Automatização do Processo de Assinatura Digital: Desenvolvimento e Aplicações

Pedro Henrique Boiko[1] Isabelle Cordova Gomes[1]

[1]Centro Universitário Campo Real

Rua Comendador Norberto, 1299 - Santa Cruz – Guarapuava – PR – Brasil

{engs-pedroboiko@camporeal.edu.br, prof_isabellecordova@camporeal.edu.br}

RESUMO

Este estudo apresenta o desenvolvimento de uma ferramenta de automatização de assinaturas digitais em uma empresa, utilizando integração com APIs (*Application Programming Interface*) para assinar automaticamente declarações geradas pelo sistema de um *software house*. Com a vinda do novo governo no ano de 2022, foram criadas novas portarias, que aumentam a burocracia para clubes e entidades de tiro esportivo. Esta portaria exige que todos os documentos da mesma, sejam assinadas com certificado digital, e também deve apresentar o selo ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira). Está solução permite que clientes utilizem suas assinaturas digitais em um menu dedicado, garantindo que documentos sejam validados e carimbados automaticamente em conformidade com os padrões exigidos. A verificação de autenticidade é facilitada pela integração com o GOV BR[1] (Portal unificado do Governo Federal do Brasil), o que reforça a confiabilidade dos documentos emitidos. Os resultados evidenciam uma significativa redução de tempo e erros humanos no processo de assinatura, otimizando o fluxo interno e proporcionando maior segurança e confiança para os clientes. A ferramenta destaca o impacto positivo da inovação tecnológica no ambiente corporativo, ao automatizar um processo antes complexo e repetitivo. O sucesso da implementação sugere que essa abordagem automatizada pode ser expandida para outras áreas, aumentando a eficiência e credibilidade da empresa. Com a modernização do processo de assinaturas, a empresa fortalece sua imagem e ganha agilidade operacional, demostrando como a tecnologia pode otimizar operações e gerar benefícios consistentes.

[1] https://www.gov.br/

Palavras-chave: Certificação Eletrônica. Validação Automática. Inovação Tecnológica. Segurança da Informação. ICP-Brasil.

ABSTRACT

This study presents the development of a digital signature automation tool in a company, using integration with APIs (Application Programming Interface) to automatically sign declarations generated by a software house system. With the arrival of the new government in 2022, new regulations were created, increasing bureaucracy for clubs and shooting sports entities. These regulations require that all their documents be signed with a digital certificate and must also feature the ICP-Brazil seal (Brazilian Public Key Infrastructure). This solution allows clients to use their digital signatures through a dedicated menu, ensuring that documents are automatically validated and stamped in accordance with the required standards. Authentication verification is facilitated through integration with GOV BR (the unified portal of the Brazilian Federal Government), which strengthens the reliability of the issued documents. The results show a significant reduction in time and human errors in the signing process, optimizing internal workflows and providing greater security and trust for clients. The tool highlights the positive impact of technological innovation in the corporate environment by automating a previously complex and repetitive process. The success of the implementation suggests that this automated approach could be expanded to other areas, increasing the company's efficiency and credibility. With the modernization of the signing process, the company strengthens its image and gains operational agility, demonstrating how technology can optimize operations and generate consistent benefits.

Keywords: Electronic Certification. Automatic Validation. Technological Innovation. Information Security. ICP-Brasil.

1. Introdução

A digitalização de processos empresariais e governamentais intensificou a demanda por soluções que garantam segurança, agilidade e eficiência na gestão de documentos eletrônicos. A assinatura digital, nesse contexto, consolidou-se como

uma ferramenta essencial para assegurar a autenticidade e integridade de documentos, eliminando procedimentos manuais e reduzindo risco de fraudes. Além de atender à necessidade de segurança, a adoção de tecnologias de certificação digital otimiza recursos e tempo nas organizações.

Dados recentes do Ministério da Gestão e da Inovação em Serviços Públicos (2023) mostram que o uso de assinaturas digitais no Brasil cresceu significativamente, impulsionado por plataformas governamentais como o GOV BR, que facilitam o uso de certificações digitais em larga escala. Esse cenário evidencia a importância de soluções automatizadas que realizem processos digitais de maneira confiável e com mínima intervenção humana.

Este projeto teve como objetivo automatizar o processo de assinatura digital, permitindo a validação rápida e segura de documentos eletrônicos sem a intervenção constante de usuário. A justificativa para este trabalho baseou-se na busca por maior eficiência e segurança, com a automatização reduz o tempo de gerenciamento e eliminando riscos associados a falhas humanas, além de garantir conformidade como o ICP-Brasil (Instituto Nacional de Tecnologia da Informação).

O projeto desenvolveu uma solução prática e automatizada para assinaturas digitais, empregando tecnologias como PHP, Angular, Python, Banco de Dados e Laravel, além da integração com APIs parceiras, que facilitam a comunicação com serviços de certificação digital, como o GOV.BR. A proposta incluiu interface intuitiva permitindo que o usuário gerenciasse certificados digitais com praticidade e segurança.

Ao automatizar o fluxo de assinaturas digitais para o cotidiano empresarial, o projeto contribuiu para a produtividade organizacional e para a confiabilidade de documentos digitais, mitigando fraudes e fortalecendo a validade jurídica. Ao longo do estudo, foram detalhadas as etapas de desenvolvimento do sistema, as tecnologias empregadas, os desafios enfrentados na integração de APIs de assinatura digital e os resultados obtidos em termos de eficiência e segurança.

2. Referencial Teórico

Hipoteticamente, embora uma assinatura manuscrita seja única para cada pessoa, uma assinatura digital não possui essa mesma característica. Além de estar vinculada a uma entidade emissora, uma assinatura digital está associada à transação

específica em que é utilizada, sendo exclusiva para cada transação realizada pelo emissor e possuindo sempre um período de validade definido (PEREIRA, 2008).

O certificado digital é a tecnologia que assegura a identificação confiável de uma mensagem ou transação eletrônica, garantindo confidencialidade, integridade e validade jurídica. A certificação digital estará cada vez mais presente em várias áreas do governo, contribuindo para democratizar o acesso aos serviços públicos, proporcionando economia de tempo, praticidade e, sobretudo, segurança devido à autenticação digital (VOLPI, 2001).

2.1. Assinatura Digital e Tipos de Certificação Digital

A Assinatura Digital, como o próprio nome diz, serve para assinar qualquer documento eletrônico. Tem validade jurídica inquestionável e equivale a uma assinatura de próprio punho. É uma tecnologia que utiliza a criptografia e vincula o certificado digital ao documento eletrônico que está sendo assinado. Assim, dá garantias de integridade e autenticidade (QUALISIGN, 2005-2017).

No certificado tipo A1 o par de chaves pública/privada é gerado em seu computador, no momento da solicitação de emissão do certificado. A chave pública será enviada para a Autoridade Certificadora (AC) com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada em seu computador, devendo, obrigatoriamente, ser protegida por senha de acesso. Este certificado for instalado no mesmo computador onde foi efetuada a solicitação do certificado e tem validade de 1 (um) ano (ASS TECNOLOGIA, 2012).

O certificado tipo A3 oferece mais segurança, justamente porque o par de chaves é gerado em hardware específico, isto é, num cartão inteligente ou token que não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada. Também no certificado tipo A3 a chave pública será enviada para a AC junto com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada no cartão ou token, impedindo tentativas de acesso de terceiros. Com este método, você poderá transportar a sua chave privada e o seu certificado digital de maneira segura, podendo realizar transações eletrônicas onde desejar. O certificado tipo A3 tem validade de 3 (três) anos (ASS TECNOLOGIA, 2012).

O Certificado Digital e-CPF é a versão eletrônica do CPF (Cadastro de Pessoa Física) e permite realizar operações na internet com a mesma validade jurídica que o

documento físico. Também pode ser usado em instituições privadas, como já fazem alguns bancos para determinadas transações. Em instituições públicas como a Receita Federal e a Caixa, sua utilização é indispensável (GALUCCI, 2024).

O tipo e-CNPJ é o Certificado Digital para empresas, vinculado ao CNPJ, que possibilita a realização de transações online de maneira segura e com validade jurídica. O e-CNPJ deve ser emitido para o representante legal da empresa na Receita Federal. (GALUCCI, 2024).

Os certificados NF-e são feitos especialmente para a empresa que precisa assinar as notas fiscais eletrônicas de forma segura e com validade jurídica, e precisa da flexibilidade de ser emitido para alguém diferente do representante legal na Receita Federal (RFB), como o responsável pela emissão das notas. Além disso, serve também para outras aplicações com essa característica, como o Conhecimento de Transporte Eletrônico (CTE). (GALUCCI, 2024).

2.2. ICP- Brasil - Benefícios da Automatização e a Implementação

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos (ITI, 2016a).

Os atuais recursos de comunicação eletrônica colaboram e impõem práticas que podem influenciar positivamente a redução do uso de papel. Além disso, a agilidade exigida para atividades empresariais pode colaborar para que os indivíduos convertam as informações, tradicionalmente impressas, para meios digitais (TURBAN; MCLEAN; WETHERBE, 2004). A certificação digital assegura a autenticidade da assinatura digital ao unir elementos tecnológicos e jurídicos. No Brasil, tem sido empregada para conferir valor legal a documentos eletrônicos, garantindo sua validade como prova em processos legais (PEREIRA, 2008).

2.3. Rastreabilidade, Controle do Fluxo e Validade Legal das Assinaturas Digitais

Ribeiro (1999) define automatização como a substituição de trabalho humano ou animal por máquinas, ou seja, é a operação de máquinas ou sistemas automáticos com a mínima interferência possível do operador. O autor complementa dizendo que a automatização pode reduzir a mão de obra empregada, porém ainda requer acompanhamento, programação e ajustes, ao invés de fazer a tarefa diretamente o operador controla a máquina. Também Moraes (2007) enfatiza que a automatização traz maior nível de qualidade, expressa por especificações numéricas de tolerância, maior flexibilidade para o mercado, maior segurança dos operários, menores perdas, mais disponibilidade e qualidade da informação sobre o processo produtivo, melhor planejamento e controle da produção.

A segurança jurídica proporcionada pela automatização da assinatura digital é um dos principais benefícios desse sistema. O uso do padrão ICP-Brasil introduz uma camada de criptografia que protege o documento contra adulterações, garantindo que apenas o titular da chave privada possa realizar a assinatura. Essa segurança adicional assegura que os documentos mantêm sua integridade e são aceitos em contextos legais, como processos judiciais e negociações contratuais complexas.

A automatização do processo de assinatura digital não apenas resolve os problemas do método manual, como também introduz novas possibilidades de integração, segurança e eficiência. O fluxo de trabalho torna-se mais ágil, preciso e seguro, permitindo que empresas atendam às exigências de um ambiente cada vez mais digitalizado, enquanto reduzem o tempo necessário para validar e concluir transações importantes.

2.4. Público-Alvo e Segurança do Sistema

O público-alvo da solução são os presidentes e proprietários de entidades de tiro esportivo, que, de acordo com as novas normas, devem utilizar uma assinatura eletrônica certificada pelo padrão ICP-Brasil. Cordeiro (2008, p. 7) define o certificado digital como “um documento eletrônico que identifica pessoas e empresas no mundo digital, comprovando sua identidade.” Caso essa exigência não seja cumprida, o Exército Brasileiro não aceita os documentos anexados.

Para garantir a segurança, o acesso ao menu de assinaturas digitais é restrito e permitido apenas quando o cliente está logado no sistema, que utiliza autenticação em dois fatores (2FA), com um código enviado ao celular cadastrado do usuário. Além disso, somente usuários com acesso administrativo têm permissão para utilizar a área de assinaturas digitais, que inclui o anexo do certificado. Um campo adicional para senha é requerido durante o anexo do certificado, e, caso a senha esteja incorreta ou o campo esteja vazio, o sistema bloqueia o procedimento e exibe uma mensagem de erro.

O sistema é compatível exclusivamente com arquivos de certificado no formato .pfx. Caso um arquivo em outro formato seja anexado, o sistema impede o envio e emite uma mensagem de erro. Conforme Behrens (2007), o uso de assinaturas digitais em documentos eletrônicos oferece um meio de prova legalmente reconhecido para a existência de negócios jurídicos, reforçando a segurança e a confiança nos contratos eletrônicos.

3. Estado da Arte

Este capítulo apresenta um mapeamento sistemático, sobre a questão das assinaturas digitais. O objetivo deste estudo, é analisar se existe ferramentas que automatize esse processo dentro das empresas que utilizam os certificados digitais. A principal contribuição do estudo é levantar informações se já existem ferramentas que automatizam o processo de assinatura digital. A Seção 3.1 descreve as questões utilizadas dentro das pesquisas. 3.2 Apresenta as *strings* que foram utilizadas para a busca dos artigos já publicados. 3.3 Faz a análise dos artigos já encontrados. A Seção 3.4 apresenta a classificação dos artigos, e também a organização dos dados encontrados 3.5 relata as considerações finais do capítulo.

O mapeamento sistemático é uma metodologia no qual compreende uma pesquisa criteriosa na literatura, tendo como o maior objetivo avaliar a abrangência, o escopo e o volume de estudos publicados, geralmente referidos como estudos primários, dentro de um domínio específico de interesse (PETERSON et al., 2008).

3.1. Questões da Pesquisa

O objetivo da pesquisa teórica é encontrar respostas para questões essenciais relacionadas ao desenvolvimento do projeto, permitindo uma análise sobre a existência de estudos ou projetos semelhantes. Esse levantamento proporciona embasamento teórico, identificando soluções, desafios e práticas previamente exploradas que podem ser adaptadas ou aprimoradas no projeto atual.

As questões de pesquisa (QP) consideradas neste mapeamento são as seguintes:

- Q1: Quais são as tecnologias mais utilizadas para a automatização de assinaturas digitais nos últimos cinco anos?
- Q2: Quais são os requisitos mínimos de segurança para chaves criptográficas simétricas e chaves públicas, e como funciona o sistema criptográfico para proteger mensagens?
- Q3: Como funciona o sistema de chaves assimétricas em um certificado digital, e qual é o papel da chave pública na verificação das informações?

3.2. *Strings* de Busca

Para buscar os trabalhos acadêmicos, foi criado uma *string* com palavras chaves referente aos artigos. A busca foi realizada no *Google Scholar*[2], uma ferramenta utilizada justamente para esse tipo de pesquisa.

O Quadro 1 mostra quais as *strings* que foram utilizadas na busca pelos trabalhos:

Quadro 1 – *String* de Busca

String	Expressão
1	("assinatura digital" OR "icp-brasil" OR "certificado digital.

Fonte: O autor, 2024.

[2] https://scholar.google.com/

3.3. Análise dos Artigos

Para a análise e seleção dos artigos, foi estabelecido critérios de inclusão (CI) sendo:

- CI1: Artigos escritos em português.
- CI2: Artigos completos.
- CI3: Artigos referente a certificados digitais, infraestrutura de chaves públicas brasileiras, e automatização de processos de assinatura digital.
- CI4: Trabalhos publicados após 2001.

Os artigos que atenderem estes critérios, serão reavaliados sobre os critérios de exclusão (CE), trabalhos nos quais não atendam algum destes critérios são retirados do mapeamento. Sendo assim os critérios de exclusão adotados, foram:

- CE1: Artigos que não envolvam assinatura digital.
- CE2: Artigos duplicados.
- CE3: Artigos que possam ser visualizados de forma integral.

3.4. Classificação dos Artigos e Extração dos Dados

De acordo com a *string* de busca utilizadas, identificou-se um total de 15 artigos que possuem correlação com os temas de assinatura digital, certificado digital ou ICP-Brasil. Todos os artigos atendem aos critérios de inclusão estabelecidos para a pesquisa. Ao analisar o conteúdo dos artigos, constatou-se que nenhum aborda especificamente a automatização do processo de assinatura com o uso de certificados digitais. Porém trazem certas informações que também estão dentro do mesmo contexto.

A maioria dos artigos concentra-se em aspectos de segurança associados ao uso de certificados digitais, detalhando medidas de proteção e boas práticas para garantir a autenticidade e integridade das assinaturas digitais. Além disso, diversos artigos exploram e explicam as Infraestruturas de Chaves Públicas Brasileira (ICP-Brasil), abordando desde sua estrutura até o papel fundamental na garantia da segurança das transações digitais no país. Também foi identificado artigos que tratam

sobre a verificação da autenticidade e validade dos certificados digitais, destacando métodos e ferramentas para assegurar sua confiabilidade.

A partir dos trabalhos selecionados, serão respondidas as perguntas feitas previamente.

Q1: Quais são as tecnologias mais utilizadas para a automatização de assinaturas digitais nos últimos cinco anos?

Como não se identificaram trabalhos relacionados especificamente à automatização do processo de assinatura digital, não há uma linguagem específica recomendada para essa aplicação. Qualquer tecnologia capaz de integrar com APIs de terceiros pode ser utilizada nesse contexto. O fator decisivo é a adaptação da empresa desenvolvedora às ferramentas já existentes ou a uma tecnologia previamente definida. Em um dos artigos revisados, o processo de verificação da autenticidade do certificado foi desenvolvido em Java, uma escolha feita pela preferência do autor. No entanto, essa funcionalidade poderia ser implementada em diversas outras tecnologias, dependendo dos requisitos e do ambiente de desenvolvimento.

Q2: Quais são os requisitos mínimos de segurança para chaves criptográficas simétricas e chaves públicas, e como funciona o sistema criptográfico para proteger mensagens?

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT (2010), uma chave criptográfica simétrica é considerada segura quando possui pelo menos 128 bits. Já uma chave pública precisa ter no mínimo 1024 bits, enquanto chaves usadas em aplicações militares geralmente possuem 4096 bits. Esse nível de segurança exigiria milhares de anos de tentativa de força bruta (testando todas as combinações possíveis) para ser quebrado por um computador.

Um sistema criptográfico é definido como um conjunto de técnicas usadas para embaralhar ou cifrar mensagens, tornando-as aparentemente ilegíveis, de modo que seja possível recuperar a mensagem original a partir do texto cifrado (STALLINGS, 2007).

Q3: Como funciona o sistema de chaves assimétricas em um certificado digital, e qual é o papel da chave pública na verificação das informações?

Esse sistema pode ser comparado a um cadeado com duas chaves diferentes, porém conectadas: uma para trancar e outra para destrancar. Uma das chaves é usada para assinar o certificado digital, enquanto a outra permite verificar o certificado e, se necessário, decifrar a informação caso tenha sido previamente cifrada. A chave pública do signatário precisa estar presente no certificado digital para validar as informações no documento, podendo ser verificada na Infraestrutura de Chaves Públicas em uso (NAKAMURA, 2007).

3.5. Considerações Finais do Mapeamento Sistemático

Com base nas informações reunidas por meio do mapeamento sistemático, conclui que, atualmente, não existem soluções específicas voltadas exclusivamente para a automatização das assinaturas digitais. Embora a automatização desse processo ainda não seja amplamente abordada, constatou-se uma forte presença de estudos e iniciativas voltados para segurança e criptografia, aspectos fundamentais para garantir a confiabilidade das transações digitais.

Além disso, a criação da ICP-Brasil representou um avanço expressivo para a modernização das práticas de autenticação e segurança digital no país. A ICP-Brasil trouxe um padrão nacional confiável, promovendo maior proteção nas operações que exigem autenticidade e integridade de dados.

Assim, ainda que a automatização de assinaturas digitais não esteja plenamente desenvolvida, o Brasil tem avançado significativamente na construção de uma base segura para futuras inovações tecnológicas, especialmente em segurança e criptografia.

4. Metodologia

O projeto foi desenvolvido utilizando a combinação de tecnologias de *back-end* e *front-end*, incluindo PHP, Laravel, Angular e APIs de parceiros. A integração dessas ferramentas possibilitou a criação de uma plataforma automatizada para a assinatura digital de documentos. Segundo Moreno (2005), a assinatura digital envolve a cifração de um documento utilizando uma chave privada, cuja validade é verificada com a

chave pública correspondente. Esse processo assegura a autenticidade e a integridade do documento, uma vez que apenas o detentor da chave privada pode gerar o criptograma.

4.1. Tecnologias Utilizadas

Para atender à necessidade de automatização do processo de assinatura digital, diversas tecnologias de desenvolvimento web foram utilizadas, sendo o PHP, o Laravel e o Angular. Estas ferramentas se destacam por sua flexibilidade, robustez e capacidade de integração, facilitando a criação de aplicações escaláveis e seguras.

A linguagem de programação PHP (do inglês, *Pre-Hypertext Preprocessor*) foi utilizada em função da necessidade de uma dinâmica para escolha dos objetos a serem projetados na aplicação. O PHP é uma linguagem de programação interpretada, baseada em *scripts* para desenvolvimento de sistemas *web*. Sua sintaxe é semelhante à linguagem C, podendo ser mesclada ao código desenvolvido em HTML (*HyperText Markup Language*). Uma característica importante desta linguagem reside no fato desta ser *server side*, ou seja: é uma linguagem que executa no lado do servidor, deixando que o cliente faça apenas as requisições e receba as respostas em HTML. Segundo Niederauer (2004, p.21), “Quando você acessa uma página PHP por meio de seu navegador, todo código PHP é executado no servidor, e os resultados são enviados para o seu navegador”.

Laravel, como diz seu slogan *The PHP framework for Web Artisans*, é um *framework* PHP para artesãos (de *software*) e tem o sentido de levar a mensagem de que um artesão mistura a técnica com a arte. Laravel é uma ferramenta para criação de sistemas web complexos e completos. Gabardo (2017) afirma que em pouco tempo de prática com o *framework*, é nítido sua clareza e bom desenvolvimento além de ter um código limpo e elegante. O Laravel "é um *framework* PHP MVC sob o paradigma de orientação a objetos" (GABARDO, 2017). Ou seja, ele é baseado na linguagem PHP e tem sua arquitetura MVC - Model, View, Controller. De acordo com o relatório *State of PHP Frameworks* de 2024, Laravel é o *framework* PHP mais usado globalmente, sendo amplamente adotado para aplicações que exigem robustez e facilidade de manutenção.

Outro componente essencial para o desenvolvimento do sistema é o Angular, Segundo Santos (2017), O Angular é um *framework* bastante complexo que exige

conhecimentos técnicos prévios em WebPack, módulos Node.js, npm e TypeScript. Por essa razão, segundo o autor, a curva de aprendizado é aumentada pela combinação da complexidade da ferramenta com esses conhecimentos prévios, resultando em uma curva de aprendizado elevada. De acordo com o relatório *State of JavaScript* de 2022, o Angular continua entre os *frameworks front-end* mais utilizados, consolidando sua posição como uma das principais escolhas para aplicações modernas e escaláveis.

A combinação dessas tecnologias proporciona uma base sólida para o desenvolvimento de um sistema de assinatura digital automatizado, possibilitando alta escalabilidade, segurança e flexibilidade. Ao utilizar uma *stack* robusta e amplamente aceita no mercado, o projeto não só atende às necessidades imediatas de automatização e segurança, como também garante a sustentabilidade e a manutenção do sistema a longo prazo.

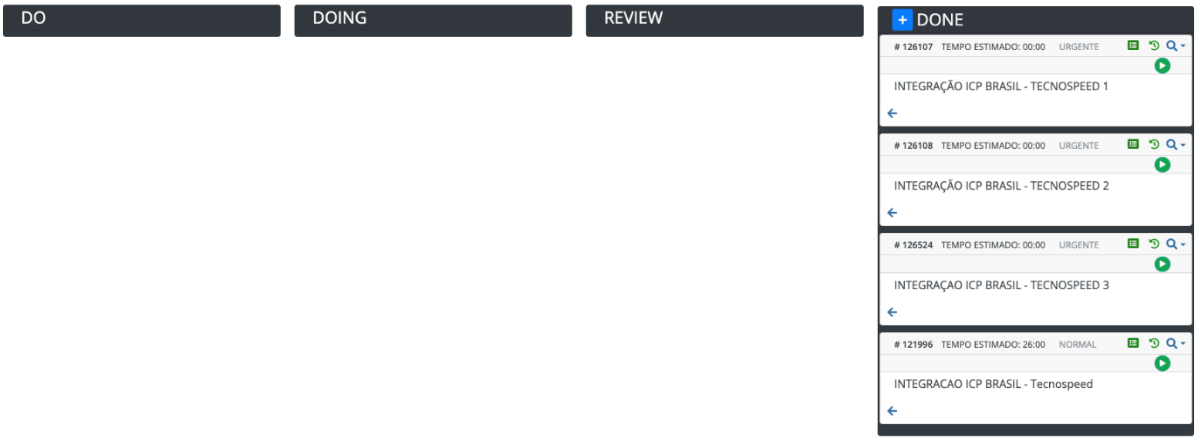
Além destas linguagens, também foi utilizado Python, que nos auxilia na criação da API para busca do marcador dentro do documento gerado. O Python é uma das linguagens de programação que mais tem crescido, graças à sua compatibilidade ampla (funciona na maioria dos sistemas operacionais) e à sua capacidade de integrar-se e colaborar com outras linguagens. Programas como Dropbox, Reddit e Instagram são escritos em Python, com a ferramenta *Jupyter* é possível realizar várias tarefas em um curto espaço de tempo, e em apenas uma compilação (BARRO, 2022). É uma linguagem de programação recomendada por ser interpretada, orientada a objetos, de alto nível e com semântica dinâmica, o que a torna ideal para a automatização de processos. A simplicidade reduz a necessidade de manutenção de um programa e aumenta a facilidade de ser realizada, suporta módulos pacotes, que encoraja a programação modularização e reuso de código.

Para o armazenamento de informações foi utilizado o Banco de Dados MySql. O MySQL é um dos bancos de dados relacionais de código aberto mais conhecidos do mundo. Essa popularidade é resultado de seu uso generalizado em sites de comércio eletrônico, mídias sociais e aplicativos, entre eles o Drupal, Joomla, Magento e o WordPress. Ele também é parte essencial da amplamente utilizada pilha de aplicativos da Web Linux-Apache-MySQL-PHP/Perl/Python (LAMP) , que serve de base para muitos aplicativos, sites e serviços conhecidos. Além disso, é classificado como o segundo banco de dados mais usado no mundo, pelo DB-Engines. (GOOGLE CLOUD, 2024)

4.2. Metodologia ágil

A metodologia ágil escolhida para o desenvolvimento do sistema de automatização de assinaturas digitais foi o Kanbam ilustrado na Figura 1. Na obra de Martins (2006), o autor afirma que o Kanban desempenha funções específicas dentro do processo de produção, como visibilidade (em que a informação e o fluxo de materiais são combinados e se deslocam com os componentes) e produção (controlando os estágios da produção ao indicar o tempo, a quantidade e o tipo de componente a ser produzido).

Figura 1 - Quadro Kanban



Fonte: O Autor, 2024.

A utilização da metodologia ágil foi fundamental para o desenvolvimento do sistema de automatização de assinaturas digitais, promovendo um foco em entregas contínuas e incrementais. Essa abordagem permitiu uma adaptação rápida às necessidades dos usuários e ajustes constantes durante todo o processo de desenvolvimento, facilitando a incorporação de feedbacks e a resposta a novas exigências. A metodologia ágil viabilizou uma colaboração próxima entre a equipe de desenvolvimento e os stakeholders, assegurando que o sistema evoluísse conforme as necessidades operacionais e de negócio.

5. Resultados e Discussões

Este tópico tem como objetivo apresentar os resultados obtidos durante o desenvolvimento da aplicação web de automatização de assinaturas digitais.

5.1. Banco de Dados MySql

Para o armazenamento de dados, foi utilizado o Banco de Dados MySql, com uma estrutura que comporte todas as informações que seriam utilizadas durante todo o processo.

Figura 2 – Diagrama do Banco de Dados

Fonte: O Autor, 2024.

Como demonstrado na Figura 2, a estrutura foi projetada para armazenar informações essenciais a serem utilizadas ao longo de todo o processo. O campo *user_id* é utilizado para identificar o certificado anexado, sendo essencial na etapa de assinatura. As colunas *name*, *password* e *path* são preenchidas na tela de anexo do certificado. Já os campos *site_email* e *site_password* são atualizados com base na resposta da API. Essas informações são armazenadas por questões de segurança, já que o usuário não precisa acessá-las diretamente. Para finalizar, os campos padrões *id*, *created_at*, *updated_at* e *deleted_at* são utilizados como auxiliares e identificadores, garantindo a integridade e rastreabilidade dos dados.

5.2. Desenvolvimento da Interface do Usuário

A interface foi projetada para proporcionar ao cliente uma experiência simplificada e eficiente, permitindo que, com apenas alguns cliques, ele possa anexar e configurar seu certificado digital para uso imediato. Um menu dedicado à gestão de certificados facilita esse processo, centralizando em uma única área todas as ações necessárias, desde o anexo do arquivo .pfx até a validação das informações de segurança, como a senha do certificado.

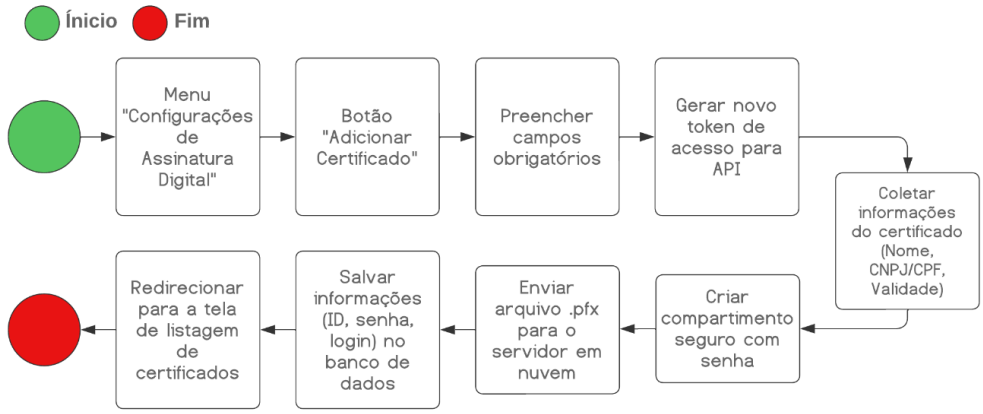
Esse *design* minimiza etapas e reduz a necessidade de treinamento ou suporte adicional, uma vez que o cliente segue o mesmo fluxo que já utiliza para gerar documentos, agora com a funcionalidade adicional de assinatura digital integrada. Assim, ele pode manter seu processo habitual de criação de documentos, com a segurança de que as assinaturas estão em conformidade com as exigências regulatórias.

Desenvolvida com foco na eficiência e praticidade, a interface garante ao usuário uma transição ágil e intuitiva, permitindo que ele se concentre em suas tarefas principais enquanto o sistema gerencia os aspectos técnicos da assinatura digital.

5.2.1. Fluxo de Adição de Certificado

O fluxo apresentado na Figura 3 ilustra as etapas de configuração do certificado digital no sistema. O usuário acessa o menu "Configurações de Assinatura Digital" e seleciona "Adicionar Certificado". Em seguida, ele preenche os campos obrigatórios, como nome e senha, e um novo token de acesso à API é gerado. As informações do certificado, incluindo nome, CNPJ/CPF e validade, são coletadas e armazenadas de forma segura em um compartimento protegido com senha.

Figura 3 - Fluxo de Adição de Certificado



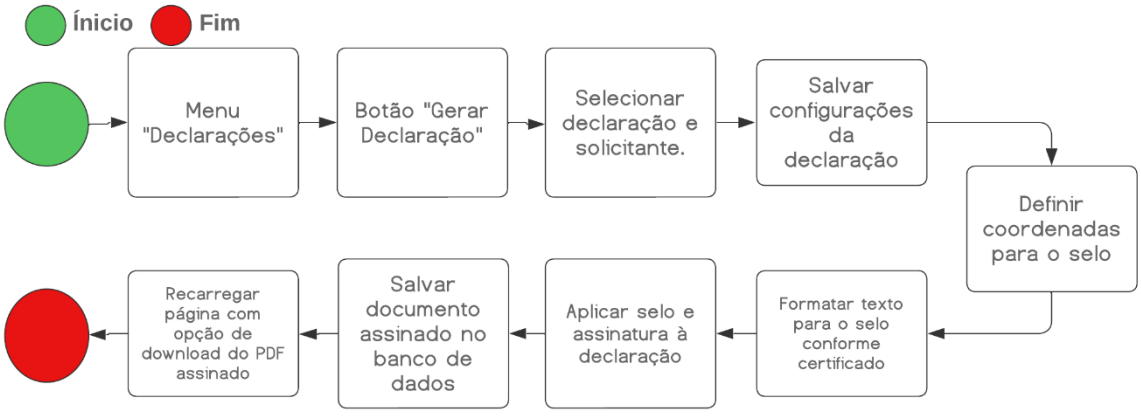
Fonte: O Autor, 2024.

O arquivo .pfx é enviado para o servidor em nuvem, e todos os dados, como ID do compartimento, senha e login, são registrados no banco de dados. Após a conclusão desse processo, o usuário é redirecionado para a tela de listagem de certificados, onde pode visualizar e gerenciar os certificados configurados.

5.2.2. Fluxo de Assinatura de Documentos

O segundo fluxo apresentado na Figura 4, detalha o processo de geração e assinatura de uma declaração no sistema. O usuário acessa o menu "Declarações" e seleciona a opção "Gerar Declaração".

Figura 4 - Fluxo de Assinatura de Documentos



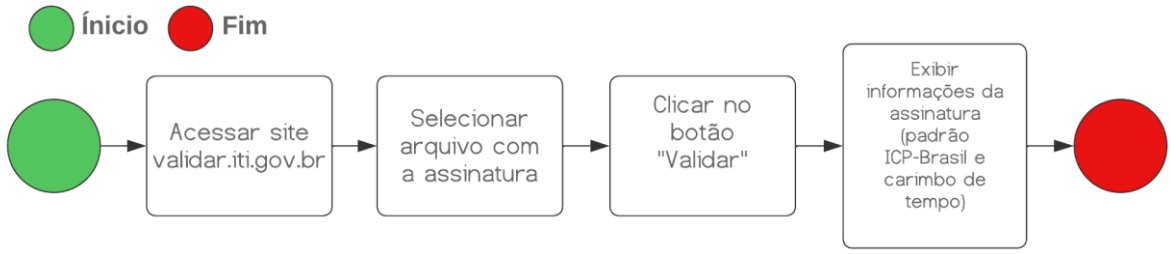
Fonte: O Autor, 2024.

Em seguida, define os parâmetros desejados, incluindo a posição do selo de autenticação e a formatação do texto conforme as informações do certificado digital. O selo e a assinatura são então aplicados ao documento, que é salvo no banco de dados. Após a finalização, o documento assinado é disponibilizado para *download* quando a página é recarregada.

5.2.3. Validação da Assinatura

Para validar a assinatura digital, o cliente deve acessar o site oficial do governo destinado à verificação de assinaturas digitais, disponível em validar.iti.gov.br. No site, o cliente seleciona o arquivo do documento assinado que deseja verificar. Em seguida, o sistema processa o arquivo e exibe todos os detalhes relevantes sobre a assinatura digital, incluindo informações de autenticidade, validade do certificado, identidade do signatário e carimbo de tempo, conforme os padrões estabelecidos pelo ICP-Brasil.

Figura 5 - Fluxo de Validação da Assinatura



Fonte: O Autor, 2024.

De acordo com a Figura 5, esse processo de validação é essencial para garantir que o documento não foi adulterado após a assinatura e que a identidade do assinante é legítima e certificada. Ao visualizar as informações de autenticidade e conformidade no site oficial, o cliente pode ter plena confiança de que o documento possui validade jurídica e está de acordo com as normas de segurança e integridade requeridas. Essa etapa reforça a confiança nos documentos digitais e é especialmente importante para processos que exigem alto nível de segurança, como transações contratuais e documentos oficiais.

5.3. Integração com a API *PlugSign*

A integração com a API PlugSign inicia-se quando o usuário pressiona o botão de salvar na área de anexo do certificado. Após as validações necessárias — confirmação da senha, verificação do formato .pfx e preenchimento completo dos campos —, as informações são enviadas por meio de rotas que fornecem os dados necessários para realizar a assinatura digital durante a geração dos documentos.

A primeira rota acionada cria o perfil da empresa no *software house*, representando as entidades de tiro esportivo. Em seguida, a segunda rota cria o usuário responsável pelo certificado, geralmente o proprietário ou presidente da entidade, utilizando tanto os dados do login quanto as informações preenchidas no momento do anexo do certificado. Assim, o usuário é configurado com seu certificado pronto para uso em documentos gerados.

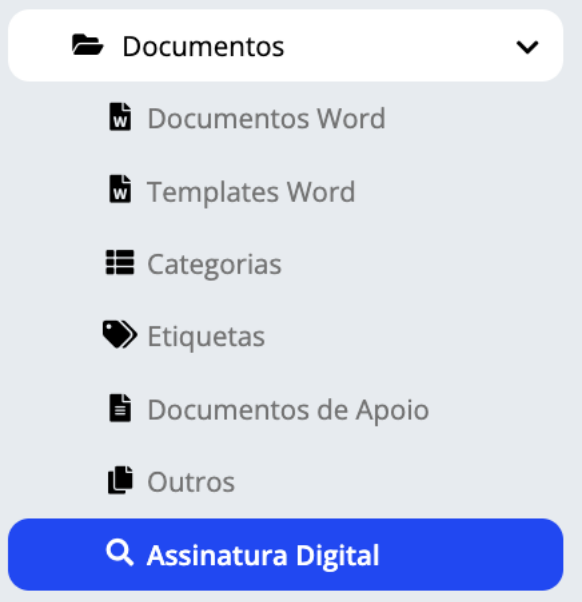
Por fim, a última rota é acionada durante a assinatura do documento. Nesse ponto, o sistema envia o usuário e o arquivo do documento que ele deseja assinar. A API retorna o documento assinado, que é convertido em PDF e disponibilizado para *download*.

5.4. Funcionalidades do Sistema e Telas de Interface

Para incorporar a funcionalidade de assinatura digital ao sistema, foi desenvolvido um menu específico que facilita a configuração e o gerenciamento de certificados. Esse menu intuitivo permite que o usuário navegue diretamente para a seção de certificação, onde é possível adicionar, visualizar e administrar certificados de forma centralizada e organizada.

A interface foi projetada com clareza e acessibilidade, tornando o processo simples e direto para o cliente. Todas as ações relacionadas à assinatura digital, desde o upload do certificado até a verificação de autenticidade, estão centralizadas nesse menu apresentado na Figura 6, o que garante uma experiência de uso fluida e eficiente. Dessa forma, os clientes podem configurar e administrar seus certificados rapidamente, atendendo com facilidade aos requisitos regulamentares, como o padrão ICP-Brasil, e aos requisitos operacionais do sistema.

Figura 6 - Menu de configuração e gerenciamento de certificados digitais no sistema.



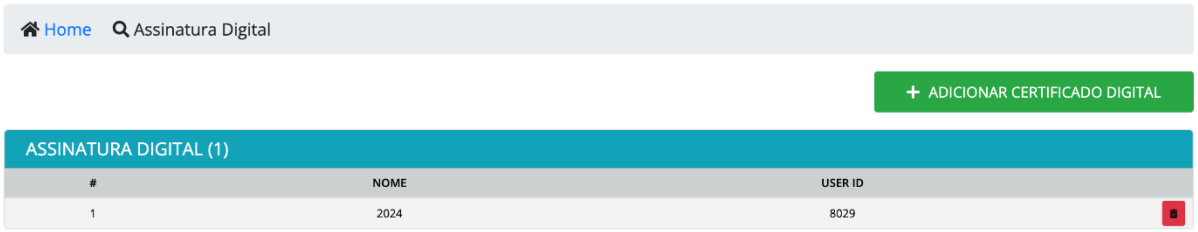
Fonte: O Autor, 2024.

Além disso, o menu permite que o cliente acompanhe o *status* dos certificados e visualize documentos já assinados, fornecendo maior controle e segurança. Essa abordagem contribui para a eficiência do processo e minimiza a necessidade de suporte adicional, uma vez que o sistema guia o usuário em cada etapa, desde o anexo do certificado até a assinatura dos documentos.

5.4.1. Tela de Listagem de Certificados.

A tela de listagem de certificados demonstrada na Figura 7, foi projetada para oferecer uma experiência simples e intuitiva aos clientes. Ao selecionar o menu "Assinatura Digital", o cliente é automaticamente direcionado para essa tela inicial, onde todos os certificados anexados ao sistema são exibidos de maneira organizada. A interface apresenta informações essenciais para facilitar a identificação dos certificados, como o apelido atribuído pelo cliente, um identificador exclusivo no sistema e o identificador fornecido pela API. Esses dados permitem que o cliente reconheça rapidamente cada certificado e gerencie seu uso conforme necessário.

Figura 7 - Tela de Listagem de Certificados



Fonte: O Autor, 2024.

Além disso, a tela conta com um botão de exclusão, que permite ao cliente remover certificados indesejados ou desatualizados. Essa funcionalidade fornece flexibilidade e controle sobre os certificados armazenados, permitindo que o cliente realize atualizações ou exclusões de forma prática e segura, atendendo aos requisitos operacionais e de segurança do sistema.

5.4.2. Tela de Adição de Certificado

Na seção de adição de certificados demonstrado na Figura 8, são apresentados três campos fundamentais para o registro de um novo certificado digital. O primeiro campo é o "Nome", onde o cliente pode inserir um apelido personalizado para facilitar a identificação do certificado no sistema. Esse recurso auxilia o usuário a distinguir rapidamente entre diferentes certificados, caso possua mais de um. Em seguida, há o campo "Senha", onde deve ser inserida a senha do certificado, essencial para garantir a segurança do processo de autenticação.

Figura 8 - Tela de Adição de Certificado

Fonte: O Autor, 2024.

Por fim, o campo "Arquivo" permite que o usuário anexe o arquivo .pfx, correspondente ao seu certificado digital. Esse arquivo contém a chave privada necessária para a assinatura digital, assegurando a conformidade com os padrões de segurança exigidos pelo ICP-Brasil. A interface foi projetada para tornar esse processo o mais intuitivo possível, guiando o cliente em cada etapa de forma prática e direta.

5.4.3. Assinatura de Documentos

Após o usuário selecionar o documento que deseja assinar, o processo é iniciado por meio de uma rota de API desenvolvida para identificar a posição exata onde o selo de assinatura deve ser inserido. Essa API foi implementada em Python, utilizando a biblioteca *pdfplumber*, que permite extrair o conteúdo do PDF e convertê-lo em texto. Com os dados do documento convertidos em *strings*, o sistema executa um *loop* de busca no conteúdo textual, procurando por um marcador específico que atua como referência para a inserção do selo.

Figura 9 - Rota de API para identificação da posição do selo de assinatura.

```python
# Função para encontrar o marcador no PDF usando pdfplumber
def encontrar_marcador_pdfplumber(pdf_stream, marcador):
    coordenadas = []

    # Abrir o PDF usando pdfplumber
    with pdfplumber.open(pdf_stream) as pdf:
        for page_num, page in enumerate(pdf.pages):
            text = page.extract_text()

            # Verifica se o marcador existe na página
            if marcador in text:
                # Extrair todas as palavras e suas coordenadas
                for word in page.extract_words():
                    if marcador in word['text']:
                        coordenadas.append({
                            'pagina': page_num + 1,
                            'x': word['x0'],
                            'y': word['top']
                        })
                        break  # Parar ao encontrar o marcador

    return coordenadas
```

Fonte: O Autor, 2024.

Como mostra a Figura 9, esse marcador facilita a localização da área destinada ao selo, permitindo que a API retorne uma coordenada aproximada para posicioná-lo de maneira precisa e automatizada. Com base nessas coordenadas, o selo é inserido no local apropriado dentro do documento, garantindo que a assinatura digital esteja corretamente posicionada e visível, de acordo com os requisitos de validação e conformidade do sistema.

Com as coordenadas obtidas, o sistema permite que o arquivo seja enviado para assinatura como demonstra a Figura 10, especificando o local exato onde o selo de assinatura deve ser exibido no documento. Dessa forma, a assinatura digital é inserida de maneira precisa, garantindo que o posicionamento esteja de acordo com as diretrizes visuais e regulatórias do sistema, proporcionando ao usuário uma experiência automatizada e segura.

Figura 10 - Rota de Envio de Requisição para a API de Assinatura

```
// Enviar a requisição para a API de assinatura
$responseSignFile = $client->post(
    Config::get('app.digitalSignatureAddress') . '/files/sign', [
        'headers' => [
            'Authorization' => 'Bearer ' . $clubCms->token_assinatura_digital,
            'Accept' => 'application/json',
        ],
        'json' => [
            'document_key' => $documentKey,
            'user_id' => $digitalSignature->user_id,
            'page' => $coordenadas['coordenadas'][0]['pagina'],
            'xPos' => $xPos,
            'yPos' => $yPos,
        ],
    ]
);

$responseDownloadFile = $client->get(
    Config::get('app.digitalSignatureAddress') . '/files/download/' . $documentKey, [
        'headers' => [
            'Authorization' => 'Bearer ' . $clubCms->token_assinatura_digital,
            'Accept' => 'application/json',
        ],
    ]
);
```

Fonte: O Autor, 2024.

Após o retorno das informações, o cliente pode acessar imediatamente o documento assinado, disponível para *download*. Esse processo ágil e automatizado

garante que o documento esteja pronto para uso, com a assinatura digital corretamente aplicada e validada, oferecendo ao cliente uma experiência prática e eficiente.

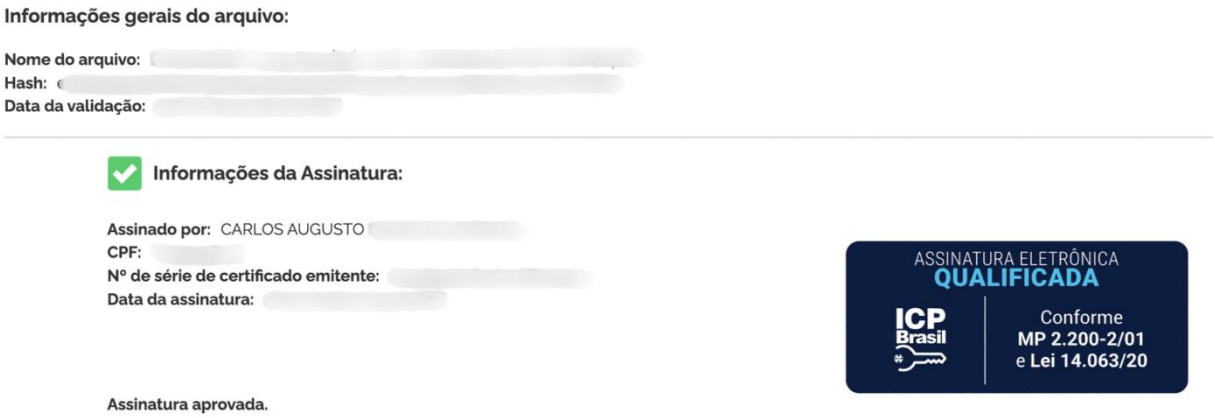
Figura 11 - Exemplo de Selo Gerado com a Assinatura Validada

Fonte: O Autor, 2024.

5.4.4. Tela de Validação de Assinatura

A verificação da assinatura digital é realizada diretamente no site oficial do governo brasileiro. O usuário deve primeiro baixar o arquivo PDF assinado, disponibilizado pelo sistema, e, em seguida, fazer o upload no site https://validar.iti.gov.br/ como é demonstrado na Figura 12.

Figura 12 - Tela de Verificação da Assinatura



Fonte: O Autor, 2024.

O sistema do governo executará a validação da assinatura, confirmando se ela está aprovada e se atende às qualificações do padrão ICP-BRASIL, garantindo a autenticidade e a conformidade do documento de acordo com as exigências legais.

5.5. Análise dos Resultados

Após a implementação do sistema de automatização de assinaturas digitais, foi realizada uma pesquisa de satisfação com os usuários da plataforma para avaliar a eficiência, segurança e usabilidade da solução, além de medir seu impacto na redução de erros manuais e no aumento da produtividade nas empresas. A pesquisa contou com a participação de 21 usuários, todos representantes de empresas que integraram o sistema em seus processos documentais.

O resultado desta pesquisa foi: todos os 21 respondentes atribuíram uma avaliação positiva ao sistema, selecionando a opção "Satisfeito" quanto à experiência geral de uso. Esse *feedback* positivo demonstra que a solução atendeu plenamente às expectativas dos usuários, proporcionando uma experiência prática, segura e eficiente na assinatura digital de documentos. A avaliação positiva também ressalta o valor do sistema na otimização dos fluxos documentais e na conformidade com as exigências regulatórias.

O gráfico gerado a partir dessas respostas reflete essa unanimidade, com 100% dos participantes classificando sua experiência como "Satisfeito." Esses resultados permitem concluir que a automatização do processo de assinatura digital trouxe benefícios claros, particularmente em termos de economia de tempo e eliminação de falhas recorrentes nos métodos manuais.

Figura 13 - Dados coletados referente a satisfação do cliente com o serviço de assinatura criado.

Fonte: O Autor, 2024.

De acordo com a Figura 13, a resposta unânime indica sinais de sucesso da implementação. Além de reduzir o tempo necessário para a assinatura e validação de documentos, a plataforma oferece aos usuários um ambiente digital seguro, onde todos os processos podem ser gerenciados de forma intuitiva e eficiente. Com base nesses resultados, é possível afirmar que o sistema de automatização de assinaturas digitais trouxe avanços significativos para as empresas que o adotaram, modernizando seus fluxos documentais e garantindo a confiabilidade e a conformidade das assinaturas digitais.

6. Considerações Finais

O desenvolvimento deste projeto de automatização de assinaturas digitais trouxe avanços expressivos para a eficiência, segurança e confiabilidade dos processos documentais, especialmente para empresas que necessitam gerenciar um grande volume de assinaturas eletrônicas. A integração de tecnologias como PHP, Angular, Laravel, Python e APIs de parceiros mostrou-se uma solução robusta e eficaz, proporcionando uma significativa redução no tempo necessário para a validação de documentos e aprimorando a experiência do usuário por meio de uma interface intuitiva e processos simplificados.

A automatização demonstrou ser uma ferramenta valiosa na minimização de erros manuais, anteriormente comuns nos métodos tradicionais que exigiam

impressão, assinatura física e digitalização de documentos. Este novo modelo não só elimina etapas manuais, como também aumenta a confiabilidade do processo, garantindo que os documentos assinados digitalmente atendam aos requisitos legais do ICP-Brasil. Dessa forma, o sistema promoveu um aumento considerável na produtividade das empresas usuárias, permitindo um gerenciamento mais ágil e seguro dos fluxos documentais.

Outro benefício significativo foi o aumento da confiança dos clientes em relação à validade jurídica das assinaturas, uma vez que o sistema permite a verificação direta das assinaturas no site oficial do governo brasileiro. Essa segurança adicional fortalece a credibilidade das empresas, protegendo contra fraudes e garantindo a integridade dos documentos assinados.

O sucesso desta implementação abre novas perspectivas para aprimoramentos e expansões futuras. Recomenda-se, para os próximos desenvolvimentos, explorar o suporte a múltiplos tipos de certificados digitais, ampliando a plataforma para atender a uma maior variedade de cenários empresariais. A integração com novas APIs de assinatura digital também pode expandir o alcance da solução, permitindo sua adaptação a mercados internacionais ou a empresas que utilizam diferentes padrões de certificação.

Essa solução pode ser aplicada em qualquer outra plataforma, desde que o documento que precisa ser assinado já tenha sido gerado anteriormente. Ou seja, o processo pode ser adaptado para diversos tipos de sistemas ou ambientes, sendo necessário apenas que o arquivo digital do documento esteja disponível para ser assinado. Com isso, a flexibilidade da solução permite que ela seja utilizada em diferentes contextos e plataformas, proporcionando uma alternativa eficiente e prática para a assinatura de documentos em formato digital.

Por fim, a inovação proporcionada por este projeto não apenas moderniza os processos internos das empresas, mas também representa um avanço significativo na transformação digital de rotinas corporativas que, por muito tempo, dependeram de métodos manuais. A implementação desta solução reafirma o potencial da tecnologia para otimizar processos, melhorar a segurança e criar ambientes empresariais mais eficientes e confiáveis.

Referências

ASS TECNOLOGIA. **Certificado Digital**. 2012. Disponível em: http://www.asstecnologia.com.br/blog/?p=2232. Acesso em: 9 dez 2024.

BEHRENS, Fabiele. **Assinatura eletrônica & negócios jurídicos**. Curitiba: Juruá, 2007. P.63.

BARRO, Bruna B. **As 10 Linguagens de Programação Mais Usadas em 2022: Aprimore suas Habilidades em Desenvolvimento Web**. Disponível em: https://www.hostinger.com.br/tutoriais/linguagens-de-programacao-mais-usadas#:~:text=1.-,Python,desenvolvimento%2C%20prototipa%C3%A7%C3%A3o%20e%20automa%C3%A7%C3%A3o%20web. Acesso em: 03 nov. 2024

CORDEIRO, Luiz Gustavo. Certificação digital: conceitos e aplicações; modelo brasileiro e australiano. Rio de Janeiro: Ciência Moderna, 2008.

GABARDO, A. C. **Laravel para Ninjas.** 1. ed.. ed. [S.l.]: Novatec Editora Ltda, 2017. ISBN 9788575226063.

GALUCCI. **Certificação Digital**. 2024. Disponível em: https://www.galucci.srv.br/certificado-digital. Acesso em: 9 dez 2024.

GOOGLE CLOUD. **O que é o MySql?**. 2024. Disponível em: https://cloud.google.com/mysql?hl=pt-BR. Acesso em: 9 dez 2024.

ITI. Instituto Nacional de Tecnologia da Informação**. ICP-Brasil** 2020. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/perguntas-frequentes/icp-brasil . Acesso em: 09 dez 2024

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Uso da Assinatura Eletrônica GOV.BR cresce 203% em 2023**. 2023. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/setembro/uso-da-assinatura-eletronica-gov-br-cresce-203-em-2023#:~:text=Implantada%20em%202020%2C%20o%20uso,ano%20passado%2C%20foram%2017%20milh%C3%B5es. Acesso em: 18 set. 2024

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. 1.ed. São Paulo: Novatec Editora Ltda., 2005.

MARTINS, G; LAUGENI, F. P. **Administração da produção**–2.ed.rev.aum. E atual. São Paulo: Saraiva, 2006.

MORAES, C. C.; CASTRUCCI, P. L. **Engenharia de Automação Industrial**. Editora LTC. 2. ed. Rio de Janeiro, 2007.

NIEDERAUER, J. (2004) Desenvolvimento de Websites com PHP: aprenda a criar Websites dinâmicos e interativos com PHP e banco de dados. São Paulo: Novatec.

NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos.** 1ª ed. São Paulo: Novatec Editora. 2007.

PETERSON, K., Feldt, R., Mujtaba, S. and Mattsson, M. (2008) Systematic mapping studies in software engineering. In Proceedings of the international conference on Evaluation and Assessment in Software Engineering, 68-77.

PEREIRA, S. R. **O sistema criptográfico de chaves públicas RSA**. Dissertação apresentada à Universidade Católica de Santos, UNISANTOS. 2008.

QUALISIGN. **Conceito de assinatura digital**. 2005-2017. Disponível em: https://www.qualisign.com.br/assinatura-digital. Acesso em: 9 dezembro 2024.

RIBEIRO, M. A. **Automação Industrial:** 4. Ed. Salvador: Tek Treinamento & Consultoria Ltda, 1999.

STALLINGS, W. **Criptografia e segurança de redes**. 4ª edição Ed. Prentice Hall, 2007.

State of JavaScript (2022). **The State of JavaScript 2022 Report**. Disponível em: https://2022.stateofjs.com/en-US/libraries/front-end-frameworks/. Acesso em: 23 out. 2024

SANTOS, Daniel. **Tabela de comparação entre Angular, React + Redux e Vue.js**. 2017. Disponível em: https://medium.com/@daniel.dia/compara%C3%A7%C3%A3o-entre-angular-react-reduxe-vue-js-a256d0fce8e0. Acesso em: 03 nov. 2024.

The Best PHP Frameworks for 2024. 2024. Disponível em: https://www.sitepoint.com/best-php-frameworks/. Acesso em: 23 out. 2024

TURBAN, E.; MCLEAN, E; WETHERBE, J. Tecnologia da Informação para Gestão: Transformando os Negócios na Economia Digital. Porto Alegre: Bookman, 2004.

VOLPI, M. M. **Assinatura digital: aspectos técnicos, práticos e legais**. Rio de Janeiro: Axcel Books do Brasil, 2001.