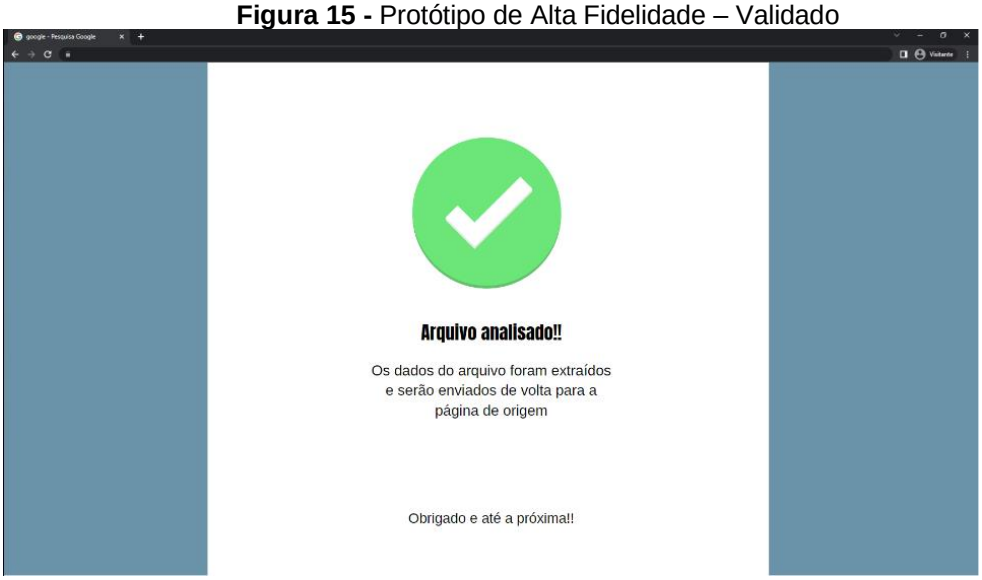
Figura 14 - Protótipo de Alta Fidelidade – Analisando arquivo



Fonte: elaborado pelos autores.

Na Figura 15, a seguir da figura anterior, caso o sistema tenha validado os dados retirados da imagem fornecida, será mostrado uma tela de arquivo analisado e que o usuário será redirecionado para a página de origem.

Figura 15 - Protótipo de Alta Fidelidade – Validado



Fonte: elaborado pelos autores.

E por fim, na Figura 16, a seguir da figura 14, caso o sistema não tenha validado os dados retirados da imagem fornecida, será mostrado uma tela de erro ao analisar o arquivo enviado e ele será redirecionado para a página inicial (Figura 12)

Figura 16 - Protótipo de Alta Fidelidade – Erro de Validação

Fonte: elaborado pelos autores.

Cada tipo de protótipo possui seu propósito e nível de detalhe, atendendo a diferentes estágios e necessidades do projeto. O rabiscoframe é ideal para a exploração inicial de ideias, o *wireframe* para a estruturação do fluxo de navegação e validação do *design*, e o Protótipo de Alta Fidelidade para a simulação precisa da experiência do usuário.

Ao utilizar esses diferentes tipos de protótipos ao longo do processo de desenvolvimento, é possível aprimorar a qualidade e a eficiência do projeto, garantindo que as soluções propostas atendam aos requisitos e expectativas dos usuários.

12. Considerações finais

Com a conclusão do processo, foi obtido um arquivo de texto contendo as informações extraídas da imagem processada, que foram organizadas de acordo com a estrutura do documento original, facilitando a leitura e a interpretação dos resultados.

É importante ressaltar que a precisão da extração depende da qualidade da imagem e da clareza do texto presente nela. A API de reconhecimento óptico de caracteres do Google Cloud Vision oferece uma solução poderosa para extrair informações de imagens de maneira automatizada.

Nesse contexto, é evidente que a implementação de um sistema de validação de acesso baseado em reconhecimento de imagem representa um procedimento altamente seguro e suscetível a um amplo escopo de aplicação no que tange à segurança de redes e dados sensíveis.

Neste conjunto de textos, exploram de maneira detalhada a implementação de um sistema de reconhecimento de imagem voltado para segurança cibernética, que tem como objetivo fortalecer a autenticação e o acesso a sistemas

por meio do reconhecimento de documentos pessoais. Ao longo dos textos, diversos aspectos cruciais foram abordados, destacando a relevância e a complexidade dessa abordagem inovadora.

Iniciamos discutindo o contexto atual da segurança cibernética, no qual os ataques estão se tornando cada vez mais sofisticados e frequentes. Nesse cenário, o reconhecimento de imagem surge como uma solução promissora para verificar a identidade dos usuários e proteger sistemas sensíveis. Esse enfoque se baseia na capacidade das tecnologias de reconhecimento de imagem em identificar padrões complexos em imagens digitais, como documentos pessoais.

Foram abordadas questões éticas, ressaltando a importância de considerar a privacidade e a segurança dos dados pessoais dos usuários ao implementar sistemas de reconhecimento de imagem. A escolha da linguagem de programação Python se justifica pela sua facilidade de aprendizado, grande comunidade e bibliotecas específicas para processamento de imagem.

A codificação do projeto foi minuciosamente explicada, desde a configuração do ambiente de desenvolvimento até a utilização da API de Reconhecimento Óptico de Caracteres (OCR) do Google Cloud Vision para extrair informações de documentos pessoais. A análise do resultado obtido demonstrou o processo de extração de informações, organização e validação, enquanto ressaltou a necessidade de considerar as cobranças associadas ao uso da API.

Ao reunir todas essas informações, fica claro que o projeto de reconhecimento de imagem para segurança cibernética é uma abordagem promissora e abrangente. A combinação de tecnologias avançadas, como OCR e reconhecimento de imagem, com práticas de segurança sólidas, cria um ambiente que pode reforçar a autenticação de usuários e a proteção de dados sensíveis em diversas aplicações, desde sistemas bancários até serviços governamentais.

No entanto, é vital lembrar que a implementação e o uso dessas tecnologias exigem um equilíbrio delicado entre inovação, segurança e ética. À medida que continuamos a avançar em direção a um mundo cada vez mais digital, projetos como esse destacam a necessidade de manter a segurança dos usuários como prioridade máxima, ao mesmo tempo em que aproveitamos as vantagens das tecnologias emergentes.

Ao longo desta jornada, nossa experiência pessoal e acadêmica se entrelaçam de maneira significativa. Como novos entusiastas da segurança cibernética, podemos apreciar a importância da proteção de dados pessoais na era digital. Aprendemos a equilibrar inovação tecnológica com responsabilidade ética, enquanto aprimoramos nossas habilidades técnicas e compreendia as complexidades legais e éticas da implementação de sistemas de reconhecimento de imagem. Essa experiência reforçou nossa dedicação em se manter atualizado com as tendências em segurança cibernética e destacou a importância da colaboração com colegas e especialistas para impulsionar a melhoria contínua dos sistemas e práticas de segurança.

13. Referências Bibliográficas

ALMEIDA, Bruno. A importância da ética na análise de dados e IA: garantindo decisões justas e responsáveis. **LinkedIn**, 4 mar. 2023. Disponível em: https://pt.linkedin.com/pulse/import%C3%A2ncia-da-%C3%A9tica-na-an%C3%A1lise-de-dados-e-ia-decis%C3%B5es-bruno-almeida. Acesso em: 21 set. 2023.

AWS. O que é reconhecimento de caractere óptico (OCR)?. **amazon**, [s. d.]. Disponível em: https://aws.amazon.com/pt/what-is/ocr/#:~:text=Optical%20character%20recognition%20(OCR%20%E2%80%93%20reconhecimento,como%20um%20arquivo%20de%20imagem. Acesso em: 21 set. 2023.

COMO USAR o Google Cloud Vision API para reconhecimento de imagem em sua aplicação? **Nobug**, 6 maio 2023. Disponível em: https://nobug.com.br/como-usar-o-google-cloud-vision-api-para-reconhecimento-de-imagem-em-sua-aplicacao/. Acesso em: 21 set. 2023.

CTA. Ferramentas OCR – entenda o que são e sua relação com a acessibilidade. **CTA**, 17 dez 2018. Disponível em: https://cta.ifrs.edu.br/ferramentas-ocr-entenda-o-que-sao-como-funcionam-e-qual-sua-relacao-com-a-acessibilidade/. Acesso em: 25 out. 2023.

DELISJULIA. O que é reconhecimento facial? Entenda como a tecnologia funciona. **idblog**, 25 set 2023. Disponível em: https://blog.idwall.co/o-que-e-reconhecimento-facial/. Acesso em: 21 set. 2023.

LIPPI, Paula. Imagens de vigilância, reconhecimento facial e a Lei Geral de Proteção de Dados. **Revista Segurança Eletrônica**, [s. d.]. Disponível em: https://revistasegurancaeletronica.com.br/imagens-de-vigilancia-reconhecimento-facial-e-a-lei-geral-de-protecao-de-dados/. Acesso em: 07 jul. 2023.

LISBOA, Paulo. Aprenda sobre Reconhecimento de Imagens com Python: Tudo o que Você Precisa Saber. **Awari**, 24 ago 2023. Disponível em: https://awari.com.br/aprenda-sobre-reconhecimento-de-imagens-com-python-tudo-o-que-voce-precisa-saber/?utm_source=blog&utm_campaign=projeto+blog&utm_medium=Aprenda%20sobre%20Reconhecimento%20de%20Imagens%20com%20Python:%20Tudo%20o%20que%20Voc%C3%AA%20Precisa%20Saber. Acesso em: 27 out. 2023.

MPPR, Felipe. Conheça o escopo do projeto e a estrutura analítica do projeto (EAP). **MPPR**, 16 mar 2011. Disponível em: https://mppr.mp.br/Noticia/Conheca-o-escopo-do-projeto-e-estrutura-analitica-do-projeto-EAP. Acesso em: 27 out. 2023.

NONES, Fernanda. LGPD: o que diz a lei de proteção de dados e como ela pode impactar a sua estratégia de marketing e vendas. **Resultados Digitais**, 6 out 2022. Disponível em: https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/. Acesso em: 23 out. 2023.

ROOKE DA SILVA, Felipe. Documento de Requisitos do Sistema. **MINISTÉRIO DA EDUCAÇÃO**, 17 fev 2016. Disponível em: https://www2.ufjf.br/diavi//files/2016/07/DocumentosdeRequisitosdoSistema.pdf. Acesso em: 27 out. 2023.

SCIELO. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **scielo**, [s. d.]. Disponível em: https://www.scielo.br/j/ea/a/wXBdv8yHBV9xHz8qG5RCgZd/. Acesso em: 21 set. 2023.