ASSINATURA DIGITAL NAS EMPRESAS.

SIGNATURE IN DIGITAL COMPANIES.

Thais Torres Ribeiro[1]

Ângelo Ávila Mesquita[2]

RESUMO

O trabalho foi desenvolvido através de um estudo bibliográfico com enfoque na assinatura digital nas organizações, com o intuito de auxiliar nos processos administrativos, no isolamento social, otimização de tempo nos atendimentos e na redução do consumo de papel. O estudo da assinatura digital se faz necessário para evidenciar e demonstrar os benefícios na gestão empresarial e econômica, proporcionando redução de impactos ambientais ao reduzir o consumo de papel, além agilidade nas atividades, como: aprovação de contratos, liberação em geral nas execuções dos processos burocráticos. Visando um dos momentos de crise mundial, a pandemia do *Covid-19*, proporcionando o isolamento social, garantindo a preservação da saúde dos colabores e a oportunidade de dar continuidade nas demandas. O estudo foi realizado através de pesquisas bibliográfica, em livros e artigos científicos, revistas, para embasamento teórico. Evidenciando a importância da implementação do Sistema de Assinatura Digital com o objetivo de agilizar a comunicação e aprovação dos processos. Evidenciando as etapas para o desenvolvimento da assinatura digital, o entendimento do que é a assinatura digital, a diferença entre assinatura digital e assinatura eletrônica, criptografia, função do resumo *hash*, certificado digital, Autoridade certificadora, Segurança da Informação e Sustentabilidade nas empresas.

Palavras-Chave: Assinatura digital. Otimização. Pandemia. Aprovação. Criptografia. Certificado Digital.

ABSTRACT

The work was developed through a bibliographic study with a focus on digital signature in organizations, with the aim of assisting in administrative processes, social isolation, time optimization in attendance and reduction of paper consumption. The study of the digital signature is necessary to evidence and demonstrate the benefits in business and economic management, providing reduction of environmental impacts by reducing paper consumption, in addition to agility in activities, such as: approval of contracts, general release in the execution of processes bureaucratic. Aiming at one of the moments of global crisis, the Covid-19 pandemic, providing social isolation, ensuring the preservation of the

[1] Graduanda do Curso de Engenharia de Produção do Centro Universitário do Sul de Minas. E-mail: thais.ribeiro@alunos.unis.edu.br

[2] Professor orientador do Centro Universitário do Sul de Minas. Email: angelo.mesquita@professor.unis.edu.br

health of employees and the opportunity to continue demands. The study was carried out through bibliographic searches, in books and scientific articles, magazines, for theoretical basis. Evidencing the importance of implementing the Digital Signature System in order to streamline the communication and approval of processes. Evidencing the steps for the development of the digital signature, the understanding of what is the digital signature, the difference between digital signature and electronic signature, encryption, hash summary function, digital certificate, Certification Authority, Information Security and Sustainability in companies.

Keywords:. *Digital signature. Optimization. Pandemic. Approval. Cryptography. Digital certificate.*

1 INTRODUÇÃO

No trabalho em questão foi desenvolvido em um estudo bibliográfico com o enfoque na aplicação de assinatura digital nas organizações. Sendo necessário para auxiliar na otimização de tempo nos atendimentos aos colaboradores, clientes, fornecedores e contribuição para o isolamento social, redução do consumo de papel, proporcionando melhorias na gestão e comunicação com os setores envolvidos.

Com a necessidade de aprovação rápida nas demandas a assinatura digital será um meio de agilização e eficácia no desenvolvimento das atividades, principalmente as contratuais. Proporcionando a aceleração dos processos burocráticos da empresa através de um sistema de assinatura digital. Demonstrando os benefícios através da viabilidade para a organização.

O estudo da assinatura digital se faz necessário para mostrar como os aspectos e técnicas de um sistema eletrônico podem gerar benefícios na gestão empresarial e econômica, bem como auxiliar na agilização do processo de contratos e documentações em geral. Pois se trata da otimização e eliminação de resíduos de papel, proporcionando a redução de impactos ambientais. Além da agilidade da realização dos processos administrativos, principalmente na ausência dos responsáveis pela autorização das atividades em andamento. Um exemplo seria durante a pandemia do *Covid-19* onde o contato físico fica limitado, causando atraso em alguns processos que necessitam da assinatura dos Presidentes, Diretores e Gestores.

O estudo foi realizado através de pesquisas bibliográfica, em livros e artigos científicos, revistas, para embasamento teórico. Evidenciando a importância da implementação do Sistema de Assinatura Digital com o objetivo de agilizar a comunicação e aprovação dos processos.

O estudo foi realizado a partir do conhecimento sobre a assinatura digital, a diferença entre assinatura digital e assinatura eletrônica, criptografia, função do resumo *hash*, certificado digital, Autoridade certificadora, Segurança da Informação e Sustentabilidade, demonstrando as vantagens de implantação do sistema de assinatura digital.

2 ASSINATURA DIGITAL

Segundo a Digix (2019) a assinatura é importante tanto no setor privado quanto no setor público, pois uma das grandes demandas nesses setores é a otimização de processos, através da adoção de métodos e estratégias nas rotinas administrativas, que promovam melhorias e agilidades nos processos dos responsáveis pelas tomadas de decisões.

Conforme a FolhaCerta (2018), a assinatura digital possui vários benefícios como a praticidade, redução de gastos, segurança, sustentabilidade proporcionando facilidade na gestão das empresas, resultando em trabalhos realizados de forma prática e rápida, não exigindo longos processos e deslocamentos para outras localidades.

2.1 Definição da Assinatura Digital

Conforme Ferrari e Amaral (2020), a assinatura digital é uma tecnologia que utiliza a criptografia e vincula o certificado digital, através da tecnologia proporciona que equivalência ao documento assinado a próprio punho.

Segundo a InfoPath (2013), a assinatura digital é utilizada para autenticação de informações digitais, como modelos de formulários, e-mails e documentos, usando a criptografia do computador. As assinaturas digitais ajudam a garantir os seguintes fatores:

a) Autenticidade: ajuda a garantir que o assinante é quem ele diz ser;

b) Integridade: ajuda a garantir que o conteúdo não foi modificado desde que foi assinado digitalmente.

c) Não repúdio: ajuda a garantir a originalidade do conteúdo assinado para todas as partes.

De acordo com Silveira (2020), a assinatura digital conta com a tecnologia criptográfica do certificado digital para assinar um documento eletrônico equivalendo ao documento registrado em cartório.

Segundo a CERT.BR (2017), a assinatura digital permite comprovar a veracidade da informação, garantindo que realmente o documento foi gerado pelo autor responsável e confirma que ele não foi alterado.

Segundo Custódio (2003), uma assinatura tanto na forma manuscrita quando na forma digital, define um vínculo entre quem assina e o documento em si, porém na assinatura digital a ligação entre o autor e o documento é feita por algoritmo de autenticação. Os dois métodos de assinaturas estabelecem as mesmas finalidades de garantir ao criador que não seja alterado ou violado.

De acordo Monteiro (2007) uma assinatura no papel possui uma ligação entre a informação impressa e a pessoa que assina o documento. Já na assinatura digital um algoritmo que possibilita a união do autor com o objeto criado, através de um código que irá agir como assinatura.

Segundo Stallings (2008), a assinatura digital é método de que se refere como substituta da assinatura física. Garante a originalidade e a integridade das informações, onde a autenticação permite que o criador de uma mensagem possa anexar um código que atue como uma assinatura. Envolvendo dois processos criptográficos: o *hash* da mensagem e criptografando-a com a chave privada do autor.

Hoje duas são as principais técnicas empregadas para criptografar: a criptografia simétrica ou convencional (de chave privada) e a criptografia assimétrica (de chave pública) sendo que a segurança da criptografia, em qualquer de suas modalidades, relaciona-se diretamente com a consistência do algoritmo utilizado no processo e do tamanho da chave. (MARCACINI, 2002, p.40).

De acordo com Da Silva (2004), a assinatura digital é enviada somente pelo emissor, gerando um valor, onde apenas o receptor pode verificar através de um processo especifico, satisfazendo cinco critérios das assinaturas de papel, onde só o emissor conhece a sua chave privada, é autêntica, inalterável, não é reutilizável e intransferível. Qualquer alteração no documento, quanto na assinatura deixam de ser válidos. As assinaturas são comprovadas através da certificação digital, que é o mesmo método de comprovação da assinatura a próprio

punha que é realizado o reconhecimento de firma em cartório, que ajuda a associar entre pessoa física ou jurídica através de uma chave privativa a um objeto digital.

Zaccoli (2000) afirma que a Utah Digital Signature Actdefine definiu a assinatura digital como:

> Uma transformação de uma mensagem usando um sistema de criptografia assimétrica tal que uma pessoa, tendo a mensagem inicial e a chave pública do signatário possa, com precisão, determinar se: (a) a transformação foi criada usando a chave privada que corresponde à chave pública do signatário; e (b) a mensagem não foi alterada desde que a transformação foi feita. (ZACCOLI, 2000, p.183.)

Segundo Lacorte (2015) o documento asssinado de forma digital é reconhecido e validado juridicamente através da identificação de autoria e não violação da mensagem.

2.2 Diferença de Assinatura Digital e Assinatura Eletrônica

Segundo Silveira (2020) a assinatura eletrônica é o nome dado a todos mecanismos que permitem a assinatura de documentos digitais com validade jurídica, com o objetivo de identificar que assinou e validar o documento. Já a assinatura digital, trará um tipo de assinatura mais segura, pois é certificada pelo ICP-Brasil, onde o mesmo comprova a autoria da firma e utiliza criptografia para associar o documento assinado pelo usuário, equivalendo a assinatura a próprio punho reconhecida em cartório.

De acordo com Ferrari e Amaral (2020), a assinatura digital possui validade jurídica dos documentos eletrônicos, através da assinatura com certificação digital no padrão ICP-Brasil, onde possui o mesmo efeito do reconhecimento em cartório. Já a assinatura eletrônica tem a eficácia probatória de acordo com as evidências colhidas, tais como imagem, biometria, carimbo do tempo, código de acesso e chaves eletrônicas. A assinatura eletrônica é um conjunto de dados que conectam, de um lado, um documento eletrônico específico, e, de outro, uma determinada pessoa utilizando algum método de autoria, passando a ter validade jurídica.

2.3 Criptografia

Segundo a CERT.BR (2017), a criptografia é conhecida como a ciência e a arte de escrever mensagens em forma cifrada ou em código, onde é considerada umas das principais formas de mecanismos de segurança para proteger os usuários dos riscos associados a internet. A criptografia está integrada aos sistemas operacionais ou ela pode ser facilmente adicionada ao processo sistêmico. Possuindo termos empregados para criptografar de forma segura.

Quadro 1: Termo empregado em criptografia e comunicações via Internet.

Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de *bits*
Canal de comunicação	Meio utilizado para a troca de informações

Remetente	Pessoa ou serviço que envia a informação
Destinatário	Pessoa ou serviço que recebe a informação

Fonte: CERT.BR (2017)

De acordo com Marcacini (2002) as principais técnicas para criptografar são: a criptografia simétrica ou convencional (de chave privada) e a criptografia assimétrica (de chave pública).

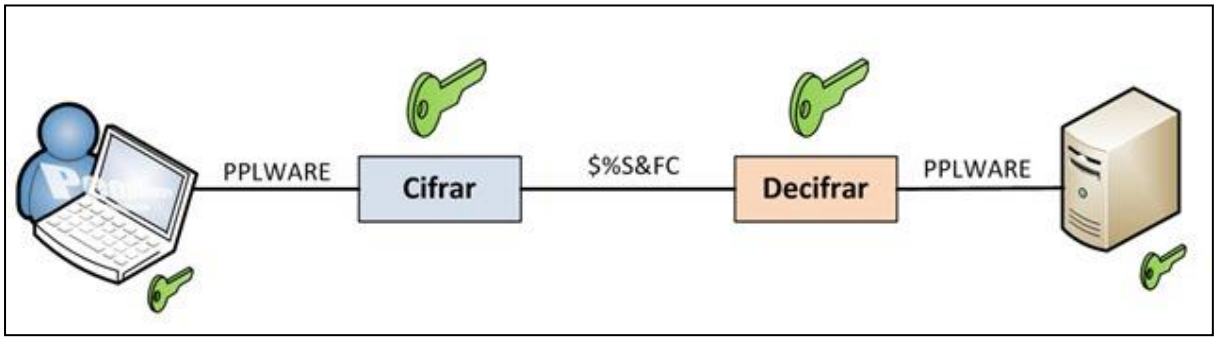
A Criptografia Simétrica é conhecida por chave secreta ou privada utilizada para cifrar e decifrar um texto. Já a Criptografia Assimétrica é caracterizada por um par de chaves, sendo uma pública e outra privada, onde uma é utilizada para cifrar e outra para decifrar, devendo ser utilizada a chave adequada nas mensagens. A chave pública é utilizada por todas as pessoas interessadas com o objetivo de validar com assinatura, diferente da privada que apenas o titular tem acesso e para assinar o documento. (MAIA; PAGLIUSI, 2006)

De acordo com Marcacini (2002) as principais técnicas para criptografar são: a criptografia simétrica ou convencional (de chave privada) e a criptografia assimétrica (de chave pública).

2.3.1 Criptografia Simétrica

Segundo a CERT.BR (2017), Criptografia de chave simétrica, também conhecida como chave secreta ou única, onde sua principal finalidade é garantir a confidencialidade dos dados, nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. A chave secreta deve ser previamente combinada por meio de um canal de comunicação seguro para não comprometer a confidencialidade.

Imagem 1: Criptografia Simétrica



Fonte: PPLWARE (2001)

De acordo com a CERT.BR (2017), também afirma que a chave simétrica quando comparada a assimétrica é mais indicada para garantir a confidencialidade de grandes volumes de dados, devido seu processo ser mais rápido.

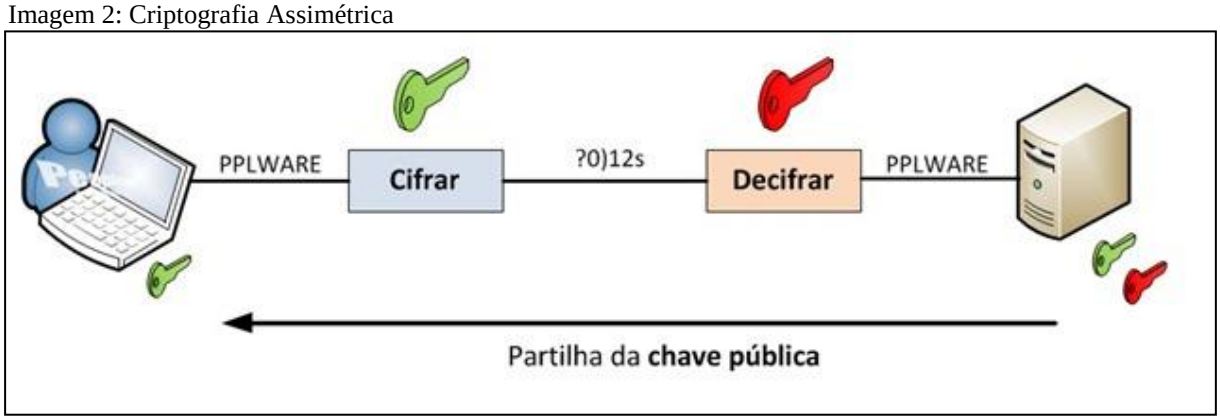
Segundo Pagliusi (2006) Criptografia Simétrica é conhecida por chave secreta ou privada utilizada para cifrar e decifrar um texto.

2.3.2 Criptografia Assimétrica

A Criptografia Assimétrica é caracterizada por um par de chaves, sendo uma pública e outra privada, onde uma é utilizada para cifrar e outra para decifrar, devendo ser utilizada a chave adequada nas mensagens. A chave pública é utilizada por todas as pessoas interessadas

com o objetivo de validar com assinatura, diferente da privada que apenas o titular tem acesso e para assinar o documento. (MAIA; PAGLIUSI, 2006)

Imagem 2: Criptografia Assimétrica



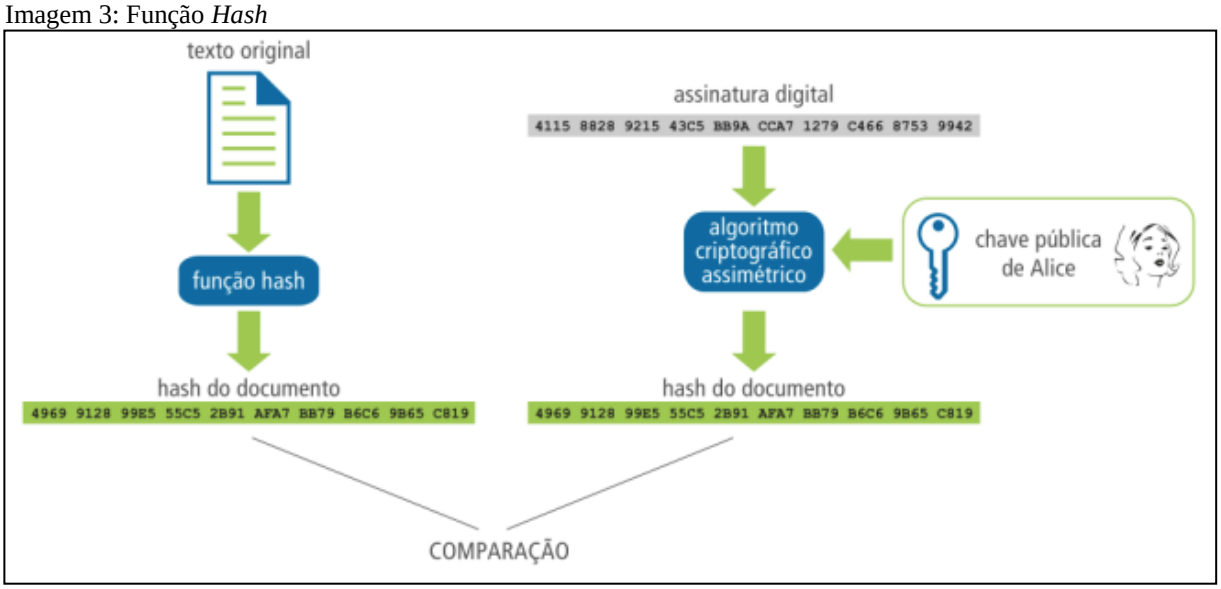
Fonte: PPLWARE (2001)

Segundo a CERT.BR (2017), a Criptografia de chaves assimétricas, conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que exige sigilo pelo usuário, podendo ser armazenada de diferentes formas, como por exemplo em um arquivo no computador. A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

2.3.3 Função de resumo *(Hash)*

Segundo a Cert.Br (2017), a função de resumo é um método criptográfico que, ele gera um resultado único e tamanho fixo, independentemente do tamanho do documento, é chamado *hash*[3]. Que é utilizado para verificar e a integridade de um arquivo armazenado no computador ou obtido pela internet, ele também proporciona a verificação se o arquivo foi corretamente transmitido.

Imagem 3: Função *Hash*



Fonte: Diego Macêdo (2012)

De acordo com Root (2019), um *hash* é uma sequência de bits geradas por um algoritmo, que permite a visualização em letras e números, ou seja, é a transformação de dados, de uma grande quantidade de informações para uma pequena.

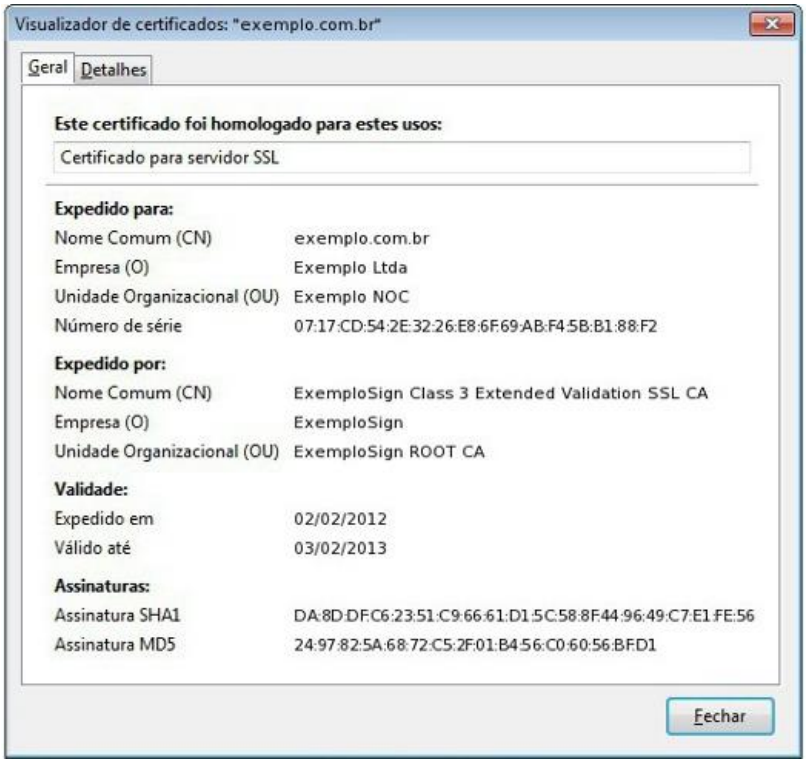
2.4 Certificado Digital

Conforme Macêdo (2012), é um documento eletrônico assinado que pode associar a uma pessoa ou entidade, onde essas informações são seguradas pelo certificado digital., que deve apresentar nome da pessoa ou entidade, período de validade e eficácia a ser associada a chave pública, período de validade do certificado, chave pública, nome e assinatura da entidade que assinou o certificado e o número de série.

De acordo com CERT.BR (2017) os certificados digitais são apresentados nos navegadores Web e padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais. De forma geral, os dados básicos que compõem um certificado digital são: versão e número de série do certificado; dados que identificam a AC que emitiu o certificado; dados que identificam o dono do certificado (para quem ele foi emitido); chave pública do dono do certificado; validade do certificado (quando foi emitido e até quando é válido); assinatura digital da AC emissora e dados para verificação da assinatura.

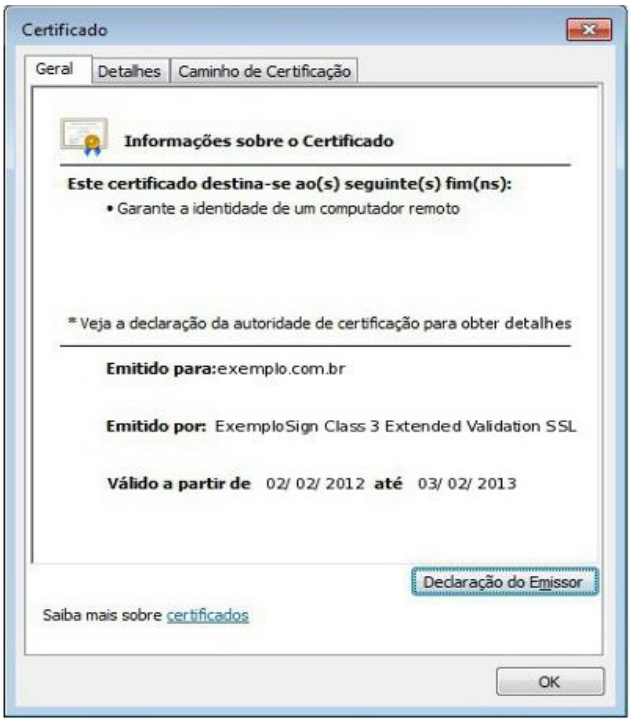
A imagem abaixo demonstra como o certificado digital foi homologado.

Imagem 4: Certificado Digital



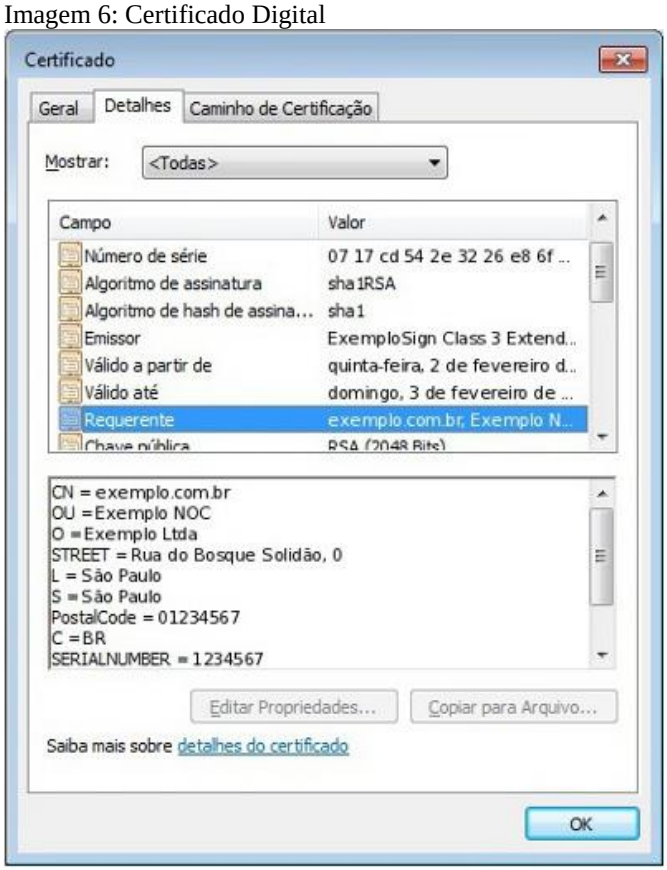
Fonte: CERT.BR (2017)

Imagem 5: Certificado Digital



Fonte: CERT.BR (2017)

Imagem 6: Certificado Digital



Fonte: CERT.BR (2017)

Segundo Barreto (2002), de modo a assegurar o seu uso confiável e a sua validade legal, bem como combater a fraude, a assinatura digital depende de técnicas confiáveis de geração, armazenamento e certificação, que garantam sua autenticidade.

De acordo com Rohrmann (2005), o documento assinado digitalmente ou por uma chave pública é validado através do certificado, que significa uma confirmação do objeto.

Segundo Lozupone (2018), para que os procedimentos técnicos sejam definidos é necessária uma política nacional de certificação digital.

O certificado digital é emitido com prazo de validade determinado, através de uma estrutura de dados sob a forma eletrônica, assinada eletronicamente por parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. (MENKE, 2005).

2.5 Autoridade Certificadora e Validade Jurídica

De acordo com a FolhaCerta (2018), a criação de Chaves Públicas Brasileira (ICP Brasil) desde o ano de 2001 os documentos digitais passaram a ter validade jurídica e podem ser utilizados no território nacional, substituindo totalmente o papel.

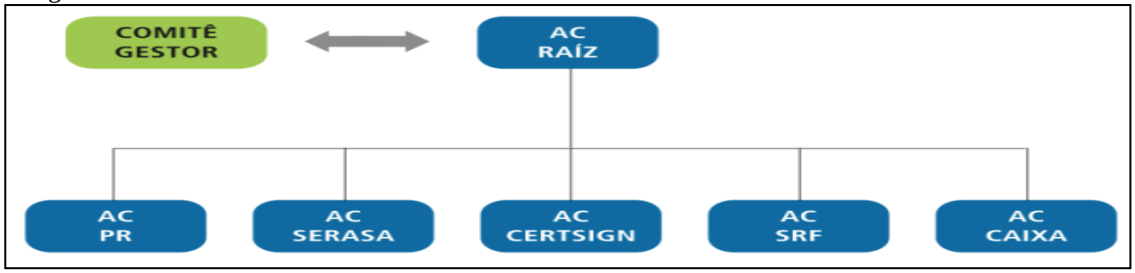
De acordo com Ferrari e Amaral (2020), a validade da assinatura digital e a admissibilidade legal são garantidas pelo Art. 10 da MP 2.200-2, que assegura a veracidade as declarações constadas nos documentos eletrônicos que utilizam o certificado digital. Tendo como um dos principais aspectos o não repúdio, isto é, previne que uma parte, possa agir de forma desonesta. O certificado digital pode ser utilizado tanto por pessoas físicas quanto por pessoas jurídicas, com diversas finalidades.

Segundo Gonzales (2020), a legislação brasileira reconhece e valida as assinaturas digital dos documentos eletrônicos em geral, podendo ser utilizada tanto a certificação através de Chaves Públicas Brasileira (ICP-Brasil), quanto qualquer outra, desde que com a anuência de ambas as partes e que permita a validação da integridade e autoria do documento (conforme Medida Provisória 2.200- 2/2001).

De acordo com Creci-RJ. (2020), a assinatura digital substitui o documento autentificado a próprio punho. Por meio da certificação a autenticação dos documentos, proporciona a verificação e guarda das informações digitais. São essas informações que irão indicar que a assinatura e o contrato são confiáveis e válidos. O processo de validade passa por três etapas principais: autenticidade, integridade e o não repúdio, cada uma dessas etapas é responsável por garantir que as informações presentes no documento são verdadeiras e confiáveis. Alguns dos dados coletados que dão confiabilidade a assinatura e ao contrato são os registros de data e hora, registros de IP e geolocalização, tokens e chaves de segurança e as informações pessoais como e-mail, data de nascimento e CPF.

Conforme Macêdo (2012), A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais.

Imagem 4: Autoridade Certificadora



Fonte: Diego Macêdo (2012)

Segundo o conceito de Brasil (2000), as chaves são entregues por autoridades de entidade e legal habilitada para exercer essa função, certificando o titular da assinatura digital da chave pública e da chave privada.

A autoria e a integridade do documento são dois elementos fundamentais que se destacam quanto sua eficácia, garantindo através da autenticação que o usuário não é falso, e visa a integridade e vericidade do documento após sua concepção. (GANDINI; JACOB; SALOMÃO, 2006).

A tempestividade é outro elemento relacionado à validade jurídica, consiste na protocolização digital, apontando a data e hora que o documento foi submetido ao processo de protocolização, garantindo que o mesmo foi produzido naquele determinado momento. (COSTA; CUSTÓDIO; DIAS, 2006).

2.6 Segurança da Informação

Segundo a FolhaCerta (2018), com a utilização da criptografia, são criados mecanismos que evitam que terceiros acessem os dados e utilizem para realização de transações ilícitas. Isso torna possível através da utilização de chaves privadas que possibilitam apenas pessoas autorizadas, com uso de senha, além do controle dos usuários que podem emitir ou criar documentos em nome da empresa.

Segundo Ferreira (2008), a Segurança da Informação é um dos termos mais importantes dentro de uma organização, devido à grande importância do sigilo e segurança das informações.

> [...] O Entendimento daquilo que precisa ser protegido está além do simples hardware e software que compõem os sistemas, abrangendo, também, as pessoas e os processos de negócio. Deve-se considerar o hardware, software, dados e documentação, identificando de quem esses elementos necessitam ser protegidos. Nesta análise, aspectos sobre a segurança dos dados, backup, propriedade intelectual e respostas a incidentes devem ser levados em consideração. (FERREIRA, 2008)

De acordo com Leal (2009), tanto os documentos físicos quanto os eletrônicos, devem conter medidas que impeçam sua alteração, garantindo que não tenha fraude ou qualquer outra alteração, sem a autorização do responsável pela emissão do documento. A integridade do documento eletrônico está ligada em assegurar que não sofreu nenhuma adulteração de conteúdo.

2.7 Sustentabilidade

Segundo a FolhaCerta (2018), a utilização dos recursos como a assinatura digital, proporcionam as organizações redução de papel e assim contribuem para a preservação do meio ambiente e dos recursos naturais.

De acordo com Leonardo (2020), todas as inovações impactam a vida das sociedades e ao redor, e no aspecto de mobilidade e agilidade as assinaturas digitais são resultados de eficiência e sustentabilidade sobre a economia de água, energia e reciclagem. Essas responsabilidades sociais vai além de um indivíduo e sim de toda sociedade.

2.8 Resultados Esperados

Segundo Aarãos (2017), muitas empresas estão implantando o sistema de assinatura digital, um exemplo é a Câmara de Comercialização de Energia (CCEE) que junto com a empresa *Certisign* desenvolveram um portal para que os documentos fossem assinados

digitalmente. Onde em seis meses foram assinados cinco mil contratos, envolvendo 141 empresas, resultando em uma economia de 35% devido à redução de papel, deslocamento e autenticações.

De acordo com a Infoco (2019), além da redução de custos que a assinatura digital proporciona as organizações, gera-se ganho de espaço físico, agilidade e qualidade nos atendimentos, melhoria na relação com fornecedores, colaboradores e demais envolvidos nos processos administrativos.

3 METODOLOGIA

O método a ser utilizado caracteriza-se de natureza básica, realizado através de pesquisas bibliográficas, artigos científicos de tecnologia da informação/comunicação que abrangerá estudos tecnológicos com base qualitativa nos resultados referentes à assinatura digital.

O estudo possui finalidade exploratória através de pesquisas, a fim de conhecer diferentes contribuições cientificas disponíveis sobre o uso da assinatura digital, no cenário atual de crise na saúde, no período de maio a outubro do ano de 2020, analisando os processos e necessidades dessa aplicação.

Na realização das pesquisas será possível identificar a praticidade e agilidade na execução das atividades, como por exemplo, o caso da Pandemia do Novo Coronavírus (*Covid-19),* onde os colaboradores passaram a trabalhar em home office devido ao isolamento social, trazendo dificuldades nas aprovações das atividades realizadas, contratos e por se tratar de documentos que possuem obrigatoriedade as assinaturas dos responsáveis. O estudo evidenciará e demonstrará a importância da assinatura digital.

Na aplicação do estudo, serão consideradas todas as informações necessárias, que contribuem para aplicação do sistema de assinatura digital nas organizações.

4 RESULTADOS E DISCUSSÕES

Segundo Ferrari e Amaral (2020), no cenário atual da crise de saúde pública e econômica, com o objetivo de evitar o contato físico entre as pessoas, a fim de reduzir a transmissão do vírus e preservar a saúde dos envolvidos, a utilização de recursos tecnológicos se tornam indispensáveis, principalmente nas questões de contratos, renovações de documentos e entre outros assuntos de relações jurídicas. Com a oportuna publicação do Decreto nº 10.278, de 18 de março de 2020, que regulamenta parte do artigo 3º da Lei nº 13.874/2019 (Lei da Liberdade Econômica), os documentos digitalizados passam a produzir os mesmos efeitos legais dos documentos físicos ou originais.

De acordo com Gonzales (2020), diante do momento atual de crise na saúde, se tornou ainda mais necessária a utilização dos meios de assinatura e autenticação digitais em pagamentos, acordos, contratos e documentos. É importante observar que as relações se materializam no ambiente digital, desde as leis mais antigas até no cenário atual.

Segundo Creci-RJ. (2020), quando esse momento de pandemia passar, esses métodos tecnológicos permanecerão ativo, pois mesmo antes dessa crise na saúde mundial, a assinatura digital vinha sendo adotada por várias empresas. Dessa forma o cliente quando se desloca bastante, perde tempo, gera gastos. Através da assinatura digital, ele encaminha os documentos, transmite as informações a distância, reduzindo custos com o processo de deslocamento.

5 CONSIDERAÇÕES FINAIS

No atual cenário da crise de saúde mundial, a tecnologia vem trazendo um grande diferencial para as organizações, visando agilidade, segurança, inovação nos processos administrativos.

Através do isolamento social, é possível garantir a saúde dos colaboradores, realizando suas atividades, utilizando meios tecnológicos e um deles é a assinatura digital, facilitando as aprovações de contratos e de documentos em geral que necessitam da autenticação.

Com a certificação digital é possível garantir a segurança, a não violação de dados e informações dos documentos. Somente as pessoas responsáveis pelas assinaturas, aprovações que podem ter acesso e assinar os arquivos.

A assinatura digital é um método capaz de substituir as assinaturas a próprio punho, proporcionando benefícios, sociais, econômicos e ambientais.

REFERÊNCIAS

AARÃO, Maria Tereza. **Como a assinatura digital está transformando as empresas**. Disponível em: 23 de março de 2017. https://administradores.com.br/noticias/como-a-assinatura-digital-esta-transformando-as-empresas. Acesso em 23 de outubro de 2020.

BARRETO, Ana Carolina Horta. **Assinaturas eletrônicas e certificação**. In: ROCHA FILHO, Valdir de Oliveira; BARRETO, Ana Carolina Horta et al. O Direito e a internet. Rio de Janeiro: Forense Universitária, 2002, p. 1-65.

BRASIL, Ângela Bittencourt. (2000) **Assinatura digital não é assinatura formal.** http://www.jus.com.br/doutrina/assidig2.html

[Braga and Dahab 2015b] Braga, A. and Dahab, R. (2015b). **Introdução à Criptografia para Programadores: Evitando Maus Usos da Criptografia em Sistemas de Software**. In Caderno de minicursos do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2015, pages 1–50. Sociedade Brasileira de Computação.

CERT..BR. **Criptografia.** Disponível em: 16 de março de 2017. https://cartilha.cert.br/criptografia/. Acesso em: 12 de outubro de 2020.

CRYPTO ID, Últimas Notícias. **Assinatura Digital é sinônimo de economia sustentável.** Disponível em: 26 de março de 2020. https://cryptoid.com.br/identidade-digital-destaques/assinatura-digital-e-sinonimo-de-economia-sustentavel/. Acesso em: 16 de outubro de 2020.

CUSTÓDIO, F. Ricardo., DIAS, Júlio S., ROLT, Carlos R. de. **Revista: BRy Tecnologia S.A,** Laboratório de Tecnologia de Gestão – Labges – UDESC, [s.d.].

DA SILVA, L. S. **Public key infrastructure pki: conheça a infra-estrutura de chaves públicas e a certificação digital.** São Paulo: Novatec, 2004.

DIGIX. **Gestão de processos digitais: como implementar a assinatura digital no governo.** Disponível em: 02 de abril de 2019. https://www.digix.com.br/gestao-de-processos-digitais-como-implementar-a-assinatura-digital-no-governo/. Acesso em: 10 de outubro de 2020.

FERRARI, AMARAL, Carlos, Felipe. **Artigo – Estadão – Assinatura digital diante da pandemia.** Disponível em:09 de abril de 2020. https://www.anoreg.org.br/site/2020/04/09/artigo-estadao-assinatura-digital-diante-da-pandemia-por-carlos-ferrari-e-felipe-amaral/. Acesso em 21 de abril de 2020.

FERREIRA, Fernando Nicolau Freitas. ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação** : Guia prático para elaboração e implementação / Fernando Nicolau Freitas Ferreira, Márcio Tadeu de Araújo. - Rio de Janeiro : Editora Ciência Moderna, 2008.

FOLHACERTA. **Assinatura digital: o que é e como adotar na sua empresa?** Disponível em: 31 de outubro de 2018. https://folhacerta.com/assinatura-digital-o-que-e-e-como-adotar-na-sua-empresa/. Acesso em: 20 de outubro de 2020.

GANDINI; JACOB; SALOMÃO**. A segurança dos documentos digitais**. Disponível em: 25 out. 2006. INBIO. In: INTELIGÊNCIA INFORMÁTICA. Acesso em: 01 de jun. 2020.

INFOCO, Certificação Digital. Certificado digital para profissionais da saúde: entenda a importância e os benefícios. Disponível em 8 de agosto de 2019. https://www.infocodigital.com.br/certificado-digital-para-profissionais-da-saude-entenda-a-importancia-e-os-beneficios/. Acesso em: 20 de outubro de 2020.

INFOPATH. **Introdução às assinaturas digitais.** Disponível em: 2013. https://support.microsoft.com/pt-br/office/introdu%C3%A7%C3%A3o-%C3%A0s-assinaturas-digitais-d2f92222-abb1-486b-bc07-884ecac99c59. Acesso em: 10 de outubro de 2020.

LACORTE, Christiano Vitor de Campos - **A validade jurídica do documento digital**, 2005. 30 f. Artigo (Curso de Ciência Jurídica) – Instituto de Educação Superior de Brasília, Brasília. 2005.

LOZUPONE, V. Analyze encryption and public key infrastructure (PKI). **International Journal of Information Management,** v. 38, n. 1, p. 42–44, 2018. Elsevier. Disponível em: 2018

MACÊDO, Diego. **Assinatura e Certificação Digital**. Disponível em: 03 de março de 2012. https://www.diegomacedo.com.br/assinatura-e-certificacao-digital/. Acesso em: 15 de outubro de 2020.

MARCACINI, Augusto Tavares Rosa. **Direito e informática:** Uma abordagem jurídica sobre criptografia. Rio de Janeiro: Forense, 2002.

MENKE, Fabiano. **Assinatura eletrônica: aspectos jurídicos no direito brasileiro**. São Paulo: Revista dos Tribunais, 2005.

MONTEIRO, Emiliano S., MIGNONI, Maria Eloisa. **Certificados Digitais** : Conceitos e Práticas / Emiliano S. Monteiro, Maria Eloisa Mignoni. – Rio de Janeiro : Brasport, 2007.

PPLWARE. **Criptografia simétrica e assimétrica. Sabe a diferença?** Disponível em: 07 de dezembro de 2010. https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/. Acesso em 26 de outubro de 2020.
ROHRMANN, Carlos Alberto. Curso de direito virtual. Belo Horizonte: Del Rey, 2005.

ROOT, Terminal. **O que é e como gerar uma HASH?.** Disponível em: 27 de maio de 2019. https://terminalroot.com.br/2019/05/o-que-e-e-como-gerar-uma-hash.html. Acesso em: 16 de outubro de 2020.

STALLINGS, W. **Criptografia e Segurança de Redes. Princípios e Práticas.** 4 ed. São Paulo: Prentice Hall, 2008

SILVEIRA, Lais. **Artigo: Assinatura digital em tempos de pandemia.** Disponível em: 14 de agosto de 2020. https://jornaldecampinas.com.br/artigo-assinatura-digital-em-tempos-de-pandemia/. Acesso em: 20 de outubro de 2020.

ZOCOLLI, Dinemar. **Autenticidade e integridade dos documentos eletrônicos: a firma eletrônica**. In: Aires José Rover (Coord.). Direito, Sociedade e Informática. Florianópolis: Fundação Boiteux, 2000. 130 – 216 p.