UNIVERSIDADE DE SOROCABA
PRÓ-REITORIA DE (GRADUAÇÃO E ASSUNTOS ESTUDANTIS)

LUCAS MASSARANI BOTEGA
MATHEUS SOUSA DA SILVA
SAMUEL MOISES DE SOUZA

CERTIFICAÇÃO DIGITAL EM EVENTOS: PROPOSTA DE PLATAFORMA COM VALIDAÇÃO DE PRESENÇA VIA QR CODE E GEOLOCALIZAÇÃO

Sorocaba/SP
2025

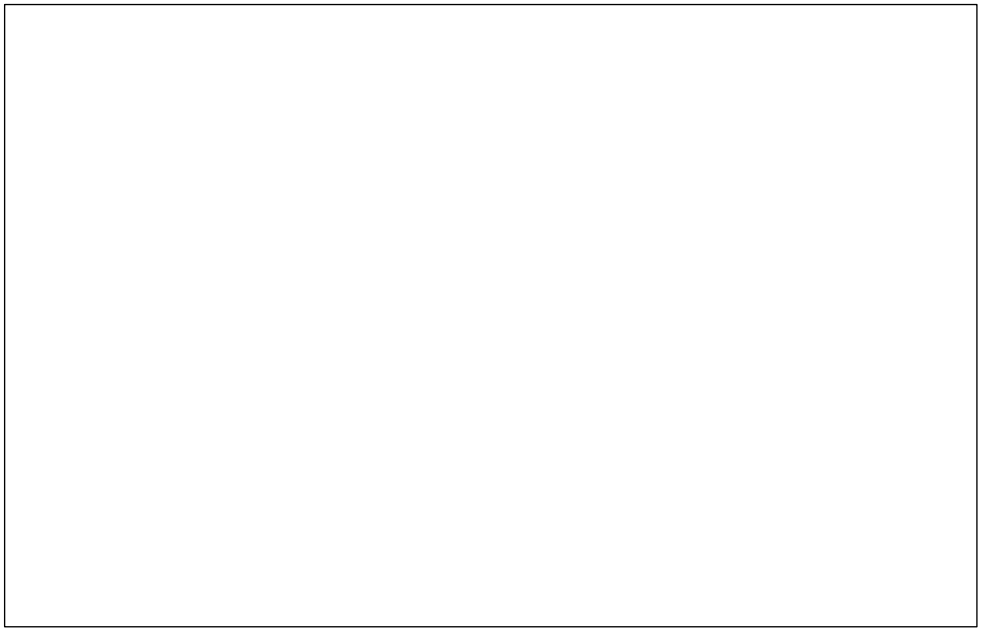
LUCAS MASSARANI BOTEGA
MATHEUS SOUSA DA SILVA
SAMUEL MOISES DE SOUZA

CERTIFICAÇÃO DIGITAL EM EVENTOS: PROPOSTA DE PLATAFORMA COM VALIDAÇÃO DE PRESENÇA VIA QR CODE E GEOLOCALIZAÇÃO

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do Diploma de Graduação em Engenharia da Computação, da Universidade de Sorocaba.

Orientador: Professor Me. Denicezar Angelo Baldo

Sorocaba/SP
2025



LUCAS MASSARANI BOTEGA
MATHEUS SOUSA DA SILVA
SAMUEL MOISES DE SOUZA

CERTIFICAÇÃO DIGITAL EM EVENTOS: PROPOSTA DE PLATAFORMA COM VALIDAÇÃO DE PRESENÇA VIA QR CODE E GEOLOCALIZAÇÃO

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do Diploma de Graduação em Engenharia da Computação, da Universidade de Sorocaba.

Aprovado em: ___/____/_____

BANCA EXAMINADORA:

Prof. Me. Denicezar Angelo Baldo
Universidade de Sorocaba

Prof. Me. Raphael Hungaro Moretti
Universidade de Sorocaba

Dedico este trabalho à minha família, pelo apoio incondicional e incentivo constante ao longo de toda a minha trajetória acadêmica. Agradeço também aos meus amigos e colegas de curso, que estiveram presentes nas dificuldades e conquistas desta jornada.

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador, Professor Mestre Denicezar Angelo Baldo, pela orientação, paciência e por todo o suporte acadêmico durante a execução deste trabalho.

Agradecemos também aos professores da Universidade de Sorocaba, que contribuíram para a nossa formação acadêmica e nos motivaram a seguir com empenho nas pesquisas e práticas.

Aos nossos colegas de curso, que compartilharam suas experiências e desafios, oferecendo sempre apoio e colaboração durante essa jornada. A interação com vocês foi fundamental para o nosso aprendizado.

Por fim, agradecemos à Universidade de Sorocaba pela infraestrutura e pelos recursos que proporcionaram, permitindo a execução deste trabalho com qualidade.

“A tecnologia não é nada. O importante é que você tenha fé nas pessoas, que elas são basicamente boas e inteligentes, e se você lhes der as ferramentas, elas farão coisas maravilhosas com elas.” – Steve Jobs

RESUMO

A transformação digital tem impulsionado a modernização de diversos setores, incluindo a organização de eventos e a emissão de certificados. Contudo, a autenticidade desses documentos, bem como a verificação da presença efetiva dos participantes, ainda representa desafios importantes no cenário atual. Este trabalho apresenta o desenvolvimento da plataforma Certified, uma solução digital voltada à emissão segura de certificados de participação em eventos acadêmicos, corporativos ou institucionais. A proposta parte da necessidade de garantir confiabilidade e transparência ao processo de certificação, mitigando riscos de fraudes por meio da utilização de tecnologias como QR Code, geolocalização e validação eletrônica. A plataforma foi construída com foco em responsividade, usabilidade e acessibilidade, respeitando diretrizes estabelecidas pela Lei Brasileira de Inclusão (LBI) e pela Lei Geral de Proteção de Dados (LGPD). Utilizando a ferramenta Lovable.dev, o sistema foi estruturado com tecnologias modernas como React e Vite, além de ser integrado ao Supabase, uma solução de backend que fornece autenticação, banco de dados e armazenamento em nuvem. Entre as funcionalidades ativas estão o cadastro e login de usuários (participantes e organizadores), a criação e inscrição em eventos, o envio automático de e-mails, a emissão e visualização de certificados digitais em PDF e a validação por QR Code. A interface foi projetada com base em princípios de design centrado no usuário, garantindo uma experiência fluida e intuitiva, mesmo em dispositivos móveis. Os resultados obtidos até o momento demonstram que a Certified é uma solução funcional, escalável e alinhada às exigências atuais de segurança, confiabilidade e acessibilidade. O projeto serve como uma prova de conceito robusta e plenamente aplicável a contextos reais.

Palavras-chave: Certificação digital. Verificação de presença. QR Code. Supabase. LGPD.

ABSTRACT

Digital transformation has driven the modernization of various sectors, including event management and the issuance of participation certificates. However, ensuring the authenticity of these documents and verifying participants' actual presence still pose significant challenges. This work presents the development of Certified, a digital solution aimed at securely issuing participation certificates for academic, corporate, or institutional events. The proposal addresses the need to provide reliability and transparency to the certification process by incorporating technologies such as QR Code, geolocation, and electronic validation.
The platform was built with a focus on responsiveness, usability, and accessibility, in compliance with the Brazilian Inclusion Law (LBI) and the General Data Protection Law (LGPD). Developed using the Lovable.dev tool, the system is based on modern technologies such as React and Vite, and it is integrated with Supabase, a backend-as-a-service solution that offers authentication, database, and cloud storage. The active features include user registration and login (for participants and organizers), event creation and registration, automated email dispatch, PDF certificate generation and visualization, and QR Code validation.The interface design follows user-centered principles to ensure a smooth and intuitive experience, even on mobile devices. The results obtained thus far demonstrate that Certified is a functional, scalable solution that meets current demands for security, trustworthiness, and digital accessibility. This project serves as a robust proof of concept, with practical applications in real-world contexts.

Keywords: Digital certification. Attendance validation. Supabase. QR Code. LGPD. Digital accessibility.

LISTA DE ILUSTRAÇÕES

Figura 1 - Certificação Digital: Segurança na Comunicação 16
Figura 2 - Mulher falsifica diploma para conseguir emprego em escola infantil no AP 18
Figura 3. Certificação Digital no SIGSIF 20
Figura 4. Blockchain 21
Figura 5. Selo de Ação Ética 23
Figura 6. RG Digital 24
Figura 7 - Exemplo de Certificado antigo 25
Figura 8 - ICP-Brasil 26
Figura 9 - Exemplo de verificação para validação de um certificado 27
Figura 10 - Os três tipos de assinatura eletrônica 28
Figura 11 - Assinatura eletrônica na DocuSign 29
Figura 12 - Exemplo de token para confirmação de assinatura eletrônica 30
Figura 13 - Exemplo de assinatura eletrônica na Certisign 32
Figura 14 - Exemplo de envio de certificados via e-mail na Even3 33
Figura 15 - Modelo da ISO 9241-210 34
Figura 16 - Lei Brasileira de Inclusão (LBI) 35
Figura 17 - Lovable.dev: Como Funciona 38
Figura 18. Página Inicial 39
Figura 19. Página Sobre 40
Figura 20. Página Como Funciona 41
Figura 21. Página Contato 42
Figura 22. Página Eventos (sem login) 43
Figura 23 - Tela de Login 45
Figura 24 - Tela de Cadastro 46
Figura 25 - Dashboard do Participante 47
Figura 26 - Meus Eventos (Participante) 48
Figura 27 - Meus Certificados 49
Figura 28 - Visualização do Certificado 49
Figura 29 - Nenhum Certificado Disponível 50
Figura 30 - Analytics 51
Figura 31 - Gerenciar Eventos 52
Figura 32 - Detalhes do Evento (Presenças) 53
Figura 33 - Detalhes do Evento (Emissão) 54
Figura 34 - Detalhes do Evento (Certificado) 55
Figura 35 - Detalhes do Evento (Relatórios) 56
Figura 36 - Detalhes do Evento (Exportar Relatórios) 56
Figura 37 - Criar Novo Evento 57
Figura 38 - Criar Novo Evento (Final) 58
Figura 39 - Pré-visualização do certificado 59
Figura 40 - Layout e personalização 60
Figura 41 - QR Code do Evento 61
Figura 42 - Escanear QR Code 62
Figura 43 - Escanear QR Code (Mobile) 62
Figura 44 - Excluir Conta 64

Figura 45 - Excluir Evento 65
Figura 46 - Políticas e Termos de Serviço 66
Figura 47 - API de Mapas 67
Figura 48 - Preferência de Cookies 68
Figura 49 – Integração, Lovable & Supabase 72
Figura 50 - Permissão para usar a localização 73
Figura 51 - Eventos Criados 75
Figura 52 - Eventos Disponíveis 76
Figura 53 - Meus Eventos Inscritos 76
Figura 54 – Sistema de Validação e Rastreamento 77
Figura 55 - Comparativo: Inscrições e Presenças por Evento 79
Figura 56 - Sistema de Avaliação de Eventos 80

LISTA DE SIGLAS E ABREVIATURAS

ICP - Brasil	Infraestrutura de Chaves Públicas Brasileiras
LBI	Lei Brasileira de Inclusão
LGPD	Lei Geral de Proteção de Dados
QR Code	Código de Resposta Rápida
AC	Autoridades Certificadoras
AR	Autoridades de Registro
SSL	Secure Sockets Layer
JWT	JSON Web Token
PJe	Processo Judicial Eletrônico
e-CNPJ	Certificado Digital de Pessoa Jurídica
e-CPF	Certificado Digital de Pessoa Física
API	Interface de Programação de Aplicações
TST	Tribunal Superior do Trabalho

SUMÁRIO

1 INTRODUÇÃO 13
2 OBJETIVOS 15
2.1 OBJETIVOS GERAIS 15
2.2 OBJETIVOS ESPECÍFICOS 15
3 REVISÃO DE LITERATURA 16
3.1 Fraudes em Certificados e Documentos Públicos 17
3.2 Tendências e Boas Práticas em Certificação Digital 19
3.3 Segurança e Ética 21
3.4 Evolução da Emissão de Certificados 24
3.5 Assinaturas Eletrônicas vs. Assinaturas Digitais: Diferenças Técnicas e Aplicações no Brasil 27
3.6 Plataformas Concorrentes na Emissão de Certificados Digitais 31
3.7 User Experience (UX) em Plataformas de Certificação Digital: a Importância da Usabilidade e Acessibilidade 33
4 DESENVOLVIMENTO 37
4.1 Lovable.dev no Desenvolvimento da Plataforma Certified 38
4.2 Interface do Usuário e Estrutura das Páginas do Sistema 39
5 RESULTADOS 70
5.1 Integração com o Supabase 71
5.2 Limitações Identificadas 73
5.3 Testes Realizados 74
5.4 Planejamento Futuro e Possíveis Expansões 78
6 CONSIDERAÇÕES FINAIS 81
7 REFERÊNCIAS 83

1 INTRODUÇÃO

A organização de eventos e a emissão de certificados passaram por grandes transformações nos últimos anos. As plataformas digitais tornaram esses processos mais acessíveis e eficientes, facilitando tanto a gestão das atividades quanto a distribuição de certificados de participação. Essa evolução permitiu a expansão de eventos em formato online e híbrido, ampliando o alcance de públicos diversos e tornando a certificação digital uma prática comum em ambientes acadêmicos e profissionais (PSIUEducação).

Contudo, a digitalização também trouxe desafios relevantes, especialmente no que diz respeito à autenticidade dos certificados e à segurança na aquisição de ingressos. A falsificação de certificados de participação compromete diretamente a credibilidade de eventos e instituições. Indivíduos mal-intencionados podem criar ou adulterar certificados com o objetivo de obter vantagens indevidas, como comprovação de qualificações que não foram adquiridas. De modo semelhante, a comercialização de ingressos está suscetível a fraudes, impactando tanto consumidores quanto organizadores. Golpistas criam sites falsos que simulam plataformas legítimas de venda, enganando usuários e promovendo a distribuição de ingressos inexistentes. Além disso, revendedores não autorizados comercializam bilhetes inválidos, gerando prejuízos financeiros e afetando a reputação dos eventos (ClearSale).

A crescente exigência por comprovações formais tem impulsionado a valorização dos certificados digitais como instrumentos legítimos de validação de competências e experiências. Em ambientes acadêmicos e corporativos, esses documentos assumem papel importante em processos seletivos, progressão de carreira e atribuição de créditos. No entanto, sua efetividade depende diretamente da confiabilidade do sistema que os emite. Diante desse cenário, investir em plataformas que aliam tecnologia, segurança e rastreabilidade torna-se essencial não apenas para coibir fraudes, mas também para fortalecer a confiança social na certificação digital como um recurso institucional válido e transparente (CryptoID).

Outro fator determinante é o avanço da digitalização e a crescente demanda por soluções tecnológicas que otimizem a organização de eventos e a emissão de certificações. Um sistema inovador que adote métodos de verificação da participação, como monitoramento de presença, QR Codes ou validação por meio de inteligência

artificial, pode não apenas mitigar riscos de fraude, mas também agregar valor ao setor de certificação digital. Segundo a plataforma Even3, “os certificados digitais devem ser emitidos com qualidade para impressão e um código de autenticidade que permita validação online, garantindo segurança ao organizador e ao participante” (Even3, 2025).

A confiabilidade da certificação digital também está diretamente relacionada à experiência do usuário e à credibilidade das instituições emissoras. Em um cenário em que processos seletivos, certificações profissionais e participações acadêmicas dependem cada vez mais de documentos digitais, torna-se fundamental que as plataformas responsáveis por sua emissão adotem mecanismos de validação robustos e transparentes. A ausência desses mecanismos pode gerar não apenas prejuízos individuais, mas também abalar a confiança em sistemas educacionais e organizacionais como um todo. Dessa forma, investir em soluções tecnológicas que garantam autenticidade, rastreabilidade e fácil verificação dos certificados não é apenas uma questão de eficiência, mas também de responsabilidade institucional e de garantia de direitos (CryptoID).

Além disso, a emissão profissional de certificados pode ajudar a aumentar a satisfação e o engajamento dos participantes. Os certificados podem servir como uma forma de reconhecimento pelo esforço e dedicação dos participantes no evento, o que pode ajudar a incentivar sua participação em eventos futuros e a aumentar a sua fidelidade à marca ou organização responsável pelo evento. E muitos participantes ainda compartilham a conquista de seus certificados em redes sociais importantes, como o LinkedIn (E-Certificado).

2 OBJETIVOS

2.1 OBJETIVOS GERAIS

Desenvolver uma plataforma digital segura e automatizada para a emissão de certificados de participação em eventos, garantindo a autenticidade dos documentos por meio de mecanismos de verificação e controle de presença.

2.2 OBJETIVOS ESPECÍFICOS

- Implementar um sistema de cadastro para organizadores, eventos e participantes.
- Desenvolver mecanismos de verificação de presença, incluindo o uso de geolocalização (GPS) e QR Codes.
- Criar uma interface intuitiva e responsiva para administradores e usuários finais.
- Garantir a emissão de certificados digitais com código único de autenticação.
- Integrar um sistema de validação pública de certificados para conferência por terceiros.

3 REVISÃO DE LITERATURA

A emissão de certificados digitais é uma prática comum em eventos, cursos e treinamentos, no entanto, muitos sistemas utilizados atualmente ainda apresentam falhas significativas de segurança, especialmente no que diz respeito à verificação da participação efetiva do usuário.

Grande parte das plataformas permite a geração de certificados sem qualquer tipo de comprovação presencial ou digital, o que favorece a ocorrência de fraudes e falsificações. Essa fragilidade compromete a credibilidade dos documentos emitidos e coloca em risco a reputação das instituições envolvidas.

A ausência de mecanismos robustos de autenticação nos processos de certificação digital expõe organizadores e participantes a prejuízos. A emissão de certificados inválidos pode ser usada como ferramenta para obtenção de vantagens indevidas, como comprovação de capacitações não realizadas ou participação fictícia em eventos.

Figura 1 - Certificação Digital: Segurança na Comunicação

Fonte: https://consultasaj.tjam.jus.br/WebHelp/id_seguranca_da_informacao.htm

A autenticidade dos certificados digitais é um fator essencial para garantir a validade de registros acadêmicos e profissionais. Instituições que não adotam medidas de controle eficazes correm o risco de comprometer sua imagem e credibilidade no mercado.

Portanto, desenvolver uma plataforma que una usabilidade e segurança, garantindo que apenas participantes que cumpram os critérios definidos pelos

organizadores tenham acesso à certificação, representa uma resposta direta a essa lacuna identificada nos sistemas tradicionais.

A necessidade de garantir a autenticidade de certificados digitais e a segurança nos processos de validação de presença em eventos motivou a criação da plataforma Certified. Muitas das soluções disponíveis atualmente não exigem comprovação efetiva da participação, o que abre espaço para fraudes e compromete a credibilidade dos documentos emitidos. Diante disso, este trabalho busca desenvolver uma ferramenta confiável e inovadora, que assegure que apenas participantes devidamente presentes nos eventos possam emitir seus certificados.

O cenário atual demonstra um crescimento expressivo na preocupação de empresas e instituições com a prevenção a fraudes em ambientes digitais. Segundo pesquisa da Serasa Experian (2024), 58% das empresas brasileiras relataram aumento na preocupação com fraudes nos últimos 12 meses, o que reflete a urgência em adotar soluções tecnológicas mais seguras. Esse movimento acompanha uma tendência mais ampla de digitalização dos processos de validação e controle de autenticidade documental.

Além disso, um estudo encomendado pela Mastercard ao Instituto Datafolha apontou que 64% das empresas brasileiras são alvo de fraudes ou ataques digitais com média ou alta frequência. Tais dados ressaltam a necessidade de implementar tecnologias antifraude de ponta, com destaque para o uso de inteligência artificial e validações automatizadas como ferramentas estratégicas de segurança.

3.1 Fraudes em Certificados e Documentos Públicos

Fraudes na emissão de certificados não são incomuns e afetam diferentes setores. No contexto acadêmico e corporativo, já houve casos em que indivíduos falsificaram certificados de participação em eventos e cursos para obter vantagens profissionais. O Conselho Internacional de Museus (ICOM), por exemplo, alertou sobre golpes envolvendo certificados falsos de autenticidade e exportação, usados para enganar instituições e colecionadores de arte. Situações semelhantes ocorrem em outras áreas, como na certificação fitossanitária, onde empresas fraudulentas emitiram documentos falsos alegando que produtos agrícolas haviam sido inspecionados, afetando a credibilidade dos exportadores brasileiros.

No Brasil, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) tem desempenhado um papel crucial na emissão de certificados digitais seguros. Segundo a Associação Nacional de Certificação Digital (ANCD), "em outubro de 2024, foram emitidos 911.953 certificados digitais no padrão da ICP-Brasil, marcando a primeira vez que a emissão ultrapassou 900 mil certificados em um único mês de outubro" (ANCD, 2024). Esses números destacam a importância de infraestruturas robustas e confiáveis na prevenção de fraudes relacionadas à certificação digital.

Ainda no contexto do Brasil, casos de fraudes de certificados no país vem aumentando recentemente. Em dezembro de 2022, a Polícia Federal desarticulou um esquema no estado do Rio de Janeiro, onde uma quadrilha fraudava certificados digitais para emitir alvarás judiciais falsos. Os investigados acessavam sistemas eletrônicos de órgãos públicos com identidades forjadas e geravam documentos jurídicos fraudulentos para movimentar valores indevidos (G1, 2022).

Outro episódio marcante ocorreu em julho de 2024, quando a Polícia Federal deflagrou uma operação no interior de São Paulo contra a falsificação de diplomas de graduação. Os diplomas fraudulentos estavam sendo usados por indivíduos sem qualificação formal para exercer cargos que exigem formação superior, o que levanta sérias preocupações sobre a integridade dos processos de certificação no país (G1, 2024).

Figura 2 - Mulher falsifica diploma para conseguir emprego em escola infantil no AP

Fonte: https://g1.globo.com/ap/amapa/noticia/2018/11/28/mulher-falsifica-diploma-para-conseguir-emprego-em-escola-infantil-no-ap-ela-foi-indiciada-por-estelionato.ghtml

A falsificação de certificados digitais representa uma ameaça significativa à segurança das transações eletrônicas e à integridade das identidades digitais. Embora os casos de fraude divulgados na mídia frequentemente envolvam figuras públicas ou autoridades, há uma preocupação crescente com fraudes que afetam cidadãos comuns. Criminosos podem utilizar certificados digitais falsificados para criar empresas fictícias, obter dados pessoais indevidamente e contrair empréstimos fraudulentos, resultando em prejuízos financeiros e danos à reputação das vítimas. (JUSBRASIL, 2024).

O Instituto Nacional de Tecnologia da Informação (ITI), por meio da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), é responsável por regulamentar a emissão de certificados digitais no país. Apesar de existirem mais de 20 autoridades certificadoras registradas e de serem emitidos aproximadamente 3,5 milhões de certificados digitais anualmente, a incidência de fraudes é relativamente baixa, estimada em 0,0002% ao ano. No entanto, esses casos isolados evidenciam vulnerabilidades no sistema de certificação que podem ser exploradas por fraudadores. (JUSBRASIL, 2024).

Do ponto de vista jurídico, as autoridades certificadoras têm a responsabilidade de adotar protocolos rigorosos de verificação de identidade ao emitir certificados digitais. Falhas nesse processo podem comprometer a autenticidade dos documentos e a segurança jurídica das partes envolvidas. Em situações onde a certificadora não observa as devidas cautelas na verificação da identidade do solicitante, ela pode ser responsabilizada pelos danos causados às vítimas de fraudes.

3.2 Tendências e Boas Práticas em Certificação Digital

A certificação digital tem passado por transformações significativas, impulsionadas pela crescente digitalização dos processos e pela necessidade de garantir segurança, autenticidade e rastreabilidade na emissão de documentos eletrônicos. Entre as principais tendências observadas, destaca-se a incorporação de códigos QR como ferramenta para autenticação de certificados. Essa tecnologia permite que qualquer pessoa, com o uso de um dispositivo móvel, acesse instantaneamente os dados associados ao certificado, facilitando a verificação por parte de empresas e instituições. Um exemplo de aplicação prática ocorreu no âmbito governamental, quando o Ministério da Agricultura, Pecuária e Abastecimento (MAPA)

implementou assinaturas eletrônicas em certificados sanitários, incluindo QR Codes e códigos de autenticação para garantir a validade dos documentos emitidos (GOV.BR, 2022).

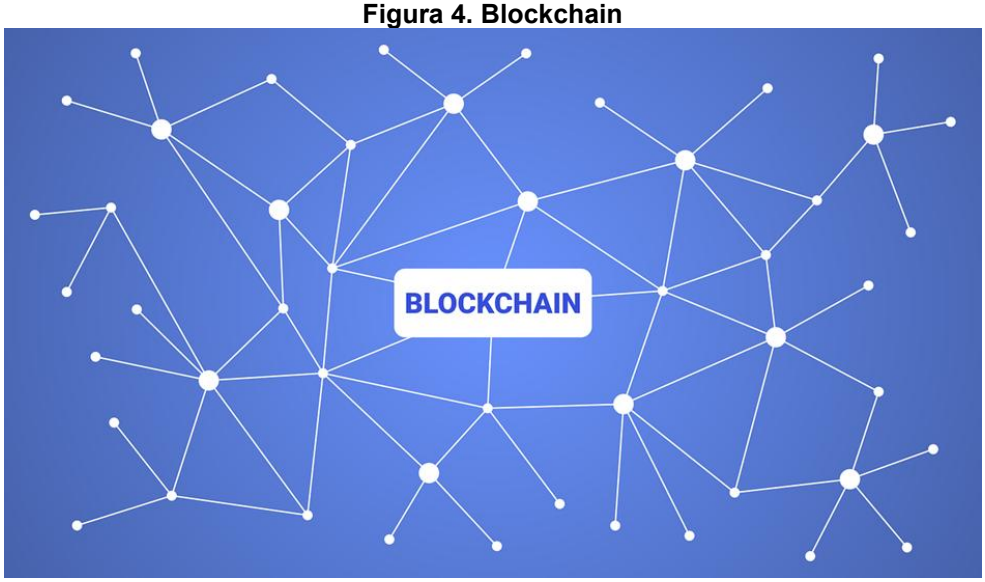
Figura 3. Certificação Digital no SIGSIF

Fonte: https://www.youtube.com/watch?v=H6hefIo-1ZM

Outra inovação promissora é o uso da geolocalização como mecanismo de validação. Ao registrar a localização do participante no momento do evento, a plataforma adiciona uma camada de segurança adicional, assegurando que o usuário esteve fisicamente presente no local. Essa tecnologia tem sido adotada inclusive em processos jurídicos, como demonstrado pelo Tribunal Superior do Trabalho (TST), que reconheceu a geolocalização como prova digital válida na comprovação da jornada de trabalho de um bancário. O uso dessa abordagem em sistemas de certificação digital fortalece a integridade dos dados e contribui para prevenir fraudes na emissão de certificados.

Além disso, a tecnologia blockchain tem ganhado espaço como solução inovadora na certificação digital. Ao registrar os certificados em blocos encadeados e imutáveis, o sistema garante que nenhuma informação seja alterada ou adulterada após a emissão. Essa característica de imutabilidade reforça a confiança nas certificações emitidas, especialmente em ambientes acadêmicos e corporativos, onde a validade de registros é crucial. Conforme análise apresentada por Sánchez González e colaboradores (2021), a aplicação do blockchain em processos de certificação assegura transparência, rastreabilidade e resistência a fraudes.

Figura 4. Blockchain



Fonte: https://pixabay.com/vectors/blockchain-cryptocurrency-network-3277336/

Observa-se também um crescimento global na adoção de identificação biométrica associada a certificados digitais, elevando o nível de segurança das autenticações. Combinando características únicas do indivíduo, como impressões digitais ou reconhecimento facial, ao processo de certificação, as plataformas conseguem garantir, de forma praticamente inequívoca, que o titular do documento é de fato a pessoa que participou do evento ou obteve determinada qualificação. Essa abordagem atende às exigências contemporâneas por sistemas mais robustos e à prova de fraudes.

Por fim, é importante destacar que a adoção de tecnologias como os códigos QR exige o cumprimento de boas práticas para assegurar sua segurança. Entre essas práticas estão a geração dos códigos por fontes confiáveis, o uso de sistemas com certificados SSL para evitar interceptações e o monitoramento constante para detectar tentativas de clonagem ou uso indevido. Conforme alerta o portal QR Code Tiger (2024), mesmo uma tecnologia amplamente difundida como o QR Code pode ser explorada de forma maliciosa caso não haja atenção aos protocolos de segurança.

3.3 Segurança e Ética

A segurança da informação e a ética na gestão de dados são pilares indispensáveis em qualquer sistema que envolva a emissão de certificados digitais. Em um cenário onde a digitalização dos serviços cresce exponencialmente, garantir a confidencialidade, a integridade e a autenticidade dos dados é uma exigência técnica

e legal. A certificação digital lida diretamente com informações sensíveis, como identidade civil, dados de eventos e qualificações profissionais, o que requer mecanismos eficazes de proteção contra acessos não autorizados e tentativas de fraude.

Nesse sentido, recomenda-se o uso de práticas como criptografia robusta, autenticação multifatorial e auditorias periódicas dos sistemas, a fim de mitigar vulnerabilidades. Segundo o Manual de Boas Práticas publicado pela Certisign, a adoção de boas práticas de segurança deve envolver tanto a infraestrutura tecnológica quanto a educação dos usuários, promovendo uma cultura de responsabilidade digital (CERTISIGN, 2018). A conscientização dos participantes sobre os riscos relacionados à má gestão de certificados, como compartilhamento indevido de dados ou uso de plataformas não seguras, é parte fundamental de um sistema ético e seguro.

Do ponto de vista ético, destaca-se a importância da transparência nas relações entre os responsáveis pela certificação e os usuários. Iniciativas como o Selo de Ação Ética na Certificação Digital, desenvolvido pela Associação das Autoridades de Registro do Brasil (AARB), são exemplos concretos de esforços para garantir condutas responsáveis no setor. Ao aderirem ao selo, as certificadoras se comprometem com diretrizes de governança, integridade nas transações e respeito ao consumidor. A Protense, por exemplo, foi a primeira certificadora a aderir à proposta, demonstrando o valor da autorregulação como instrumento de credibilidade (AARB, 2024).

Figura 5. Selo de Ação Ética

Fonte: https://aarb.org.br/seloacaoetica/

Além das práticas institucionais, a conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) é indispensável. A LGPD estabelece critérios rigorosos para o tratamento de dados pessoais, incluindo o princípio da finalidade, o livre acesso, a segurança e a prevenção. Tais diretrizes são especialmente relevantes em processos que envolvem a coleta, armazenamento e validação de dados de participantes em plataformas de certificação. Ao seguir essas exigências legais, as instituições não apenas evitam sanções, mas também fortalecem a confiança dos usuários em seus serviços.

Um exemplo concreto da aplicação de princípios de segurança e ética na certificação digital é o novo modelo da carteira de identidade nacional (RG digital). Implementado em diversos estados brasileiros desde 2022, o documento conta com um QR Code único e assinatura digital padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), permitindo a validação rápida e segura da identidade do cidadão. Além de centralizar dados de vários documentos em um único registro, o RG digital visa combater fraudes e facilitar a verificação por parte de órgãos públicos e privados. Segundo o Governo Federal, o objetivo da nova identidade digital é “aumentar a segurança, simplificar a identificação dos brasileiros e reduzir o número de fraudes” (GOV.BR, 2022).

Figura 6. RG Digital

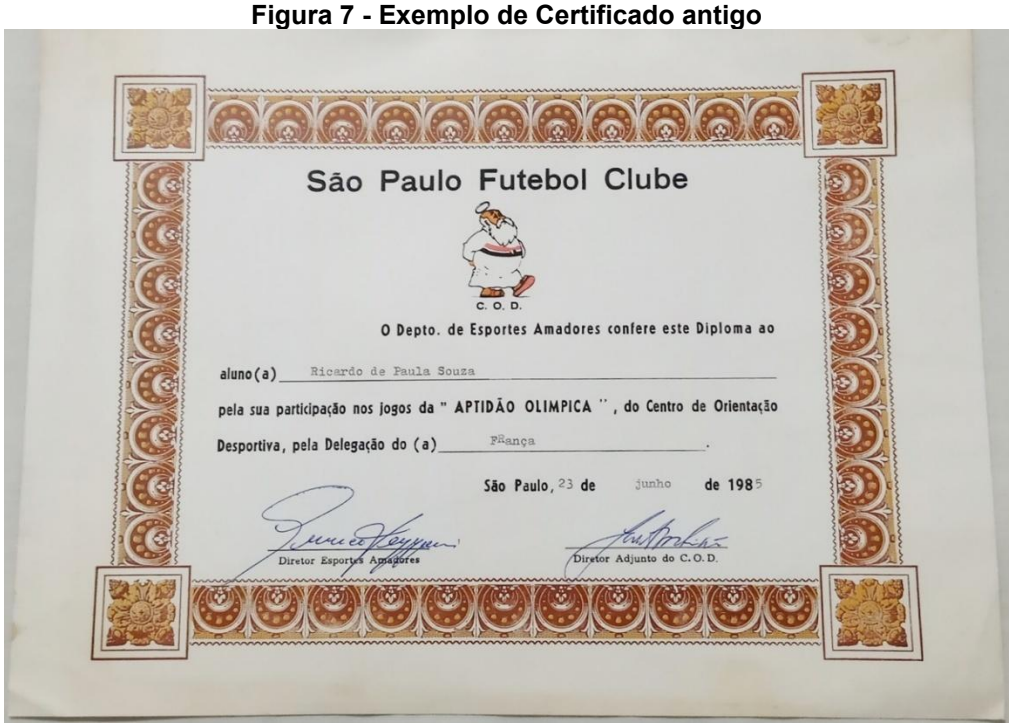
Fonte: https://idososbrasil.com.br/rg-digital-para-idosos-evite-perder-beneficios-mantendo-o-documento-atualizado/

Portanto, o desenvolvimento de uma plataforma de certificação digital não deve se limitar à aplicação de tecnologias, mas considerar o ecossistema ético, jurídico e social no qual ela está inserida. A segurança das informações e o respeito aos direitos dos usuários são fatores que consolidam a legitimidade dos certificados emitidos e garantem o sucesso e a aceitação da plataforma no mercado.

3.4 Evolução da Emissão de Certificados

A emissão de certificados passou por uma transformação significativa ao longo das últimas décadas, impulsionada pelo avanço tecnológico e pela crescente digitalização dos processos administrativos e acadêmicos. Inicialmente, os certificados eram elaborados manualmente, impressos em papel timbrado e assinados fisicamente. Esse modelo tradicional envolvia altos custos com impressão, autenticação, armazenamento e logística de distribuição, além de oferecer pouca ou nenhuma proteção contra fraudes, extravios e falsificações (CERTBRASIL, 2024).

Figura 7 - Exemplo de Certificado antigo

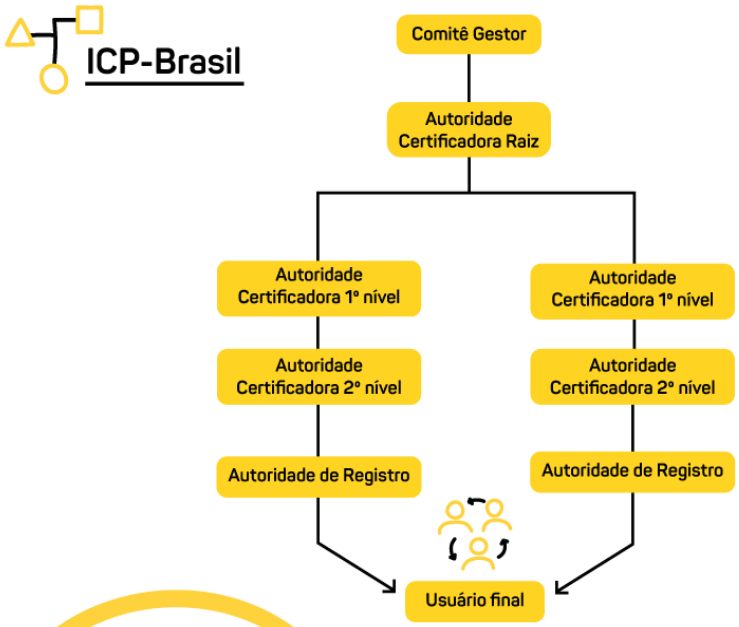


Fonte: https://www.flaviasantosleiloes.com.br/peca.asp?ID=11310607

Com o surgimento e a consolidação da internet, especialmente a partir da década de 1990, cresceu a demanda por métodos mais eficientes e seguros para emissão e verificação de documentos. Nesse contexto, a certificação digital emergiu como uma solução baseada em criptografia assimétrica, permitindo a autenticação de identidades e a verificação de integridade de documentos eletrônicos. Países como os Estados Unidos, Alemanha e Japão foram pioneiros na normatização do uso de certificados digitais para transações seguras (CERTBRASIL, 2024).

No Brasil, o marco legal da certificação digital foi estabelecido com a publicação da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Essa estrutura definiu uma cadeia hierárquica de confiança composta por Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs), responsáveis pela emissão, gestão e revogação dos certificados digitais, garantindo sua validade jurídica em território nacional (BRASIL, 2001).

Figura 8 - ICP-Brasil



Fonte: https://assinei.digital/mp-2200-2/

A certificação digital passou a ser incorporada de forma progressiva em setores-chave da administração pública. A Receita Federal do Brasil, por exemplo, passou a aceitar e utilizar certificados digitais como meio válido para a entrega de declarações fiscais e autenticação em seus sistemas, promovendo maior segurança e agilidade nos processos, enquanto o sistema do Processo Judicial Eletrônico (PJe) adotou assinaturas digitais como forma de autenticar petições e garantir a integridade dos processos. A emissão de Notas Fiscais Eletrônicas (NF-e) também é viabilizada por meio de certificados digitais, demonstrando sua ampla aplicabilidade em processos que exigem confiabilidade e autenticidade (CERTBRASIL, 2024).

A evolução tecnológica permitiu ainda a incorporação de novas funcionalidades aos sistemas de certificação, como a inserção de QR Codes nos documentos, a validação de presença via geolocalização e, mais recentemente, a integração com blockchain para fins de rastreabilidade e imutabilidade de registros. Essas inovações estão alinhadas com as exigências contemporâneas por soluções mais escaláveis, transparentes e resistentes a fraudes (ANCD, 2024).

Figura 9 - Exemplo de verificação para validação de um certificado

Fonte: https://suporte.certisign.com.br/duvidas-suporte/certificado-servidor/ssl-icpbrasil/solicitacao-do-certificado

Em 2024, a ICP-Brasil registrou o maior número de emissões de certificados digitais de sua história, superando a marca de 10,5 milhões de emissões. O dado evidencia a consolidação da certificação digital como uma ferramenta fundamental para a transformação digital segura no Brasil, especialmente em tempos de avanço do governo eletrônico, ensino remoto e automação de processos administrativos (ANCD, 2024).

3.5 Assinaturas Eletrônicas vs. Assinaturas Digitais: Diferenças Técnicas e Aplicações no Brasil

Embora os termos “assinatura eletrônica” e “assinatura digital” sejam frequentemente utilizados como sinônimos, trata-se de conceitos distintos tanto do ponto de vista técnico quanto jurídico. A assinatura eletrônica é uma categoria ampla que abrange qualquer mecanismo de autenticação em ambiente digital, como aceite por e-mail, login com senha ou biometria. Já a assinatura digital é baseada em criptografia assimétrica e requer o uso de um certificado digital emitido por autoridade certificadora vinculada à ICP-Brasil. Segundo a Serasa Experian (2023), apenas a assinatura digital garante, tecnicamente, a integridade e a autenticidade do

documento em nível elevado, sendo recomendada para processos com alta exigência legal.

A regulamentação brasileira estabelece três tipos de assinatura eletrônica: simples, avançada e qualificada. A assinatura qualificada corresponde à assinatura digital com certificado ICP-Brasil, sendo a única com presunção legal de veracidade. Conforme detalhado pelo Governo Federal, esse modelo é obrigatório em documentos que exigem a máxima garantia de autoria e integridade, como contratos públicos, registros médicos e declarações judiciais (GOV.BR, 2023).

Além da aplicação em serviços públicos, o uso da assinatura digital se estende a serviços bancários, acadêmicos e corporativos. A plataforma Gov.br, por exemplo, permite que usuários com conta de nível prata ou ouro assinem documentos digitais com validade jurídica reconhecida, integrando de forma segura diferentes esferas da administração pública (GOV.BR, 2023).

Figura 10 - Os três tipos de assinatura eletrônica

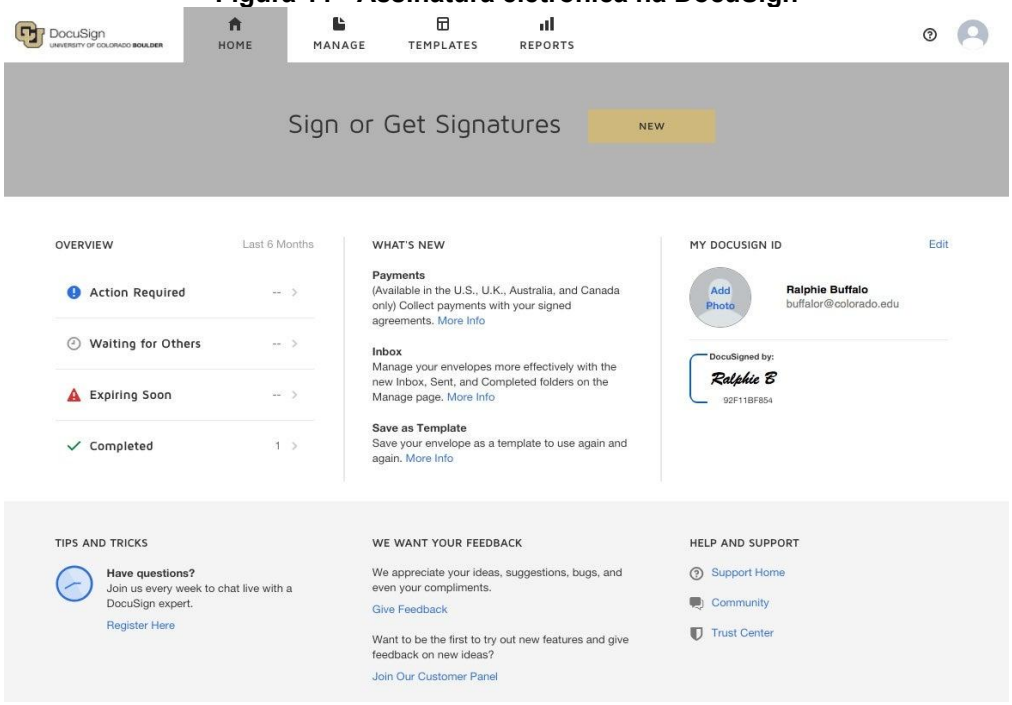
Fonte: https://kb.ufla.br/books/solicitacoes-de-servicos/page/classificacao-de-assinaturas-eletronicas

Diversas empresas privadas também incorporaram ferramentas de assinatura eletrônica e digital para otimizar processos e garantir segurança documental. Entre elas estão a Docusign, Clicksign e ZapSign, que oferecem níveis diferentes de autenticação com base nas necessidades de cada transação. Essas plataformas têm contribuído para a digitalização segura de processos internos e externos, com respaldo jurídico crescente (DOCUSIGN, 2023).

A DocuSign é uma das líderes globais em soluções de assinatura eletrônica, oferecendo uma plataforma robusta que atende a diversas necessidades

empresariais. Sua tecnologia permite que documentos sejam assinados eletronicamente com segurança, com conformidade internacional, inclusive com legislações como o GDPR e o eIDAS europeu. Além disso, oferece funcionalidades avançadas de gerenciamento de contratos, trilhas de auditoria e integrações com diversos sistemas corporativos, o que a torna uma solução completa para empresas que buscam confiabilidade e escalabilidade (DOCUSIGN, 2023).

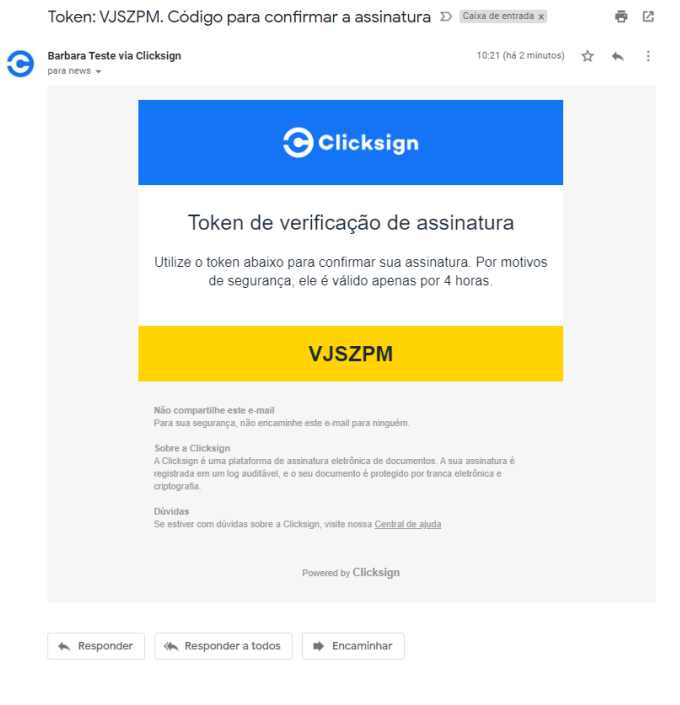
Figura 11 - Assinatura eletrônica na DocuSign



Fonte: https://oit.colorado.edu/services/business-services/docusign

A Clicksign, plataforma nacional pioneira em assinaturas eletrônicas, oferece uma abordagem acessível e segura, integrando múltiplas formas de autenticação, como biometria facial, autenticação via SMS e integração com certificados ICP-Brasil. A solução também permite personalização de marca e fluxos de assinatura em etapas, além de oferecer conformidade com a Lei Geral de Proteção de Dados (LGPD), garantindo segurança jurídica para empresas que operam com contratos digitais em larga escala (CLICKSIGN, 2023).

Figura 12 - Exemplo de token para confirmação de assinatura eletrônica



Fonte: https://blog.b2bstack.com.br/clicksign-assinatura-eletronica/

Essas soluções digitais não apenas modernizam os fluxos de trabalho, mas também promovem economia de tempo e recursos. A digitalização da assinatura elimina etapas manuais, reduz o uso de papel, facilita a rastreabilidade dos documentos e acelera o fechamento de contratos. Segundo a DocuSign, empresas que adotam sua solução economizam, em média, 82% do tempo gasto em processos de assinatura, além de observarem aumento significativo na satisfação dos clientes e colaboradores (DOCUSIGN, 2023).

A escolha entre essas ferramentas depende das necessidades específicas de cada organização. Enquanto empresas de grande porte podem se beneficiar das soluções completas e integradas da DocuSign, organizações que priorizam simplicidade e rapidez podem optar por plataformas como ZapSign. A Clicksign, por outro lado, oferece um equilíbrio entre segurança jurídica e facilidade de uso, sendo bastante utilizada por escritórios de advocacia, imobiliárias e instituições de ensino (CLICKSIGN, 2023).

Dessa forma, a adesão a plataformas de assinatura eletrônica e digital se consolidou como uma etapa essencial da transformação digital no setor privado. Com soluções adaptáveis às mais diversas demandas, essas ferramentas viabilizam operações mais eficientes, seguras e sustentáveis, contribuindo para a maturidade digital das empresas brasileiras (MIGALHAS, 2023).

Diante das diversas alternativas disponíveis no mercado, a escolha entre assinatura eletrônica e assinatura digital deve ser pautada pelas exigências legais e pelo nível de segurança requerido em cada aplicação. Documentos que envolvem maior responsabilidade jurídica ou que exigem garantia de autenticidade, como certificados de participação, contratos jurídicos ou registros acadêmicos, tendem a se beneficiar da assinatura digital vinculada à ICP-Brasil. Já procedimentos de menor risco podem ser devidamente formalizados com assinaturas eletrônicas simples ou avançadas, desde que respeitados os critérios de validade e consentimento.

Com o avanço das tecnologias e a consolidação de práticas digitais em diversos setores, as soluções de assinatura eletrônica e digital tornaram-se aliadas indispensáveis para a modernização de processos. A compreensão clara das diferenças entre esses modelos, aliada à escolha adequada da ferramenta, contribui não apenas para a eficiência operacional, mas também para a confiabilidade e legitimidade das transações realizadas em ambiente digital. Segundo a Bry (2024), a assinatura digital é uma ferramenta essencial para empresas que desejam modernizar seus processos, garantir segurança jurídica e aumentar a eficiência operacional. (BRY, 2024).

3.6 Plataformas Concorrentes na Emissão de Certificados Digitais

O mercado brasileiro de certificação digital tem experimentado um crescimento significativo nos últimos anos, impulsionado pela digitalização de processos e pela necessidade de segurança nas transações eletrônicas. Em 2024, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) registrou um recorde histórico, com mais de 10,6 milhões de certificados digitais emitidos, representando um aumento de 11,3% em relação ao ano anterior (ANCD, 2025).

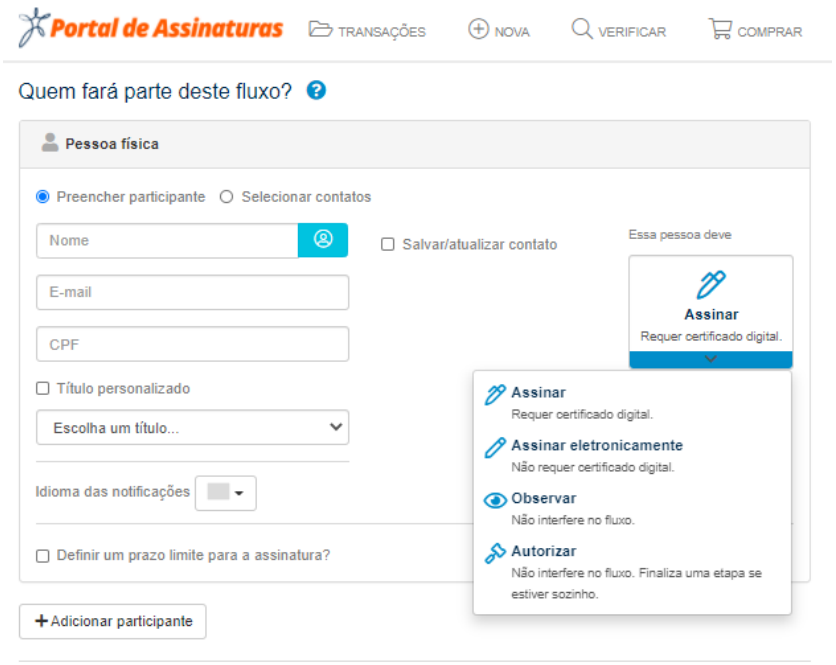
Nesse contexto de expansão e amadurecimento do mercado, destacam-se empresas como a Certisign e a Even3, que oferecem soluções tecnológicas avançadas que atendem tanto às exigências legais quanto às demandas operacionais de diversos segmentos. Essas plataformas combinam segurança criptográfica, usabilidade e infraestrutura escalável, permitindo a emissão e a gestão de certificados digitais com validade jurídica e elevado grau de confiabilidade.

Certisign: Fundada em 1996, a Certisign é uma das pioneiras no setor de certificação digital no Brasil. A empresa oferece uma ampla gama de produtos,

incluindo certificados para pessoas físicas (e-CPF) e jurídicas (e-CNPJ), além de soluções de assinatura eletrônica e identificação digital. A Certisign também disponibiliza certificados SSL/TLS para sites e plataformas, garantindo a segurança das informações transmitidas online. Além disso, a empresa oferece soluções específicas para setores como saúde, educação e financeiro, demonstrando sua versatilidade e capacidade de atender a diferentes demandas do mercado (CERTISIGN, 2025).

A Certisign também oferece soluções específicas para setores como saúde, educação e financeiro, demonstrando sua versatilidade e capacidade de atender a diferentes demandas do mercado. Por exemplo, a empresa disponibiliza o certificado digital OAB para advogados, permitindo o peticionamento eletrônico com rapidez e segurança (CERTISIGN, 2025).

Figura 13 - Exemplo de assinatura eletrônica na Certisign



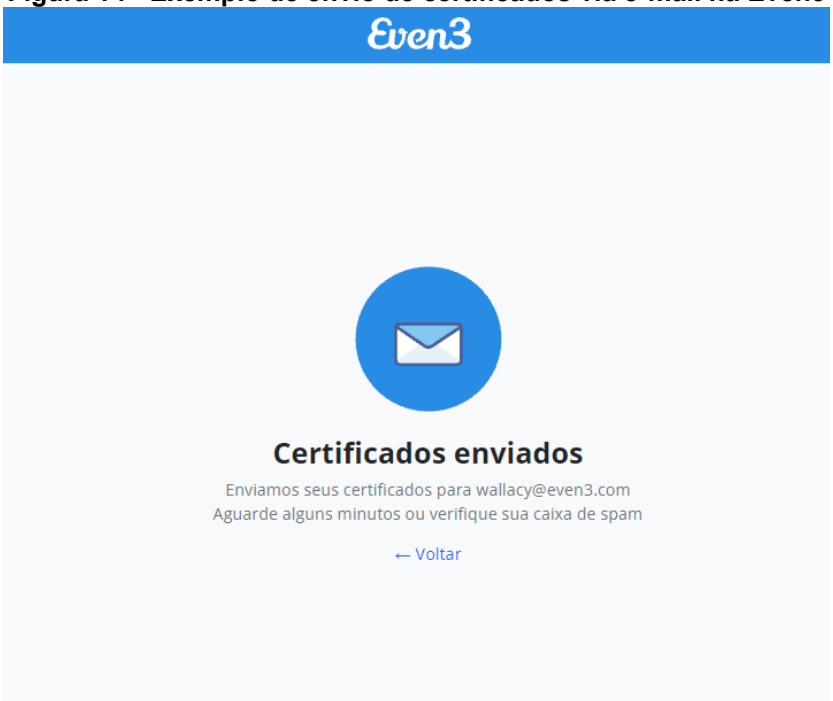
Fonte: https://blog.certisign.com.br/como-criar-um-fluxo-de-assinatura-digital-ou-eletronica/

Even3: A Even3 é uma plataforma especializada na organização de eventos acadêmicos e científicos, oferecendo soluções que abrangem desde a inscrição até a emissão de certificados digitais. A plataforma permite a criação automática de certificados personalizados, com códigos de autenticidade e disponibilidade na nuvem, facilitando o acesso por parte dos participantes. Além disso, a Even3 oferece funcionalidades como submissão de trabalhos, credenciamento e transmissão online,

proporcionando uma experiência completa para organizadores e participantes de eventos (EVEN3, 2025).

A Even3 também se destaca por sua abordagem sustentável, reduzindo custos e o uso de papel ao permitir a emissão e distribuição digital de certificados. A plataforma oferece recursos como geração de certificados em massa, códigos de autenticidade para evitar fraudes e armazenamento na nuvem, garantindo que os certificados estejam sempre disponíveis para os participantes (EVEN3, 2025).

Figura 14 - Exemplo de envio de certificados via e-mail na Even3

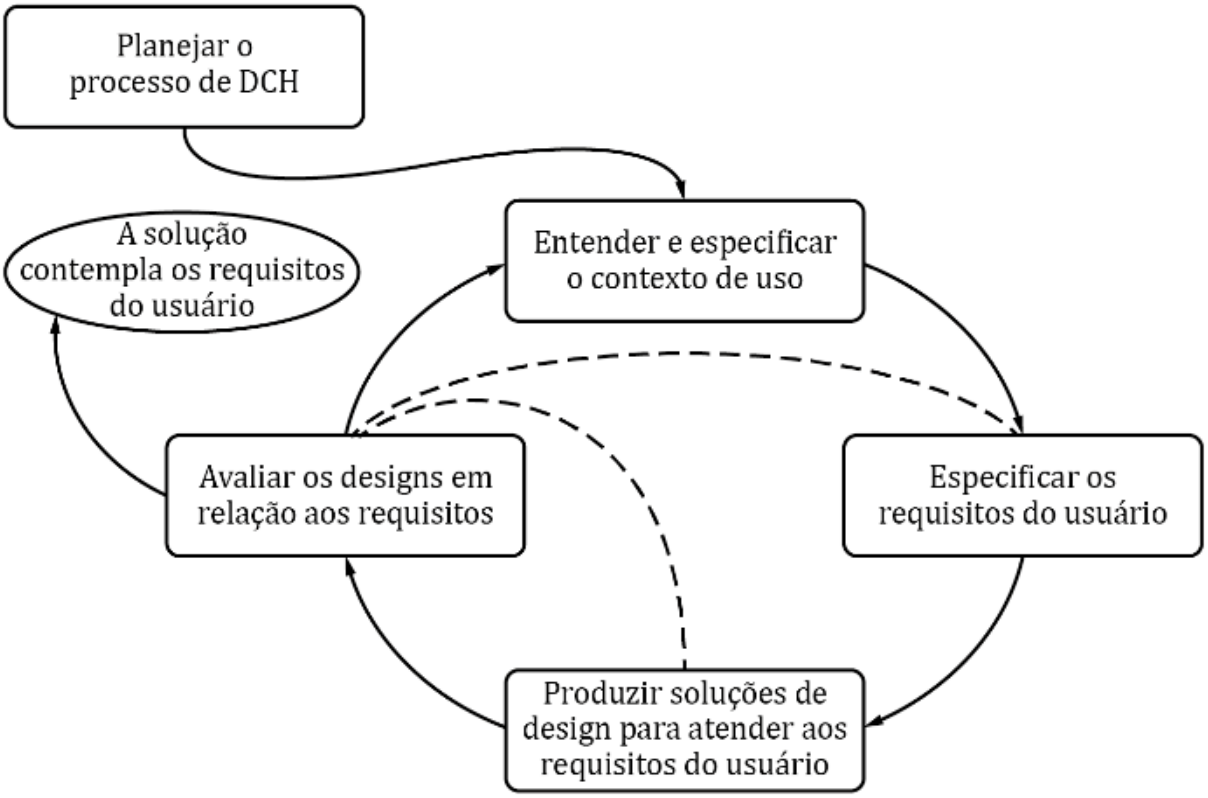


Fonte: https://ajuda.even3.com.br/hc/pt-br/articles/360024002051-Acessar-meus-certificados

3.7 User Experience (UX) em Plataformas de Certificação Digital: a Importância da Usabilidade e Acessibilidade

O conceito de User Experience (UX) refere-se à qualidade da experiência percebida pelo usuário ao interagir com um sistema, produto ou serviço digital, considerando aspectos como eficiência, facilidade de uso e satisfação. De acordo com a norma ISO 9241-210, UX envolve todas as percepções e respostas de uma pessoa resultantes do uso e da antecipação de uso de um sistema interativo, sendo um fator fundamental para o sucesso de qualquer plataforma digital (ISO, 2019).

Figura 15 - Modelo da ISO 9241-210



Fonte: https://www.researchgate.net/figure/Figura-10-Modelo-da-ISO-9241-2102010-Fonte-os-autores-com-base-na-ISO-9241-2102010_fig3_326541430

Em plataformas de certificação digital, como a proposta pela Certified, a atenção à UX é essencial para garantir a confiança e a adesão dos usuários. A clareza na apresentação das informações, a simplicidade na navegação e a rapidez na execução de tarefas são elementos que impactam diretamente na eficiência do sistema e na satisfação do usuário. Conforme destaca Norman (2013), um design centrado no usuário não apenas facilita a interação, mas também reduz a ocorrência de erros e melhora a percepção de segurança da plataforma (NORMAN, 2013).

Além da usabilidade, a acessibilidade digital é um aspecto indispensável em plataformas voltadas para emissão de certificados, visto que tais sistemas devem estar disponíveis e utilizáveis por pessoas com diferentes níveis de habilidade, incluindo aquelas com deficiência. A Lei Brasileira de Inclusão (LBI) estabelece que websites e aplicativos devem garantir o acesso de pessoas com deficiência, respeitando padrões internacionais como as Diretrizes de Acessibilidade para Conteúdo da Web (WCAG) do W3C (BRASIL, 2015). Implementar recursos como contraste adequado, navegação por teclado e descrições alternativas para imagens é essencial para assegurar que a certificação digital seja uma ferramenta inclusiva. Além disso, o design responsivo desempenha papel fundamental nesse contexto,

garantindo que a interface da plataforma se adapte adequadamente a diferentes dispositivos e tamanhos de tela, como smartphones e tablets, ampliando o acesso e proporcionando uma experiência consistente e satisfatória para todos os usuários (MORVILLE; ROSENFELD, 2007).

Figura 16 - Lei Brasileira de Inclusão (LBI)

Fonte: https://coddede.blogspot.com/2020/06/lei-brasileira-de-inclusao_22.html

A aplicação de princípios clássicos de usabilidade, como as heurísticas de Nielsen, também é recomendada para sistemas de certificação. Entre essas heurísticas estão a consistência, a prevenção de erros e a visibilidade do status do sistema, que contribuem para uma interação mais intuitiva e segura. Como destaca Nielsen (1995), sistemas que aderem a esses princípios oferecem uma experiência mais previsível e confiável para os usuários, especialmente em contextos críticos como a validação de certificados digitais (NIELSEN, 1995).

Outro elemento fundamental para aprimorar a experiência do usuário em plataformas de certificação digital é o fornecimento de feedback em tempo real durante as interações. Mensagens claras que indicam o sucesso ou a falha de uma ação — como o envio de um formulário ou a validação de dados — são essenciais para reduzir a incerteza e aumentar a confiança do usuário no sistema. Estudos apontam que sistemas que oferecem feedback imediato são percebidos como mais eficientes e confiáveis, contribuindo significativamente para a satisfação do usuário e

a adoção da plataforma (LAUREL, 2014). No contexto da certificação digital, esse recurso se torna ainda mais importante, uma vez que confirma ao usuário etapas críticas como a submissão de dados para emissão de certificados ou o registro de presença em eventos.

Assim, ao considerar a UX no desenvolvimento de plataformas de certificação, promove-se não apenas uma interface mais amigável, mas também um sistema mais confiável, acessível e eficiente. Incorporar boas práticas de UX é uma estratégia fundamental para ampliar a adoção da plataforma, reduzir barreiras de uso e assegurar a qualidade e a credibilidade dos serviços prestados.

4 DESENVOLVIMENTO

O desenvolvimento da plataforma Certified envolveu a aplicação de conceitos fundamentais de engenharia de software, com foco na criação de um sistema seguro, eficiente e acessível para a emissão de certificados digitais. O objetivo principal foi atender às crescentes demandas no cenário de digitalização de eventos, onde a garantia de autenticidade dos documentos e a comprovação de participação são questões essenciais para assegurar a confiança no processo.

O trabalho foi estruturado de modo a priorizar tanto a experiência do usuário quanto a segurança do sistema, adotando tecnologias modernas que permitiram o desenvolvimento de uma plataforma funcional e escalável. O processo de criação da Certified envolveu desde a concepção da interface até a integração com soluções de backend, sempre alinhado às melhores práticas de usabilidade e acessibilidade. Também foram levadas em consideração as exigências legais, especialmente a Lei Geral de Proteção de Dados (LGPD), que orientou o tratamento de dados pessoais dentro da plataforma.

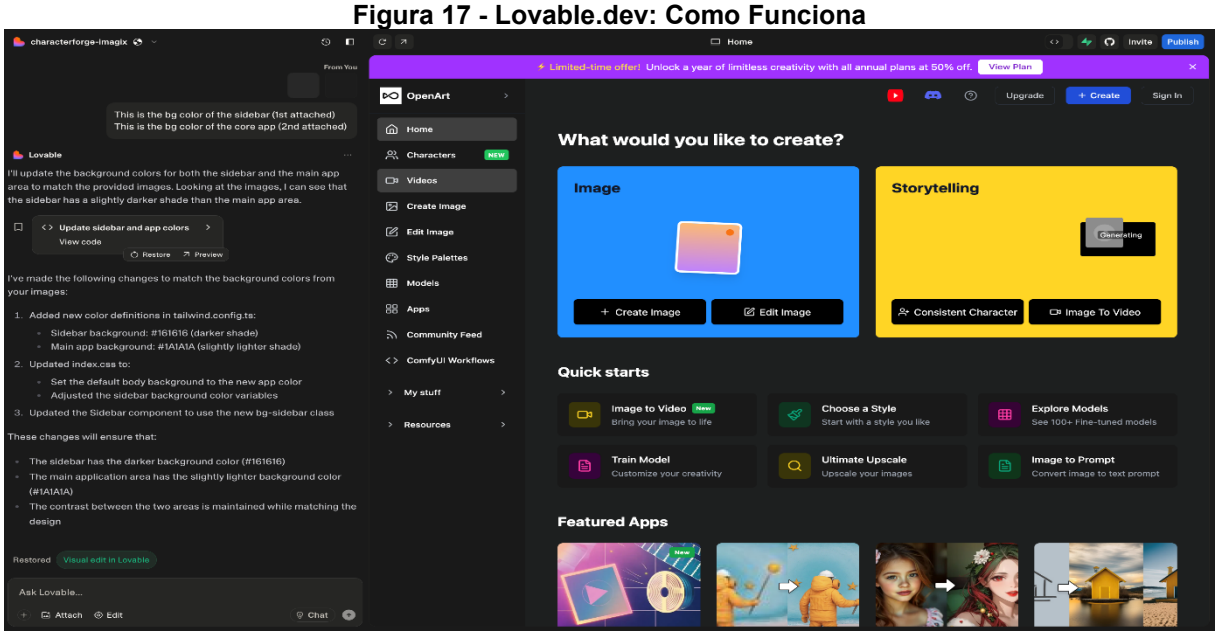
A escolha de ferramentas e tecnologias adequadas foi uma etapa fundamental para garantir a eficiência do sistema. A plataforma foi desenvolvida utilizando Lovable.dev, uma ferramenta no-code que possibilitou a construção ágil da interface e a integração com o backend, proporcionando a flexibilidade necessária para uma solução adaptável e de rápida implementação. A combinação dessa ferramenta com o Supabase, que oferece recursos de banco de dados e autenticação, foi essencial para a criação de um sistema robusto e seguro, permitindo a gestão eficiente de dados e a emissão de certificados digitais.

O desenvolvimento da plataforma também envolveu desafios, principalmente relacionados à personalização da interface e à integração de funcionalidades avançadas. Esses desafios foram superados por meio da utilização de soluções externas, como APIs, para garantir a implementação das funcionalidades desejadas de maneira eficiente.

4.1 Lovable.dev no Desenvolvimento da Plataforma Certified

A escolha do Lovable.dev como ferramenta para o desenvolvimento da plataforma Certified foi motivada por sua abordagem no-code, que facilita a criação de aplicações web de maneira ágil e eficiente, sem a necessidade de codificação manual. O uso de plataformas no-code tem ganhado destaque no desenvolvimento de soluções digitais, pois permite a construção rápida de protótipos e sistemas com funcionalidades essenciais, com foco na usabilidade e na experiência do usuário (PEREIRA; LOPES, 2022).

Figura 17 - Lovable.dev: Como Funciona



Fonte: https://docs.lovable.dev/introduction

O Lovable.dev possibilitou a construção de uma interface responsiva, adaptável a dispositivos móveis e desktop, garantindo que a plataforma fosse acessível e funcional para uma ampla gama de usuários. A integração com React e Vite possibilitou a criação de uma interface dinâmica e de alta performance, otimizando o tempo de carregamento e melhorando a experiência do usuário ao interagir com o sistema. A ferramenta no-code permitiu, assim, uma configuração eficiente da parte visual da plataforma, enquanto o Supabase foi integrado para lidar com as funcionalidades de backend, incluindo o gerenciamento de dados, autenticação de usuários e armazenamento em nuvem. Essa integração foi fundamental para garantir a persistência das informações e a emissão segura dos certificados digitais.

Apesar de suas vantagens, o Lovable.dev apresenta limitações em termos de customização avançada e integração com sistemas externos mais complexos. Em alguns momentos, a equipe de desenvolvimento precisou recorrer ao uso de APIs externas para implementar funcionalidades que não eram diretamente suportadas pela ferramenta, como a personalização de certos elementos de interface e a integração com sistemas de geolocalização para validação de presença. Tais limitações foram contornadas de maneira eficiente, permitindo que o projeto seguisse dentro dos parâmetros desejados, mas evidenciando a necessidade de flexibilidade nas ferramentas utilizadas.

A adoção do Lovable.dev, portanto, foi estratégica para o desenvolvimento inicial da plataforma, possibilitando que o projeto fosse realizado dentro de um cronograma reduzido e com custos controlados, sem comprometer a qualidade das funcionalidades essenciais. Esse tipo de plataforma se alinha com a tendência crescente de desenvolvimento ágil, permitindo a criação de soluções funcionais e adaptáveis, especialmente para sistemas de certificação digital, que exigem alta confiabilidade e segurança.

4.2 Interface do Usuário e Estrutura das Páginas do Sistema

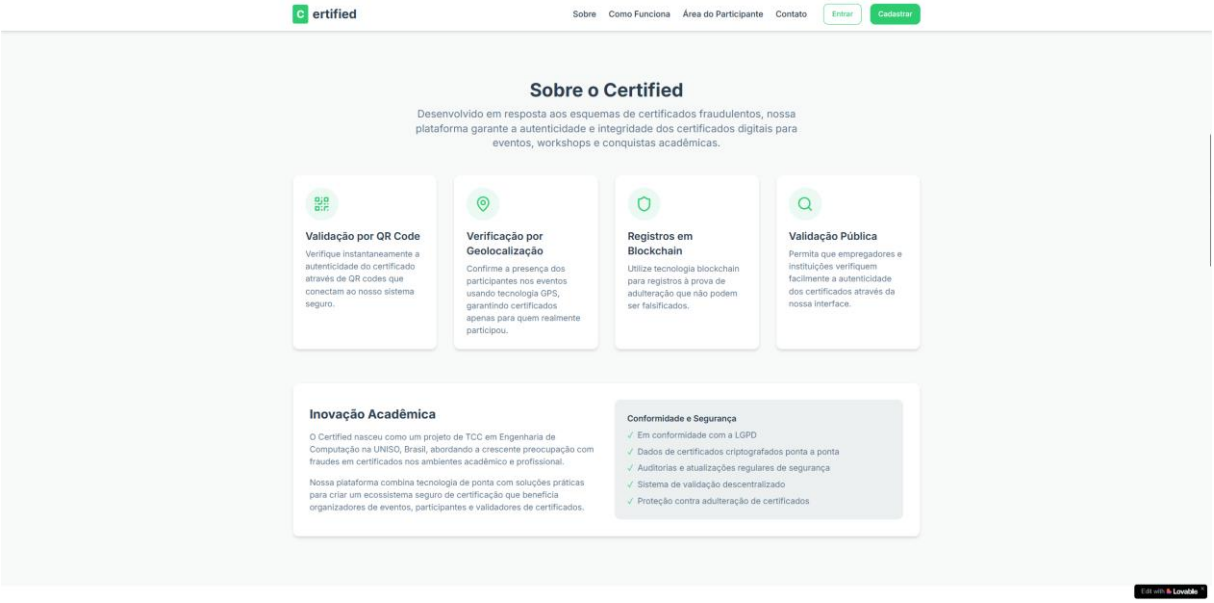
Figura 18. Página Inicial

Fonte: Elaboração Própria

Na Figura 18, observa-se a página principal da plataforma Certified, projetada para comunicar de forma direta a proposta do sistema: emissão de certificados digitais

com foco em autenticidade e segurança. O layout destaca um herói visual com imagem de fundo e chamada central, em que os termos de valor aparecem realçados em verde, reforçando os pilares da solução. Os botões de ação — “Participe de um evento” e “Sou organizador” — estão posicionados de forma estratégica logo abaixo do título para orientar, respectivamente, participantes à listagem pública de eventos e organizadores ao painel de gestão. O cabeçalho fixo reúne as seções Sobre, Como Funciona, Área do Participante e Contato, mantendo a navegação consistente. Todo o design é responsivo, garantindo boa usabilidade em desktop, tablets e smartphones, com foco na experiência desde o primeiro acesso.

Figura 19. Página Sobre

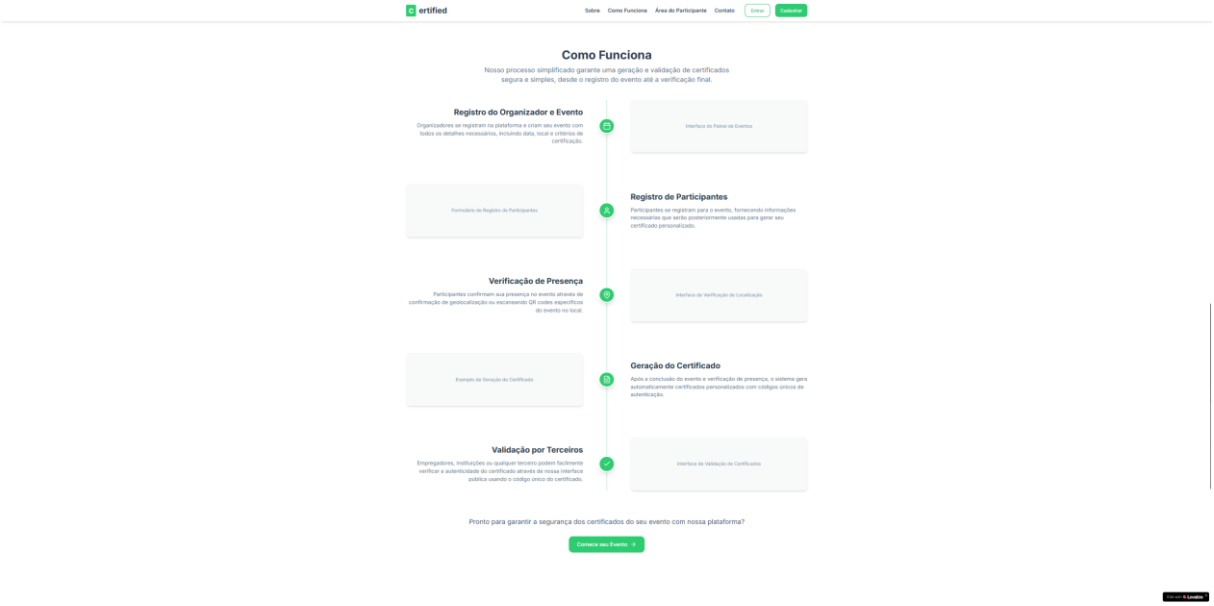


Fonte: Elaboração Própria

Na Figura 19, observa-se a seção “Sobre o Certified”, que tem como objetivo apresentar de forma clara e objetiva os diferenciais tecnológicos e conceituais da plataforma. Essa seção destaca os pilares que fundamentam a proposta do projeto, como a validação por QR Code, verificação de presença por geolocalização, uso de blockchain para registros imutáveis e a possibilidade de validação pública de certificados. Cada funcionalidade é exibida em blocos individuais, com ícones intuitivos e textos explicativos, facilitando a compreensão por parte do usuário. Abaixo desses elementos, a plataforma enfatiza seu caráter acadêmico e experimental, mencionando sua origem como projeto de TCC em Engenharia da Computação, além de apresentar os principais compromissos com segurança e conformidade legal, como a aderência à Lei Geral de Proteção de Dados (LGPD) e a utilização de criptografia

ponta a ponta. O layout limpo e bem distribuído reforça o compromisso da plataforma com a transparência e a inovação.

Figura 20. Página Como Funciona



Fonte: Elaboração Própria

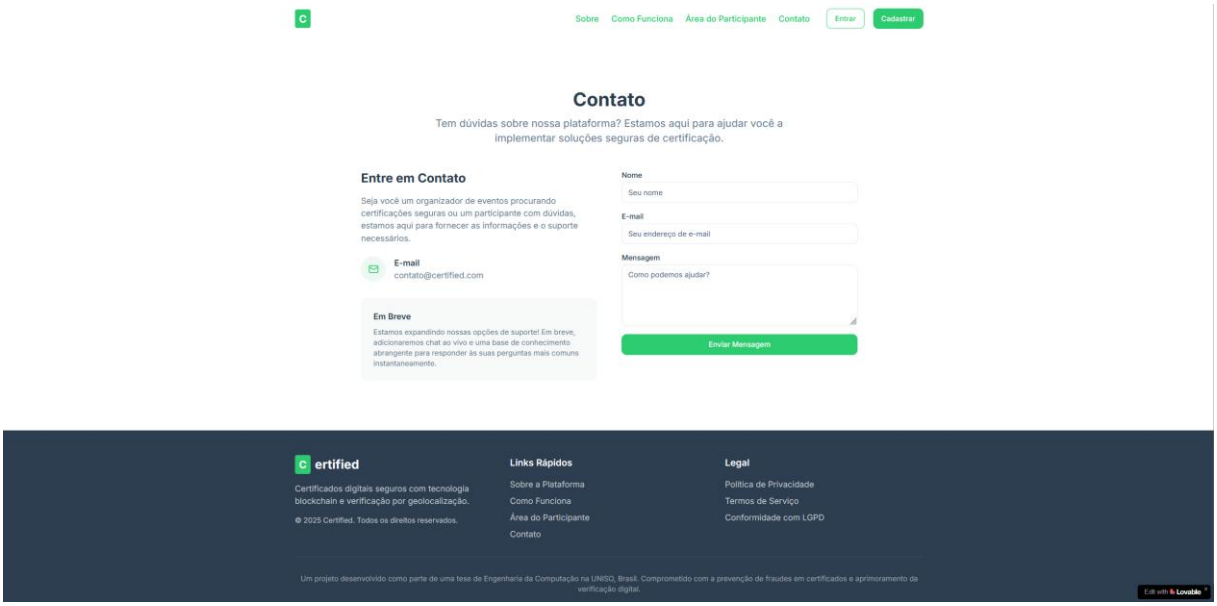
Na Figura 20, visualiza-se a seção “Como Funciona”, que apresenta de maneira sequencial e organizada as principais etapas do processo de certificação digital proposto pela plataforma Certified. Estruturada em formato de linha do tempo vertical, essa seção permite ao usuário compreender facilmente o fluxo completo, desde o registro do organizador até a verificação do certificado por terceiros. A primeira etapa mostra o registro do organizador e do evento, onde são definidos os critérios, local, data e outras informações relevantes. Em seguida, destaca-se o registro de participantes, com coleta dos dados necessários para geração personalizada dos certificados.

Na terceira etapa, observa-se a verificação de presença, que pode ser realizada por meio de geolocalização ou escaneamento de QR Codes disponibilizados no evento, garantindo que apenas participantes efetivamente presentes tenham direito ao certificado. A geração do certificado ocorre automaticamente, com a criação de um código único de validação vinculado ao documento. Por fim, a etapa de validação por terceiros permite que instituições, empregadores ou qualquer interessado verifique a autenticidade do certificado por meio de uma interface pública de consulta.

Essa abordagem transparente e visualmente segmentada reforça a confiabilidade da solução, ao mesmo tempo em que facilita a compreensão do

processo por diferentes perfis de usuários. O uso de ícones intuitivos e descrições objetivas contribui para uma comunicação clara e acessível, alinhada com os princípios de design centrado no usuário.

Figura 21. Página Contato



Fonte: Elaboração Própria

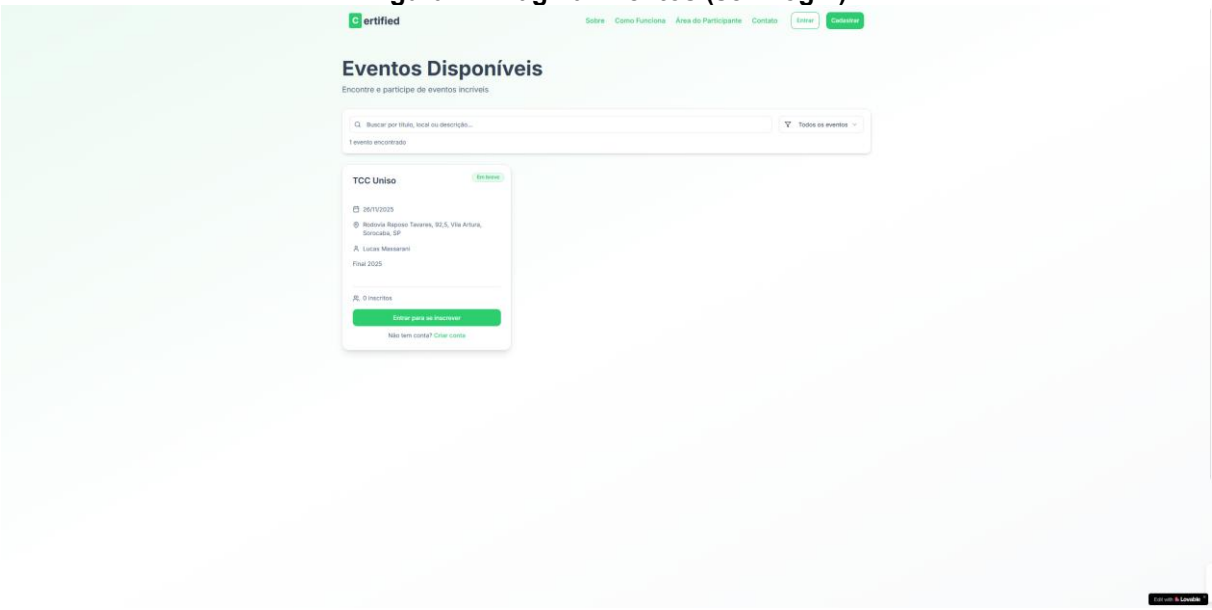
Na Figura 21, observa-se a seção “Contato”, localizada no rodapé da página inicial da plataforma Certified. Essa área foi projetada para estabelecer um canal direto de comunicação entre os usuários e os desenvolvedores da plataforma, reforçando o compromisso com o suporte e a transparência. À esquerda, encontra-se um texto introdutório que orienta o usuário sobre as formas de contato, incluindo um endereço de e-mail institucional (contato@certified.com). Logo abaixo, destaca-se um aviso de que novas funcionalidades de suporte — como chat ao vivo — estão em desenvolvimento, o que demonstra a intenção de evolução contínua do sistema.

À direita da seção, há um formulário simples e funcional com campos para nome, e-mail e mensagem. Essa estrutura visa atender tanto organizadores de eventos quanto participantes, permitindo que enviem dúvidas, sugestões ou relatem problemas de forma prática. O botão “Enviar Mensagem”, destacado em verde, garante visibilidade e facilita a ação do usuário. O layout da seção foi desenhado com foco na simplicidade e na acessibilidade, respeitando boas práticas de usabilidade e design responsivo.

Por fim, no rodapé da plataforma, há três colunas com links rápidos, informações legais e a identidade da marca. Apesar de os links para Política de

Privacidade, Termos de Serviço e Conformidade com a LGPD ainda não estarem funcionais, sua presença já sinaliza o alinhamento do projeto com requisitos legais e práticas modernas de proteção de dados, reforçando o compromisso com a transparência e a segurança jurídica.

Figura 22. Página Eventos (sem login)



Fonte: Elaboração Própria

Na Figura 22, observa-se a página “Eventos Disponíveis”, acessível pelo botão “Participe de um evento” na página inicial. O topo reúne título, subtítulo, barra de busca em largura total e contagem de resultados, permitindo localizar rapidamente eventos por título, local ou descrição. Os eventos são apresentados em cards verticais com badge de status (ex.: Em breve), data, endereço completo com ícone de localização, nome do organizador e breve descrição, favorecendo leitura rápida e comparação entre opções.

Para usuários deslogados, cada card exibe o CTA “Entrar para se inscrever” e, abaixo, o atalho “Não tem conta? Criar conta”, incentivando a conversão sem fricção. O layout segue a identidade visual da plataforma, com espaçamentos consistentes, tipografia legível e componentes responsivos, garantindo boa experiência tanto em telas amplas quanto em dispositivos móveis, além de manter escalabilidade para inclusão de novos eventos sem perder a coerência estética e funcional.

Atualmente, a página está plenamente integrada ao banco de dados por meio do Supabase, o que permite a exibição dinâmica de eventos cadastrados por organizadores. O fluxo de inscrição foi implementado com envio automatizado de e-

mails para confirmação, o que amplia a funcionalidade da plataforma e proporciona uma experiência mais próxima de um ambiente de produção. Essa evolução marca a transição de um protótipo estático para uma aplicação funcional, consolidando a proposta do sistema.

A relevância de um bom design de interface se justifica não apenas pela estética, mas sobretudo pela sua influência direta na experiência do usuário. Conforme destaca a empresa Devintec, a organização visual das informações e a fluidez da navegação são elementos determinantes para a confiança do usuário e para a eficiência na interação com sistemas web (DEVINTEC, 2023).

Em complemento, a responsividade do layout representa uma exigência fundamental, dado o crescimento do acesso a plataformas digitais por meio de dispositivos móveis. De acordo com Sites Recife, a adaptação da interface a diferentes tamanhos de tela não apenas amplia o alcance do sistema, como também assegura uma experiência de uso mais consistente e inclusiva para todos os perfis de usuários (SITES RECIFE, 2023).

Adicionalmente, a estrutura atual do formulário de contato serve como base para futuras integrações com recursos mais avançados, como APIs de atendimento ou chatbots. Segundo a agência Techlise, a adoção de princípios de usabilidade e design centrado no usuário não apenas melhora a experiência imediata do público, como também contribui para a escalabilidade da solução e sua integração com novas tecnologias (TECHLISE, 2023).

Dessa forma, conclui-se que a atenção à experiência do usuário por meio de um layout funcional e acessível não é um mero detalhe técnico, mas uma estratégia essencial para a efetividade e credibilidade de uma plataforma digital voltada à emissão segura de certificados.

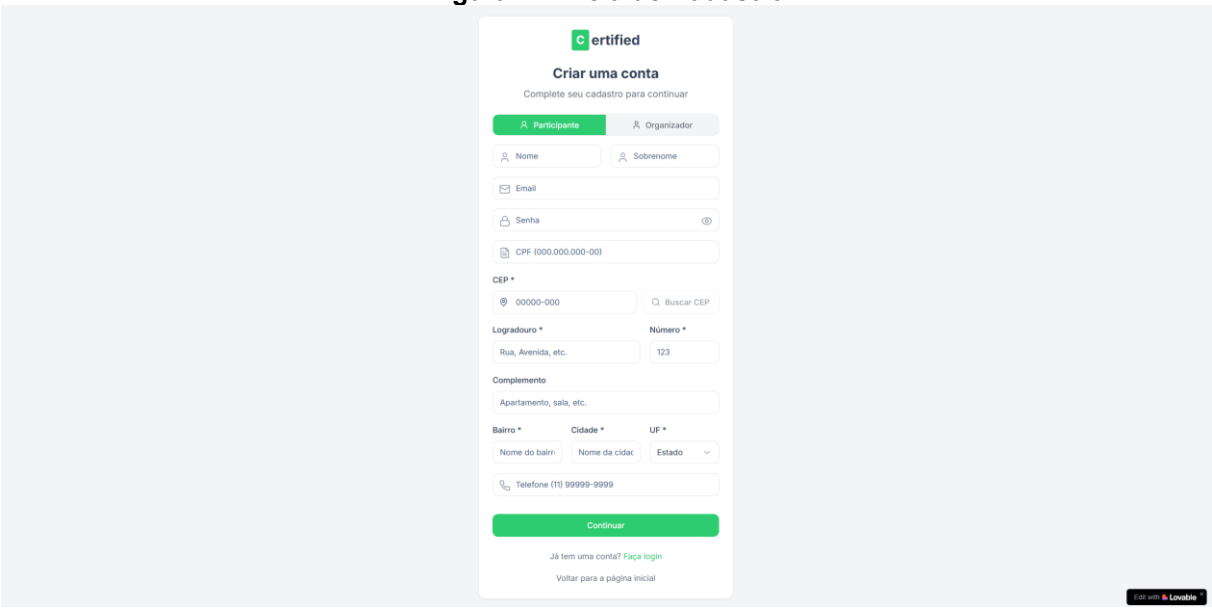
Figura 23 - Tela de Login

Fonte: Elaboração Própria

Na Figura 23, apresenta-se a tela de login da plataforma Certified, acessível a partir dos fluxos de entrada do usuário. O layout é minimalista e direto, com campos de e-mail e senha, botão principal “Entrar”, opção “Lembrar-me” para persistência de sessão e atalho “Esqueceu sua senha?” para recuperação de credenciais. A hierarquia visual destaca os elementos de ação e reduz distrações, facilitando o preenchimento rápido e seguro.

A interface é responsiva e mantém legibilidade em diferentes resoluções (desktop, tablet e mobile), com espaçamento consistente e ícones de apoio nos campos. Abaixo do formulário, há o convite “Não tem uma conta? Cadastre-se”, direcionando novos usuários ao registro. O conjunto reforça uma experiência clara e eficiente, alinhada à identidade visual da plataforma.

Figura 24 - Tela de Cadastro

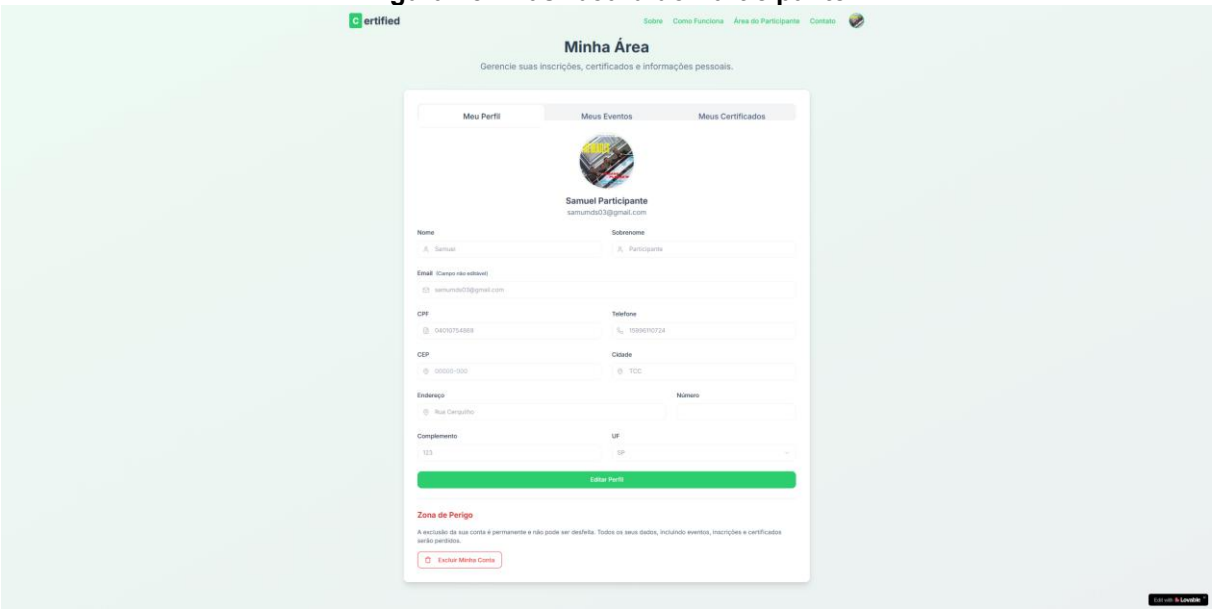


Fonte: Elaboração Própria

Na Figura 24, apresenta-se a tela de cadastro com duas abas de perfil (Participante e Organizador), mantendo um layout limpo e hierarquia visual clara. O formulário destaca campos básicos de identificação (nome, sobrenome, e-mail, senha) com ícones de apoio e opção de visualizar a senha, além do botão principal “Continuar” em evidência. A navegação secundária traz o atalho “Faça login” para quem já possui conta e o link para voltar à página inicial, preservando a fluidez do fluxo em desktop e mobile.

A versão atual incorpora campos estruturados para CPF, CEP, logradouro, número, complemento, bairro, cidade, UF e telefone, todos com máscaras de entrada para padronização (CPF, CEP e telefone). O CEP conta com o botão “Buscar CEP”, que consulta um serviço de endereços (ex.: ViaCEP) e preenche automaticamente logradouro, bairro, cidade e UF, reduzindo erros e acelerando o cadastro. Os dados passam por validações imediatas no front-end, com mensagens de ajuda e estados de erro/sucesso, garantindo consistência antes do envio ao back-end.

Figura 25 - Dashboard do Participante



Fonte: Elaboração Própria

Na Figura 25, o dashboard do participante (Minha Área) foi reorganizado para privilegiar segurança e consistência dos dados. Todos os campos permanecem em modo leitura por padrão — reduzindo o risco de alterações acidentais — e só podem ser modificados após o clique em “Editar Perfil”. Nessa transição, os inputs são habilitados e surge o botão “Salvar alterações”, deixando explícito o estado de edição e o fluxo de confirmação.

A foto de perfil passou a contar com um fluxo dedicado: o aviso “clique na câmera para alterar a foto” só aparece quando o usuário está no modo de edição. Há validação de tamanho (até 2 MB) e de formato de arquivo, com pré-visualização imediata; em caso de falha, uma mensagem de erro orienta a correção. Quando não há imagem, um avatar padrão é exibido, preservando a identidade visual da plataforma.

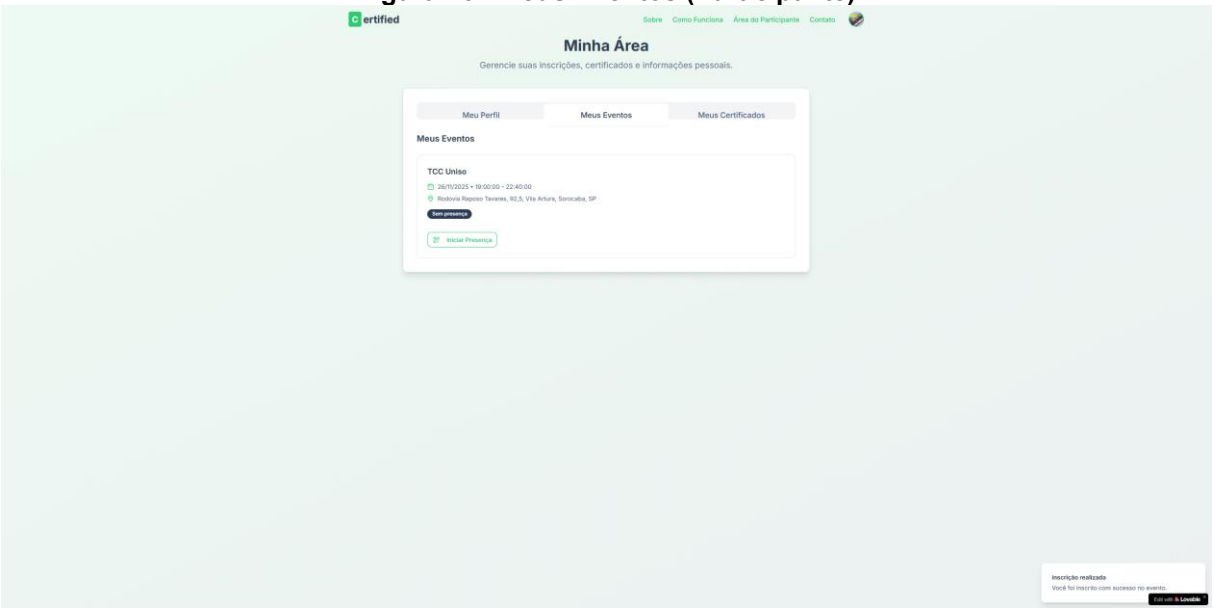
Para reforçar a integridade da conta, o e-mail permanece não editável. Demais campos (nome, sobrenome, CPF, telefone, CEP, endereço, número, complemento, cidade e UF) utilizam máscaras e validações em tempo real, evitando formatações inválidas e aumentando a qualidade do cadastro. Quando o CEP é ajustado, o endereço pode ser preenchido automaticamente, acelerando a atualização com menos digitação.

A navegação está segmentada em abas — Meu Perfil, Meus Eventos e Meus Certificados — permitindo ao participante alternar rapidamente entre dados pessoais, inscrições e documentos emitidos. Estados de carregamento, sucesso e erro são

comunicados por toasts e mensagens inline, oferecendo feedback imediato e transparente em todas as ações.

Do ponto de vista de UX e acessibilidade, o layout é responsivo, com tipografia legível, contraste adequado e elementos clicáveis com áreas generosas. Atalhos de teclado no modal de confirmação (quando aplicável) e rótulos aria-label melhoram a experiência para leitores de tela. Essa estrutura cria base sólida para evoluções futuras (p. ex., preferências de notificação, histórico de alterações e autenticação em duas etapas) sem comprometer a simplicidade do uso diário.

Figura 26 - Meus Eventos (Participante)

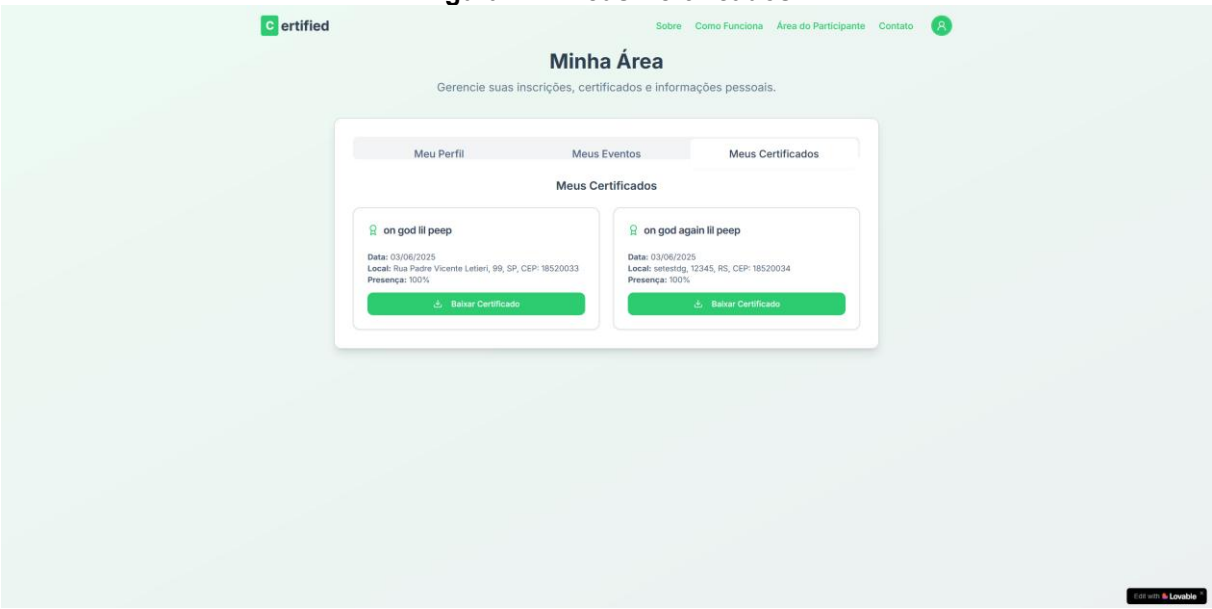


Fonte: Elaboração Própria

Na Figura 26, a aba “Meus Eventos” da Minha Área apresenta os eventos em que o participante está inscrito em cards limpos e legíveis. Cada card destaca o título do evento, a data e janela de horário com ícone de calendário, e o endereço completo com ícone de localização, mantendo a identidade visual da plataforma e a leitura rápida das informações essenciais.

Abaixo dos dados do evento, um badge de status informa a situação da presença (ex.: “Sem presença”) e um CTA contextual “Iniciar Presença” (com ícone de QR) permite iniciar o processo de validação diretamente do card. O layout é responsivo, prioriza espaçamentos confortáveis e oferece um fluxo objetivo: visualizar informações-chave e acionar a conferência de presença em um único clique, sem navegar para outras páginas.

Figura 27 - Meus Certificados



Fonte: Elaboração Própria

Figura 28 - Visualização do Certificado

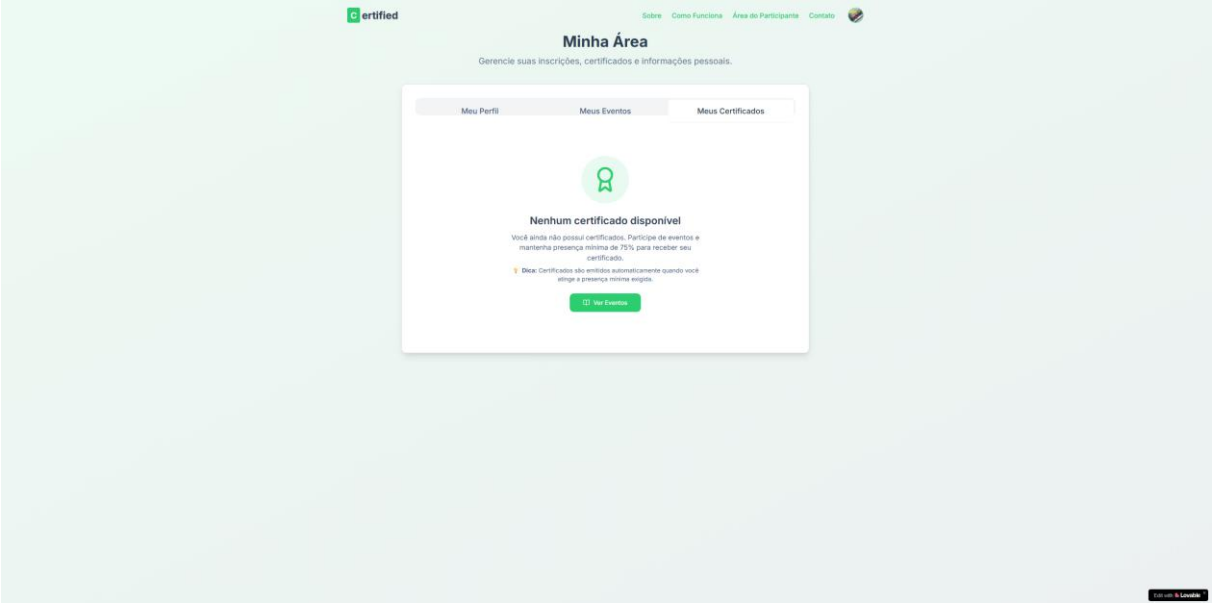
Fonte: Elaboração Própria

Com base nas Figuras 27 e 28, observa-se a seção "Meus Certificados", acessível na área do participante após o login. Nesta página, a plataforma Certified lista de forma clara os certificados disponíveis, organizados em cartões individuais contendo o nome do evento, a data de realização, o local e a porcentagem de presença registrada. Essa estrutura permite que o usuário identifique com facilidade os certificados já emitidos, promovendo uma experiência de navegação intuitiva e eficiente.

A principal ação disponível nessa seção é o botão “Baixar Certificado”, posicionado de maneira centralizada e destacado com um ícone representativo. Com apenas um clique, o participante pode realizar o download do documento em formato PDF, o que garante acessibilidade e praticidade no armazenamento e compartilhamento do certificado. A remoção da funcionalidade de visualização prévia em janela modal, que existia em versões anteriores, simplifica ainda mais o fluxo de uso, concentrando as ações diretamente no ato de obtenção do certificado.

O layout da seção mantém a consistência visual da plataforma, com cores suaves, tipografia clara e espaçamento adequado entre os elementos. Esse cuidado com o design reforça a proposta de proporcionar uma solução digital não apenas segura e funcional, mas também agradável e inclusiva para todos os perfis de usuários.

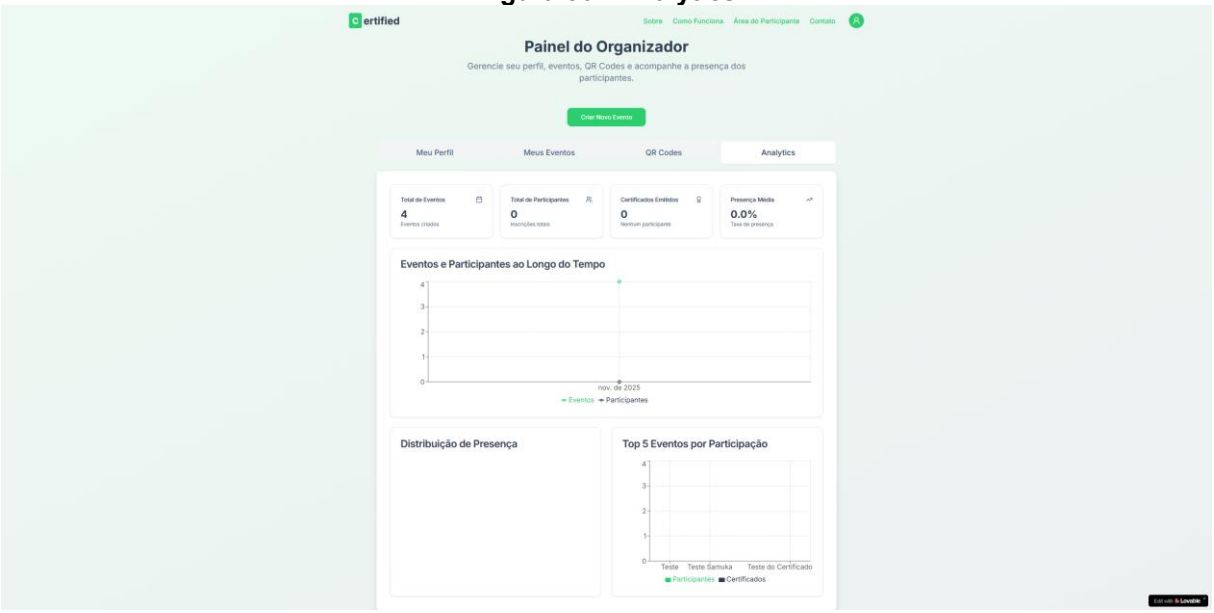
Figura 29 - Nenhum Certificado Disponível



Fonte: Elaboração Própria

Na Figura 29, observa-se a visualização da seção “Meus Certificados” quando o participante ainda não possui certificados disponíveis para download. A interface apresenta uma mensagem informativa e um ícone ilustrativo no centro da tela, indicando que nenhum certificado foi gerado até o momento. Abaixo da mensagem principal, há um aviso adicional explicando que os certificados só ficam disponíveis após o participante atingir 75% de presença no evento.

Figura 30 - Analytics



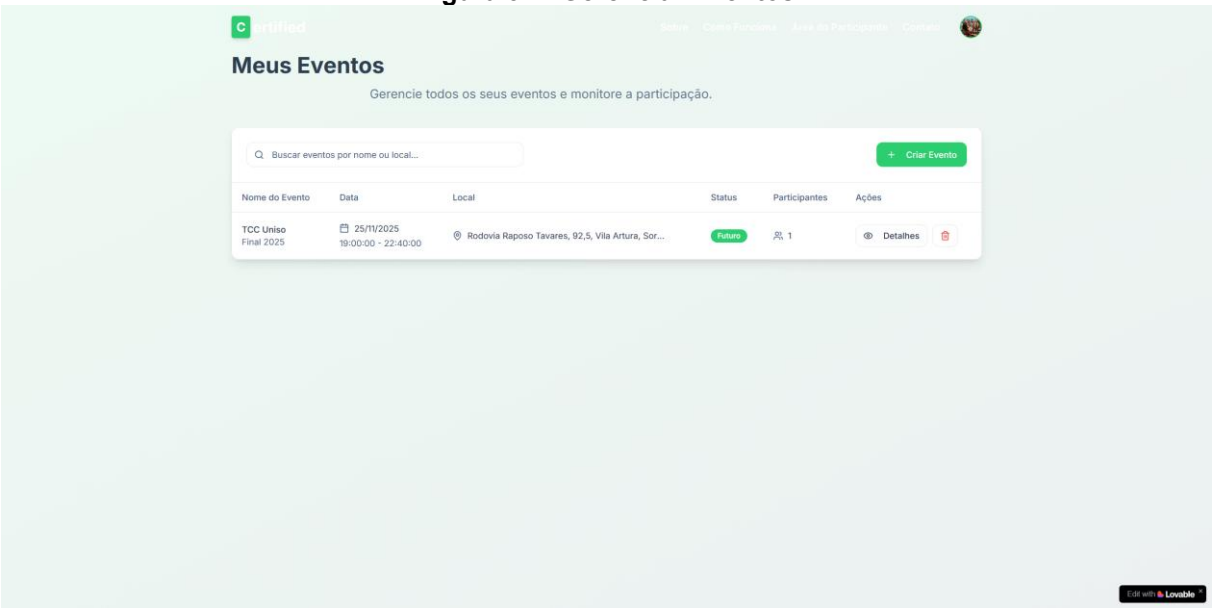
Fonte: Elaboração Própria

A página de Analytics do painel do organizador consolida indicadores operacionais e de engajamento em uma visão única e de leitura rápida. No topo, cartões-resumo apresentam Total de Eventos, Total de Participantes, Certificados Emitidos e Presença Média, oferecendo um panorama imediato da operação.

Em seguida, um gráfico temporal mostra a evolução de eventos e participantes ao longo do tempo, útil para acompanhar sazonalidade e impacto de ações de divulgação. Painéis complementares exibem a distribuição de presença (para identificar concentração de ausências/presenças) e o Top 5 eventos por participação, comparando visualmente inscritos/participantes e certificados emitidos.

A interface foi construída com estados “vazios” informativos (quando não há dados), hierarquia visual consistente e responsividade, priorizando compreensão rápida e suporte à decisão—como priorizar eventos com baixa adesão, ajustar comunicação e medir a efetividade da certificação ao longo das edições.

Figura 31 - Gerenciar Eventos

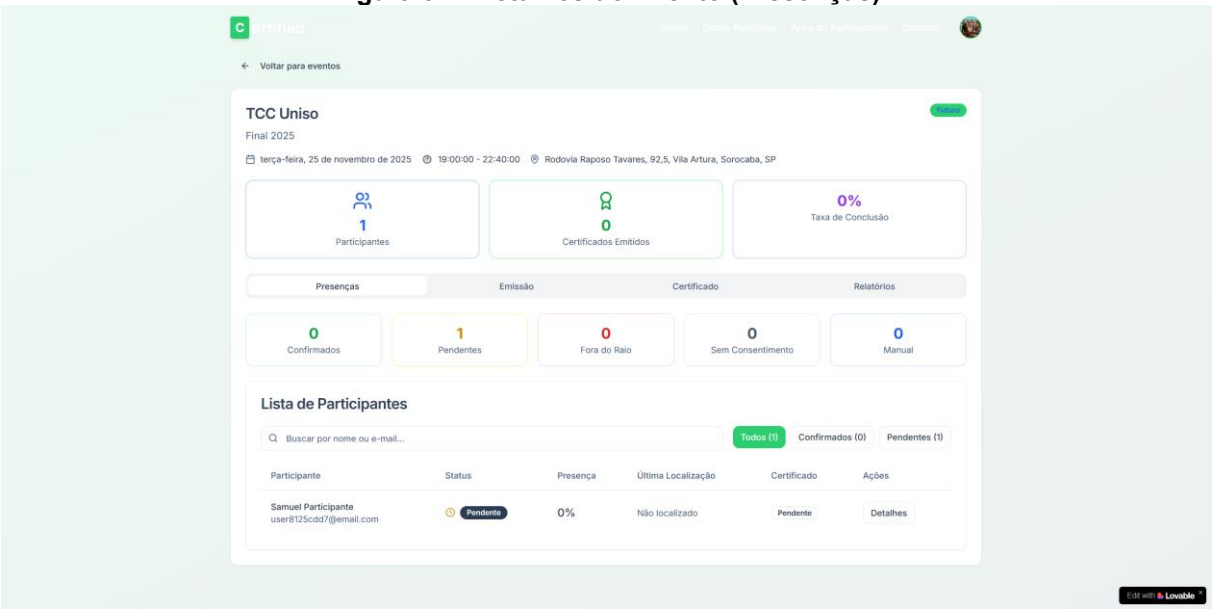


Fonte: Elaboração Própria

Na Figura 31, a página “Meus Eventos” do organizador lista todos os eventos em uma tabela com busca no topo e o atalho “Criar Evento”. Cada linha exibe Nome do Evento (com subtítulo), Data (data e janela de horário), Local (endereço resumido com ícone), Status (badge, p.ex. Futuro), Participantes (ícone + contagem) e Ações. O fluxo foi simplificado para consulta rápida e manutenção contínua do portfólio de eventos.

As ações por evento ficam concentradas em dois botões: “Detalhes” (ícone de visualização), que abre a página completa do evento com informações estendidas e operações adicionais (como gerenciamento e materiais), e excluir (ícone de lixeira), com confirmação antes da remoção definitiva. Assim, a tela equilibra visão geral ágil e acesso aprofundado — os detalhes completos do evento só são exibidos após clicar em “Detalhes”.

Figura 32 - Detalhes do Evento (Presenças)



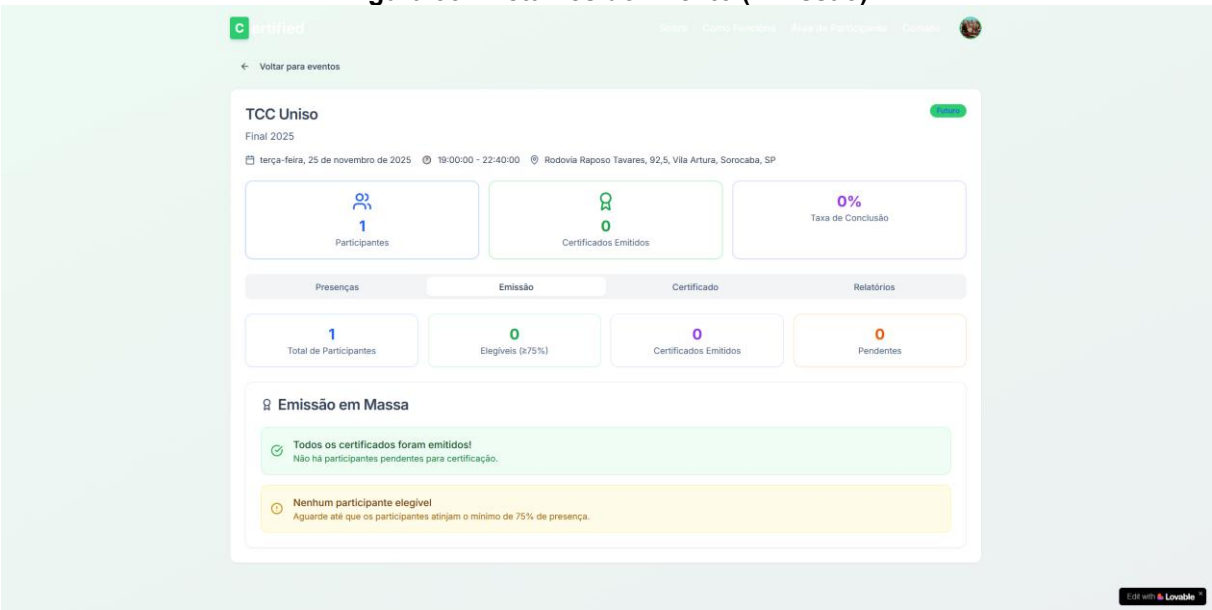
Fonte: Elaboração Própria

Na tela de Detalhes do Evento, o cabeçalho traz um resumo executivo com título do evento, subtítulo (ex.: trilha/tema), data (com dia da semana), janela de horário e endereço completo, acompanhados de ícones para leitura rápida e um badge de status (ex.: Futuro). Abaixo, três cartões-síntese exibem Participantes, Certificados Emitidos e Taxa de Conclusão (%), permitindo ao organizador avaliar, de imediato, o tamanho do público, o progresso de emissão e a efetividade geral.

Logo depois, a página organiza as operações por abas funcionais — Presenças, Emissão, Certificado e Relatórios. No contexto de Presenças, aparecem indicadores em cartões com contagens por categoria: Confirmados, Pendentes, Fora do Raio (quando há geolocalização ativa), Sem Consentimento e Manual. Esses painéis ajudam a identificar gargalos (p. ex., muitos pendentes ou fora do raio) e orientar ações corretivas durante o evento, além de refletirem as regras de validação configuradas (raio, tolerâncias, etc.).

Por fim, a Lista de Participantes apresenta um buscador por nome/e-mail, filtros rápidos (Todos, Confirmados, Pendentes) e uma tabela com colunas para Participante, Status (com badge), Presença (% acumulado), Última Localização (quando aplicável), Certificado (estado atual) e Ações (ex.: Detalhes para inspeção individual). Esse grid é o centro operacional do organizador: permite acompanhar quem já validou presença, quem ainda precisa de intervenção e o estágio de certificação, mantendo o controle do evento em tempo real com navegação simples e responsiva.

Figura 33 - Detalhes do Evento (Emissão)

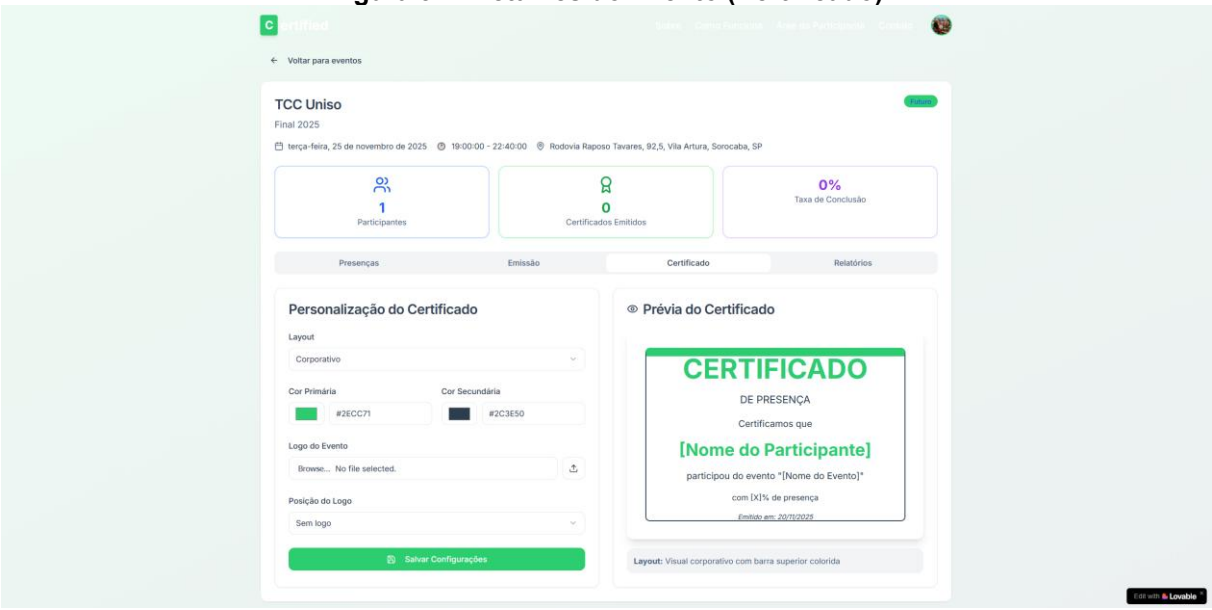


Fonte: Elaboração Própria

A aba Emissão organiza o fluxo de certificação por elegibilidade, deixando explícito quantos inscritos atingiram o limiar de presença (≥75%), quantos já foram certificados e quantos permanecem pendentes. Os cards-resumo funcionam como “marcadores de prontidão” para a ação de emitir, evitando tentativas quando não há participantes elegíveis ou quando tudo já foi concluído.

A seção “Emissão em Massa” padroniza boas práticas: exibe mensagens de estado (sucesso, atenção) e bloqueia/habilita botões conforme regras de negócio. Isso minimiza erros operacionais, garante rastreabilidade e encurta o ciclo entre o fechamento do evento e a disponibilização dos certificados, mantendo o processo claro para o organizador.

Figura 34 - Detalhes do Evento (Certificado)

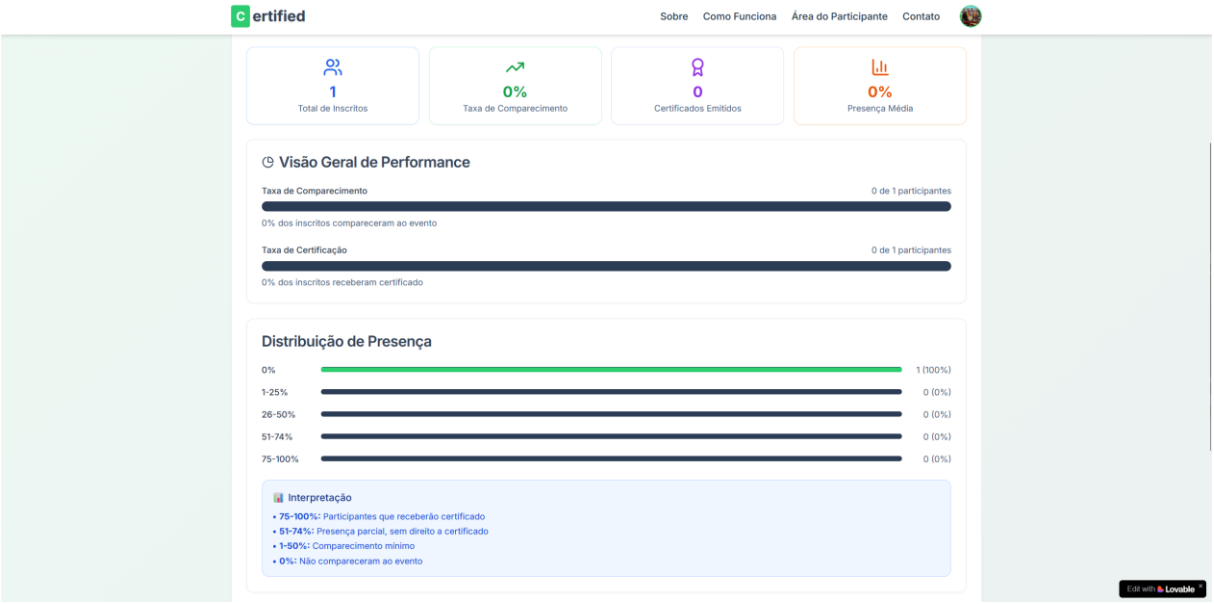


Fonte: Elaboração Própria

Na aba Certificado, o organizador personaliza o documento de forma visual e orientada. É possível escolher o layout (p.ex., “Corporativo”), definir cores primária e secundária com picker e hex, anexar o logotipo e posicioná-lo conforme a identidade do evento. A pré-visualização do certificado ao lado reflete as alterações em tempo real, reduzindo tentativa e erro e assegurando consistência estética.

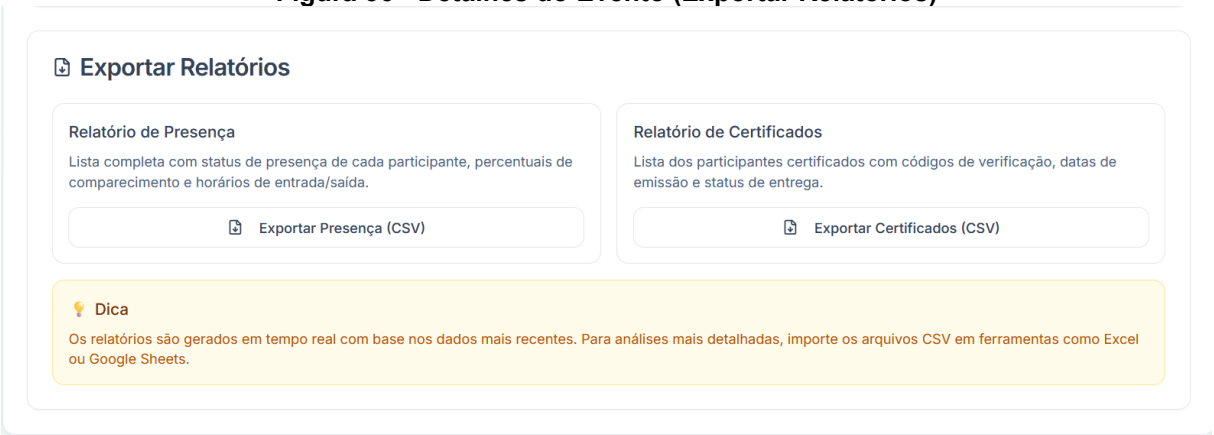
Além do ganho de eficiência, a separação entre configuração (à esquerda) e prévia (à direita) ajuda a validar contraste, hierarquia tipográfica e legibilidade de campos dinâmicos (nome do participante, evento, data, percentual de presença). O botão “Salvar Configurações” versiona as preferências do evento, garantindo que a emissão posterior reproduza exatamente o padrão aprovado.

Figura 35 - Detalhes do Evento (Relatórios)



Fonte: Elaboração Própria

Figura 36 - Detalhes do Evento (Exportar Relatórios)



Fonte: Elaboração Própria

A seção de Visão Geral de Performance apresenta os indicadores principais do evento em cartões de fácil leitura — total de inscritos, taxa de comparecimento, certificados emitidos e presença média. Logo abaixo, barras de progresso resumem o andamento do evento, permitindo perceber rapidamente, por exemplo, quantos participantes já compareceram e quantos receberam certificação, sempre com contagem absoluta e percentual.

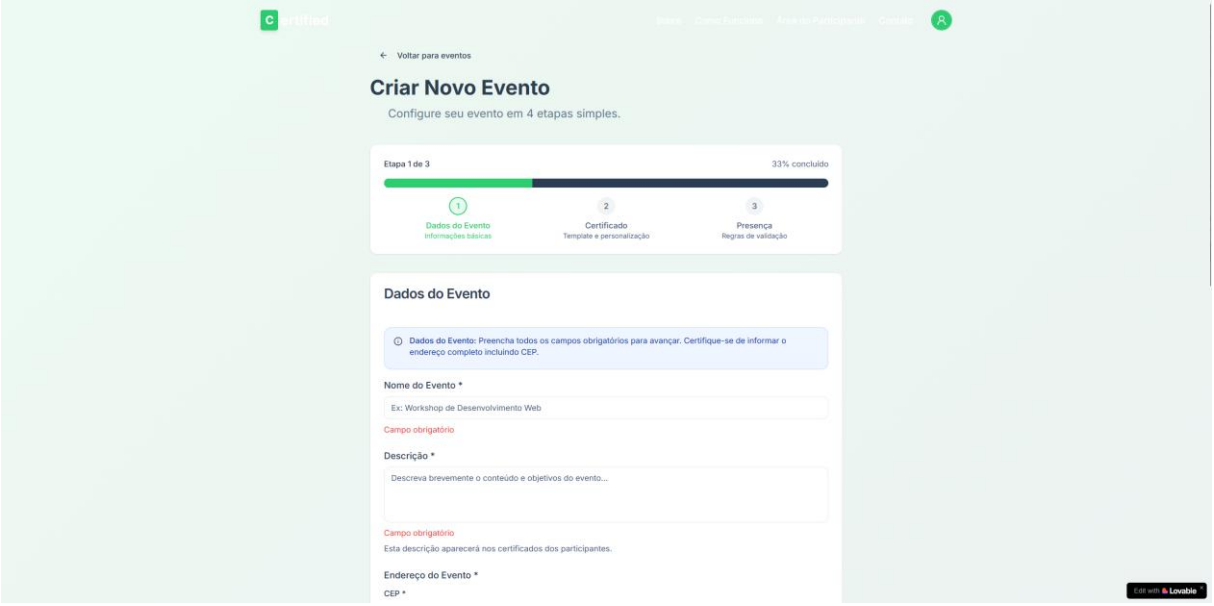
Em seguida, a Distribuição de Presença detalha como os participantes se distribuem por faixas (0%, 1–25%, 26–50%, 51–74% e 75–100%). Esse gráfico ajuda o organizador a identificar gargalos de presença e a tomar decisões práticas (como reforçar comunicação ou ajustar regras). A legenda interpretativa complementa a

leitura: quem está em 75–100% tende a ser elegível ao certificado; entre 51–74% tem presença parcial; e abaixo disso, o comparecimento é mínimo ou inexistente.

A área de Exportar Relatórios oferece dois downloads em CSV: o Relatório de Presença, com status individual, percentuais e janelas de entrada/saída; e o Relatório de Certificados, com códigos de verificação, datas de emissão e status de entrega. Esses arquivos permitem auditoria e acompanhamento detalhado fora da plataforma, mantendo rastreabilidade das ações.

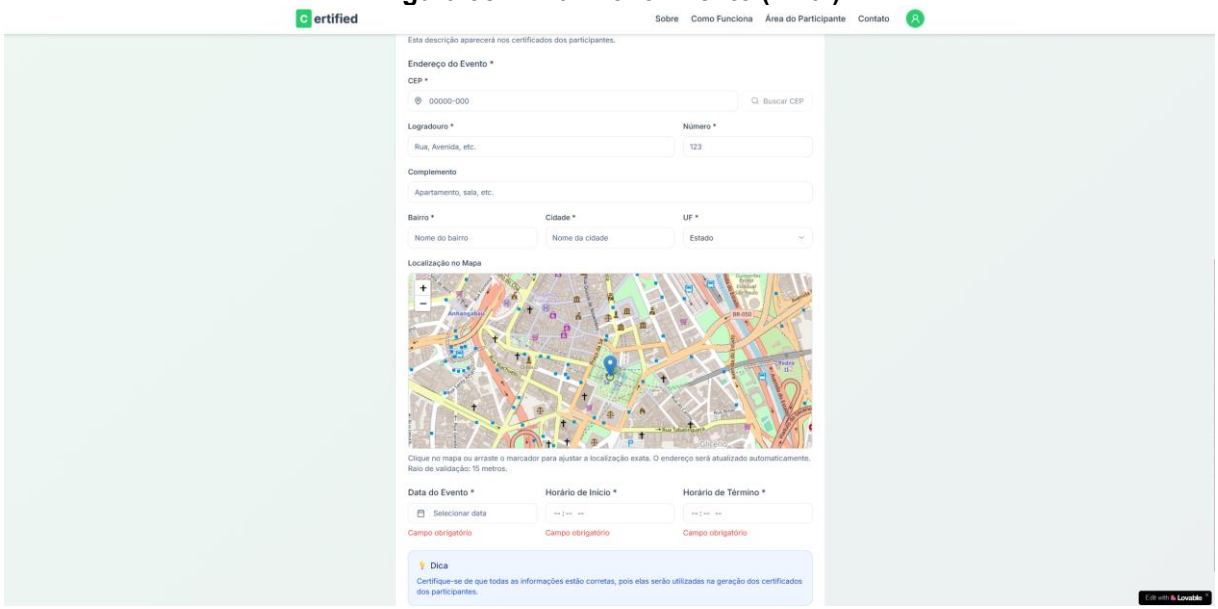
Por fim, a plataforma reforça uma dica operacional: os relatórios são gerados em tempo real e pensados para análises posteriores em ferramentas como Excel ou Google Sheets. Dessa forma, o organizador pode cruzar dados, criar painéis personalizados e acompanhar a evolução dos indicadores com mais profundidade, sem perder a consistência com o que está sendo monitorado na interface.

Figura 37 - Criar Novo Evento



Fonte: Elaboração Própria

Figura 38 - Criar Novo Evento (Final)



Fonte: Elaboração Própria

A tela de "Criar Novo Evento", apresentada nas Figuras 37 e 38, é destinada exclusivamente aos usuários com perfil de organizador. Nessa interface, é possível cadastrar eventos inserindo informações essenciais como título, descrição, data, horário de início e término, local e critérios de certificação. A estrutura do formulário é clara e objetiva, com campos bem delimitados e instruções auxiliares que orientam o preenchimento correto, facilitando o uso mesmo para usuários com menor familiaridade com ferramentas digitais. O layout da página permanece coerente com a identidade visual da plataforma, priorizando a simplicidade e a usabilidade.

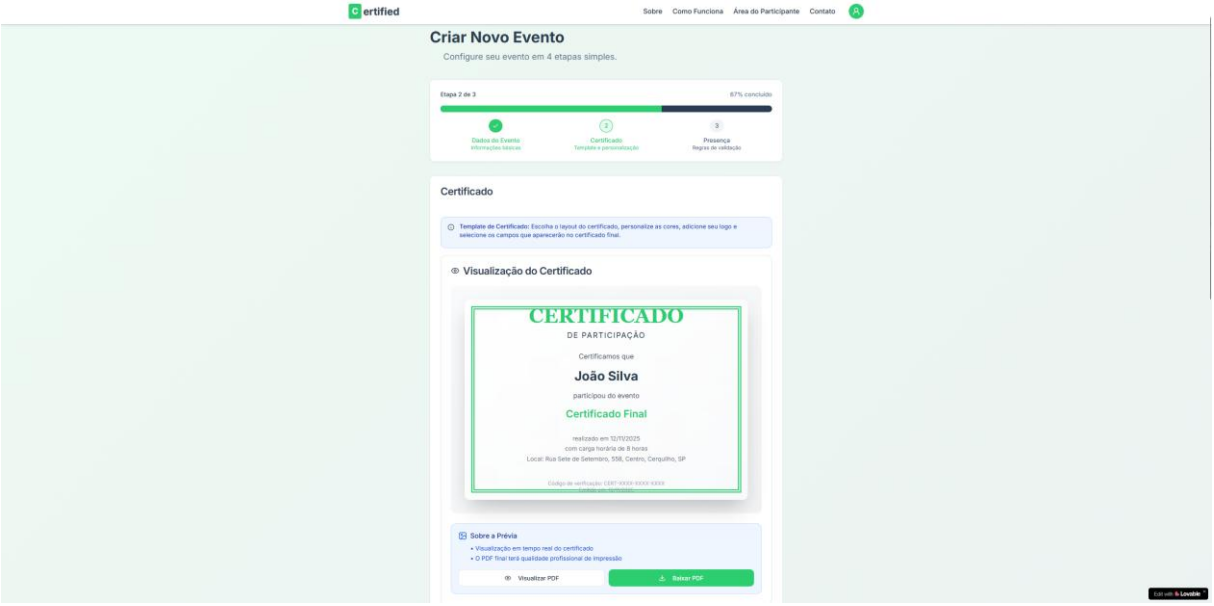
A parte inferior do formulário inclui um bloco informativo com os critérios automáticos de certificação definidos pela plataforma, como presença mínima de 75% do tempo total do evento, validação por GPS em um raio de 15 metros, rastreamento ativo durante o período do evento e disponibilidade do QR Code a partir de 15 minutos antes do início. Essas informações são essenciais para garantir transparência e alinhamento com os objetivos da plataforma quanto à autenticidade da certificação.

A a tela exibe um mapa interativo (Leaflet/Mapbox/OSM) que permite definir o endereço no mapa: o organizador pode clicar ou arrastar o marcador para ajustar a localização exata do evento, e as coordenadas são salvas automaticamente.

A tela de criação de eventos passou a disponibilizar uma pré-visualização em tempo real do certificado, refletindo imediatamente as alterações de conteúdo e estilo definidas pelo organizador. Esse painel permite validar tipografia, hierarquia informacional, balanceamento de margens e destaque do código de verificação antes

da emissão. Além da visualização, a interface inclui controles para abrir a prévia em PDF e baixar o arquivo com qualidade profissional de impressão, assegurando padronização visual e redução de retrabalho gráfico entre diferentes eventos.

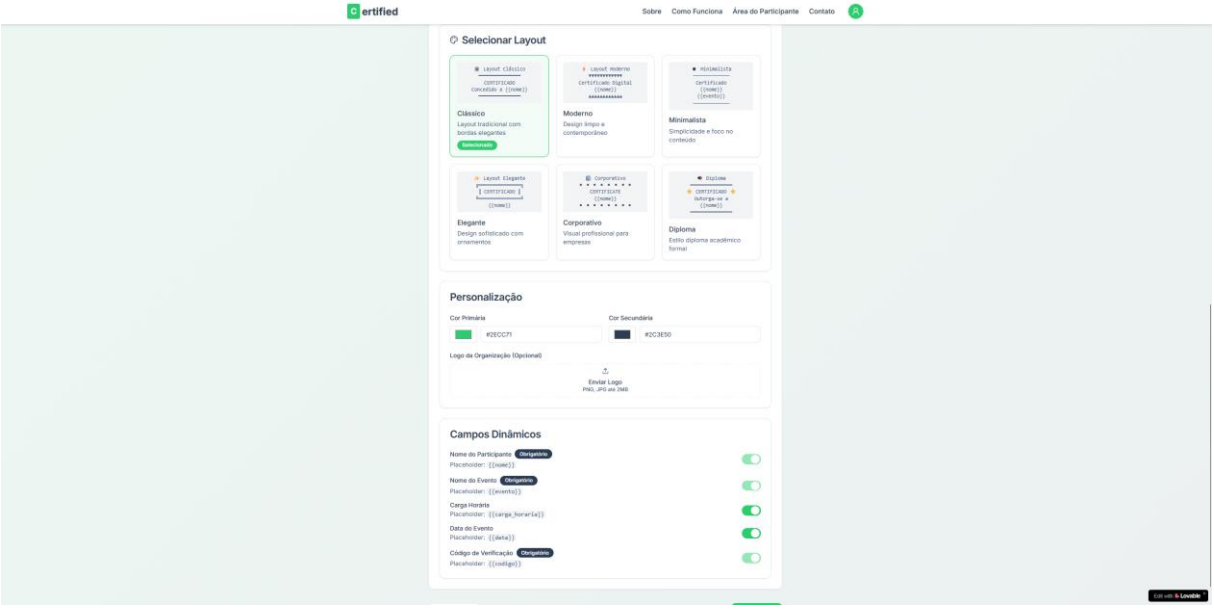
Figura 39 - Pré-visualização do certificado



Fonte: Elaboração Própria

A tela de criação de eventos passou a disponibilizar uma pré-visualização em tempo real do certificado, refletindo imediatamente as alterações de conteúdo e estilo definidas pelo organizador. Esse painel permite validar tipografia, hierarquia informacional, balanceamento de margens e destaque do código de verificação antes da emissão. Além da visualização, a interface inclui controles para abrir a prévia em PDF e baixar o arquivo com qualidade profissional de impressão, assegurando padronização visual e redução de retrabalho gráfico entre diferentes eventos.

Figura 40 - Layout e personalização

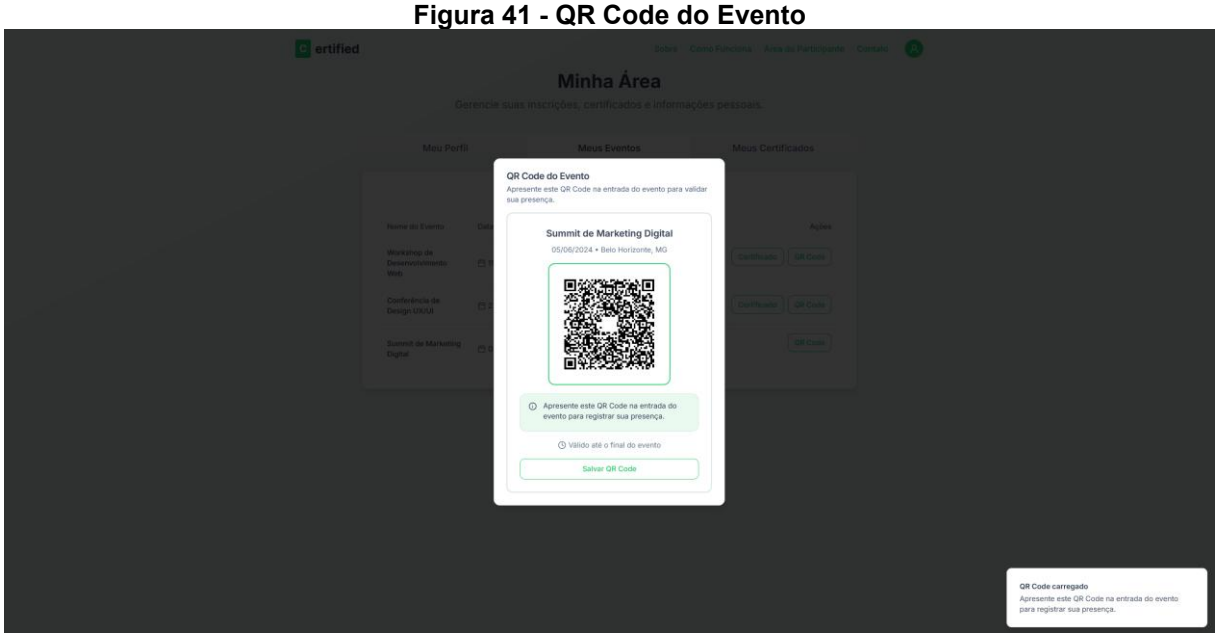


Fonte: Elaboração Própria

O módulo apresenta um catálogo de modelos com seis opções — Clássico, Moderno, Minimalista, Elegante, Corporativo e Diploma — cada uma acompanhada de miniatura, descrição e rótulo de seleção ativa. Essa organização facilita a escolha de um estilo coerente com a identidade do evento (ex.: linguagem acadêmica, institucional ou promocional), preservando consistência estética entre turmas e edições. A seleção do layout atua como base estrutural do documento, sobre a qual incidem as demais customizações (cores, logomarca e campos), garantindo previsibilidade no resultado final.

Após selecionar o layout, o organizador ajusta cores institucionais (primária e secundária por código hexadecimal), inclui a logomarca (PNG/JPG até 2 MB) e define os campos dinâmicos que comporão o certificado: nome do participante ({{nome}}), nome do evento ({{evento}}), carga horária ({{carga_horaria}}), data ({{data}}) e código de verificação ({{codigo}}). Os campos obrigatórios são indicados na interface e as alterações são refletidas instantaneamente na pré-visualização, reduzindo erros de digitação e garantindo conformidade com os requisitos de validação pública. Esse fluxo de customização acelera a emissão em escala, preserva a identidade visual da organização e integra, de forma transparente, a camada de autenticação do documento (código/QR) ao template final.

Figura 41 - QR Code do Evento



Fonte: Elaboração Própria

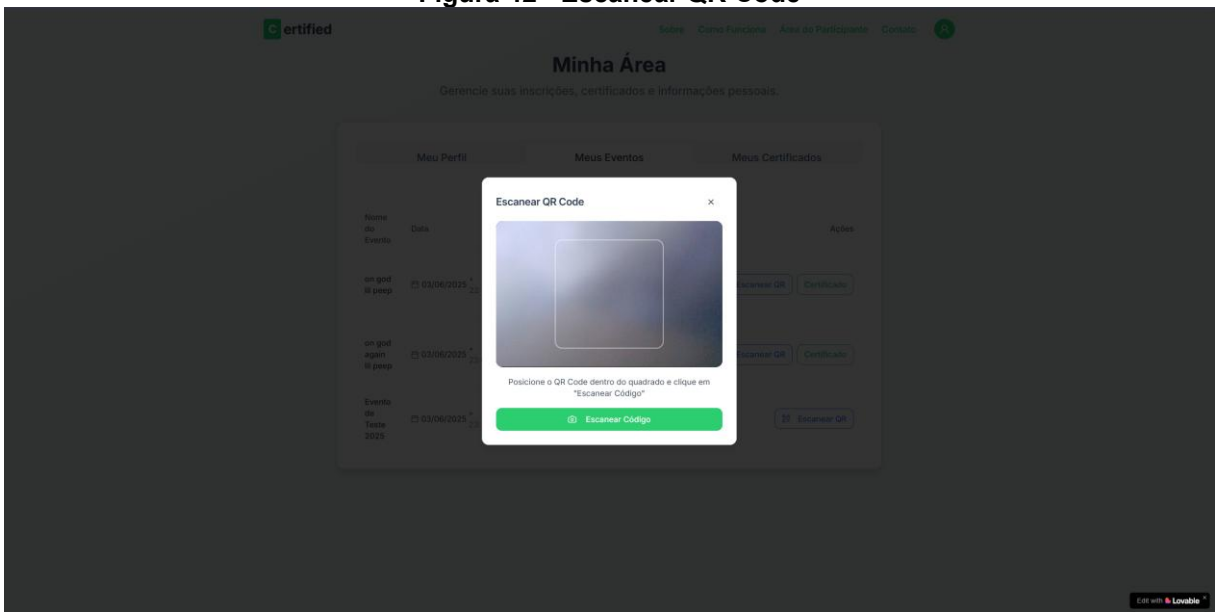
Na Figura 41, observa-se a funcionalidade de geração e exibição de QR Codes vinculados aos eventos criados por organizadores na plataforma Certified. Essa ferramenta tem como principal objetivo facilitar o controle de presença dos participantes nos eventos, promovendo segurança e automação no processo de validação. A interface exibe, de forma organizada, todos os eventos criados, acompanhados das respectivas informações — como nome, data, horário e local — e o status atual do QR Code.

No exemplo apresentado, é possível visualizar dois eventos finalizados, nos quais o sistema indica de forma clara a indisponibilidade do QR Code com a mensagem “QR Code não disponível – evento finalizado”. Essa validação automática é essencial para garantir que os códigos só estejam acessíveis no momento adequado, impedindo o uso indevido antes ou após o período programado do evento. Essa medida reforça a integridade do sistema e a confiabilidade da presença registrada.

A lógica de funcionamento foi projetada para que o QR Code permaneça visível apenas dentro de uma janela de tempo específica, geralmente iniciando 15 minutos antes do horário oficial do evento. A exibição do código é feita exclusivamente na conta do organizador, que deve disponibilizá-lo fisicamente ou em tela para que os participantes possam escaneá-lo utilizando a câmera de seus próprios dispositivos móveis. Essa abordagem visa garantir que a confirmação de presença seja feita de forma presencial, no local do evento, com base na leitura do código.

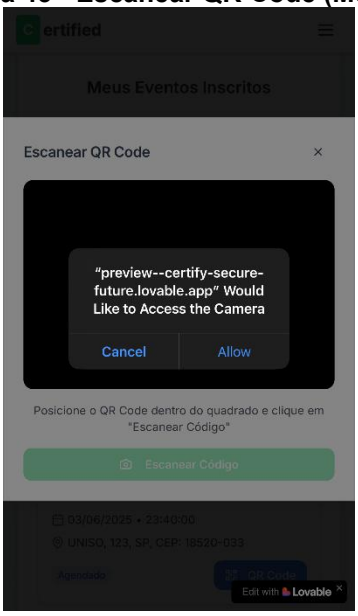
Além disso, o sistema permite que o organizador baixe ou imprima o QR Code gerado, facilitando sua exibição em ambientes com pouca conectividade ou com grandes volumes de público. A implementação dessa funcionalidade aproxima o sistema das práticas modernas adotadas em eventos presenciais e híbridos, promovendo eficiência, transparência e controle no processo de certificação de participação.

Figura 42 - Escanear QR Code



Fonte: Elaboração Própria

Figura 43 - Escanear QR Code (Mobile)



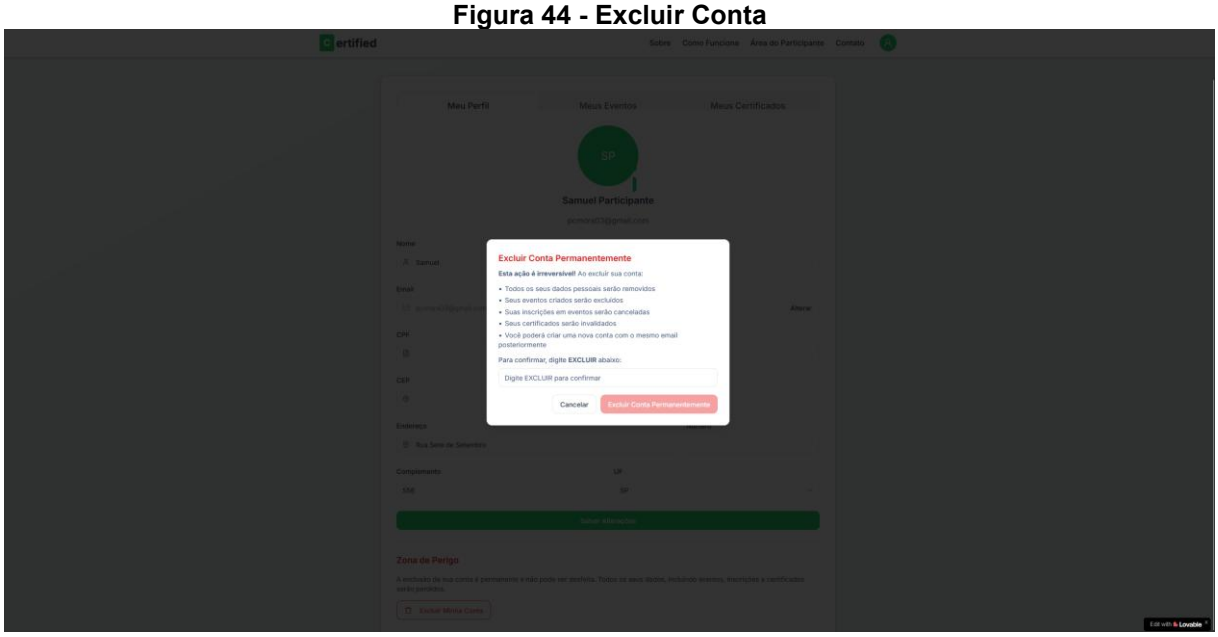
Fonte: Elaboração Própria

Nas Figura 42 e 43, observa-se o início da funcionalidade de escaneamento de QR Code para validação de presença nos eventos cadastrados na plataforma Certified. Esse recurso, acessado por meio da aba “Eventos Disponíveis” ou diretamente na “Área do Participante”, permite que o usuário utilize a câmera do seu próprio dispositivo para realizar a leitura do QR Code gerado para cada evento. O sistema, ao abrir o modal de escaneamento, solicita ao navegador a permissão de uso da câmera, o que garante a funcionalidade mesmo em dispositivos móveis. Essa abordagem proporciona uma experiência fluida e acessível, sem a necessidade de plugins adicionais.

A leitura do QR Code, neste momento, opera de forma básica, reconhecendo o código e preparando o sistema para futura integração com validações adicionais. Embora funcional, o recurso ainda não incorpora camadas de verificação avançadas, como validação cruzada em tempo real com base na geolocalização e rastreamento contínuo de presença. No entanto, essas funcionalidades mais robustas já estão previstas no escopo de melhorias da plataforma, especialmente no que diz respeito à segurança e à precisão da autenticação da presença dos participantes.

A interface do modal mantém o padrão visual da plataforma, com uma área centralizada para enquadrar o QR Code e botões de ação claros. Instruções simples orientam o participante a posicionar o código corretamente para leitura. Esse recurso representa um importante avanço na automação do controle de presença, consolidando o uso de tecnologias acessíveis e eficazes em ambientes acadêmicos e corporativos.

Figura 44 - Excluir Conta

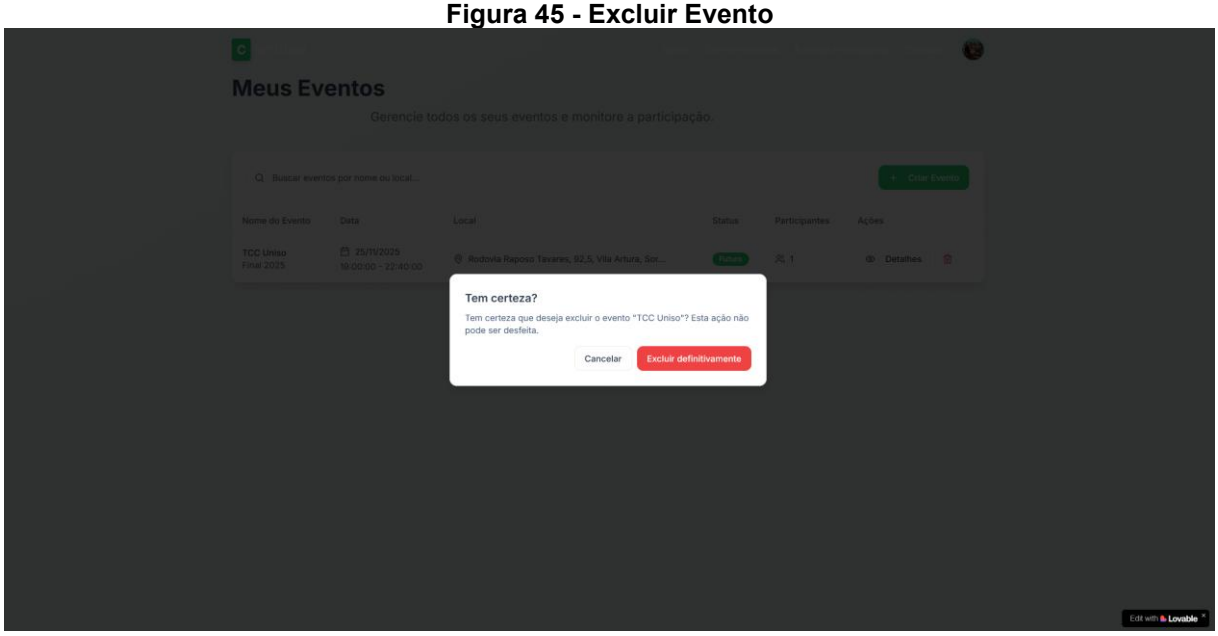


Fonte: Elaboração Própria

Observa-se na imagem 44 que foi implementada uma função de exclusão permanente de conta. Quando o usuário decide excluir sua conta, uma janela de confirmação é exibida, explicando detalhadamente as consequências da ação. A mensagem destaca que todos os dados do usuário, como informações pessoais, eventos criados, inscrições e certificados, serão excluídos, tornando a ação irreversível.

Para garantir que o usuário tenha plena consciência da ação, é solicitado que ele digite "EXCLUIR" no campo indicado para confirmar a exclusão da conta. Após essa confirmação, o botão "Excluir Conta Permanentemente" é habilitado, permitindo que o processo seja finalizado.

Figura 45 - Excluir Evento



Fonte: Elaboração Própria

Observa-se na imagem 45 que foi implementada a funcionalidade de exclusão de evento para o organizador. Quando o organizador decide excluir um evento, uma janela de confirmação aparece, detalhando as consequências dessa ação. A mensagem alerta que a exclusão é irreversível e que todos os dados relacionados ao evento, como inscrições, rastreamento e certificados, serão perdidos.

Assim como na exclusão de conta, é necessário confirmar a exclusão do evento clicando no botão "Excluir". Esse recurso garante que o organizador tenha consciência total das implicações de sua escolha, evitando ações acidentais. A interface permite que o organizador tenha controle total sobre seus eventos e facilite o processo de exclusão de maneira clara e segura.

Figura 46 - Políticas e Termos de Serviço

Fonte: Elaboração Própria

Na Figura 46, observa-se a seção "Legal", presente no rodapé da plataforma Certified, que consolida os links para as páginas de Política de Privacidade, Termos de Serviço e Conformidade com a LGPD. Esses elementos desempenham um papel essencial na garantia da transparência, ética e conformidade legal da aplicação, aspectos indispensáveis em sistemas que envolvem o tratamento de dados pessoais e a emissão de certificados digitais. Ao disponibilizar essas informações de forma acessível e clara, a plataforma demonstra seu alinhamento com a legislação vigente, especialmente com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), além de reforçar o compromisso com boas práticas de governança digital, proteção do usuário e responsabilidade jurídica em ambiente eletrônico.

Além de reforçar a conformidade legal, a presença desses links no rodapé contribui para a credibilidade da plataforma, demonstrando ao usuário que seus direitos estão resguardados e que há um compromisso institucional com a transparência. Essa prática, comum em sistemas digitais consolidados, favorece a confiança do público-alvo e atende aos princípios da responsabilidade ativa previstos na LGPD, como a necessidade de informação clara, livre acesso aos dados e possibilidade de revogação do consentimento. Tais recursos são especialmente relevantes no contexto da certificação digital, em que a manipulação e proteção de dados sensíveis são aspectos centrais para o funcionamento ético e seguro da plataforma.

Figura 47 - API de Mapas

Fonte: Elaboração Própria

A plataforma passou a incorporar um componente de mapa interativo na etapa de criação e edição de eventos, utilizando o framework Leaflet em conjunto com tiles do Mapbox e dados cartográficos do OpenStreetMap. Tecnicamente, o front-end instancia o mapa a partir de coordenadas iniciais e adiciona um marcador arrastável, permitindo que o organizador selecione visualmente o ponto exato em que o evento ocorrerá. Cada movimentação do marcador atualiza dinamicamente os valores de latitude e longitude mantidos no estado da aplicação, que são então persistidos no banco de dados e utilizados nos processos de validação de presença. O sistema também exibe o raio de validação em metros, de forma que o usuário compreenda visualmente a área de cobertura em que o check-in será considerado válido.

Para o consumo dos serviços do Mapbox, é utilizada uma chave de acesso (access_token) configurada como variável de ambiente, por exemplo NEXT_PUBLIC_MAPBOX_TOKEN. Essa chave não é inserida diretamente no código-fonte, mas fornecida ao front-end por meio das environment variables do ambiente de execução (preview e produção). Esse arranjo segue boas práticas de segurança, pois reduz a exposição da credencial em repositórios públicos e facilita a sua rotação, caso necessário. A URL do tile layer é parametrizada com essa variável de ambiente, permitindo ainda que diferentes ambientes (desenvolvimento, homologação e produção) utilizem chaves com permissões distintas. A combinação entre Leaflet, Mapbox e OpenStreetMap materializa, na interface, a lógica de geolocalização descrita no projeto: a mesma coordenada salva no momento da

criação do evento é utilizada posteriormente para comparar a posição do participante, considerando o raio de tolerância definido na configuração do evento.

Figura 48 - Preferência de Cookies

Fonte: Elaboração Própria

Foi também implementado um mecanismo de gestão de cookies e consentimento, organizado em um painel de preferências acessível ao usuário. Em vez de um aviso genérico, a interface apresenta categorias distintas de cookies, tais como estritamente necessários, funcionais, analytics, marketing e geolocalização. Os cookies estritamente necessários permanecem sempre ativos, por estarem relacionados ao funcionamento básico da plataforma (como autenticação de sessão e segurança). As demais categorias podem ser habilitadas, desabilitadas ou personalizadas pelo usuário, que dispõe de opções como “Recusar não essenciais”, “Salvar preferências” ou “Aceitar todos”.

Do ponto de vista técnico, as escolhas de consentimento são registradas em um cookie específico ou em armazenamento local (por exemplo, localStorage), na forma de um objeto que indica, para cada categoria, se o uso está autorizado. Antes da inicialização de serviços externos — como ferramentas de análise de tráfego (ex.: Google Analytics, cuja identificação também pode ser configurada por meio de variáveis de ambiente) ou pixels de marketing — o front-end consulta essas preferências e apenas carrega os scripts correspondentes quando houver consentimento expresso. No caso da categoria de geolocalização, a aplicação utiliza as configurações registradas para decidir se solicitará ou não a permissão nativa do

navegador (navigator.geolocation) durante o processo de check-in. Dessa forma, a plataforma restringe o acesso à localização do participante às situações em que existe autorização explícita, alinhando a implementação prática às exigências de transparência, minimização de dados e base legal previstas na LGPD.

As telas e fluxos descritos nesta seção refletem o estado atual do protótipo. Elementos indicados como ‘em desenvolvimento’ e funcionalidades avançadas de rastreamento permanecerão desativados na demonstração pública para preservar a segurança e a privacidade dos usuários.

5 RESULTADOS

Além das funcionalidades já descritas, é importante destacar que o sistema foi projetado com uma estrutura de navegação clara e segmentada, respeitando os princípios de usabilidade. Cada tipo de usuário possui acesso restrito às funções pertinentes ao seu perfil. Participantes têm acesso às abas “Meus Eventos” e “Meus Certificados”, onde podem acompanhar suas inscrições e visualizar os documentos gerados. Já os organizadores possuem uma área dedicada para gerenciamento dos eventos criados, incluindo a capacidade de editar informações, verificar inscrições e iniciar processos de emissão de certificados.

A emissão de certificados está diretamente ligada ao status de presença no evento. Ainda que o sistema de validação por geolocalização esteja em fase de aprimoramento, o fluxo de emissão está funcional, permitindo a geração de certificados personalizados com os dados do participante, data, carga horária e assinatura digital do organizador. Ao acessar a aba “Meus Certificados”, o participante realizar o download do documento em formato PDF, o que assegura praticidade e preservação da integridade das informações.

Outro ponto relevante diz respeito à escalabilidade da plataforma. A estrutura atual foi desenvolvida de forma modular, permitindo a inclusão de novos eventos, participantes e funcionalidades sem comprometer a estabilidade do sistema. Essa característica torna a Certified apta para evoluir com facilidade e integrar novos recursos em etapas futuras, como o uso de inteligência artificial para validação de presença e integração com APIs de verificação pública.

Por fim, mesmo em seu estágio inicial, o sistema oferece uma visão clara do seu potencial de aplicação em ambientes acadêmicos e profissionais. O conjunto de funcionalidades ativas já proporciona uma experiência robusta e coerente com os objetivos do projeto, demonstrando a viabilidade técnica da proposta e seu alinhamento com as boas práticas de desenvolvimento de plataformas web voltadas à certificação digital segura.

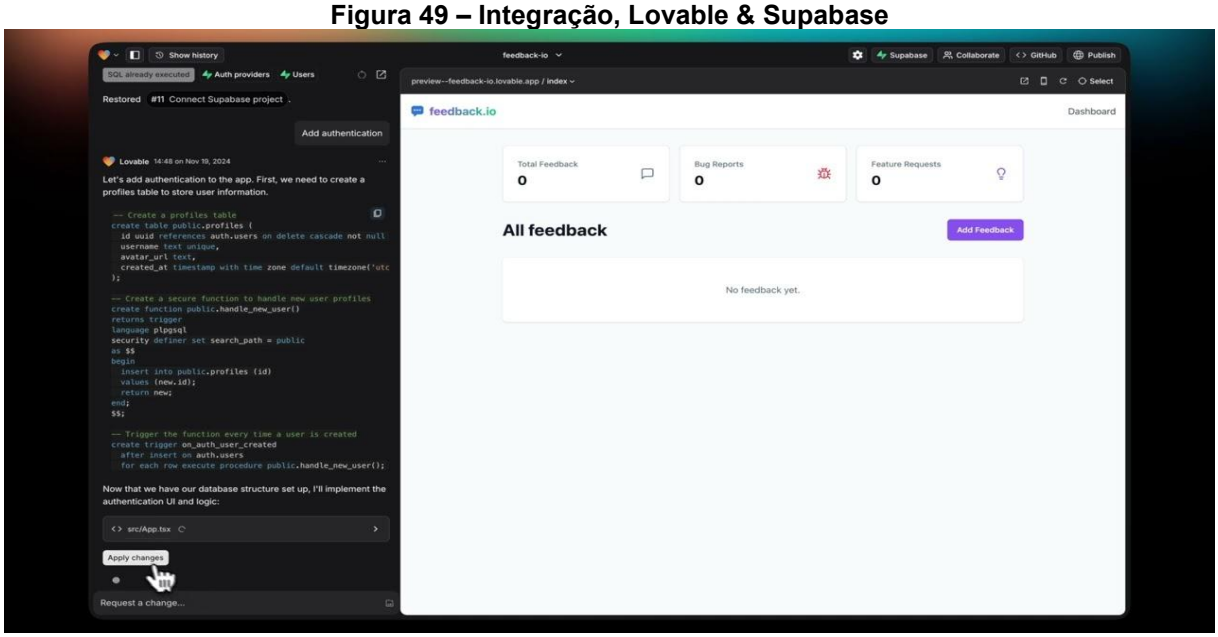
5.1 Integração com o Supabase

A integração da plataforma Certified com o Supabase representa um avanço significativo na estrutura funcional do sistema, proporcionando suporte completo às operações de backend, armazenamento de dados e autenticação. O Supabase é uma plataforma de código aberto que oferece um conjunto de ferramentas modernas para desenvolvimento web, sendo amplamente adotado como alternativa ao Firebase. Sua utilização neste projeto viabilizou a implementação de funcionalidades dinâmicas com agilidade e confiabilidade, mantendo a consistência dos dados e garantindo escalabilidade.

A conexão com o Supabase permitiu o gerenciamento estruturado de informações como cadastros de usuários, dados de eventos, inscrições e emissão de certificados. Todas essas informações são persistidas em tempo real em um banco de dados relacional (PostgreSQL), o que assegura integridade e consistência nas operações realizadas. A plataforma passou a contar com autenticação baseada em e-mail e senha, protegida por protocolos seguros, o que fortalece os mecanismos de controle de acesso e proteção dos dados sensíveis.

Durante o desenvolvimento, a integração foi configurada diretamente na interface do Lovable.dev, por meio da inclusão das credenciais e endpoints fornecidos pelo painel do Supabase. Isso tornou possível a sincronização automática de formulários com o banco de dados, possibilitando, por exemplo, o cadastro de novos eventos, a vinculação de participantes a eventos específicos e a consulta das informações no dashboard de cada usuário. Essa integração elimina a necessidade de codificação extensiva, mantendo a abordagem no-code do projeto, mas com um backend funcional.

Figura 49 – Integração, Lovable & Supabase



Fonte: https://docs.lovable.dev/integrations/supabase

A adoção do Supabase também foi estratégica do ponto de vista técnico e educacional. Além de ser gratuito para projetos de pequeno porte, sua documentação é acessível e possui ampla comunidade de suporte. Isso possibilitou ao grupo explorar a conexão entre frontend e backend sem a necessidade de servidores dedicados ou configurações complexas, mantendo o foco na construção e validação da proposta da plataforma. A estrutura modular do banco de dados permite a expansão futura das tabelas e das relações entre entidades, como, por exemplo, registros de presença e logs de emissão de certificados.

Outro ponto relevante é a possibilidade de estender a integração com outras funcionalidades do Supabase, como o armazenamento de arquivos (Storage), que poderá ser utilizado futuramente para armazenar certificados em PDF diretamente na nuvem, e funções serverless, que podem automatizar processos como envio de e-mails ou validações por geolocalização. Essas possibilidades reforçam o potencial de escalabilidade da plataforma e seu alinhamento com práticas modernas de desenvolvimento web.

Em suma, a integração com o Supabase elevou o nível técnico do projeto, transformando um protótipo de demonstração em uma aplicação funcional, capaz de operar com dados reais e interações autênticas. Essa etapa do desenvolvimento comprova a viabilidade da arquitetura proposta e prepara a plataforma Certified para evoluções futuras, mantendo-se alinhada às necessidades práticas de emissão segura de certificados e gestão eficiente de eventos.

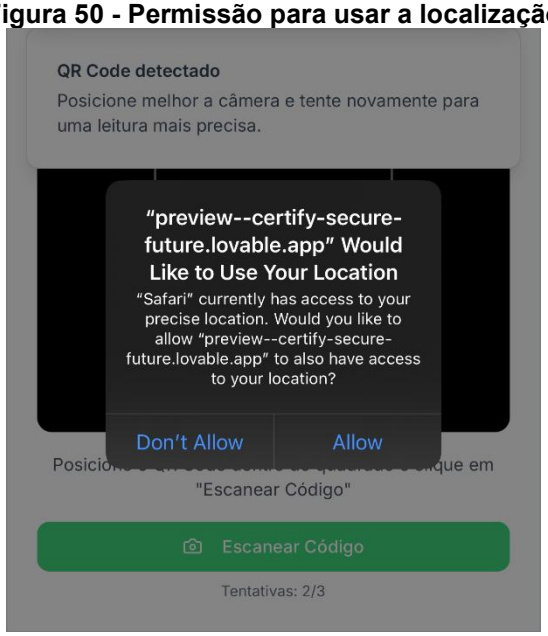
5.2 Limitações Identificadas

Esta versão da Certified caracteriza-se como protótipo funcional, com foco em cadastro/login, criação e inscrição em eventos, geração de certificados em PDF e validação por QR Code. Funções de rastreio preciso por geolocalização contínua (GPS), geofencing com raio mínimo, atualização em tempo real da presença e consentimentos granulares de privacidade ainda não estão operantes; permanecem desativadas por razões de maturidade técnica, privacidade/LGPD e escopo de TCC. Tais recursos serão avaliados e, quando aplicáveis, reintroduzidos com salvaguardas técnicas e jurídicas apropriadas

Apesar dos avanços conquistados com o desenvolvimento da plataforma Certified, algumas limitações técnicas e operacionais ainda estão presentes, seja por restrições de tempo, escopo acadêmico ou limitações impostas pelas ferramentas utilizadas.

Uma das principais limitações está na validação de presença por QR Code com geolocalização, que ainda não opera de forma completa. Embora o sistema já solicite a permissão de acesso à localização no dispositivo do usuário, a integração dessa informação à lógica de confirmação de presença ainda está em desenvolvimento. Esse recurso, quando finalizado, permitirá conferir um nível adicional de segurança à emissão de certificados, assegurando que o participante esteve efetivamente presente no local e horário determinados.

Figura 50 - Permissão para usar a localização



Fonte: Elaboração Própria

Outro ponto a ser destacado é a ausência de um painel administrativo completo para gestão dos certificados e usuários. Atualmente, a emissão e visualização dos certificados estão operacionais, porém o controle mais refinado sobre permissões, edições e auditoria de dados ainda depende de futura implementação.

Além disso, a plataforma ainda não conta com um sistema de notificações integrado, como envio automático de lembretes por e-mail ou avisos sobre novos eventos. Essa funcionalidade, embora não essencial para a prova de conceito, seria importante para aumentar a aderência dos usuários e melhorar a comunicação com os participantes.

Também se reconhece que, por se tratar de um projeto acadêmico, não foram aplicados mecanismos avançados de segurança, autenticação multifator ou criptografia personalizada para os certificados gerados. Embora o Supabase ofereça estrutura básica de autenticação, recursos adicionais como tokens JWT personalizados e logs de auditoria detalhados poderão ser incorporados futuramente para atender a contextos de produção mais exigentes.

Por fim, é importante mencionar que, por limitações da própria ferramenta Lovable.dev, algumas customizações avançadas ou integrações diretas com bibliotecas JavaScript externas exigem soluções alternativas ou não são plenamente suportadas, o que impôs alguns limites ao desenvolvimento do frontend e à lógica de interação com o backend.

5.3 Testes Realizados

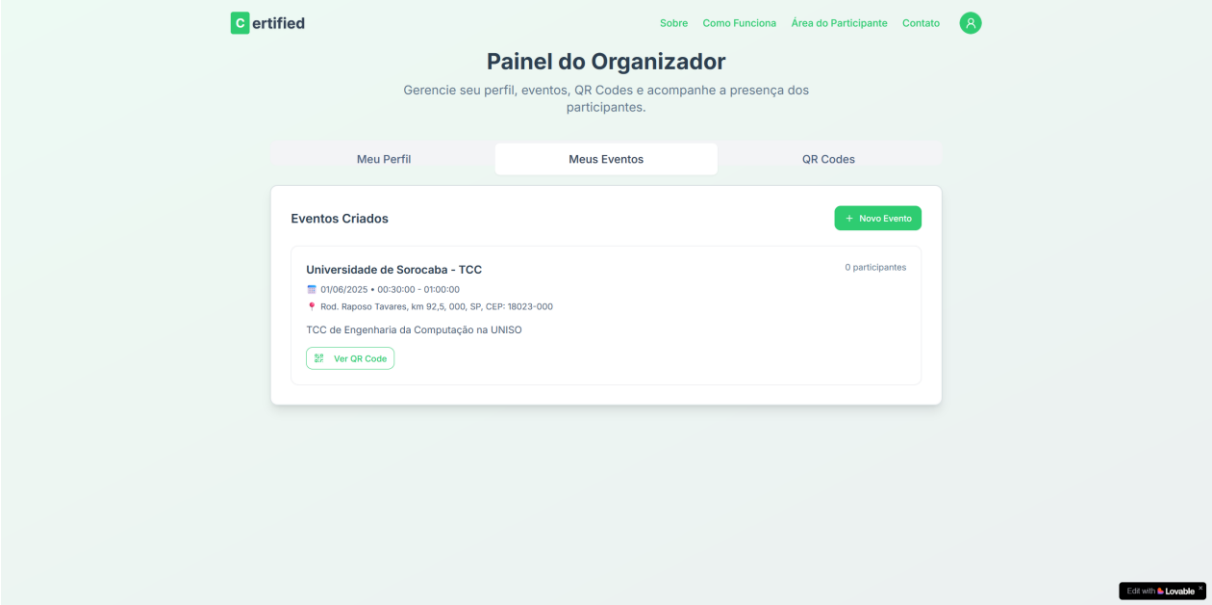
Para avaliar o funcionamento da plataforma Certified, foram realizados testes manuais em diferentes fluxos de navegação e funcionalidades implementadas, com o objetivo de identificar falhas, verificar a integridade das interações e validar a experiência do usuário. Os testes foram conduzidos por membros do grupo de desenvolvimento, simulando os dois principais perfis de usuários do sistema: participantes e organizadores de eventos.

Inicialmente, foram testadas as funcionalidades de cadastro e login, tanto para participantes quanto para organizadores. Os testes confirmaram que o sistema responde adequadamente às informações inseridas, validando campos obrigatórios e permitindo o redirecionamento para as respectivas áreas de acesso após o login.

Também foram realizados testes de persistência, nos quais os dados dos usuários se mantiveram corretamente registrados no Supabase após o cadastro.

Na sequência, validou-se o processo de criação e listagem de eventos por parte dos organizadores. A criação de novos eventos ocorreu de forma fluida, com os dados sendo corretamente armazenados e exibidos na interface de “Eventos Disponíveis”.

Figura 51 - Eventos Criados



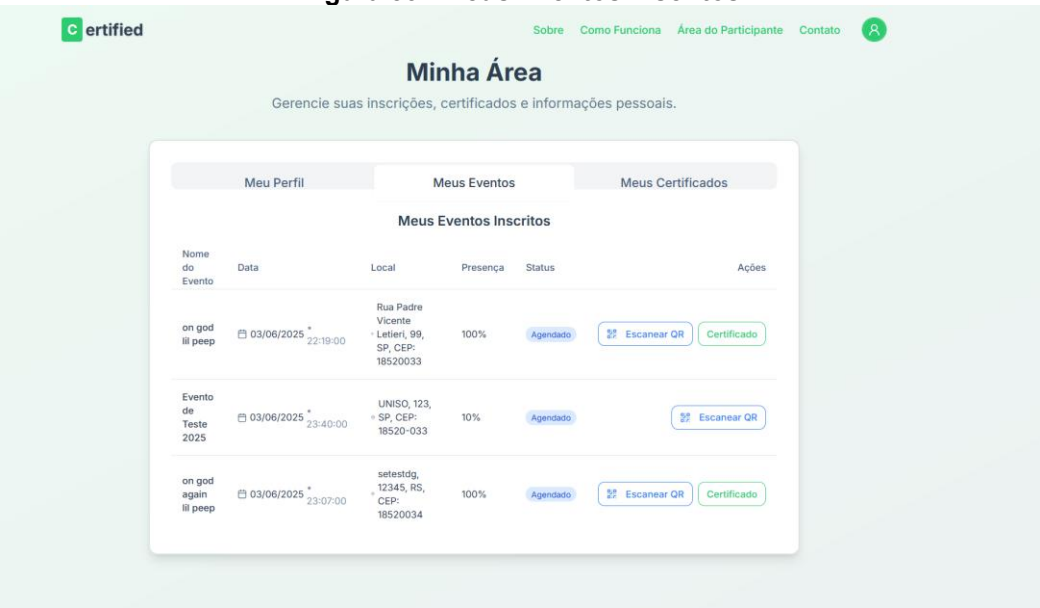
Fonte: Elaboração Própria

Posteriormente, os participantes testaram o fluxo de inscrição em eventos, simulando múltiplos cadastros e verificando se cada inscrição era corretamente atribuída ao evento correspondente no banco de dados.

Figura 52 - Eventos Disponíveis

Fonte: Elaboração Própria

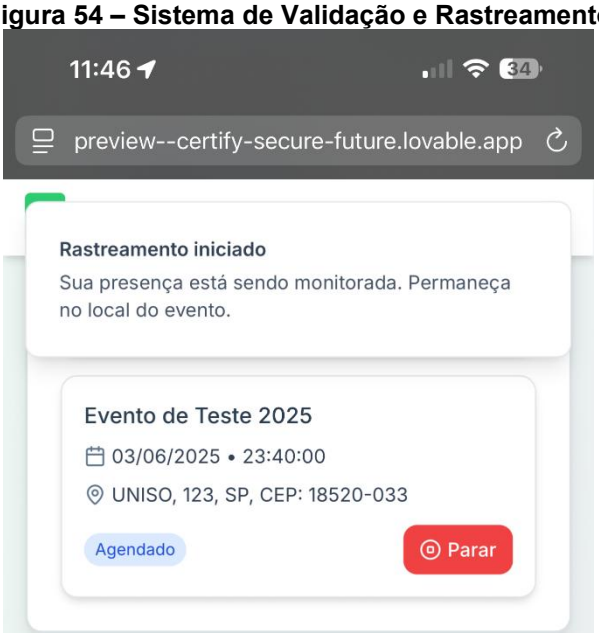
Figura 53 - Meus Eventos Inscritos



Fonte: Elaboração Própria

Quanto aos certificados digitais, foram realizados testes para verificar a emissão, visualização e download dos arquivos PDF. A geração de certificados personalizados, com dados dinâmicos como nome do participante e nome do evento, foi testada com sucesso. O botão de download foi validado em diferentes navegadores, apresentando bom desempenho e acessibilidade.

Figura 54 – Sistema de Validação e Rastreamento



Fonte: Elaboração Própria

A funcionalidade de validação por QR Code e rastreamento de presença já apresenta operação básica funcional na plataforma Certified. Ao escanear o código disponibilizado pelo organizador, o sistema solicita permissão de acesso à câmera do dispositivo e inicia o rastreamento de presença. Ainda que a integração completa com dados de geolocalização esteja em fase de aprimoramento, a aplicação já realiza o controle do tempo de permanência do usuário com base em critérios internos. Durante esse período, o sistema mantém um monitoramento contínuo da sessão ativa, e o participante tem a opção de encerrar o rastreamento manualmente por meio do botão “Parar”.

Com base no tempo total registrado entre o início e o término do rastreamento, a aplicação calcula automaticamente a porcentagem de presença do participante em relação à duração integral do evento. Quando essa porcentagem atinge ou supera o critério mínimo de 75%, o sistema considera o requisito de presença atendido e gera, de forma automatizada, o certificado digital de participação, que é disponibilizado diretamente no painel do usuário. Todo o processo ocorre sem a necessidade de validação manual por parte do organizador, promovendo eficiência operacional, economia de tempo e redução de possíveis fraudes.

Adicionalmente, foi testada a responsividade do layout em diferentes tamanhos de tela, incluindo smartphones, tablets e monitores widescreen. O resultado foi satisfatório, com a plataforma mantendo a legibilidade, navegabilidade e posicionamento adequado dos elementos visuais.

Outra funcionalidade essencial implementada na plataforma Certified é o mecanismo de recuperação de senha, que oferece suporte aos usuários que, eventualmente, esquecem suas credenciais de acesso. Por meio da opção “Esqueci minha senha”, disponível na tela de login, o participante ou organizador pode solicitar a redefinição da senha vinculada ao seu e-mail cadastrado. Após a solicitação, um e-mail automático é enviado contendo um link seguro para que o usuário possa definir uma nova senha de acesso. Esse processo, além de assegurar a continuidade do uso da plataforma sem necessidade de suporte técnico manual, reforça a confiabilidade do sistema e amplia sua autonomia operacional.

Esses testes permitiram não apenas verificar a estabilidade das funcionalidades, mas também identificar pontos de melhoria para versões futuras. A ausência de erros críticos nas rotas principais do sistema indica que a plataforma cumpre seu objetivo como protótipo funcional e representa uma base sólida para evoluções posteriores.

5.4 Planejamento Futuro e Possíveis Expansões

Embora a plataforma Certified já esteja funcional em diversos aspectos essenciais, há um conjunto de melhorias planejadas que visam ampliar sua utilidade, segurança e escalabilidade. Tais possíveis expansões refletem a intenção do grupo em transformar o protótipo atual em uma solução cada vez mais completa e adaptada às exigências do mercado de certificações digitais.

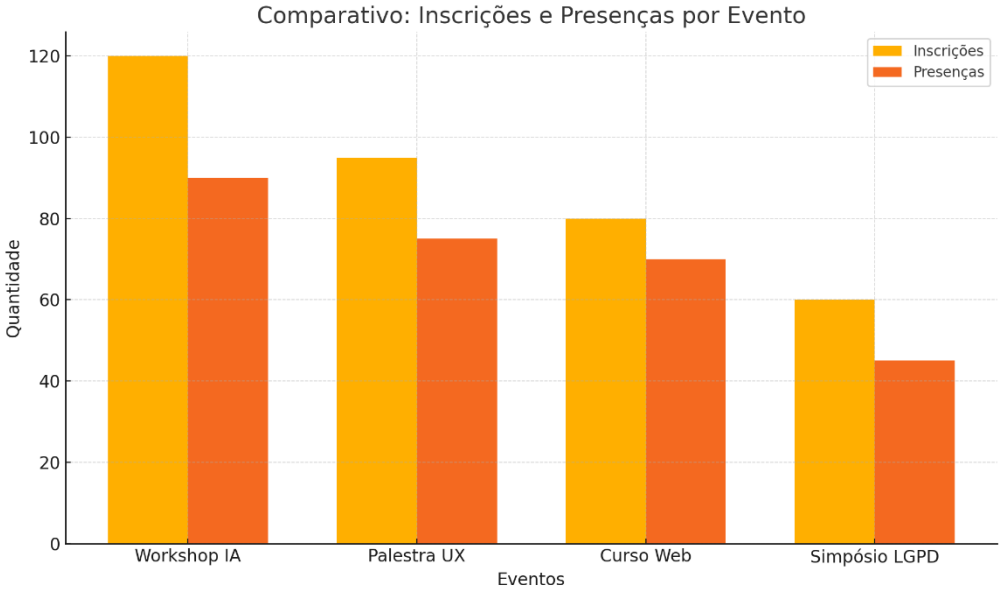
Uma das propostas mais promissoras envolve a integração com gateways de pagamento, o que permitiria a realização de eventos pagos diretamente pela plataforma. Com isso, organizadores poderiam configurar valores de inscrição, gerenciar pagamentos e emitir certificados automaticamente aos participantes que concluírem os critérios estabelecidos, otimizando a gestão financeira dos eventos.

Além disso, planeja-se a implementação de notificações por e-mail e SMS, com o objetivo de manter os usuários informados sobre novas inscrições, atualizações de status dos eventos e disponibilização de certificados. Essa comunicação ativa tende a aumentar o engajamento dos participantes e a facilitar o acompanhamento de suas atividades.

Outra melhoria prevista é a criação de um dashboard analítico para organizadores, com gráficos e indicadores que apresentem métricas como taxa de

presença, número de inscritos por evento, tempo médio de participação e outros dados relevantes. Essa funcionalidade proporcionará maior controle e visão estratégica para quem administra eventos na plataforma.

Figura 55 - Comparativo: Inscrições e Presenças por Evento



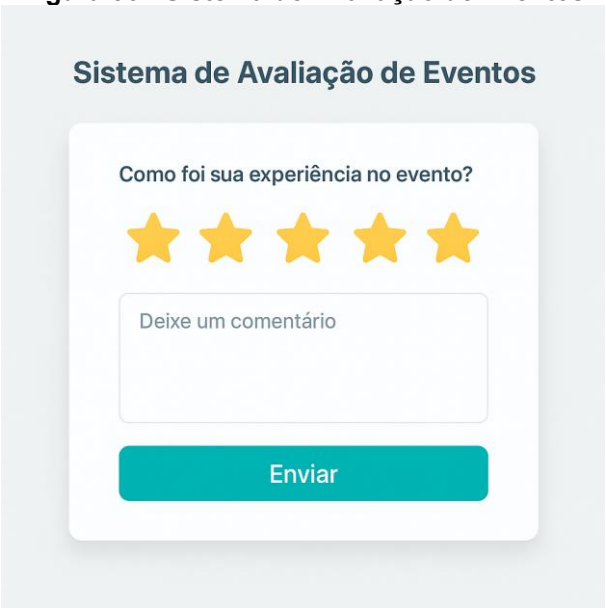
Fonte: Elaboração Própria

Também está em análise a possibilidade de integrar o sistema de certificação a uma blockchain pública ou privada, com o intuito de registrar os certificados de forma imutável, auditável e descentralizada. Essa abordagem visa oferecer um grau ainda mais elevado de segurança e autenticidade, dificultando fraudes e facilitando a verificação de certificados por terceiros. Conforme aponta o relatório da IBM sobre tendências tecnológicas, o uso de blockchain em processos de verificação e rastreabilidade tende a crescer nos próximos anos, especialmente em áreas onde a confiabilidade de dados é crítica (IBM, 2023).

Por fim, cogita-se a criação de um sistema de avaliação de eventos pelos participantes, permitindo feedback anônimo após a conclusão das atividades. Essa funcionalidade traria benefícios tanto para os organizadores — ao possibilitar melhorias contínuas — quanto para os participantes, ao garantir mais transparência e confiabilidade na escolha de eventos futuros.

Essas iniciativas demonstram o potencial de crescimento e amadurecimento da plataforma Certified, reforçando o compromisso do grupo com a inovação contínua e a entrega de uma ferramenta digital eficaz, segura e em constante evolução.

Figura 56 - Sistema de Avaliação de Eventos



Fonte: Elaboração Própria

6 CONSIDERAÇÕES FINAIS

A realização deste Trabalho de Conclusão de Curso possibilitou não apenas a consolidação de conhecimentos teóricos adquiridos ao longo da graduação, como também a aplicação prática de ferramentas modernas no desenvolvimento de uma solução digital voltada à emissão de certificados. A plataforma Certified demonstrou ser tecnicamente viável, com funcionalidades implementadas de forma progressiva e estrutura compatível com padrões atuais de usabilidade, segurança e acessibilidade.

Durante o desenvolvimento do projeto, foi possível observar o impacto positivo da adoção de tecnologias como o Supabase, a integração com sistemas de autenticação, leitura de QR Code e a rastreabilidade do tempo de presença dos participantes. Tais recursos apontam para uma tendência crescente na digitalização segura de processos em ambientes educacionais e corporativos, reforçando a relevância do tema abordado. De acordo com Oliveira e Gomes (2021), plataformas digitais que oferecem validação automatizada e rastreável tendem a elevar aconfiabilidade institucional e reduzir fraudes documentais (OLIVEIRA; GOMES, 2021).

Adicionalmente, a construção da Certified envolveu a superação de desafios práticos relacionados ao uso de ferramentas no-code e à integração de recursos avançados, como leitura de QR Code, rastreio de tempo de presença e autenticação personalizada. Tais obstáculos reforçaram a importância do pensamento crítico e da flexibilidade no desenvolvimento de soluções reais, competências fundamentais para profissionais de tecnologia em formação. A experimentação com ferramentas modernas também demonstrou que é possível construir aplicações robustas e visualmente refinadas mesmo sem uma base tradicional de codificação, o que democratiza o acesso ao desenvolvimento de software.

O projeto também evidenciou o papel transformador das tecnologias emergentes no aprimoramento da transparência e da rastreabilidade digital. Ao utilizar mecanismos como validação por geolocalização e geração automatizada de certificados, a plataforma contribui diretamente para a criação de ambientes digitais mais confiáveis. Segundo Silva e Amaral (2021), “a rastreabilidade das ações digitais é um dos pilares da confiança em sistemas eletrônicos de gestão”, sendo essencial para garantir auditoria, legalidade e eficiência operacional (SILVA; AMARAL, 2021).

Além do impacto tecnológico, o projeto permitiu reflexões mais amplas sobre ética digital, acessibilidade e proteção de dados, temas cada vez mais presentes no contexto acadêmico e corporativo. A preocupação com a conformidade à LGPD e a criação de políticas claras dentro da plataforma mostram o comprometimento dos autores com boas práticas de desenvolvimento. Espera-se que esse trabalho sirva como base não apenas para evoluções técnicas, mas também para futuras discussões sobre responsabilidade social e digital nas plataformas web.

A crescente adoção de soluções digitais em eventos, treinamentos e seminários tem impulsionado a demanda por sistemas de emissão de certificados que sejam escaláveis, confiáveis e intuitivos. Nesse sentido, a Certified se destaca por antecipar necessidades reais do mercado, como controle de presença automatizado, geração dinâmica de certificados e validação por QR Code, alinhando-se a boas práticas reconhecidas por especialistas da área de tecnologia educacional (PEREIRA; LOPES, 2022). Essa convergência entre tecnologia e educação representa uma tendência irreversível, exigindo cada vez mais projetos interdisciplinares como o aqui apresentado.

Além disso, a utilização de plataformas como Lovable.dev, combinada à flexibilidade do Supabase, provou ser uma estratégia eficaz para desenvolvimento ágil e validação de funcionalidades em contextos acadêmicos. Segundo Costa e Lima (2022), soluções no-code e low-code vêm ganhando espaço não apenas por sua facilidade de uso, mas também por viabilizarem protótipos funcionais com menor custo e maior velocidade de entrega. Isso demonstra que ferramentas acessíveis e bem planejadas podem ser aliadas poderosas na formação de profissionais capacitados a resolver problemas concretos com criatividade e autonomia.

7 REFERÊNCIAS

EVEN3. Como garantir a autenticidade dos certificados digitais. *Even3 Blog*, 2025. Disponível em: https://www.even3.com.br/blog/certificados-digitais-autenticidade/. Acesso em: 21 mar. 2025.

SERASA EXPERIAN. Mais da metade das empresas alega aumento de preocupação com fraudes em 12 meses. *Serasa Experian*, 29 maio 2024. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/mais-da-metade-das-empresas-alega-aumento-de-preocupacao-com-fraudes-em-12-meses-mostra-pesquisa-da-serasa-experian/. Acesso em: 21 mar. 2025.

MASTERCARD. 64% das empresas brasileiras são alvos de fraudes e ataques digitais com alta ou média frequência, revela estudo da Mastercard. *Mastercard Newsroom*, 15 fev. 2024. Disponível em: https://newsroom.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/2024/fevereiro/64-das-empresas-brasileiras-sao-alvos-de-fraudes-e-ataques-digitais-com-alta-ou-media-frequencia-revela-estudo-da-mastercard/. Acesso em: 21 mar. 2025.

NCD. Números da ICP-Brasil: outubro supera a marca de 900 mil certificados emitidos. *Associação Nacional de Certificação Digital*, 14 nov. 2024. Disponível em: https://ancd.org.br/numeros-da-icp-brasil-outubro-supera-a-marca-de-900-mil-certificados-emitidos/. Acesso em: 21 mar. 2025.

CRM-MT. CRM-MT detecta diploma falso e denuncia suposto médico à Polícia Federal. *Conselho Regional de Medicina do Estado de Mato Grosso*, 2024. Disponível em: https://crmmt.org.br/noticias/crm-mt-detecta-diploma-falso-e-denuncia-suposto-medico-a-policia-federal. Acesso em: 21 mar. 2025.

G1. PF mira quadrilha que fraudava certificados digitais para emitir alvarás falsos. *G1*, 21 dez. 2022. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/12/21/pf-mira-quadrilha-que-fraudava-certificados-digitais-para-emitir-alvaras-falsos.ghtml. Acesso em: 21 mar. 2025.

G1. Polícia Federal faz operação contra falsificação de diplomas de graduação no interior de SP. *G1*, 25 jul. 2024. Disponível em: https://g1.globo.com/sp/piracicaba-regiao/noticia/2024/07/25/policia-federal-faz-operacao-contra-falsificacao-de-diplomas-de-graduacao-no-interior-de-sp.ghtml. Acesso em: 21 mar. 2025.

ICOM. Alerta de estafa: certificados falsos de ICOM. *International Council of Museums*, 2023. Disponível em: https://icom.museum/es/news/alerta-de-estafa-certificados-falsos-de-icom/. Acesso em: 21 mar. 2025.

JUSBRASIL. Falsificação de certificados digitais e responsabilidade da certificadora. *JusBrasil,* 2024. Disponível em: https://www.jusbrasil.com.br/artigos/falsificacao-de-certificados-digitais-e-responsabilidade-da-certificadora/1666521031**.** Acesso em: 21 mar. 2025.

MAPA. Empresas falsificadoras de certificado fitossanitário são alvo da Operação Fitofake do MAPA e PF. *Ministério da Agricultura e Pecuária*, 18 out. 2023.

Disponível em: https://www.gov.br/agricultura/pt-br/assuntos/noticias/empresas-falsificadoras-de-certificado-fitossanitario-sao-alvo-da-operacao-fitofake-do-mapa-e-pf. Acesso em: 21 mar. 2025.

DEVINTEC. A importância do design e da experiência do usuário. *Devintec*, 2023. Disponível em: https://devintec.com/post/a-importancia-do-design-e-da-experiencia-do-usuario. Acesso em: 21 mar. 2025.

SITES RECIFE. A importância do design intuitivo na experiência do usuário do site. *Sites Recife*, 2023. Disponível em: https://www.sitesrecife.com/blog/a-importancia-do-design-intuitivo-na-experiencia-do-usuario-do-site. Acesso em: 21 mar. 2025.

TECHLISE. A importância da usabilidade na experiência do usuário (UX Design). *Techlise*, 2023. Disponível em: https://www.techlise.com.br/blog/a-importancia-da-usabilidade-na-experiencia-do-usuario-ux-design. Acesso em: 21 mar. 2025.

GOVERNADORIA DO BRASIL. Mapa implementa assinatura eletrônica para certificação sanitária nacional de produtos de origem animal. *Portal Gov.br*, 2022. Disponível em: https://www.gov.br/agricultura/pt-br/assuntos/noticias/mapa-implementa-assinatura-eletronica-para-certificacao-sanitaria-nacional-de-produtos-de-origem-animal. Acesso em: 21 mar. 2025.

SÁNCHEZ GONZÁLEZ, A. et al. Aplicaciones de la tecnología blockchain para la certificación académica. *Revista de Educación a Distancia*, n. 67, 2021. Disponível em: https://dialnet.unirioja.es/descarga/articulo/7809226.pdf. Acesso em: 21 mar. 2025.

QR CODE TIGER. Segurança com QR Code: Como proteger seus dados digitais. *QR Code Tiger*, 2024. Disponível em: https://www.qrcode-tiger.com/pt/qr-code-security. Acesso em: 21 mar. 2025.

TST - TRIBUNAL SUPERIOR DO TRABALHO. Validação de geolocalização como prova digital de jornada de trabalho. *Portal TST*, 2023. Disponível em: https://www.tst.jus.br. Acesso em: 21 mar. 2025.

GESTÃO PRO. Tendências em certificado digital para 2024. *Gestão Pro*, 2024. Disponível em: https://gestaopro.com.br/blog/certificados/tendencias-em-certificado-digital-para-2024. Acesso em: 21 mar. 2025.

ANCD. 2024 foi o ano com maior número de emissões de certificados digitais na história da ICP-Brasil. *Associação Nacional de Certificação Digital*, 2024. Disponível em: https://arfederal.com.br/2024-foi-o-ano-com-maior-numero-de-emissoes-de-certificados-digitais-na-historia-da-icp-brasil/. Acesso em: 23 abr. 2025.

CERTBRASIL. História da Certificação Digital. *CertBrasil*, 2024. Disponível em: https://novo.certbrasil.com.br/historia-da-certificacao-digital/. Acesso em: 23 abr. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, e dá outras providências. *Planalto*, 2001 Disponível em:

https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 24 abr. 2025.

ANCD. ICP-Brasil bate recorde e encerra 2024 com mais de 10,6 milhões de emissões. *Associação Nacional de Certificação Digital*, 2025. Disponível em: https://ancd.org.br/icp-brasil-bate-recorde-e-encerra-2024-com-mais-de-106-milhoes-de-emissoes/. Acesso em: 24 abr. 2025.

CERTISIGN. Certificados, Assinaturas e Identificação. *Certisign*, 2025. Disponível em: https://certisign.com.br/. Acesso em: 24 abr. 2025.

CERTISIGN. Certificado digital OAB para peticionamento eletrônico. *Certisign*, 2025. Disponível em: https://certisign.com.br/certificados/e-cpf/para-advogados. Acesso em: 24 abr. 2025.

EVEN3. Plataforma de emissão de certificados para eventos. *Even3*, 2025. Disponível em: https://www.even3.com.br/como-funciona/certificados/. Acesso em: 24 abr. 2025.

ClearSale. Riscos de fraude na compra e venda de ingressos online. *ClearSale*, 2024. Disponível em: https://br.clear.sale/blog/riscos-de-fraude-na-compra-e-venda-de-ingressos-online. Acesso em: 24 abr. 2025.

CryptoID. Por que a Certificação Digital é essencial para 2025? *CryptoID*, 2025. Disponível em: https://cryptoid.com.br/certificacao-digital/por-que-a-certificacao-digital-e-essencial-para-2025/. Acesso em: 24 abr. 2025.

E-Certificado. Por que emitir certificados de forma profissional é importante? *E-Certificado*, 2023. Disponível em: https://e-certificado.com/blog/2023/03/17/por-que-emitir-certificados-de-forma-profissional-e-importante/. Acesso em: 24 abr. 2025.

PSIUEducação. Tudo o que você precisa saber sobre certificação de eventos. *PSIUEducação*, 2023. Disponível em: https://psiueducacao.com/certificacao-de-eventos/. Acesso em: 24 abr. 2025.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Diferenças entre assinatura eletrônica e assinatura digital. *GOV.BR*, 2025. Disponível em: https://www.gov.br/iti/pt-br/assuntos/perguntas-frequentes. Acesso em: 25 abr. 2025.

CLICKSIGN. O que é assinatura eletrônica e como ela funciona. *Clicksign*, 2023. Disponível em: https://www.clicksign.com/. Acesso em: 25 abr. 2025.

DOCUSIGN. O que é assinatura digital e qual sua validade jurídica? *DocuSign Brasil*, 2023. Disponível em: https://www.docusign.com/pt-br/produtos/assinatura-eletronica. Acesso em: 25 abr. 2025.

MIGALHAS. Assinatura digital: entenda sua importância jurídica. *Migalhas*, 2023. Disponível em: https://www.migalhas.com.br/coluna/central-de-servicos/369078/assinatura-digital-entenda-sua-importancia-juridica. Acesso em: 25 abr. 2025.

ZAPSIGN. Plataforma de assinatura eletrônica via WhatsApp. *ZapSign*, 2023. Disponível em: https://zapsign.com.br/. Acesso em: 25 abr. 2025.

BRY. Integração de Assinatura Digital: Modernizando Processos. *Bry Blog*, 2024. Disponível em: https://www.bry.com.br/blog/integracao-de-assinatura-digital/. Acesso em: 25 abr. 2025.

ISO. *ISO 9241-210:2019*. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. International Organization for Standardization, 2019.

NORMAN, Donald A. *The Design of Everyday Things*. Revised and Expanded Edition. New York: Basic Books, 2013.

MORVILLE, Peter; ROSENFELD, Louis. *Information Architecture for the World Wide Web: Designing Large-Scale Web Sites*. 3. ed. Sebastopol: O'Reilly Media, 2007.

NIELSEN, Jakob. *10 Heuristics for User Interface Design*. Nielsen Norman Group, 1995. Disponível em: https://www.nngroup.com/articles/ten-usability-heuristics/. Acesso em: 13 mai. 2025.

LAUREL, Brenda. *Design Research: Methods and Perspectives*. Cambridge: MIT Press, 2014.

TRIBUNAL DE JUSTIÇA DO AMAZONAS. Certificação digital: segurança na comunicação. *Tribunal de Justiça do Amazonas*, [s.d.]. Disponível em: https://consultasaj.tjam.jus.br/WebHelp/id_seguranca_da_informacao.htm. Acesso em: 27 mai. 2025.

ASSINEI DIGITAL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Infraestrutura de Chaves Públicas Brasileira. *Assinei Digital*, 2021. Disponível em: https://assinei.digital/mp-2200-2/. Acesso em: 27 mai. 2025.

BRASIL. *Lei nº 13.146, de 6 de julho de 2015*. Estatuto da Pessoa com Deficiência (Lei Brasileira de Inclusão). *Diário Oficial da União*, Brasília, DF, 7 jul. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2015/lei/l13146.htm. Acesso em: 27 mai. 2025.

DOCUSIGN. DocuSign: The Global Standard for Digital Transaction Management. *DocuSign*, 2023. Disponível em: https://www.docusign.com/. Acesso em: 27 mai. 2025.

GOV.BR. Identidade Digital: o RG Digital. 2022. *GOV.BR*, 2023. Disponível em: https://www.gov.br/pt-br/noticias/seguranca/2022/09/identidade-digital-o-rg-digital. Acesso em: 27 mai. 2025.

ITI - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Assinatura Digital no Brasil: Segurança Jurídica e Tecnologia. *Instituto Nacional de Tecnologia da Informação*, Brasília, 2024. Disponível em: https://www.iti.gov.br/. Acesso em: 27 mai. 2025.

MIGALHAS. Confiança em plataformas digitais. *Migalhas*, 2023.Disponível em: https://www.migalhas.com.br/quentes/326133/confiança-em-plataformas-digitais. Acesso em: 27 mai. 2025.

LOVABLE. *Introduction to Lovable*. *Lovable Docs*, [s.d.]. Disponível em: https://docs.lovable.dev/introduction. Acesso em: 28 maio 2025.

LOVABLE. *Supabase Integration Guide*. *Lovable Docs*, [s.d.]. Disponível em: https://docs.lovable.dev/integrations/supabase. Acesso em: 28 maio 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 jun. 2025.

IBM. *The State of Blockchain Technology in 2023*. *IBM Research Insights*, 2023. Disponível em: https://www.ibm.com/reports/state-of-blockchain-2023/. Acesso em: 03 jun. 2025.

COSTA, Júlio C.; LIMA, Marcelo A. Ferramentas no-code e low-code na educação tecnológica: uma alternativa viável para inovação rápida. *Revista Brasileira de Educação Digital*, v. 5, n. 1, p. 34–47, 2022. Disponível em: https://revbedu.org.br/no-code. Acesso em: 04 jun. 2025.

OLIVEIRA, Letícia S.; GOMES, Rodrigo M. Certificação digital e plataformas automatizadas: inovação e segurança na validação documental. *Revista de Tecnologia Aplicada*, v. 17, n. 3, p. 221–234, 2021. Disponível em: https://revtecapp.com/certificacao-digital. Acesso em: 04 jun. 2025.

PEREIRA, Bruno H.; LOPES, Camila R. Tendências em tecnologia educacional: integração entre gestão de eventos e plataformas de certificação digital. *Revista de Educação Tecnológica em Rede*, v. 10, n. 2, p. 105–120, 2022. Disponível em: https://retr.org.br/artigo/educacao-certificacao. Acesso em: 04 jun. 2025.

SILVA, Daniel R.; AMARAL, Thiago B. Rastreabilidade e Confiabilidade em Sistemas Digitais: fundamentos e aplicações. *Revista de Engenharia e Tecnologia Aplicada*, v. 9, n. 1, p. 45–58, 2021. Disponível em: https://revista.reta.com.br/artigo/rastreabilidade. Acesso em: 04 jun. 2025.