



**INSTITUTO
FEDERAL**

Piauí

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS FLORIANO
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

CLEBER HENRIQUE LACERDA DUARTE

**SISTEMA DE RECONHECIMENTO FACIAL PARA REGISTRO DE CONSULTAS
CLÍNICAS COM ARMAZENAMENTO SEGURO DE DADOS BIOMÉTRICOS**

**FLORIANO – PI
2026**

CLEBER HENRIQUE LACERDA DUARTE

**SISTEMA DE RECONHECIMENTO FACIAL PARA REGISTRO DE CONSULTAS
CLÍNICAS COM ARMAZENAMENTO SEGURO DE DADOS BIOMÉTRICOS**

Trabalho de Conclusão de Curso (Artigo Científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Floriano.

Orientador: Prof. Me. Ronaldo Pires Borges

SISTEMA DE RECONHECIMENTO FACIAL PARA REGISTRO DE CONSULTAS CLÍNICAS COM ARMAZENAMENTO SEGURO DE DADOS BIOMÉTRICOS

Cleber Henrique Lacerda Duarte¹
Prof. Me. Ronaldo Pires Borges²

RESUMO

Este artigo científico tem como objetivo propor e avaliar uma arquitetura de sistema para registro de consultas clínicas via reconhecimento facial, fundamentada na computação de borda e orientada por requisitos de conformidade com a LGPD. A metodologia utilizada baseia-se na Design Science Research (DSR), envolvendo a construção de um artefato tecnológico físico-lógico e sua subsequente auditoria computacional e matemática. Como referencial teórico, utilizam-se os trabalhos clássicos sobre Deep Learning na extração de vetores faciais (FaceNet) e literatura atual sobre biometria cancelável e segurança da informação em ambientes de saúde. A pesquisa justifica-se pela ineficiência, tempo de espera e os severos riscos de exposição de dados sensíveis inerentes ao processo manual de recepção clínica tradicional. Os resultados demonstram que o artefato, operando em um microcomputador Labrador, alcança uma taxa de 20 a 30 quadros por segundo, reduzindo o tempo de check-in para menos de 1 segundo de forma passiva, mesmo com oclusões faciais. A avaliação de segurança comprovou a eficácia da proteção dos dados em repouso por meio de criptografia AES-128 e da irreversibilidade biométrica via matriz ortogonal (Bio-hashing), resistindo a simulações de engenharia reversa. Este estudo contribui para a área de Tecnologia em Saúde apresentando um modelo prático e escalável que soluciona o gargalo administrativo da identificação de pacientes garantindo a máxima privacidade desde a concepção.

¹ IFPI – Campus Florianópolis. E-mail: caflo.2024114tads0005@aluno.ifpi.edu.br

² IFPI – Campus Florianópolis. E-mail: ronaldo.borges@ifpi.edu.br

Palavras-chave: reconhecimento facial; computação de borda; segurança da informação; Lei Geral de Proteção de Dados; saúde digital.

ABSTRACT

This scientific article aims to propose and evaluate a system architecture for clinical consultation check-in via facial recognition, grounded in edge computing and guided by LGPD compliance requirements. The methodology used is based on Design Science Research (DSR), involving the construction of a physical-logical technological artifact and its subsequent computational and mathematical audit. As a theoretical framework, classical works on Deep Learning for facial vector extraction (FaceNet) and current literature on cancelable biometrics and information security in healthcare environments are used. The research is justified by the inefficiency, waiting times, and severe risks of exposing sensitive data inherent in the traditional manual clinical reception process. The results demonstrate that the artifact, operating on a Labrador microcomputer, achieves a rate of 20 to 30 frames per second, reducing check-in time to under 1 second passively, even with facial occlusions. The security evaluation proved the effectiveness of data-at-rest protection through AES-128 encryption and biometric irreversibility via an orthogonal matrix (Bio-hashing), successfully resisting reverse engineering simulations. This study contributes to the Health Technology field by presenting a practical and scalable model that solves the administrative bottleneck of patient identification while ensuring maximum privacy by design.

Keywords: facial recognition; edge computing; information security; General Data Protection Law; digital health.

Data de aprovação: 09/07/2026

1 INTRODUÇÃO

A crescente digitalização dos serviços de saúde tem promovido avanços significativos na gestão de informações clínicas e administrativas. Sistemas informatizados passaram a desempenhar papel central na organização de fluxos de atendimento, no armazenamento de dados de pacientes e na melhoria da eficiência operacional de clínicas e hospitais. Contudo, muitos processos ainda permanecem dependentes de intervenções manuais, especialmente no que se refere ao registro de presença e identificação de pacientes. Essa dependência pode ocasionar filas, retrabalho e

ineficiências operacionais significativas (Kurniasari et al., 2025), além de aumentar o risco de erros de identificação que comprometem a segurança do paciente (Sadahide et al., 2024).

No contexto das clínicas de saúde e desenvolvimento familiar, o processo de *check-in* frequentemente exige o preenchimento manual de dados cadastrais e a validação da presença do paciente por profissionais da recepção. Além de consumir tempo, esse procedimento expõe informações sensíveis a riscos de segurança e falhas de conformidade com a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes rigorosas para o tratamento de dados pessoais, especialmente os de natureza biométrica (Instituto Brasileiro de Defesa do Consumidor, 2023).

Diante desse cenário, tecnologias de reconhecimento facial baseadas em técnicas de *Deep Learning*³ têm se destacado como soluções viáveis para a automação da identificação de indivíduos (Lei et al., 2025). Estudos recentes demonstram elevados índices de acurácia mesmo em ambientes adversos, como hospitais e clínicas, onde variáveis como iluminação e posicionamento do paciente são desafiadoras (Sadahide et al., 2024). Além disso, a viabilidade técnica de implementar tais soluções em dispositivos de borda (*edge computing*)⁴ de baixo custo já foi demonstrada na literatura recente (Dalvi et al., 2025). No entanto, a adoção dessa tecnologia não pode se limitar à eficiência técnica, sendo imprescindível considerar aspectos éticos, legais e de segurança da informação (Lei et al., 2025).

A utilização de dados biométricos, por sua natureza sensível e irreversível, impõe desafios adicionais. Vazamentos ou usos indevidos desses dados podem causar danos permanentes aos titulares, uma vez que características biométricas não podem ser substituídas como senhas convencionais (Manisha; Kumar, 2020). Assim, a conformidade com a LGPD exige a adoção de princípios como *privacy by design*⁵, minimização de dados e mecanismos de proteção que reduzam riscos de exposição e discriminação (Gajmal; Udayakumar, 2023).

Nesse contexto, este trabalho apresenta o desenvolvimento de uma arquitetura de sistema para o registro de chegada e entrada na fila de atendimento clínico por meio de reconhecimento facial, fundamentada na computação de borda e orientada por requisitos de segurança e conformidade legal. A solução busca eliminar a dependência de servidores externos, evitar a persistência de imagens faciais e assegurar o tratamento adequado dos dados biométricos, alinhando-se às tendências de processamento local para preservação de privacidade (Dalvi et al., 2025).

O processo tradicional de registro de presença em clínicas de saúde e

³ Subcampo da Inteligência Artificial que utiliza redes neurais com múltiplas camadas para modelar e processar dados complexos, imitando o funcionamento do cérebro humano.

⁴ Modelo em que o processamento de dados ocorre no próprio dispositivo local (ou muito próximo a ele), em vez de depender de servidores em nuvem, garantindo maior rapidez e segurança.

⁵ Metodologia que determina que a proteção de dados deve ser incorporada em todas as etapas do desenvolvimento de um sistema, desde o seu rascunho inicial.

desenvolvimento familiar é predominantemente manual e dependente de intervenção humana constante na recepção, o que gera filas e retrabalho, amplia o risco de falhas na identificação de pacientes e expõe dados pessoais sensíveis a vulnerabilidades. Desse cenário emerge a questão que orienta esta investigação: como automatizar o registro inicial (*check-in*) em clínicas de saúde por meio de reconhecimento facial, garantindo a eficiência operacional e, simultaneamente, a segurança e a privacidade dos dados biométricos em estrita conformidade com a LGPD? A formulação atende aos critérios de clareza, precisão e operacionalidade apontados por Gil (2019, p. 57-58), e traduz a necessidade de alinhar a inovação tecnológica no setor de saúde às exigências legais de proteção de dados, mitigando os riscos associados à irreversibilidade da biometria sem comprometer a agilidade do atendimento.

Como resposta provisória a essa questão — formulada, conforme recomendam Marconi e Lakatos (2017, p. 126, 129), em termos mensuráveis e empiricamente verificáveis —, admite-se que a implementação de uma arquitetura de reconhecimento facial baseada em computação de borda e pseudonimização criptográfica permite automatizar o registro de consultas clínicas de forma segura, garantindo a não persistência de imagens faciais brutas e a adequação aos princípios da LGPD (H1). Dessa proposição decorrem duas hipóteses secundárias: que microcomputadores de placa única (SBC)⁶ de baixo custo dispõem de capacidade computacional suficiente para executar algoritmos de detecção e *embedding* facial com latência aceitável para a dinâmica de uma recepção clínica (H2); e que o desempenho técnico alcançado pelo protótipo indica viabilidade para substituir o processo manual pela autenticação biométrica passiva, otimizando o tempo de *check-in* e mitigando erros de identificação (H3). Tais hipóteses foram testadas mediante a construção de um protótipo funcional e a execução de ensaios em ambiente controlado, o que permitiu comprovar a viabilidade técnica da arquitetura e estimar os ganhos operacionais sem intervenção direta no fluxo real de atendimento da clínica.

O estudo adota a metodologia da *Design Science Research* (DSR), conforme definida por Hevner et al. (2004), que permite a criação e avaliação de um artefato tecnológico voltado à resolução de um problema prático. A condução da pesquisa segue o processo metodológico proposto por Peffers et al. (2007). Como contribuição, espera-se apresentar uma proposta viável e segura para a automação do processo de *check-in* em clínicas de saúde, alinhando inovação tecnológica, eficiência operacional e respeito à legislação vigente.

⁶ Do inglês *Single Board Computer*, refere-se a um computador completo construído em uma única placa de circuito impresso (como o Raspberry Pi ou a placa Labrador), muito utilizado em projetos de eletrônica embarcada.

1.1 OBJETIVOS

Este capítulo estabelece as metas da pesquisa, divididas entre o objetivo geral de desenvolver um protótipo de reconhecimento facial seguro e os objetivos específicos que detalham as etapas técnicas e metodológicas para sua execução.

1.1.1 Objetivo geral

Propor uma arquitetura de sistema para registro de consultas clínicas via reconhecimento facial, baseada na análise de requisitos de segurança e conformidade com a LGPD para o tratamento de dados biométricos.

1.1.2 Objetivos específicos

1. Realizar uma revisão bibliográfica sobre reconhecimento facial, segurança de dados biométricos e os princípios da LGPD;
2. Analisar o processo de registro de consultas da clínica;
3. Projetar a arquitetura de software do sistema, prevendo a integração com sistemas legados e os protocolos de segurança;
4. Desenvolver um protótipo funcional;
5. Avaliar a usabilidade, desempenho e a conformidade do protótipo funcional.

1.2 JUSTIFICATIVA

O processo de registro de presença na clínica de saúde e desenvolvimento familiar, objeto de estudo deste trabalho, atualmente se baseia em um fluxo de trabalho manual. Conforme apurado, o *check-in* é centralizado na recepção, onde os colaboradores realizam a identificação do paciente e o preenchimento de sua chegada no sistema. Este cadastro exige a inserção de um extenso conjunto de dados, que abrange desde informações civis e de contato (como nome, CPF, endereço e responsáveis) e dados clínicos (tipo sanguíneo, convênio), até preferências pessoais voltadas à humanização do atendimento (como preferência musical e personagens favoritos).

Esta dependência da intervenção humana para validar a presença insere-se em um contexto mais amplo da segurança do paciente, onde erros de identificação são uma causa significativa de erros médicos evitáveis (Sadahide et al., 2024). Essa dificuldade na gestão da presença em tempo real representa, portanto, uma clara oportunidade para otimização, eliminando processos manuais e, outrossim, mitigando riscos de erros.

Diante desse cenário, a aplicação de tecnologias de reconhecimento facial surge como uma solução promissora (Lei et al., 2025). A viabilidade e segurança desta abordagem em ambientes hospitalares já foram demonstradas, com estudos clínicos

comprovando altas taxas de autenticação mesmo em condições adversas (Sadahide et al., 2024). No contexto brasileiro, a proposta alinha-se às principais aplicações de Inteligência Artificial (IA) já em uso no setor, que se destinam majoritariamente a organizar processos clínicos e administrativos (Comitê Gestor da Internet no Brasil, 2024).

Contudo, a implementação de tal tecnologia transcende o desafio puramente técnico, adentrando uma área de alta complexidade: a segurança e o tratamento ético de dados biométricos. Com a vigência da Lei Geral de Proteção de Dados (LGPD), torna-se imperativo que sistemas dessa natureza sejam pautados por uma arquitetura robusta, preenchendo uma lacuna crítica, visto que a adequação à LGPD ainda é um desafio para a maioria dos estabelecimentos de saúde no país (Comitê Gestor da Internet no Brasil, 2024).

Para endereçar tais desafios e alinhar inovação à conformidade regulatória, este trabalho propõe uma arquitetura de sistema para registro de consultas clínicas via reconhecimento facial, baseada na análise de requisitos de segurança e conformidade com a LGPD para o tratamento de dados biométricos.

Portanto, este trabalho justifica-se pela necessidade de desenvolver uma solução que resolva um problema prático de gestão em diversas clínicas que atuam no segmento de saúde e desenvolvimento familiar, operando de maneira responsável, inovadora e alinhada a uma tecnologia com eficácia já validada. A pesquisa contribuirá com a proposição de uma arquitetura de sistema de reconhecimento facial segura e em conformidade com os requisitos da LGPD, oferecendo um modelo escalável.

2 REFERENCIAL TEÓRICO

2.1 A REVOLUÇÃO DO DEEP LEARNING NO RECONHECIMENTO FACIAL

Até o início da década de 2010, o reconhecimento facial em ambientes não controlados (*'in the wild'*)⁷ apresentava barreiras significativas de precisão. Um dos marcos que iniciou a superação desses desafios foi o sistema DeepFace, apresentado por Taigman et al. (2014). Este trabalho foi um dos primeiros a demonstrar que uma Rede Neural Profunda (DNN)⁸, treinada com um conjunto de dados em larga escala, poderia alcançar um desempenho próximo ao da capacidade humana.

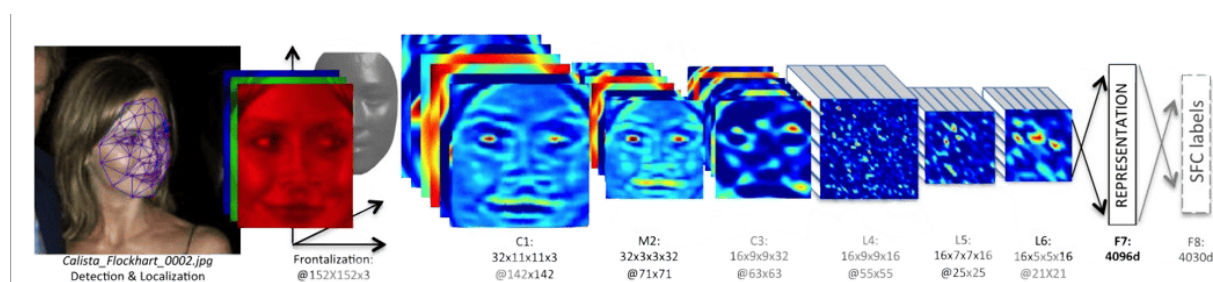
O sistema DeepFace utilizava uma rede de nove camadas com mais de 120 milhões de parâmetros, treinada em um dos maiores conjuntos de dados da época, composto por quatro milhões de imagens faciais de mais de 4.000 identidades (Taigman et al., 2014). Uma das principais contribuições do DeepFace foi a introdução de um

⁷ Jargão acadêmico para descrever testes realizados em ambientes cotidianos do mundo real, sem o controle de iluminação ou posicionamento típico de laboratórios.

⁸ Do inglês *Deep Neural Network*, é uma rede neural artificial com diversas camadas ocultas de processamento entre a entrada e a saída de dados.

sistema de alinhamento facial baseado em modelagem 3D explícita. Esse método permitia “frontalizar” faces detectadas em diferentes poses, normalizando a entrada e aumentando a robustez da rede. Como resultado, o DeepFace atingiu uma precisão de 97,35% no renomado benchmark⁹ *Labeled Faces in the Wild* (LFW), provando a superioridade da abordagem de *deep learning* sobre os métodos tradicionais (Taigman et al., 2014). A arquitetura completa deste sistema está ilustrada na Figura 1.

Figura 1 – Arquitetura da rede neural profunda DeepFace



Taigman et al. (2014, p. 4).

2.2 FACENET: MAPEANDO FACES PARA UM ESPAÇO DE SIMILARIDADE

Seguindo o sucesso do DeepFace, Schroff, Kalenichenko e Philbin (2015), do Google, propuseram uma arquitetura ainda mais eficiente e direta: o FaceNet. Este sistema introduziu uma mudança de paradigma: em vez de treinar a rede para classificar um número fixo de identidades, o objetivo passou a ser aprender um “*embedding*”¹⁰ unificado.

Um *embedding* é um mapeamento direto de uma imagem de rosto para um vetor em um espaço euclidiano¹¹ compacto, neste caso, de 128 dimensões (Schroff; Kalenichenko; Philbin, 2015). A inovação central do FaceNet é que, neste espaço, a distância euclidiana (L2) entre os vetores de duas imagens corresponde diretamente à medida de similaridade facial. Desta forma, imagens da mesma pessoa são mapeadas para pontos muito próximos nesse espaço, enquanto imagens de pessoas distintas são mapeadas para pontos distantes (Schroff; Kalenichenko; Philbin, 2015).

Para alcançar esse resultado, os autores introduziram uma nova função de perda chamada “*triplet loss*”¹². Durante o treinamento, a rede analisa um “triplete” de imagens:

⁹ Um teste de avaliação padronizado utilizado na computação para comparar o desempenho e a precisão de diferentes sistemas ou algoritmos sob as mesmas condições.

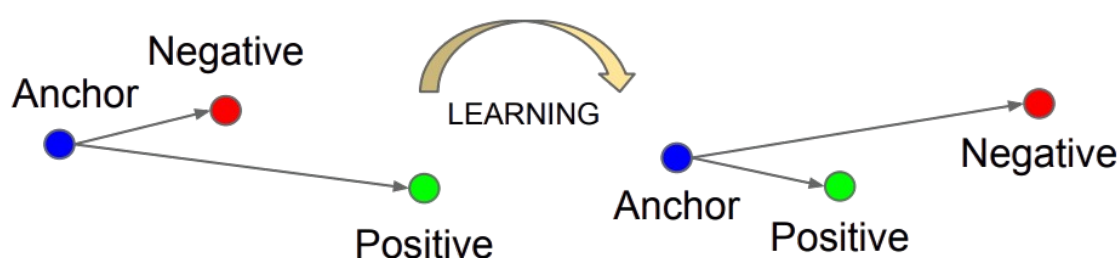
¹⁰ Representação matemática e vetorial das características de um rosto, transformando a imagem em um conjunto de números que a máquina consegue ler e comparar.

¹¹ Conceito matemático onde a similaridade entre duas faces é medida pela distância geométrica entre seus vetores. Quanto menor a distância, maior a probabilidade de pertencerem à mesma pessoa.

¹² Algoritmo de treinamento que ensina a rede neural comparando três imagens simultaneamente: uma base (âncora), uma da mesma pessoa (positiva) e uma de pessoa diferente (negativa), aproximando matematicamente rostos iguais e afastando os diferentes.

uma imagem “âncora”(x^a), uma imagem “positiva”(x^p) (outra foto da mesma pessoa) e uma imagem “negativa”(x^n) (foto de uma pessoa diferente). O objetivo da rede é aprender a minimizar a distância entre a âncora e a positiva ($\|f(x^a) - f(x^p)\|^2$), ao mesmo tempo em que maximiza a distância entre a âncora e a negativa ($\|f(x^a) - f(x^n)\|^2$) (Schroff; Kalenichenko; Philbin, 2015). O processo de aprendizado por meio desta função é representado na Figura 2.

Figura 2 – Representação do processo de aprendizado pela função Triplet Loss



Fonte: Schroff, Kalenichenko e Philbin (2015, p. 817).

Este método de treinamento “end-to-end”¹³ permitiu ao FaceNet estabelecer um novo recorde de precisão no LFW, com 99,63%, e sua abordagem de *embedding* tornou-se a base para a maioria dos sistemas de reconhecimento, verificação e agrupamento de faces modernos.

A infraestrutura de hardware adotada para a implementação do protótipo baseia-se na arquitetura de computação de borda, utilizando o microcomputador de placa única Labrador de 32 bits. Conforme as especificações técnicas fornecidas pelo fabricante (Caninos Loucos, 2024), o dispositivo é equipado com uma CPU Quad-core ARM® Cortex™-A9R4, 2GB de memória RAM LPDDR3 e armazenamento interno de 16GB eMMC, executando o sistema operacional Linux (distribuição Debian).

A escolha por este hardware de baixo custo e portabilidade impõe, contudo, restrições computacionais. Como observam Wang e Deng (Wang; Deng, 2021), a execução de modelos de reconhecimento facial baseados em redes neurais profundas demanda alto poder de processamento para garantir baixa latência¹⁴, o que é um desafio em dispositivos embarcados sem aceleração dedicada (GPU). Portanto, a utilização da Labrador neste projeto serve para validar a viabilidade da arquitetura

¹³ Abordagem de aprendizado de máquina onde a rede neural aprende todo o processo diretamente dos dados de entrada (imagem bruta) até o resultado final, sem exigir programação manual de etapas intermediárias.

¹⁴ O tempo de atraso entre o envio de uma informação e a resposta do sistema. Em sistemas em tempo real, busca-se sempre a menor latência possível.

proposta em cenários de recursos limitados, assumindo-se o compromisso (*trade-off*)¹⁵ entre custo de implantação e tempo de inferência.

2.3 VALIDAÇÃO DO RECONHECIMENTO FACIAL NO SETOR DE SAÚDE

A eficácia das tecnologias de *deep learning* descritas, até então validadas em bancos de dados públicos, começou a ser testada rigorosamente em aplicações práticas no setor de saúde. A identificação correta de pacientes é um pilar para a segurança no atendimento, sendo que erros de identificação ocorrem em todas as etapas do diagnóstico e tratamento (Sadahide et al., 2024).

Esses achados de Sadahide et al. (Sadahide et al., 2024) possuem relevância direta para a aplicação proposta neste trabalho, especialmente no que tange à humanização do atendimento. Em uma clínica voltada ao desenvolvimento familiar, é comum o acolhimento de pacientes que podem apresentar sensibilidade sensorial, aversão ao contato direto com equipamentos de monitoramento ou inquietação motora, dificultando a manutenção de uma postura estática para a captura de imagem. A validação do algoritmo em cenários onde o sujeito não está posando ativamente (como pacientes deitados ou de olhos fechados, conforme o estudo) sugere que a tecnologia é capaz de realizar a identificação de forma menos intrusiva. Isso viabiliza um processo de *check-in* fluido e passivo, mitigando o estresse de pacientes que teriam dificuldade em colaborar com protocolos rígidos de posicionamento frente à câmera. A Figura 3 ilustra os diversos cenários de validação clínica abordados no estudo.

¹⁵ Termo técnico que designa um compromisso de engenharia onde se abdica de uma vantagem (ex: altíssimo poder de processamento) para obter outra (ex: hardware de baixo custo e menor consumo de energia).

Figura 3 – Cenários de avaliação do reconhecimento facial em ambiente hospitalar



Fonte: Sadahide et al. (2024, p. 3).

Os resultados demonstraram uma robustez notável da tecnologia. A taxa de certificação correta em pacientes sem máscara foi de 99,7% (Sadahide et al., 2024). Mais importante ainda, mesmo em condições simuladas de sono noturno (baixa iluminação de 3-4 lux¹⁶, olhos fechados e em posição supina ou lateral), a taxa de autenticação foi superior a 99% (99,3%) (Sadahide et al., 2024). Embora o uso de máscaras tenha reduzido a precisão geral, o sistema ainda alcançou 100% de sucesso para pacientes sentados e com os olhos abertos (Sadahide et al., 2024). O estudo concluiu que o reconhecimento facial é um sistema “seguro e aceitável” para a identificação de pacientes, onde a precisão é crucial. Esta validação empírica fornece uma base sólida que justifica a proposição de sistemas de check-in automatizados por biometria facial, como o proposto neste trabalho.

Não obstante os resultados promissores, a implementação dessa tecnologia demanda o reconhecimento de suas limitações intrínsecas. Conforme evidenciado no estudo e corroborado pela literatura especializada, oclusões parciais — como o uso de máscaras cirúrgicas — comprometem a extração de características fiduciais¹⁷, ocasionando redução na precisão comparativamente a faces descobertas. Ademais, a generalização para populações heterogêneas constitui um desafio crítico; auditorias

¹⁶ Unidade de medida padronizada internacionalmente para quantificar a iluminância, ou seja, a quantidade de luz que incide sobre uma superfície.

¹⁷ Pontos de referência fixos no rosto humano (como distância entre os olhos, ponta do nariz e contorno da boca) utilizados pelos algoritmos de mapeamento facial.

independentes, como a conduzida por Buolamwini e Gebru (Buolamwini; Gebru, 2018), revelam que algoritmos de análise facial podem exibir disparidades acentuadas de acurácia entre distintos grupos demográficos, o que impõe a necessidade de validação contínua para mitigar vieses raciais ou de gênero em aplicações de saúde.

2.4 PROTEÇÃO DE DADOS BIOMÉTRICOS E CONFORMIDADE COM A LGPD

A implementação de sistemas biométricos no setor de saúde impõe desafios rigorosos quanto à privacidade e proteção de dados. No Brasil, a Lei Geral de Proteção de Dados (LGPD) classifica os dados biométricos como **dados pessoais sensíveis**, exigindo salvaguardas técnicas robustas para evitar acessos não autorizados e vazamentos que poderiam resultar em discriminação ou danos irreparáveis aos titulares (Aragão; Schiocchet, 2020). A adequação do Sistema Único de Saúde (SUS) e de clínicas privadas a essa norma demanda não apenas revisões administrativas, mas a adoção de arquiteturas de segurança da informação que garantam a confidencialidade desde a concepção.

Um dos principais riscos associados à biometria é a **irreversibilidade**: diferentemente de uma senha, que pode ser alterada em caso de comprometimento, características faciais são permanentes. Para mitigar esse risco, a literatura propõe o conceito de **Biometria Cancelável** (*Cancelable Biometrics*)¹⁸. Segundo Manisha e Kumar (2020), essa abordagem consiste em aplicar transformações matemáticas intencionais aos dados biométricos originais antes do armazenamento. Dessa forma, armazena-se apenas o *template* transformado; caso este seja comprometido, ele pode ser descartado (“cancelado”) e um novo pode ser gerado, garantindo que a imagem original da face do paciente nunca seja exposta ou armazenada diretamente.

Além da proteção do dado armazenado em repouso (*data-at-rest*)¹⁹, a segurança do sistema envolve a garantia da autenticidade durante a captura. Sistemas de reconhecimento facial estão sujeitos a ataques de *spoofing*²⁰, onde terceiros tentam burlar a autenticação utilizando fotos ou vídeos da vítima. Sharma e Selwal (Sharma; Selwal, 2023) destacam que a incorporação de mecanismos de *Liveness Detection*²¹ é um requisito essencial para garantir a integridade do processo de check-in, impedindo fraudes de identidade no ambiente clínico.

¹⁸ Técnica de segurança que armazena uma versão matematicamente distorcida do rosto do usuário. Se o banco de dados for invadido, essa distorção pode ser descartada e substituída por uma nova, protegendo a face real do indivíduo.

¹⁹ Termo de cibersegurança que se refere aos dados que estão armazenados fisicamente no disco rígido ou banco de dados, em oposição aos dados em trânsito (que estão sendo enviados pela rede).

²⁰ Tentativa de enganar o sistema de reconhecimento facial utilizando fotos impressas, vídeos ou máscaras tridimensionais de outra pessoa.

²¹ Mecanismo de segurança que verifica se a face apresentada à câmera pertence a uma pessoa viva e presente no local, combatendo fraudes e ataques.

2.4.1 A lei nº 13.709/2018 e o tratamento de dados biométricos

A Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — constitui o marco normativo que disciplina o tratamento de dados pessoais no Brasil, inclusive por meio digital, e cujos fundamentos incluem o respeito à privacidade, a autodeterminação informativa e a inviolabilidade da intimidade, da honra e da imagem (Brasil, 2018). Sua incidência sobre o artefato proposto é direta, uma vez que a captura, a extração de características e o armazenamento de representações faciais configuram, nos termos do art. 5º, inciso X, operações de tratamento.

O ponto de partida da análise é a qualificação jurídica do dado. O art. 5º, inciso II, define como **dado pessoal sensível** aquele referente a origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou à vida sexual e, expressamente, o **dado genético ou biométrico** quando vinculado a uma pessoa natural (Brasil, 2018). Trata-se, portanto, de categoria submetida a regime jurídico mais rigoroso: enquanto o tratamento de dados pessoais comuns admite dez hipóteses autorizativas (art. 7º), o de dados sensíveis restringe-se às hipóteses do art. 11, entre as quais o consentimento destacado e específico do titular e a tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde ou por autoridade sanitária. No contexto de uma recepção clínica, a base legal aplicável é o consentimento específico e destacado, previsto no art. 11, inciso I, o que impõe que a adesão ao *check-in* biométrico seja facultativa e que permaneça disponível a alternativa de atendimento convencional.

O art. 6º enumera os princípios que devem orientar toda atividade de tratamento, três dos quais estruturaram diretamente as decisões de projeto descritas neste trabalho. O princípio da **finalidade** (inciso I) exige propósitos legítimos, específicos e explícitos, vedando o tratamento posterior de forma incompatível — razão pela qual o vetor biométrico do artefato serve unicamente à confirmação de presença, não alimentando qualquer outra função. O princípio da **necessidade** (inciso III) determina a limitação ao mínimo indispensável para a realização das finalidades, o que fundamenta a decisão de descartar a imagem facial imediatamente após a extração das características, preservando-se apenas o vetor numérico. Por fim, o princípio da **segurança** (inciso VII) impõe a utilização de medidas técnicas aptas a proteger os dados de acessos não autorizados, materializado no artefato pela cifragem do repositório e pela pseudonimização dos identificadores nominais.

A Lei oferece ainda instrumento específico que sustenta a arquitetura adotada. O art. 13, § 4º, define **pseudonimização** como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação mantida separadamente pelo controlador em ambiente controlado e seguro (Brasil, 2018). Complementarmente, o art. 12 estabelece que os dados anonimizados não são considerados dados pessoais para os fins da Lei, salvo quando o

processo de anonimização puder ser revertido com esforços razoáveis. É precisamente nesse dispositivo que reside a relevância jurídica da biometria cancelável discutida na seção anterior: ao aplicar uma transformação matemática irreversível ao vetor facial antes da persistência, busca-se afastar a possibilidade de reversão com esforços razoáveis, reduzindo a superfície de risco em caso de incidente de segurança.

Deve-se registrar que o art. 46 atribui aos agentes de tratamento o dever de adotar medidas de segurança aptas a proteger os dados pessoais, e que o art. 46, § 2º, estende essa obrigação desde a fase de concepção do produto ou serviço até a sua execução — consagração normativa do princípio de *privacy by design* que orienta a arquitetura aqui proposta. O descumprimento sujeita o controlador às sanções administrativas do art. 52, que alcançam multa de até 2% do faturamento, limitada a cinquenta milhões de reais por infração. Soma-se a isso o rol de direitos do titular previsto no art. 18, entre os quais a confirmação da existência de tratamento, o acesso aos dados, a eliminação dos dados tratados com consentimento e a revogação do consentimento — direitos cujo atendimento pressupõe que o sistema permita, a qualquer tempo, o descarte do registro biométrico de um paciente específico.

2.4.2 Riscos éticos e vieses algorítmicos

A conformidade com a LGPD no uso de dados biométricos transcende a segurança da informação, abrangendo também a garantia de tratamento não discriminatório dos titulares. A literatura técnica evidencia que sistemas de reconhecimento facial podem reproduzir e amplificar preconceitos sociais se não forem auditados rigorosamente. O estudo seminal *Gender Shades*, conduzido por Buolamwini e Gebru (2018), revelou disparidades críticas de precisão em algoritmos comerciais de análise facial. As autoras demonstraram que, enquanto a taxa de erro para homens de pele clara era inferior a 1%, para mulheres de pele escura essa taxa chegava a 34,7%, evidenciando um viés interseccional decorrente de conjuntos de dados de treinamento desbalanceados (Buolamwini; Gebru, 2018).

Corroborando esses achados em escala global, o relatório do *Face Recognition Vendor Test* (FRVT), publicado pelo *National Institute of Standards and Technology* (NIST), analisou 189 algoritmos de reconhecimento facial e identificou diferenciais demográficos consistentes (Grother; Ngan; Hanaoka, 2019). O estudo apontou que as taxas de falsos positivos²² são significativamente mais altas para mulheres, idosos, crianças e, notadamente, para populações da África Ocidental e do Leste Asiático (Grother; Ngan; Hanaoka, 2019). No contexto de uma clínica médica, tais vieses representam um risco ético inaceitável, podendo resultar em constrangimentos ou negação de acesso, o que viola o princípio da não discriminação previsto na LGPD.

²² Em sistemas de biometria, ocorre quando o sistema identifica incorretamente uma pessoa, confundindo-a com outra que está cadastrada no banco de dados.

Portanto, a arquitetura proposta mitiga esses riscos ao manter a validação *human-in-the-loop*²³ no processo para casos de falha e ao adotar o princípio da transparência sobre as limitações da tecnologia.

2.5 ESTUDOS RELACIONADOS

A implementação de sistemas de reconhecimento facial em dispositivos de borda tem sido objeto de estudos recentes, visando aliar baixo custo de *hardware* à eficiência de processamento. A revisão da literatura buscou identificar trabalhos que utilizassem arquiteturas de microcomputadores de placa única similares ao Labrador 32-bits adotado neste projeto.

No âmbito da viabilidade técnica, Dalvi et al. (2025) apresentaram um sistema de detecção facial em tempo real utilizando a plataforma Raspberry Pi. Os autores demonstraram que dispositivos com processadores ARM e recursos limitados de memória são capazes de executar algoritmos de Inteligência Artificial, como Haar Cascades e redes *MobileNet*²⁴, atingindo taxas de processamento entre 15 e 20 quadros por segundo (FPS). Este estudo é fundamental para validar a escolha do *hardware* deste TCC, comprovando que a arquitetura de computação de borda pode substituir servidores dedicados em tarefas de vigilância e controle de acesso.

Avançando para a aplicação em controle de presença, (Kurniasari et al., 2025) desenvolveram um sistema de monitoramento inteligente, também baseado em Raspberry Pi, integrado a algoritmos de *Local Binary Patterns* (LBP) e detecção Haar Cascade. O trabalho descreve um fluxo operacional onde a captura, detecção e reconhecimento ocorrem localmente no dispositivo. Os resultados obtidos, com acurácia média superior a 92% em distâncias de até 30 cm, reforçam a eficácia de SBCs para automação de *check-in*. Contudo, a arquitetura proposta por (Kurniasari et al., 2025) foca primordialmente na funcionalidade operacional sem detalhar mecanismos avançados de proteção dos *templates* biométricos.

Embora os trabalhos de Dalvi et al. (2025) e Kurniasari et al. (2025) validem a infraestrutura tecnológica, a aplicação em ambientes de saúde exige camadas adicionais de segurança não abordadas nesses estudos. Conforme alertam Gajmal e Udayakumar (2023), sistemas de *Smart Healthcare* são alvos frequentes de ataques. A conformidade com a LGPD, discutida no contexto brasileiro por Oliveira e Costa (2019) e nas notas técnicas do INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (2023), impõe que o tratamento de dados sensíveis garanta a irreversibilidade da biometria.

²³ Modelo de operação onde a Inteligência Artificial não toma decisões críticas de forma 100% autônoma, exigindo a supervisão ou validação de um ser humano (neste caso, o atendente da recepção).

²⁴ Haar Cascades, MobileNet e *Local Binary Patterns* (LBP) são algoritmos e arquiteturas clássicas de visão computacional, conhecidos por serem mais leves e rápidos que as redes neurais densas, facilitando o uso em dispositivos com hardware limitado.

Dessa forma, este trabalho se diferencia da literatura correlata ao propor uma arquitetura híbrida: apropria-se da viabilidade técnica demonstrada por Dalvi et al. (2025) e do fluxo de automação de Kurniasari et al. (2025), mas inova ao implementar uma camada de segurança baseada em criptografia e não-persistência de imagens brutas, preenchendo a lacuna de privacidade crítica para aplicações clínicas. As principais características dos estudos analisados em comparação com a presente proposta são sintetizadas no Quadro 1.

Quadro 1 – Quadro comparativo de trabalhos relacionados

Trabalhos	Processamento na borda (SBC)	Automação de presença	Aplicação em saúde	Conformidade LGPD	Criptografia / <i>template</i>
Dalvi et al. (2025)	✓	–	–	–	–
Kurniasari et al. (2025)	✓	✓	–	–	–
Gajmal e Udayakumar (2023)	–	–	✓	✓	✓
Oliveira e Costa (2019)	–	–	–	✓	–
Este trabalho	✓	✓	✓	✓	✓

Legenda: ✓ Atendido; – Não abordado.

Fonte: Dados obtidos de Dalvi et al. (2025), Kurniasari et al. (2025), Gajmal e Udayakumar (2023), Oliveira e Costa (2019).

3 METODOLOGIA

3.1 CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa caracteriza-se, quanto aos seus objetivos, como *aplicada e descritiva*, uma vez que visa desenvolver um artefato tecnológico para resolver um problema prático no setor de saúde. Segundo Gil (2019, p. 43-44), pesquisas aplicadas objetivam gerar conhecimentos para aplicação prática na solução de problemas específicos.

Quanto à abordagem, trata-se de uma pesquisa *quali-quantitativa*, pois combina a análise qualitativa (viabilidade ética, requisitos LGPD) com a medição quantitativa de dados (tempo de inferência e tempo de check-in). Creswell (2010, p. 21-22) destaca que a abordagem mista é adequada quando a complexidade do fenômeno exige tanto a análise numérica quanto a compreensão interpretativa dos processos.

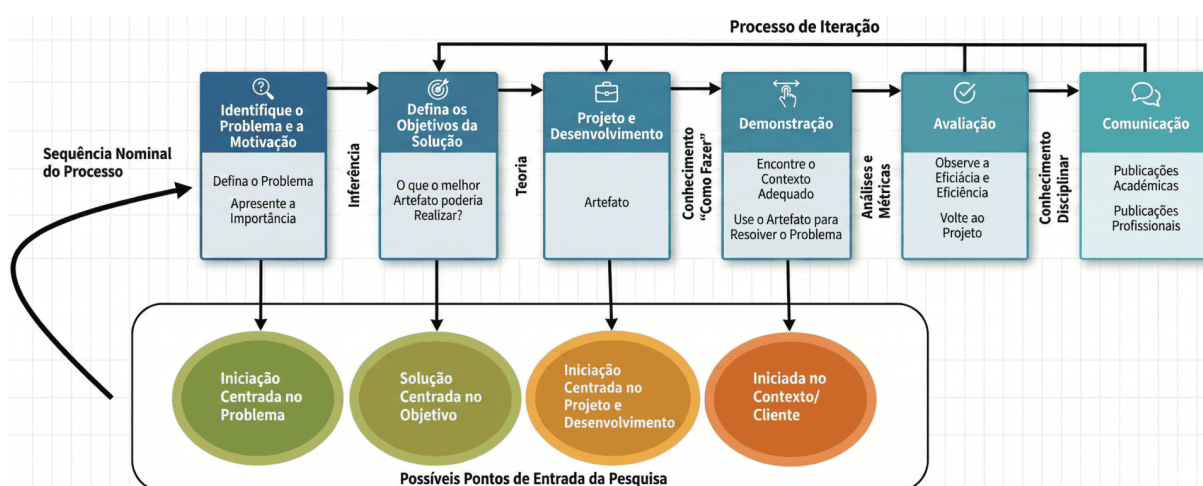
Em relação aos procedimentos técnicos, foi realizado um estudo de caso alinhado ao paradigma da *Design Science Research* (DSR), que se caracteriza pela construção e avaliação de artefatos tecnológicos visando a resolução de problemas organizacionais (Hevner et al., 2004).

3.2 PROCEDIMENTOS METODOLÓGICOS (DSRM)

Para o desenvolvimento deste trabalho, adotou-se a abordagem da *Design Science Research* (DSR). Segundo Hevner et al. (2004), o paradigma da *Design Science* busca estender as fronteiras das capacidades humanas e organizacionais através da criação de artefatos novos e inovadores. Diferente das ciências comportamentais, que buscam desenvolver teorias para explicar ou prever fenômenos, a DSR foca na construção e avaliação de artefatos tecnológicos para resolver problemas organizacionais identificados.

A condução da pesquisa seguiu o *Design Science Research Methodology* (DSRM), um modelo de processo proposto por Peffers et al. (2007) que sintetiza a DSR em um fluxo lógico e rigoroso. Este fluxo metodológico, composto por seis atividades sequenciais e iterativas, foi ilustrado na Figura 4.

Figura 4 – Modelo de Processo da Design Science Research (DSRM)



Fonte: Adaptado de Peffers et al. (2007)

3.2.1 Identificação do problema e motivação

O estudo partiu da análise das vulnerabilidades presentes no processo manual de registro de presença na clínica de saúde e desenvolvimento familiar. Identificou-se que a gestão tradicional de dados, baseada em fichas físicas ou sistemas não criptografados, expunha os pacientes a riscos de privacidade e gerava ineficiência operacional (filas e erros de digitação). A motivação central residuiu na necessidade de adequação desses ambientes à Lei Geral de Proteção de Dados (LGPD), garantindo segurança sem comprometer a agilidade do atendimento.

3.2.2 Definição dos objetivos da solução

Estabeleceu-se como meta o desenvolvimento de um protótipo de reconhecimento facial seguro e de baixo custo. Os objetivos específicos definidos para o artefato foram:

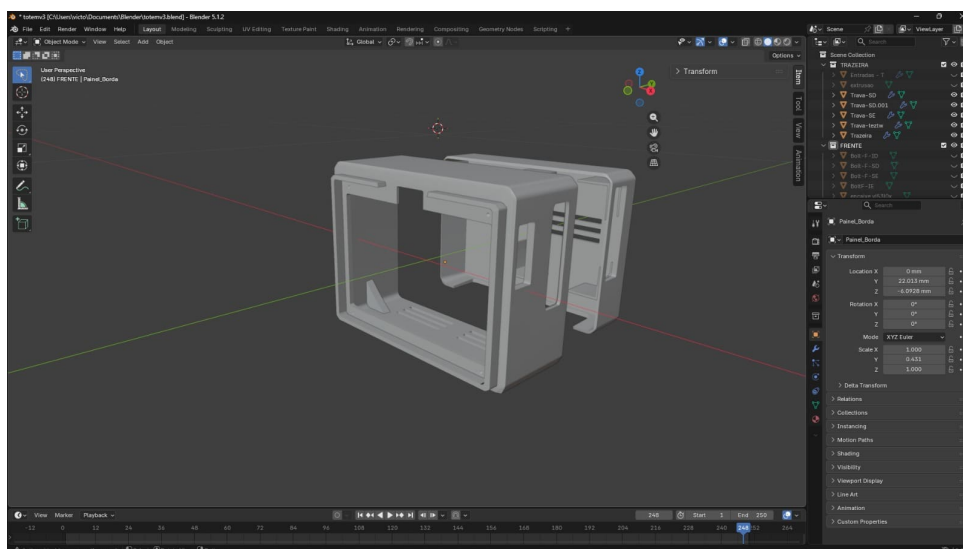
- Operar em arquitetura de borda para eliminar a dependência de servidores externos;
- Garantir a não-persistência de imagens faciais brutas (privacidade desde a concepção);
- Manter custo de *hardware* acessível para viabilizar a adoção em clínicas de pequeno e médio porte.

3.2.3 Design e desenvolvimento

Esta etapa compreendeu a construção física e lógica do artefato, concebido sob o paradigma da computação de borda. Adotou-se uma arquitetura distribuída e integrada via rede local sem fio (Wi-Fi), composta por um nó sensor para captura de imagem e um nó de processamento principal. Essa divisão isolou a carga de processamento de visão computacional, mitigando limitações térmicas e de memória.

Fisicamente, o protótipo foi alojado em uma carcaça customizada. A modelagem tridimensional estrutural (CAD) foi inteiramente desenvolvida no *software* Blender, conforme ilustrado na Figura 5, sendo projetada para acomodar os componentes eletrônicos de forma segura e incorporar ergonomicamente um *display touch* HDMI de 7 polegadas para a interface com o usuário. Após a validação do *design* virtual, a estrutura foi materializada por meio de impressão 3D.

Figura 5 – Modelagem tridimensional da carcaça do protótipo no *software* Blender



Fonte: Elaborado pelo autor (2025).

A Figura 6 registra o artefato já materializado. Na imagem *a* observa-se a carcaça impressa em 3D fechada, com o *display* embutido e a abertura frontal superior destinada ao módulo de câmera; a inclinação da face frontal foi dimensionada para posicionar a lente na altura aproximada do rosto de um adulto em pé, dispensando ajuste manual por parte do paciente. A imagem *b* apresenta o totem em operação, exibindo a interface no estado de espera — com a mensagem de aproximação, o painel de vídeo e os botões de captura e de modo servidor —, enquanto o gatilho de *hardware* mantém a inferência biométrica em repouso.

Figura 6 – Protótipo do totem materializado por impressão 3D



(a) Carcaça fechada



(b) Interface em operação

Fonte: Elaborado pelo autor (2026).

Para o módulo de aquisição de imagem, utilizou-se um microcontrolador ESP32-CAM equipado com sensor OV2640. Seu *firmware* foi desenvolvido em linguagem C++, utilizando a API nativa ESP-IDF²⁵, para atuar como um servidor HTTP. O dispositivo proveu um fluxo de vídeo contínuo no formato MJPEG²⁶, configurado dinamicamente com resolução VGA (640x480) e compressão JPEG em nível 10, visando otimizar o *payload*²⁷ transmitido pela rede. O endereçamento do módulo foi gerenciado via protocolo DHCP²⁸.

O processamento principal foi executado em um microcomputador Labrador 32-bits, cujo *software* central, desenvolvido em Python, orquestrou a interface gráfica e a inferência de redes neurais por meio da biblioteca *Face Recognition*. Para contornar

²⁵ Conjunto de ferramentas oficiais de desenvolvimento da Espressif para os microcontroladores da família ESP32.

²⁶ *Motion JPEG* é um formato de vídeo onde cada quadro da imagem é comprimido individualmente, facilitando a transmissão fluida pela rede Wi-Fi.

²⁷ Em redes de computadores, refere-se à quantidade real de dados transmitidos em um pacote, excluindo os cabeçalhos e as informações de controle da rede.

²⁸ Protocolo de rede que atribui automaticamente endereços IP aos dispositivos conectados, evitando conflitos de conexão na rede local.

gargalos de *hardware*, foram implementadas duas estratégias de otimização. A primeira consistiu em um gatilho de *hardware* baseado em eventos (*Event-Driven*)²⁹, utilizando um sensor de tempo de voo (ToF)³⁰ a laser VL53L0X via barramento I2C³¹, que manteve a Inteligência Artificial em repouso até detectar a presença de um corpo a menos de 80 cm de distância. A segunda estratégia envolveu o processamento assíncrono, no qual a inferência biométrica operou em uma *thread*³² paralela, garantindo a fluidez do sistema e do vídeo durante a extração dos vetores faciais.

No que tange à segurança e à conformidade com a Lei Geral de Proteção de Dados (LGPD), o sistema estruturou-se sob o conceito de proteção de dados *by design*. A arquitetura garantiu a minimização de dados ao processar as imagens brutas exclusivamente em memória RAM volátil³³, descartando-as de forma irreversível logo após a extração das características faciais. Adotou-se também o modelo de biometria cancelável, armazenando vetores faciais transformados por uma matriz ortogonal aleatória³⁴, o que permite a invalidação dos dados sem comprometer a face original do indivíduo. Como camadas adicionais de proteção, o arquivo físico de *encodings* foi cifrado com criptografia AES-128³⁵ (módulo Fernet) e os identificadores nominais registrados no banco de dados SQLite foram ofuscados via função *hash* SHA-256³⁶.

Todo esse fluxo de processamento seguro e de anonimização dos dados biométricos está demonstrado na Figura 7.

²⁹ Paradigma de programação em que o sistema fica inativo e só inicia o processamento pesado de Inteligência Artificial quando um evento físico ocorre (neste caso, o disparo do sensor a laser).

³⁰ Sensor óptico que mede a distância entre o dispositivo e um objeto calculando o tempo que um feixe de luz (neste caso, laser) leva para ir e voltar.

³¹ Protocolo de comunicação serial muito utilizado na eletrônica embarcada para conectar sensores e microcontroladores na mesma placa de circuito.

³² *Thread* é uma linha de execução dentro de um programa. O processamento assíncrono permite que o computador realize mais de uma tarefa ao mesmo tempo (como capturar vídeo e processar faces) sem travar a interface gráfica.

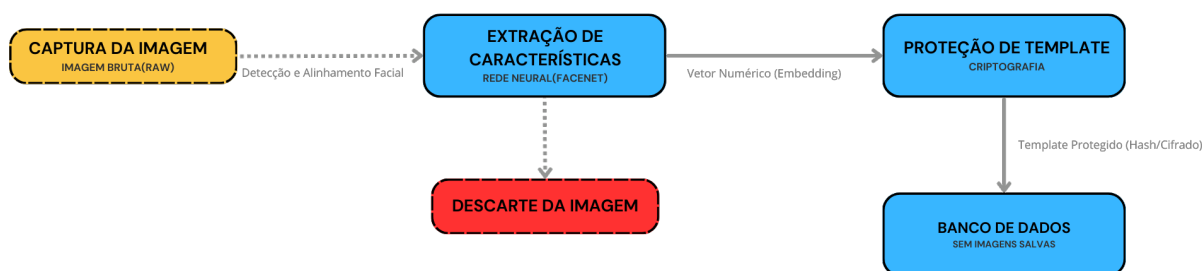
³³ Memória temporária de curtíssimo prazo do computador. Os dados armazenados nesta memória são total e permanentemente apagados assim que o processamento termina ou se o equipamento for reiniciado.

³⁴ Ferramenta matemática que multiplica o vetor da face por um padrão geométrico, "embaralhando" a biometria de forma estruturada. É o mecanismo base da biometria cancelável.

³⁵ Um dos padrões de criptografia simétrica mais seguros e utilizados no mundo, que cifra os dados em blocos usando uma chave de 128 bits.

³⁶ Algoritmo matemático unidirecional que transforma qualquer texto em um código irreversível de tamanho fixo de 256 bits, ocultando os dados nominais da tabela.

Figura 7 – Fluxo de processamento seguro e anonimização de dados biométricos



Fonte: Elaborado pelo autor (2025).

3.2.4 Demonstração

A viabilidade da solução foi demonstrada em ambiente controlado (bancada de testes), simulando o fluxo de *check-in* de uma recepção clínica. O artefato foi submetido a cenários de uso que mimetizaram condições reais e adversas, incluindo tentativas de reconhecimento com oclusões parciais (uso de máscaras) e variações de iluminação, visando validar a robustez do algoritmo em situações cotidianas de saúde.

3.2.5 Avaliação

A eficácia do sistema foi mensurada em três dimensões independentes: desempenho computacional, acurácia biométrica e conformidade com a LGPD.

O desempenho computacional foi aferido pela coleta do tempo de inferência e da temperatura do processador na CPU do microcomputador Labrador, registrados automaticamente na tabela de auditoria do banco de dados a cada evento de reconhecimento.

A acurácia biométrica foi avaliada por meio de um protocolo de identificação 1:N com conjuntos disjuntos de matrícula e de teste. Para cada indivíduo da amostra, três imagens foram destinadas à **galeria** — o conjunto efetivamente cadastrado no cofre biométrico — e as demais foram reservadas como **sondas genuínas**, isto é, capturas da mesma pessoa que o sistema nunca havia processado. Adicionalmente, um subconjunto de identidades foi deliberadamente excluído da galeria, constituindo o grupo de **sondas impostoras**. Sem esse grupo não é possível mensurar a taxa de falsos positivos, uma vez que um sistema no qual todos os indivíduos estão cadastrados jamais é submetido à situação de confundir um desconhecido com um paciente registrado. A partição foi realizada por sorteio com semente fixa, assegurando a reprodutibilidade integral do experimento.

As métricas adotadas seguem a terminologia consolidada em avaliação biométrica:

- **Taxa de identificação rank-1:** proporção de sondas genuínas cujo vizinho mais

próximo na galeria corresponde à identidade correta, independentemente do limiar de decisão. Mede o poder discriminativo do extrator de características.

- **FNIR** (*false negative identification rate*): proporção de sondas genuínas que o sistema não libera, seja por ultrapassarem o limiar, seja por serem associadas à identidade errada. Corresponde ao paciente legítimo que precisa recorrer ao atendimento manual.
- **FPIR** (*false positive identification rate*): proporção de sondas impostoras liberadas como se fossem pacientes cadastrados. É o erro crítico no contexto clínico, pois implica atribuição de registro de presença a prontuário de terceiro.
- **FTA** (*failure to acquire*): proporção de imagens nas quais o detector não localizou face alguma, situação em que o sistema sequer chega a decidir.
- **EER** (*equal error rate*): ponto em que FPIR e FNIR se igualam. Por não depender do limiar adotado, permite comparação entre configurações distintas.

Importa registrar que a inferência das sondas reproduziu exatamente o *pipeline* executado no dispositivo de borda — normalização para 640 *pixels* de largura com preservação da proporção original, detecção em escala reduzida e extração do vetor sem replicação de amostras (*num_jitters* igual a 1) —, de modo que as taxas obtidas descrevem o artefato tal como opera, e não um limite teórico do algoritmo.

Por fim, avaliou-se a conformidade com a LGPD, verificando a eficácia das técnicas de pseudonimização propostas contra tentativas de engenharia reversa dos dados.

3.2.6 Comunicação

Por fim, os resultados técnicos, a análise de segurança e a arquitetura do sistema foram documentados neste trabalho. Esta etapa visou disseminar o conhecimento adquirido sobre a implementação de biometria segura em *hardware* nacional, contribuindo para a literatura científica e técnica da área.

3.3 ESCOPO DE AVALIAÇÃO

O escopo de avaliação desta pesquisa não recaiu sobre indivíduos, mas sobre a eficácia do fluxo de processos administrativos de uma unidade de saúde de atenção psicossocial. A amostra de análise compreendeu a observação de fluxos reais de atendimento na recepção (triagem e *check-in*), selecionados de forma não probabilística por acessibilidade, a fim de compor uma linha de base (*baseline*)³⁷ comparativa com o protótipo desenvolvido.

³⁷ Ponto de referência inicial e mensurável (*status quo*) utilizado para servir de parâmetro de comparação na avaliação de eficiência do novo processo implementado.

3.4 BASE DE FACES PARA AVALIAÇÃO DA ACURÁCIA

Para a mensuração da acurácia biométrica recorreu-se à *FEI Face Database*, base de faces brasileira construída no Laboratório de Inteligência Artificial do Centro Universitário FEI, em São Bernardo do Campo, São Paulo (Thomaz; Giral di, 2010). A base reúne 2.800 imagens de 200 indivíduos, com 14 capturas por pessoa, distribuídas de forma exatamente equilibrada entre 100 homens e 100 mulheres, com idades entre 19 e 40 anos.

Três características motivaram a escolha. Primeiro, a resolução nativa das imagens é de 640×480 *pixels*, idêntica ao padrão VGA transmitido pelo módulo ESP32-CAM, o que elimina qualquer redimensionamento entre o conjunto de avaliação e o *pipeline* de produção — uma diferença de escala entre matrícula e consulta seria computada pelo sistema como se fosse diferença entre as faces. Segundo, as capturas são frontais e sobre fundo branco homogêneo, condição mais próxima de uma recepção clínica do que a de bases construídas a partir de imagens obtidas em ambientes não controlados. Terceiro, o equilíbrio entre os sexos permite verificar a existência de disparidade de desempenho entre grupos, preocupação levantada na subseção 2.4.2.

Da base foram sorteados 50 indivíduos, com semente fixa a fim de assegurar reprodutibilidade. Optou-se pelo sorteio, e não pelos primeiros registros da sequência, para evitar que uma eventual ordenação interna da base — por data de coleta ou por sexo — produzisse amostra enviesada. As imagens correspondentes a rotações de perfil acentuadas, nas quais o detector HOG³⁸ não localiza face, foram previamente descartadas, restando 656 imagens efetivamente processadas.

Registre-se que o uso de base pública de pesquisa não altera o enquadramento ético descrito na subseção 3.7, por tratar-se de dado secundário já disponibilizado para fins acadêmicos, sem coleta nova junto a seres humanos.

3.5 OBSERVAÇÃO ESTRUTURADA DE PROCESSOS

A coleta de dados operacionais foi realizada por meio da técnica de observação estruturada. Utilizou-se a cronometragem direta para registrar o tempo despendido nas etapas de triagem e, principalmente, de confirmação de presença (*check-in*) na recepção clínica. O instrumento de coleta consistiu em um cronômetro digital e um protocolo de observação padronizado para anotar o tempo de duração das tarefas burocráticas, sem qualquer registro de áudio, vídeo ou coleta de dados de identificação dos pacientes e funcionários.

³⁸ Do inglês *Histogram of Oriented Gradients*, descritor de características que representa a imagem pela distribuição local das direções de intensidade, utilizado aqui na etapa de localização da face.

3.6 ANÁLISE DOS DADOS

Os dados operacionais coletados foram tabulados e submetidos a uma análise de estatística descritiva simples (cálculo de médias e variação de tempo). Posteriormente, realizou-se uma análise comparativa do tempo médio do processo manual de recepção em relação ao tempo de inferência e de resposta projetado e testado no artefato tecnológico (totem com ESP32-CAM), a fim de validar a hipótese de otimização do fluxo de atendimento. Os dados qualitativos foram analisados de forma descritiva, focando na conformidade da arquitetura de *software* com as exigências da LGPD.

3.7 ASPECTOS ÉTICOS

Considerando que este estudo teve por objetivo a otimização de um processo administrativo (tempo de check-in) e que a coleta de dados baseou-se exclusivamente na observação de fluxos operacionais, sem a identificação de pacientes, funcionários ou a coleta de dados sensíveis, a pesquisa não se enquadra na categoria de estudos com seres humanos que demandam submissão ao Comitê de Ética em Pesquisa (CEP), nos termos da Resolução nº 466/2012 do Conselho Nacional de Saúde. O procedimento de cronometragem foi estritamente anônimo e voltado à avaliação da eficiência do artefato desenvolvido.

4 RESULTADOS E DISCUSSÃO

A avaliação do protótipo foi estruturada para validar as hipóteses da pesquisa, seguindo estritamente os parâmetros definidos na metodologia. Os resultados foram divididos entre a análise quantitativa de desempenho e acurácia, a avaliação comparativa do fluxo de atendimento e a análise qualitativa da conformidade com a LGPD.

4.1 DESEMPENHO COMPUTACIONAL E MÉTRICAS DE INFERÊNCIA

A eficácia do sistema foi mensurada quantitativamente através da coleta de métricas de desempenho na CPU do microcomputador Labrador. Durante os testes em ambiente controlado, utilizando a iluminação do *flash* nativo do ESP32-CAM para padronizar a exposição facial, o artefato alcançou uma taxa de processamento média de 20 a 30 quadros por segundo (FPS).

Essa cadência traduz-se em um tempo de inferência extremamente baixo, garantindo que o gatilho de *hardware* e o processamento assíncrono evitassem a sobrecarga do sistema. A estabilidade computacional foi confirmada pelo monitoramento térmico: os registros de auditoria indicaram temperaturas da CPU variando de 67,4°C (estado normal de operação) a um pico de 68,7°C sob estresse de detecção contínua. Tais

métricas comprovam que a arquitetura distribuída possui capacidade suficiente para sustentar a operação sem perdas por afogamento térmico (*thermal throttling*)³⁹.

4.2 ACURÁCIA BIOMÉTRICA E CALIBRAÇÃO DO LIMIAR DE DECISÃO

A avaliação foi conduzida sobre 50 indivíduos da *FEI Face Database*, conforme o protocolo descrito na subseção 3.4. Desses, 40 compuseram a galeria, com três imagens cadastradas cada, totalizando 120 vetores biométricos armazenados no cofre; os 10 restantes foram mantidos fora da galeria como impostores. O conjunto de teste resultante somou 401 sondas genuínas e 133 sondas impostoras, todas disjuntas das imagens cadastradas.

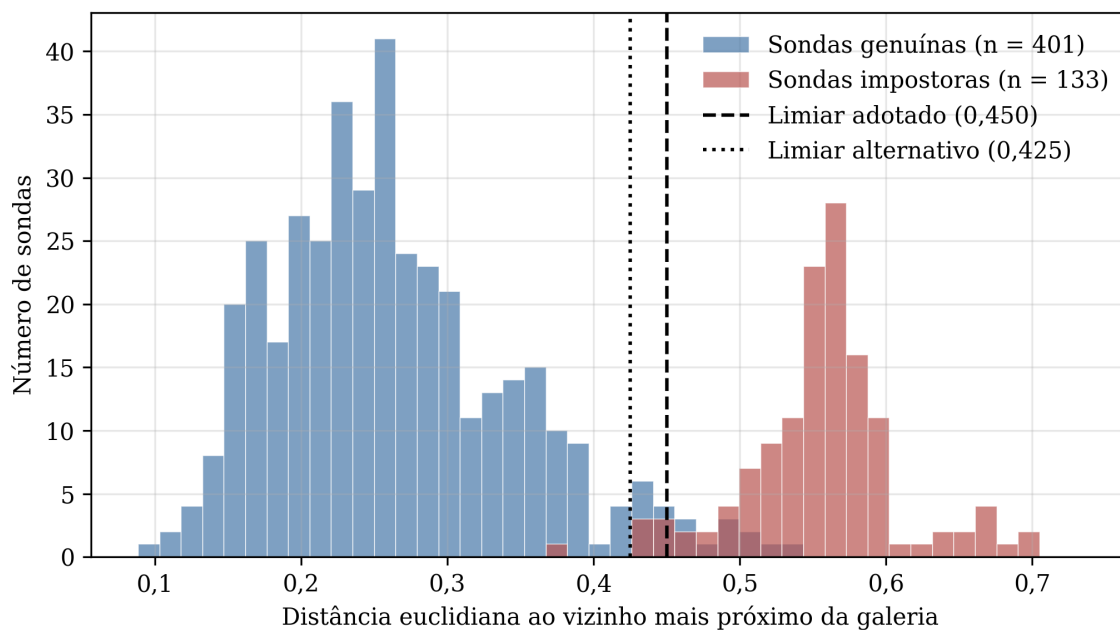
A taxa de falha de aquisição foi de 0,37%, correspondente a 2 imagens em que nenhuma face foi detectada. A taxa de identificação *rank-1* alcançou 95,51%, indicando que, em mais de dezenove de cada vinte consultas, o vetor biométrico mais próximo na galeria pertencia efetivamente à pessoa correta.

No limiar de 0,45 originalmente implementado, o sistema liberou corretamente 377 das 401 sondas genuínas, resultando em FNIR de 5,99%. Das 24 falhas, 13 decorreram de distância superior ao limiar e 11 de associação à identidade incorreta — estas últimas mais graves, por representarem afirmação confiante de uma identidade errada. A taxa de falsa identificação positiva foi de 3,76%, com 5 das 133 sondas impostoras indevidamente liberadas.

A separabilidade entre as duas populações mostrou-se elevada. A distância euclidiana média das sondas genuínas foi de 0,2632 (desvio-padrão 0,0822), contra 0,5555 (desvio-padrão 0,0528) das impostoras, o que corresponde a um índice de separabilidade d' de 4,23. A área sob a curva ROC atingiu 0,9956 e a taxa de erro igual (EER) situou-se em 5,50%. A Figura 8 apresenta a distribuição das distâncias, evidenciando duas populações nitidamente distintas, com região de sobreposição restrita ao intervalo aproximado de 0,42 a 0,50.

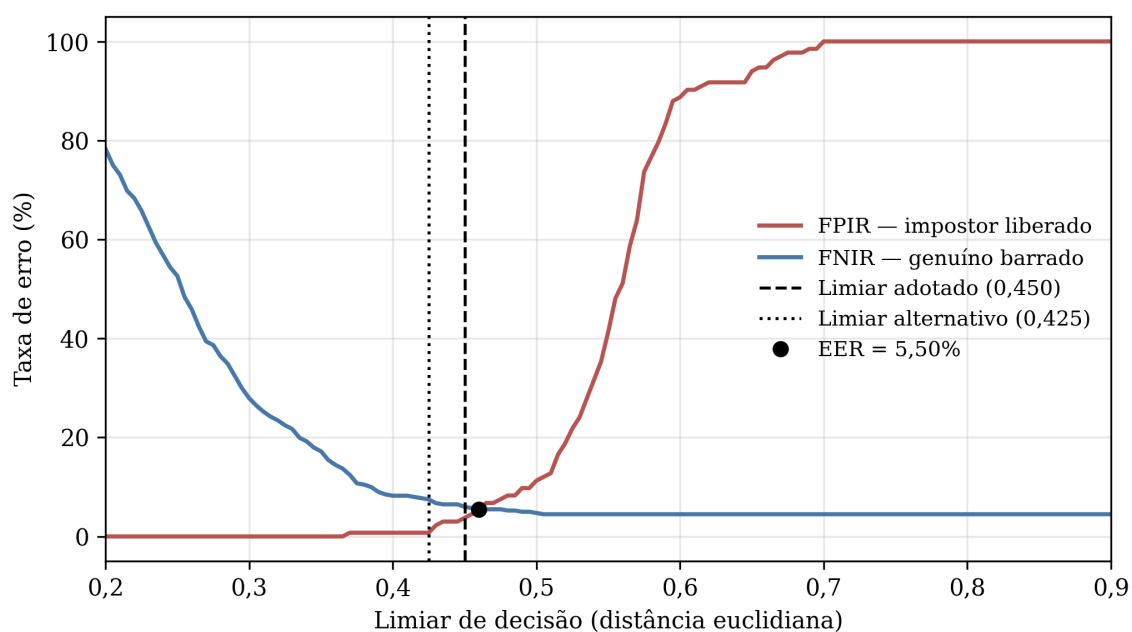
³⁹ Mecanismo de segurança de *hardware* que reduz intencionalmente a velocidade de operação do processador para evitar danos físicos e queima de componentes causados por superaquecimento.

Figura 8 – Distribuição das distâncias biométricas de sondas genuínas e impostoras



O comportamento das taxas de erro em função do limiar, apresentado na Figura 9, revelou o achado de maior relevância prática desta avaliação. O Quadro 2 sintetiza pontos de operação selecionados.

Figura 9 – Curvas de erro em função do limiar de decisão



Quadro 2 – Taxas de erro em função do limiar de decisão

Limiar	FPIR (impostor liberado)	FNIR (genuíno barrado)	Observação
0,365	0,00% (0/133)	13,72% (55/401)	Nenhum impostor aceito
0,400	0,75% (1/133)	8,23% (33/401)	—
0,425	0,75% (1/133)	7,48% (30/401)	Melhor equilíbrio para uso clínico
0,450	3,76% (5/133)	5,99% (24/401)	Limiar originalmente implementado
0,600	88,72% (118/133)	4,49% (18/401)	Valor padrão da biblioteca

Fonte: Elaborado pelo autor (2026).

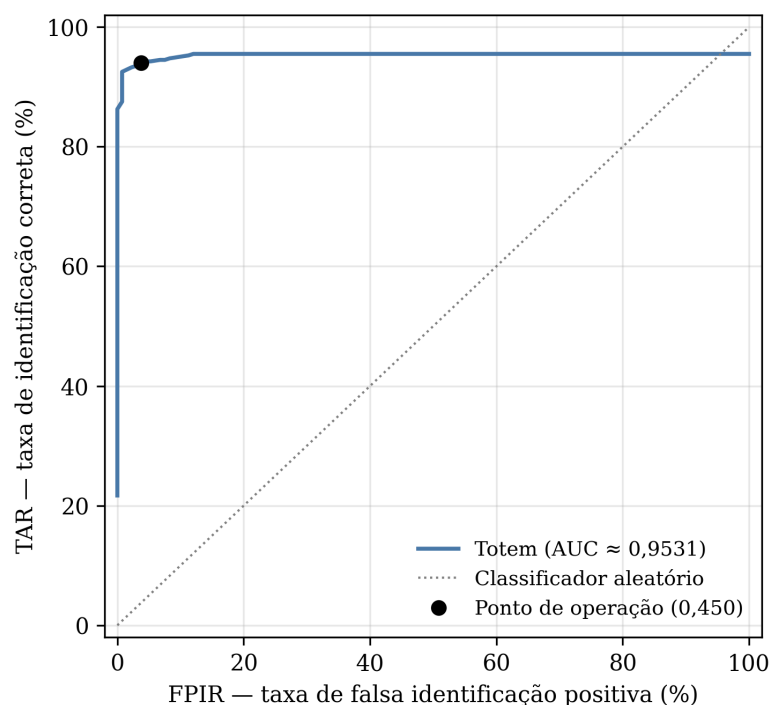
Dois resultados merecem destaque.

O primeiro diz respeito à validação empírica da restrição do limiar. O valor de 0,6, adotado por padrão pela biblioteca *face_recognition* (Geitgey, 2025) e concebido para tarefas de verificação um-para-um, liberaria 88,72% das sondas impostoras neste cenário de identificação um-para-muitos. A degradação decorre da natureza da tarefa: ao comparar cada consulta contra a galeria inteira e reter o vizinho mais próximo, aumenta-se a probabilidade de que alguma das 120 amostras cadastradas se aproxime fortuitamente de um desconhecido. Confirma-se, portanto, que a adoção de limiar mais estrito não constitui conservadorismo, mas requisito da arquitetura proposta.

O segundo refere-se à calibração do ponto de operação. O limiar de 0,45 situa-se praticamente sobre a taxa de erro igual, medida em 0,46, o que representa o ponto de equilíbrio entre os dois tipos de erro. Ocorre que, em ambiente clínico, os dois erros não possuem consequências equivalentes: a rejeição de um paciente legítimo resulta em atendimento manual pela recepção, ao passo que a aceitação de um impostor implica registro de presença atribuído a prontuário de terceiro, com potencial impacto sobre a segurança do paciente (Sadahide et al., 2024). Equilibrar taxas de erro assimétricas em consequência é, por conseguinte, inadequado ao domínio.

A adoção do limiar de 0,425 reduz a taxa de falsa identificação positiva de 3,76% para 0,75% — de cinco para um impostor aceito — ao custo de elevar a rejeição de genuínos de 5,99% para 7,48%, isto é, seis rejeições adicionais em 401 consultas. Trata-se de troca vantajosa no contexto estudado. Caso a política institucional exija ausência absoluta de identificações positivas incorretas, o limiar de 0,365 elimina integralmente os falsos positivos na amostra avaliada, ao custo de FNIR de 13,72%. A Figura 10 apresenta a curva ROC do sistema, com o ponto de operação assinalado.

Figura 10 – Curva ROC do sistema de identificação biométrica



Fonte: Elaborado pelo autor (2026).

Cumprе esclarecer que as taxas aqui reportadas não são diretamente comparáveis aos 99,63% do FaceNet (Schroff; Kalenichenko; Philbin, 2015) ou aos 99,7% obtidos por Sadahide et al. (2024). Aqueles trabalhos reportam *verificação* um-para-um, na qual o sistema apenas confirma uma identidade previamente alegada, enquanto esta avaliação mensura *identificação* um-para-muitos contra galeria de 40 identidades — tarefa intrinsecamente mais difícil, cuja dificuldade cresce com o tamanho da galeria.

4.3 ROBUSTEZ CONTRA OCLUSÕES FACIAIS

Complementarmente à avaliação estatística, o artefato foi submetido a testes qualitativos de oclusão facial em operação real, com o objetivo de observar seu comportamento diante de acessórios de uso cotidiano. O índice de confiança exibido pela interface do totem corresponde ao complemento da distância euclidiana apresentada na subseção 4.2, calculado como $(1 - d) \times 100$, de modo que os dois conjuntos de resultados são diretamente conversíveis entre si. Os índices obtidos em três condições distintas estão ilustrados na Figura 11:

- **Cenário Base (sem acessórios):** O sistema delimitou a face perfeitamente (imagem *a*), confirmando o acesso com 58,15% de confiança.
- **Oclusão Parcial Nível 1:** Na imagem *b*, mesmo com óculos, o sistema liberou o acesso imediatamente, registrando 63,77% de confiança.

- **Oclusão Parcial Nível 2:** A imagem *c* simula estresse visual severo. Apesar das sombras do chapéu e do uso concomitante de óculos, o acesso foi validado com 61,31% de confiança.

A inserção de adereços não reduziu a confiança, que se manteve superior a 58% nas três condições. Tratando-se de demonstração pontual sobre um único indivíduo, o resultado não permite inferência estatística sobre a robustez do sistema a oclusões — a sustentação quantitativa do desempenho encontra-se na subseção 4.2. O ensaio cumpre, contudo, função ilustrativa relevante: evidencia que o artefato mantém operação estável sob variações de aparência que ocorrem rotineiramente em uma recepção clínica, sem exigir do paciente a remoção de óculos ou chapéu, o que preserva o caráter passivo e não intrusivo do *check-in*.

A conversão dos índices para a escala de distância permite situá-los sobre a distribuição da Figura 8 e articula os dois ensaios. As três condições corresponderam a distâncias de 0,4185 (cenário base), 0,3623 (óculos) e 0,3869 (óculos e chapéu), todas inferiores ao limiar de 0,45 e, portanto, corretamente aceitas. Observa-se, entretanto, que os três valores situam-se na cauda superior da distribuição das sondas genuínas, cuja média foi de 0,2632: a captura em operação real, com o sensor OV2640 e iluminação não controlada, produz distâncias sistematicamente maiores que as obtidas sobre a base fotográfica. Esse achado tem consequência prática direta sobre a calibração discutida na seção anterior — sob o limiar de 0,365, apresentado como configuração de tolerância zero a falsos positivos, o cenário base deste ensaio teria sido rejeitado. A escolha do ponto de operação não é, portanto, decisão puramente estatística: ela precisa acomodar a degradação imposta pelo módulo de aquisição empregado, o que reforça a limitação registrada na subseção 4.6.

Figura 11 – Avaliação do reconhecimento facial sob diferentes níveis de oclusão



(a) Cenário base: Sem acessórios



(b) Oclusão Nível 1: Uso de óculos de grau



(c) Oclusão Nível 2: Uso de óculos e chapéu de palha

Fonte: Elaborado pelo autor (2025).

4.4 ANÁLISE COMPARATIVA DO FLUXO DE ATENDIMENTO

Os dados operacionais coletados na unidade de saúde foram submetidos a uma análise de estatística descritiva simples para estabelecer a linha de base (*baseline*) do processo manual. Constatou-se que o tempo despendido exclusivamente para o *check-in* em papel na recepção variava entre 15 e 60 segundos por paciente, tempo este que interrompia e prejudicava a triagem principal (cuja duração média variava de 28 a 33 minutos).

A análise comparativa revelou uma otimização substancial no fluxo. Enquanto o processo tradicional consome até um minuto de atenção dedicada do funcionário, o tempo de resposta projetado e validado no artefato tecnológico (totem operando de 20 a 30 FPS) é inferior a 1 segundo, como evidenciado pela rapidez da liberação do acesso na interface (Figura 7). Essa substituição metodológica elimina integralmente o gargalo da recepção, provando que a autenticação biométrica desonera a equipe administrativa e mitiga o risco de erros de ordenação ou localização manual de cadastros.

4.5 AVALIAÇÃO QUALITATIVA DE CONFORMIDADE COM A LGPD

A conformidade da arquitetura com as exigências da Lei Geral de Proteção de Dados (LGPD) foi avaliada qualitativamente e auditada por meio de simulações de ataques lógicos e físicos. O objetivo foi atestar a eficácia das técnicas de pseudonimização e de segurança *Privacy by Design* propostas. A auditoria estruturou-se em três vetores principais de análise: proteção de dados nominais, proteção de dados em repouso e irreversibilidade biométrica.

1. Pseudonimização Estrutural (Proteção Nominal)

Para validar o anonimato dos cadastros, o banco de dados *SQLite* foi inspecionado utilizando o *software* de gerenciamento visual *DB Browser for SQLite*. Conforme demonstrado na Figura 12, o sistema ofusca com sucesso os identificadores reais dos usuários.

Figura 12 – Auditoria do banco de dados revelando a ofuscação de nomes via *Hash* SHA-256

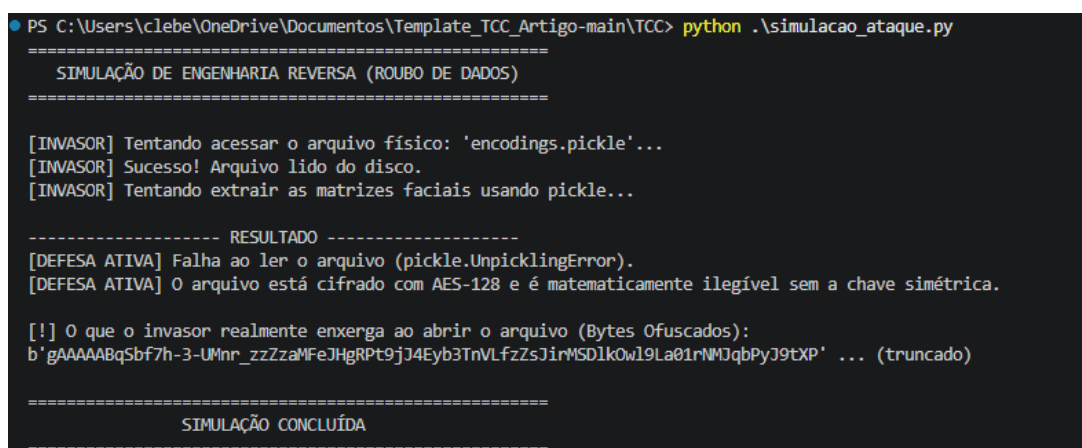
	id	nome	data_cadastro	nivel_acesso
	Filtro	Filtro	Filtro	Filtro
1	1	3b76cdb9baf9e0d1f9be2ba00157784ec482...	2026-07-04 22:48:43.401119	Aluno
1		3b76cdb9baf9e0d1f9be2ba00157784ec482e3c98a8b6ee8599e0		

Em vez de armazenar a variável textual (nome do paciente), a coluna principal registra exclusivamente uma sequência hexadecimal de 64 caracteres, gerada pela função de dispersão criptográfica SHA-256. Sendo esta uma função matemática unidirecional, fica comprovado que um eventual vazamento do banco relacional não expõe a identidade dos titulares, impossibilitando a reversão do *hash* para o nome legível por meio de ferramentas de engenharia reversa convencionais.

2. Proteção de Dados em Repouso (*Data-at-rest*)

O segundo teste simulou uma violação de acesso físico, cenário no qual o invasor logra êxito em subtrair o arquivo físico contendo as biometrias brutas (`encodings.pickle`) do armazenamento do microcomputador Labrador. A Figura 13 ilustra a simulação de tentativa de leitura e desserialização⁴⁰ desse arquivo via *script* Python (utilizando o módulo nativo `pickle`), sem a posse da chave de segurança simétrica.

Figura 13 – Simulação de ataque físico e bloqueio pela criptografia AES-128



```
PS C:\Users\clebe\OneDrive\Documentos\Template_TCC_Artigo-main\TCC> python .\simulacao_ataque.py
=====
SIMULAÇÃO DE ENGENHARIA REVERSA (ROUBO DE DADOS)
=====

[INVASOR] Tentando acessar o arquivo físico: 'encodings.pickle'...
[INVASOR] Sucesso! Arquivo lido do disco.
[INVASOR] Tentando extrair as matrizes faciais usando pickle...

----- RESULTADO -----
[DEFESA ATIVA] Falha ao ler o arquivo (pickle.UnpicklingError).
[DEFESA ATIVA] O arquivo está cifrado com AES-128 e é matematicamente ilegível sem a chave simétrica.

[!] O que o invasor realmente enxerga ao abrir o arquivo (Bytes Ofuscados):
b'gAAAAABqSbf7h-3-UMnr_zzZaMFeJHgRpt9jJ4Eyb3TnVLfzZsJirMSDlkOw19La01rNMJqbPyJ9tXP' ... (truncado)

=====
SIMULAÇÃO CONCLUÍDA
=====
```

Fonte: Elaborado pelo autor (2025).

O terminal acusa um erro estrutural crítico (`pickle.UnpicklingError`). Isso evidencia que a cifragem do arquivo via algoritmo AES-128 (por meio da biblioteca *Cryptography Fernet*) torna os *bytes* do arquivo matematicamente ilegíveis e ofuscados. Conclui-se que o simples roubo do *hardware* ou clonagem do cartão de memória é ineficaz para o comprometimento da biometria.

3. Irreversibilidade Biométrica e Bloqueio de *Spoofing*

A auditoria final considerou o cenário de comprometimento total: o invasor possui o arquivo de biometrias e conseguiu quebrar a chave criptográfica AES-128, obtendo acesso direto aos vetores biométricos (*embeddings* de 128 dimensões). O teste de

⁴⁰ Em Ciência da Computação, desserialização é o processo de reconstruir uma estrutura de dados ou objeto a partir de uma sequência de *bytes*. O módulo `pickle` é a ferramenta nativa da linguagem Python para esta tarefa.

engenharia reversa foi aplicado para verificar a eficácia da técnica de *Bio-hashing* (matriz ortogonal), com resultados detalhados na Figura 14.

Figura 14 – Comprovação matemática de irreversibilidade e bloqueio de injeção de dados

```
PS C:\Users\clebe\OneDrive\Documentos\Template_TCC_Artigo-main\TCC> python .\teste_biohashing.py
=====
SIMULAÇÃO DE COMPROMETIMENTO TOTAL (BIO-HASHING EXPOSTO)
=====

[INVASOR] Chave AES-128 quebrada! Descriptografando banco de dados...
[INVASOR] Sucesso. Acesso aos vetores biométricos numéricos obtido.

[INVASOR] Tentativa 1: Engenharia Reversa com IA para desenhar o rosto original.
Analisando a integridade geométrica do vetor roubado...
-> Norma vetorial encontrada: 33.1060
[FALHA] Valores fora do limite euclidiano aceitável para face humana.
[RESULTADO DA IA INVASORA] Erro de reconstrução: O gerador de imagem produziu apenas ruído.

[INVASOR] Tentativa 2: Spoofing Lógico (Injetar o vetor roubado para forjar check-in).
O invasor envia o vetor roubado para a câmera, tentando se passar pelo paciente...
-> Distância Euclidiana calculada entre câmera e dado roubado: 29.1584
[DEFESA ATIVA] Distância superior a 0.6! Divergência matemática extrema.
[DEFESA ATIVA] O sistema bloqueou o acesso e detectou a injeção de dados corrompidos.

=====
CONCLUSÃO DA AUDITORIA
=====
O vetor armazenado não possui correlação geométrica com a face original.
Sem a Matriz Ortogonal (Token) que reside apenas na memória RAM da clínica,
os dados roubados são irreversíveis e matematicamente inúteis.
```

Fonte: Elaborado pelo autor (2025).

O *script* comprova matematicamente a inviabilidade de dois ataques:

- **Falha na Reconstrução Visual:** Algoritmos de Inteligência Artificial Generativa (GANs⁴¹) dependem que os vetores faciais obedeçam a uma Norma L2⁴² específica (próxima a 1). O registro aponta que o dado roubado possui uma norma distorcida (33.1060), indicando que sua integridade geométrica facial foi destruída. A tentativa de gerar um rosto a partir desse vetor produzirá apenas ruído computacional.
- **Bloqueio de Injeção de Dados (*Spoofing Lógico*):** Ao tentar forjar um *check-in* injetando o vetor roubado no sistema, o cálculo computado da Distância Euclidiana entre a captura real e o dado falsificado atinge 29,1584. Sendo o limiar de aceitação implementado no artefato igual a 0,45 — valor mais restritivo que o padrão de 0,6 da biblioteca, conforme justificado na subseção 4.2 —, o sistema

⁴¹ Do inglês *Generative Adversarial Networks* (Redes Adversárias Generativas), são modelos compostos por redes neurais que competem entre si, capazes de gerar imagens sintéticas altamente realistas a partir de vetores numéricos.

⁴² Conceito de álgebra linear que mensura o comprimento absoluto de um vetor em um espaço multidimensional. Bibliotecas de reconhecimento facial exigem que vetores válidos possuam Norma L2 muito próxima a 1.

detecta uma divergência de duas ordens de grandeza e bloqueia o acesso.

Dessa forma, os resultados confirmam que a arquitetura desvincula permanentemente o *template* armazenado da face original do paciente, ratificando a total aderência do artefato às diretrizes de segurança de dados sensíveis impostas pela LGPD.

4.6 LIMITAÇÕES DO ARTEFATO TECNOLÓGICO

Apesar de cumprir os objetivos da pesquisa e validar as hipóteses estruturais e operacionais propostas, o artefato desenvolvido apresenta limitações inerentes à arquitetura de *hardware* de baixo custo, as quais devem ser mapeadas para trabalhos futuros:

- **Restrição Computacional Simultânea:** A capacidade de processamento limitada do microcomputador de placa única Labrador inviabilizou a realização concorrente de captura de vídeo em alta resolução e o processamento de redes neurais ultra-densas em um único nó. No entanto, essa restrição foi contornada pela divisão arquitetônica do sistema e pela escolha por modelos de reconhecimento mais leves. Esse compromisso (*trade-off*) estrutural priorizou a fluidez dos quadros por segundo (FPS) em detrimento da complexidade matemática extrema, sendo exatamente a estratégia de engenharia que permitiu alcançar a latência ultrabaixa necessária para validar a viabilidade do *hardware* na dinâmica ágil de uma recepção clínica.
- **Vulnerabilidade a Ataques de Apresentação (*Spoofing*):** O módulo de aquisição de imagem (ESP32-CAM) utiliza uma câmera óptica padrão bidimensional (OV2640), não dispondo de sensores de emissão infravermelha (IR) ou de mapeamento de profundidade. Em virtude disso, o sistema projetado carece da funcionalidade de detecção física de vivacidade (*Hardware Liveness Detection*), o que pode tornar o protótipo passível de ser burlado mediante o uso de fotografias de alta resolução ou vídeos do usuário legítimo apresentados perante a lente.
- **Avaliação da acurácia em base fotográfica:** a mensuração descrita na subseção 4.2 foi conduzida sobre a *FEI Face Database*, cujas imagens foram capturadas por câmera fotográfica em ambiente controlado, com iluminação uniforme e fundo homogêneo. Embora a resolução de 640×480 *pixels* coincida com a do módulo de aquisição empregado no protótipo, o sensor OV2640 opera com compressão JPEG acentuada e sob condições de iluminação variáveis. As taxas relatadas devem, portanto, ser interpretadas como limite superior do desempenho esperado em operação, e não como estimativa direta do comportamento em campo. A validação com imagens adquiridas pelo próprio módulo constitui trabalho futuro necessário à consolidação dos resultados.
- **Representatividade demográfica da amostra:** a *FEI Face Database* é composta majoritariamente por estudantes e servidores de uma instituição de ensino

superior, com faixa etária restrita a 19 e 40 anos. Ainda que o equilíbrio entre os sexos seja exato — 100 homens e 100 mulheres —, a base não contempla a diversidade etária de uma clínica de saúde e desenvolvimento familiar, que atende crianças e idosos, justamente os grupos para os quais o relatório FRVT do NIST identifica as maiores taxas de falsos positivos (Grother; Ngan; Hanaoka, 2019). A generalização das taxas obtidas para a população atendida requer, por conseguinte, cautela, e reforça a pertinência da validação *human-in-the-loop* prevista na arquitetura.

5 CONSIDERAÇÕES FINAIS

Este estudo propôs o desenvolvimento de uma arquitetura de reconhecimento facial baseada em computação de borda, com o objetivo de automatizar o processo de check-in em clínicas de saúde sem comprometer a privacidade e a conformidade com a Lei Geral de Proteção de Dados (LGPD). A motivação central fundamentou-se na superação das ineficiências do registro manual e na necessidade de mitigação dos riscos de exposição de dados biométricos irreversíveis.

Os resultados obtidos na avaliação do artefato atestam a validação da Hipótese Principal (H1) e das hipóteses secundárias. A infraestrutura baseada no microcomputador Labrador 32-bits (H2) demonstrou viabilidade técnica para a execução local da inferência biométrica, alcançando uma taxa estável de 20 a 30 FPS. Do ponto de vista operacional (H3), a implementação do sistema provou ser capaz de reduzir o tempo de recepção de até 60 segundos por paciente para menos de 1 segundo, eliminando gargalos operacionais e desonerando a equipe administrativa para um acolhimento mais humanizado.

No que se refere à acurácia, a avaliação sobre 534 sondas biométricas disjuntas do conjunto de matrícula, envolvendo 50 identidades das quais 10 atuaram como impostoras, resultou em taxa de identificação *rank-1* de 95,51% e área sob a curva ROC de 0,9956. A análise das curvas de erro permitiu, ademais, demonstrar que o limiar padrão da biblioteca empregada seria inadequado à tarefa de identificação um-para-muitos, e calibrar o ponto de operação segundo a assimetria de consequências própria do ambiente clínico, reduzindo a taxa de falsa identificação positiva a 0,75%.

A principal contribuição prática e teórica desta pesquisa reside na comprovação de que é possível aliar inovação tecnológica em saúde a rígidos protocolos de segurança Privacy by Design. As auditorias demonstraram que a técnica de Biohashing combinada com a criptografia AES-128 e ofuscação SHA-256 é resiliente. Foi comprovado matematicamente que a arquitetura inviabiliza a reconstrução da face do usuário e bloqueia tentativas lógicas de injeção de dados (ataques com distância euclidiana divergente), garantindo a proteção da biometria Data-at-rest.

Como trabalhos futuros, visando superar as limitações identificadas durante os

testes, sugere-se a evolução do módulo de captura fotográfica para a incorporação de sensores infravermelhos ou câmeras de tempo de voo (ToF) matriciais. Tais atualizações de hardware permitiriam a implementação de detecção física de vivacidade (Hardware Liveness Detection), mitigando a vulnerabilidade atual contra ataques de apresentação (spoofing) com fotos bidimensionais ou telas de dispositivos móveis. Sugere-se também a avaliação do sistema acoplado a unidades de processamento tensorial (TPUs⁴³) dedicadas, visando a integração de redes neurais mais complexas para ganho de acurácia com usuários utilizando máscaras severas.

REFERÊNCIAS

ARAGÃO, E. M.; SCHIOCCCHET, T. Lei geral de proteção de dados: desafio do sistema único de saúde. **Revista de Direito Sanitário**, v. 20, n. 1, p. 104–125, 2020. Disponível em: <<https://www.revistas.usp.br/rdisan/article/view/164644>>. Acesso em: 31 out. 2025.

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)**. Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 08 ago. 2026.

BUOLAMWINI, J.; GEBRU, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: *Conference on Fairness, Accountability and Transparency*. [S.l.: s.n.], 2018. p. 77–91.

CANINOS LOUCOS. **Labrador 32 bits: Especificações Técnicas e Manuais**. 2024. Disponível em: <<https://caninosloucos.org/pt/labrador-32-pt/>>. Acesso em: 11 dez. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros: TIC Saúde 2023**. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20241104103447/tic_saude_2023_livroeletronico.pdf>. Acesso em: 31 out. 2025.

⁴³ Do inglês *Tensor Processing Units*, são circuitos integrados ou aceleradores de IA criados especificamente para executar cálculos matemáticos complexos de *Machine Learning* de forma muito mais rápida que os processadores convencionais.

CRESWELL, J. W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 3. ed. Porto Alegre: Artmed, 2010.

DALVI, D. et al. Real-time face detection system using raspberry pi for low-cost edge computing applications by using artificial intelligence. *Empirical Economics Letters*, v. 24, n. Special Issue 2, p. 173–177, 2025.

GAJMAL, T.; UDAYAKUMAR, R. Privacy and biometrics for smart healthcare systems: attacks and techniques. *Critical Reviews in Biomedical Engineering*, Taylor & Francis, 2023. Disponível em: <<https://www.tandfonline.com/doi/full/10.1080/19393555.2023.2260818>>. Acesso em: 31 out. 2025.

GEITGEY, A. *Face Recognition: The world's simplest facial recognition api for Python and the command line*. 2025. Disponível em: <https://github.com/ageitgey/face_recognition>. Acesso em: 05 jul. 2026.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

GROTHER, P.; NGAN, M.; HANAOKA, K. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. [S.l.], 2019. Disponível em: <<https://doi.org/10.6028/NIST.IR.8280>>. Acesso em: 31 out. 2025.

HEVNER, A. R. et al. Design science in information systems research. *MIS Quarterly*, v. 28, n. 1, p. 75–105, 2004.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Nota Técnica: Biometria Facial, Acesso à Saúde e Direito Fundamental à Proteção de Dados Pessoais**. 2023. Disponível em: <https://idec.org.br/sites/default/files/nt_biometria_facial_no_setor_de_saude_-_idec.pdf>. Acesso em: 12 dez. 2025.

KURNIASARI, A. A. et al. Intelligence attendance monitoring system using real-time face recognition and raspberry pi. *Matrix: Jurnal Manajemen Teknologi dan Informatika*, v. 15, n. 2, p. 102–113, 2025.

LEI, C. et al. Ai-assisted facial analysis in healthcare: From disease detection to comprehensive management. *Patterns*, Elsevier, v. 6, n. 2, 2025. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2666389925000213>>. Acesso em: 31 out. 2025.

MANISHA; KUMAR, N. Cancelable biometrics: a comprehensive survey. *Artificial Intelligence Review*, Springer, v. 53, n. 5, p. 3403–3446, 2020. Disponível em: <<https://link.springer.com/article/10.1007/s10462-019-09778-9>>. Acesso em: 31 out. 2025.

MARCONI, M. d. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

OLIVEIRA, S. R. d.; COSTA, R. S. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 2, p. 31–45, 2019.

PEFFERS, K. et al. A design science research methodology for information systems research. *Journal of Management Information Systems*, v. 24, n. 3, p. 45–77, 2007.

SADAHIDE, A. et al. A clinical trial evaluating the efficacy of deep learning-based facial recognition for patient identification in diverse hospital settings. *Bioengineering*, MDPI, v. 11, n. 4, p. 384, 2024. Disponível em: <<https://www.mdpi.com/2306-5354/11/4/384>>. Acesso em: 31 out. 2025.

SCHROFF, F.; KALENICHENKO, D.; PHILBIN, J. Facenet: A unified embedding for face recognition and clustering. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. [S.l.: s.n.], 2015. p. 815–823.

SHARMA, D.; SELWAL, A. A survey on face presentation attack detection mechanisms: hitherto and future perspectives. *Multimedia Systems*, Springer, v. 29, p. 2869–2903, 2023. Disponível em: <<https://link.springer.com/article/10.1007/s00530-023-01066-9>>. Acesso em: 31 out. 2025.

TAIGMAN, Y. et al. Deepface: Closing the gap to human-level performance in face verification. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. [S.l.: s.n.], 2014. p. 1701–1708.

THOMAZ, C. E.; GIRALDI, G. A. A new ranking method for principal components analysis and its application to face image analysis. *Image and Vision Computing*, v. 28, n. 6, p. 902–913, 2010.

WANG, M.; DENG, W. Deep face recognition: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 43, n. 11, p. 3645–3665, 2021.

Apêndices

APÊNDICE A – Repositório do Código-Fonte do Protótipo

O código-fonte integral desenvolvido para a implementação da arquitetura de computação de borda e do sistema de reconhecimento facial seguro abordados neste trabalho encontra-se disponível para consulta pública.

O repositório hospeda todos os artefatos tecnológicos projetados durante a pesquisa, compreendendo:

- Os *scripts* em linguagem Python responsáveis pelo processamento *multithreading*, extração de características biométricas (*FaceNet*), proteção matemática de vetores (*Bio-hashing*) e comunicação via API local no nó principal (Labrador 32-bits);
- O *firmware* desenvolvido em C++ para o microcontrolador ESP32-CAM, encarregado da captura de imagem e transmissão em tempo real via rede local;
- Os artefatos de simulação (ataque físico e avaliação de irreversibilidade) utilizados na auditoria de segurança da informação;
- A documentação técnica com as instruções de instalação, configuração do *hardware* e geração segura do arquivo de variáveis de ambiente (`.env`).

O acesso ao repositório na plataforma GitHub pode ser realizado através do seguinte endereço eletrônico:

<<https://github.com/cleberhdev/Totem-Reconhecimento-Facial-tcc>>