FACULDADE VIASAPIENS – FVS
CURSO DE BACHARELADO EM ADMINISTRAÇÃO

MARÍLIA GABRIELA RICARDO DE LIMA RODRIGUES

IMPACTOS DA CERTIFICAÇÃO DIGITAL NA GESTÃO DE IDENTIDADES E SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS BRASILEIRAS

TIANGUÁ-CE
2025

MARÍLIA GABRIELA RICARDO DE LIMA RODRIGUES

IMPACTOS DA CERTIFICAÇÃO DIGITAL NA GESTÃO DE IDENTIDADES E SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS BRASILEIRAS

Artigo apresentado à banca examinadora da Faculdade ViaSapiens, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientador: Profº Me. Francisco Alves de Souza Neto, Me.

TIANGUÁ-CE

2025

Ficha catalográfica

Dados Internacionais de Catalogação na Publicação
Ficha catalográfica elaborada pela Biblioteca da Faculdade ViaSapiens
com os dados fornecidos pelo(a) autor(a)

353i de Lima Rodrigues, Marília Gabriela Ricardo.
IMPACTOS DA CERTIFICAÇÃO DIGITAL NA GESTÃO DE IDENTIDADES E SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS BRASILEIRAS: / Marília Gabriela Ricardo de Lima Rodrigues - 2025.
28 f.

Trabalho de Conclusão de Curso (graduação) - Faculdade ViaSapiens, Bacharelado em Administração, . 2025
Orientação: Prof(a) Me. Prof. Francisco Alves de Souza Neto
1. Certificação Digital. 2. Segurança da Informação. 3. e-CPF. 4. e-CNPJ. 5. Eficiência Digital. I. Título.

CDD 342.81

FACULDADE ViaSapiens
A IDENTIDADE DO CONHECIMENTO

RODRIGUES
Acadêmico

MARÍLIA GABRIELA RICARDO DE LIMA RODRIGUES

IMPACTOS DA CERTIFICAÇÃO DIGITAL NA GESTÃO DE IDENTIDADES E SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS BRASILEIRAS

Artigo apresentado à Faculdade ViaSapiens, como exigência parcial para a obtenção do título de Bacharel em Administração.

Aprovado em: 08 / 12 / 25 .

BANCA EXAMINADORA:

Orientadora: Profº Me. Francisco Alves de Souza Neto

Membro: Profª Esp. Alaide Mara de Albuquerque Sá

Membro: Prof. Esp. João Harlley de Menezes Vasconcelos

AGRADECIMENTO

Gostaria de expressar minha profunda gratidão ao Professor Francisco Alves de Souza Neto, orientador deste trabalho, pelo apoio, orientação e pelos valiosos ensinamentos durante todo o desenvolvimento deste estudo. Sua paciência, dedicação e comprometimento foram fundamentais para o sucesso desta pesquisa.

Agradeço também aos membros da banca examinadora, cuja contribuição foi imprescindível para o aprimoramento deste trabalho.

Minha sincera gratidão aos meus familiares e amigos, que sempre me incentivaram e estiveram ao meu lado nos momentos de desafios e conquistas. A todos que, de alguma forma, contribuíram para a realização deste trabalho, deixo o meu muito obrigado.

Agradeço à Faculdade ViaSapiens por oferecer os recursos necessários para a realização de meus estudos e pesquisas, além de proporcionar um ambiente acadêmico enriquecedor.

RESUMO

Este estudo tem como objetivo analisar os impactos da certificação digital na gestão de identidades e na segurança da informação nas empresas brasileiras, focando na autenticação de usuários e na proteção de dados sensíveis. O problema de pesquisa aborda como a certificação digital contribui para a segurança das informações empresariais e quais desafios limitam sua adoção e utilização efetiva no Brasil. O objetivo geral é examinar o papel da certificação digital na promoção de segurança e eficiência nas transações digitais, além de identificar os principais desafios e oportunidades que essa tecnologia oferece no cenário brasileiro. A metodologia utilizada é qualitativa, com uma revisão bibliográfica exploratória e descritiva, baseada em artigos acadêmicos, livros e documentos técnicos, selecionados de acordo com critérios de relevância e atualidade. A análise de conteúdo foi aplicada para interpretar criticamente os dados coletados, permitindo uma visão aprofundada do impacto dessa tecnologia. Os resultados demonstram que a certificação digital, com o uso de ferramentas como e-CPF e e-CNPJ, facilita a autenticação segura de identidades, garante a integridade das informações e reduz custos operacionais, além de aumentar a agilidade dos processos administrativos. No entanto, identificam-se desafios significativos, como a complexidade dos processos de implementação, a falta de capacitação técnica adequada e a baixa conscientização dos usuários. Conclui-se que a certificação digital tem a fundamental relevância para a segurança da informação e a modernização das operações empresariais, mas sua adoção plena ainda depende de ações que visem a disseminação do conhecimento e a simplificação dos processos.

Palavras-chaves: Certificação Digital; Segurança da Informação; e-CPF. e-CNPJ; Eficiência Digital.

ABSTRACT

This study aims to analyze the role of digital certification in promoting security and efficiency in digital transactions in Brazil, identifying the main challenges and opportunities associated with this technology. The methodology adopted was qualitative, based on a literature review of relevant documents and academic articles, including contributions from Monteiro and Mignoni (2007), Martini (2008), and Moreira (2009). The data analysis was conducted using content analysis techniques, allowing for critical interpretation and identification of relevant patterns. The main results indicate a growing adoption and use of digital certificates, such as e-CPF and e-CNPJ, which have facilitated the secure authentication of identities and document management. These certificates provide significant advantages, such as operational cost reduction, process agility, and the reliability of online operations. However, the research reveals that the expansion of these technologies faces challenges, such as the need for greater public awareness and the complexity of implementation processes. It concludes that digital certification is a crucial component for the security and modernization of business and government operations in Brazil. Nonetheless, to fully realize its potential, it is necessary to overcome challenges related to public awareness and the simplification of adoption processes. The research contributes to the understanding of the underlying technologies of digital certification and its practical applications, highlighting the importance of this tool in the digital era. The study's limitations include the absence of empirical data and a limited focus on specific technical aspects of digital certificate implementation. Future research should include empirical studies to assess user perceptions and explore the impact of digital certification in specific sectors, such as finance and government.

Keywords: Digital Certification; Information Security; e-CPF. e-CNPJ; Digital Efficiency.

LISTA DE QUADROS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A certificação digital emergiu como uma ferramenta importante para garantir a autenticidade e integridade das informações em um ambiente digital cada vez mais prevalente. Com o crescimento das transações eletrônicas, a demanda por métodos seguros para proteger dados e validar identidades tornou-se imprescindível. A tecnologia de certificação digital, que se baseia na utilização de chaves criptográficas públicas e privadas, oferece uma camada adicional de segurança e confiança, salutar para operações em contextos virtuais. Nesse cenário, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) desempenha um papel fundamental na regulação e auditoria da emissão de certificados digitais, conforme destacado por Alecrim (2016).

O problema de pesquisa deste estudo está relacionado à necessidade de aprofundar a compreensão sobre os impactos e desafios inerentes à implementação e utilização da certificação digital no Brasil. Apesar dos diversos benefícios, como a redução de custos operacionais e a celeridade nos processos administrativos e comerciais, persistem obstáculos significativos, incluindo a complexidade técnica e a falta de conscientização acerca dessas tecnologias. O objetivo geral desta pesquisa é analisar o papel da certificação digital na promoção de segurança e eficiência nas transações digitais, bem como identificar os principais desafios e oportunidades apresentados por essa tecnologia no cenário brasileiro.

A abordagem metodológica adotada é de caráter qualitativo, com ênfase em uma revisão bibliográfica. A análise foi realizada a partir de uma seleção criteriosa de documentos e artigos acadêmicos relevantes, com destaque para as contribuições de Monteiro e Mignoni (2007), Martini (2008) e Moreira (2009), que exploram os aspectos técnicos e legais da certificação digital. A coleta de dados ocorreu entre os meses de março e setembro de 2024, utilizando-se de fontes acadêmicas e bases de dados especializadas. A análise dos resultados foi conduzida através da técnica de análise de conteúdo, permitindo uma interpretação crítica e a identificação de padrões relevantes.

Os resultados indicam uma crescente adoção e uso de certificados digitais, como o e-CPF e o e-CNPJ, que têm facilitado a autenticação de identidades e a gestão documental de forma segura. Entretanto, a expansão dessas tecnologias enfrenta desafios, como a necessidade de maior conscientização pública e a complexidade dos processos de implementação. A contribuição deste estudo consiste em oferecer uma visão abrangente e crítica sobre o estado atual e as perspectivas futuras da certificação digital no Brasil.

Este artigo está estruturado em cinco seções: a introdução, que contextualiza o tema e apresenta o problema de pesquisa; o referencial teórico, que discute os conceitos e definições fundamentais; os procedimentos metodológicos, que detalham a abordagem e as técnicas empregadas; a descrição e análise dos dados, que examina os resultados da pesquisa; e as considerações finais, que resumem os principais achados e indicam direções para futuras pesquisas.

2 REVISÃO DE LITERATURA

De acordo com Alecrim (2016), a certificação digital é uma tecnologia de identificação que permite que transações eletrônicas sejam realizadas considerando os aspectos da integridade, autenticidade e confidencialidade, de forma a evitar que adulterações, interceptações de informações privadas ou outros tipos de ações indevidas ocorram.

Ou seja, essa tecnologia funciona como uma espécie de "documento de identidade eletrônico" com validade jurídica e que garante a identificação e a proteção das partes envolvidas nas transações no meio eletrônico.

Azevedo e Mariano (2009 *apud* Moreira, 2009, p.17), explicam que Certificação Digital pode ser definida como "[...] a tecnologia que provê os mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas das mensagens e documentos trocados na Internet".

2.1 Definição de Certificado Digital

> Um Certificado Digital, ou identidade digital, é um arquivo digital de computador que, além de conter os dados de um indivíduo ou entidade, inclui também uma Chave Pública do assinante. Esses documentos eletrônicos são autenticados digitalmente pela Autoridade Certificadora, com o propósito de vincular a Chave Pública a uma pessoa ou entidade, tendo o mesmo valor legal que documentos físicos, como carteira de identidade, passaporte e cartões de crédito. Eles são usados para identificar indivíduos ou entidades na rede, servindo como prova de identidade quando apresentados (Monteiro e Mignoni, 2007, p.15).

De acordo com o (ITI, 2017), o certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação realizada em meios eletrônicos, como a internet. Certificados digitais são arquivos que estabelecem uma ligação entre um sujeito, seja uma pessoa física ou jurídica, e uma autoridade

certificadora. O padrão mais utilizado para essa certificação é o X.509, atualmente em sua versão 3 (Martini, 2008).

Os campos que compõem um certificado digital na versão X.509 são descritos no Quadro abaixo:

Quadro 1 – Descrição dos campos de um certificado no formato X.509 v3.

Campos	Descrição
Versão	Número da versão X.509 do certificado.
Número de série	Identificador único do certificado representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma AC.
Algoritmo de Assinatura da AC	Identificador do algoritmo usado para assinatura do certificado pela AC.
Nome do Emissor	Nome da AC que produziu e assinou o certificado.
Período de Validade	Intervalo de tempo que determina até quando um certificado deve ser considerado válido.
Nome do Sujeito	Identifica o dono do Certificado.
Chave Pública do Sujeito	Contém o valor da chave pública do certificado juntamente com informações sobre os algoritmos com os quais a chave deve ser usada.
ID único do Emissor	Campo para permitir o reuso de um emissor com o tempo.
ID único do Sujeito	Campo para permitir o reuso de um sujeito com o tempo.
Extensões	Campos complementares para personalizar um Certificado.

Fonte: Silva *et al.* (*apud* Moreira, 2009, p. 20-21)

2.1.2 Chave pública e privada

A chave pública é um componente acessível a todos e contém dados do proprietário do certificado. Esses dados são utilizados por aplicativos para gerar *logs* de eventos, autenticar o usuário no sistema e validar informações antes de executar qualquer ação. Segundo o ITI (2016a), "as principais informações presentes em um certificado digital são: chave pública do titular; nome e endereço de e-mail; período de validade do certificado; nome da Autoridade Certificadora (AC) que emitiu o certificado; número de série do certificado digital; assinatura digital da AC."

A chave privada, por outro lado, deve ser conhecida apenas pelo proprietário do certificado, funcionando como uma senha de acesso ao certificado digital. A verificação de uma Assinatura Digital garante que ela foi criada pela Chave Privada correspondente à Chave

Pública listada no certificado do signatário e que a mensagem associada não foi alterada desde a criação da assinatura. Quem confiar em uma assinatura que não possa ser verificada ou que apresente falhas na verificação estará assumindo todos os riscos e se isentando de quaisquer direitos relacionados ao uso da assinatura (Monteiro; Mignoni, 2007, p. 90).

2.1.3 ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma estrutura hierárquica e de confiança que facilita a emissão de certificados digitais para a identificação virtual de cidadãos. O modelo adotado pelo Brasil é o de uma certificação com raiz única, onde o ITI, além de atuar como Autoridade Certificadora Raiz (AC-Raiz), é responsável por credenciar e descredenciar outros participantes da cadeia, supervisionar e auditar os processos (ITI, 2016a).

O controle da certificação digital em todo o território nacional é realizado pelo ITI – Instituto Nacional de Tecnologia da Informação, que se dedica à inovação e ampliação da cidadania digital. Como uma autarquia federal vinculada à Casa Civil da Presidência da República, o ITI é a primeira autoridade na cadeia de certificação – AC Raiz.

A Medida Provisória 2.200-2, de 24 de agosto de 2001, deu início à implantação do sistema nacional de certificação digital da ICP-Brasil. Isso significa que o Brasil possui uma infraestrutura pública mantida e auditada por um órgão público, o ITI, que opera de acordo com regras estabelecidas pelo Comitê Gestor da ICP-Brasil. Esse comitê, composto por membros representantes dos poderes públicos, sociedade civil organizada e pesquisa acadêmica, é nomeado pela Presidência da República.

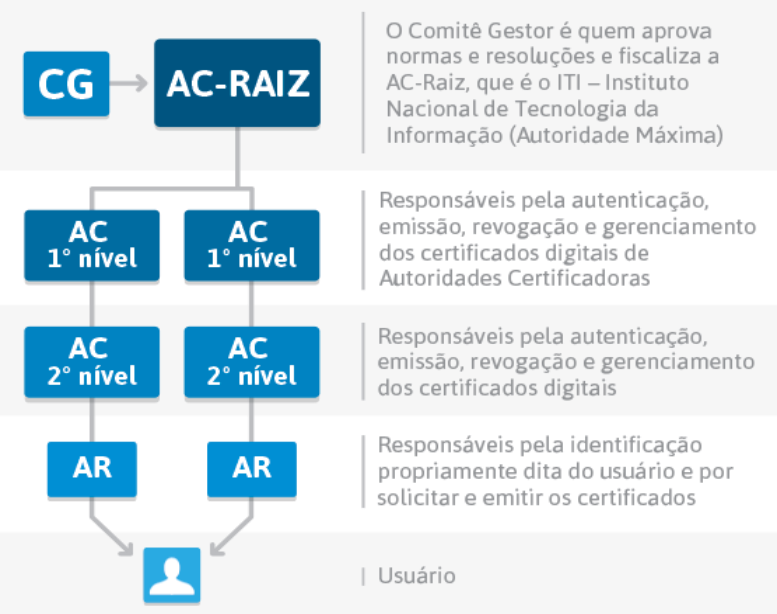
O ITI também é responsável por estimular e coordenar projetos de pesquisa científica e desenvolvimento tecnológico voltados para a ampliação da cidadania digital. Suas ações principais incluem a popularização da certificação digital ICP-Brasil e a inclusão digital, abordando questões como sistemas criptográficos, hardware compatível com padrões abertos e universais, convergência digital de mídias, desmaterialização de processos, entre outras (ITI, 2016b).

A ICP-Brasil define diretrizes e normas que devem ser seguidas por todas as certificadoras e empresas que oferecem esse serviço. É ela quem estabelece as políticas de certificados e normas técnicas e operacionais, todas aprovadas por um comitê gestor organizado pela própria ICP-Brasil.

2.1.4 Hierarquias da certificação

Para assegurar a qualidade e a confiança na certificação digital, a segunda versão do certificado digital ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) foi implementada em 1º de janeiro de 2012. A cadeia de confiança da certificação digital é composta por uma hierarquia de componentes dentro da ICP-Brasil. Esses componentes incluem a AC Raiz (Autoridade Certificadora Raiz), as ACs (Autoridades Certificadoras) de primeiro e segundo níveis, as ARs (Autoridades de Registro) e, por fim, o usuário final (Benefícios e Aplicações da Certificação Digital, 2013).

Figura 1- Componentes da ICP-Brasil



Fonte: Benefícios da Certificação Digital (2013)

2.1.4.1 AC – Raiz

A Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a entidade principal na cadeia de certificação. Ela é responsável por implementar as Políticas de Certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. A AC-Raiz tem a função de emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente inferior. Além disso, a AC-Raiz é encarregada de emitir a lista de certificados revogados (LCR) e de supervisionar e auditar as Autoridades

Certificadoras (ACs), as Autoridades de Registro (ARs) e outros prestadores de serviço habilitados na ICP-Brasil. Ela também verifica se as ACs estão operando de acordo com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil (ITI, 2016c).

2.1.4.2 AC – Autoridade Certificadora

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, que faz parte da hierarquia da ICP-Brasil. Ela é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. A AC verifica se o titular do certificado possui a chave privada correspondente à chave pública associada ao certificado. A AC cria e assina digitalmente o certificado, que representa uma declaração da identidade do titular com um par único de chaves (pública/privada). A AC também emite a lista de certificados revogados (LCR) e mantém registros de suas operações, sempre em conformidade com as práticas definidas na Declaração de Práticas de Certificação (DPC). Além disso, ela estabelece e aplica políticas de segurança necessárias para garantir a autenticidade da identificação realizada pelas Autoridades Registradoras (ARs) a ela vinculadas (ITI, 2016c).

2.1.4.3 AR – Autoridade de Registro

A Autoridade de Registro (AR) atua como intermediária entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, a AR é responsável por receber, validar e encaminhar solicitações de emissão ou revogação de certificados digitais, bem como realizar a identificação presencial dos solicitantes. A AR deve manter registros de suas operações e pode estar fisicamente localizada em uma AC ou funcionar como uma entidade de registro remota (ITI, 2016c).

2.1.4.4 ACT – Autoridade Certificadora do Tempo

Uma Autoridade Certificadora do Tempo (ACT) é uma entidade responsável por emitir Carimbos do Tempo. A AC-Raiz da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é a responsável pelo credenciamento das ACTs que desejam fazer parte da estrutura, de acordo com critérios estabelecidos nos documentos reguladores. A ACT garante que um documento, após ser assinado e criptografado, foi autenticado em uma data e hora específicas

(dia, mês, ano, hora, minuto e segundo). Assim, o conteúdo do documento pode ser validado quanto ao momento em que foi assinado (ITI, 2016b).

2.2 Tipos de Certificado Digital

De acordo com a ICP-Brasil, existem três tipos de certificados digitais, classificados com base em sua aplicabilidade e nos requisitos de segurança para a Chave Privada. Esses certificados são categorizados como:

Certificados Tipo A – Assinatura Digital: Segundo Brocardo (2016), este é o tipo de certificado mais comum. Ele é utilizado para realizar assinaturas digitais em diversos tipos de documentos e transações eletrônicas, entre outras aplicações. Suas funções incluem identificar o assinante, atestar a autenticidade da operação e confirmar a integridade do documento assinado. Os certificados mais utilizados nesta categoria são o A1 e o A3.

Certificados Tipo S – Sigilo: Esse certificado é destinado exclusivamente para garantir o sigilo de transações. Ele permite criptografar dados de um documento, que só podem ser acessados com um certificado digital autorizado para abrir o arquivo. É utilizado para o envio seguro de informações, mantendo o conteúdo em sigilo (Brocardo, 2016).

Certificados Tipo T – Tempo: De acordo com Brocardo (2016), os certificados do tipo T são conhecidos como carimbo de tempo ou *timestamp*. Esse tipo de certificado é um documento eletrônico emitido por uma parte confiável, que serve como prova de que uma informação digital existia em uma determinada data e hora no passado. O carimbo de tempo busca a data e hora de uma fonte segura e confiável, sendo essencial para garantir a temporalidade e tempestividade de documentos importantes. É utilizado em conjunto com outros tipos de certificados digitais.

Quanto aos requisitos de segurança, os certificados digitais são classificados conforme mostrado no Quadro 2 abaixo:

Quadro 2 – Classificação dos certificados Digitais quanto à segurança

Tipo	Tamanho da Chave	Geração do Par de Chaves	Validade máxima do certificado
A1/S1	2048	*Software*	1 ano
A3/S3	2048	*Hardware*	Até 5 anos
A4/S4	4096	*Hardware*	Até 6 anos

Fonte: Benefícios e Aplicações da Certificação Digital (2013)

Alecrim (2016) explica que o armazenamento do par de chaves em hardware é realizado em um cartão inteligente (*smart card*) com *chip* ou *token* USB, dispositivos protegidos por senha, como ilustrado na Figura 2. Martini (2008, p.39) afirma: "O sistema ICP-Brasil tem um protagonista essencial, o *smart card*, o cartão com *chip* ISO-7816. Nele, a chave privada é gerada e armazenada, sem nunca usar a memória volátil do sistema, o que, por fim, ajuda a garantir mais segurança."

Figura 2 – Cartão inteligente (*smart card*) e *token* USB

Fonte: Certisign (2017)

No caso de se utilizar o cartão inteligente, é necessária também uma leitora de cartão, como a ilustrada na Figura 3, que é conectada via USB.

Figura 3 – Leitora de cartão inteligente

Fonte: Certisign (2017)

3 PROCEDIMENTOS METODOLÓGICOS

A metodologia adotada neste estudo é de natureza qualitativa, com ênfase em uma revisão bibliográfica exploratória e descritiva. O objetivo é compreender os impactos da certificação digital na segurança da informação e na gestão de identidades nas empresas brasileiras. Para isso, foi realizada uma análise crítica e interpretativa da literatura existente sobre o tema, com foco em artigos acadêmicos, livros, relatórios técnicos e documentos institucionais pertinentes à área de certificação digital.

3.1 Levantamento de Dados

A coleta de dados foi realizada entre os meses de março e setembro de 2024. Utilizou-se como fontes principais bibliotecas digitais, bases de dados acadêmicas e sites especializados em segurança da informação e certificação digital. Os documentos foram selecionados com base em critérios de relevância, atualidade e qualidade das publicações, priorizando estudos que abordassem as contribuições da certificação digital para a segurança das transações eletrônicas e os desafios enfrentados pelas empresas na adoção dessa tecnologia.

3.2 Análise de Conteúdo

A análise dos dados coletados seguiu a técnica de análise de conteúdo, conforme descrita por Bardin (2016), que possibilita a identificação e interpretação de padrões, categorias e temas emergentes nos textos revisados. Esta técnica foi escolhida por sua capacidade de fornecer uma visão crítica sobre a evolução do tema da certificação digital, identificando as contribuições teóricas, práticas e as lacunas existentes na literatura.

3.3 Critérios de Inclusão e Exclusão

Os critérios de inclusão envolveram a seleção de artigos, livros e documentos que tratassem diretamente da certificação digital, segurança da informação, gestão de identidades e suas aplicações nas empresas brasileiras. Foram incluídos também trabalhos que abordassem os principais desafios, oportunidades e impactos da implementação dessas tecnologias. Os

critérios de exclusão abrangeram publicações desatualizadas ou que não tratassem diretamente dos aspectos técnicos e práticos da certificação digital.

3.4 Limitações da Metodologia

Este estudo apresenta como principal limitação a ausência de dados empíricos, uma vez que se baseia exclusivamente em fontes bibliográficas secundárias. A falta de uma pesquisa de campo ou entrevistas com profissionais da área limita a análise das percepções reais sobre as dificuldades e benefícios da certificação digital nas empresas. Portanto, sugere-se que futuras pesquisas complementem este estudo com dados empíricos para validar e aprofundar as conclusões aqui apresentadas.

4 DESCRIÇÃO E ANÁLISE DOS DADOS

De acordo com Moreira (2009, p.42), a certificação digital proporciona uma segurança aprimorada para indivíduos, empresas, softwares e computadores em suas atividades digitais. Ela assegura a integridade, autenticidade, confidencialidade, disponibilidade e não-repúdio das informações transmitidas.

Conforme o ITI (2017), a certificação digital possibilita a realização de várias operações, como comércio eletrônico, assinatura de contratos digitais e operações bancárias virtuais. Com o certificado digital, é possível realizar uma série de procedimentos virtualmente, eliminando a necessidade de deslocamento físico até órgãos governamentais ou empresas e evitando a impressão de documentos. Entre os usos mais comuns estão:

- **Assinatura de documentos e contratos digitais:** Documentos assinados digitalmente possuem a mesma validade legal que os assinados fisicamente. Isso não apenas economiza recursos como papel e tinta, mas também acelera os processos, permitindo que documentos sejam assinados e enviados por e-mail de qualquer lugar.
- **Autenticação em sistemas:** Muitos sistemas que contêm informações confidenciais exigem confirmação de identidade para acesso. O certificado digital garante a autenticidade do usuário, permitindo acesso remoto a esses sistemas sem a necessidade de presença física.
- **Atualização de informações em sistemas:** Além de garantir acesso seguro, o certificado digital facilita a atualização de informações, evitando processos burocráticos demorados.

- **Categorias profissionais:** Diversas profissões, como médicos, advogados, contadores e militares, já utilizam certificados digitais em suas rotinas diárias. O uso de sistemas virtuais unificados e seguros facilita a integração e desburocratização dos processos no setor.

4.1 NF-e

Segundo Alecrim (2016), a Nota Fiscal Eletrônica (NF-e) é um documento fiscal digital que registra a transferência de propriedade de bens ou serviços. Parte do SPED (Sistema Público de Escrituração Digital) desde 2007, a NF-e é obrigatória no Brasil e possui validade fiscal e jurídica, garantida por uma assinatura digital. De acordo com a *Valid* Certificadora Digital, um certificado digital NF-e, destinado a pessoas jurídicas, não só permite a emissão de notas fiscais eletrônicas, mas também garante a veracidade dos dados emitidos e o acompanhamento em tempo real das notas fiscais.

4.2 e-CPF e e-CNPJ

Os certificados mais conhecidos e utilizados no Brasil são o e-CPF e o e-CNPJ, ambos servindo como certificados de assinatura digital. O e-CPF é destinado a pessoas físicas e atua como uma extensão do CPF, enquanto o e-CNPJ é direcionado a pessoas jurídicas, funcionando como uma extensão do CNPJ.

Conforme a *Valid* Certificadora Digital, o e-CPF é um documento digital que assegura a autenticidade das informações transmitidas, permitindo assinar contratos, fazer procurações eletrônicas e acessar serviços exclusivos da Receita Federal e de outras instituições. Já o e-CNPJ permite a validação de transações jurídicas, garantindo a integridade e autenticidade das operações realizadas por empresas.

Alecrim (2016) destaca que tanto o e-CPF quanto o e-CNPJ não são gratuitos e devem ser adquiridos através de entidades conveniadas à Receita Federal, como Certisign e Serasa, com preços variando conforme a instituição e o tipo de certificado.

4.3 Análise dos Resultados e Discussão

Após a aplicação dos critérios de inclusão e exclusão definidos, foram selecionados 8 artigos que atendem aos objetivos desta revisão. A análise desses estudos possibilitou a

identificação das principais contribuições da certificação digital nas empresas brasileiras, além de destacar os desafios mais comuns encontrados na literatura. No Quadro 3, estão descritos os artigos escolhidos, com informações sobre os autores, ano de publicação, título, objetivos, principais resultados e conclusões. Essa tabela oferece uma visão geral e comparativa do que já está documentado nas evidências científicas sobre o tema.

Quadro 3- artigos selecionados

AUTOR/ANO	TÍTULO	OBJETIVOS	PRINCIPAIS RESULTADOS	CONCLUSÕES
Sell; Oliveira Trindade (2025)	Impactos na Privacidade, Segurança e Confiança nas Relações Digitais nas Empresas: Desafios e Perspectivas na Era da LGPD	Discutir os impactos da LGPD nas práticas de certificação digital e segurança da informação nas empresas	A LGPD impulsionou a adoção da certificação digital, promovendo maior confiança nas relações digitais	A LGPD tem sido um fator-chave para a adoção da certificação digital nas empresas
Paula *et al.* (2024)	Certificados digitais: navegando pelas dificuldades enfrentadas pelas empresas contábeis em Benjamin Constant, Amazonas	Analisar os problemas enfrentados por empresas contábeis da região amazônica na adoção de certificação digital	Foram identificados desafios como falta de compreensão dos clientes, custos elevados, dificuldade de acesso à internet e escassez de profissionais	A certificação digital enfrenta barreiras estruturais, educacionais e logísticas em regiões isoladas, exigindo políticas públicas e investimentos
Machado *et al.* (2024)	A segurança da informação para empresas no Brasil	Analisar as práticas de segurança da informação e como a certificação digital contribui para a proteção de dados em empresas	Certificação digital, junto a outras medidas, garante proteção contra fraudes e ataques cibernéticos	Para proteção efetiva, deve ser implementada com outras práticas de segurança
Souza; Rezende (2023)	Benefícios do uso da certificação digital para pessoa física e jurídica na informatização de processos	Avaliar os benefícios da certificação digital em processos administrativos e jurídicos para pessoas físicas e jurídicas	A certificação digital contribui para a redução de custos e agilização de processos, além de garantir maior segurança nas transações eletrônicas	A adoção da certificação digital é vantajosa para empresas e cidadãos, mas requer maior conscientização sobre seus benefícios
Ramos *et al*. (2023)	Contabilidade 4.0: avanços da tecnologia da informação contábil em uma empresa do setor Sucroalcooleiro/MT	Analisar os impactos dos avanços da tecnologia da informação no contexto da contabilidade	A modernização tecnológica contribuiu para melhorias nos processos de controle, automação e análise contábil	A aplicação da TI no setor contábil favorece a eficiência operacional e a confiabilidade das informações gerenciais

		aplicada à indústria		
Ramos; Cabral (2021)	Influências da criação de uma identidade digital baseada em blockchain no comércio de certificados digitais	Avaliar como a introdução de blockchain pode melhorar a autenticidade e segurança na certificação digital	Blockchain aumenta segurança, rastreabilidade e confiança nos dados autenticados	A integração entre blockchain e certificação digital pode transformar a gestão de identidades e transações
Piacente (2020)	Análise da padronização do trabalho na área de certificação digital: um estudo de caso	Analisar as implicações da padronização dos processos de certificação digital em diversos setores e seus impactos na segurança	A padronização é essencial para garantir a interoperabilidade e a confiabilidade dos sistemas de certificação digital	A padronização e regulamentação da certificação digital devem ser fortalecidas para melhorar sua eficácia em todos os setores
Franco *et al.* (2020)	Contabilidade 4.0: análise dos avanços dos sistemas de tecnologia da informação no ambiente contábil	Discutir os avanços tecnológicos aplicados à contabilidade, com ênfase nos impactos da TI e automação no ambiente organizacional	Adoção de tecnologias, como certificação digital e sistemas integrados, ampliou produtividade, segurança e tomada de decisão contábil	A tecnologia é essencial para a transformação digital, com a certificação digital como pilar da modernização

Fonte: autoria própria, 2025.

A implementação da certificação digital tem gerado impactos significativos nas empresas brasileiras, especialmente na informatização dos processos administrativos. Ramos et al. (2023) afirmam que o uso de ferramentas como o e-CPF e o e-CNPJ tem simplificado a autenticação de identidades, permitindo maior segurança nas transações digitais. Paula et al. (2024) corroboram essa afirmação, destacando que esses certificados também ajudam na redução de custos operacionais, ao eliminar a necessidade de validações manuais e do envio físico de documentos.

A padronização dos processos de certificação digital é outro fator determinante para a eficiência dessa tecnologia. Piacente (2020) observa que a uniformização dos procedimentos facilita a integração entre diferentes sistemas e plataformas, promovendo uma adoção mais ampla. Franco *et al.* (2020) complementam que essa padronização é essencial para garantir a interoperabilidade, especialmente entre os setores público e privado, criando uma base sólida para a expansão da transformação digital no Brasil.

No entanto, a adoção plena da certificação digital ainda enfrenta desafios relacionados à capacitação técnica dos profissionais. Paula *et al.* (2024) destacam que muitos

profissionais e empresas não possuem o treinamento adequado para utilizar corretamente essas ferramentas. Machado *et al*. (2024) apontam que a falta de compreensão sobre os benefícios da certificação digital pode dificultar a implementação dessa tecnologia, resultando em uma utilização incompleta das suas vantagens.

Além disso, Souza e Rezende (2023) afirmam que a conscientização sobre a importância da certificação digital é fundamental para sua adoção em larga escala. Muitas empresas ainda não compreendem totalmente os benefícios dessa tecnologia, o que pode levar à subutilização do e-CPF e e-CNPJ. Piacente (2020) reforça que, para que a certificação digital tenha o impacto esperado, é necessário um esforço contínuo de educação e capacitação dos profissionais, além de uma maior divulgação de seus benefícios.

Machado *et al.* (2024) também alertam para a importância de um suporte técnico adequado, especialmente para pequenas e médias empresas, que enfrentam dificuldades para implementar a certificação digital devido à falta de infraestrutura e recursos financeiros. Sell e Oliveira Trindade (2025) concluem que, apesar das barreiras existentes, a adoção dessas tecnologias tem o potencial de transformar os processos empresariais e governamentais, garantindo maior segurança e eficiência nas operações.

A segurança das transações digitais é um dos principais benefícios da certificação digital, conforme apontado por Franco *et al*. (2020). A utilização de e-CPF e e-CNPJ permite que as empresas e indivíduos validem transações de forma mais segura, prevenindo fraudes e garantindo a integridade dos dados. Machado *et al*. (2024) afirmam que, além de assegurar a autenticidade das informações, os certificados digitais são essenciais para fortalecer a confiança nas operações realizadas no meio digital, contribuindo para a segurança cibernética.

Por outro lado, a implementação da certificação digital também exige a adaptação da infraestrutura tecnológica nas empresas. Piacente (2020) discute que, para garantir a eficácia da certificação digital, é necessário que os sistemas das empresas sejam compatíveis com as novas tecnologias de autenticação e criptografia. Paula *et al*. (2024) reforçam que a falta de integração entre esses sistemas pode resultar em falhas operacionais e dificuldades no processo de digitalização, impedindo a maximização dos benefícios da certificação.

A necessidade de políticas públicas de incentivo à digitalização também foi mencionada por Souza e Rezende (2023), que ressaltam que, embora a certificação digital traga benefícios evidentes, a sua adoção pode ser dificultada pela falta de incentivos governamentais. Sell e Oliveira Trindade (2025) destacam que é fundamental que o governo promova campanhas de conscientização e ofereça suporte financeiro para as empresas, especialmente as

de pequeno porte, de modo a garantir a inclusão digital e a plena utilização das tecnologias de certificação.

Além disso, o papel da capacitação técnica na implementação da certificação digital não pode ser subestimado. Machado *et al.* (2024) afirmam que, embora os certificados digitais ofereçam maior segurança e eficiência, sua adoção depende do treinamento adequado dos profissionais que lidam com esses sistemas. Ramos *et al.* (2023) complementam que a educação sobre as vantagens da certificação digital deve ser uma prioridade para garantir que as empresas se sintam confiantes em adotar as novas tecnologias, principalmente nas áreas de contabilidade e gestão.

Em relação à segurança da informação, Paula *et al*. (2024) observam que a certificação digital também é crucial para o cumprimento das normas e regulamentações de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados). A utilização do e-CPF e e-CNPJ tem garantido maior proteção aos dados pessoais e sensíveis dos usuários, promovendo a conformidade com as leis de privacidade. Franco *et al.* (2020) acrescentam que a certificação digital, ao assegurar a confidencialidade das transações, também reforça a confiança dos usuários nos serviços digitais oferecidos pelas empresas.

Por fim, é importante considerar os avanços na utilização da certificação digital no Brasil, especialmente com o crescente uso de blockchain e outras tecnologias emergentes. Ramos e Cabral (2021) destacam que a criação de uma identidade digital baseada em blockchain pode aumentar ainda mais a segurança e a confiabilidade das transações realizadas com certificados digitais. Sell e Oliveira Trindade (2025) reforçam que, com a evolução das tecnologias, é possível que novas formas de autenticação digital surjam, oferecendo ainda mais proteção às transações realizadas no ambiente online.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa analisou o papel da certificação digital na promoção de segurança e eficiência nas transações digitais, identificando os principais desafios e oportunidades dessa tecnologia no cenário brasileiro. A metodologia utilizada foi de caráter qualitativo, com uma revisão bibliográfica abrangente de documentos e artigos acadêmicos relevantes.

A pesquisa revelou que a certificação digital é uma ferramenta essencial para garantir a segurança e a eficiência em transações digitais. A implementação de certificados como e-CPF e e-CNPJ mostrou-se eficaz na autenticação de identidades e na gestão

documental, proporcionando vantagens como a redução de custos operacionais e a agilidade nos processos. Compreende-se, portanto, que, apesar dos benefícios claros, há uma necessidade urgente de aumentar a conscientização sobre a importância e o uso dessas tecnologias, uma vez que ainda existem barreiras significativas, como a complexidade dos processos de implementação e a falta de conhecimento técnico por parte dos usuários.

Depreende-se que, a certificação digital é um componente importante para a segurança e a modernização das operações empresariais e governamentais. No entanto, para que seu potencial seja plenamente realizado, é necessário superar desafios relacionados à conscientização pública e à simplificação dos processos de adoção.

Esta pesquisa oferece uma análise ampla e crítica do estado atual e das perspectivas futuras da certificação digital no Brasil. Ela contribui para o entendimento das tecnologias subjacentes, suas aplicações práticas e os desafios enfrentados por empresas e indivíduos ao adotar essas soluções. A principal limitação desta pesquisa é a ausência de dados empíricos, uma vez que se baseou exclusivamente em revisão bibliográfica. Como também, a pesquisa não abordou em profundidade aspectos técnicos específicos da implementação de certificados digitais.

Futuras pesquisas poderiam incluir estudos empíricos para avaliar a percepção dos usuários sobre a certificação digital e os desafios enfrentados na prática. Por isso, investigações focadas em aspectos técnicos, como a segurança de diferentes tipos de chaves criptográficas, poderiam enriquecer a compreensão sobre o tema. A pesquisa também poderia explorar o impacto da certificação digital em setores específicos, como o financeiro e o governamental, para identificar oportunidades de melhorias e inovação.

REFERÊNCIAS

ALECRIM, Emerson. **O que é Certificação Digital?** Disponível em: https://www.infowester.com/assincertdigital.php. Acesso em: 14 março. 2024.

BENEFÍCIOS E APLICAÇÕES DA CERTIFICAÇÃO DIGITAL. **O que é certificação digital?** 2013. Disponível em: http://www.beneficioscd.com.br/cartilha_online/. Acesso em: 14 abril. 2024.

BROCARDO, Marcelo Luiz. **Tipos de certificados digitais.** Disponível em: https://blog.bry.com.br/tipos-de-certificados-digitais/. Acesso em: 14 abril.2024.

CERTISIGN. **Apresenta informações sobre: produtos de certificado digital fornecidos pela autoridade certificadora, informações relacionadas a certificação digital e**

recomendações de uso dos certificados. Disponível em:< https://www.certisign.com.br/>. Acesso em 14 maio. 2024.

FRANCO, G.; FARIA, R. O. P.; MACIEL, A. L. M.; DUARTE, S. Contabilidade 4.0: análise dos avanços dos sistemas de tecnologia da informação no ambiente contábil. CAFI: **Revista de Contabilidade & Finanças**, São Paulo, v. 4, n. 1, p. 55–73, 2020. Disponível em: https://revistas.pucsp.br/index.php/CAFI/article/view/51225. Acesso em: 13 nov. 2025.

INFORMAÇÃO BRASILEIRA. 2009. 56 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdades Unificadas Doctum de Cataguases, Cataguases, 2009. Disponível em: https://pt.slideshare.net/danilogmoreira/monografia-oficial-danilo-gomes-moreirav2. Acesso em: 078 maio. 2024.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Apresenta informações sobre: ICP-Brasil e sua estrutura, certificação digital e dados relacionados a emissão de certificados.** Disponível em: http://www.iti.gov.br/. Acesso em 14 junho. 2024.

ITI. Instituto Nacional de Tecnologia da Informação. **Como funciona? 2016b.** Disponível em: http://www.iti.gov.br/index.php/icp-brasil/como-funciona. Acesso em: 14 maio. 2024.

ITI. Instituto Nacional de Tecnologia da Informação. **ICP-Brasil. 2016c.** Disponível em: http://www.iti.gov.br/icp-brasil. Acesso em: 18 julho. 2024.

ITI. Instituto Nacional de Tecnologia da Informação. **O que é? 2016a.** Disponível em: http://www.iti.gov.br/icp-brasil/o-que-e. Acesso em: 10 maio. 2024.

MACHADO, K. R.; PRETA, K. O. C.; PUNGIRUM, J. C. M. A segurança da informação para empresas no Brasil. **Revista Multidisciplinar do Nordeste Mineiro**, v. 10, n. 1, p. 1–18, 2024. Disponível em: https://www.revista.unipacto.com.br/index.php/multidisciplinar/article/view/2985. Acesso em: 12 nov. 2025. DOI: https://doi.org/10.61164/rmnm.v10i1.2985

MARTINI, Renato da Silveira. **Tecnologia e Cidadania Digital: ensaio sobre tecnologia, sociedade e segurança.** Rio de Janeiro: Brasport, 2008.

MONTEIRO, Emiliano S.; MIGNONI, Maria E. **Certificados digitais: conceitos e práticas.** Rio de Janeiro: Brasport, 2007.

MOREIRA, Danilo Gomes. **A certificação digital na sociedade da informação brasileira.** 2009. 56 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdades Unificadas Doctum de Cataguases, Cataguases, 2009. Disponível em: https://pt.slideshare.net/danilogmoreira/monografia-oficial-danilo-gomes-moreirav2. Acesso em: 14 julho. 2024.

PAULA, M. E. S.; OLAVO, A. V. A.; REIS, L. K. G.; CIRINO, A. L. Certificados digitais: navegando pelas dificuldades enfrentadas pelas empresas contábeis em Benjamin Constant, Amazonas. CAFI: **Revista de Contabilidade & Finanças**, São Paulo, v. 11, n. 33, p. 133–148, 2024. Disponível em: https://revistas.pucsp.br/index.php/CAFI/article/view/68340. Acesso em: 13 nov. 2025. DOI: https://doi.org/10.23925/cafi.71.68340

PIACENTE, F. J. Análise da padronização do trabalho na área de certificação digital: um estudo de caso. **Research, Society and Development**, v. 9, n. 10, e309108394, 2020. Disponível em: https://www.researchgate.net/publication/345247143_Analise_da_padronizacao_do_trabalho_na_area_de_certificacao_digital_um_estudo_de_caso. Acesso em: 12 nov. 2025.

RAMOS, J. K. A. P.; SERVILHA, G. O. A.; SANTOS, J. S. C.; SILVA, R. W. Contabilidade 4.0: avanços da tecnologia da informação contábil em uma empresa do setor sucroalcooleiro/MT. **Revista Foco**, v. 16, n. 2, p. 1–28, 2023. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/681. Acesso em: 13 nov. 2025.

RAMOS, J. M.; CABRAL, R. H. **Influências da criação de uma identidade digital baseada em blockchain no comércio de certificados digitais**. 2021. Disponível em: http://www.repositorio.unis.edu.br/handle/prefix/2269. Acesso em: 12 nov. 2025.

SELL, L. C.; OLIVEIRA TRINDADE, R. Impactos na privacidade, segurança e confiança nas relações digitais nas empresas: desafios e perspectivas na era da Lei Geral de Proteção de Dados (Lei n. 13.709/2018). **Direito em Revista**, n. 37, p. 185–222, 2025. Disponível em: https://revistas.cesul.br/rdr/article/view/9. Acesso em: 12 nov. 2025.

SOUZA, L. F.; REZENDE, S. R. G. Benefícios do uso da certificação digital para pessoa física e jurídica na informatização de processos. **Revista Mirante**, Anápolis, v. 16, n. 2 (edição especial), p. 289–306, jun. 2023. Disponível em: https://core.ac.uk/download/568037264.pdf. Acesso em: 12 nov. 2025.