**FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"**
**Curso Superior de Tecnologia em Tecnologia de Segurança da Informação**

João Victor Ceron Blanco

# As implicações do uso do certificado digital durante a pandemia

**Americana, SP**

**2021**

**FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"**

**Curso Superior de Tecnologia em Tecnologia de Segurança da Informação**

João Victor Ceron Blanco

# As implicações do uso do certificado digital durante a pandemia

Trabalho de Conclusão de Curso (TCC) desenvolvido em cumprimento à exigência curricular do CursoSuperior de Tecnologia em de Segurança da Informação, da Faculdade de Tecnologia de Americana-SP, sob a orientação do Prof. Dr. Daives Arakem Bergamasco.
Área de concentração: Segurança da Informação.

**Americana, SP**

**2021**

João Victor Ceron Blanco

**As implicações do uso do certificado digital durante a pandemia**

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 08 dezembro de 2021.

**Banca Examinadora:**

Daives Arakem Bergamasco (Presidente)
Doutor
Fatec Americana

Benedito Luciano Antunes de França (Membro)
Mestre
Fatec Americana

Marcus Vinicius Lahr Giraldi (Membro)
Especialista
Fatec Americana

## AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a todos os professores e colegas que me auxiliaram nessa jornada, sempre apoiando, incentivando e motivando o desenvolvimento educacional, profissional e pessoal.

## DEDICATÓRIA

Aos meus pais que sempre estiverem durante toda essa jornada apoiando e incentivando a se comprometer com os estudos.

**RESUMO**

O texto a seguir tem como principal objetivo apresentar os principais conceitos que envolvem a certificação digital, principalmente os que são relacionados a Tecnologia da Informação e a Segurança da Informação, as principais tecnologias relacionadas a ela, como a certificação digital é utilizada no Brasil atualmente, suas aplicações e como ela tem se tornado cada vez mais uma tecnologia facilitadora no contexto da pandemia do COVID-19. Foi feito um estudo sobre as principais tecnologias que envolvem a certificação digital, e suas relações com a Segurança da Informação, além. O texto apresenta também um levantamento sobre como é a organização das emissões do certificado digital no Brasil atualmente são estruturadas, ou seja, ele apresenta as principais entidades que estão envolvidas com essa tecnologia no Brasil. Além disso apresenta possibilidades futuras para sua utilização no contexto da tecnologia da informação, não só aplicações que envolvem sites e serviços online que são disponibilizados pelo governo, mas também para empresas privadas.

**Palavras-Chave:** Certificado Digital; Criptografia; Segurança da Informação

**ABSTRACT**

*The main objective of the following text is to present the main concepts involving digital certification, especially those related to Information Technology and Information Security, the main technologies related to it, as digital certification is used in Brazil today, its applications and how it has increasingly become an enabling technology in the context of the COVID-19 pandemic. A study was carried out on the main technologies involved in digital certification, and their relationship with Information Security, in addition. The text also presents a survey on how the organization of digital certificate emissions in Brazil is currently structured, in other words, it presents the main entities involved with this technology in Brazil. Furthermore, it presents future possibilities for its use in the context of information technology, not only applications involving websites and online services that are made available by the government, but also for private companies.*

**Keywords:** *Digital Certificate; Cryptography; Information Security*

## ABSTRACT

## LISTA DE FIGURAS



## LISTA DE TABELAS



.

**SUMÁRIO**

## INTRODUÇÃO

Antes de entendermos a importância do certificado digital e suas implicações nos tempos atuais, devemos primeiramente observar os fatos que levaram a criação e a implementação desse sistema de registro de dados de pessoas físicas e pessoas jurídicas. Fatos esses que apontam para a necessidade de se manter os registros dos indivíduos e das entidades presentes em uma sociedade moderna.

Podemos dizer que os registros das pessoas e das entidades pertencentes a uma sociedade, possuem sua origem ainda na antiguidade com os escribas do Egito antigo que tinham não só a função de copiar textos existentes, mas também a função de editar registros já existentes e criar novos registros, registros esses que possuíam informações como cartas pessoais, testamentos e outros documentos legais como por exemplo: proclamações oficiais, registros fiscais, documentos administrativos, econômicos e religiosos, e assim por diante (HILL, 2018).

Já no Brasil o registro universal de pessoas naturais teve início em 1850 com a lei 586 de 06 de setembro de 1850, em seu artigo 17 §3º (BRASIL, 1850). Porém por se tratar de um período em que o Brasil ainda era um império ainda havia empecilhos por conta da maioria desses registros serem realizados por padres, bispos ou outras autoridades da igreja católica. Após a Proclamação da República, a ideia era separar o estado do âmbito religioso, sendo assim o estado passou a ser o principal responsável pela coleta dos dados dos registros civis (TIZIANI, 2016).

Porém só foi no ano de 1907 que a primeira Carteira de Identidade foi emitida sendo o Sr. Edgard Costa seu portador (LAGO, 2001). A criação do registro civil e da Cartearia de Identidade demonstra um grande avanço na sociedade atual e de como nós nos organizamos. Com o passar dos anos os processos jurídicos se tornaram cada vez mais importante, se tornando parte essencial sociedade brasileira atualmente. Esses processos têm cada vez avançado mais, e com esses avanços novos desafios são apresentados.

As novas tecnologias que foram disponibilizadas nos últimos anos proporcionaram uma interação pessoal, social e comercial sem precedentes, permitindo assim que os processos jurídicos e comerciais passassem a ser feitos não só fisicamente, mas também digitalmente. Esses processos digitais no ano de 2020 com o cenário atual de pandemia global, deixaram de ser apenas opções de como processos e interações poderiam ser realizadas e passaram a ser essenciais para que eles pudessem ocorrer, e isso incluí processos jurídicos que são essenciais.

Já que grande parte das interações deixarem de ser físicas e terem que ser conduzidas digitalmente, devemos também então levar em consideração a segurança dessas interações, já que entre essas interações existem documentos digitais e processos digitais que são

extremamente delicados e que possuem informações que devem ser íntegras e que não devem ser acessadas indevidamente. E para garantir essa segurança temos algumas opções, entre elas a Certificação Digital.

A Certificação Digital se apresenta como uma das opções viáveis. A Certificação Digital no Brasil deu um passo fundamental no ano de 2001, com a edição da medida provisória 2200-2/01, que regulamentou e instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos eletrônicos, aplicações que utilizem o certificado digital e a realização de transações eletrônicas de maneira segura (BRASIL, 2001).

O escopo principal do trabalho se trata de demonstrar e enfatizar a importância da utilização da Certificação Digital no Brasil atual, como forma de autenticar documentos eletrônicos e assegurar sigilo e segurança a transações realizadas eletronicamente. Além de evidenciar as características que apresentam a segurança que a Certificação Digital fornece.

O ano de 2020 foi marcado por uma pandemia global em que a maioria dos indivíduos e das organizações tiveram que adaptar seus processos ao novo cenário, já que a maioria das interações sociais deixaram de ser físicas e presenciais e passaram a ser de maneira virtual e a distância. Como pode ser observado com o aumento da utilização de aplicativos para videoconferências no período de quarentena (RIBEIRO, 2020). Com esse cenário a principal preocupação das organizações e das pessoas se tornou a garantia da privacidade e da integridade dos ambientes virtuais.

Com a utilização de ambiente virtuais no Brasil e no mundo se tornando cada vez mais requisitadas e essenciais para a sociedade, um dos maiores problemas e com a segurança desses ambientes. Só no mês de outubro estima-se no total que pelo menos 2,2 milhões de brasileiros tenham sido vítimas de algum golpe virtual (SOUZA,2020). Deste modo, uma das maiores preocupações é a de garantir a segurança desses ambientes, e a autenticidade dos dados que utilizam esses meios virtuais.

O objetivo do trabalho é apresentar a Certificação Digital como caminho para se obter a autenticidade, a integridade e o reconhecimento de autoria, para realizar transações eletrônicas e documentos eletrônicos. Avaliando essa tecnologia do ponto de vista técnica. E avaliar do ponto de vista jurídico, sua validade e segurança em garantir a autenticidade de documentos. Especificamente os objetivos:

- Apresentar os principais conceitos relacionados a Certificação Digital brasileira, apresentando sua estrutura hierárquica;
- Apresentar as tecnologias utilizadas no processo de Certificação Digital no Brasil;
- Avaliar seu impacto no modo como são conduzidas operações eletrônicas e virtuais;
- Apresentar as principais aplicações da Certificação Digital.

Este trabalho utiliza o método bibliográfico de natureza científica aplicada. Utiliza referenciais teóricos baseados em artigos e livros de especialistas, além de fazer uso de manuais disponibilizados em sites de órgão públicos, como o ITI (Instituto Nacional de Tecnologia da Informação), Setores do Judiciários e Legislativo, universidades, entre outros.

O trabalho está estruturado em ---- capítulos. Sendo o primeiro capítulo a introdução, expondo um breve histórico do Registro Civil no Brasil, que por meio dele se originaram as primeiras carteiras de identidade. O segundo capítulo expõe ao leitor de maneira técnica os principais conceitos que envolvem a certificação digital, isso incluí criptografia e outras tecnologias que estão relacionadas a certificação digital. O capítulo 3 aborda como o certificado digital é utilizado no Brasil e os órgãos que fiscalizam os processos que envolvem a certificação digital, nesse capítulo são apresentados a hierarquia da ICP-Brasil as entidades que a compõem, suas atribuições, e a legislação que a envolve. O quarto capítulo aborda as principais aplicações do certificado digital nas instituições e na sociedade, expondo ao leitor o que o uso do certificado digital proporciona a segurança da informação. Ao final conclusões sobre o tema e as referências.

# 1 REFERENCIAL TEÓRICO

Com as constantes evoluções referente a tecnologia da informação, compartilhar as informações de forma efetiva, rápida e segura passou a ser uma prática moderna de gestão e indispensável para as empresas e organizações. Porém ao mesmo tempo que as auxiliam essa troca de informações, novos desafios surgem, e consequentemente novas tecnologias são desenvolvidas para superar esses novos desafios.

Entre essas novas tecnologias o certificado digital se apresenta com uma tecnologia capaz de auxiliar a troca de informação dentro do espaço cibernético digital de forma segura e que não haja uma perca dessas informações.

O Referencial teórico abordara os principais conceitos da segurança da informação e os principais conceitos que envolvem a tecnologia do certificado digital.

## 1.1 Segurança da informação

Como a Associação Brasileira de Normas Técnicas (ABNT), através da norma ABNT NBR ISO/IEC 27002:2013 define o termo Segurança da Informação:

> é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios.

Importante mencionar que a segurança da informação vai além apenas da tecnologia da informação, e está presente em diversas áreas de nosso cotidiano. Ela tem como principal objetivo preservar, assegurar e proteger determinado conjunto de informações de um determinada indivíduo.

Como descrito por Peixoto (2006) existem três principais atributos ou princípios da Segurança da Informação. Sendo o primeiro a confidencialidade, que se refere as ferramentas tecnológicas da segurança que tem como objetivo proteger o sigilo da informação, limitando assim o acesso a ela. O princípio da confidencialidade garante que apenas pessoas que devam ter o acesso a ela possuam esse acesso. De acordo com Sêmola (2014), a confidencialidade basicamente permite o acesso à informação aos agentes autorizados e o não acesso aos agentes não autorizados.

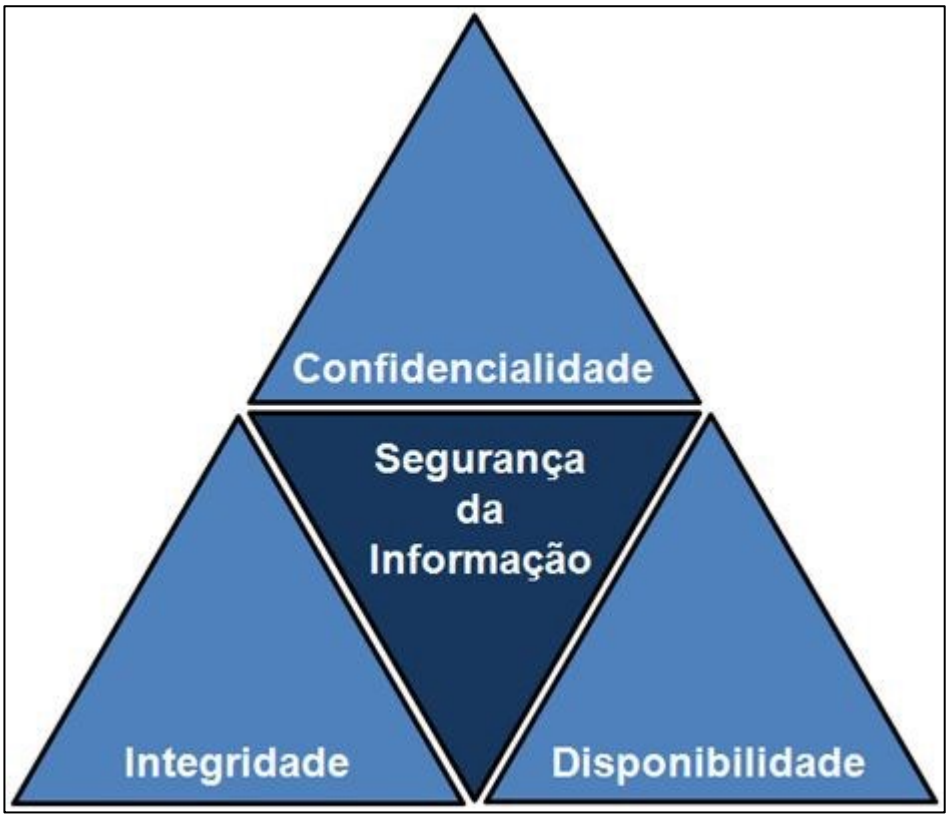
O próximo princípio se refere a integridade da informação, esse princípio tem como objetivo manter as características originais da informação, características essas que são definidas pelo autor da informação, ou seja, o princípio da integridade não permite as alterações de informações originais. Do mesmo modo que Peixoto (2006), Sêmola (2014) relaciona a integridade a permitir que somente agentes autorizados possam alterar a informação e que agentes não autorizados não possuam esse acesso, impedindo-os de

comprometer a informação.

O terceiro princípio se refere à disponibilidade, esse conceito define que a informação poderá ser acessada pelos agentes autorizados a qualquer momento, garantindo que a informação sempre estará disponível quando necessária (PEIXOTO, 2006).

Na Figura 1 é destacada os princípios que regem a segurança da informação:

Figura 1: Princípios da Segurança da Informação




Fonte: Afonso (2018)

Com o passar dos anos e a constante evolução da tecnologia a quantidade e complexidade das informações que possuímos aumentou drasticamente, principalmente nas últimas décadas com a chamada Terceira Revolução Industrial, termo esse que se refere às mudanças radicais trazidas pela computação da segunda metade do século, marcando início da era da informação (CHATFIELD, 2012).

Sendo assim a Segurança da Informação passou a ser um fundamental em todas as áreas da sociedade, tornando-se cada vez mais necessária e presente nas organizações, já que ela oferece ferramentas e metodologias que auxiliam a mantermos a informação segura, íntegra e disponível.

O Certificado Digital é uma dessas tecnologias que foi implementada nos últimos anos principalmente nas empresas e organizações do Brasil, como forma de manter os pilares da Segurança da Informação nessas organizações.

## 1.2 Criptografia

O funcionamento de um certificado digital se baseia na criptografia, que é uma tecnologia da segurança da informação utilizada para garantir que a informação seja compreendida somente por quem tem os privilégios necessários.

A criptografia era usada antigamente principalmente por militares, que tinham a necessidade de enviar informações importantes de um ponto ao outro, porém sem que essas informações fossem interceptadas, e que caso isso acontecesse os inimigos não fossem capazes de compreendê-las.

Segundo Singh (2007), os primeiros relatos do tipo de mensagem criptografada foram descritos por Heródoto, um grande historiador, que descreve a guerra entre Pérsia e Grécia no século V AC.

Xerses, o líder dos persas naquele período planejou um ataque as cidades-estados Atenas e Esparta, porém, um grego exilado na Pérsia, obteve essas informações, diante da descoberta e preocupado com sua pátria, decidi enviar mensagem à Grécia para avisar sobre o ataque planejado pelo líder Pérsia. No entanto, era necessário que sua mensagem não fosse interceptada pelos persas.

Para ocultar as informações o grego infiltrado no país inimigo decidiu utilizar um par de tabuletas de madeira. Primeiro ele rapou a cera da madeira, e escreveu a mensagem na mesma, e aplicou novamente a cera. Desta maneira, a mensagem pode ser enviada sem ser interceptada, e obtida de forma segura pelos gregos.

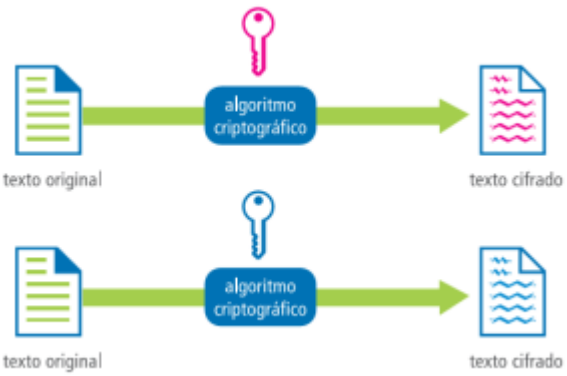
Sendo assim o conceito de criptografia é de proteger uma mensagem, texto ou informação. Na criptografia existem dois tipos de textos ou informações, a primeira é a informação que deseja ser transmitida pelo emissor, chamada de texto claro ou texto puro. O texto claro então passa por um processo de encriptação que que assume uma nova forma, essa nova forma é chamada de texto cifrado. O receptor recebe então o texto cifrado e então faz o processo de descriptografar, que transforma o texto cifrado em no texto claro novamente (CARVALHO, 2001).

O processo de encriptação e decriptação utiliza algoritmos, que são sequencias de operações e regras que determinam como o texto claro será transformado no texto cifrado. A ICP[1] Brasil define algoritmo como uma “série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema[...]” (ICP, 2007) nesse caso a tarefa é de transformar uma informação clara em uma cifrada e vice-e-versa.

A figura 2 ilustra o processo de encriptação:

[1] ICP é a abreviação de Infraestrutura de Chaves Públicas Brasileira.

Figura 2: Processo de encriptação




Fonte: Rossi (2010)

### Chave criptográficas

Como ilustrado na imagem acima o processo de encriptação utiliza chaves. Essas chaves são chamadas de chaves criptográficas, como definido por SILVA (2008) essas chaves são valores matemáticos que determinam como o texto pleno é criptografado para produzir o texto cifrado.

As chaves complementam o algoritmo para cifrar o texto claro, elas são valores inseridos nos algoritmos que fazem com que o texto claro seja encriptado. O valor da chave é secreto o que faz que seja necessário que o invasor possua a informação da chave, se ele não possuir essa informação ele será forçado a quebrar o algoritmo, o que é uma tarefa extremamente difícil já que os algoritmos utilizados na criptografia moderna são seguros e exaustivamente testados. Na criptografia as chaves criptográficas são essenciais para garantir a segurança da informação, elas garantem que apenas o emissor e o receptor terão acesso à informação.

Na criptografia de chaves existem dois tipos de criptografias: simétrica e assimétrica.

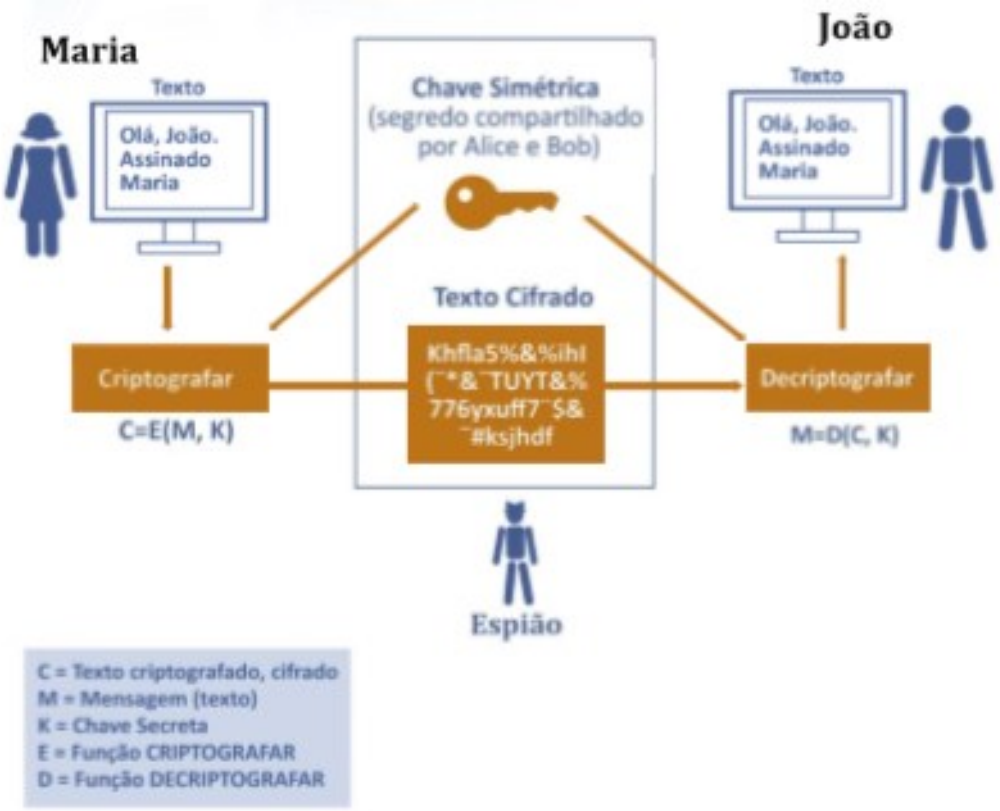
### Criptografia Simétrica

A criptografia simétrica utiliza um algoritmo que depende da mesma chave, essa chave é utilizada tanto no processo de criptografar quanto no de descriptografar o texto. Sendo assim o emissor e o receptor da mensagem devem possuir a chave. A principal vulnerabilidade desse método de criptografia é que é necessário que a chave seja compartilhada com todos que precisam acessar a mensagem, e a dificuldade está em disponibilizar essa chave a todos que precisam de maneira segura (ITI, 2020a).

Na Criptografia Simétrica existem basicamente dois tipos de algoritmos, os cifradores seriais (ou em série), que criptografam a informação de forma serial, ou seja, dado a dado e os cifradores de blocos, onde a informação é dividida em blocos e esses blocos são cifrados.

O processo da criptografia simétrica funciona da seguinte maneira: O emissor da mensagem utiliza um algoritmo e a chave para criptografar o texto claro, e então envia o texto cifrado ao receptor, este que o utiliza a mesma chave para descriptografar o texto cifrado obtendo novamente o texto claro. Conforme a figura3 um exemplo do funcionamento da criptografia simétrica:

Figura 3: Sistema de criptografia simétrica




Fonte: Certisign (2018)

Conforme a Tabela1 com exemplos de algoritmos utilizados na criptografia simétrica:

**Tabela 1 – Algoritmos utilizados na criptografia simétrica.**

| **Algoritmos cifradores de blocos** | |
|---|---|
| **Mais comuns:** | AES, Blowfish, DES, triple DES, Serpent, TWofish |
| **Padrões Internacionais:** | AES process, CRYPTREC, NESSIE |
| **Algoritmos Cifradores em série** | |
| **Mais comuns:** | RC4 e Block ciphers in stream mode |

Fonte: Certisign (2018)

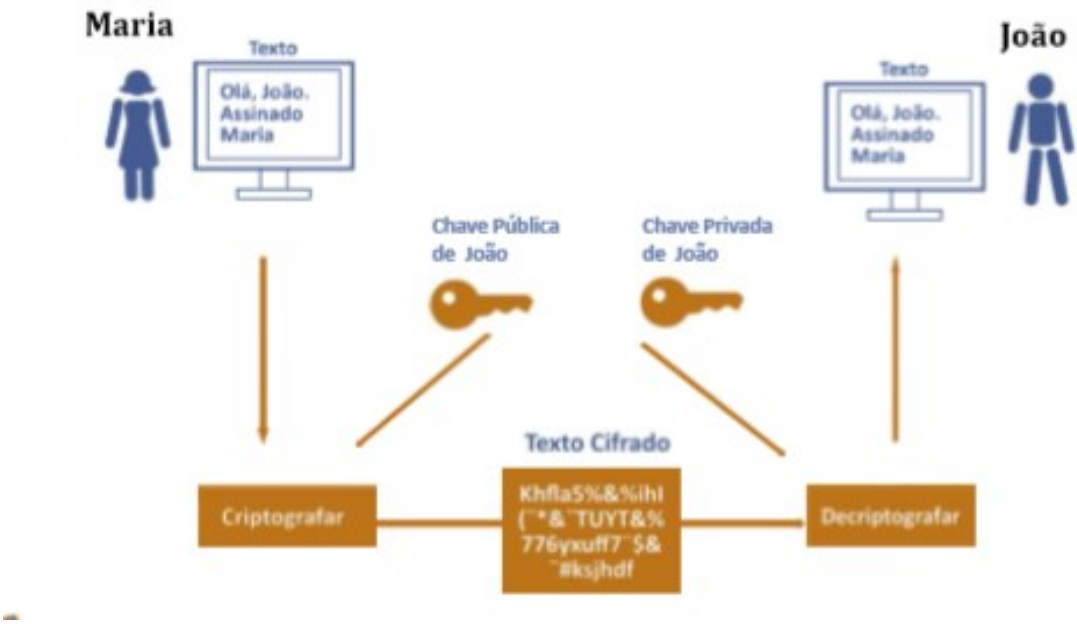
**Criptografia Assimétrica**

A criptografia assimétrica ou criptografia de chave pública utiliza um par de chaves diferentes, mas que são relacionadas matematicamente, chamadas de chave pública e chave privada. A chave pública pode ser disponibilizada livremente já a chave privada deve ser mantida em sigilo pelo seu titular (ITI, 2020a).

A relação entre o par de chaves pública e privada é o que permite que um texto cifrado por uma chave somente poderá ser decifrado pela sua chave complementar.

A criptografia assimétrica, é utilizada quando se quer inserir a característica de privacidade em uma troca de informações sigilosa, o emissor deverá encriptar a informação com a chave pública do receptor do texto claro, chave essa que é disponibilizada livremente. Deste modo apenas o receptor previsto poderá decifrar o texto cifrado já que somente ele possui a chave privada complementar a que foi utilizada no processo de encriptação. A Figura 4 ilustra e exemplifica o processo da criptografia assimétrica:

Figura 4: Sistema de criptografia assimétrica




Fonte: Certisign (2018)

A criptografia assimétrica é apresenta uma segurança maior que a criptografia simétrica, já que não é necessário que a chave privada seja compartilhada. Mesmo que a chave pública ainda assim possa ser manipulada, por ser utilizada uma chave privada em seu processo sua segurança é maior.

## 1.3 Função de resumo (*Hash*)

Uma função de resumo ou também conhecido como função *Hash* segundo o Cert.Br (2017) é um algoritimo matemático que quando aplicada sobre uma informação gera um resultado único e de tamanho fixo (normalmente 16 ou 20 bytes de extensão),

independentemente do tamanho da informação original, normalmente menor do que a informação que ele foi aplicado, chamado *hash*. Sendo esse processo unidirecional, ou seja, é praticamente impossível se obter a mensagem original através do *hash*. Por utilizar informação em bits, o *hash* é alterada a qualquer alteração que seja no conteúdo original. Sendo assim caso haja uma alteração de um bit, o valor do *hash* será diferente.

A função *hash* é então utilizada para verificar se a mensagem original está íntegra, uma aplicação para a função por exemplo seria no seguinte cenário: o emissor afim de provar a integridade de uma informação envia a um receptor o texto claro junto ao *hash* gerado dessa mensagem. O receptor por sua vez recebe o *hash* e sua respectiva informação e gera novamente o *hash* baseado na informação recebida. Comparando os dois *hashe* o receptor poderá confirmar se a mensagem foi alterada caso os dois *hashes* sejam idênticos.

Podemos citar alguns exemplos de funções *hash*: SHA-1, SHA-256 e MD5 (CERT.BR, 2017).

## 1.4 Assinatura Digital

Da mesma forma que a assinatura no mundo real tem a função de comprovar através da assinatura em forma escrita, que a entidade ou pessoal está vinculada formalmente ao documento assinado. Desta forma através da assinatura é declarado formalmente as entidades ou pessoas que assinam o documento estão de acordo com as informações contidas nele, não permitindo, que no futuro seja expresso desconhecimento dos termos.

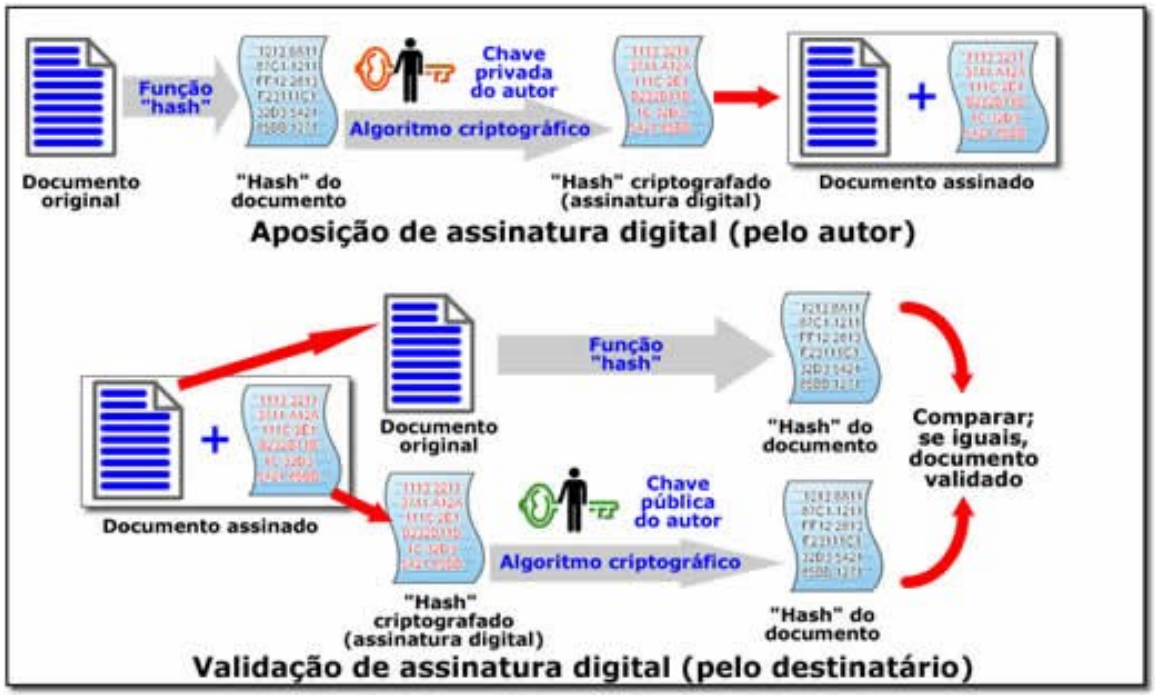
O conceito da assinatura digital é o mesmo, apesar de não ser uma declaração escrita. Uma imagem de uma assinatura em um documento digital não pode comprovar a autenticidade já que a origem dessa imagem não está relacionada ao dono dessa necessariamente.

O processo da assinatura digital funciona da seguinte forma: primeiro é aplicado uma função de *hash* a mensagem que o emissor deseja assinar, então utilizando sua chave privada ele criptografa o resumo gerado pela função *hash*, o resultado é denominado Assinatura Digital da mensagem (SILVA, 2008).

Essa Assinatura digital será anexada a mensagem e enviada ao receptor, que ao recebê-las irá decifrar a assinatura utilizando a chave pública do emissor, obtendo o resumo. Logo após o receptor aplica a mesma função *hash* utilizada pelo emissor ao documento recebido obtendo assim um segundo resumo. Desta forma o receptor compara os dois resumos que possui, e verifica se são os mesmos. Casos os dois resumos sejam iguais o documento está íntegro.

Conforme a Figura 5 ilustra o processo de assinatura digital:

Figura 5: Processo de Assinatura Digital




Fonte: overbr (2018)

## 1.5 A Certificação Digital

A certificação digital é definida pelo Instituto Nacional de Tecnologia da Informação como “[..]uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meio eletrônico[..]” (ITI, 2020a).

Essas técnicas e processos consideram os pilares da segurança da informação: integridade, autenticidade e confidencialidade. A certificação digital é uma tecnologia de identificação que tem por objetivo evitar adulterações e interceptações de informações privadas ou outros tipos de ameaças que possam prejudicar de alguma maneira a informação ou o transporte dela.

Ou seja, essa tecnologia funciona como uma “identificação eletrônica” que valida não só eletronicamente, mas também juridicamente a procedência da informação e a integridade dela no ambiente eletrônico.

AZEVEDO et. Al (2009) o conteúdo de um certificado digital normalmente é composto de:

- Informações sobre a entidade que emitiu o certificado digital (nome, e-mail, CPN / CNPJ, etc.);
- Chave pública refere-se à chave privada detida pela entidade especificada no certificado;
- Prazo de validade;

- A empresa que emitiu o certificado digital (Autoridade Certificadora);
- Número de série do certificado digital;
- Localização do "centro de revogação" (URL[2] para baixar a lista de certificados revogados ou localização para pesquisa OCSP[3]);
- Assinatura digital da Autoridade Certificadora.

O Certificado digital permite que as informações sejam transmitidas por meio digitais com maior segurança, já que esses Certificados digitais são emitidos por uma Autoridade Certificadora (AC) que garante a autenticidade desse certificado digital. É baseado no fundamento de uma terceira parte confiável, que oferece confiabilidade entre os envolvidos que utilizam os Certificados Digitais. Deste modo, existe uma Infraestrutura de chaves públicas, cuja principal função é definir técnicas e procedimentos (SILVA, 2008).

A Infraestrutura de chaves públicas Brasileira (ICP-Brasil), foi estabelecida com a medida provisória 2.200-2 (BRASIL, 2001).

[2] URL é a abreviação de Uniform Resource Locator, ou Localizador Uniforme de Recurso. URL é o mesmo que endereço web, o texto apresentado na barra de endereços dos navegadores ao acessar um website.
[3] OCSP (do inglês Online Certificate Status Protocol - OCSP) é um protocolo de Internet usado para obter o status de revogação de um certificado digita.

# 2 CERTIFICADO DIGITAL ICP-BRASIL

Como vimos a criptografia assimétrica apresenta uma maior segurança, sendo assim é a mais recomendada para transmissão de mensagens e informações por meios eletrônicos. Porém como já citado ainda assim temos a vulnerabilidade da chave pública que pode ser manipulada, adulterada ou até mesmo substituída.

A tecnologia dos Certificados Digitais, apresenta uma solução a essa vulnerabilidade, já que ele define um sistema de padrões para os certificados digitais uniformemente, garantindo mais confiabilidade.

O Certificado Digital que pertence Infraestrutura ICP-Brasil, é gerado e assinado por uma terceira parte confiável, uma Autoridade Certificadora (AC). Essa assinatura deve estar associada a "[..]uma entidade, pessoa, processo servidor a um par de chaves criptográficas[..]" (ITI, 2020a).

As ACs atestam a identidade do usuário no momento da emissão do certificado digital. Uma analogia, para entendermos melhor o funcionamento das autoridades certificadoras, as Autoridades Certificadoras funcionam como o DETRAN em relação a carteira de motorista, é a entidade responsável por licenciar o certificado digital.

Como a ITI descreve "[..]no procedimento da emissão, são verificados os dados pessoais de cada adquirente, conforme a Política de Segurança de cada Autoridade Certificadora[..]" (ITI,2020). Sendo assim a AC verifica os dados do adquirente validando assim a utilização desse certificado digital em meios eletrônicos.

## 2.1 Estrutura ICP Brasil

O modelo adotado pelo Brasil para sua infraestrutura de chaves públicas é o de certificação com raiz única, sendo o ITI, o resposável de Autoridade Certificadora Raiz (AC-Raiz), e possui a função de credenciar e descredenciar as demais entidades pertencentes a hierarquia, além de supervisionar e auditar os processos relacionados as chaves públicas (ITI ,2017).

A ICP Brasil é gerenciada pelo Comitê Gestor da ICP- Brasil normativamente e, conforme o Decreto 6.605 de 14 de outubro de 2008 definiu, o comitê "[..]exerce a função de autoridade gestora de políticas da referida Infra-Estrutura[..]", o comitê é formado por "[..]doze membros e respectivos suplentes, sendo cinco representantes da sociedade civil, integrantes de setores interessados[..]" e membros de ministérios que possam estar relacionados a esturutra (BRASIL, 2008).

Em resumo a estrutura da ICP Brasil está em formato de arvore, de forma hierárquica. A AC Raiz está no topo da hierarquia, nesse caso o ITI é a AC Raiz, logo após as ACs de

nível 1, então as ACs de nível 2 e as Autoridades de Registro (AR) (ITI, 2021a).

Hoje existem diversas ACs abaixo da AC raiz, abaixo uma lista das ACs de nível 1 pertencentes a Estrutura ICP (ITI, 2021a):

- AC CERTISIGN
- AC CERTISIGN ICP BRASIL CODE
- AC CERTISIGN ICP-BRASIL SSL
- AC DEFESA
- AC DIGITAL MAIS
- AC DIGITALSIGN ACP
- AC DOCCLOUD
- AC IMPRENSA OFICIAL SP
- AC INMETRO
- AC JUS
- AC MRE
- AC PR
- AC PRODEMGE BR
- AC RFB
- AC SAFEWEB
- AC SERASA SSL EV
- AC SERPRO
- AC SERPRO SSL
- AC SOLUTI
- AC SOLUTI CS EV
- AC SOLUTI SSL EV
- AC VALID
- AC VALID CODESIGNING
- AC VALID SSL EV
- SERASA ACP

Abaixo das ACs de nível 1 existem as ACs de nível 2, ou as ARs, isso varia de acordo como a AC se organiza, a lista de ACs de níveis 2 e ARs é extensa, já que desde que a estrutura da ICP foi instituída diversas ACs de níveis 2 e ARs foram credenciadas, e muitas outras foram credenciadas nos últimos anos.

Importante destacarmos que como podemos ver, apesar do processo de certificação digital ser monitorado e regularizado por órgãos governamentais, ele não é concessão pública, e sim uma atividade privada.

mas as vezes vamos chamar aqui elas podem ser entidades públicas ou privadas

### Autoridade Certificadora Raiz da ICP-Brasil (AC Raiz)

A Autoridade Certificadora Raiz é a primeira autoridade da hierarquia que compõe o processo de certificação digital no Brasil, ela executa as principais políticas, normas técnicas e operacionais, que o Comitê Gestor da ICP Brasil aprovar. Sua função é emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras dos níveis abaixo do seu. Ela também emite a Lista de Certificados Revogados – LCR e fiscaliza e audita as ACs, ARs e outras entidades pertencentes a ICP-Brasil (ITI, 2020b).

### Autoridade Certificadora (AC)

As Autoridades Certificadoras abaixo da AC Raiz, podem ser entidades públicas ou privadas, que na hierarquia da ICP-Brasil respondem diretamente a ela e as normas definidas pelo Comitê Gestor. Possui as funções de emitir, distribuir, renovar, revogar e gerenciar certificados digitais, verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado, cria e realiza a assinatura digital do certificado do assinante, comprovando a identidade do titular (ITI, 2020b).

Além disso a AC também tem a responsabilidade de emitir LCR e manter seus registros operacionais e sempre cumprindo as práticas definidas na Declaração de Práticas de Certificação – DPC, que é um documento que é publicado e revisado periodicamente, nele estão contidas as práticas e procedimentos que envolvem a certificação digital (OLIVEIRA ,2020). Além disso também é responsável por estabelecer e credenciar novas ARs e faze-lás cumprir as políticas de segurança da informação que garantam a autenticidade das identificações dos certificados digitais emitidos (ITI, 2020b).

### Autoridade de Registro (AR)

A Autoridade de Registro, se encontra logo abaixo das ACs, e é responsável por realizar a conexão entre o usuário do certificado digital e a AC. Toda AR deve estar vinculada em uma AR, ela tem a função de receber, validar e encaminhar as solicitações de emissões de certificados digitais, identificar de forma presencial os solicitantes desses certificados digitais e de mesmo modo deve manter registros operacionais (ITI, 2020b).

### Autoridade Certificadora do Tempo (ACT)

Uma Autoridade Certificadora do Tempo é uma entidade em que os usuários do serviço de carimbo do tempo confiam as emissões desses carimbos. O ACT é responsável por fornecer o Carimbo do Tempo com data e hora, que é um conjunto de atributos fornecidos

pela parte confiável do tempo, que é associado a uma assinatura digital e fornece a prova de sua existência dentro de um determinado período de tempo (ITI,2020b).

### Prestador de Serviço de Suporte (PSS)

Prestador de Serviço de Suporte, são empresas contratadas por uma Autoridade Certificadora, Autoridade de Registro ou uma Autoridade de Carimbo do Tempo para disponibilizar infraestrutura física, lógica ou recursos humanos especializados desempenhando atividades das Políticas de Certificado – PC definidas pelo Comitê Gestor e na DPC de seu contratante (ITI, 2020b).

### Prestador de Serviço Biométrico (PSBio)

Um Prestador de Serviço Biométrico Provedora de Serviços Biométricos-PSBio é uma entidade com capacidade de realizar tecnologia biométrica, realizando o cadastro único do solicitante do certificado digital para um ou mais bancos/sistemas de dados biométricos disponibilizando para toda ICP-Brasil através da verificação biométrica do solicitante. E compara as características biológicas com características perenes e únicas de acordo com os padrões internacionais (ITI, 2020b).

## 2.2 Aumento do Mercado

Em 2019 o mercado de certificação digital alcançou o maior índice de crescimento em 18 anos (GARCIA ,2019). E o mercado só vem aumentando com o passar dos anos, muito por conta da simplificação no processo de credenciamento de novas ARs.

Com a atualização dos DOC-ICP, que são as resoluções da ICP-Brasil em vigor, pela Resolução 151 de 30 de Maio de 2019 (BRASIL, 2019), houve uma simplificação do credenciamento de novas ARs. Como descrito pelo Art. 12 as Instalações Técnicas, Instalações Técnicas Secundárias, Postos Provisórios de Autoridades de Registro e os Prestadores de Serviço de Suporte de AR, bem como as cotas para emissão externa e obrigatoriedade do georreferenciamento, foram extintas.

Isso reduziu os custos de novas ARs, já que todas essas instalações e cotas geravam custos, além de requerimentos físicos, aberturas de filiais e outras burocracias que foram extintas, permitindo assim que a ARs e pontos de atendimento de ARs sejam mais simples e práticos de serem credenciados.

Hoje, o agente registrado só precisa estabelecer vínculo empregatício com a AR e seu nome publicado no CAR (Cadastro do Agente de Registro). O agente registrado pode se mover livremente e usar sua estação de trabalho para verificar documentos, coletar dados

biométricos de clientes e, em seguida, emitir certificados (GARCIA, 2019).

# 3 A APLICAÇÃO DO CERTIFICADO DIGITAL

Com a publicação da medida provisória 2200-2/01 em 2001, sendo essa à medida que que instituiu a ICP-Brasil ou Infraestrutura de Chaves Públicas Brasileira, documentos ou transações digitais que forem assinadas digitalmente por um certificado digital emitido e que esteja de acordo com as normas e regulamentos da ICP-Brasil tem a mesma validade jurídica que documentos que foram emitidos por procedimentos tradicionais (BRASIL, 2001). A publicação dessa medida permitiu então que fossem implementados projetos técnicos por meio de informações digitais confiáveis e seguras e com um suporte jurídico.

Desde a sua implementação em 2001, o setor de certificados digital apresenta um contínuo crescimento (SERASA, 2016). Com a pandemia, esse mercado trouxe novidades, aumentando ainda mais o leque de atividades do ramo. Durante esse período, o crescimento e a clareza do que as assinaturas digitais podem fornecer para as empresas alcançaram ainda mais visibilidade.

O Instituto Nacional de Tecnologia de Informação (ITI) publica a quantidade de certificados com o passar dos anos em 2010, nove anos após o começo da utilização do certificado digital no Brasil o número de emissões já era de mais de um milhão de certificados digitais emitidos (ITI, 2010). A quantidade das emissões só aumentou com o passar dos anos, foram quase 5 milhões de certificados digitais emitidos em 2019 antes da pandemia provocada pela COVID-19 (ITI, 2019).

Ou seja, só em 2019 a quantidade de emissões do ano foi aproximadamente o quíntuplo do total de certificados emitidos até 2010. E ao contrário de muitos setores que sofreram retrocessos por conta dos obstáculos e novos desafios causados pela pandemia, o setor de certificação digital cresceu ainda mais durante esse período, quebrando o recorde de emissões mensais a cada novo mês. Como o próprio ITI (ITI, 2021b) publicou em um de seus artigos “são mais de 10 milhões de certificados digitais ativos no país, sendo quase 6,5 milhões deles emitidos apenas nos últimos 12 meses”.

Esse aumento ocorreu devido a diversos fatores, entre eles, a nova forma de emissão de certificado digital por videoconferência regulamentada pela instrução normativa nº 05 de 22 de fevereiro de 2021 (BRASIL, 2021), que permite que a emissão do certificado digital seja feita remotamente, dispensando assim a necessidade de que o proprietário do certificado digital esteja fisicamente no momento da emissão do certificado, disponibilizando assim uma opção ainda mais prática e viável para a emissão do certificado digital, facilitando mais o processo para se obter o certificado.

Outro fator que contribuiu para o aumento das emissões do certificado digital são as novas soluções em que o certificado digital está sendo usado como facilitador de processos que antes eram totalmente analógicos, processos esses que serão abordados mais

detalhadamente nesse capítulo.

Deste modo o cenário da certificação digital já crescia antes mesmo das crises causadas pela COVID-19, já que a transformação digital que está ocorrendo nas organizações anda junto a certificação digital. Afinal, com esta ferramenta, além de satisfazer as obrigações das autoridades governamentais, é possível realizar negócios em todo o mundo com muito mais segurança, praticidade e agilidade.

## 3.1 Segurança proporcionada pelo certificado digital

No cenário atual pandêmico, além da preocupação causada pelo próprio vírus da Covid-19, as empresas e organizações governamentais, também devem se atentar com o aumento de ataques cibernéticos que vem ocorrendo, aumento esse que se deve muito ao fato da vulnerabilidade dessas organizações ter aumentado devido a muitas delas passarem a utilizar o acesso remoto dos sistemas via home office.

Um levantamento feito pela empresa russa de cibersegurança Kasperky entre fevereiro e abril de 2020, período que teve início a pandemia, houve um aumento de 333% de ataques cibernéticos realizados a ferramentas que permitem acesso remoto no Brasil (OLIVEIRIA; ROSSI, 2020).

A pandemia forçou com que milhões de organizações tivessem que adotar o Home Office da noite para o dia, e a grande maioria dessas organizações não possuíam uma estrutura segura nem o treinamento necessário para lidar com as vulnerabilidades inerentes ao Home Office. Deste modo, o número de vulnerabilidades aumentou e os hackers maliciosos vem se aproveitando desse cenário.

O Certificado Digital aliado a outras tecnologias se apresenta como uma das alternativas para se obter uma maior segurança e credibilidade. O acesso via VPN (Virtual Private Network) por exemplo, permite que usuários utilizem redes privadas e que seja realizado a troca de dados criptografados, essa tecnologia combinada ao uso de certificados digitais, garante a identificação dos profissionais que a estão utilizando, evitando que acesso indevidos sejam realizados a essa rede privada, criando assim um ambiente seguro para o ambiente online da empresa.

Como o certificado digital, como mencionado anteriormente, funciona como identidade virtual ele pode ser utilizado para validar a identidade de um usuário, permitindo assim que apenas usuários que possuam permissão para isso, acessem a rede VPN, impedindo assim invasores a essa rede privada.

Além de um aliado a VPN, que o torna uma validação na utilização dessa tecnologia aumentando ainda mais a segurança em sua utilização, o certificado oferece opções de segurança e facilidades para profissionais de diversas áreas.

## 3.2 Microempreendedor Individual

Para os profissionais liberais e para os profissionais autônomos o certificado é utilizado hoje para as emissões de notas fiscais eletrônicas (NFEs), embora a emissão de NFEs não seja obrigatória para os microempreendedores individuais (MEIs) quando a venda ou o serviço prestado é direcionado para pessoas físicas, a NFE torna-se necessária nas vendas para pessoas jurídicas (VHSYS, 2021).

De acordo com a sua localidade, existem especificidades, leis e procedimentos para emissão de nota fiscal eletrônica. Em muitos municípios não é permitido a emissão de NFEs sem o certificado digital, e os procedimentos que podem ser utilizados para emitir notas ficais eletrônicas sem o certificado, nos municípios que permitem esse tipo de emissão, podem causar infrações e possíveis punições caso não seja realizado o procedimento corretamente (ARTUS, 2020).

No entanto, com um certificado, tudo o que você precisa fazer é comprar um software de emissão de notas e se registar na Secretaria da Fazenda de seu estado, e você pode emiti-los remotamente.

## 3.3 Contabilidade

Quando se trata de área contábil o certificado digital se tornou essencial pois ele permite que profissionais dessa área realizem diversas transações obrigatórias de forma prática e segura.

Quando falamos de contabilidade e trabalho remoto, o foco é o acesso total ao portal e-Social (dedicado a simplificar o cumprimento de obrigações auxiliares como GFIP e Caged) e e-CAC (portal IRS). A lista de serviços que podem ser obtidos apenas fornecendo certificados digitais através do e-CAC é muito extensa, e está disponível no site oficial da receita (RECEITA FEDERAL, 2021), podemos destacar:

> Consulta e emissão de Comprovante de Inscrição e de Situação Cadastral no CNPJ;
> consulta aos dados cadastrais no CPF;
> Consulta Quadro de Sócios e Administradores no CNPJ;
> Atualizar o endereço no cadastro CPF;
> Extrato de malha fiscal;
> Obtenção de cópia de exercícios ficais;
> Assinatura e transmissão da DCTFWeb etc.

## 3.4 Direito

O certificado digital específico para profissionais do direito é o eJurídico, tornou-se uma realidade para os advogados. Antes mesmo da pandemia, o certificado proporcionava

aos profissionais a comodidade de acessar petições e citações, emitir autorizações e acompanhar o processo sem a necessidade de recorrer a fóruns. Na situação atual, garantir que o trabalho prossiga sem problemas e evitar a exposição tornou-se um problema (VALID, 2020).

No processo de garantia do acesso aos advogados através da utilização da certificação digital, podemos citar os seguintes sistemas:

- e-Pet – Peticionamento Eletrônico;
- e-Doc – Sistema da Justiça do Trabalho;
- Cert- JUS – Superior Tribunal de Justiça, o Conselho da Justiça Federal e toda Justiça Federal (VALID, 2020).

Ainda, o certificado digital possibilita ao profissional assinar contratos e transações online com total validade jurídica.

## 3.5 Recursos Humanos

Por sua vez, além das funções e facilidades padrão dos certificados digitais, os profissionais de RH também podem encontrar oportunidades de RH digital e sem papel em assinaturas digitais.

Os documentos atualmente impressos na área de recursos humanos podem ser digitalizados e assinados digitalmente de acordo com o padrão ICP-Brasil - isso só pode ser feito por meio de certificados digitais. Com documentos digitais, você pode acessá-los a qualquer hora, em qualquer lugar, inclusive trabalhando em casa.

Durante o trabalho remoto, outro possível aliado para profissionais de RH é o carimbo de tempo, também conhecido pelo nome em inglês *timestamp*. Um carimbo de data / hora é um certificado digital usado para garantir a oportunidade da criação, assinatura ou modificação de um documento (VALID, 2020).

Na prática, o *timestamp*, desde que emitido por uma Autoridade de Carimbo do Tempo (ACT), atesta, com validade jurídica, que algo aconteceu em dado momento. Empresas que trabalham com ponto eletrônico, por exemplo, podem adicionar uma nova camada de segurança jurídica com o carimbo do tempo.

## CONSIDERAÇÕES FINAIS

Com a crise da saúde pública e econômica recente, um dos principais esforços foi o de se evitar o contato físico entre as pessoas, já que essa era a principal recomendação dos principais órgãos de saúde do mundo. Sendo assim a utilização de recursos eletrônicos que fizessem essa função de reduzir o contato físico se tornaram essenciais para, principalmente nas questões de contratos, renovações de contratos entre outros assuntos jurídicos.

Com Decreto nº 10.278, de 18 de março de 2020, que regulamenta parte do artigo 3º da Lei nº 13.874/2019 (BRASIL, 2020), os documentos digitais passaram a produzir os mesmos efeitos jurídicos que os documentos físicos ou originais. Diante da crise de saúde, o uso de assinaturas digitais e métodos de autenticação em pagamentos, convênios, contratos e documentos tornou-se mais necessário.

Já estamos saindo do momento de pandemia, muitas atividades já retornaram a sua normalidade, porém o que podemos observar, é os métodos tecnológicos que foram implementados ainda permanecerão ativos, pois mesmo antes dessa crise na saúde mundial, a certificação digital vinha sendo adotada por várias empresas.

Assim através da certificação digital as pessoas podem hoje além de permanecerem mais seguros, economizam tempo, gastos.

A tecnologia trouxe grandes mudanças para as organizações, visando melhorar a agilidade, segurança e inovação dos processos administrativos. Através do isolamento social, é possível garantir a saúde dos colaboradores, realizar as suas atividades e utilizar a certificação digital, para promover a aprovação de contratos e documentos que geralmente requerem autenticação.

Além de permitir também que os colaboradores possam acessar a rede empresarial de forma segura através da certificação digital, permitindo que a empresa controle o acesso a rede e a segurança da mesma e dos colaboradores que a utilizam.

A certificação digital se mostrou e se mostra uma tecnologia importantíssima para a evoulução dos processos dentro das organizações e a partir dela foi e é possível realizar processos que antes só eram possíveis fisicamente, mas que hoje podem ser feitos de maneira eletrônica e o mais importante segura.

## REFERÊNCIAS BIBLIOGRÁFICAS

AFONSO, Monica Gonçalves. **O que é segurança da informação?.** 2018. Disponível em: https://medium.com/crypt0-women/o-que-é-segurança-da-informação-9185d18dcd9f Acesso em: 20 set. 2021.

ARTUS, Rodrigo. Como emitir NFS-e sem certificado digital?. **Migrate**. 2020. Disponível em: https://migrate.info/blog/como-emitir-nfs-e-sem-certificado-digital/. Acesso em: 8 mai. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO/IEC 27002:2013:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: 2013

AZEVEDO, Omsmar Reis: MARIANO, Paulo Antonio. **Sped - Sistema Público de Escrituração Digital**. 1º São Paulo: Iob, 2009.

BRASIL. **Lei nº 1850, de 17 de setembro de 1850**. Manda reger no exercício de 1851 a 1852 a Lei do Orçamento Nº 555 de 15 de Junho do corrente ano. Rio de Janeiro, 17 set. 1850. Disponível em: https://legis.senado.leg.br/norma/542104/publicacao/15632072. Acesso em: 22 nov. 2021.

BRASIL. **Medida provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasilia, DF, 24 ago. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm#:~:text=MEDIDA%20PROVIS%C3%93RIA%20No%202.200,autarquia%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 22 nov. 2021.

BRASIL. **Decreto nº 6605, de 14 de outubro de 2008.** Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC. Brasilia, DF, 14 out. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6605.htm. Acesso em: 18 nov. 2020.

BRASIL. **Resolução nº 151, de 30 de maio de 2019**. Regulamenta requisitos para conformidade ao Programa WebTrust de Princípios e Critérios para as entidades da ICP-Brasil e simplifica processos da ICP-Brasil. Brasilia, DF Edição 114, Seção 1, p.

1, 14 jun. 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-151-de-30-de-maio-de-2019-163675789#:~:text=Regulamenta%20requisitos%20para%20conformidade%20ao,simplifica%20processos%20da%20ICP-Brasil. Acesso em: 10 nov. 2021.

BRASIL. **Decreto nº 151, de 18 de março de 2020**. Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. Brasilia, DF, 19 mar. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm. Acesso em: 22 nov. 2021.

BRASIL. **Instrução Normativa nº 5, de 22 de fevereiro de 2021**. Aprova a versão 4.0 do DOC-ICP-05.02, aprova a versão 2.0 do DOC-ICP-05.05 e altera o DOC-ICP-05.03 para prever a emissão de certificados digitais por videoconferência. Brasília, DF, 22 fev. 2021. Edição 34-A. Seção 1. p. 1. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-iti-n-5-de-22-de-fevereiro-de-2021-304617035. Acesso em: 3 mai. 2021

CARVALHO, Daniel Balparda. **Criptografia**: Métodos e Algoritmos. Editora Book Express, 2001.

CERTISIGN. Como a criptografia funciona no Certificado Digital?. **Blog Certisign**. 2018. Disponível em: https://blog.certisign.com.br/como-a-criptografia-funciona-no-certificado-digital/. Acesso em: 3 mai. 2021.

CERT.BR, Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para Internet.** Comitê Gestor da Internet no Brasil. 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em 3 mai. 2021.

Chatfield, T. (2012). **Como aproveitar ao máximo a era digital**. (J. Henrriques, Trad.) Alfragide: Lua de Papel.

GARCIA, André Pinto. O mercado de certificação digital alcança maior índice de crescimento em 18 anos de história com quase 30% em 2019. **Terra. 2019**. Disponível em: https://www.terra.com.br/noticias/dino/o-mercado-de-certificacao-digital-alcanca-maior-indice-de-crescimento-em-18-anos-de-historia-com-quase-30-em-2019,610ef04c3a5e012b0cb46802f9449963f2x3uech.html. Acesso em: 10 nov. 2021.

HILL, Jenny. Scribes in ancient Egypt. **Ancient Egypt Online**, 2018. Disponível em: https://ancientegyptonline.co.uk/scribe/. Acesso em: 4 nov. 2020.

ICP Brasil, InfraEstrutura de Chaves Públicas Brasileira. **GLOSSÁRIO ICPBRASIL**. 2007, Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/glossario-icp-brasil-versao-1-2-novo-2-pdf. Acesso em: 08/11/2021

ITI, Instituto de Nacional de Tecnologia da Informação. Emissão de certificados digitais supera um milhão em 2010. **Instituto de Nacional de Tecnologia da Informação**. 2010. Disponível em: https://antigo.iti.gov.br/noticias/17-indice-de-noticias/3257-emissao-de-certificados-digitais-supera-um-milhao-em-2010. Acesso em: 3 mai. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. ICP-Brasil. **Instituto de Nacional de Tecnologia da Informação**. 2017. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 12 dez. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. Mercado de certificação digital registra alta expansão no Brasil. **Instituto de Nacional de Tecnologia da Informação**. 2019. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/iti-na-midia/mercado-de-certificacao-digital-registra-alta-expansao-no-brasil. Acesso em: 3 mai. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. Certificação Digital. **Instituto de Nacional de Tecnologia da Informação**. 2020a. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/perguntas-frequentes/certificacao-digital. Acesso em: 27 set. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. Entes da ICP-Brasil. **Instituto de Nacional de Tecnologia da Informação**. 2020b. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil/entes-da-icp-brasil. Acesso em: 3 mai. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. Estrutura ITI. **Instituto de Nacional de Tecnologia da Informação**. 2021a. Disponível em: https://estrutura.iti.gov.br. Acesso em: 30 out. 2021.

ITI, Instituto de Nacional de Tecnologia da Informação. Março bate mais um recorde de emissões ICP-Brasil em 2021. **Instituto de Nacional de Tecnologia da Informação**. 2021b. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/indice-de-noticias/marco-bate-mais-um-recorde-de-emissoes-icp-brasil-em-2021. Acesso em: 3 mai. 2021.

LAGO, Laurenio. **Supremo Tribunal de Justiça e Supremo Tribunal Federal: dados biográficos** 1828-2001. 3. ed. Brasília: Supremo Tribunal Federal, 2001. p. 342-345. Disponível em: http://www.stf.jus.br/portal/ministro/verMinistro.asp?periodo=stf&id=177. Acesso em 4 nov. 2020.

OLIVEIRA, Regiane; ROSSI, Mariana. No submundo da internet, prospera o lucrativo negócio de chantagear empresas em meio à pandemia**:** Cibercriminosos criam verdadeiras empresas de sequestro de dados e extorsão, expondo informações de companhias como Cosan, Aliansce Sonae, Arteris e CPFL, e promovem leilões em tempo real. Ataques aumentam mais de 300% entre fevereiro e abril. **EL PAÍS**, São Paulo, 3 jul. 2020. Disponível em: https://brasil.elpais.com/tecnologia/2020-07-03/no-submundo-da-internet-prospera-o-lucrativo-negocio-de-chantagear-empresas-em-meio-a-pandemia.html. Acesso em: 5 maio 2021.

OLIVEIRA, Ângela Maria de. DPC – Um Guia Prático na Emissão de Certificados ICP-Brasil. **Instituto Nacional de Tecnologia da Informação**, 2020. Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/artigos/dpc-um-guia-pratico-na-emissao-de-certificados-icp-brasil. Acesso em: 08 nov 2021

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

**Receita Federal**. Serviços Disponíveis no Portal e-CAC. 2021. Disponível em: https://servicos.receita.fazenda.gov.br/servicos/servicos-ecac/default.aspx#wrapper. Acesso em: 11 nov.2021.

RIBEIRO, Denise. Com pandemia, demanda por videoconferências dispara em empresas brasileiras.**CNN Brasil**, 2020. Disponível em: https://www.cnnbrasil.com.br/business/2020/04/15/com-pandemia-demanda-por-videoconferencias-dispara-em-empresas-brasileiras. Acesso em: 18 nov. 2020.

SAGRERA, Renato. TJRS – Resolução estabelece normas para a digitalização de processos físicos no Judiciário. **Associação de Advogados de São Paulo**, 14 set. 2020. Disponível em: https://www.aasp.org.br/noticias/tjrs-resolucao-estabelece-normas-para-a-digitalizacao-de-processos-fisicos-no-judiciario/. Acesso em: 11 nov. 2020.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2014.

Serasa Experian. ICP-Brasil completa 15 anos com evolução tecnológica e fortalecimento dos processos. **Blog - Serasa Experian**. 2016. Disponível em: https://serasa.certificadodigital.com.br/blog/icp-brasil-completa-15-anos-com-evolucao-tecnologica-e-fortalecimento-dos-processos. Acesso em: 3 mai. 2021.

SILVA, Luiz Gustavo Cordeiro da; SILVA, Paulo Caetano da; BATISTA, Eduardo Mazza; HOMOLKA, Herbert Otto; AQUINO, Ivanilso Jose de Souza Júnior; LIMA, Marcelo Ferreira de. **Certificação Digital – Conceitos e Aplicações**, Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

SINGH, S. **O livro dos códigos**. 7. ed. Rio de Janeiro: Record, 2007.

SOUZA, Ramon de. 2,2 milhões de brasileiros foram vítimas de golpes virtuais em outubro. **Canal Tech**. Disponível em: https://canaltech.com.br/seguranca/2-2-milhoes-de-brasileiros-foram-vitimas-de-golpes-virtuais-em-outubro-174653/. Acesso em: 01 Dez. 2020.

TIZIANI, Marcelo Gonçalves. Uma breve história do registro civil contemporâneo. Jus.com.br, out. 2016. Disponível em: https://jus.com.br/artigos/52705/uma-breve-historia-do-registro-civil-contemporaneo#_ftn2. Acesso em: 30 oct. 2020.

Valid**. Como o certificado facilita o trabalho remoto na sua empresa**. **Blog – Valid**. 2020. Disponível em: https://blog.validcertificadora.com.br/como-o-certificado-facilita-o-trabalho-remoto-na-sua-empresa/. Acesso em: 15 nov. 2021

Vhsys. MEI precisa emitir notas fiscais? Saiba mais sobre as obrigações do Microempreendedor Individual. **Blog vhsys**. 2021. Disponível em: https://blog.vhsys.com.br/mei-pode-emitir-nota-fiscal/#:~:text=O%20MEI%20é%20obrigado%20a%20emitir%20nota%20fiscal%20em%20todas,nota%20se%20o%20cliente%20exigir. Acesso em: 8 mai. 2021.

ROSSI, Ythalo. Criptografia Digital. **YRoss**. 2010. Disponível em: https://yross.wordpress.com/2010/07/13/criptografia-digital/. Acesso em: 30 oct. 2021.