INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

JOÃO VICTOR NOGUEIRA RODRIGUES
FRANCISLÚCIO SENA PORTELA

SISTEMA DE CERTIFICAÇÃO DIGITAL NAS RELAÇÕES JURÍDICAS

TRABALHO DE CONCLUSÃO DE CURSO

SÃO LUÍS - MA
2019

JOÃO VICTOR NOGUEIRA RODRIGUES
FRANCISLÚCIO SENA PORTELA

SISTEMA DE CERTIFICAÇÃO DIGITAL NAS RELAÇÕES JURÍDICAS

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Carlos Rayllan Lima Sousa

SÃO LUÍS – MA
2019

JOÃO VICTOR NOGUEIRA RODRIGUES
FRANCISLÚCIO SENA PORTELA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: / /

BANCA EXAMINADORA

_____

Prof. Esp. Carlos Rayllan Lima Sousa (Orientador)

_____

_____

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Esp. Carlos Rayllan Lima Sousa, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala.

À Secretaria do Curso, pela cooperação.

Gostaria de deixar registrado também, o meu reconhecimento em especial à minha família, e meus amigos, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

RESUMO

NOGUEIRA RODRIGUES, João Victor; SENA PORTELA, Francislúcio. Título do trabalho: Sistema de certificação digital nas relações jurídicas. 2019. 28 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Com o advento da internet ficou fácil compartilhar e acessar informações. Mediante isso as empresas e órgãos públicos começaram a utilizar serviços automatizados que antes eram realizados de forma manual e com pouca eficiência. Então como garantir que práticas do dia a dia das entidades jurídicas como Confidencialidade, integridade e segurança das informações estarão presentes e garantir que somente as partes autorizadas possuam acesso.

A certificação digital vem prover essas garantias dos processos analógicos para o meio digital com maior eficiência e disponibilidade para todas as partes.

Serão apresentados aqui, conceitos fundamentais e suas aplicabilidades, a fim de gerar entendimento sobre o funcionamento e garantias da Certificação Digital nos órgãos públicos e privados praticados nas relações jurídicas.

Palavras-chave: Certificado Digital. Jurídico. Criptografia. Chave Privada. Chave Pública. Segurança.

ABSTRACT

NOGUEIRA RODRIGUES, João Victor; SENA PORTELA, Francislúcio. Title of the working: Digital certification system in legal relations. 2019. 28 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

With the advent of the internet, it was easy to share and access information. Through this, companies and public agencies began to use automated services that were previously performed manually and with little efficiency. So how to ensure that day-to-day practices of legal entities such as Confidentiality, integrity and security of information will be present and ensure that only authorized parties have access.

Digital certification provides these guarantees from analogue to digital media processes with greater efficiency and availability to all parties.

Here, fundamental concepts and their applicability will be presented, in order to generate understanding about the functioning and guarantees of Digital Certification in public and private bodies practiced in legal relationships.

Keywords: Digital Certificate. Legal. Encryption. Private Key. Public Key. Safety.

SUMÁRIO

1. INTRODUÇÃO

Desde a antiguidade as pessoas utilizam assinaturas à caneta, carimbos, selos e outros recursos para comprovar a autenticidade de documentos, expressar concordância com determinados procedimentos, declarar responsabilidade, dar certificação a alguma coisa, reconhecimento ou a demarcação, através de sinais de uma propriedade. Atualmente muitos desses procedimentos são feitos através internet. Mas, como garantir a autenticidade no mundo eletrônico?

O uso maciço da Internet trouxe muitas e (cada vez mais) vulnerabilidades para a grande rede. Os problemas de segurança vêm sendo amplamente discutidos e recebendo tratamento especial, tais como: os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam vir a comprometer a integridade da informação.

Com isso, novas rotinas foram criadas, para a utilização de tais arquivos e garantir a autenticidade, expressar concordância ou declarar responsabilidade no mundo digital: a certificação digital. O que garante mais agilidade, eficiência e segurança na realização do trabalho nas empresas.

Pretende-se mostrar aos usuários as vantagens de um certificado digital, através dos seus resultados obtidos, que apesar de necessitar de certos investimentos, sua implantação traz benefícios que superam em larga escala seus custos e dificuldades. Assim, evitar a espionagem industrial nas empresas, fraudes, erros, crackers, invasões, vírus, e outras ameaças que diariamente tentam passar pelas brechas de segurança.

A metodologia científica utilizada é a Pesquisa Bibliográfica que traça um histórico sobre o objeto de estudo feito a partir da análise de fontes secundárias que abordam, de diferentes maneiras, o tema proposto. Como também a Pesquisa Descritiva, por proporcionar novas visões sobre uma realidade já conhecida do mundo digital, em forma de levantamentos de dados que permite estabelecer relações de dependência entre variáveis, sendo possível generalizar os resultados.

Assim, o presente estudo acredita ser uma realidade preocupante com a segurança digital e, contudo pretende-se esclarecer e incentivar a prática dos certificados, tendo em vista a necessidade cada vez mais latente de se obter segurança, rapidez e praticidade ao realizar qualquer atividade on-line, principalmente nas organizações públicas e transações jurídicas.

2. JUSTIFICATIVA

A rapidez com que as mudanças ocorrem no mundo atual, provavelmente a informática é um dos setores que muitas pessoas não conseguem acompanhá-la. Com os riscos de segurança que a internet proporciona como, fraudes, erros, crackers, invasões, vírus, e outras ameaças, todo processo inovador traz consigo incerteza na confiabilidade. Naturalmente, o surgimento de algo novo tira o indivíduo de sua zona de conforto.

Há séculos, acostumados com o uso documental em formato palpável, a difícil aceitação por parte da sociedade do documento digital é comum. Da mesma forma que a Assinatura Digital ainda é de difícil compreensão por boa parte das pessoas, cabe aos envolvidos na área contribuir para sua divulgação e aceitação.

O esclarecimento do tema proposto e prova de sua confiabilidade tem papel fundamental para sua aceitação, bem como esclarecer as suas vantagens de segurança que superam seus investimentos. O uso da certificação digital garante a autenticidade, eficiência, agilidade e integridade das informações, principalmente nas transações jurídicas.

3. OBJETIVOS

3.1. Objetivo Geral

O presente trabalho tem como objetivo geral apresentar de que forma o uso dos certificados digitais podem intervir nos problemas de segurança causados pelos usuários fraudulentos da internet. Incentivar o uso da certificação tendo como benefício à legitimidade e segurança das informações nos documentos digitais e transações online, principalmente nos órgãos públicos e privados nas relações jurídicas.

3.2. Objetivos Específicos

- Apresentar referencial teórico e bibliográfico para interpretação das características da internet e os possíveis problemas de segurança.
- Avaliar os aspectos legais que validam documentos e assinaturas digitais e criam cadeia de confiabilidade da Infra-estrutura da ICP-Brasil.
- Discutir as vantagens e desvantagens do uso da certificação digital.
- Analisar os erros de compatibilidade e instalação dos certificados e soluções possíveis.
- Apresentar medidas de segurança a serem adotadas a fim de preservar a integridade e legitimidade das informações em uma transação online.

4. ESTRUTURA DO TEXTO

As declarações citadas nessa pesquisa foi retirada dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil, que presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916, atualmente art. 219 da Lei nº 10.406 de 10 de janeiro de 2002 - Código Civil em vigor- (parágrafo 1º do artigo 10 da Medida Provisória 2.200-02/2001).

5. FUNDAMENTAÇÃO TEÓRICA

O impacto revolucionário da informação provoca transformação na economia, na sociedade, nos mercados de trabalho e igualmente nas relações de consumo. Segundo Bill Gates, as companhias de sucesso no futuro serão as que utilizarem ferramentas digitais para reinventar sua maneira de trabalhar. Se a empresa converter cada documento de papel em um arquivo digital, ela se tornará mais competitiva. Para ele:

> O papel estará conosco infinitamente, mas sua importância como meio de encontrar, preservar e distribuir informação já está diminuindo. (...) À medida que os documentos ficarem mais flexíveis, mais riscos de conteúdo de multimídia e menos presos ao papel, as formas de colaboração e comunicação entre as pessoas se tornarão mais ricas e menos amarradas ao local onde estão instaladas. (GATES, Bill. A estrada do futuro. São Paulo: Companhia das Letras, 1995).

Com o advento da Internet surge o Comércio Eletrônico, pessoas físicas e jurídicas, governos e outras entidades realizam procedimentos e transações, fecham negócios, emitem ou recebem documentos, acessam informações sigilosas, de maneira rápida e precisa, economizando tempo e dinheiro, evitando processos burocráticos. Os documentos tradicionais em papeis não correspondem às necessidades de rapidez na circulação das informações.

Contudo, da mesma forma que a internet oferece meios para tudo isso, também pode ser alvo de usuários fraudadores. Para preservar a integridade das informações de uma transação online, foi criada a certificação digital. É um tipo de tecnologia de identificação que permite segurança nas transações eletrônicas, preservando sua integridade, autenticidade, evitando adulterações, interceptações ou qualquer tipo de fraude. A certificação digital funciona com base em um documento eletrônico chamado certificado digital e um recurso denominado assinatura digital.

> Segundo definição do Professor Luiz Gustavo Cordeiro da Silva, Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. Permite que informações transitem pela Internet com maior segurança. É baseada na existência de Certificados Digitais emitidos por uma Autoridade Certificadora(AC), considerada confiável pelas partes envolvidas. (Silva, AT EL., 2008 p.X) Garantindo o conteúdo de mensagens ou textos, sua autoria e data em que foi assinada. Baseia-se no princípio da terceira parte confiável, que oferece confiabilidade entre partes que se utilizem de Certificados Digitais. Para isso utiliza-se de uma Infra-estrutura de chaves públicas, cuja principal função é definir técnicas e procedimentos. A Medida Provisória 2.200-2, de agosto de 2001 estabelece a Infra-estrutura de Chaves públicas Brasileira – ICP-Brasil. (Silva, AT EL., 2008 p.XII).

5.1. Certificado Digital

O certificado digital contém um nome e um número público exclusivo, chamado de chave pública, o que visa garantir a identificação segura do trânsito de uma mensagem ou negócio eletrônico, além de permitir assinar, digitalmente, as mensagens e transações on-line com confidência, integridade e validade jurídica.

Surgiu no Brasil em 2001, foi criado pela medida provisória 2.200-2, quando o governo federal identificou necessidade em agilizar e informatizar seus processos. Ao longo do tempo muitos setores aderiram esse mecanismo para realizar serviços de forma segura. Em 2006, a Receita Federal passou a exigir o envio de declarações por meio eletrônico das empresas que optam pela tributação, lucro real e arbitrado.

Em 2010, as empresas que declaram com opção pelo lucro presumido se enquadram nessa necessidade. No mês de janeiro de 2011 contabilizava-se cerca de 1,3 milhões de empresas enquadradas nesse regime que terão, obrigatoriamente, o uso da certificação digital. O Instituto Nacional de Tecnologia da Informação – ITI publicou cerca 1,25 milhões de certificados emitidos em 2010.

O certificado digital pode ser requisitado por pessoas físicas, empresas e instituições públicas ou privadas.

Em resumo, o certificado digital é um documento eletrônico assinado digitalmente por uma autoridade certificadora, o qual contém diversos dados sobre o emissor e o seu titular. Sua função é de vincular uma pessoa ou uma entidade a uma chave pública.

5.2. Assinatura Digital

Suponha-se a seguinte situação: Pedro está em uma viagem de negócios e precisa enviar um documento importante à sua empresa. Caso opte por enviar esse documento em papel, certamente os assinaria a caneta para comprovar a autenticidade das informações e sua responsabilidade sobre ele.

Poderia utilizar um serviço de entrega de sua confiança, no entanto, pode demorar dias seu recebimento. Outra opção seria enviar por e-mail e escannear o documento com sua assinatura, mas, qualquer pessoa pode altera-la em programas de edição de imagens. Enviar documentos via e-mail sem qualquer proteção tem seus riscos, já que alguém pode intercepta-los.

Nesse caso, o recomendado e seguro é utilizar a assinatura digital. A assinatura digital é um mecanismo eletrônico que faz uso de criptografia ou *chaves criptográficas*.

Atributos da assinatura digital:

- Ser única para cada documento, independente se é o mesmo signatário;
- Comprovar a autoria do documento eletrônico;
- Possibilitar a verificação da integridade do documento, sempre que houver qualquer alteração, o destinatário terá como percebê-la;
- Assegurar ao destinatário o "não repúdio" do documento eletrônico, pois, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.

Assim, assinatura digital garante ao destinatário que o documento não seja alterado ao ser enviado, dando-lhe integridade, comprova a autoria do emitente comprovando sua autenticidade.

6. DIFERENÇA ENTRE UMA ASSINATURA E CERTIFICADO DIGITAL

A assinatura digital é um mecanismo que usa a criptografia e relaciona o certificado digital ao documento que irá ser assinado, garantindo a integridade e autenticidade do mesmo. Já o certificado digital é uma chave, como se fosse uma caneta do usuário da empresa.

6.1. O ciclo de vida de um certificado e onde adquirir

Ao solicitar um certificado, sua validação dar-se-á após a comprovação do pagamento da sua respectiva taxa. Sua emissão terá um período de validade, posteriormente de uma renovação ou uma revogação.

A emissão de um certificado digital é através de uma Autoridade de Certificação (AC) e é assinada com a Chave Privada desta AC. Uma Identificação Digital normalmente contém: a Chave Pública do proprietário; o nome do proprietário; a data de vencimento da Chave Pública; o nome do emissor (a AC que emitiu a Identificação Digital); o número de série da Identificação Digital; a assinatura digital do emissor.

O Instituto Nacional de Tecnologia da Informação (ITI), a autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora

Raiz da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), é o órgão que credencia empresas a fornecer certificados padrão ICP-Brasil.

7. TIPOS DE CERTIFICADO DIGITAL

A escolha do Certificado Digital pelo usuário depende do sistema/aplicação onde ele será utilizado.

Tipo A1: emitido diretamente no computador e fica armazenado no navegador da internet.

Tipo A3: é emitido e armazenado em uma mídia criptográfica, cartão inteligente ou token.

mobileID: é emitido e armazenado em dispositivo móvel, celular ou tablete, concedendo ao titular mais mobilidade.

7.1. Hardware

Smart Cards e tokens são dispositivos portáteis que funcionam como mídias de armazenamento. Nos chips estão contidas as chaves privadas do usuário, ou seja, os certificados digitais. O acesso às informações é feito através da autenticação de uma senha pessoal do titular. O smart card é semelhante à um cartão magnético, sendo necessário ser acompanhado de um aparelho leitor usb para o funcionamento do mesmo. Já o token é semelhante à uma pequena chave ou um pen drive que é inserido na porta usb do computador.

7.2. Pessoas Físicas e Jurídicas

- Certificado Digital e-CPF

  No meio eletrônico, o e-CPF é a Identidade Digital da Pessoa Física a ser utilizado na assinatura de documentos com validade jurídica, fazer comunicação com a Receita Federal do Brasil (RFB) e dar andamento aos serviços oferecidos pelos governos estadual e federal, ter acesso ao eSocial e Conectividade Social, enviar a Declaração do Imposto de Renda com muito mais facilidade, entre outras aplicações. Ele permite que diversos serviços sejam realizados sem a necessidade da presença física, agilizando nos processos sustentabilidade e redução de custos.

- Certificado Digital e-CNPJ

  O e-CNPJ é a identidade digital da pessoa jurídica no meio eletrônico, realiza a autenticação em sistemas públicos ou privados em nome da empresa. Garantindo a confiabilidade, integridade das informações e não repúdio nas operações que são realizadas por meio da certificação dando-lhe validação jurídica.

- Certificado Digital NF-e/NFC-e

  O Certificado Digital NF-e destina-se à emissão de notas fiscais eletrônicas podendo ser atribuído ao funcionário. Com mais segurança e controle no processo, onde o empresário pode nomear o responsável por emitir notas fiscais, sem ter que compartilhar o e-CNPJ da empresa e senha.

- Certificado Digital OAB

  O Certificado Digital OAB é exclusivo para os advogados regularmente inscritos na Ordem dos Advogados do Brasil (OAB). Viabiliza o peticionamento eletrônico, a assinatura digital de documentos com validade jurídica, entre outras aplicações.

- Certificado Digital para celular: mobileID

  O Certificado Digital mobileID pode ser emitido e armazenado em dispositivos móveis, smartphone e tablets. Ser usado para a autenticação e assinatura de documentos e é compatível com as plataformas Android e iOS.

- Certificado Digital na nuvem: remoteID

  O remoteID é um Certificado Digital que mesmo armazenado na nuvem e é tão seguro quanto os demais certificados, com a diferença que ele tem dupla autenticação. Não necessita do uso de mídias criptográficas e é gerenciável, permitindo, entre outros diferenciais, sua utilização em múltiplos computadores. Basta ter conexão com a internet para acessa-lo a qualquer hora ou em qualquer lugar, podendo ser usado nos principais navegadores e sistemas operacionais, inclusive no MAC OS.

7.3. Desvantagens da Certificação Digital

As desvantagens são:

Prendem-se principalmente com as limitações dos sistemas informáticos.

Com o desenvolvimento do processamento dos computadores aumenta a possibilidade de falsificação de assinaturas mais antigas, razão pela qual tem um prazo de validade.

Possibilidade de roubo do código ou password que assina o documento.

7.4. Validade jurídica do documento digital

As empresas têm investido na Certificação Digital a fim de garantir autenticidade, confidencialidade e integridade às informações dos documentos na *web*. Um documento, seja eletrônico ou não, precisa apresentar condições para ter validade jurídica.

> Para a prevenção deste tipo de situação, surgiu a certificação digital. Seu funcionamento pode ser comparado a de um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma autoridade certificadora [responsável pela emissão do certificado digital] que possui registrado, em sua base de informações, a chave pública [usada para decifrar a mensagem – criptoanálise] do emissor do documento. Através de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico. (VOLPI; MARLON, p, 36).

No documento eletrônico, o que valida sua capacidade probatória é a assinatura digital, assegurando-lhe autenticidade e integridade.

> Assinatura digital é um método que garante que determinada mensagem não seja alterada durante seu trajeto. Esse processo envolve criar a mensagem, cifrá-la [criptografia, utilizando a chave privada do emissor para cifrar a mensagem] e enviá-la conjuntamente tanto da mensagem original como da cifrada. Uma vez recebidas, o destinatário compara o conteúdo da mensagem original com o da cifrada, para se certificar de que não houve alteração. (Volpi, Marlon Marcelo. Assinatura Digital. Aspectos Técnicos, Práticos e Legais. Axcel Books. 2001. Pág.4).

As consequências jurídicas propriamente ditas referente à certificação eletrônica, a responsabilidade maior deve ser da certificadora. Uma eventualidade de descredenciamento da certificadora, caso esta descumpra as normas a ela atribuídas, traria grande insegurança jurídica, além do que todos os documentos assinados digitalmente estariam sob suspeita.

Até mesmo o ITI (Instituto Nacional de Tecnologia da Informação, que é uma autarquia federal vinculada à Casa Civil da Presidência da República) sendo um órgão superior, em razão de ter suas atividades aprovadas pelo Comitê Gestor, também está sujeito à fiscalização e a descredenciamento.

As fraudes podem ocorrer tanto no mundo físico quanto no mundo digital. A falsificação de uma certidão digital tem as mesmas consequências jurídicas que a falsificação de uma certidão de papel (física).

8. INFRAESTRUTURA DA ICP-BRASIL

Segundo o Instituto Nacional de Tecnologia da Informação, a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

O modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. Compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

Uma Autoridade Certificadora – AC é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

A Autoridade Certificadora também emite Listas de Certificados Revogados – LCR e mantém os registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação – DPC. Além de estabelecer e fazer cumprir, pelas Autoridades de Registro – ARs a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

9. COMO ADQUIRIR UM CERTIFICADO DIGITAL

1. Escolha uma das Autoridades Certificadoras – ACs da ICP-Brasil;

2. Solicite no site da AC escolhida a emissão do seu certificado digital de pessoa física ou jurídica. Os tipos mais comercializados são:
A1: validade de um ano – armazenado no computador;
A3: validade de até cinco anos – armazenado em cartão ou token criptográfico. A própria AC informará sobre os custos do certificado, as formas de pagamento, os equipamentos necessários e a documentação obrigatória para emissão.

3. É necessário agendar o dia e horário de comparecimento na Autoridade de Registro – AR: para a emissão do certificado digital é necessário que o solicitante vá pessoalmente a uma Autoridade de Registro – AR da Autoridade Certificadora escolhida para validar os dados preenchidos na solicitação. Além de levar os documentos obrigatórios, o solicitante passará pelo processo de cadastramento biométrico, com a coleta da biografia facial (foto) e das digitais. Esse processo é chamado de validação presencial e será agendado diretamente com a AR que instruirá o solicitante sobre todo o processo.

4. Após a verificação de todos os documentos e confirmação da identidade do solicitante na AR, o certificado já estará pronto. No caso do certificado tipo A1: A AC notificará o cliente sobre os procedimentos para baixar o certificado;
No caso do certificado tipo A3: o certificado é entregue em cartão ou token na própria AR. Em caso de dúvida ou dificuldade após a aquisição do certificado, entre em contato com sua Autoridade Certificadora – AC. Ela deve prestar todo suporte técnico para o correto uso e instalação do certificado digital.

10. PROCESSO JUDICIÁRIO ELETRÔNICO (PJE)

O PJE é uma ferramenta de tramitação de processos, criado e desenvolvido pelo CNJ (Conselho Nacional de Justiça), em conjunto com a OAB (Ordem dos Advogados do Brasil).

O Sistema Judiciário implementou o uso do PJE à partir de 2009, tendo como objetivo simplificar o trâmite dos processos, e reduzir custos. Além disso, com a ferramenta, os advogados têm mais autonomia e o sistema judiciário se livra de adquirir licenças ou instalar softwares pra acompanhar o processo.

> O processo eletrônico visa à eliminação do papel na tramitação das mais diversas ações, afastando a tradicional realização dos atos mecânicos, repetitivos, como o ato de protocolar uma inicial, a autuação do processo, a numeração de folhas. Acaba a tramitação física dos autos a distribuição para a secretaria (ou cartório), desta para o gabinete do promotor ou do magistrado, e a necessidade de cargas dos autos. Facilita a comunicação dos atos processuais com a intimação de advogados e de partes, realizada diretamente no sistema Agiliza a confecção de mandados, ofícios, publicações, expedição de precatórias cartas de ordem e outros.Marcelo Mesquita Silva (SILVA,2012,p13)

10.1. Vantagens e Desvantagens do PJE

10.2. Vantagens

- Diminui o uso de papel desnecessário.
- Diminuição de burocracia.
- Diminui o risco de roubo de documentos.
- Agiliza na tramitação de processos de segunda instância.
- Redução de custos;
- Redução de trâmite de processos, agilizando as causas.

> “Com a informatização, pela experiência vivenciada em pesquisas realizadas desde o ano de 2002, ao invés de perdermos o humano, ampliamos o processamento dos feitos”. Alexandre Atheniense.

10.3. Desvantagens

- Falhas no sistema impedem o trâmite dos processos.
- Vulnerabilidade à ações de hackers, crackers e outros criminosos virtuais.
- Danos à saúde.
- Necessidade de backup para evitar perda de dados.

- O pje não suporta arquivos doc com grandes volumes.
- Ilegibilidade de documentos.

11. CONCEITOS DE SEGURANÇA DE COMPUTADORES

A área de segurança de rede e de Internet consiste de medidas para detectar, prevenir, corrigir e impedir violações de segurança envolvidas na transmissão das informações.

Pode se definir a segurança de computadores como a proteção oferecida para um sistema de informação automatizado a fim de preservar a integridade, disponibilidade e confidencialidade das informações do mesmo (incluindo hardware, software, firmware, informações/dados e telecomunicações).

Esse conceito é a **tríade CIA** (do acrônimo em inglês para *confidentiality, integrity and availability*) é conhecido como o coração da segurança por envolver os objetivos fundamentais da segurança de computadores, tanto para dados quanto para serviços de informação e computação.

- **Confidencialidade**: Impõe restrições sobre o acesso e divulgação da informação para proteger a privacidade de indivíduos e informações privadas. Uma a divulgação não autorizada de informação é uma falha de confidencialidade.

- **Integridade**: Impõe restrições sobre a modificação ou destruição da informação, incluindo também a garantia de irretratabilidade e autenticidade dela. A modificação ou destruição não autorizada da informação é uma falha de integridade.

- **Disponibilidade**: A infraestrutura do serviço deve assegurar confiabilidade e rapidez no acesso a informação. A perda do acesso ou redução da capacidade de uso do serviço é uma falha de disponibilidade.

Embora a **tríade CIA** tenha um conceito bem forte e estruturado para prover a segurança de serviços de computação e dados, alguns conceitos logo após foram

introduzidos no campo da segurança a fim de apresentar um quadro mais completo. Vejamos dois desses conceitos que são mais mencionados:

- **Autenticidade**: a propriedade de se provar ser genuíno e capaz de ser verificado e tornar-se confiável. Isso significa verificar que os usuários são quem dizem ser e que, além disso, cada entrada no sistema vem de uma fonte confiável.

- **Responsabilização**: a propriedade de segurança que gera o requisito para que ações de uma entidade sejam atribuídas exclusivamente a ela. Isso provê irretratabilidade, detecção e prevenção de intrusão, além de recuperação pós-ação e ações legais. Afinal como sistemas não são totalmente seguros, temos que ser capazes de associar uma violação de segurança a uma parte responsável. Assim os sistemas precisam manter logs de suas atividades a fim de permitir análises posteriores.

12. ARQUITETURA DE SEGURANÇA

É preciso antes de tudo avaliar a necessidade de segurança que o ambiente da organização necessita, para assim escolher entre os diversos produtos e politicas de segurança disponíveis. Em si isso já é bem difícil em redes locais e fica bem mais complicado quando o cenário muda quando sistemas precisam ser distribuídos para prover serviços a clientes que utilizam acesso remoto.

X.800 da ITU-T, especificamente o Telecommunication Standardization Sector (ITU-T), é uma agência patrocinada pelas Nações Unidas que desenvolve padrões, chamados de Recomendações, que foca em *oferecer conceitos* de ataques, mecanismos e serviços de segurança relacionados a telecomunicações e a Open Systems Interconnection (OSI). Eles podem ser definidos da seguinte forma:

- **Ataque à segurança**: qualquer ação que comprometa a segurança da informação pertencida a uma organização.

- **Mecanismo de segurança**: um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou recuperar-se de um ataque à segurança.

- **Serviço de segurança**: um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e das transferências de informação de uma organização. Os serviços servem para frustrar ataques à segurança, e utilizam um ou mais mecanismos para isso.

Normalmente usamos os termos ameaça e ataque para a mesma coisa. Porem as definições retiradas da **RFC 4949** - Internet Security Glossary, defini da seguinte forma:

Ameaça: uma chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade.

Ataque: um ataque à segurança do sistema, derivado de uma ameaça inteligente; ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de fugir dos serviços de segurança e violar a política de segurança de um sistema.

Uma maneira útil de classificar os ataques à segurança, usada tanto na X.800 quanto na RFC 4949, é em termos de ataques passivos e ataques ativos. Um ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta os seus recursos. Um ataque ativo tenta alterar recursos do sistema ou afetar sua operação.

13. ATAQUES À SEGURANÇA

13.1. Ataques Passivos

Esse tipo de ataque tem por natureza o ato de monitorar e bisbilhotar as informações, que estão sendo transmitidas. São exemplos de ataques passivos o vazamento de conteúdo de mensagens e a analise de trafego.

- **Vazamento de conteúdo de mensagens:** como uma conversa telefônica, mensagem de e-mail ou um arquivo transferido, podem conter informações confidenciais de um processo jurídico sensível às partes, e que não poderiam ter se tornado de conhecimento público.

- **Analise de trafego:** é outro tipo, porem mais sútil. Ataques passivos são muito difíceis de detectar, pois as informações não sofrem qualquer alteração nos dados. O trafego envolve apenas o envio e recebimento em um padrão aparentemente normal entre emissor e receptor, sendo que eles não estão cientes de um terceiro lendo suas mensagens. Sendo assim a forma de se defender desse tipo de ataque está na prevenção e não na detecção, e a técnica mais comum de mascarar ou camuflar o conteúdo dessas mensagens é por meio da encriptação.

13.2. Ataques Ativos

Envolvem algum tipo de alteração no fluxo dados ou criando um novo fluxo de dados falso, e se subdividem em quatro categorias especificas, sendo elas:

- **Disfarce**: Uma entidade finge ser outra e geralmente complementa o nível de ataque em junção de alguma outra forma de ataque ativo. Por exemplo, após capturar alguma sequencia de autenticação de uma entidade ele as reproduz e quando houver uma delas, válida, permitindo assim que essa entidade agora autorizada antes com poucos privilégios agora obtenha alguns extras, personificando outra entidade que os possua. Podemos citar o caso de um usuário de sistema que através desse processo conseguiu elevar seus níveis de permissões para administrador.

- **Repasse**: É uma captura passiva de unidade de dados, que subsequentemente é retransmitido para produzir um efeito não autorizado. Exemplo: Uma entidade do ataque está recebendo e repassando as informações do emissor para produzir um efeito de não autorização.

- **Modificação de mensagens**: Significa que a entidade responsável pelo ataque esta alterando alguma parte legítima da mensagem, ou que as mensagens são adiadas ou reordenadas, para produzir um efeito de não autorização.
  Exemplo: Uma mensagem com a premissa (Permitir que Waine leia o arquivo confidencial contas) é modificada para (Permitir que Alfred leia o arquivo confidencial contas).

- **Negação de serviço**: Impede ou inibe o uso ou gerenciamento normal do meio de comunicação. Esse ataque pode ter um único alvo; como uma entidade que envie mensagens para determinado destino (por exemplo, um advogado querendo homologar um processo no serviço de auditoria). Como também pode ter como alvo a negação do serviço para todas as entidades, seja desativando o serviço ou sobrecarregando-o com mensagens para prejudicar seu desempenho.
  Exemplo: Um ataque DDNs, onde o servidor recebe uma grande massa de mensagens o que acaba sobrecarregando seu desempenho, causando lentidão e interrupção do serviço.

14. SERVIÇOS DE SEGURANÇA

Os serviços de segurança devem ser fornecidos como uma camada de protocolo de comunicação em sistemas abertos, que visa garantir a segurança dos sistemas, e das transferências de dados.

Segundo a RFC494, um serviço de processamento ou comunicação que é fornecido por um sistema para fornecer algum tipo de proteção especifica aos recursos do sistema. Assim os serviços de segurança propriamente ditos

implementam políticas (regras ou diretrizes) de segurança que são implementados pelos mecanismos de segurança.

A X.800 classifica esses serviço em cinco categorias e quatorze serviços específicos(autenticação, controle de acesso, confidencialidade, integridade e irretratabilidade).

- **Autenticação:** Significa provar a identidade de alguém. A função do serviço de autenticação é garantir ao destinatário que a mensagem tem a origem de que ela afirma ter vindo. Para estabelecer a conexão, o serviço antes precisa garantir a autenticidade das duas entidades, que cada uma é quem afirma ser. Depois, o serviço precisa garantir que a conexão não sofra interferência de modo que um terceiro possa fingir ser uma das duas entidades, e assim evitar transmissão ou recepção não autorizada. Dentro da Autenticação existe ainda:

- **Controle de Acesso:** Sua função é limitar e controlar o acesso a sistemas e aplicações, a entidade que solicitar acesso antes precisa ser identificada (autenticada) só assim seus direitos de acessos são ajustados.

- **Confidencialidade de dados**: Conhecido também como “privacidade”, protege os dados contra divulgações não autorizadas. Essa proteção esta presente sobre toda a mensagem ou campos em específico. Outro aspecto da confidencialidade é a proteção do fluxo de tráfego contra análise (Impedindo que um atacante não consiga observar as características do tráfego durante uma comunicação como a origem e destino, frequência ou tamanho de blocos de dados).

- **Integridade de dados**: Assim como na confidencialidade, a integridade pode ser aplicada a uma única mensagem, a campos específicos dentro de uma mensagem ou a um fluxo de mensagens. A técnica mais útil e direta é a proteção total do fluxo.

- **Irretratabilidade**: Comumente conhecido como “não repúdio”, impede que o emissor ou o receptor neguem que uma mensagem foi transmitida ou recebida e ambos podem provar de fato que ocorreu.

15. CRIPTOGRAFIA

A criptografia é uma ferramenta fundamental para permitir que apenas o emissor e o receptor tenham acesso livre à informação trabalhada.

O termo criptografia surgiu das palavras gregas “kryptós” e “gráphein”, que significam: oculto e escrever, ou escrita oculta. É um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e receptor tenham acesso, a fim de impedir que intrusos a interpretem-na.

> Dentre as diversas tentativas de definir criptografia de maneira precisa, pode-se dizer, de um modo simples, que criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria seja maior que o custo obtido com a informação. Ela prevê formas de embaralhar ou cifrar mensagens visando torná-las inelegíveis e que posteriormente se possa obter a mensagem original. Para isso faz uso de chaves. Chave é um valor numérico para cifrar e decifrar um texto. a segurança de um criptossistema pode então ser mensurado baseado no tamanho do espaço de chaves e no poder computacional atualmente disponível. (Luiz Gustavo cordeiro da Silva, professor).

As chamadas *chaves criptográficas* é um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Ou seja, receptor da mensagem usa uma chave incompatível com a chave do emissor, não conseguirá extrair a informação. Um emissor pode usar o mesmo algoritmo (mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Os valores em bits expressam o tamanho de uma chave. Quanto mais bits forem utilizados na chave, mais segura será a criptografia. Exemplo: caso um algoritmo use chaves 128 bits (128 elevado a 2) resultaria em uma quantidade extremamente grande de combinações, tornando assim, a informação criptografada bem mais segura que uma chave com bits menores.

As chaves criptográficas classificam-se em dois tipos: chaves simétricas e chaves assimétricas.

15.1. Chave Simétrica

A chave simétrica é tipo de chave única, o qual o emissor e o receptor fazem uso da mesma chave para codificação e decodificação da informação. Alguns algoritmos fazem uso das chaves simétricas, tais como:

- DES: É um algoritmo que usa chaves de 56 bits, permitindo até 72 quatrilhões de combinações.

- IDEA: É um algoritmo que usa chaves de 128 bits e tem estrutura semelhante ao DES.

- RC: É um algoritmo que usa chaves de 8 a 1024 bits. Há várias versões: RC2, RC4, RC5 e RC6. Cada uma delas difere da outra por trabalhar com chaves de maior complexidade.

15.2. Chave Assimétrica

A chave assimétrica, também conhecida como “chave pública”, trabalha com duas chaves: a privada e a pública. Na chave pública, um emissor deve criar uma chave de codificação e enviá-la a quem for lhe enviar mensagens. Já a chave privada é criada para a decodificação e é secreta.

Entre os algoritmos que usam chaves assimétricas são: RSA (o mais conhecido) e o Diffie-Helman. A criptografia só pode ser considerada quando forem oferecidos: confidencialidade, autenticidade, integridade da informação e não repúdio (o remetente não pode negar o envio da informação). Sendo assim, um recurso de fundamental importância na transmissão de informações pela internet, e mesmo assim, não é capaz de garantir 100% de segurança, porque ainda há maneiras de quebrar uma codificação. Com isso, técnicas são aperfeiçoadas e outras são criadas, como a Criptografia Quântica e a função Hashing e aplicações, usada em assinaturas digitais.

16. METODOLOGIA

O método utilizado nessa pesquisa é de caráter bibliográfico de natureza cientifica aplicada. Por meio de referenciais teóricos baseados em livros de especialistas, uso de periódicos, cartilhas e manuais encontrados em sites de órgãos públicos. No que tange a questões de direito, referencia-se em Medidas provisórias, Leis e normas vigentes.

A pesquisa bibliográfica tem como objetivo reunir as informações e dados que servirão de base para a construção da investigação proposta a partir da temática; segurança digital e o uso das certificações.

Dessa forma, além de traçar um histórico sobre o objeto de estudo, também ajuda a identificar contradições e respostas anteriormente encontradas sobre as perguntas formuladas. Averiguar se outras pesquisas com problemáticas semelhantes já foram realizadas e fomentar a valorização da investigação, a partir de fontes secundárias.

Segue também a linha da Pesquisa Descritiva, porque cabe ao pesquisador do respectivo estudo, a análise, o registro e a interpretação dos fatos do mundo físico, sem a manipulação ou interferência pessoal. O qual deve descobrir com que frequência o fenômeno ocorre ou como se estrutura dentro de um determinado sistema, método, processo ou realidade operacional.

De acordo com Gil (2008), as pesquisas descritivas possuem como objetivo a descrição das características de uma população, fenômeno ou de uma experiência. Ela pode utilizar técnicas padronizadas de coleta de dados para apresentar as variáveis propostas, que podem estar ligadas às características socioeconômicas de um grupo ou outras características que podem ser alteradas durante o processo. A Pesquisa Descritiva também pode aparecer sob diversos tipos de pesquisa, tais como: documental, estudo de campo, levantamento de dados, entre outras.

17. CRONOGRAMA DE ATIVIDADES

1	Revisão Bibliográfica	Jan	Fev	Mar	Abr	Mai	Jun	Jul
2	Discursão teórica em função da determinação dos objetivos	x						
3	Localização e identificação das fontes de obtenção dos dados ou documentos		x	x				
4	Determinação de categorias para tratamento dos dados documentais			x				
5	Análise e interpretação				x			
6	Redação do TCC				x	x		
7	Revisão do TCC						x	
8	Defesa do TCC							x

18. CONSIDERAÇÕES FINAIS

No presente estudo, foi abordada a importância da certificação digital para as novas formas de se comprovar a autenticidade de documentos e informações. Processos antes realizados de forma analógica e que demandava maior esforço e tempo ao se locomover para fóruns e cartórios agora são realizados de forma automatizada e de acesso global com o advento da internet.

A observação dos aspectos, conclui-se que com a certificação digital possui uma série de vantagens, tais como: agilidade, segurança e confiabilidade nos arquivos emitidos, além de um maior controle no acompanhamento dos processos. A certificação digital veio para sanar o problema do sistema atual de atendimento, que ainda possui gargalos e atrasos no acesso as informações existentes e com maior rigor para impedir vazamentos e fraudes.

Instituições públicas e privadas que já reconhecem a importância dessa não tão nova tecnologia saíram ganhando juntamente com os usuários e clientes do sistema. Por isso, a expectativa é que surjam cada vez mais serviços a utilizar certificações digitais em suas operações.

19. REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo. Processo eletrônico e teoria geral do processo eletrônico: a informatização judicial no Brasil: 4ª Ed. Rio de Janeiro: Editora Forense, 2011.

Argolo, Paula. O sistema de Processo Judicial eletrônico (PJe): O que é e como se cadastrar. Disponível em: <https://paulaargolo.jusbrasil.com.br/artigos/267157445/o-sistema-de-processo-judicial-eletronico-pje-o-que-e-e-como-se-cadastrar>. Acesso em: 03 fev.2019.

Darlan, Vivian. O que é um certificado digital?. Disponível em: <https://www.bry.com.br/blog/o-que-e-um-certificado-digital/>. Acesso em: 21 jan.2019.

Gandini, João. Salomão Diana. Jacob, Cristiane. A segurança dos documentos digitais. Disponível em: <https://jus.com.br/artigos/2677/a-seguranca-dos-documentos-digitais/1>. Acesso em: 13 mar.2019.

ICP-BRASIL. Instituto Nacional de Tecnologia da Informação. Disponível em: <https://www.iti.gov.br/index.php>. Acesso em: 03 fev.2019.

Luz, Clarissa P. da, Centro de Certificação Digital: Construção, Administração e Manutenção, Rio de Janeiro: Editora Ciência Moderna, 2008.

Macêdo, Samir. Desvantagens do processo eletrônico. Disponível em: <https://samirmacedo.jusbrasil.com.br/artigos/424668735/desvantagens-do-processo-eletronico>. Acesso em: 13 mar.2019.

Machado, Robson Carvalho. Certificação Digital ICP-Brasil: 1ª Ed. Editora Impetus, 2010.

Marcel Boff. Assinatura Digital: Tudo o que você precisa saber. Disponível em: <https://www.santocontrato.com.br/assinatura-digital-tudo-o-que-voce-precisa-saber>>. Acesso em: 03 fev.2019.

Moecke, Cristian. O que é uma assinatura digital?. Disponível em: <https://www.bry.com.br/blog/o-que-e-uma-assinatura-digital/>. Acesso em: 21 mar.2019.

Silva, Luiz Gustavo Cordeiro da Silva, L.et al.Certificação Digital – Conceitos e Aplicações, Rio de Janeiro: Editora Ciência Moderna, 2008.

SILVA, Marcelo Mesquita Silva. Processo Judicial Eletrônico Nacional: Uma visão prática sobre o processo judicial eletrônico nacional (A certificação digital e a lei n 11419/06) São Paulo: Editora Milenium, 2012.

Stallings, William. Criptografia e segurança de redes: princípios e práticas: 6ª Ed. São Paulo: Editora Pearson Education do Brasil, 2015.

VOLPI, Marlon Marcelo. Assinatura Digital – Aspectos Técnicos, Práticos e Legais. Rio de Janeiro, Ed. Axcel Books, 2001.