SISTEMA DE CONTROLE DE ACESSO ACADÊMICO: Desenvolvimento e Implantação de Barreira de Segurança.

Daniel Felipe de Sousa Rodrigues[1],

Fernando Henrique Machado[2],

Leonardo Garcia Andrade[3]

Resumo

O presente artigo apresenta o desenvolvimento de um sistema de controle de acesso acadêmico, concebido como solução para reforçar a segurança em instituições de ensino, especialmente diante de riscos de acesso indevido por pessoas externas. O sistema foi projetado com funções específicas para o controle de entradas e saídas, atendendo às necessidades da instituição de forma direcionada. O cliente identificado foi uma escola que, até então, utilizava uma ferramenta voltada à gestão de eventos para monitorar a entrada de alunos, pais e membros da comunidade. Apesar de funcional, o software em uso mostrava-se inadequado, pois continha recursos excedentes, como relatórios financeiros e de receitas, que não possuíam relevância para a demanda. Diante dessa realidade, surge a pergunta da pesquisa: Como a implementação de um programa computacional voltado à segurança pode contribuir para a prevenção de massacres em instituições de ensino? Esse incômodo surgiu após os atentados ocorridos em 2023 nas escolas. Para tanto, o estudo tem como objetivo desenvolver um sistema simples, eficiente e focado exclusivamente na gestão de acessos. A metodologia adotada é a qualitativa que envolve levantamento de requisitos, modelagem, desenvolvimento com tecnologias atuais e a implementação de um protótipo funcional. Como resultado, compreende-se ganhos de praticidade, maior controle na gestão de usuários e redução da complexidade de uso, demonstrando que soluções personalizadas podem oferecer benefícios e segurança nos ambientes de ensino.

Palavras-chave: Controle de acesso. Segurança. Software acadêmico.

1 INTRODUÇÃO

Com o aumento da violência em ambientes escolares, torna-se necessário adotar soluções tecnológicas que garantam segurança, organização e praticidade no gerenciamento do acesso de pessoas. Segundo o relatório Ataques de violência extrema em escolas no Brasil – causas e caminhos, coordenado pela professora Telma Vinha, ocorreram 22 casos de violência extrema entre fevereiro de 2022 e outubro de 2023, representando 58,33% do total registrado em 22 anos. A professora destaca que vários fatores, inter-relacionados, explicam esse aumento acelerado de ataques, o primeiro é que esses adolescentes estão cada vez mais na superfície da internet, antes, os jovens precisavam navegar na *deep web* para ter acesso aos conteúdos prejudiciais, violentos e extremistas. Atualmente, esses conteúdos são facilmente encontrados em plataformas e redes sociais. A pandemia contribuiu para um fator agravante, pois o isolamento social intensificou o contato com os conteúdos prejudiciais e contribuiu para o adoecimento psíquico de muitos jovens. Além disso, observa-se uma ampliação do ecossistema de fomento à violência, caracterizado por um ambiente de ódio formado por lideranças, portais de comunicação e redes sociais com discursos conspiratórios e agressivos. Esses discursos são interpretados por alguns como apoio

velado a agressões e ataques contra inimigos, criando um clima de medo e insegurança nas escolas.

Nesse cenário, cresce a necessidade de sistemas que reforcem a segurança em ambientes educacionais, diversos prédios e organizações utilizam softwares voltados para segurança e controle de acesso, incluindo a escola cliente deste projeto, que empregava um sistema de gerenciamento de eventos para controlar a entrada e saída de pessoas. Apesar de atender parcialmente à demanda, o software mostrou-se inadequado, pois incluía funções complexas e desnecessárias, como relatórios financeiros, controle de vendas e gestão de recursos de eventos, que não se aplicavam ao contexto acadêmico. Essa inadequação resultava em desperdício de tempo, dificuldades no treinamento dos usuários e sobrecarga de informações irrelevantes.

A presente pesquisa tem como objetivo geral criar uma solução eficiente para o controle de entrada e saída de pessoas, que possa futuramente ser ampliada com recursos como catracas eletrônicas e biometria, sem perder sua essência de simplicidade. Diante disso, propôs-se o desenvolvimento de um sistema de controle de acesso exclusivo para ambientes de instituições de ensino, projetado para ser simples, objetivo e de fácil utilização.

2. REFERENCIAL TEÓRICO E TRABALHOS CORRELATOS

2.1 SISTEMAS DE CONTROLE DE ACESSO

Os controles de acesso regulam a admissão de usuários em áreas confiáveis da organização – acesso lógico aos sistemas de informação e acesso físico às instalações da organização. O controle de acesso é mantido por meio de um conjunto de políticas, processos para realizar essas políticas, e tecnologias que impõem as políticas (MACEDO, 2021, p. 24).

Foram realizadas pesquisas sobre controle de acesso, nas quais se constatou a existência de diversos artigos e softwares voltados tanto ao controle físico de ambientes quanto ao acesso lógico a sistemas de informação. Observa-se, portanto, a necessidade de mecanismos de controle de acesso para proteger recursos que não devem estar disponíveis a todos. Essa proteção se aplica tanto a espaços físicos que precisam ser resguardados contra a entrada de pessoas mal-intencionadas quanto a sistemas e infraestruturas críticas de organizações públicas e privadas.

No entanto, a segurança não pode ser focada em um único mecanismo. Ao analisar as diretrizes de prevenção do crime através do desenho urbano, é fundamental reconhecer que 'quatro pontos importantes são identificados como precursores dos estudos..., são eles: vigilância natural, controle natural dos acessos, territorialidade e manutenção dos espaços públicos' (CPTED-GUIA DE BOAS PRÁTICAS, 2013 *apud* GONÇALVES e LIRA, 2019, p. 100). Tais princípios demonstram que o sistema de controle de acesso atua como uma camada de segurança eficaz apenas quando complementado por ações que reforçam a vigilância e o senso de pertencimento ao espaço.

O controle informatizado de acesso ao CEJA (CIAC), testado e implantado em uma escola pública do programa EJA (Educação de Jovens e Adultos) no estado do Ceará. Essa instituição adota o modelo de “escola aberta”, no qual os discentes podem entrar e sair a qualquer momento, com o objetivo de proporcionar maior flexibilidade e acesso ao ambiente escolar. Entretanto, essa característica gera vulnerabilidades significativas, uma vez que não há controle sobre quem ingressa nas dependências da escola, qual a rotatividade de

pessoas, a média de fluxo por turno e quem, de fato, acessa os diferentes espaços escolares.

O projeto de Santiago, Bento e Costa (2019), denominado LetMeIn, propõe a utilização de Internet das Coisas (IoT) para o controle de acesso em ambientes educacionais, como salas de aula, bibliotecas e laboratórios. O sistema utiliza um Raspberry Pi como controlador principal para o destravamento das fechaduras, associado a um aplicativo móvel responsável por solicitar a abertura do ambiente.

O modelo faz uso de uma API RESTFUL para validação das credenciais do usuário, comunicação via *Application Server* e a integração de tecnologias como NAT e VPN, possibilitando uma conexão segura entre os dispositivos e a rede local, mesmo diante de restrições de endereçamento IP. Assim, o Raspberry Pi recebe a requisição validada e envia o sinal elétrico para a abertura da fechadura. Além disso, o dispositivo também realiza o envio periódico de mensagens ao servidor, garantindo monitoramento em tempo real do seu *status* e funcionamento.

A proposta do LetMeIn evidencia a tendência de utilizar dispositivos embarcados, comunicação em nuvem e práticas de mobilidade para aumentar a segurança e reduzir vulnerabilidades associadas a métodos tradicionais. Esse trabalho mostra que o uso de *smartphones* como credenciais digitais pode ser uma solução prática, uma vez que esses dispositivos já fazem parte do cotidiano da maioria dos usuários.

3. DESENVOLVIMENTO DO PROJETO (METODOLOGIA)

O desenvolvimento do sistema de controle de acesso acadêmico foi realizado em etapas estruturadas, combinando análise de necessidades, modelagem, documentação e implementação.

I) Definição do projeto e levantamento inicial: a equipe reuniu-se para definir o escopo do projeto, motivada pelos recentes casos de violência em escolas e pelo uso inadequado de um software de eventos em uma instituição conhecida. Visitas à escola cliente permitiram compreender as necessidades reais, resultando na definição dos objetivos do sistema.

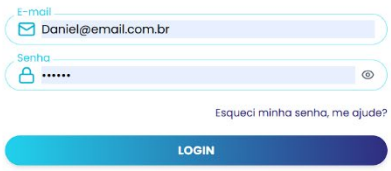
II) Planejamento e análise estratégica: foram elaborados o TAP (Termo de Abertura do Projeto), a análise SWOT, e o plano de ação, além do levantamento de requisitos funcionais e não funcionais e da modelagem de processos utilizando BPMN.

III) Modelagem e documentação do sistema: a equipe produziu diagrama UML, incluindo de Uso, Classes, Atividade, Estado e Sequência, e a Matriz de Rastreabilidade para vincular requisitos às funcionalidades. Também foi realizada documentação sobre portabilidade, quantidade de usuários e métricas de desempenho.

Com a documentação concluída, iniciou-se a implementação do protótipo funcional, utilizando: Python no *back-end* e Flask, React.js, e Next.js no *Front-end*. Como banco de dados foi utilizado PostgreSQL e para autenticação QR Codes únicos por usuário.

Figura 1 – Tela de Login

A tela de login demonstra que o sistema de controle de acesso adota uma abordagem moderna de segurança (login e senha). Essa interface garante que a entrada no sistema seja segura, intuitiva e funcional, configurando-se como o início do gerenciamento de



acesso da unidade.

Fonte: Elaborado pelos autores

Figura 2 – Tela de cadastro de estudantes

A tela de Cadastro de Estudantes do SamaPass é uma interface de gerenciamento de dados completa, projetada para a função CRUD (Create, Read, Update, Delete) de registros de usuários. Ela permite a inclusão de novos estudantes de forma estruturada e a consulta, edição e exclusão de registros existentes, centralizando as principais operações de gestão em uma única tela.

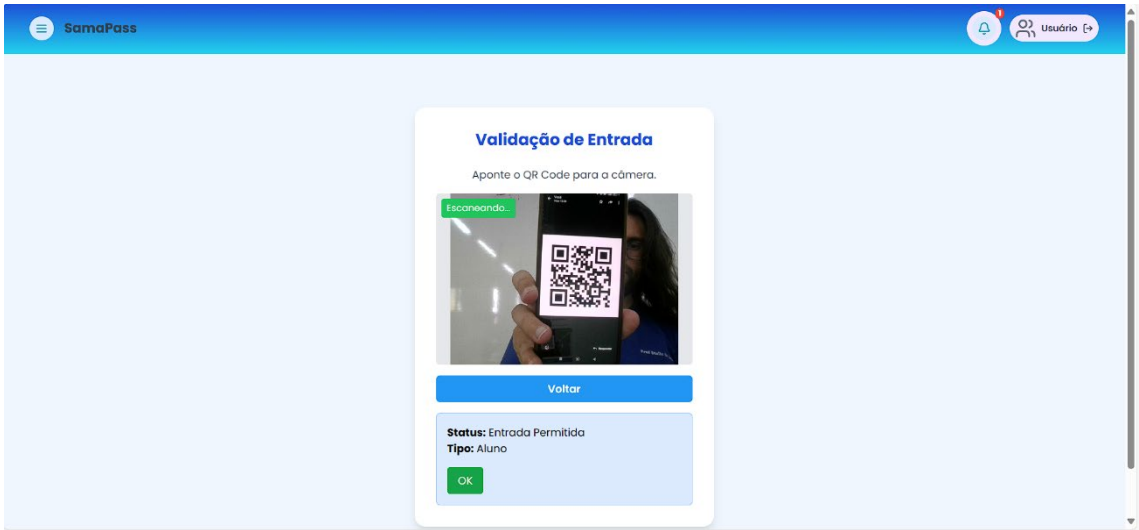
Fonte: Elaborado pelos autores

Figura 3 – Leitura do QR Code

A validação de entrada é a etapa de Autenticação e Autorização no sistema SamaPass. Ela demonstra um processo de controle de acesso eficiente, onde a leitura do QR Code (identificação) é imediatamente seguida pela validação do *status* e do tipo de usuário (autorização), culminando na permissão de entrada. Isso confirma a eficácia do sistema na utilização de tecnologias digitais para o gerenciamento de fluxo de pessoas.

Fonte: Elaborado pelos autores

O protótipo permite cadastro de usuários, geração de QR Codes e validação de acessos, funcionando com uma versão inicial do sistema, ainda sem refinamentos avançados de



segurança, usabilidade e escalabilidade. Ele serve como prova de conceito e base para futuras melhorias, como integração com catracas eletrônicas ou biométricas.

Com base no levantamento de requisitos e na modelagem, o *SamaPass* foi concebido com uma arquitetura de funcionamento clara, focada em segurança, controle de privilégios e fluidez de acesso. O sistema opera a partir da seguinte lógica:

Controle de Privilégios e Autenticação Inicial: A segurança do sistema é fundamentada em um controle de acesso lógico estrito. Inicialmente, um usuário com privilégios de Administrador (ADM) é criado para gerenciar e configurar todo o ambiente. Tanto o usuário ADM quanto os Usuários Operacionais (responsáveis pela leitura de QR Codes e pelo cadastro de novos indivíduos) acessam o sistema por meio de uma autenticação segura que exige *login* (utilizando e-mail ou CPF) e senha.

Gerenciamento de Fluxo e Funções CRUD: Após o login, a tela principal apresenta três *cards* direcionando para as funções de gerenciamento de usuários. O cadastro e o gerenciamento de Usuários Operacionais são exclusivos do ADM. O sistema suporta as operações CRUD (*Create, Read, Update, Delete*) para as seguintes categorias:

Aluno: Campos obrigatórios incluem Nome, Número da Matrícula, Data de Nascimento e CPF.

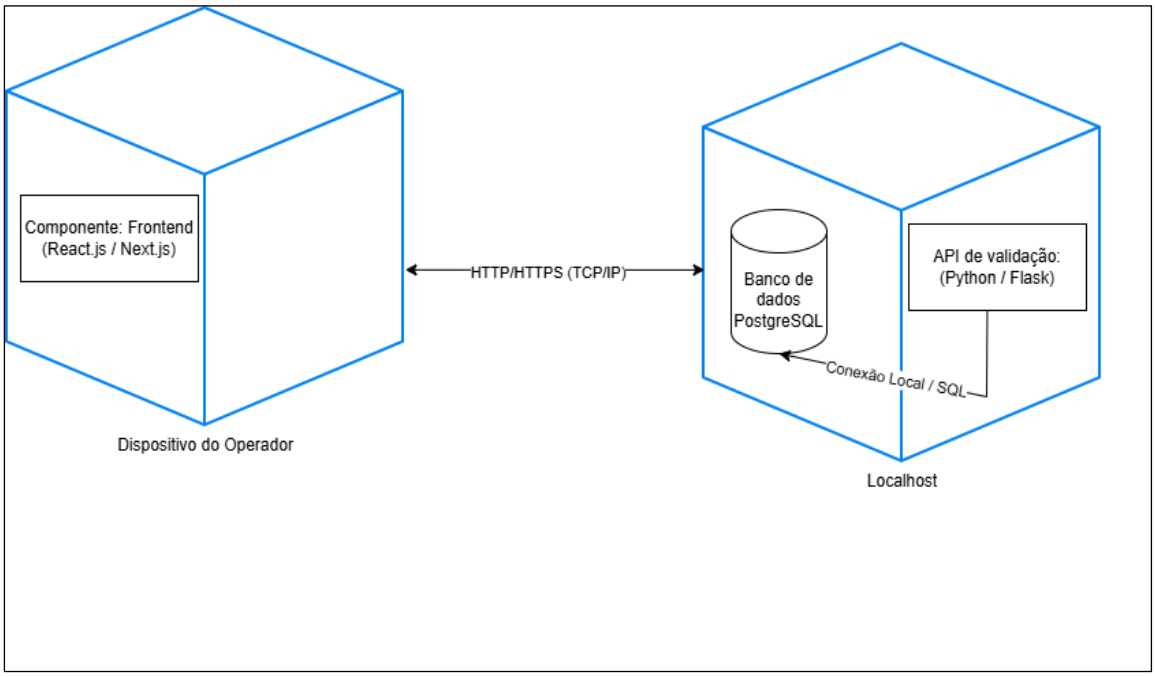
Visitante: Campos coletados incluem Nome, E-mail, Telefone, Data de Nascimento e CPF.

Usuário Operacional: Campos incluem Nome, Endereço, E-mail, Senha e Confirmação de Senha.

Processo de Autenticação por QR Code: O funcionamento central do sistema reside na geração e validação imediata do QR Code. Após o cadastro bem-sucedido de Aluno ou Visitante, um QR Code único é criado automaticamente. Este código pode ser baixado e enviado ao indivíduo para ser utilizado como credencial de acesso. A Validação de Entrada (demonstrada na Figura 3) ocorre quando o Usuário Operacional utiliza a câmera do dispositivo para ler o QR Code, acionando o processo de Autenticação e Autorização no *back-end*. O sistema verifica as credenciais do usuário e exibe instantaneamente o *Status* e o *Tipo* de acesso permitido.

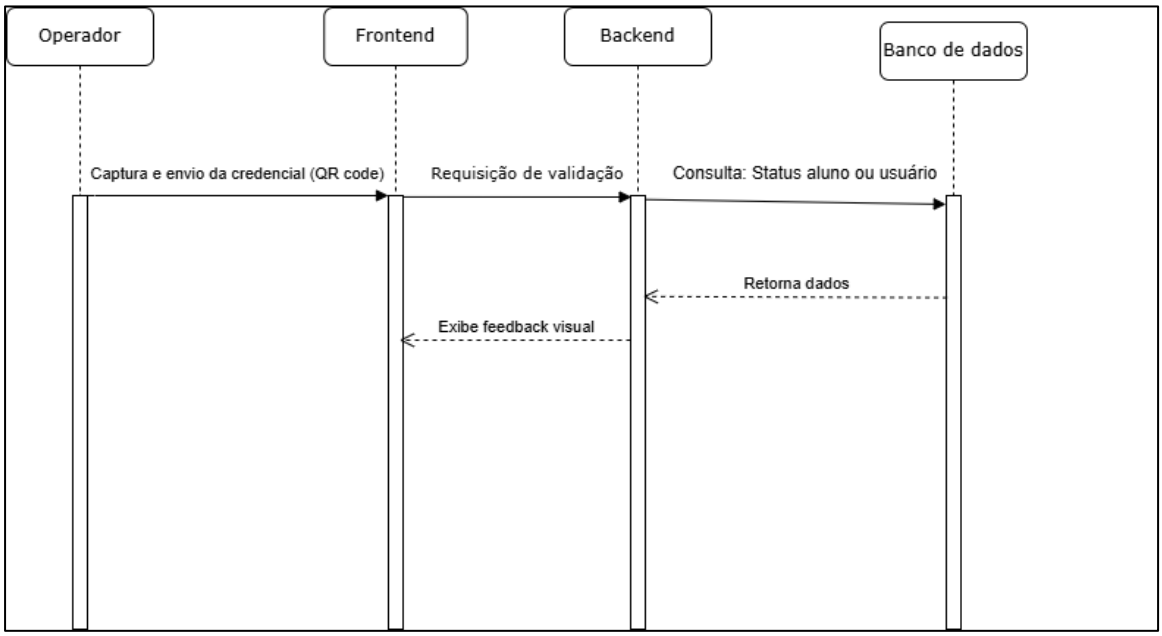
Essa estrutura garante que o *SamaPass* cumpra seu objetivo de gerenciar o fluxo de pessoas de forma objetiva, segura e com rastreabilidade, oferecendo uma base sólida para a implementação de novas funcionalidades.

Figura 4 - Diagrama de Implantação (Arquitetura) do Sistema SamaPass.



Fonte: Elaborado pelos autores

Figura 5 - Diagrama de Sequência do Processo de Validação de Acesso via QR Code



Fonte: Elaborado pelos autores

3.1 TECNOLOGIAS APLICADAS

O QR Code (Código de Resposta Rápida) é um código de barras bidimensional (2D) desenvolvido pela empresa japonesa Denso Wave para rastreamento de peças automotivas. Diferente dos códigos convencionais, apresenta maior capacidade de armazenamento, resistência a danos podendo ser lido mesmo que até 30% da imagem esteja comprometida e legibilidade em 360°, tornando-o eficiente para sistemas de controle de acesso (MATHURIA, 2017).

O Python é uma linguagem de programação versátil, de sintaxe simples e tipagem dinâmica, amplamente utilizada em desenvolvimento web, análise de dados e aplicações empresariais, possibilitando produtividade e rapidez (PYTHON, 2025).

O Flask é um framework WSGI leve para aplicações web, caracterizado por sua flexibilidade e expansibilidade. Ele é adequado tanto para sistemas simples quanto para aplicações mais complexas, oferecendo suporte a extensões para autenticação, banco de dados e manipulação de formulários (FLASK, 2025).

O PostgreSQL é um sistema de banco de dados relacional robusto e confiável, capaz de armazenar e gerenciar dados complexos com integridade, segurança e alto desempenho (POSTGRESQL, 2025).

O React é uma biblioteca JavaScript destinada à construção de interfaces de usuário baseadas em componentes reutilizáveis, permitindo o desenvolvimento de aplicações web dinâmicas, interativas e fáceis de manter (REACT, 2025).

4. RESULTADOS E DISCUSSÕES

Com o levantamento de requisitos visando entender a necessidade do cliente, e facilitar a experiência operacional com o software, o sistema para controle de fluxo de pessoas em instituições acadêmicas teve resultados positivos em relação ao software terceirizado para eventos que a escola utilizava.

O sistema para controle de fluxo nomeado como SamaPass, apresenta pontos importantes que resolvem as necessidades do cliente de implementar segurança maior no ambiente escolar. Observa-se que o sistema apresenta uma interface clara e objetiva, composta por *cards* bem estruturados que reúnem informações essenciais, como endereço do visitante ou vínculo com o aluno. À medida que um novo cadastro é realizado, os dados são exibidos imediatamente em um *card* ao lado do formulário, possibilitando ao usuário um controle em tempo real sobre as informações processadas. O menu de navegação utiliza ícones representativos e de fácil identificação, facilitando a compreensão das funcionalidades de cada página. Na seção destinada ao QR Code, disponibiliza a opção de validação, leitura por câmera de forma clara e direta facilitando a leitura do usuário. Após a verificação, mensagens de sucesso ou erro são exibidas na própria interface, assegurando uma experiência intuitiva e de fácil uso.

Constata-se que o sistema apresenta alto desempenho na leitura de QR Codes, contribuindo para a fluidez nos acessos e evitando congestionamentos nas entradas e saídas escolares. A estrutura de banco de dados foi implementada de forma simples e otimizada, o que favorece a rápida validação das informações, mesmo em situações de conexão instável. Ademais, a baixa dependência do navegador permite o uso em dispositivos de diferentes níveis de qualidade. O uso do QR Code, por sua leveza e agilidade, torna-se uma solução eficaz para controle de fluxo em horários de pico, garantindo atualização imediata e identificação precisa das pessoas que acessam o ambiente escolar.

O software apresenta uma grande flexibilidade nas opções de validação dos usuários, além do QR Code, pode ser integrado a catracas e leitores biométricos, melhorando o controle de congestionamento e da segurança. Isso possibilita à instituição de ensino diversificar espaços para entrada e saída de pessoas. O sistema é altamente flexível para implementação de novas funcionalidades como geração de relatórios, e chamadas on-line, já que o software apresenta uma listagem com os dados de todas as pessoas cadastradas no sistema.

Por ser adaptado para o uso de QR Code, não é necessário o uso de periféricos de alto custo e estrutura de cabeamento. O uso do celular da própria instituição é o suficiente para o bom funcionamento do software. Isso diminui o uso de recursos adicionais nos servidores da aplicação, contribuindo para mensalidades mais baratas desses serviços de hospedagem.

Em contrapartida, algumas limitações ainda precisam ser superadas, pois verifica-se a ausência de módulos avançados de segurança, tais como mecanismos de leitura detalhada e sofisticada de QR Codes, capazes de identificar possíveis tentativas de fraude por parte de visitantes. Além disso, não há garantias robustas de proteção quanto ao acesso privado aos códigos gerados individualmente para cada pessoa, o que pode expor a instituição a riscos de clonagem ou compartilhamento indevido de dados sensíveis. A inexistência desses recursos compromete a confiabilidade do processo de autenticação e fragiliza a segurança geral do sistema.

Outro ponto crítico identificado é a dependência do uso de câmera para a leitura dos QR Codes. Tal limitação acarreta riscos em instituições que não dispõem de dispositivos com câmeras de qualidade adequada, além de demandar infraestrutura operacional externa para o correto funcionamento. Torna-se, portanto, imprescindível a disponibilização de um método alternativo de validação, como uma caixa de texto para inserção manual do código, garantindo assim a continuidade do processo mesmo em cenários de indisponibilidade ou falhas técnicas nos equipamentos utilizados.

Apesar dessas limitações, a solução se mostra promissora para escolas que buscam alternativas simples e eficazes de controle de acesso.

5. CONSIDERAÇÕES FINAIS

Este projeto teve o compromisso de realizar uma análise do cenário alarmante de violência crescente em instituições de ensino brasileiras, evidenciadas pelos ataques ocorridos entre 2022 e 2023. O estudo demonstrou a relevância do desenvolvimento de soluções tecnológicas voltadas à segurança e à gestão eficiente do acesso de pessoas nesses ambientes. O sistema proposto denominado *SamaPass* foi proposto como resposta direta à necessidade de mecanismos práticos, acessíveis e direcionados ao contexto educacional, em contraposição a softwares genéricos e complexos, originalmente destinados à gestão de eventos, mas que acabavam sendo utilizados de forma inadequada em escolas.

A partir da análise realizada, que envolveu o levantamento de requisitos, a modelagem e o desenvolvimento de um protótipo funcional com base em tecnologias atuais como Python, Flask, React e PostgreSQL, constatou-se que é possível criar um sistema simples e ao mesmo tempo eficiente, capaz de otimizar o controle de entrada e saída. A integração do QR Code como método de autenticação demonstrou-se eficaz, proporcionando rapidez na leitura, redução de filas e melhor organização do fluxo de pessoas, além de representar uma alternativa de baixo custo para as instituições de ensino.

Os resultados alcançados evidenciam ganhos significativos de praticidade, transparência e controle operacional, assegurando ao gestor escolar uma visão em tempo real das movimentações no ambiente institucional. A interface intuitiva, aliada à estrutura leve do sistema, contribui para a facilidade de uso e reduz a necessidade de treinamento intensivo dos colaboradores, o que representa avanço em termos de eficiência administrativa. Além disso, O SamaPass apresenta um potencial para expansões futuras em termos de escalabilidade e integração física. Pode-se desenvolver funcionalidades para a integração de catracas eletrônicas e leitores biométricos, o que automatizará o controle de acesso e elevará a capacidade de resposta em ambientes de alto fluxo, tornando-o uma ferramenta mais robusta e adaptável às demandas de diferentes instituições.

Entretanto, é preciso reconhecer que o sistema ainda apresenta limitações técnicas e estruturais que requerem aprimoramento. A ausência de mecanismos robustos de segurança avançada, como a criptografia reforçada dos códigos gerados e a detecção de tentativas de clonagem, ainda representa um ponto vulnerável, especialmente diante de ameaças cibernéticas e riscos de manipulação indevida de dados. Para minimizar esse risco, o próximo passo essencial é implementar criptografia reforçada na geração e transmissão do QR code, visando prevenir tentativas de fraude e clonagem. Outro desafio refere-se à dependência exclusiva da leitura por câmera, que pode restringir o uso em escolas com equipamentos de baixa qualidade ou infraestrutura limitada. Assim, a continuidade operacional será garantida com a inclusão de métodos alternativos de

validação, como a inserção manual de dados de documentos de identificação (como o CPF) ou o próprio código de acesso, em versões futuras do software.

Sob o ponto de vista social e preventivo, o projeto reafirma a importância da tecnologia como instrumento de proteção e promoção da segurança escolar, podendo atuar como barreira inicial para inibir o ingresso de pessoas não autorizadas e, consequentemente, contribuir para a redução de riscos de incidentes violentos. Embora o controle de acesso por si só não elimine as causas profundas da violência escolar, sua integração a políticas institucionais de convivência, e monitoramento preventivo de comportamentos pode representar um avanço concreto na construção de ambientes educacionais mais seguros e acolhedores.

Assim, conclui-se, que o *SamaPass* demonstra viabilidade técnica e relevância social ao oferecer uma alternativa tecnológica viável e acessível às escolas, especialmente diante da urgência de reforçar as medidas de segurança sem comprometer a autonomia e a rotina pedagógica das instituições. Sua implementação não apenas reforça a proteção física dos alunos e funcionários, mas também simboliza um passo importante na modernização das práticas de gestão escolar, aproximando a tecnologia da função social da educação: garantir o desenvolvimento humano em um espaço de paz, respeito e segurança.

REFERÊNCIAS

D3E. *Ataques em escolas no Brasil: relatório*. nov. 2023. Disponível em: https://d3e.com.br/wp-content/uploads/relatorio_2311_ataques-escolas-brasil.pdf. Acesso em: 2 out. 2025.

JORNAL DA UNICAMP. *Escolas registram explosão de casos de violência extrema em 2022 e 2023*. 11 dez. 2023. Disponível em: https://jornal.unicamp.br/noticias/2023/12/11/escolas-registram-explosao-de-casos-de-violencia-extrema-em-2022-e-2023. Acesso em: 2 out. 2025.

MACEDO, Marcus. *Introdução à Segurança da Informação Corporativa*. Recife: Centro de Formação dos Servidores e Empregados Públicos do Poder Executivo Estadual – CEFOSPE, 2021. 1. ed. Disponível em: https://www.egape.pe.gov.br/images/media/1665420043_Apostila%20Introducao%20Segurança%20Informacao%20Corporativa.pdf. Acesso em: 2 out. 2025.

MATHURIA, *Manish. A Review on QR Code*. 2017. Disponível em: https://www.researchgate.net/profile/Manish-Mathuria/publication/316177848_A_Review_on_QR_Code/links/5d4832e592851cd046a2d5df/A-Review-on-QR-Code.pdf. Acesso em: 2 out. 2025.

NEXT.JS. *Next.js Documentation*. 2025. Disponível em: https://nextjs.org/. Acesso em: 2 out. 2025.

POSTGRESQL. *About PostgreSQL*. 2025. Disponível em: https://www.postgresql.org/about. Acesso em: 2 out. 2025.

PYTHON. *Tutorial Python*. 2025. Disponível em: https://docs.python.org/pt-br/dev/tutorial/index.html#tutorial-index. Acesso em: 2 out. 2025.

FLASK. Flask Documentation. 2025. Disponível em: https://flask-palletsprojects-com.translate.goog/en/stable/. Acesso em: 2 out. 2025.

REACT. *React Documentation*. 2025. Disponível em: https://react.dev. Acesso em: 2 out. 2025.

REVISTA DOCENTES. *A revista Docentes*. Ceará: Secretaria da Educação, 2023. Disponível em: https://periodicos.seduc.ce.gov.br/revistadocentes/article/view/178/104. Acesso em: 2 out. 2025.

SANTIAGO, Eike D.; BENTO, Diogo F.; COSTA, Breno J. D. *LetMeIn: sistema de controle de acesso baseado em IoT para ambientes educacionais*. ERBase, 2023. Disponível em: https://sol.sbc.org.br/index.php/erbase/article/view/8999. Acesso em: 2 out. 2025.

GONÇALVES, Mariana Cezar; LIRA, Pablo**.** Arquitetura do medo sob a perspectiva da prevenção do crime através do desenho ambiental (CPTED). Geografia em Questão, Cascavel, PR, v. 12, n. 02, p. 96-109, 2019. ISSN 2178-0234. Disponível em: https://saber.unioeste.br/index.php/geoemquestao/article/view/18765/14677. Acesso em: 28 out. 2025.