



UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS RUSSAS
CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

DAVI FERNANDES ALVES DA SILVA

**DESENVOLVIMENTO DE UM SISTEMA DE CONTROLE DE PRESENÇA
BASEADO EM RECONHECIMENTO FACIAL PARA AMBIENTES DE
COMPUTAÇÃO EM NUVEM**

RUSSAS

2024

DAVI FERNANDES ALVES DA SILVA

DESENVOLVIMENTO DE UM SISTEMA DE CONTROLE DE PRESENÇA BASEADO
EM RECONHECIMENTO FACIAL PARA AMBIENTES DE COMPUTAÇÃO EM
NUVEM

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Engenharia de Software da Universidade Federal do Ceará - Campus Russas, como requisito parcial à obtenção do título de bacharel em Engenharia de Software.

Orientador: Prof. Ms. Valéria Maria da Silva Pinheiro

RUSSAS

2024

DAVI FERNANDES ALVES DA SILVA

DESENVOLVIMENTO DE UM SISTEMA DE CONTROLE DE PRESENÇA BASEADO
EM RECONHECIMENTO FACIAL PARA AMBIENTES DE COMPUTAÇÃO EM
NUVEM

Trabalho de Conclusão de Curso apresentado
ao Curso de Bacharelado em Engenharia de
Software da Universidade Federal do Ceará -
Campus Russas, como requisito parcial à
obtenção do título de bacharel em Engenharia
de Software.

Aprovada em 03/10/2024.

BANCA EXAMINADORA

Prof. Ms. Valéria Maria da Silva Pinheiro (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Cenez Araújo de Rezende
Universidade Federal do Ceará (UFC)

Ms. Fernanda Ferreira Do Nascimento
Universidade Federal do Ceará (UFC)

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S579d Silva, Davi Fernandes Alves.

Desenvolvimento de um sistema de controle de presença baseado em reconhecimento facial para ambientes de computação em nuvem / Davi Fernandes Alves Silva. – 2024.
87 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas, Curso de Engenharia de Software, Russas, 2024.

Orientação: Profa. Ma. Valéria Maria da Silva Pinheiro.

1. computação em nuvem. 2. reconhecimento facial. 3. engenharia de software. 4. amazon web services.
5. desenvolvimento. I. Título.

CDD 005.1

A Todos que um dia acreditaram em mim.

AGRADECIMENTOS

Ao Estado do Ceará, expresso meu reconhecimento pelo acolhimento e suporte oferecidos, proporcionando um ambiente propício para a pesquisa e desenvolvimento deste trabalho.

À Universidade Federal do Ceará, agradeço pela oportunidade de aprender e crescer academicamente. Agradeço também por proporcionar recursos. A UFC é uma fonte inesgotável de conhecimento, e sou grato por fazer parte desta instituição.

Ao meus pais Charles Fernandes Alves da Silva e Maria do Socorro Oliveira Alves, pelo apoio incondicional, por todos os sacrifícios feitos para que eu pudesse alcançar meus objetivos.

A Prof Ms. Valéria Maria da Silva Pinheiro. expresso minha profunda gratidão pela orientação, dedicação e paciência em me auxiliar apesar de todas as dificuldades enfrentadas. Agradeço por compartilhar seu conhecimento e tempo comigo, sendo essencial para a conclusão deste trabalho.

RESUMO

O registro de frequência desempenha um processo crucial em diversos contextos, exigindo monitoramento e controle em ambientes variados. Sua prática é utilizada em diversas áreas, como avaliação de desempenho, cumprimento de leis ou regras, monitoramento de saúde, gerenciamento, transparência e responsabilidade. A presente pesquisa explora os aspectos práticos e teóricos do problema, desenvolvendo um sistema em nuvem dedicado à realização e gestão da presença, com a utilização da técnica de reconhecimento e identificação facial como forma de identificação dos usuários. O sistema foi desenvolvido através de processos metodológicos da Engenharia de Software, como a elicitação de requisitos por meio de questionário, *benchmarking* e revisão bibliográfica, além do projeto arquitetônico, desenvolvimento, verificação e validação, que incluem o monitoramento, testes de conformidade, revisão de requisitos e testes automatizados. A aplicação seguirá conforme as necessidades específicas de um ambiente em nuvem, obtendo-se economia de custo, elasticidade, disponibilidade de serviço, segurança, integridade e resiliência.

Palavras-chave: computação em nuvem; reconhecimento facial; engenharia de software.

ABSTRACT

The attendance record plays a crucial role in various contexts, requiring monitoring and control in different environments. Its practice is used in various areas, such as performance evaluation, compliance with laws or regulations, health monitoring, management, transparency, and accountability. This research explores the practical and theoretical aspects of the issue, developing a cloud-based system dedicated to attendance management, using facial recognition and identification techniques as a means of user identification. The system was developed through Software Engineering methodological processes, including requirements elicitation via questionnaires, benchmarking, and literature review, as well as architectural design, development, verification, and validation processes, which include monitoring, compliance testing, requirements review, and automated tests. The application will adapt to the specific needs of a cloud environment, achieving cost savings, elasticity, service availability, security, integrity, and resilience.

Keywords: cloud computing; facial recognition; software engineering.

LISTA DE FIGURAS

Figura 1 - Evolução do reconhecimento facial	25
Figura 2 - Etapas do desenvolvimento do sistema	30
Figura 3 - Arquitetura Spring security	36
Figura 4 - Camadas do Json Web Token	37
Figura 5 - Arquitetura da aplicação com Json Web token.	38
Figura 6 - Requisição entre domínios diferentes.	39
Figura 7 - Questionário aceitação - Respostas 01	45
Figura 8 - Questionário faixa etária - Respostas 02	46
Figura 9 - Questionário registro de presença - Respostas 03	46
Figura 10 - Questionário frequência registro de presença- Respostas 04	47
Figura 11 - Questionário ambientes de captura de presença - Respostas 05	47
Figura 12 - Questionário métodos de realização de frequência - Respostas 06	48
Figura 13 - Questionário acesso a internet - Respostas 07	49
Figura 14 - Arquitetura de baixo orçamento	57
Figura 15 - Arquitetura de médio orçamento	58
Figura 16 - Arquitetura de alto orçamento	59
Figura 17 - Diagrama do banco de dados	62
Figura 18 - Camadas de segurança	64
Figura 19 - Telas de início do sistema e login	65
Figura 20 - Telas de cadastro de usuário	66
Figura 21 - Tela de perfil do usuário	67
Figura 22 - Telas de organização e listagem de grupos	68
Figura 23 - Telas de grupo e justificativa de ausência	69
Figura 24 - Telas de realização de frequência e galeria	70

Figura 25 -Tela de relatório de frequência	71
Figura 26 - Monitoramento da aplicação com o grafana	72

LISTA DE QUADROS

Quadro 1	- Comparação dos modelos de precificação na nuvem	19
Quadro 2	- Aplicações do reconhecimento facial	22
Quadro 3	- Comparação algoritmos de reconhecimento facial.	24
Quadro 4	- Comparação entre os trabalhos relacionados e este trabalho.	29
Quadro 5	- Requisitos <i>Benchmarking</i> Godswill	50
Quadro 6	- Requisitos <i>Benchmarking</i> Rao	51
Quadro 7	- Requisitos funcionais elicitados	52
Quadro 8	- Requisitos não funcionais elicitados	55
Quadro 9	- Regras de negócio levantadas	55
Quadro 10	- Cabeçalhos de segurança	63

LISTA DE ABREVIATURAS E SIGLAS

AWS	<i>Amazon Web Services</i>
CAN	<i>Campus area network</i>
CAPEX	<i>Capital Expenditure/Despesa de capital</i>
CDN	<i>Content Delivery Network</i>
CORS	<i>Cross-Origin Resource Sharing</i>
CPU	<i>Central process unit</i>
DDoS	<i>Distributed Denial of Service</i>
DNS	<i>Domain Name Service</i>
EC2	<i>Elastic Compute Cloud</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IaaS	<i>infrastructure as a service/Infraestrutura como serviço</i>
ISO	<i>International Organization for Standardization.</i>
JVM	<i>Java virtual machine</i>
LBPH	<i>Local binary patterns Histogram</i>
LCD	<i>Display de cristal liquido/Liquid Crystal Display</i>
LFW	<i>Labeled Faces in the Wild</i>
LGPD	<i>Lei geral de proteção aos dados pessoais</i>
MVC	<i>Model, View and Controller</i>
NIST	<i>National Institute of Standards and Technology</i>
OPEX	<i>Operational Expenditure/despesas operacionais</i>
OS	<i>Operating System</i>
PaaS	<i>Plataforma como serviço/Platform as a Service</i>
PDF	<i>Portable Document Format</i>
PINs	<i>Personal Identification Numbers</i>
QR	<i>Quick response</i>
RBAC	<i>Role-based Access Control</i>
REST	<i>Representational State Transfer</i>
SaaS	<i>Software as a Service/Software como um serviço</i>
SIFT	<i>Scale-invariant feature transform</i>
SMS	<i>Short Message Service ou Serviço de Mensagens Curtas</i>
SSL	<i>Security Socket Layer</i>

SUFT	Speeded Up Robust Features
SVM	<i>Support Vector Machine</i>
TCLE	Termo de Consentimento Livre e Esclarecido
TLS	<i>Transport Layer Security</i>
WAF	<i>Web Application Firewall</i>
XSS	<i>cross-site scripting</i>

SUMÁRIO

1	INTRODUÇÃO.....	14
2	OBJETIVOS.....	15
2.1	Objetivo geral.....	15
2.2	Objetivo específico.....	15
3	FUNDAMENTAÇÃO TEÓRICA.....	16
3.1	Computação em nuvem.....	16
3.1.1	Modelos de serviço.....	17
3.1.2	Modelos de Implantação.....	18
3.1.3	Precificação na Nuvem.....	18
3.2	Reconhecimento Facial.....	21
4	TRABALHOS RELACIONADOS.....	26
4.1	Comparativo do estado da arte.....	28
5	METODOLOGIA.....	30
5.1	Revisão bibliográfica.....	30
5.2	Elicitação de requisitos.....	32
5.2.1	Benchmarking.....	32
5.2.2	Questionário.....	33
5.3	Projeto Arquitetural.....	34
5.3.1	Arquitetura REST.....	34
5.3.2	Segurança da Aplicação.....	35
5.3.2.1	Spring Security.....	36
5.3.2.2	oAuth2.....	37
5.3.2.3	JSON Web Token (JWT).....	37
5.3.2.4	Cross-Origin Resource Sharing (CORS).....	38
5.3.2.5	Cabeçalhos de segurança.....	39
5.4	Desenvolvimento.....	39
5.4.1	Tecnologias utilizadas.....	40
5.4.2	Processo de Prototipação.....	40

5.4.3	Processo de desenvolvimento.....	40
5.4.4	Recursos.....	41
5.4.5	Lei Geral de Proteção de Dados Pessoais (LGPD).....	41
5.5	Verificação e Validação.....	43
6	RESULTADOS.....	45
6.1	Aplicação do Questionário.....	45
6.2	Aplicação do Benchmarking.....	49
6.3	Requisitos Seleccionados.....	52
6.4	Propostas Arquiteturais.....	56
6.4.1	Proposta de banco de dados.....	61
6.5	Segurança do sistema.....	63
6.6	Protótipo desenvolvido.....	65
6.7	Monitoramento da solução.....	72
7	CONCLUSÃO.....	73
7.1	Considerações finais.....	73
7.2	Trabalhos futuros.....	74
	REFERÊNCIAS.....	75
	APÊNDICE A – QUESTIONÁRIO DE COLETA DE DADOS.....	79
	APÊNDICE B – TERMO DE CONSENTIMENTO.....	81
	APÊNDICE C – POLÍTICA DE PRIVACIDADE.....	83
	APÊNDICE D – REPOSITÓRIO DO PROJETO.....	86

1 INTRODUÇÃO

A prática de registrar a frequência é um importante processo, sendo fundamental em diferentes contextos, como locais de trabalho, ambientes de cuidados com a saúde e ambientes acadêmicos. Sua realização é essencial para conduzir procedimentos de monitoramento, medições e avaliações. A qual, a frequência contribui nas decisões estratégicas e organizacionais.

No âmbito educacional, a frequência é parte fundamental na avaliação dos discentes, conforme Romero e Lee (2007), no ambiente acadêmico a assiduidade tem um papel primordial na evolução e desempenho do aluno, o absenteísmo está correlacionado de forma negativa ao desenvolvimento dos estudantes. Sua afirmativa pode ser reforçada com o art. 2 do decreto nº 6.094, de 24 de abril de 2007, a frequência é um indicador primordial, tendo-se o compromisso do combate à evasão, inclusão, desenvolvimento e monitoramento do indivíduo do âmbito federativo até o núcleo familiar (BRASIL, 2007a).

Realizar o acompanhamento e o monitoramento da evasão escolar pode ser uma tarefa bem difícil para as instituições de ensino. Conforme apontado por Ferreira e Oliveira (2020), poucas escolas possuem programas estruturados para o combate à evasão, visto que os motivos que levam o aluno a evadir, são variados. Portanto, é fundamental o desenvolvimento de projetos pedagógicos para se obter uma educação de qualidade. De tal maneira, aplica-se então a proposta de um sistema de controle de presenças com a utilização do reconhecimento facial voltando para a implantação em ambiente de nuvem. O sistema assim, forma conjunto de funcionalidade para auxiliar o monitoramento da frequência, com uma economia de custos, conforme a demanda da organização.

Este estudo explora os âmbitos teórico e prático de um sistema na nuvem. A diversidade de processos disponíveis para a realização de frequência, têm potencial de acabar gerando inconsistências, enfrentando os desafios de erros humanos, riscos de fraudes, grande volume de frequências e problemas de armazenamento.

O presente trabalho está estruturado da seguinte maneira: No capítulo 2, são apresentados os objetivos a serem alcançados com esta pesquisa; O capítulo 3 apresenta a fundamentação teórica; O capítulo 4 apresenta os trabalhos relacionados a esta pesquisa; O capítulo 5 detalha a metodologia de desenvolvimento deste trabalho; No capítulo 6, são apresentados e discutidos os resultados encontrados na pesquisa; Por fim, o capítulo 7 encontram-se as conclusões da pesquisa.

2 OBJETIVOS

2.1 Objetivo geral

Esta pesquisa tem como objetivo geral o desenvolvimento de uma aplicação para realização de frequências, utilizando-se da computação em nuvem para operação e implantação.

2.2 Objetivo específico

- Realizar estudo de viabilidade da solução;
- Levantar os requisitos do sistema;
- Definir a arquitetura do sistema;
- Validar o sistema a ser desenvolvido;
- Desenvolver um sistema nativo em nuvem;
- Realizar o reconhecimento facial dos usuários registrados;
- Avaliar o sistema desenvolvido;
- Desenvolver um sistema *open-source* para a realização e monitoramento das frequências.

3 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os principais conceitos sobre os quais nortearam a pesquisa. No capítulo 3.1 é apresentado o conceito de computação em nuvem. Posteriormente no capítulo 3.2 se é apresentado os fundamentos do reconhecimento facial desde sua origem.

3.1 Computação em nuvem

A computação em nuvem marca uma grande ruptura entre os modelos tradicionais de entrega e solicitação de serviços de recurso computacional. Sua ascensão já tinha sido vislumbrada por Chellappa (1997), revolucionando o modelo de provisionamento de recursos computacionais ao abrir uma gama de novas soluções de forma ágil e eficiente, sobre demanda, oferecendo uma solução volátil para o problema da ociosidade computacional.

Como definido pelo *National Institute of Standards and Technology* (NIST) dos Estados Unidos através dos seus pesquisadores Mell e Grance (2011, p. 6, tradução nossa):

A computação em nuvem é um modelo que permite acesso onipresente, conveniente e sob demanda à rede para um ambiente compartilhado, conjunto de recursos de computação configuráveis como, redes, servidores, armazenamento, aplicativos e serviços.

Ainda de acordo com Mell e Grance (2011), o modelo de computação em nuvem apresenta algumas características, entre as quais se destacam:

- **Auto serviço sob demanda:** Somente o consumidor de forma exclusiva consegue provisionar recursos de forma automática sem a necessidade de qualquer interação humana com o provedor;
- **Amplio acesso à rede:** Os recursos devem poder ser acessados através de uma rede, por meio de mecanismos padrões, estando disponíveis de forma indiferente independente da complexidade ou simplicidade da plataforma dos clientes;
- **Reserva de recursos:** O provedor deve ter os recursos organizados para atender aos consumidores usando o modelo *Multi-tenant* com os recursos de forma dinâmica de acordo com a demanda do consumidor;
- **Rápida elasticidade:** Capacidade de se provisionar e liberar recursos de forma

dinâmica, de forma rápida, ágil e se possível de maneira automática, a qualquer momento;

- **Medição de serviço:** Os provedores de nuvem devem realizar de forma automática o controle, automatização de recursos, sendo os recursos em utilização monitorados, controlados e reportando de forma transparente entre o provedor e o cliente.

3.1.1 Modelos de serviço

A Computação em Nuvem é altamente configurável, sua utilização se aplica a diferentes problemas e contextos visto que há três modelos de serviço principais que podem ser adotados. Esses modelos são uma parte importante da definição do modelo arquitetural da solução, sua definição de forma correta é de suma importância. (MELL;GRANCE, 2011, p. 6-7).

De acordo com a definição feita pela NIST esses modelos podem ser definidos como:

- **Infraestrutura como Serviço (IaaS):** é capacidade de prover ao cliente, recursos computacionais como processamento, armazenamento ou rede, deixando-o responsável por esses recursos tanto a nível de *hardware* como a nível de *software*, não tendo domínio sobre a nuvem, mas possuindo controle sobre as operações;
- **Plataforma como Serviço (PaaS):** é capacidade de prover ambiente que apresentam ferramentas que podem ser configuradas, parametrizadas ou gerenciadas pelo cliente, que tem o ambiente a seu dispor porém não possuindo acesso à infraestrutura da nuvem;
- **Software como um Serviço (SaaS):** capacidade de prover ao cliente uma aplicação, sem, que ele tenha que se preocupar com configurações de infraestrutura como redes, servidores, sistemas operacionais, armazenamento ou até a escalabilidade do servidor, tendo-se toda essa parte abstraída do cliente, provendo toda a infraestrutura através da nuvem.

3.1.2 Modelos de Implantação

A computação em nuvem pode ser implantada de modos diferentes, dependendo do tipo de organização e de suas necessidades. Essa transição pode ser feita de diferentes formas. Segundo Gorelik (2013), há quatro modelos comumente usados para implantação, sendo eles:

- **Public Cloud:** A nuvem opera como um conjunto de recursos computacionais gerenciados e providos por um terceiro.
- **Private Cloud:** A nuvem é construída e gerenciada para uma única organização.
- **Hybrid Cloud:** Nuvem numa mistura entre *public cloud* e *private cloud* onde os recursos podem ser providos por ambos.
- **Community Cloud:** Nuvem divide recursos entre várias organizações, podendo ser gerenciada por uma das organizações ou por um terceiro.

Cada modelo de implantação tem suas vantagens e desvantagens, sendo assim cabe à organização definir o mais adequado para suas necessidades, havendo também a possibilidade de uma estratégia *multi-cloud*, combinando os modelos de implantação para extrair o melhor de suas características.

3.1.3 Precificação na Nuvem

A versatilidade da computação em nuvem não se restringe apenas a sua maneira de operar e aprovisionar recursos, mas também a maneira como precificar esses recursos, impactando diretamente o planejamento financeiro da organização. Ao adotar a computação em nuvem, as organizações transitam das despesas de capital (CAPEX) para despesas operacionais (OPEX), conforme destacado por Armbrust *et al* (2009, p. 12).

Essa transição implica em uma redução dos riscos em novos projetos, eliminando a necessidade de um aporte financeiro para aquisição de recursos computacionais, alocando os recursos na nuvem conforme as necessidades do seu negócio, podendo proporcionar uma gestão mais eficaz diante de imprevistos financeiros, recessões econômicas e crises

financeiras. A computação em nuvem nos leva a novos modelos econômicos e formar inovadores de precificação por recursos, advindo assim um novo mercado.

Os modelos de precificação se enquadram em duas categorias básicas, como definido por Ibrahim (2017) os dois esquemas de precificação em nuvem são:

- **Precificação estática:** Estabelece todos os preços para todo o período de tempo. Os serviços de computação em nuvem são altamente dependentes do tempo, então o intervalo de tempo do serviço oferecido é predeterminado.
- **Precificação dinâmica:** Estabelece um preço variável que pode mudar entre as solicitações dependendo da demanda pelo recurso.

O Quadro 1 a seguir demonstra exemplos de modelos de precificação na nuvem, apresentando diferentes vantagens e desvantagens. Essa diversidade permite que os clientes escolham o modelo mais adequado a suas necessidades. Contudo, a disponibilidade do modelo de cobrança depende do provedor de recursos.

Quadro 1 - Comparação dos modelos de precificação na nuvem

Modelo de precificação	Abordagem de precificação	Prós	Contras
Modelo pague conforme uso	Preço é definido pelo provedor de recursos e permanece constante(estático)	<ul style="list-style-type: none"> ● O cliente está ciente do preço exato a ser pago. ● Recursos são reservados para o cliente pelo período pago. 	<ul style="list-style-type: none"> ● O provedor de serviços pode reservar os recursos por um período mais longo do que o utilizado pelo cliente. ● O provedor de serviços não pode aumentar o preço quando a demanda é alta; quando a demanda é baixa, o usuário paga mais do que o preço de mercado.
Assinatura	Preço baseado no período de assinatura(estático)	<ul style="list-style-type: none"> ● O cliente pode pagar menos pelos recursos reservados se ele os utiliza extensivamente. 	<ul style="list-style-type: none"> ● O cliente pode pagar mais pelos recursos reservados se ele não os utilizar extensivamente.
Modelo	Baseado nos	<ul style="list-style-type: none"> ● Oferece a máxima 	<ul style="list-style-type: none"> ● Difícil de implementar.

pague por recursos	custos(dinâmico)	utilização dos recursos do provedor de serviços.	
Modelo genético de preço em mercados de computação em nuvem	Precificação em tempo real.(dinâmico)	<ul style="list-style-type: none"> ● Alcança receitas muito altas. ● Estável contra distúrbios. ● Flexível. ● Fácil de implementar. 	<ul style="list-style-type: none"> ● Pressupõe que o mercado se comporta racionalmente, o que pode fazer com que o modelo tenha um desempenho inferior em condições de demanda muito alta ou muito baixa.
Precificação baseado em valor	Preço definido de acordo com o valor percebido pelo cliente	<ul style="list-style-type: none"> ● Alta receita em cada item vendido (vantagem do ponto de vista do produtor). 	<ul style="list-style-type: none"> ● Difícil obter e interpretar dados dos clientes, concorrentes e da própria corporação para avaliar o valor percebido pelo cliente.
Precificação baseada em custo	Preço definido pela adição de um elemento de lucro em cima do custo (dinâmico).	<ul style="list-style-type: none"> ● Simplicidade no cálculo do preço. 	<ul style="list-style-type: none"> ● Tende a ignorar o papel dos consumidores.
Precificação baseada em competição	Preço definido de acordo com os preços dos concorrentes (dinâmico).	<ul style="list-style-type: none"> ● Fácil de implementar. 	<ul style="list-style-type: none"> ● Não leva em consideração os clientes.
Precificação baseado em cliente	Preço definido de acordo com o que o cliente está disposto a pagar (dinâmico).	<ul style="list-style-type: none"> ● Leva em consideração a perspectiva do cliente. 	<ul style="list-style-type: none"> ● Raramente os clientes indicam ao vendedor o quanto estão dispostos a pagar. ● Os dados são difíceis de obter e interpretar.
Precificação híbrida	Preço alterado de acordo com os tempos de espera na fila de trabalho (estático/dinâmico).	<ul style="list-style-type: none"> ● Simples e tem baixa sobrecarga computacional. 	<ul style="list-style-type: none"> ● Deve-se chegar a um acordo sobre preços base comuns e limites de variação.

Fonte: Adaptado de Al-Roomi *et al.* (2013).

Cabendo ao cliente determinar qual provedor de recurso e qual modalidade de precificação atendem melhor aos seus requisitos, representando uma estratégia que o usuário ou a organização deverá adotar, impactando diretamente sua gestão financeira e operacional.

3.2 Reconhecimento Facial

Desde o nascimento, desenvolvemos a habilidade de identificar pessoas por suas faces, essa habilidade é constantemente aprimorada ao decorrer de nossas vidas, permitindo-nos reconhecer pessoas mesmo após um prolongado período sem vê-las. Em pouco tempo, conseguimos assimilar e reconhecer rostos, entretanto para as máquinas esse processo não é tão simples, o que ocasiona diversos estudos e pesquisas na área de visão computacional.

Em um ponto de vista mais técnico, conforme definido por Huang (1998), a visão computacional tem como objetivo desenvolver sistemas autônomos capazes de realizar tarefas que se assemelham às executadas pela visão humana, podendo, em alguns casos, superá-la. A construção de uma visão computacional capaz de realizar o reconhecimento de faces humanas é um desafio amplamente explorado por diversas áreas, devido à sua vasta aplicação em diversos problemas, conforme destacado no Quadro 2.

Quadro 2 - Aplicações do reconhecimento facial.

Áreas	Aplicações
Segurança da informação	Segurança de acesso (sistema operacional (SO), base de dados) Privacidade de dados (ex. registros médicos) Autenticação de usuário (negociações, banco <i>online</i>)
Gerenciamento de acesso	Autenticação segura de acesso (instalações restritas) Sistema baseado em permissões Registros de acesso ou trilhas de auditoria
Biometria	Identificação de pessoa (Identidades nacionais, passaportes, registros biométricos de eleitores, carteiras de motorista) Verificação automatizada de identidade (controle de fronteira)
Aplicação da lei	Vigilância por vídeo Identificação de suspeitos Rastreamento de suspeitos Envelhecimento simulado Reconstrução forense de rostos a partir de restos mortais
Segurança pessoal	Sistemas de vigilância de vídeo doméstico interpretação de expressões (Sistema de monitoramento de motoristas)
Entretenimento - Lazer	Sistemas de videogame doméstico Aplicações de câmera fotográfica

Fonte: De Carrera e Marques (2010, p. 17, tradução nossa).

O estudo do reconhecimento facial, inicialmente foi atrativo não só pelo reconhecimento da face em si, mas também pela análise das expressões humanas, voltando-se a uma visão psicológica ao analisar emoções, expressões e gestos. Isso pode ser evidenciado com os estudos realizados por Bruner (1954) que mostravam que as expressões faciais estavam ligadas com as emoções com um certo grau de precisão.

Estudos mais recentes realizados por Le Mau *et al.* (2021) mostraram que as

expressões faciais de emoções nem sempre podem ser estereotipadas por imagens ou fotos, pertencendo elas a um repertório muito maior e diverso do que só a maneira que as pessoas movem seu rosto. Sendo a face uma característica biológica crucial para a comunicação humana muito além de somente desempenhar papéis sensoriais, tornados-nos únicos e distinguíveis.

Estudos realizados por Souza (2008) mostraram um avanço no entendimento no processo de reconhecimento facial. Pesquisas psicológicas e neurológicas indicam que os primatas possuem um sistema neural exclusivo para percepção facial, sendo essencialmente envolvidos no reconhecimento da identidade facial.

Ao longo dos anos, diversos algoritmos foram desenvolvidos para realizar o reconhecimento facial, entretanto, essa tarefa mostrou-se ser extremamente complexa. alternativas surgiram como o *Local binary patterns Histogram* (LBPH), *Speeded Up Robust Features* (SURF), *Scale-invariant feature transform* (SIFT), *Eigenfaces* e *Fisherface*. Suas vantagens e desvantagens podem ser vistas no Quadro 3. No entanto, como observado por Alzu'bi *et al.* (2021, p. 15) esses métodos holísticos se mostraram bastante instáveis com mudanças faciais, mostrando-se serem pouco robustos para o mundo real de possíveis mudanças faciais.

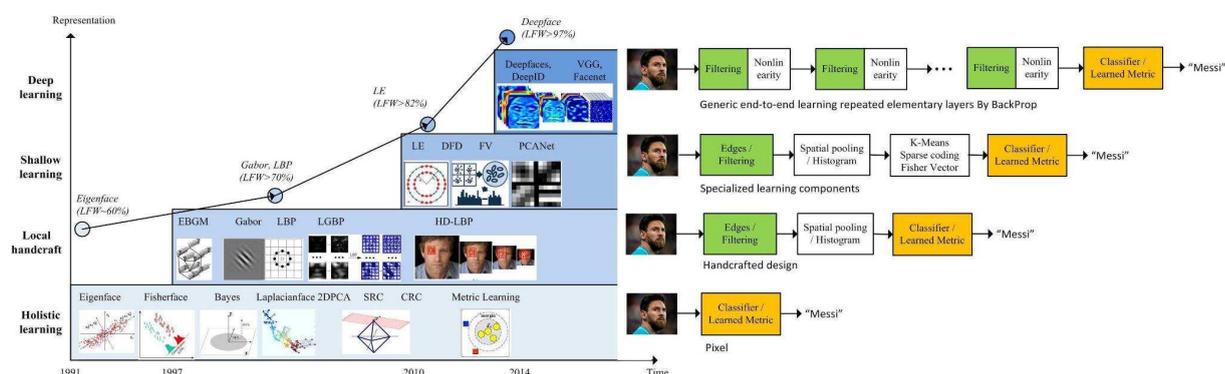
Quadro 3 - Comparação algoritmos de reconhecimento facial

Algoritmo	Ano	Pontos	Descrição
Eigenfaces	1991	Positivos	É um dos métodos mais antigos e conhecidos da área de reconhecimento facial. Insensitivo à pouca variação de iluminação.
		Negativos	A variação de pose e oclusão parcial podem prejudicar significativamente os resultados.
LBPH	1996	Positivos	Robusto em relação a transformações monotônicas em escala de cinza. Permite identificar bordas.
		Negativos	A variação de pose e oclusão parcial podem prejudicar significativamente os resultados.
Fisherfaces	1997	Positivos	Insensitivo a certa variação de iluminação e expressões faciais. Segundo os autores teve melhores resultados que o eigenfaces.
		Negativos	A variação de pose e oclusão parcial podem prejudicar significativamente os resultados.
SIFT	1999	Positivos	É invariante à escala e rotação, e parcialmente insensitivo à variação de iluminação e oclusão parcial
		Negativos	É computacionalmente mais pesado que os outros métodos
SURF	2006	Positivos	É invariante à escala e rotação, e parcialmente insensitivo à variação de iluminação e oclusão parcial
		Negativos	É computacionalmente mais pesado que os outros métodos, porém é mais rápido que o SIFT.

Fonte: Prado (2017, p. 64).

Com o passar do tempo, diversas abordagens técnicas foram desenvolvidas para o reconhecimento facial, conforme ilustrado na Figura 1. A imagem mostra a evolução das técnicas de reconhecimento facial ao longo dos anos de 1994 a 2014, comparando sua pontuação com o *benchmark Labeled Faces in the Wild (LFW)* e comparando as etapas percorridas na análise da face.

Figura 1 - Evolução do reconhecimento facial



Fonte: Wang, M e Deng (2021).

Um estudo aprofundado realizado por Wang, M e Deng (2021) revelou que os métodos de reconhecimento facial de aprendizagem superficial (*Shallow learning*) são insuficientes para lidar com as variações da face, apresentando assim resultados inconsistentes e gerando diversos falsos-positivos em aplicações do mundo real. Contudo, em 2012, a introdução das técnicas de aprendizagem profunda (*deep learning*) revolucionou esse campo de estudo. Utilizando múltiplas camadas de abstração, o *framework* DeepFace lançado em 2014, alcançou o desempenho de ponta *State-of-the-art* (SOTA) com o *benchmark* LFW, com uma acurácia de 97,35%, aproximando-se do nível de precisão humana. Após 3 anos de aprimoramentos, o modelo atingiu uma acurácia de 99.8%, com um modelo treinado com 9 camadas e 4 milhões de face.

De acordo com Taskiran, Kahraman e Erdem (2020), o reconhecimento facial, ao contrário de outros métodos biométricos, não obriga a participação ativa da pessoa, podendo ser executada de maneira não intrusiva. Foi encontrado por Pawle e Pawar (2013) também destacam que o reconhecimento facial oferece vantagens como segurança, economia, rapidez, unicidade e versatilidade, sendo assim, muito utilizada em soluções de autenticação e autorização.

4 TRABALHOS RELACIONADOS

Neste capítulo se encontram trabalhos relacionados a esta pesquisa, todos realizam a captura de frequência voltados envolvendo verificações biométricas e computação em nuvem, como objetivo da pesquisa, tendo cada um dos autores escolhido modelos e metodologias específicas para seu trabalho, ao final será exposto um quadro comparativo entre os trabalhos aqui citados e este trabalho em questão.

No trabalho de Sales (2022), a proposta foi o desenvolvimento de um *software* para automatizar o sistema de frequências de alunos com o reconhecimento facial, desenvolvida na linguagem Python com a utilização dos *frameworks*: Sanic¹ e Peewee². Para a parte de reconhecimento facial, foi utilizado *deep learning* com redes neurais convolucionais e *Support Vector Machine* (SVM), utilizando uma arquitetura *Model, View and Controller* (MVC). O objetivo do sistema é economizar tempo dos professores e garantir a inexistência de fraudes no processo da frequência. Entretanto, o autor não conseguiu realizar a integração entre os módulos de reconhecimento facial e de regras de negócio do sistema, sendo os dois módulos apenas sendo testados separadamente obtendo uma assertividade 86% no algoritmo de reconhecimento facial, com uma base de dados de 50 faces.

Godswill *et al.* (2018) propõe o desenvolvimento de um sistema *web* denominado FACECUBE, que foi desenhado para realizar as tarefas de computação intensa como detecção e reconhecimento de face, em servidores na nuvem, transferindo-as do servidor local para a nuvem, o FACECUBE tem três tipos de usuários: (i) estudantes - que podem criar sua conta e registrar seu rosto, e cadastrar em seus cursos; (ii) instrutores - que podem configurar cronogramas pessoais e solicitar presença com seu dispositivo portátil; e (iii) administrador - que é responsável por configurar as câmeras em diferentes salas de aula. A tecnologia foi projetada utilizando um servidor *on-premise* para comportar a aplicação, que se comunica através de uma rede *Campus Area Network* (CAN), se conectando com câmeras que ficam em frente às salas de aula. O sistema foi desenvolvido com a linguagem de programação C#, com o *framework* ASP.NET³ e para o reconhecimento e detecção de faces foi usado um *wrapper* do OpenCV⁴ chamado EmguCV, implementando o algoritmo Eigenface, a nuvem utilizada no projeto foi o Azure, utilizando o Azure SDK para realizar o envio das tarefas para a nuvem.

¹ <https://sanic.dev/en/>

² <https://docs.peewee-orm.com/en/latest/>

³ <https://dotnet.microsoft.com>

⁴ <https://opencv.org/>

Foi proposto por Mittal *et al.* (2017) um sistema inteligente de realização de frequência baseado em nuvem, através de transmissão de vídeo. Sendo o sistema desenvolvido para ambientes acadêmicos autenticando e identificando cada estudante da classe, projetado para ser confiável e escalável, para isso o autor optou por utilizar uma fusão entre os algoritmos EigenFace e Viola Jones, sendo o EigenFace utilizando o conceito de Vetores Eigen que são agrupados em uma matrix para realizar as análises de maneira rápida e eficiente. Tendo do outro lado o Viola Jones que é utilizado bastante para análises em tempo real, sendo bastante eficiente para imagens frontais da face, inicialmente o sistema foi desenvolvido em C e MATLAB, porém devido ao baixo valor de acurácia, os autores decidiram adotar outra abordagem utilizando Python e OpenCV. O sistema terá uma base de dados contendo as informações dos estudantes, a câmera irá escanear os estudantes que estiverem na frente da câmera e verificar se há semelhanças com os usuários presentes na base de dados e com isso realizar a frequência dos que forem reconhecidos, sendo o resultado da detecção de rosto o dado de entrada para a função de reconhecimento facial ocorrendo todo o processo de forma integrada com a nuvem. O propósito que Mittal *et al.* (2017) é que o sistema seja integrado com a nuvem no modelo de *SaaS*, habilitando o acesso a múltiplos sendo escalável.

No trabalho de Yadav et al. (2019) se ressalta a importância da realização da chamada nas instituições de ensino e todas as dificuldades enfrentadas com os métodos tradicionais, propondo uma solução utilizando impressão digital, com armazenamento das frequências na nuvem, com relatórios de frequência e notificação por Serviço de Mensagens Curtas (SMS) para os responsáveis do aluno. Para isso se utilizou um Raspberry Pi, juntamente com um scanner de impressão digital, um teclado 4x4 e uma tela *display* de cristal líquido (LCD), sendo todos esses componentes conectados através do Raspberry, o sistema deverá possuir acesso a internet para poder se conectar com a nuvem, sendo a Google cloud⁵, a utilizada na pesquisa, utilizando os serviços: Google App Engine: utilizada para construir e hospedar aplicação *web*, que foi construída utilizando a linguagem de programação PHP; Google Compute Engine: usada para provisionar uma máquina virtual, em que funciona uma aplicação baseada em Node.js que funciona como um gatilho para disparar os SMS, utilizando o serviço da Twilio⁶; Google Cloud SQL: para armazenamento das informações; Google Scripting: para Semanalmente gerar e enviar relatórios em formato Portable Document Format(PDF).

⁵ <https://cloud.google.com/>

⁶ <https://www.twilio.com/>

Masalha e Hirzallah (2014) desenvolveram uma solução para o desafio da marcação de presença de alunos em ambientes acadêmicos, focando especificamente em turmas numerosas, onde o processo manual é muito custoso, utilizando tecnologia *mobile* com a utilização de *Quick response (QR) codes*, utilizando, reconhecimento facial com verificação de localização. Tendo-se dois módulos distintos para compor a solução, um módulo do servidor e um módulo *mobile*. O módulo do servidor ficou responsável por: mediar as solicitações de frequência dos estudantes pelo sistema eLearning; Gerar um *QR code* para o instrutor; Performar validação de identidade; Performar validação de localização. O instrutor precisa inserir o *QR code* gerado em sua apresentação e permitir que os discentes possam escaneá-lo. O módulo móvel é instalado nos *smartphones* dos alunos que devem, após escanear o *QR code*, escanear suas faces, o sistema irá enviar para uma checagem as imagens justamente com a localização sendo utilizada como uma autenticação de vários fatores, para garantir a integridade dos dados.

4.1 Comparativo do estado da arte

São apresentadas as características e diferenças entre os trabalhos relacionados e este trabalho, dispondo de uma visão comparativa, apresentando assim uma perspectiva abrangente das características de cada trabalho (ver Quadro 4).

Quadro 4 - Comparação entre os trabalhos relacionados e este trabalho.

Trabalhos	Utiliza computação em nuvem	Nível de intrusividade	Despesas pré-operacionais	Nível de elasticidade	Alta Disponibilidade
Sales (2022)	Não	Baixo	Indefinido	Indefinido	Não
Godswill <i>et al.</i> (2018)	Sim	Baixo	Sim	Baixo	Não
Mittal <i>et al.</i> (2017)	Sim	Médio	Sim	Alto	Não
Yadav <i>et al.</i> (2019)	Sim	Muito baixo	Sim	Baixo	Não
Masalha e Hirzallah (2014)	Não	Alto	Indefinido	Baixo	Não
O presente trabalho	Sim	Baixo	Não	Alto	Sim

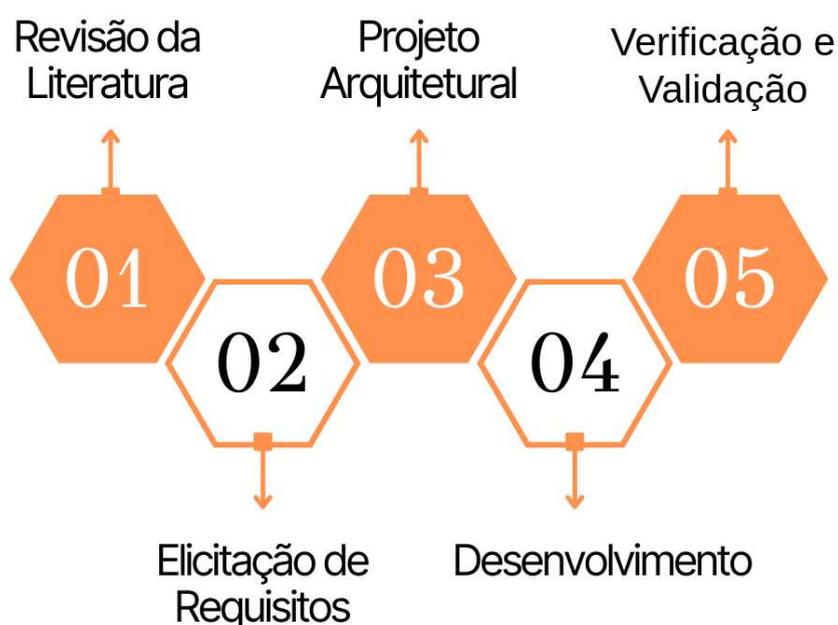
Fonte: elaborado pelo autor (2023).

O Quadro 4 é uma comparação entre o presente trabalho e algumas pesquisas relacionadas. Pode-se perceber, que o presente trabalho se diferencia ao incorporar a computação em nuvem, apresentando um baixo nível de intrusividade, não exigindo despesas pré-operacionais, oferecer alto nível de elasticidade e garantindo alta disponibilidade operacional. Essas distinções ressaltam a singularidade e a contribuição do presente estudo em contrapartida com as abordagens existentes na literatura.

5 METODOLOGIA

Nesta seção, será apresentada a metodologia utilizada para o desenvolvimento desta pesquisa. O desenvolvimento do sistema foi planejado e estruturado nas seguintes etapas (ver Figura 2).

Figura 2 - Etapas do desenvolvimento do sistema



Fonte: elaborada pelo autor (2023).

Apresentando-se os fluxos do processo de desenvolvimento desta pesquisa, dividida em cinco seções principais, que serão aprofundadas ao decorrer deste trabalho.

5.1 Revisão bibliográfica

Para a realização da revisão bibliográfica se utilizou de alguns repositórios de literatura acadêmica, foram utilizados nesta pesquisa: *google acadêmico*⁷, *IEEEExplore*⁸, *ResearchGate*⁹, *Elsevier*¹⁰ e *Scientific Electronic Library Online*¹¹. A fim de entender mais o

⁷ <https://scholar.google.com/>

⁸ <https://ieeexplore.ieee.org/>

⁹ <https://www.researchgate.net/>

¹⁰ <https://www.elsevier.com/>

¹¹ <https://www.scielo.org/>

problema e vislumbrar possíveis requisitos a serem adotados.

Durante essa fase foram utilizados vários termos para realizar as buscas nos repositórios supracitados, a fim de identificar as contribuições existentes realizadas por pesquisadores e profissionais, que utilizaram temas semelhantes. Termos em inglês e português foram utilizando como “reconhecimento facial”, “controle de presença”, “Computação em nuvem”, “*attendance control*”, “*facial recognition*”, “*biometric attendance*”, “*biometric access control*”, “*machine learning in attendance systems*”, “*cloud computing*” empregados para explorar efetivamente as contribuições da comunidade acadêmica num âmbito internacional e obter assim uma visão abrangente.

Atualmente, há uma gama de opções de nuvens públicas disponíveis no mercado, todavia, buscando uma opção que traga robustez, confiabilidade e soluções inovadoras, este trabalho optou pela Amazon Web Services. Conforme o estudo analítico e comparativo elaborado por Saraswat e Tripathi (2020), “Avaliando as nuvens Amazon Web Service, Microsoft e Google Cloud Provider”, a Amazon lidera o mercado de IaaS e PaaS com uma fatia de 47,8% e 34% do mercado, evidenciando sua maturidade e abrangência dos serviços oferecidos em relação aos seus competidores.

Outrossim, as abordagens mais eficientes para reconhecimento facial utilizam *deep learning*. Por essa razão, para este projeto foi escolhido uma ferramenta que utiliza essa metodologia, além de possuir toda a versatilidade da computação em nuvem, se utilizando do *Amazon Rekognition*.

Como documentado pela Amazon Web Services (2023a), o Amazon Rekognition é um serviço que utiliza o modelo de *deep learning*, que continua a evoluir, aumentando sua acurácia com base nos comentários dos clientes e na evolução das pesquisas de *deep learning*. Com isso, ele é capaz de reconhecer faces e identificar rostos presentes em uma coleção.

Os resultados obtidos com as as etapas de levantamento de requisitos estão descritos no capítulo 6.3.

5.2 Elicitação de requisitos

A etapa de levantamento de requisitos desempenha um papel crucial para o processo de um desenvolvimento, pois é nela que se descobrem as principais necessidades e prioridades dos *stakeholders* (Sommerville, 2019, p. 96). A elicitação de requisitos pode ser realizada utilizando várias técnicas para compreender melhor as necessidades e dores dos usuários. Neste trabalho, foram utilizadas as técnicas:

- **Questionário:** Técnica de pesquisa que colhe declarações imparciais e precisas dos *stakeholders*, colhendo grande quantidade de informação em pouco tempo, não se possuindo respostas imediatas, podendo conter falhas que só serão identificadas após a avaliação (Pohl; Rupp, 2015, p. 44).
- **Benchmarking:** Processo de comparação sistemática entre produtos ou serviços a fim de identificar as melhores práticas e abordagem e utilizá-las de forma a evitar os erros e falhas cometidos, com o propósito de se ter um produto ou serviço melhor. (Elmuti; Kathawala, 1997).
- **Revisão bibliográfica:** Abordagem de análise de conteúdos produzidos, verificando diferentes ideologias e perspectivas de maneira crítica, sendo utilizadas como bases para guiar as decisões da pesquisa. (De lunetta; Guerra. 2023).

5.2.1 Benchmarking

O *Benchmarking* é um procedimento amplamente utilizado na área da ciência da computação, em particular, para comparar ferramentas ou algoritmos a fim de levantar requisitos essenciais de maneira confiável, comparando os resultados encontrados e, assim, ampliando a competitividade e a inovação. (Beyer;Löwe;Wendler, 2019).

Na etapa de revisão bibliográfica, foram vislumbradas diversas pesquisas. Em seguida, foram realizadas leituras aprofundadas para filtrar os trabalhos mais recentes e que mais se assemelham a este, para no fim, identificar padrões e funcionalidades específicas. As seguintes pesquisas foram destacadas para a extração de requisitos: Godswill *et al*(2018); Rao (2022).

Os requisitos levantados partem de diferentes ambientes do qual se baseia está pesquisa, sendo realizado ajustes nos agentes e contextos para englobarem os possíveis usos do presente trabalho.

5.2.2 Questionário

Como explicado por Pohl e Rupp (2015) o questionário consegue elicitir uma gama de informações em um curto período de tempo a um baixo custo utilizando de perguntas abertas ou fechadas com múltiplas escolhas sendo altamente eficiente para coletar requisitos de uma grande quantidade de participantes, podendo ser executado de maneira *online* ou presencial.

Para a realização da pesquisa foi desenvolvido um Termo de Consentimento Livre e Esclarecido (TCLE), que pode ser visto no apêndice B, conforme as diretrizes e normas de regulamento para pesquisas envolvendo humanos definidas pelo Ministério da saúde (BRASIL, 2012b. p. II.23).

II.23 - Termo de Consentimento Livre e Esclarecido - TCLE - documento no qual é explicitado o consentimento livre e esclarecido do participante e/ou de seu responsável legal, de forma escrita, devendo conter todas as informações necessárias, em linguagem clara e objetiva, de fácil entendimento, para o mais completo esclarecimento sobre a pesquisa a qual se propõe participar

O questionário foi escolhido como uma alternativa para levantar requisitos do sistema em virtude de sua praticidade e baixo custo. Nesse sentido sua aplicação de maneira *online* promove uma ampla coleta de dados por alcançar uma gama maior de participantes.

A coleta se sucedeu de forma digital utilizando a ferramenta *Google Forms*¹², e esteve disponível por um período de 7 dias, do dia 29/09/2023 até o dia 06/10/2023. Composto por um total de 6 perguntas, sendo utilizadas diferentes técnicas para coleta de informações. Entre elas, perguntas demográficas, para mapear a faixa etária dos participantes, perguntas dicotômicas, com respostas simples e objetivas, perguntas de múltiplas escolhas, para entender os diferentes cenários no qual o usuário está inserido. Além disso, foi utilizado a escala Likert, para medir a intensidade que a realização de frequência está relacionada com os participantes. Todas as perguntas e as alternativas de resposta podem ser visualizadas através do apêndice A.

¹² <https://workspace.google.com/products/forms/>

5.3 Projeto Arquitetural

O projeto arquitetural é uma planta estrutural e organizacional de um sistema, sendo assim, são analisadas todas as necessidades, para que assim defina-se a abordagem mais adequada para sanar as necessidades do projeto, abrangendo todo seu ciclo de vida. (Jaiswal, 2019)

O desenvolvimento de sistema para nuvem, apresenta diversos desafios, devido a toda a versatilidade da nuvem definir uma arquitetura pode ser uma tarefa mais complexa que o normal.

Para este trabalho será utilizado o *framework* AWS-Well Architected, que como definido pela própria Amazon web services (AWS) (2023b) o *AWS Well-Architected* é um conjunto de práticas recomendadas para a projetar e operar arquiteturas em nuvem, orientado a criação de sistemas para atender aos requisitos de excelência operacional, segurança, performance, sustentabilidade, otimização de custos e confiabilidade.

Como observador por Salmijärvi (2023) o *framework* AWS *Well-Architected* sugere a reavaliação constante da arquitetura do sistema, realizando assim nas diversas etapas do desenvolvimento do sistema, com uma concepção coletiva de toda a equipe, tendo como resultado dessas reuniões pode ser visto em ações de aprimoramento da estrutura do sistema.

5.3.1 Arquitetura REST

A arquitetura utilizada na aplicação é a *Representation State Transfer* (REST) que é um estilo arquitetural muito utilizado em APIs e como dito por Azevedo (2020). A arquitetura REST é um conjunto de regras e princípios que se utilizados garantem: usabilidade, simplicidade, escalabilidade e extensibilidade, tornando os serviços independentes e escaláveis requisitos essenciais em ambientes em nuvem.

A arquitetura REST foi definida por Roy Thomas Fielding em sua tese de Doutorado, nos apresentando esse estilo arquitetural, na qual se estabelece restrições para esse novo modelo arquitetural, conforme Fielding (2000):

- **Cliente servidor:** Separando a interface do usuário do acesso aos dados, desacoplando e promovendo a portabilidade do servidor a múltiplas plataformas promovendo escalabilidade com a separação dos componentes.

- **Stateless (sem estado)** : Não há armazenamento de estado, sendo assim cada interação deve conter tudo que seja preciso para que o servidor realize o processamento, não armazenando informações dos clientes.
- **Interface Uniforme:** Estabelece uma interface uniforme entre os componentes, para com isso simplificar e padronizar a interação, promovendo interoperabilidade em toda sua camada.
- **Sistema em camadas:** A arquitetura poderá ter camadas hierárquicas, encapsulando serviços
- **Cache:** É uma restrição facultativa, buscando evitar diminuir a necessidade de interação do cliente com o servidor, promovendo eficiência, desempenho e escalabilidade para o cliente.
- **Código sob demanda:** É uma restrição facultativa, que permite o cliente acessar a pequenas funcionalidades e baixá-las através do servidor, que envia ao cliente *applets* ou *scripts* promovendo extensão das funcionalidades do cliente.

O sistema desenvolvido fundamenta-se nos princípios da arquitetura REST, atendendo às necessidades de ambientes em nuvem. A estrutura cliente-servidor assegura a modularização dos componentes do sistema, ocasionando a escalabilidade independente de cada módulo otimizando assim os recursos na nuvem. Devido a ausência do armazenamento de estado, obtém-se interoperabilidade do servidor, deste modo cada interação com o servidor é independente proporcionando operar de maneira distribuída, facilitando o balanceamento de carga e escala tanto horizontal como vertical.

5.3.2 Segurança da Aplicação

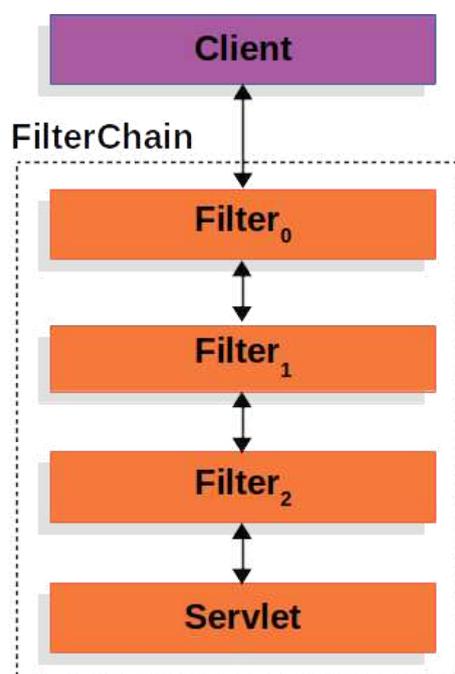
Com base nos requisitos do sistema, foram estabelecidos três papéis principais: usuário, monitor e administrador. A abordagem de controle de acesso mais adequada a essa necessidade é a *Role-based access control (RBAC)*, que se baseia em papéis pré-definidos, conseqüentemente é essencial definir o processo para garantir este controle de acesso à

aplicação atendendo as necessidades de segurança de ambientes em nuvem.

5.3.2.1 Spring Security

O Spring security é um *framework* do ecossistema spring, utilizado para controle de acesso, autenticação e autorização, oferecendo uma arquitetura modular altamente customizável, como pode ser ratificado pela Figura 3.

Figura 3 - Arquitetura Spring security.



Fonte: Spring (2024).

Devido à arquitetura modular, é possível a criação de filtros independentes, com o princípio da responsabilidade única, facilitando assim a adição de novos filtros, e mantendo-os independentes entre si.

Além disso, o spring *security* é compatível com uma gama de outros *frameworks*, proporcionando uma segurança a toda aplicação. No entanto, nem sempre ele é capaz de atender todas as necessidades do sistema.

5.3.2.2 oAuth2

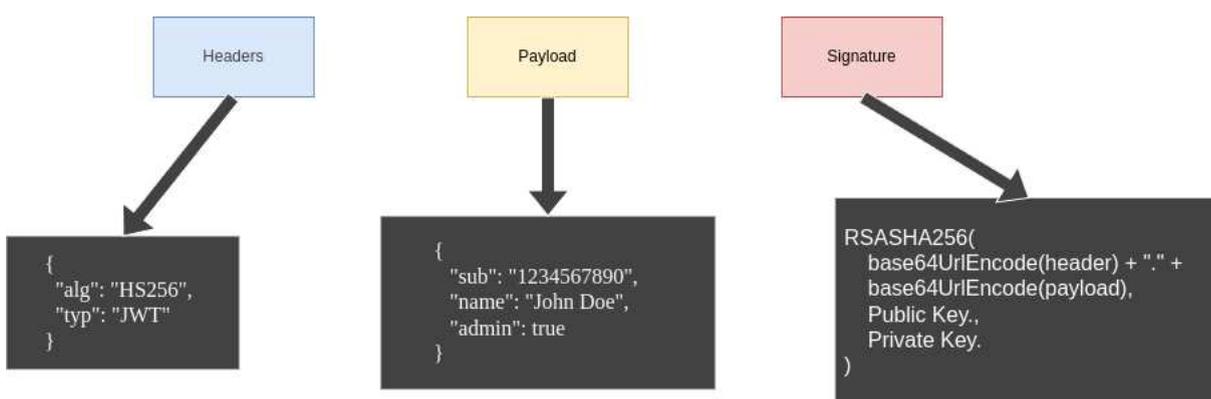
O oAuth2 é um protocolo de autenticação que permite o acesso a recursos sem a necessidade de expor as credenciais do usuário, suportando fluxos diversos de autorização, sem manter o estado no servidor.

Sua utilização se limita autenticação, por isso precisamos promover autorização de outra maneira e para isso utilizaremos também JSON Web Tokens (JWT) para permitir assim manter sessões do usuário de maneira descentralizada não guardando estado no servidor através do oAuth2 e criar *tokens* de acesso para o usuário de forma compacta e segura.

5.3.2.3 JSON Web Token (JWT)

O JSON Web Token (JWT) possui uma estrutura composta por três segmentos essenciais, como se visualiza na Figura 4, sendo eles, o cabeçalho (*headers*), carga (*payload*) e assinatura (*signature*). O cabeçalho especifica o algoritmo de assinatura que está sendo utilizado. A carga contém as informações relevantes sobre o usuário como identificação e permissões. Por fim, a assinatura digital é gerada combinando o cabeçalho e a carga, e assinando-os com as chaves usando o algoritmo especificado.

Figura 4 - Camadas do Json Web Token

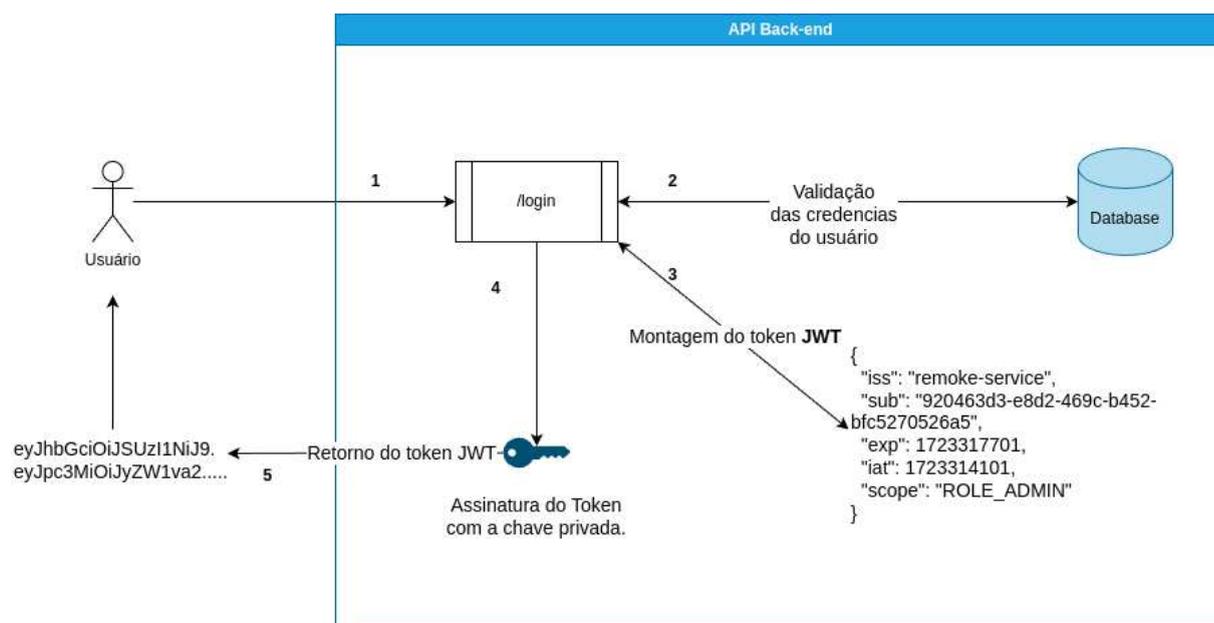


Fonte: elaborado pelo autor (2024).

O gerenciamento da autorização e autenticação opera com *tokens* seguros, gerados por criptografia assimétrica, com chaves públicas e privadas. No momento em que o usuário se autentica ao sistema suas credenciais são validadas, e caso sejam validadas, um *token* JWT é gerado.

O *token* gerado possui todas as informações necessárias sobre o usuário para que ele possa utilizar o sistema, de maneira autossuficiente, sem necessidade de serviços externos. Além disso, o conteúdo do token é assinado, garantindo que os dados não sejam alterados, como representado na Figura 5.

Figura 5 - Arquitetura da aplicação com Json Web Token.



Fonte: elaborado pelo autor (2024).

5.3.2.4 Cross-Origin Resource Sharing (CORS)

Cross-Origin Resource Sharing é um mecanismo de segurança que define como sistemas de domínios diferentes podem interagir e acessar recursos uns dos outros. O CORS define a política de acesso entre origens estabelecendo, quais origens podem interagir e utilizar recursos uns dos outros, conforme ilustrado na Figura 6.

Figura 6 -Requisição entre domínios diferentes.



Fonte: elaborado pelo autor (2024).

A sua importância é extrema para a segurança do servidor, pois através dela que definimos quais origens, cabeçalhos e métodos podem ser usados, garantindo isolamento dos recursos e um controle granularidade sobre as interações. Em ambientes em nuvem, onde diversos serviços podem ser conectados de múltiplas origens diferentes, ter esse controle é crucial para evitar ataques de origem cruzada protegendo o servidor e seus recursos.

5.3.2.5 Cabeçalhos de segurança

A aplicação de cabeçalhos de segurança no servidor para garantir a segurança do serviço e dos usuários na *web*. Os cabeçalhos são enviados juntos com as respostas das chamadas HTTP, estabelecendo algumas regras de navegação e acesso, mitigando tentativas de ataque.

Na perspectiva do sistema, a configuração dos cabeçalhos, dentro dos padrões seguros, fornece uma camada de segurança contra ataques, assegurando assim a integridade dos dados tanto do cliente quanto do servidor.

5.4 Desenvolvimento

Nesta seção, abordaremos detalhadamente os elementos relacionados com o desenvolvimento do sistema.

5.4.1 Tecnologias utilizadas

Com base nos requisitos coletados e da necessidade da flexibilidade de uma linguagem para o seu funcionamento em ambientes em nuvem, a linguagem escolhida para desempenhar o papel foi o Java, devido a toda sua robustez e desempenho, adjunto da poderosa Java Virtual Machine (JVM), que possibilita a execução do sistema em qualquer dispositivo tornando a solução portátil e flexível, livre de qualquer sistema operacional ou arquitetura de *hardware*.

Conforme as necessidades de uma aplicações nativas em nuvem, se utilizar o *framework* spring que conforme *Spring* (2023), o spring possibilita de maneira fácil o desenvolvimento de arquiteturas baseadas em micro serviços na nuvem, de forma segura, monitorando as dependências de terceiros tratando de maneira ágil as questões de segurança, fazendo seu código ‘nativo na nuvem’, possuindo uma série de serviços para desenvolver sua aplicação funcionar na nuvem, sendo um *framework* java significativamente popular.

Para o armazenamento dos dados se utilizará um banco de dados relacional e de código aberto. O MariaDB¹³ foi escolhido por oferecer uma solução de armazenamento robusta e de fácil manutenção, acatando às exigências de escalabilidade e segurança.

5.4.2 Processo de Prototipação

Para facilitar o desenvolvimento do sistema, foi pretendida a elaboração de um protótipo da interface como prova de conceito dos requisitos observados. Ademais, esse processo assegura que as decisões de *design* e arquitetura do sistema estão alinhadas com os requisitos funcionais, não funcionais e regras de negócio do sistema.

O protótipo auxilia na identificação de potenciais problemas antes de prosseguir com o desenvolvimento. Com isso conseguimos validar as propostas e a, evitando-se retrabalhos, sendo fundamental para a etapa de desenvolvimento

5.4.3 Processo de desenvolvimento

O processo de desenvolvimento de um sistema pode ser bastante desafiador, mediante a todas as mudanças internas ou externas que podem impactar nas etapas do ciclo de vida de um sistema. Para enfrentar essa dificuldade, as metodologias ágeis de

¹³ <https://mariadb.org/>

desenvolvimento de *software* são frequentemente adotadas.

Neste trabalho, se utilizará da metodologia ágil *scrum* com uma adaptação para encaixar a metodologia *kanban*, dividindo o processo de desenvolvimento em *sprints*, com a organização do *backlog* em um quadro, organizando as tarefas em colunas, realizando a cada nova *sprint* uma priorização dinâmica nas tarefas a serem desenvolvidas.

5.4.4 Recursos

Para o desenvolvimento do sistema se reservou um dispositivo com as seguintes configurações:

- Processador: AMD *Ryzen 7 6800H*.
- Placa de vídeo: Geforce RTX 3070 TI
- Memória RAM: 16GB.
- Armazenamento: 2TB.
- Sistema Operacional: *Linux Mint 20.3 Cinnamon*

A fim de realizar a prototipação do sistema, será utilizado o Figma¹⁴, que possui uma versão gratuita para estudantes. Essa versão disponibiliza recursos avançados de prototipação e *design* de interfaces, de forma gratuita impulsionando assim o desenvolvimento dos estudantes.

Para o desenvolvimento do sistema e implantação na nuvem, se utilizará uma conta AWS que se enquadra no nível gratuito disponibilizado pela Amazon. Essa abordagem permitirá realizar a integração com a nuvem de maneira eficaz, aproveitando os recursos oferecidos sem nenhum custo associado.

5.4.5 Lei Geral de Proteção de Dados Pessoais (LGPD).

No Brasil, a Lei Geral de Proteção de Dados Pessoais ainda é relativamente nova para muitas empresas, que precisaram adotar suas práticas para coletar, armazenar e tratar os dados pessoais. Para assegurar a implementação, fiscalização e cumprimento da LGPD no Brasil, foi instaurada a Autoridade Nacional de Proteção de Dados (ANPD), um órgão federal. A atuação da ANPD é imprescindível para assegurar que empresas, como a Amazon

¹⁴ <https://www.figma.com/>

Web Services (AWS), estejam em conformidade com as exigências legais atuais.

A Amazon Web Services admite um modelo de responsabilidade compartilhada, isso implica que, as conformidades legais são uma responsabilidade tanto da AWS como dos seus clientes, devido a AWS não possui visibilidade do que é carregado em sua rede, os clientes devem garantir também sua conformidade com as normas legais, como a LGPD.

Nesse sentido, a AWS garante a criptografia de dados, sejam eles em trânsito ou dados armazenados, seja em memória volátil ou não volátil, além de assegurar a segurança de toda a sua infraestrutura, possuindo as certificações de garantia de segurança organizacional: o ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI DSS Level 1 e SOC 1, 2 e 3.

No cenário atual da LGPD, o armazenamento de imagens é considerado um dado pessoal e sensível. Por isso, está sujeito a toda jurisprudência de dados pessoais, conforme o Capítulo II seção IV:

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: **I** - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; **II** - fim do período de tratamento; **III** - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou **IV** - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018, Cap. II, Seção IV)

Conforme definido na legislação após o período do tratamento, os dados devem ser excluídos. Um prazo de dois anos foi estabelecido para que os dados pudessem ser processados, auditados e, finalmente, deletados, sendo sua data de expiração ato de seu armazenamento. Entretanto, caso o usuário solicite a exclusão de sua conta, os mesmos serão deletados imediatamente.

Para garantir a transparência necessária aos usuários, foi desenvolvido uma política de privacidade do sistema, que especifica os dados que são coletados, a finalidade do uso dos dados, direitos do titular dos dados e segurança dos dados. Estando disponível para consulta proporcionando um canal aberto para esclarecimento de dúvidas. O termo pode ser visualizado no apêndice C.

5.5 Verificação e Validação

“A validação do *software*, ou em termos mais gerais, verificação e validação (V & V), destina-se a mostrar que um sistema está em conformidade com sua especificação e que satisfaz as expectativas do cliente do sistema” (Sommerville, 2019, p. 219).

O processo de validação e verificação de um *software* deve ocorrer de maneira contínua em todas as fases do desenvolvimento, em virtude de garantir a correspondência do produto final com os requisitos definidos.

Como constatado por Pizzaia e Malara (2022), o mercado de *software* enfrenta desafios para lidar com as necessidades dinâmicas e imediatistas dos clientes, buscando assim as empresas por mais agilidade na entrega de produtos. A adaptação ágil se torna crucial, mas também a qualidade do *software* se torna um fator conjunto, assim, a agilidade não deve comprometer a qualidade do produto.

Neste trabalho, serão utilizados conceitos para garantir a conformidade, visando entregar um sistema de maneira confiável e eficaz. A integração das práticas ágeis no seu processo de desenvolvimento irá garantir um *software* que atenda aos requisitos e padrões de qualidade.

- **Monitoramento:** Será utilizado no desenvolvimento do sistema um mecanismo de monitoramento, para acompanhar em tempo real as atividades realizadas pelo sistema, registrando assim as informações pertinentes para diagnósticos e soluções de problemas.
- **Testes de conformidade:** Nas próximas etapas da pesquisa, serão elucidados os regulamentos, normas e políticas de segurança da informação, garantindo a sua conformidade em todo processo de desenvolvimento, garantindo a concordância do sistema com os requisitos internos e aos regulamentos externos à solução.
- **Revisão de requisitos:** Ao final da pesquisa será apresentada a revisão dos requisitos do sistema a fim de garantir a compreensão, definição e integridade dos requisitos, sem alteração na proposta do sistema, sendo um processo contínuo em todas as etapas de desenvolvimento do sistema.

- **Testes de integração:** Os testes de integração ao final do desenvolvimento dos módulos do sistema, serão apresentados os testes de integração entre todos os componentes do sistema, evitando assim, problemas de incompatibilidade entre as partes do sistema.

6 RESULTADOS

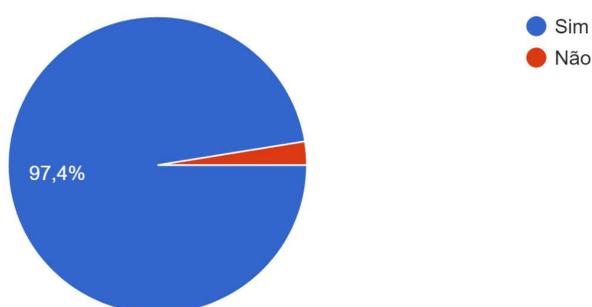
Neste capítulo estão expostos os resultados obtidos ao longo do desenvolvimento desta pesquisa. No capítulo 6.1 se é apresentando os resultados obtidos com a aplicação do questionário. O capítulo 6.2 evidencia os resultados da realização do *benchmarking*. Já no capítulo 6.3, é descrito todos os requisitos identificados no durante o curso de desenvolvimento da pesquisa. No capítulo 6.4 relatamos os modelos arquitetural alcançados com a aplicação. O capítulo 6.5 apontamos os pontos se seguranças cumpridos. Já no capítulo 6.6 observamos o protótipo desenvolvido com base nos requisitos elicitados. Por final temos o capítulo 6.7 contendo os resultados do monitoramento da aplicação.

6.1 Aplicação do Questionário

A aplicação do questionário teve como objetivo elicitare requisitos para o sistema e verificar a viabilidade da solução e evidenciar o uso da aplicação em diferentes contextos organizacionais. Na Figura 7 é observado a aceitação dos participantes à pesquisa.

Figura 7 - Questionário aceitação - Respostas 01.

Desde já agradecemos! Aceita Participar desta pesquisa?
39 respostas



Fonte: elaborado pelo autor (2023).

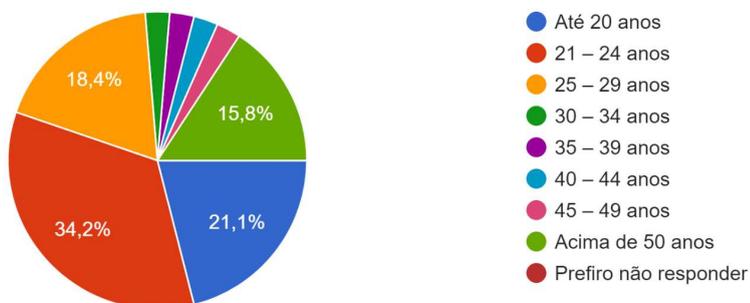
O questionário obteve um total de 39 Respostas, tendo um total de 38 (97,4%) participantes concordantes com a participação da pesquisa e 1 (2,6%) que não aceitou a participação, não permitindo assim sua continuação no preenchimento do formulário.

Na Figura 8 é possível ver as faixas etárias dos participantes.

Figura 8 - Questionário faixa etária

Faixa Etária

38 respostas



Fonte: elaborado pelo autor (2023).

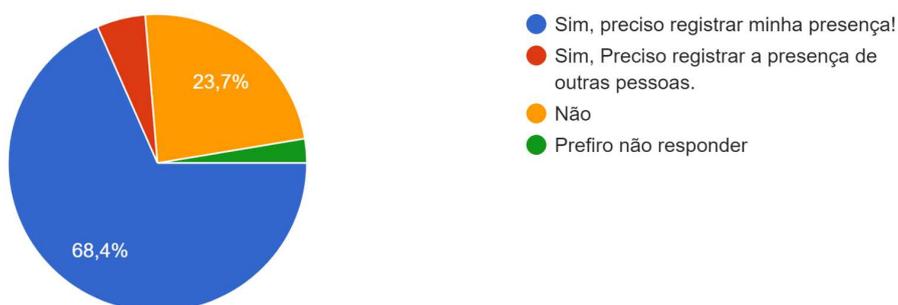
Em relação à faixa etária foi observado que o grupo respondentes apresenta uma faixa etária distribuída, porém a faixa etária mais predominante é jovem dos 20 aos 29 anos.

A Figura 9 apresenta o resultado da realização de frequência pelos participantes.

Figura 9 - Questionário registro de presença

Normalmente você precisa registrar sua presença ou de outras pessoas?

38 respostas



Fonte: elaborado pelo autor (2023).

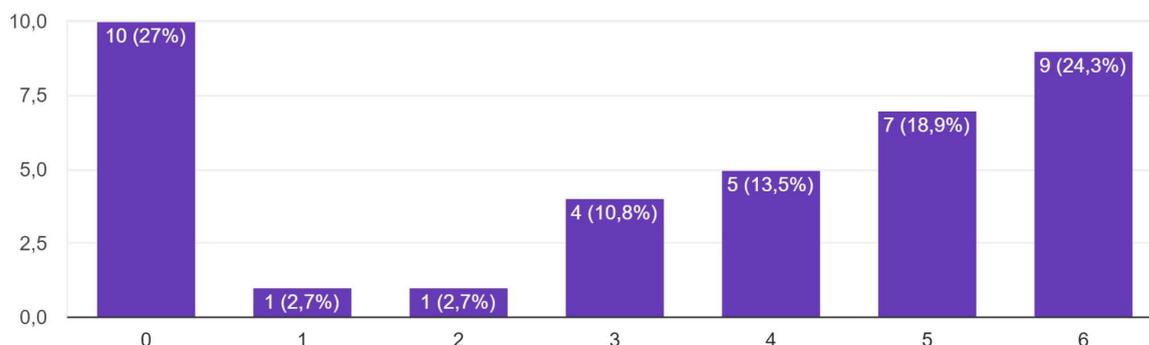
Em relação à necessidade da realização da frequência se observou que 28 pessoas (73,7%) precisam registrar frequência seja sua ou de terceiros.

Na Figura 10 é apresentado o gráfico de constância de realização de frequência.

Figura 10 - Questionário frequência registro de presença - Respostas 04.

Com que frequência você precisa registrar sua presença ou a de outras pessoas?

37 respostas



Fonte: elaborado pelo autor (2023).

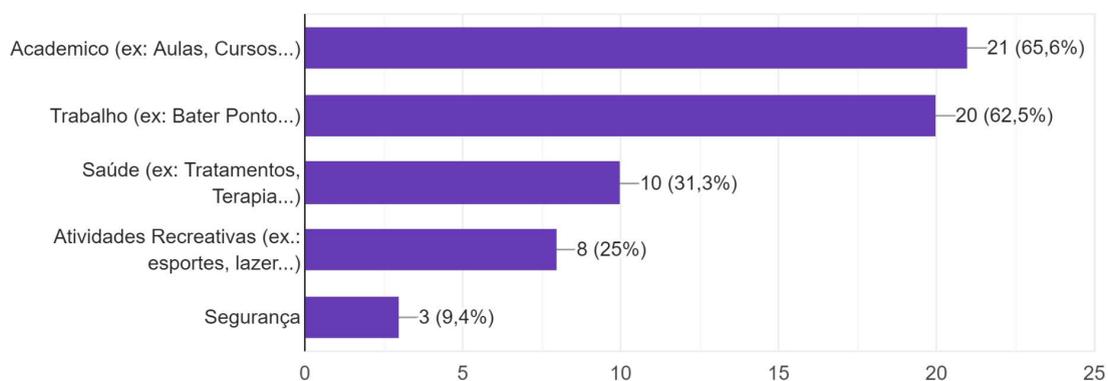
Em relação à periodicidade em que se computa a frequência, a fim de mensurar a assiduidade, se observou que 21 pessoas (56,7%) tem uma necessidade maior de realizar a frequência, 4 pessoas (10,8%) tem uma necessidade moderada e 12 pessoas (32,4%) pouca ou nenhuma necessidade de realizar frequências.

É observado na Figura 11 os ambientes onde ocorrem a realização da frequência.

Figura 11 - Questionário ambientes de captura de presença - Respostas 05.

Caso precise registrar frequência em quais tipos de ambiente ela ocorre?

32 respostas



Fonte: elaborado pelo autor (2023).

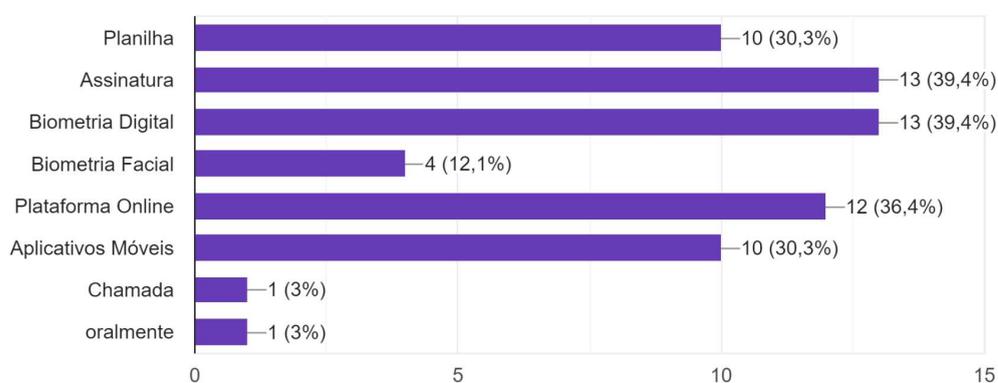
Com relação aos ambientes que ocorrem a tarefa de computação de presenças se constatou que no meio acadêmico e ambiente de trabalho se há uma predominância maior da realização de frequências, os respondentes tinham a opção de escolher mais de um ambiente e também responder com outro tipo de ambiente não listado.

Na Figura 12 se é vislumbrado os métodos de captura de frequência.

Figura 12 - Questionário métodos de realização de frequência - Respostas 06

Caso você precise computar sua frequência de que maneira ela é realizada

33 respostas

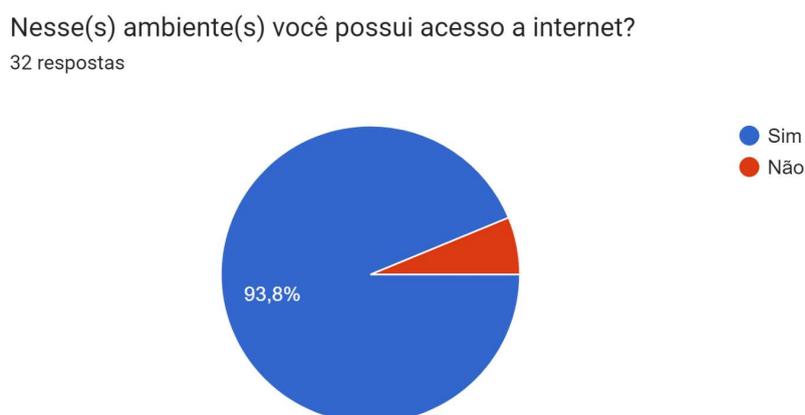


Fonte: elaborado pelo autor (2023).

Nota-se que há uma variedade de técnicas para a realização da frequência, se destacando as metodologias de assinatura, biometria digital, plataforma *online* e planilhas, foram inseridos algumas metodologias mais utilizadas, dando-se também a opção do respondente inserir alguma metodologia não listada.

A Figura 13 revela a disponibilidade de acesso a *internet* por parte dos participantes nos ambientes de realização de frequência.

Figura 13 - Questionário acesso a internet - Respostas 07.



Fonte: elaborado pelo autor (2023).

Nos ambientes que são realizadas essas frequências 30 respondentes (93,8%) apresentam acesso a *internet* e 2 respondentes (6,3%) não tem acesso a *internet*, mostrando que de forma predominante os respondentes possuem em sua maioria acesso nos ambientes de realização de frequência.

Com base no questionário realizado conseguimos tirar algumas conclusões. Verificamos que há diversidade de ambientes em que há necessidade de realização de frequência, com isso constatamos a diversa necessidade de realização de frequência em múltiplas áreas, atendendo a um público de faixa etária variável é que em sua grande maioria possui acesso a *internet*.

6.2 Aplicação do *Benchmarking*

Segundo o estudo de Godswill *et al* (2018) foi proposto um sistema de controle de frequência voltado para instituições educacionais, denominado FACECUBE, isto é através da tecnologia de reconhecimento facial que viabiliza a captura de faces a distância simplificando o processo de presença. Além disso, faz uso do paradigma da computação em nuvem, para assim se obter um sistema automatizado de gestão de presença.

A utilização de múltiplos papéis de usuários mostrou-se bastante promissora, possibilitando a divisão de tarefas gerenciais e evitando sobrecarregar em um único tipo de usuário. Isso cria uma hierarquia de usuários, facilitando o gerenciamento e gestão da

plataforma. Por fim os requisitos identificados através da análise do sistema FACECUBE foram os seguintes (ver Quadro 5)

Quadro 5 - Requisitos *Benchmarking* Godswill

Requisito	Descrição
Sistema de papéis de usuário	O sistema apresenta 3 tipos de usuários diferentes
Registro em turmas	Todos os usuário podem realizar seu cadastro em turmas
Visualização de horário	Todos os usuários podem visualizar o horário de sua turma
Configuração de horário de turmas	Os instrutores e administradores podem realizar a configuração do horário de uma turma
Gerenciamento da presença	Os instrutores e administradores podem após a presença gerar a qualquer momento a lista de frequência.
Gerência da aplicação	Toda gestão da aplicação e das atividades administrativas é de responsabilidade dos usuários administradores

Fonte: elaborada pelo autor (2023).

Conforme desenvolvido por Rao (2022) se é proposto um sistema chamado AttenFace para realizar o controle de presença, utilizando o reconhecimento facial em tempo real, para analisar, rastrear e conceder a presença aos aluno, a análise das faces acontece a cada 10 minutos, evitando uma sobrecarga dos recursos, o sistema opera de maneira totalmente autônoma.

O sistema proposto é dividido em módulos independentes, que facilita a manutenção do sistema, sendo assim mudanças em regras de negócio não impactam outros componentes, possibilitando a substituição e reutilização dos módulos devido ao baixo acoplamento, se mostrando coincidente com as necessidades de uma ambiente em nuvem. Os requisitos extraídos podem ser vistos no Quadro 6.

Quadro 6 - Requisitos *Benchmarking* Rao

Requisito	Descrição
<i>Login</i> no sistema	Os usuários precisam realizar <i>login</i> no sistema independente do seu papel
Painel <i>dashboard</i>	Painel que permita na visão dos alunos a visualização de detalhes de suas presenças. Na visão dos professores a visualização da presença de todos os alunos pertencentes a sua(s) turma(s).
Edição de presença	Administradores podem manualmente editar as presenças, realizando abono de faltas ou indicar ausência, através do painel do sistema
Limite de faltas	Professores podem determinar o limite de faltas para cada turma
Frequência por reconhecimento facial automática.	O sistema deve realizar a frequência de forma automática após a captura da imagem.
Multiplataforma	O sistema deve permitir seu uso através de multiplataformas com ênfase em <i>mobile friendliness</i>
Paralelismo	Sistema deve ser capaz de realizar processamento de forma paralela, para ser utilizado por múltiplas classes(organizações)
Visualização de frequência	Após a realização da frequência o usuário poderá verificar o status da sua presença no portal.
Módulo <i>front-end</i>	Possuir um módulo front-end possuindo acesso através da <i>web</i> ou <i>mobile</i>
Módulo <i>back-end</i>	Lidar com as interações dos usuários com o sistema, gerenciando o processo de reconhecimento facial e conexão com banco de dados.
Banco de dados	módulo responsável por armazenar as informações sobre os usuários e suas presenças, cursos e regras de frequência.

Fonte: elaborada pelo autor (2023).

Os sistemas FACECUBE, proposto por Godswill *et al.* (2018), e AttenFace, proposto por Rao (2022), nos revelam um indicativo de avanço do estudo da arte no que tange o uso de reconhecimento facial no controle de presença. Ambos os sistemas são projetados para ambientes em nuvem e adotam uma abordagem modular. A adoção de múltiplos papéis

de usuários, além da modularização da aplicação, endossa a flexibilidade, eficiência operacional e acessibilidade em diferentes plataformas e contextos.

6.3 Requisitos Selecionados

Diante dos resultados da aplicação do questionário, estudos de revisão bibliográfica e análise dos estudos semelhantes, *benchmarking*, ademais das regulamentações da LGPD e regras da Amazon web service foram analisadas as necessidades encontradas se obtendo como resultado os seguintes requisitos. Para o entendimento dos requisitos considera-se as seguintes abreviações. RF: Requisito Funcional; RNF: Requisito não funcional; RN: Regra de negócio.

O Quadro 7 apresenta os requisitos funcionais considerados nesta pesquisa.

Quadro 7 - Requisitos Funcionais elicitados

Identificação	Nome	Descrição
RF001	Configuração do horário	O sistema deverá dar suporte para configuração e edição do horário de turma
RF002	Registro em turmas	Somente os usuário administradores ou monitores podem realizar cadastro de usuários em turmas
RF003	Visualização de horário	Todos os usuários podem visualizar o horário de sua turma
RF004	Configuração de horário de turmas	Os instrutores e administradores podem realizar a configuração do horário de uma turma
RF005	Geração de lista de presença	Os instrutores e administradores podem após a presença gerar a qualquer momento a lista de frequência.
RF006	<i>Login</i> no sistema	os usuários precisam realizar <i>login</i> no sistema independente do seu papel
RF007	Painel <i>dashboard</i>	Painel que permita na visão dos alunos a visualização de detalhes de suas presenças. Na visão dos professores a visualização da presença de todos os alunos pertencentes a sua(s) turma(s).
RF008	Edição de presença	Administradores podem manualmente editar as

		presenças, realizando abono de faltas ou indicar ausência, através do painel do sistema
RF009	Limite de faltas	Professores podem determinar o limite de faltas para cada turma
RF010	Frequência por reconhecimento facial automática.	O sistema deve realizar a frequência de forma automática após a captura da imagem.
RF011	Visualização de frequência	Após a realização da frequência o usuário poderá verificar o status da sua presença no portal.
RF012	Registro de usuário	O sistema deverá permitir o registro de novos usuários, com informações básicas como nome, e-mail, data de nascimento e senha
RF013	Edição das informações do usuário	O sistema terá que permitir a edição das informações pessoais do usuário como: nome, email, senha, data de nascimento e documento.
RF014	Recuperação de senha	O sistema deverá que o usuário, já cadastrado, realize a recuperação de sua senha.
RF015	Tela inicial	O sistema deverá permitir que o usuário possa se registrar ou <i>logar</i> no sistema.
RF016	Deleção de conta	Qualquer usuário poderá deletar sua conta a qualquer momento.
RF017	Visualização das organizações	Os usuários necessitam visualizar as organizações às quais eles fazem parte.
RF018	Visualização dos grupos	Os usuários necessitam visualizar os grupos das organizações que eles fazem parte.
RF019	Acesso à política de privacidade	A política de privacidade deve ser acessível ao usuário, tanto sua compreensão quanto acesso.
RF020	<i>Download</i> relatório de presença	Os usuários administrativos e monitores podem realizar o <i>download</i> do relatório em formato csv.

Fonte: elaborado pelo autor (2023).

Foram identificados 20 requisitos funcionais, que juntos representam o conjunto de funcionalidades que o sistema deve oferecer para atender às necessidades dos usuários e alcançar os objetivos propostos.

O Quadro 8 representa os requisitos não funcionais encontrados nesta pesquisa.

Quadro 8 - Requisitos não funcionais elicitados

Identificação	Nome	Descrição
RNF001	Sistema <i>Web</i>	O Sistema deve estar disponível para os usuários na <i>web</i> .
RNF002	Amazon Rekognition	O sistema de reconhecimento de imagem deve ser integrado com o serviço Amazon Rekognition para realizar a análise de faces. O Amazon Rekognition será responsável por identificar características faciais e realizar o reconhecimento facial
RNF003	Spring boot	Para atender o máximo de produtividade e eficiência no desenvolvimento de aplicações nativas na nuvem.
RNF004	Java	Utilização dos <i>frameworks</i> disponíveis para trazer portabilidade, interoperabilidade, confiabilidade e desempenho ao projeto
RNF005	Multiplataforma	O Sistema deve ser <i>mobile-friendly</i>
RNF006	Múltiplos usuários	O Sistema deve ser capaz de lidar com múltiplos usuários simultâneas
RNF007	Paralelismo	Sistema deve ser capaz de realizar processamento de forma paralela, para ser utilizado por múltiplas classes(organizações)
RNF008	Módulo <i>front-end</i>	Possuir um módulo <i>front-end</i> possuindo acesso através da <i>web</i> ou <i>mobile</i>
RNF009	Módulo <i>back-end</i>	Lidar com as interações dos usuários com o sistema, gerenciando o processo de reconhecimento facial e conexão com banco de dados.
RNF010	Banco de dados	módulo responsável por armazenar as informações sobre os usuários e suas presenças, cursos e frequências.
RNF011	Conformidade de imagens	Após 2 anos as imagens armazenadas devem ser deletadas do sistema, sendo este o tempo

		de rotatividade necessário para realizar toda a tratativa do sistema.
RNF012	Tamanho das imagens	O Amazon rekognition suporta arquivos de imagem de até 15 MB, inseridos em Amazon S3, sendo o limite de imagens aceitado pelo sistema 15 MB
RNF013	Limite de turma	O sistema é limitado a 100 pessoas por Turma, devido ao limite de usuários por foto do Amazon Rekognition.

Fonte: elaborado pelo autor (2023).

A identificação de 13 requisitos não funcionais representa as especificações que devem ser consideradas para orientar o desenvolvimento e testes, atendendo aos critérios de desempenho e qualidade esperados.

No Quadro 9 é explicitado as regras de negócio na qual o sistema deverá atender.

Quadro 9 - Regras de negócio elicidadas

Identificação	Nome	Descrição
RN001	Tipos de Usuários	O sistema apresenta 3 papéis estabelecidos sendo eles: usuário, monitor e administrador.
RN002	Gerência da aplicação	Toda gestão da aplicação e das atividades administrativas é de responsabilidade dos usuários administradores
RN003	Limite de faltas	O monitor ou o administrador determinam o limite de faltas através das informações do grupo.
RN004	Permissão de edição de presença	Os monitores e administradores são os únicos usuários que podem realizar o abono de faltas ou indicar a ausência.
RN005	Configuração de horário de turmas	Apenas os instrutores e administradores podem realizar a configuração do horário de uma turma
RN006	Justificativa de falta	Usuários que receberam falta, podem conforme definido pelo administrador do sistema, apresentar uma justificativa para sua ausência, caso a justificativa seja aceita pelo administrador, a falta será justificada e a ausência justificada.

RN007	Limite de duração dos grupos	Os grupos de usuário podem ter no máximo a duração de dois anos contando a partir da sua data de início.
RN008	Idade mínima de registro	Os usuários para realizar o cadastro devem ser maiores de idade, possuir no mínimo 18 anos.

Fonte: elaborado pelo autor (2023).

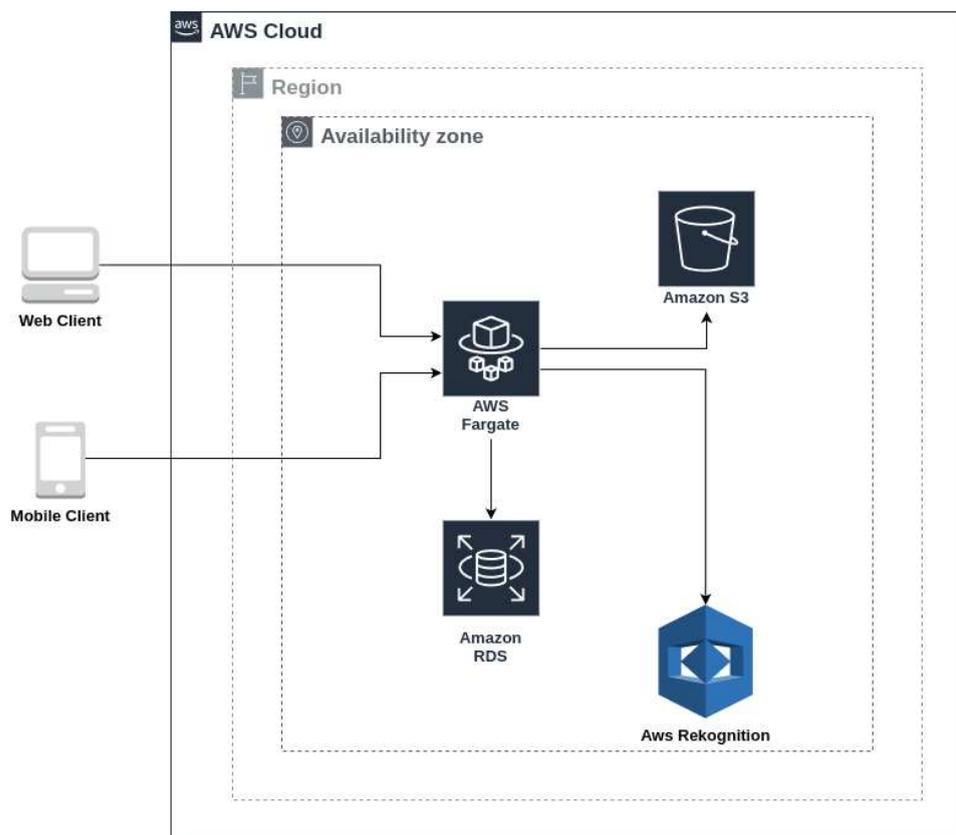
As regras de negócio regem os princípios do sistema, foram identificadas 8 regras, sendo elas responsáveis por coordenar as operações e processos, sendo crucial para o garantir alinhamento dos objetivos e processos do negócio.

6.4 Propostas Arquiteturais

O sistema por ser desenvolvido pensando em ambientes de nuvem apresenta uma enorme versatilidade de abordagens possíveis, se adaptando às necessidades do negócio e restrições ornamentais. Para atender a possíveis variações, foram avaliadas 3 possíveis abordagens arquitetônicas, que atenderam tanto os usuários vindos do *mobile* quanto do *desktop*, dispostas a três níveis de orçamento: baixo, médio e alto. A seguir serão abordados o valor agregado das soluções;

Na primeira abordagem, que pode ser vista na Figura 14, foi projetada para minimizar custos, utilizando somente os recursos necessários.

Figura 14 - Arquitetura de baixo orçamento.

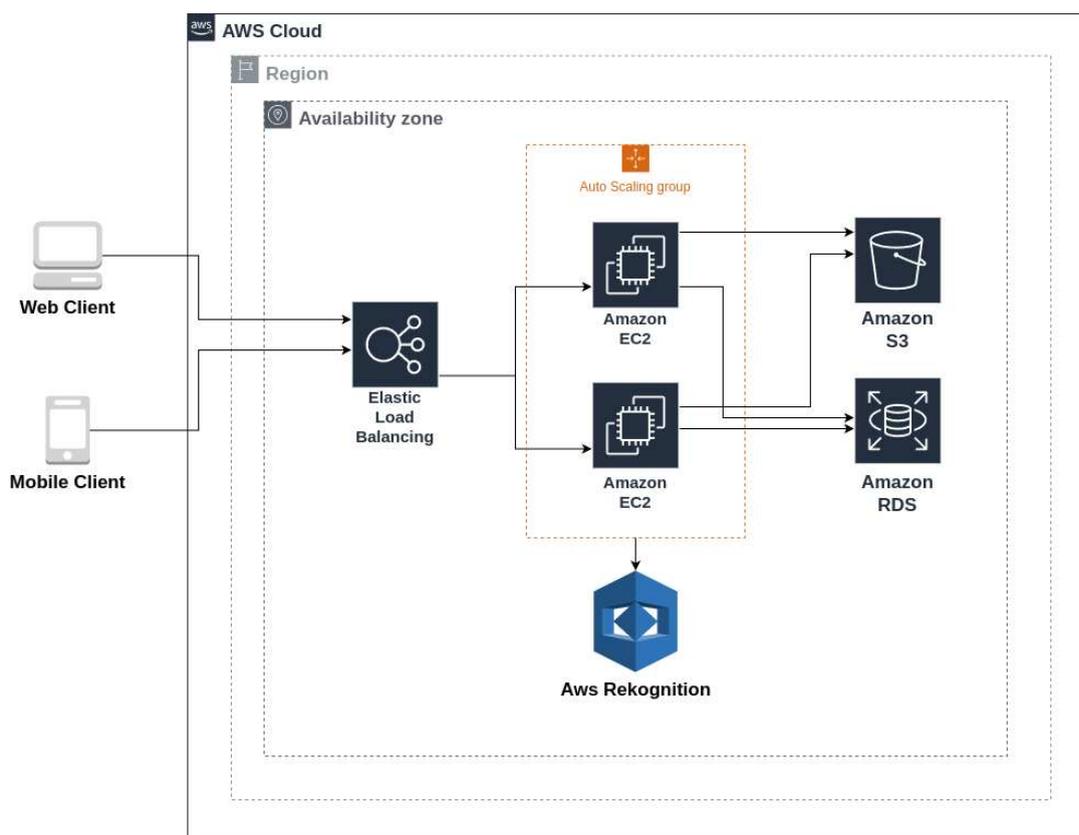


Fonte: elaborado pelo autor (2024).

A configuração foi feita utilizando um AWS Fargate para executar de containers, o que minimiza custos de utilização de gerência servidores, comportando tanto o *back-end* quanto o *front-end*, o qual irá receber as solicitações dos usuários. Ademais, temos uma instância do Amazon RDS (Relational Database Services) para o banco de dados, que simplifica a administração do banco de dados, gerenciando *backups*, *upgrades*, escalabilidade e repetição. Ademais, é utilizado o Amazon S3 para armazenar as imagens faciais, que são analisadas pelo Amazon Rekognition.

Nesta perspectiva, podemos ter também uma abordagem em que se há a necessidade de uma maior escalabilidade e resiliência, como pode ser observado pela Figura 15.

Figura 15 - Arquitetura de médio orçamento.

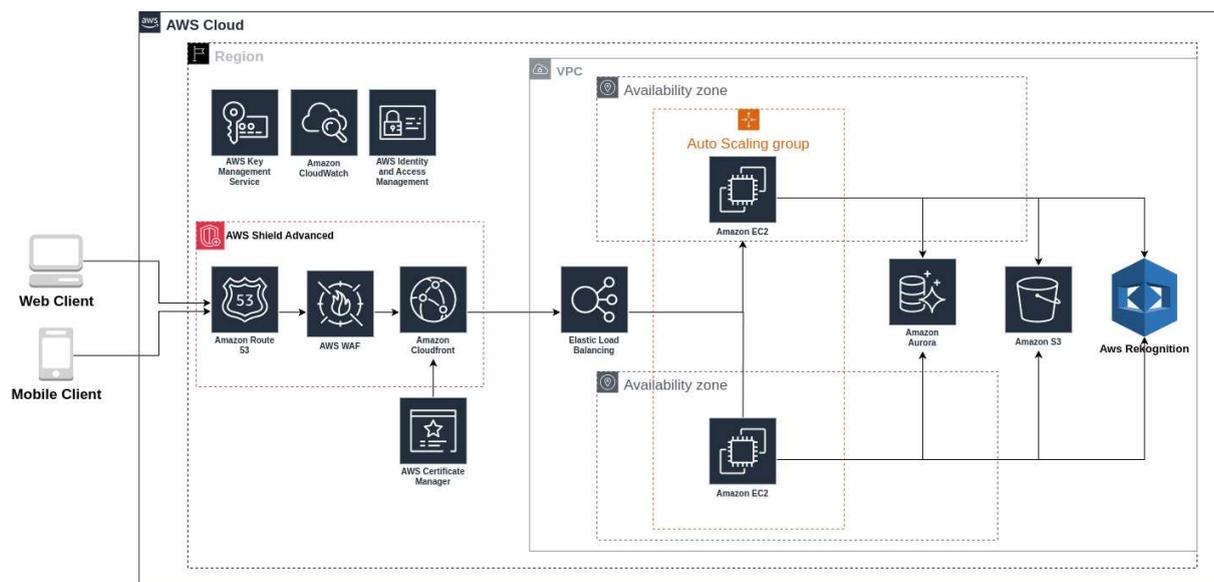


Fonte: elaborado pelo autor (2024).

Aproveita-se de instâncias Amazon Elastic Compute Cloud (EC2), configuradas com *auto scaling group* para prover escalabilidade à aplicação, através desses grupos conseguimos determinar desde a quantidade de instâncias até as suas configurações, para aumentar ou reduzir automaticamente as mesmas com base na demanda do sistema. O balanceamento de carga e recebimento das requisições pelos clientes *mobile* e *web* fica a cargo do, Elastic Load Balancer (ELB), que funcionará distribuindo o tráfego entre as instâncias, à medida que o Amazon S3 continua realizando o armazenamento das imagens faciais e o Amazon Rekognition a análise das mesmas.

Afinal, temos a configuração projetada para extrair o máximo de escalabilidade, performance, segurança, resiliência e disponibilidade do sistema. Sua arquitetura poderá ser visualizada na Figura 16.

Figura 16 - Arquitetura de alto orçamento.



Fonte: elaborado pelo autor (2024).

Há uma camada de serviços que gerencia e protege o acesso aos recursos e a rede do sistema, com o Amazon Route 53, temos um serviço de *Domain Name Service* (DNS) altamente disponível, que garante a resolução de domínio, para o sistema, facilitando o registro e renovação do domínio. Sendo assim, conseguimos manter que as requisições DNS sejam resolvidas rapidamente, sem falhas e escalando caso ocorram picos de acesso.

Fora que, com o AWS *Web Application Firewall* (WAF) oferecendo uma camada de proteção, que atua contra ataques como *SQL injection* e *cross-site scripting* (XSS). Dispondo de uma série de regras que permitem, bloqueiam ou monitoram as requisições web.

Uma vez filtradas as requisições, o Amazon CloudFront, que é uma *Content Delivery Network* (CDN), realiza a distribuição dos nossos conteúdos estáticos e dinâmicos. Com a utilização de servidores distribuídos pelo globo, entregamos com baixa latência, o conteúdo através dos servidores mais próximos do usuário, entregando independente da localização do usuário uma experiência rápida e eficiente.

Para proteger a os mecanismos de entrada do sistema, contra ataques de *Distributed Denial of Service* (DDoS), ataques volumétricos e de exploração de vulnerabilidades, o AWS Shield Advanced oferece uma proteção robusta. Ele realiza o monitoramento e mitigação de ataques que possam comprometer a disponibilidade da aplicação.

Para garantir a troca de informação entre os sistemas de forma segura, o AWS Certificate Manager, é um serviço indispensável, com ele, realiza-se o gerenciamento e

renovação de certificados de *Security Socket Layer (SSL)* e *Transport Layer Security (TLS)*, garantindo que os dados trafeguem de forma criptografada, protegendo os dados sensíveis que são trafegados na rede.

A fim de fornecer capacidade computacional elástica, usaremos instâncias do Amazon EC2 com *auto scaling group*, que provê escalabilidade dinâmica, permitindo assim, criação de novas instâncias para atender a demanda dos usuários e diminuindo as mesmas, em casos de baixa demanda. Para prover uma resiliência ainda maior ao serviço o *auto scaling group* está configurado em duas zonas de disponibilidade dentro da mesma região. Em razão disso, em casos de problemas em uma das zonas, como falta de energia, rede e conectividades, o sistema irá se manter disponível.

Desse modo, para realizar a distribuição do tráfego de entrada para as instâncias da aplicação, usaremos o *Elastic Load Balance*. Com ele aumentamos a eficiência e escalabilidade do sistema. Por sua compatibilidade com o *auto scaling group*, não há necessidade de se adicionar as regras de balanceamento às novas instâncias, identificando-os automaticamente, sem necessidade de configurações manuais.

Na iminência de um grande fluxo de usuários, precisamos de um banco de dados que acompanhe essa demanda. Para isso, contamos com o Amazon Aurora, um banco de dados projetado para sistemas que exigem alta disponibilidade e escalabilidade. Oferecendo replicação automática em diversas zonas de disponibilidades. O Amazon S3 continua realizando o armazenamento das imagens faciais, enquanto o Amazon Rekognition realiza análise das mesmas.

Dado o tráfego de dados críticos, o Amazon Key Manager Service (KMS), gerencia as chaves criptográficas, permitindo a criação e gerência de maneira centralizada. Sendo essencial para prover uma camada extra de segurança sobre os dados em trânsito e em repouso.

Administrar o acesso e as permissões aos recursos da AWS é necessário para isso, utilizamos o AWS identity and Access Management, que gerencia tanto os usuários e seus grupos além de suas permissões, garantindo que apenas os usuários autorizados acessem os recursos, controlando os acessos a EC2, S3 e ao Aurora. Adjunto ao controle de acesso temos o monitoramento dos serviços da AWS realizado pelo CloudWatch, nos proporcionando métricas, logs e eventos em tempo real. Isso auxilia na identificação de problemas, falhas de segurança ou problemas de performance em tempo real.

Essas arquiteturas mostram a versatilidade dos ambientes em nuvem que provém uma gama de possibilidades e abordagens. Utilizamos as recomendações do AWS-Well

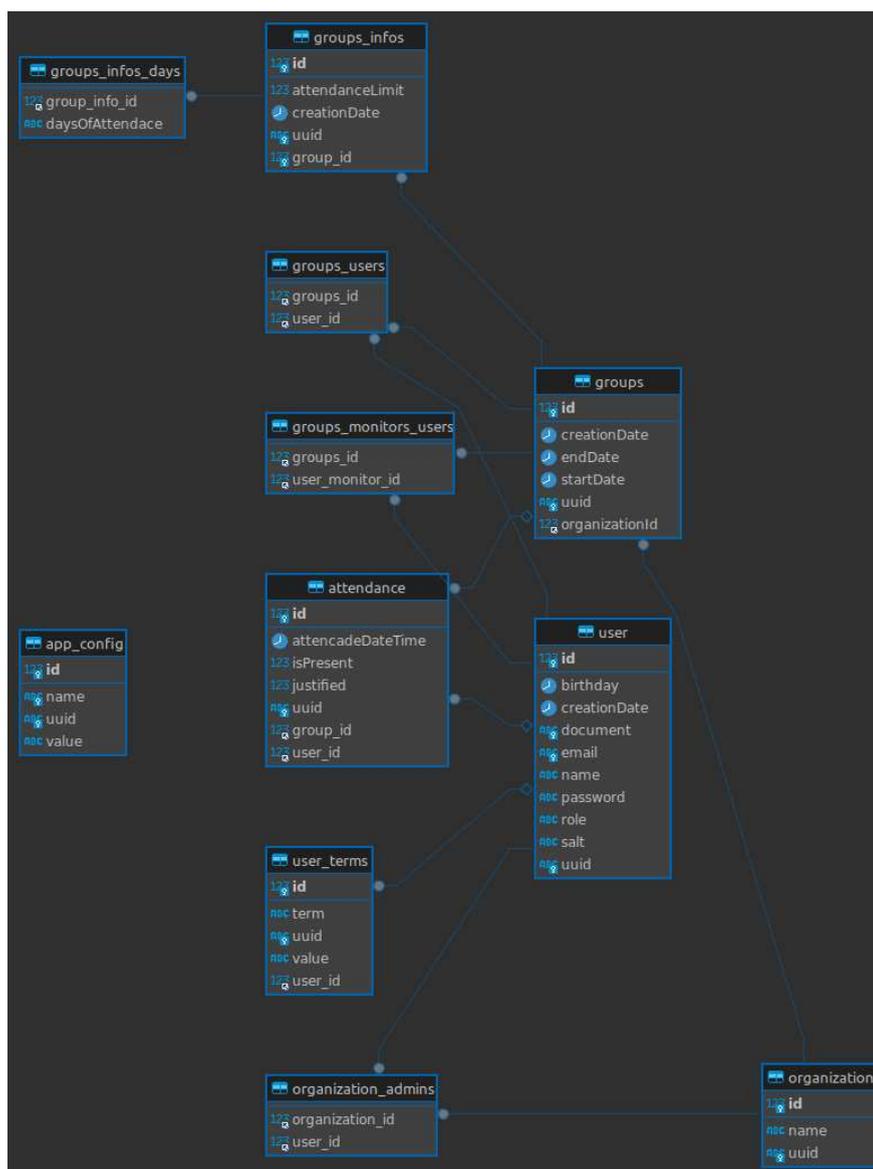
Architected, conseguimos arquitetar soluções que encaixam nas nossas necessidades de segurança, confiabilidade, orçamento, performance e sustentabilidade. Permitindo que a organização modele sua solução com base nas suas necessidades e expectativas.

6.4.1 Proposta de banco de dados

O banco de dados é um componente importante para a operação do sistema, com base nos requisitos funcionais, não funcionais e regras de negócio do sistema, foi possível modelar o banco para atender as necessidades do projeto, garantindo a integridade dos dados.

A parte do planejamento de banco de dados é uma parte importante para garantir conformidade com a LGPD, utilizando-se além de criptografias para os dados pessoais, para que mesmo que o banco de dados seja comprometido os dados possam continuar seguros, como também a utilização de *salt* por usuário, para evitar ataques de *Lookup Table*, *Reverse Lookup Table* e *Rainbow Tables*.

Figura 17 - Diagrama do banco de dados.



Fonte: elaborado pelo autor (2024).

O diagrama apresentado na Figura 17 ilustra o banco de dados e sua estrutura relacional, a modelagem baseia-se nas necessidades do sistema, em gerenciar os múltiplos tipos de usuários e ainda assim garantir a conformidade e integridade dos dados dos usuários. Permitindo assim, a organização das informações de maneira clara e coerente, em particular no que se refere ao controle de presença. Para reforçar a segurança e evitar a exposição dos dados sensíveis, o sistema usa os identificadores únicos universais, para a separação dos recursos, dificultando a rastreabilidade e a previsibilidade dos identificadores.

6.5 Segurança do sistema.

A segurança é um aspecto crítico para o sistema, com ela asseguramos, performance, integridade, excelência operacional, confiabilidade, otimização de custos e disponibilidade dos recursos em ambientes em nuvem.

Os cabeçalhos de segurança foram configurados no servidor, para que com isso, possamos mitigar riscos específicos, para a proteção tanto do serviço quanto dos usuários, evitando diversas abordagens de ataques, os cabeçalhos utilizados, suas configurações, descrição e os ataques a qual ela protege, podem ser vistos no Quadro 10.

Quadro 10 - Cabeçalhos de segurança

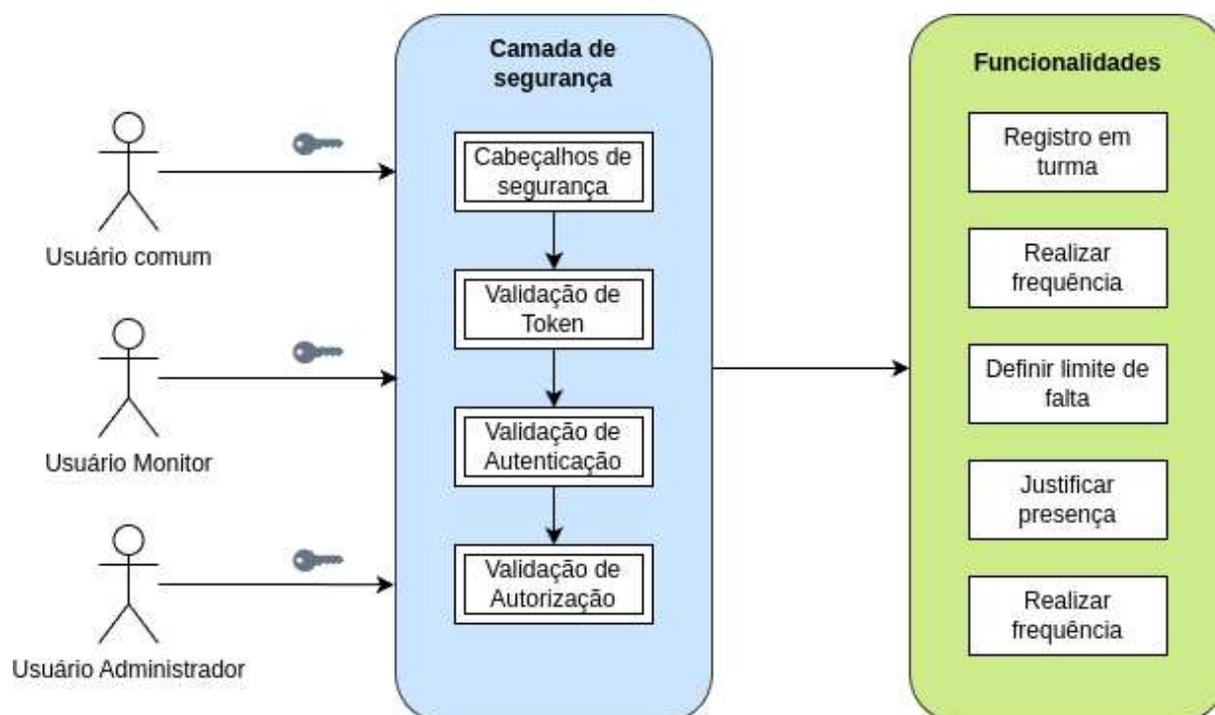
Cabeçalho	Valor	Descrição	Proteção contra
X-Frame-Options	deny	Evita que a página seja carregada em um <iframe>	Clickjacking
Content-Security-Policy	frame-ancestors 'self'	define uma política de segurança de conteúdo na qual somente a própria aplicação	Cross-Site Scripting (XSS) E Clickjacking
X-Content-Type-Options	nosniff	Indica que o tipo declarado pelo servidor deve ser respeitado.	Mime Sniffing, Cross-site Scripting(XSS)
Strict-Transport-Security	max-age=31536000 ; includeSubDomains; preload	Garante através do HSTS que o site só será acessado com o protocolo HTTPS, com duração de 1 ano e com inclusão de subdomínios.	Man-in-the-Middle, Downgrade de HTTP
Referrer-Policy	same-origin	Configuração de referenciamento para apontar o referenciamento apenas em requisições de mesma origem	Vazamento de informações
Cross-Origin Embedder Policy (COEP)	require-corp	Carrega apenas recursos de outras origens que deem permissão de uso.	Vazamento de dados entre origens
Cross-Origin Resource Policy (CORP)	same-origin	Permite o acesso a recursos apenas da mesma origem.	Proteção contra roubo de conteúdo e acesso não autorizado a conteúdo.

Cross-Origin Opener Policy (COOP)	same-origin	Isola o documento de outros contextos, evitando acesso de origens cruzadas, permitindo apenas os da mesma origem.	ataques do tipo <i>cross-origin</i>
-----------------------------------	-------------	---	-------------------------------------

Fonte: elaborado pelo autor (2024).

A vista disso, chegamos a um modelo de segurança modular, com camadas de proteção e devido a combinação do *Spring security*, *JWT*, *oAuth2* e o *CORS*, estabelecemos assim, uma abordagem robusta de segurança do sistema, garantindo que cada usuário cumpra seu devido papel, honrando as práticas e recomendações do *Well-Architected*, em concordância a Figura 18.

Figura 18 - Camadas de segurança.



Fonte: elaborado pelo autor (2024).

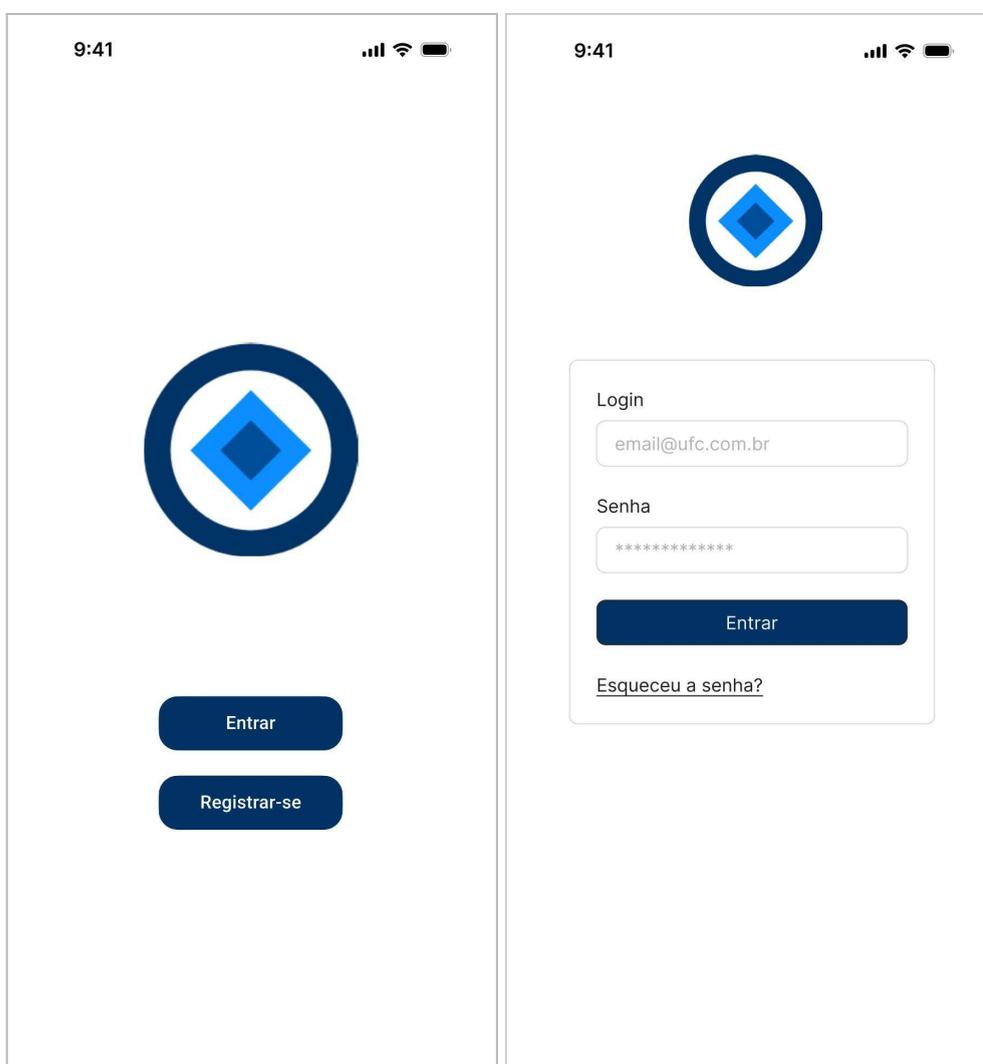
Toda a combinação de ferramentas aqui apresentada, constitui uma camada robusta de segurança, contra diversas ameaças a qual o sistema e seus usuários poderiam estar suscetíveis, garantindo que o sistema opere de maneira segura em ambientes de nuvem.

6.6 Protótipo desenvolvido

Com base nos processo de licitação de requisitos e seus resultados obtivemos um conjunto de requisitos e regras de negócio, para garantir a harmonia com o sistema final. O protótipo desenvolvido possibilita validar a viabilidade técnica e funcional do sistema, dispondo se de 14 telas. Seu resultado poderá ser visto a seguir.

Temos a tela inicial do sistema, que oferece as alternativas de registro e *login* para o usuário, como também a tela de *login* do sistema (ver Figura 19).

Figura 19 - Tela inicial do sistema e login



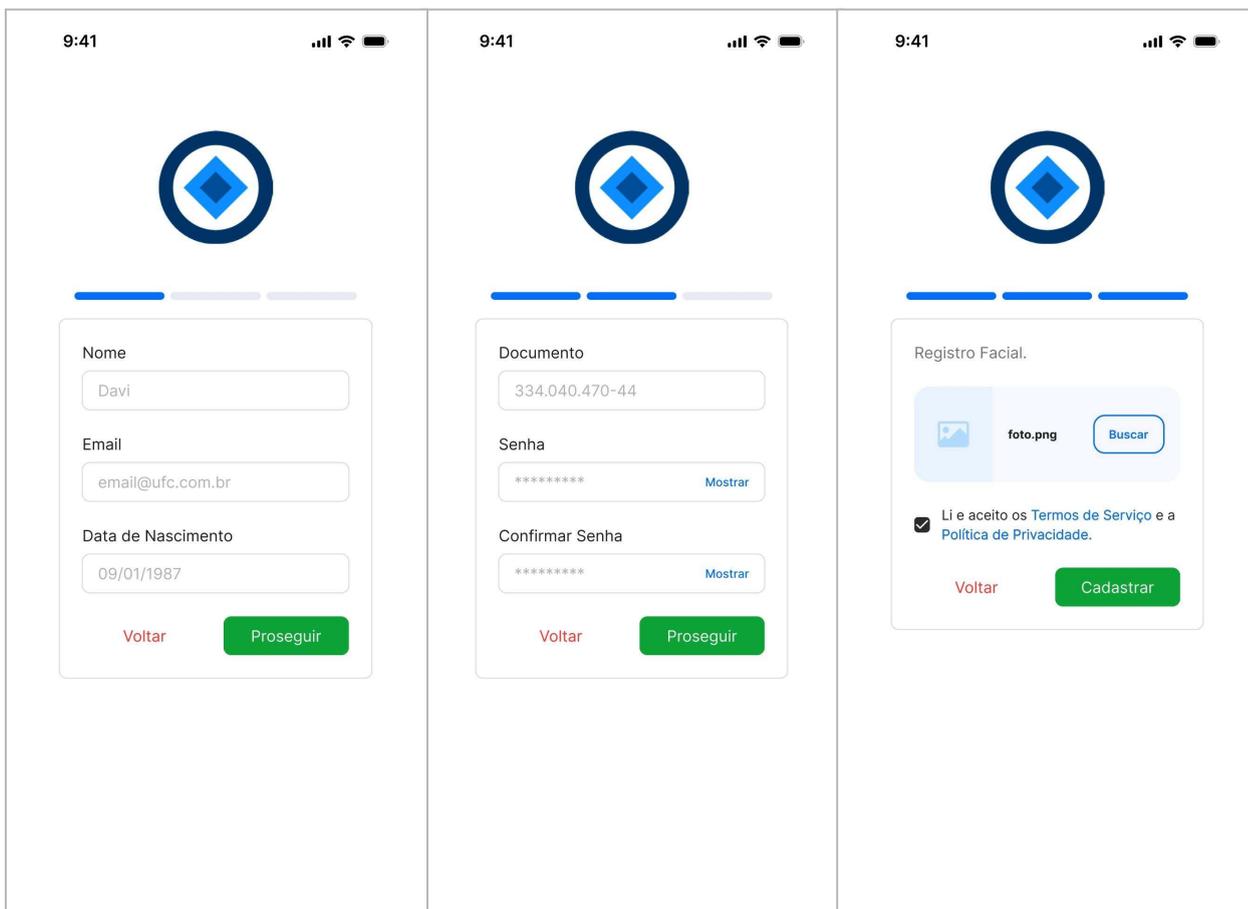
Fonte: elaborado pelo autor (2024).

Constata-se que a telas produzidas permitem o acesso do usuário ao sistema, atendendo aos requisitos, RF006 para que o usuário realize seu login no sistema e o RF014

com as opções de acesso para o usuário.

A tela de cadastro de usuário é dividida em algumas etapas, como pode ser visto na Figura 20.

Figura 20 - Telas de cadastro de usuário



Fonte: elaborado pelo autor (2024).

Identifica-se o fluxo de cadastro de um novo usuário do sistema de acordo com o RF012 e RN008 com as informações de: nome, email, data de nascimento, documento, senha e foto facial. Há também a confirmação de aceite das normas de termo de serviço e políticas de privacidade, para só assim realizar a criação do usuário conforme satisfazer a regra de negócio RN008.

Tela de perfil do usuário conforme representado através da Figura 21.

Figura 21 - Tela de perfil do usuário.

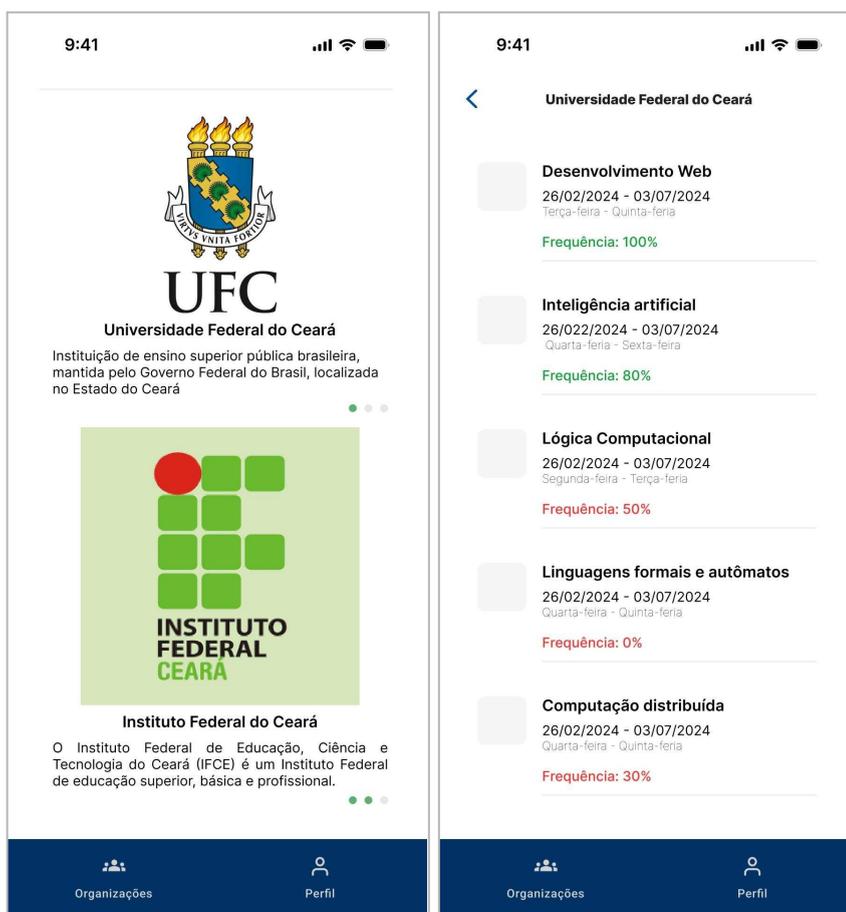


Fonte: elaborado pelo autor (2024).

Logo que o usuário já está cadastrado e dentro do sistema, ele poderá acessar suas informações, entrar em contato com os responsáveis do sistema, acessar as políticas de privacidade, editar seus dados e solicitar a deleção de sua conta, em concordância aos RF013, RF014, RF016 e RF019.

Logo após temos as telas de organizações e grupos (ver Figura 22)

Figura 22 - Telas de organização e listagem de grupos.

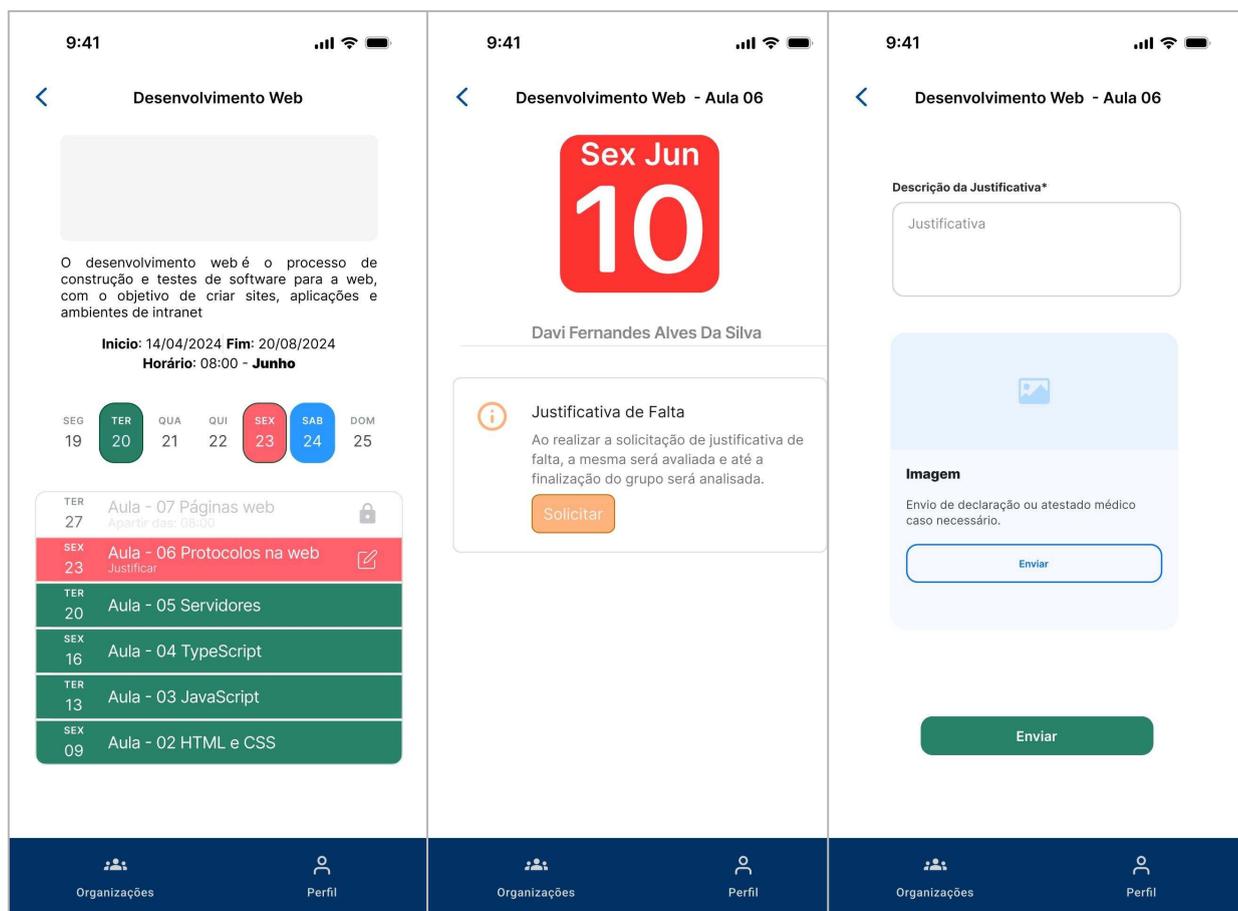


Fonte: elaborado pelo autor (2024).

Na tela das organizações o usuário irá conferir as organizações a qual ele faz parte, para que através dela ele entre irá visualizar os grupos da organização selecionada. Satisfazendo assim os requisitos RF003, RF011, RF017 e RF018.

Em decorrência temos as telas de grupo e justificativa de falta de acordo com a Figura 23.

Figura 23 - Telas de grupo e justificativa de ausência.

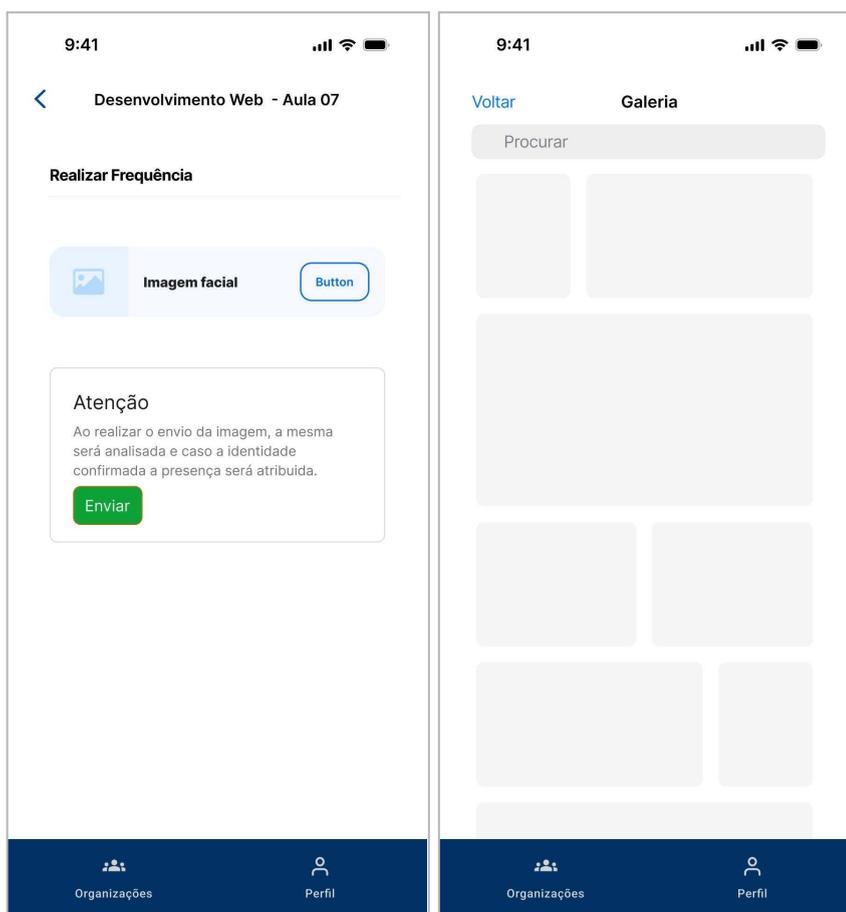


Fonte: elaborado pelo autor (2024).

Para a visualização do grupo que o usuário está inserido, pode-se visualizar a data início e fim do grupo selecionado, além do horário da atividade. Tendo um histórico de sua presença e visualizando também a data e horário dos compromissos anteriores e próximos. Em casos de falta, o usuário poderá realizar o envio de justificativa de ausência. Cumprindo assim os requisitos RF003, RF007 e RF011. Bem como atendendo a regra de negócio RN006.

A etapa de realização de frequência e acesso a galeria do usuário pode ser vista conforme ilustrado na Figura 24.

Figura 24 - Telas de realização de frequência e galeria.

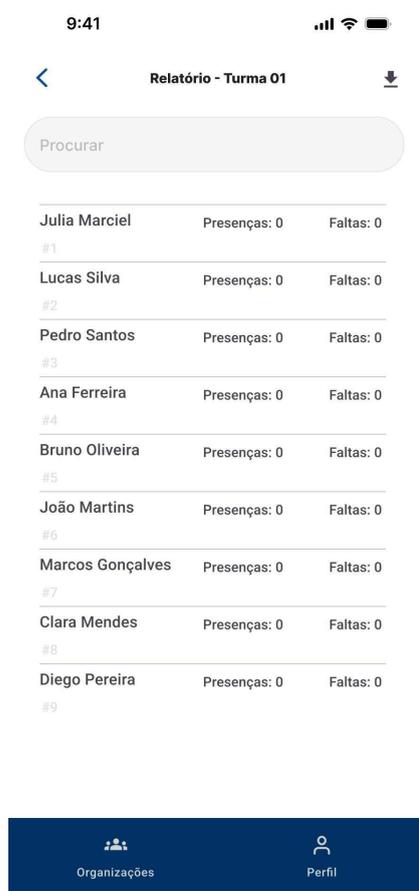


Fonte: elaborado pelo autor (2024).

O processo de realização da frequência fica disponível a partir do horário da atividade, com isso o botão na tela de grupo, vista anteriormente, se torna disponível. Para que o usuário realize sua presença, acessa-se sua galeria para a escolha e envio da imagem. Contemplando os requisitos RF010 e RNF012.

A fim dos monitores e administradores terem uma visão ampla do grupo de usuários, temos a tela de relatório (ver Figura 25).

Figura 25 - Tela de relatório de frequência.



9:41

Relatório - Turma 01

Procurar

Julia Marciel	Presenças: 0	Faltas: 0
#1		
Lucas Silva	Presenças: 0	Faltas: 0
#2		
Pedro Santos	Presenças: 0	Faltas: 0
#3		
Ana Ferreira	Presenças: 0	Faltas: 0
#4		
Bruno Oliveira	Presenças: 0	Faltas: 0
#5		
João Martins	Presenças: 0	Faltas: 0
#6		
Marcos Gonçalves	Presenças: 0	Faltas: 0
#7		
Clara Mendes	Presenças: 0	Faltas: 0
#8		
Diego Pereira	Presenças: 0	Faltas: 0
#9		

Organizações Perfil

Fonte: elaborado pelo autor (2024).

Por final a tela de relatório de frequência, possui as informações dos usuários do grupo, contendo o nome dos usuários, suas faltas e presenças, proporcionando uma visão completa. Caso seja necessário a externalização da listagem de presença, há a opção de realizar o *download* do relatório. Tornando satisfeitos os requisitos RF005, RF011 e RF020.

Em decorrência disso, chegamos numa interface para os usuários do sistema, relacionada diretamente aos requisitos funcionais e não funcionais, bem como as regras de negócio. A completude das telas endossa o alinhamento das necessidades do sistema e a proposta de interface estabelecida.

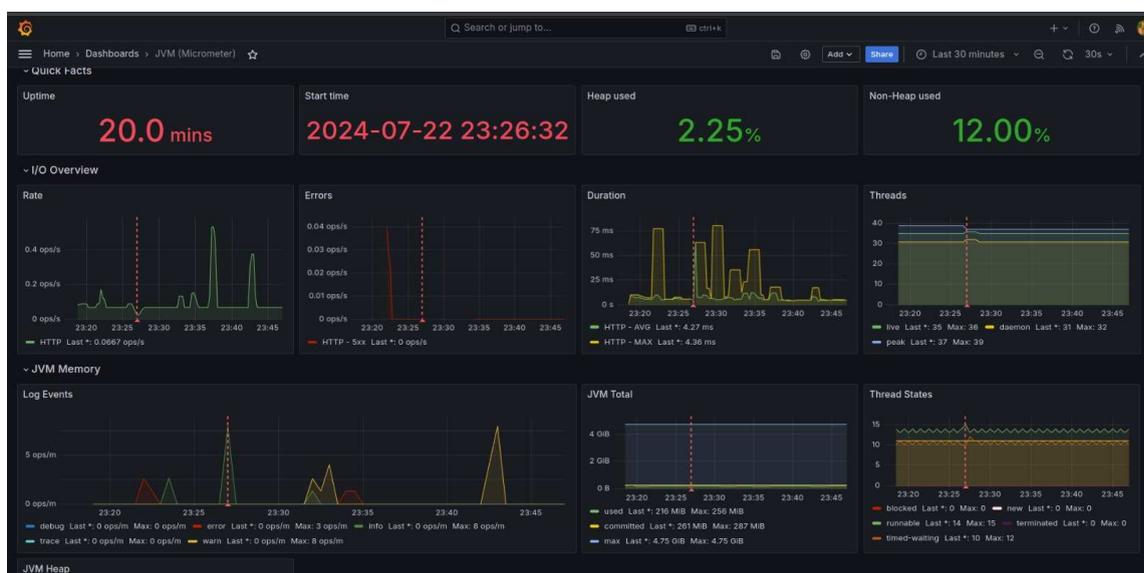
6.7 Monitoramento da solução

Planejar o monitoramento dos sistemas em nuvem é uma prática essencial, para garantir a continuidade e sustentabilidade dos serviços. Como temos um modelo de recursos dinâmicos, expandindo-se com mais facilidade do que em outros ambientes, monitorar é fundamental para identificar problemas de forma ágil.

Por meio do AWS CloudWatch podemos ter uma visão de nossa infraestrutura, porém é importante também ter a visão de dentro do serviço, para identificar pontos de gargalo e erros a nível da aplicação.

As métricas geradas com o uso da aplicação podem ser visualizadas na Figura 26

Figura 26 - Monitoramento da aplicação com o grafana.



Fonte: elaborado pelo autor (2024).

Acompanhamos assim, o *uptime* (tempo em atividade) da aplicação, a quantidade de *threads* ativas no sistema e seu estado, taxa de uso da *central process unit* (CPU), taxa de uso de memória, tanto *heap*, quanto *non-heap*, a taxa de erros retornados pelo servidor e quantidade de classes carregadas pelo sistema.

Com essa abordagem conseguimos expandir toda a linha de monitoramento do nível da infraestrutura até o nível da aplicação. Promovendo a possibilidade de monitorar, identificar problemas rapidamente, provendo resiliência e disponibilidade do sistema.

7 CONCLUSÃO

Este capítulo apresenta a conclusão obtida após todo o trabalho desenvolvido nesta pesquisa. No capítulo 7.1 se apresentam as considerações finais deste. Já no capítulo 7.2 são expostas as propostas de trabalho futuras.

7.1 Considerações finais

O presente trabalho foi elaborado com o objetivo de oferecer um sistema de código aberto para o controle de presença com reconhecimento facial para ambientes em nuvem. A solução mostrou-se moderna, eficaz e viável para o gerenciamento de frequência, devido a utilização da linguagem Java, que através da JVM possibilita a construção de maneira robusta e portátil, aliado com o *framework* spring, garantindo flexibilidade, segurança e escalabilidade, características essenciais para aplicações nativas em nuvem. Tornando assim foi possível alcançar uma solução viável de implantação para os ambientes na nuvem.

O processo de desenvolvimento seguiu as práticas de engenharia de *software*, que através das técnicas relatadas e descritas neste trabalho, conseguiu gerar os requisitos e regras de negócio do sistema. Além do mais, dando a importância da conformidade com a LGPD, possibilitou que a criação do sistema ocorresse de maneira transparente e segura. Sucederam-se diferentes abordagens arquitetônicas foram apresentadas, com base nas necessidades e limitações de cada organização, flexibilizando-se às necessidades das organizações e tornando o sistema assim mais acessível a organizações de diferentes portes.

A partir do início do ciclo de vida do sistema, foi utilizado da estratégia das metodologias ágeis, para acelerar a conclusão de tarefas de forma rápida, permitindo a evolução contínua do sistema e dos seus requisitos. Essa abordagem possibilitou a revisão dos requisitos e validação das funcionalidades, garantindo que o sistema alcançasse as demandas identificadas.

De acordo com os resultados encontrados nesta pesquisa, foi possível atestar a viabilidade da solução. O desenvolvimento do sistema de controle de presença baseado em reconhecimento facial para ambientes em nuvem demonstrou ser tecnicamente viável e eficiente. Embora o sistema ainda não encontre-se em sua completude funcional, o mesmo defronta-se em um estágio avançado de desenvolvimento e aberto a contribuições de toda comunidade científica, podendo ser acessado pelo apêndice D.

Conclui-se assim, que por mais que o sistema não tenha sido desenvolvido em toda sua extensão e completude, alcançou os objetivos propostos inicialmente, contribuindo assim com toda comunidade científica.

7.2 Trabalhos futuros.

Por mais que o sistema tenha alcançado seus objetivos, há aprimoramentos que podem ser realizados, como sugestão de trabalhos futuros temos:

- **Teste de usabilidade com o protótipo criado:** tem-se em vista que o protótipo desenvolvido precisa de testes de usabilidade, para coletar *feedbacks* dos usuários. Com esses testes podem ser encontrados erros de interações, no qual os usuários podem não entender com clareza as interações que podem ou não realizar com o sistema. Além disso, poderá haver obstáculos de navegação, em que os usuários terão dificuldades em encontrar o conteúdo que estão buscando. Problemas de acessibilidade, com usuários que possuem algum tipo de deficiência. Logo, garantindo uma experiência adequada e acessível para todos.
- **Integração com outras nuvens públicas:** A integração com outras nuvens públicas além da AWS é um aspecto importante, para que assim ao implantar o sistema a empresa escolha o provedor que melhor atende às suas necessidades, seja ela financeira ou geográfica. Deste modo proporcionando uma maior flexibilidade a solução.
- **Desenvolvimento do módulo *front-end*:** O módulo *front-end* da aplicação é de extrema importância para a interação do usuário com o sistema, seu desenvolvimento é primordial para a utilização do mesmo.
- **Internacionalização da solução:** A solução apresenta um alto potencial de utilização por diversos tipos de usuários em diferentes idiomas, fusos horários, formato de datas e características regionais. Devido ao sistema ser globalmente escalável, a expansão para um mercado global é vital.

REFERÊNCIAS

AL-ROOMI, May *et al.* Cloud computing pricing models: a survey. **International Journal of Grid and Distributed Computing**, v. 6, n. 5, p. 93-106, 2013. Disponível em: <http://dx.doi.org/10.14257/ijgdc.2013.6.5.09> ISSN: 2005-4262. Acesso em: 05 nov. 2023.

ALZU'BI, A.; ALBALAS, F.; AL-HADHRAMI, T.; YOUNIS, L. B.; BASHAYREH, A. Masked Face Recognition Using Deep Learning: A Review. **Electronics**, v. 10, n. 21, p. 2666, 2021. MDPI AG. Disponível em: <<http://dx.doi.org/10.3390/electronics10212666>>. Acesso em: 08 out 2023.

AMAZON WEB SERVICES. **Amazon Rekognition. Face Detection Model**. 2023

Disponível em:

<https://docs.aws.amazon.com/rekognition/latest/dg/face-detection-model.html>. Acesso em: 11 nov. 2023.

AMAZON WEB SERVICES. **AWS Well-Architected**. 2023 Disponível em:

<https://docs.aws.amazon.com/rekognition/latest/dg/face-detection-model.html>. Acesso em: 17 nov. 2023.

ARMBRUST, Michael *et al.* **Above the clouds: A berkeley view of cloud computing**.

Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 10 fev. 2009. Disponível em:

<https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>. Acesso em: 06 out. 2023.

AZEVEDO, Leonardo Guerreiro. Desenvolvimento de Soluções com Serviços: SOA, Cloud e Microserviços. 2020 Disponível em:<https://www.researchgate.net/publication/346493146>. Acesso em: 18 jul. 2024.

BEYER, Dirk; LÖWE, Stefan; WENDLER, Philipp. Reliable benchmarking: requirements and solutions. **International Journal on Software Tools for Technology Transfer**, v. 21, p. 1-29, 2019. Acesso em: 14 out. 2023.

BRASIL. Decreto nº 6.094, de 24 de abril de 2007. Dispõe sobre a implementação do Plano de Metas Compromisso Todos pela Educação, pela União Federal, em regime de colaboração com Municípios, Distrito Federal e Estados, e a participação das famílias e da comunidade, mediante programas e ações de assistência técnica e financeira, visando a mobilização social pela melhoria da qualidade da educação básica. Decreto nº 6.094, de 24 de Abril de 2007, Brasília, DF, 24 abr. 2007. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6094.htm. Acesso em: 21 set. 2023.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Resolução nº 466, de 12 de dezembro de 2012. Seção II.23 - Termo de Consentimento Livre e Esclarecido - TCLE.

Disponível em:https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html. Acesso em: 12 nov. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Cap. II,

Seção IV: Do Término do Tratamento de Dados. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 16 ago. 2024.

BRUNER, Jerome S.; TAGIURI, Renato. **The perception of people**. Handbook of social psychology, v. 2, p. 634-654, 1954. Acesso em: 18 out 2023.

CHELLAPPA, R. **Intermediaries in cloud-computing: A new computing paradigm**. em: INFORMS Annual Meeting, Dallas, 1997, p. 26-29. Acesso em: 28 set. 2023.

DE CARRERA, Proyecto Fin; MARQUES, Ion. Face recognition algorithms. Master's thesis in Computer Science, Universidad Euskal Herriko, v. 1, 2010. Acesso em: 02 nov 2023.

DE LUNETTA, Avaetê; GUERRA, Rodrigues. Metodologia da pesquisa científica e acadêmica. **Revista OWL (OWL Journal)-REVISTA INTERDISCIPLINAR DE ENSINO E EDUCAÇÃO**, v. 1, n. 2, p. 149-159, 2023. Acesso em: 02 nov 2023.

ELMUTI, Dean; KATHAWALA, Yunus. An overview of benchmarking process: a tool for continuous improvement and competitive advantage. **Benchmarking for Quality Management & Technology**, v. 4, n. 4, p. 229-243, 1997. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/14635779710195087/full/html>. Acesso em: 02 out 2023.

FERREIRA, Elen Cristina da Silva; OLIVEIRA, Nayara Maria de. EVASÃO ESCOLAR NO ENSINO MÉDIO: causas e consequências. Scientia Generalis, [S. l.], v. 1, n. 2, p. 39-48, 2020. Disponível em: <https://scientiageneralis.com.br/index.php/SG/article/view/v1n2a4>. Acesso em: 6 set. 2024.

FIELDING, Roy Thomas. **Architectural styles and the design of network-based software architectures**. University of California, Irvine, 2000. acesso em: 20 jun. 2024.

GODSWILL, Ofualagba *et al.* Automated student attendance management system using face recognition. **International Journal of Educational Research and Information Science**, v. 5, n. 4, p. 31-37, 2018. Disponível em: https://www.researchgate.net/publication/327671423_Automated_Student_Attendance_Management_System_Using_Face_Recognition. Acesso em: 22 out 2023.

GORELIK, Eugene. **Cloud computing models**. jan 2013. Tese de Doutorado. Massachusetts Institute of Technology. Disponível em: <https://web.mit.edu/smadnick/www/wp/2013-01.pdf>. Acesso em: 14 out. 2023.

HUANG, Thomas S. **Computer vision: Evolution and promise**. CERN European Organization for Nuclear Research-Reports-CERN, p. 21-26, 1996. Acesso em: 17 out 2023.

IBRAHIMI, Aferdita. **Cloud computing: Pricing model**. International Journal of Advanced Computer Science and Applications, v. 8, n. 6, 2017. Acesso em: 7 set 2023

JAISWAL, Manishaben. Software architecture and software design. **International Research Journal of Engineering and Technology (IRJET) e-ISSN**, p. 2395-0056, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772387. Acesso em: 07 set 2023.

LE MAU, Tuan *et al.* Professional actors demonstrate variability, not stereotypical expressions, when portraying emotional states in photographs. **Nature communications**, v. 12, n. 1, p. 5037, 2021. Disponível em: <https://doi.org/10.1038/s41467-021-25352-6>. Acesso em: 18 out 2023.

MASALHA, Fadi; HIRZALLAH, Nael. **A students attendance system using QR code**. International Journal of Advanced Computer Science and Applications, v. 5, n. 3, 2014. Disponível em: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=288f0459675d41e2d3bbb8b6b65bc927ffe57262>. Acesso em: 23 out 2023.

MELL, Peter; GRANCE, Timothy. The NIST definition of cloud computing. 2011. Acesso em: 30 set. 2023

MITTAL, Aayush *et al.* **Cloud based intelligent attendance system through video streaming**. In: 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon). IEEE, 2017. p. 1352-1357. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8358587>. Acesso em: 23 out 2023.

PAWLE, Akshay A.; PAWAR, Vrushsen P. Face recognition system (FRS) on cloud computing for user authentication. **International Journal of Soft Computing and Engineering (IJSCE)**, v. 3, n. 4, p. 189-192, 2013. Disponível em: <https://www.researchgate.net/profile/Hemant-Chaudhari/post/How-can-a-biometric-method-be-implemented-in-cloud-architecture/attachment/59d6297079197b8077987f01/AS%3A335472573337601%401456994302158/download/Easy+Paper+on+Cloud.pdf> Acesso em: 09 nov 2023.

PIZZAIA, Victor Hugo; MALARA, Rodrigo Daniel. GARANTIA DA QUALIDADE DE SOFTWARE COM DEVOPS. **RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218**, v. 3, n. 11, p. e3112193-e3112193, 2022. Acesso em: 16 nov 2023

POHL, Klaus;RUPP, Chris. **Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam-foundation level-IREB compliant**. Rocky Nook, Inc., 2015. Acesso em: 12 nov 2023

PRADO, Kelvin Salton do. **Comparação de técnicas de reconhecimento facial para identificação de presença em um ambiente real e semicontrolado**. 2018. Dissertação (Mestrado em Sistemas de Informação) - Escola de Artes, Ciências e Humanidades, University of São Paulo, São Paulo, 2017. doi:10.11606/D.100.2018.tde-07012018-222531. Acesso em: 17 out 2023.

RAO, Ashwin. AttenFace: A Real Time Attendance System Using Face Recognition. In: **2022 IEEE 6th Conference on Information and Communication Technology (CICT)**. IEEE, 2022. p. 1-5. Acesso em: 15 nov 2023

ROMERO, M.; YOUNG HO LEE. **A National Portrait of Chronic Absenteeism in the Early Grades**. 1 jan. 2007. Disponível em: <https://academiccommons.columbia.edu/doi/10.7916/D89C7650>. Acesso em: 9 jun. 2023.

SALES, Eduardo Arce de *et al.* **Desenvolvimento de um software para automatizar o**

sistema de frequencia de alunos por meio de reconhecimento facial. 2022. Disponível em: <http://repositorioinstitucional.uea.edu.br/handle/riuea/4525>. Acesso em: 22 out 2023.

SALMIJÄRVI, Arttu. **Cloud Architecture Evaluation.** 2023, Disponível em: https://www.utupub.fi/bitstream/handle/10024/174998/Salmijarvi_Arttu_thesis.pdf?sequence=1 Acesso em: 05 set 2023.

SARASWAT, Manish; TRIPATHI, R. C. Cloud computing: Comparison and analysis of cloud service providers-AWs, Microsoft and Google. In: **2020 9th international conference system modeling and advancement in research trends (SMART).** IEEE, 2020. p. 281-285. Acesso em: 17 out 2024.

SOMMERVILLE, Ian. Engenharia de Software. Edição 10.ed. São Paulo: Pearson, 2019. Disponível em: Acesso em: 12 nov. 2023.

SOUZA, Wânia C. de *et al.* Face perception in its neurobiological and social context. **Psychology & Neuroscience**, v. 1, p. 15-20, 2008. Acesso em: 20 out. 2023.

SPRING. Disponível em: <https://spring.io/>. Acesso em: 14 nov. 2023.

TASKIRAN, Murat; KAHRAMAN, Nihan; ERDEM, Cigdem Eroglu. **Face recognition: Past, present and future (a review).** Digital Signal Processing, v. 106, p. 102809, 2020. Acesso em: 09 nov 2023.

WANG, Mei; DENG, Weihong. Deep face recognition: A survey. **Neurocomputing**, v. 429, p. 215-244, 2021. Acesso em: 23 set. 2023.

YADAV, Vikas; BHOLE, G. P. **Cloud Based Smart Attendance System for Educational Institutions.** 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 97-102, doi: 10.1109/COMITCon.2019.8862182. Acesso em: 23 out 2023.

APÊNDICE A – QUESTIONÁRIO DE COLETA DE DADOS

QUESTIONÁRIO

1. Faixa Etária (Escolha)

- Até 20 anos
- 21 – 24 anos
- 25 – 29 anos
- 30 – 34 anos
- 30 – 34 anos
- 40 – 44 anos
- 45 – 49 anos
- Acima de 50 anos
- Prefiro não responder

2. Normalmente você precisa registrar sua presença ou de outras pessoas?(Escolha)

- Sim, preciso registrar minha presença!
- Sim, Preciso registrar a presença de outras pessoas.
- Não
- Prefiro não responder

3. Com que frequência você precisa registrar sua presença ou a de outras pessoas?(Escala Linear)

- 0 (Pouco
- 1
- 2
- 3
- 4
- 5
- 6 (Muito)

4. Caso precise registrar frequência em quais tipos de ambiente ela ocorre?(Caixa de seleção)

- Academico (ex: Aulas, Cursos...)
- Trabalho (ex: Bater Ponto...)

- Saúde (ex: Tratamentos, Terapia...)
 - Atividades Recreativas (ex.: esportes, lazer...)
 - Outros(Aberta)
5. Caso você precise computar sua frequência de que maneira ela é realizada (Seleção)
- Planilha
 - Assinatura
 - Biometria Digital
 - Biometria Facial
 - Plataforma *Online*
 - Aplicativos Móveis
 - Outros (Aberta)
6. Nesse(s) ambiente(s) você possui acesso a internet?
- Sim
 - Não

APÊNDICE B – TERMO DE CONSENTIMENTO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Prezado(a)

Você está sendo convidado(a) para participar de uma pesquisa em acordo com as exigências da resolução no 466/2012 do Conselho Nacional de Saúde.

Antes de você responder as perguntas relacionadas a esta pesquisa, apresentamos o Termo de consentimento livre e esclarecido (TCLE) para sua leitura e anuência.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Declaro que estou ciente e concordo voluntariamente com os termos e condições estabelecidos neste Termo de Consentimento Livre e Esclarecido (TCLE) antes de preencher o formulário de coleta de informações destinado à pesquisa acadêmica desenvolvida por Davi Fernandes Alves da Silva como parte do Trabalho de Conclusão de Curso (TCC) sobre um sistema de reconhecimento facial para realização de frequência.

Informações Gerais:

1. **Finalidade da Coleta de Dados:** Os dados fornecidos neste formulário serão coletados exclusivamente para fins da pesquisa acadêmica conduzida pelo discente Davi Fernandes Alves da Silva como parte de seu TCC, que tem como objetivo o desenvolvimento de um sistema de reconhecimento facial. As informações serão utilizadas para análise e conclusões da pesquisa.
2. **Confidencialidade:** Todas as informações fornecidas serão tratadas com estrita confidencialidade. A identidade dos participantes e suas respostas não serão compartilhadas, divulgadas ou vendidas a terceiros em nenhuma circunstância.
3. **Consentimento Voluntário:** Entendo que minha participação nesta pesquisa é voluntária e que tenho o direito de recusar fornecer informações ou de retirar meu consentimento a qualquer momento, sem sofrer qualquer consequência negativa.
4. **Anonimato e Privacidade:** As informações fornecidas não estarão vinculadas ao meu nome ou identificação pessoal. Todas as respostas serão tratadas de forma anônima, garantindo minha privacidade.
5. **Armazenamento e Prazo:** Após a conclusão da pesquisa, os dados coletados serão armazenados de forma segura e, após um período de 2 anos, serão permanentemente excluídos.
6. **Informações preenchidas** Será enviado para o participante uma cópia das informações preenchidas, sendo extremamente recomendado guardar uma cópia do documento eletrônico.
7. **Maioridade**
Declaro que sou maior de 18 anos de idade. O preenchimento deste formulário está condicionado ao atendimento deste critério de maioridade.

Concordância e Consentimento

Ao preencher e enviar o formulário, declaro que li e compreendi os termos e condições acima

e concordo voluntariamente em participar desta pesquisa acadêmica, fornecendo as informações solicitadas.

Dúvidas e Esclarecimentos Qualquer dúvida e esclarecimentos entrar em contato com o responsável através do email: daviifernandes@alu.ufc.br

APÊNDICE C – POLÍTICA DE PRIVACIDADE

Política de Privacidade

Nós, da Rekome, prezamos por sua privacidade e proteção e pensando nisso criamos a nossa política de privacidade para através dela descrever quais informações pessoais nós coletamos e como elas serão tratadas, armazenadas e compartilhadas esclarecendo todos os seus direitos;

Este documento se encontra em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD), recomendando-se a leitura para o devido respaldo legal.

A quem se aplica a Política de Privacidade?

Esta política se aplica a todos aqueles que acessarem, se cadastrarem e utilizarem o Rekome, seja através de navegação pela web ou por aplicativos mobile.

Quais dados pessoais nós coletamos?

O Sistema Rekome coleta os seguintes dados pessoais para fins de reconhecimento facial e controle de presença:

- * Imagens faciais
- * Data de aniversário
- * Nome completo
- * CPF
- * Endereço de e-mail
- * Comprovações de presença
- * Atestados médicos

Finalidade do tratamento dos dados

Nós utilizamos os seus dados pessoais para prover, manter, melhorar e personalizar nossos produtos e serviços destinados a você, existentes ou a serem criados. Detalhamos a seguir as finalidades para as quais utilizamos eles:

- * Identificação e autenticação dos usuários
- * Controle de presença
- * Geração de relatórios de frequência
- * Comunicação com os usuários

Os dados pessoais serão única e exclusivamente tratados para as finalidades descritas acima e não serão utilizados para outros fins sem o seu consentimento.

Como protegemos os seus dados?

Adotamos medidas de segurança visando à proteção dos dados pessoais, bloqueando todo e qualquer acesso não autorizado. Utilizando os mecanismos estipulados por lei, respeitando a sua privacidade e protegendo seus dados em nossos processos internos como um todo.

Só tratamos os seus dados mediante alto grau de segurança, implementando as melhores práticas em uso na indústria para a proteção de dados, tais como: técnicas de criptografia, monitoramento e testes de segurança periódicos.

Proteção de Imagens Faciais.

Para as imagens faciais, utilizamos técnicas avançadas de criptografia e anonimização para garantir que seus dados sejam protegidos contra acessos não autorizados e vazamentos. As imagens são armazenadas de forma segura e somente podem ser acessadas por pessoal autorizado.

Prazo de Retenção de Imagens Faciais.

As imagens faciais serão armazenadas por um período máximo de 2 anos, salvo quando houver necessidade legal ou regulatória de manutenção por prazo superior. Após esse período, os dados serão excluídos, entretanto, mediante solicitação de exclusão, todos os dados serão

excluídos imediatamente.

Seus direitos como Titular dos Dados

De acordo com a LGPD, você tem os seguintes direitos em relação aos seus dados pessoais:

- * Acessar seus dados pessoais
- * Corrigir dados incompletos, inexatos ou desatualizados
- * Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD
- * Solicitar a portabilidade dos dados
- * Revogar o consentimento a qualquer momento

Você pode, a qualquer momento, entrar na sua conta, seja pela plataforma mobile ou web, e solicitar a edição ou exclusão da conta, em casos de problemas técnicos, nossos canais de comunicação estão disponíveis.

Dúvidas

Se você tiver qualquer dúvida sobre esta política de privacidade ou sobre o tratamento dos seus dados pessoais, entre em contato conosco através do e-mail: privacidade@rekome.com.

Alterações na Política

Podemos atualizar esta Política de Privacidade periodicamente. Quaisquer alterações serão publicadas em nosso site e, quando necessário, notificaremos você por e-mail com antecedência para que possa revisar as mudanças.

APÊNDICE D – REPOSITÓRIO DO PROJETO

: <https://github.com/Davizex/attendance-system-face-recognition>