FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

PÓS GRADUAÇÃO MBA EM
GERENCIA DE REDES E SEGURANÇA DA INFORMAÇÃO IV

SANDRA AUGUSTA BARRETO ROLLEMBERG CONRADO

SEGURANÇA DA INFORMAÇÃO NO JUDICIÁRIO

Aracaju
2016

A INFORMATIZAÇÃO DO JUDICIÁRIO BRASILEIRO E A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NA MANUTENÇÃO DA INTEGRIDADE DOS DADOS PROCESSUAIS

Sandra Augusta Barreto Rollemberg Conrado

Resumo

Este trabalho acadêmico tem como finalidade abordar a importância da Segurança da Informação na manutenção da integridade dos documentos processuais no judiciário brasileiro. Trata-se de uma revisão bibliográfica. Com o advento da Lei 11.419/2006 de informatização dos processos judiciais, ampliou-se a necessidade de garantir segurança e celeridade nas informações processuais. A presença das tecnologias de informação (TI) no judiciário brasileiro possibilita um conjunto de medidas que objetivam uma maior aproximação do Poder Judiciário com o cidadão, via virtualização das informações jurídicas, e do direito à informações viabilizadas pelo acesso a essa informação. A adoção dessas tecnologias vem permitindo a disponibilidade de acompanhamento processual e agilidade no processamento de decisões judiciais. Os resultados indicam que a Justiça virtual, além de trocar o papel pelo armazenamento dos autos em meio digital, evita uma série de derivações causadoras de morosidade na justiça. A Segurança da Informação tende a garantir credibilidade, autenticidade e agilidade destas informações, tornando o processo virtual apto e seguro.

Palavras-chave: Segurança da Informação. Processo Judicial Eletrônico. Celeridade.

THE COMPUTERIZATION OF THE JUDICIARY AND THE IMPORTANCE OF INFORMATION SECURITY IN MAINTAINING PROCEDURAL DATA INTEGRITY

Sandra Augusta Barreto Rollemberg Conrado

Abstract

This academic work aims to address the importance of information security in maintaining the integrity of the files in the Brazilian judiciary. This is a literature review. With the enactment of Law 11.419 / 2006 of computerization of court proceedings, it increased the need to ensure security and swiftness in procedural information. The presence of information technology (IT) in the Brazilian judiciary provides a set of measures aimed at further approximation of the judiciary with the citizen via virtualization of legal information, and the right to information made possible by access to this information. The adoption of these technologies has enabled the availability of procedural monitoring and speed in processing judgments. The results indicate that the virtual Justice, and change the paper by storing the file in digital media, prevents a number of derivations causing delays in justice. Information security can guarantee credibility, authenticity and agility of this information, making the fit and secure virtual process.

Keywords: Information Security. Electronic Judicial Process. Celerity.

LISTAS

Sumário

1 INTRODUÇÃO

O acesso à informação tem sofrido diversos tipos de modificações ao longo da história humana, a primeira veio com o advento da escrita onde o conhecimento era repassado sem ser corrompido ou distorcido, surge nesta mesma onda o direito romano e medieval. Veio uma segunda onda com o advento da impressão permitindo uma divulgação mais ampla e possibilitando um maior acesso ao conhecimento No século XX, o conhecimento passa a ser difundido de forma sonora e visual com o surgimento do rádio e da televisão. Atualmente vivencia-se a onda informação interativa (LACERDA, 2014)

As diversas mudanças sofridas pela sociedade têm atingido as instituições públicas e privadas, dentre elas, o Poder Judiciário. “Nessa busca é natural que a própria instituição questione essa nova estrutura, composição e organização da sociedade, de tal forma que possa estar em sintonia com suas expectativas” (SARDETO e ROVER, 2013, p. 184)

Alvares (2011) discorre que no decorrer dos anos, com o surgimento da globalização, cumulada com o advento da era digital e o aumento da população, o crescimento de lides se torna cada vez mais constante, e faz com que a máquina do Poder Judiciário seja acionada, acarretando, consequentemente, em um aumento significativo no volume de processos em tramitação a serem solucionados, abarrotando os corredores dos Tribunais e comprometendo os julgamentos dos processos nos Tribunais.

O Poder Judiciário, procurando diminuir os volumes de processos em trâmite, e melhorar a prestação de serviços à comunidade, tem-se utilizado da tecnologia como ferramenta essencial neste processo (ALVARES, 2011)

O Processo Judicial Eletrônico (PJE) tem sido uma destas ferramentas para agilizar as demandas cada vez mais crescentes, é algo irreversível. Essa modalidade cria uma nova perspectiva aos usuários acerca de sua segurança, simplicidade de uso e desburocratização. O tempo de espera, consequência de trabalhos manuais, como distribuição, autuação, juntadas de petições, cadastros e

conclusões, tem a séria necessidade de minimização atendida com o advento da Lei n.º 11.419/2006 (RODRIGO; FLORES, 2014)

A lei nº 11.419/2006 visou padronizar os atos processuais por meios eletrônicos, a discussão entre direito e as novas tecnologias não é tão recente assim. Rodrigo e Flores (2014) discorrem que essa Lei, precedida por outras tantas que já visavam desburocratizar os serviços do Poder Judiciário, tem como objetivo implementar o Processo Judicial Eletrônico em todas as instâncias da Justiça em nível nacional. Após sua promulgação, cada tribunal passou a ter autonomia para padronizar e regulamentar suas funcionalidades e sistemáticas para a elaboração de normas de organização. Como consequência, uma grande variedade de práticas processuais por meio eletrônico surgiu em cada tribunal do Brasil.

O problema a ser enfrentado será entender qual a relevância da Segurança da Informação neste processo de informatização do judiciário brasileiro.

Como hipótese podemos destacar que a Segurança da Informação no judiciário tende a preservar a integridade das informações e dos equipamentos utilizados.

Este trabalho de pesquisa se justifica na medida que a Lei 11.419/2006, que determina de forma mais ampla a informatização do Poder Judiciário, precisar ser melhor analisada, e saber qual o papel da Segurança da Informação neste processo de modernização do judiciário. Quais as contribuições trazidas pela Segurança da Informação, principalmente, na gestão do Processo Judicial Eletrônico?

1.1 OBJETIVO GERAL

O objetivo principal deste trabalho será analisar a Segurança da Informação no Poder Judiciário.

1.2 OBJETIVOS ESPECÍFICOS

- Discorrer sobre a Segurança da Informação e a sua Evolução
- Abordar sobre a Segurança da Informação no Poder Judiciário
- Destacar a Lei 11.419/2006, o processo eletrônico nos tribunais e as inovações advindas da mesma
- Enfatizar os reflexos do processo judicial eletrônico e seu alcance
- Demonstrar a Importância da Segurança da Informação na Preservação e Integridade dos dados digitais/processuais nos Tribunais brasileiros.

1.3 METODOLOGIA

Procurando alcançar os objetivos deste trabalho, optou-se por uma pesquisa bibliográfica. Lakatos e Marconi (2003, p. 158), entende que:

> A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações

Gil (2008, p.50) complementa dizendo que “A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente”.

As fontes utilizadas serão: livros, artigos especializados na temática jurídica e da Segurança da Informação, a Lei 11.419/2006 (informatização do judiciário brasileiro), repositórios de teses e dissertações das Instituições de Ensino Superior do Brasil.

2 SEGURANÇA DA INFORMAÇÃO

2.1 CONCEITOS RELACIONADOS COM A SEGURANÇA DA INFORMAÇÃO

Conforme a Instrução Normativa nº. 1 de 13/06/2008, oriunda do Gabinete de Segurança Institucional da Presidência da República, define Segurança da Informação e Comunicações como:

> Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [...] tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos; o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta; o dever do Estado de proteção das informações pessoais dos cidadãos; a necessidade de incrementar a segurança das redes e bancos de dados governamentais; e a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta. (BRASIL, 2008).

Loureiro (2008, p.15), citando Norma ABNT NBR ISO/IEC 27002, pontua que:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades

A informação existe de diferentes formas: escrita em papel, impressa, armazenada no formato eletrônico, pelo correio, e-mail, filmes, dentre outras. Independente da forma é recomendado que as informações sejam protegidas adequadamente.

A Segurança da Informação, segundo NBR ISO/IEC 27002:2013, é a proteção de vários tipos de ameaças no intuito de minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ABNT, 2013).

A Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal instituída através do Decreto 3.505, de 13 de junho de 2000, no seu art. 2º, item II, diz:

> II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento. (BRASIL, 2000)

Através de uma revisão de literatura Miranda (1999) *apud* Loureiro (2008, p.39) estabeleceu alguns conceitos sobre informação:

- Dado é conjunto de registros conhecidos;
- Ativo é o dado conhecido, organizado, agrupado, categorizado e padronizado;
- Informação são dados organizados de modo significativo, sendo subsídio útil a tomada de decisão;
- Informação estratégica é a informação obtida do monitoramento estratégico, que subsidia a formulação de estratégias pelos tomadores de decisão nos níveis gerenciais da organização;
- Informação de acompanhamento é a informação obtida do monitoramento interno, que aliada a informação estratégica, constitui-se em conhecimento estratégico explicito;
- Sistema de informações estratégicas é o conjunto de ferramentas informatizadas que permite o tratamento dos dados coletados pelo monitoramento estratégico, transformando em informações e agregando conhecimento, a fim de que se constitua insumo para a inteligência estratégica;
- Sistema especialista é a ferramenta informatizada que agrega o conhecimento de especialistas ao processamento de informações que suportam a tomada de decisão;
- Sistema não especialista é a ferramenta informatizada que processa informações usadas na tomada de decisão sem agregar o conhecimento de especialistas no processamento.

Conforme Laureano (2005) os princípios básicos para garantir a segurança das informações, são:

- Confidencialidade: a informação somente pode ser acessada por pessoas explicitamente autorizadas; é a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

- Disponibilidade: a informação ou sistema de computador deve estar disponível a quem possa acessá-la no momento em que a mesma for necessária;

- Integridade: A informação deve ser retornada em sua forma original no momento em que foi armazenada; é a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

No decorrer dos tempos muitos conceitos foram incorporados a Segurança da Informação, no quadro 1, alguns mais comuns:

Quadro 1 Conceitos importantes em segurança da informação

CONCEITO	DESCRIÇÃO
Ameaça	É algo que oferece risco à organização através de atuação de alguém sobre alguma vulnerabilidade. Segundo Sêmola (2003) elas podem ser classificadas em: naturais (advindas de fenômenos da natureza, como terremotos, enchentes etc.); involuntárias (inconscientes por erros ou acidentes); voluntárias (ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários)
Antivírus	Programa que faz a varredura de arquivos maliciosos disseminados principalmente pela Internet ou correio eletrônico. Basicamente, sua função está atrelada à ponta do processo, isto é, ao usuário que envia e recebe dados. Uma das últimas tendências deste tipo de ameaça são os chamados "vírus polimórficos", que possuem a capacidade de mudar constantemente para driblar a vítima e dificultar sua remoção
Ataque	É a efetivação da ameaça
Ativos	Todo recurso que é precioso para a organização e deve ser protegido de um ataque
Auditoria	Processo de coleta de evidência na utilização de informações. É utilizada para identificar entidades envolvidas na comunicação. Pode resultar, por exemplo, em detecção de falhas ou responsabilização de ataques
Autenticação	São processos de identificação para disponibilizar acesso. A autenticação e conseqüente autorização de manipulação dos dados se baseiam em algo que o indivíduo sabe (uma senha, por exemplo), algo que ele tem (dispositivos como tokens, cartões inteligentes, etc.) e o que ele é (leitura de íris, linhas das mãos etc.)
Balanceamento de carga	As ferramentas de balanceamento estão relacionadas à capacidade de operar de cada servidor da empresa. Elas permitem que, em horários de grande utilização da rede, se determine a hierarquia do que trafega, bem como o equilíbrio da carga disseminada entre os servidores
Criptografia	É utilizada para garantir a confidencialidade das informações. Trata-se de uma codificação que usa um processo de decifração para restaurar os dados ao seu formato original. As chaves criptográficas podem ser simétricas (privada) ou assimétricas (pública)

Detector de Intrusão (IDS)	Estas ferramentas têm a função de monitorar o tráfego contínuo da rede, identificando ataques que estejam em execução. Como complemento do firewall, o IDS (*Intrusion Detection System*) se baseia em dados dinâmicos para realizar sua varredura, como por exemplo, pacotes de dados com comportamento suspeito, códigos de ataque e outros
Divulgação	Exposição de informações confidenciais capturadas de forma desonesta
Elevar privilégios	Alteração de nível de segurança de um usuário para níveis com maior acesso
Falsificação	Quando uma pessoa se passa por outra, por exemplo, utilizar senha de outro usuário de sistema
Firewall	Cumprem a função de controlar os acessos. São soluções que, uma vez estabelecidas suas regras, passam a gerenciar tudo o que deve entrar e sair da rede corporativa. Muitas vezes, recomenda-se a adoção do firewall para separar a intranet da companhia de seus clientes externos ou de servidores e serviços públicos. Basicamente, o firewall é um software, mas também pode incorporar um hardware especializado
Impacto	Abrangência dos danos causados pelo incidente de falha na segurança nos processos de negócio da organização
Incidente	Evento decorrente da ação de uma ameaça causando impactos nos processos do negócio
Integradores	Permite centralizar o gerenciamento de diferentes tecnologias que protegem as operações da rede. Mais que uma solução, trata-se de um conceito
Legalidade	Características de informações que possuem valor legal
Rede Privada Virtual (VPN)	Uma das alternativas mais adotadas pelas empresas na atualidade, as VPN's são canais que utilizam túneis para trafegar dados criptografados entre divisões de uma mesma companhia, parceiros de negócios etc.
Repudiação	Negar a violação/ataque, por exemplo, apagar o *log* (histórico de acessos) de uma máquina
Risco	Probabilidade de perda dos princípios da Segurança (confidencialidade, integridade e disponibilidade) através de ameaças que explorem as vulnerabilidades
Varredura de vulnerabilidades	Produtos que permitem realizar verificações regulares em determinados componentes de rede como servidores e roteadores. O objetivo destas ferramentas é encontrar brechas de sistemas ou configurações
Violação	Alteração de dados
Vulnerabilidades	Pontos susceptíveis a ataque e ameaças, como: roubos de senhas, engenharia social, segurança de dados incorreta, segurança física incorreta e transmissão de dados em criptografia. Podem ser classificadas em diversos tipos, sendo as mais comuns: de hardware, de software, de comunicação e humanas

Fonte: Nobre (2009, p. 33-34)

No entender de Ramiro (2008, p. 8) “é através da implantação de diretrizes, normas, procedimentos e controles adequados que se obtém a segurança da informação, garantindo a operação da instituição”.

2.2 SEGURANÇA DA INFORMAÇÃO NO SETOR PÚBLICO

A organização norte-americana CERT (*Computer Emergency Response Team*) foi criada em 1988 com o objetivo de monitorar a segurança na internet e coordenar a atuação de agências autorizadas na fiscalização realizada na rede mundial de computadores. Pesquisa realizada pelo CERT em 2008 destaca que incidentes de Segurança da Informação no âmbito governamental é bastante crítico. O governo americano tem cada vez mais investido na proteção de sua infraestrutura governamental (NOBRE, 2009)

Miranda e Streit (2007) discorrem que a gestão da informação em organizações públicas é mais complexa por necessitar de prestação de contas da tomada de decisão e transparência com fluxo confiável. Sem uma Gestão de Segurança da Informação adequada, amplia-se o risco de ataques e perdas que podem causar prejuízos aos cofres públicos.

As demandas de informações no serviço público exigem alto grau de confiabilidade e segurança. São cada vez maiores os investimentos demandados pelos órgãos públicos na informatização e Segurança da Informação (PLANO EDITORIAL, 2005)

As seguintes falhas podem trazer perdas ao patrimônio público:

> Ataques físicos (roubos ou danificação de equipamentos); Ataques lógicos (adulteração de dados financeiros, exclusão de multas, adulteração de valores de pagamentos etc.); Perda de credibilidade como as organizações públicas têm o papel de servir toda a sociedade, os prejuízos podem ter repercussões bem maiores e causar prejuízos mais amplos porque atingem os interesses de todos os cidadãos. Além disso, a agilidade em processos de aquisição deve ser considerada, já que na área pública a tramitação de processos desta natureza costuma ser mais lenta pelas exigências legais. Isso pode resultar em sérios problemas na segurança se não houver uma gestão adequada (NOBRE, 2009, p.40)

Sendo o Tribunal de Contas da União (TCU) o órgão de auditoria de Governo Federal, tem desempenhando ações no sentido que os órgãos da Administração Pública Federal - APF cumpram o previsto nos atos normativos sobre a segurança da informação e promovam ações com objetivo de disseminar a importância da segurança da informação. A seguir, algumas decisões do órgão sobre o tema, citado por Loureiro (2008, p. 45-46):

> Decisão nº. 669/1995 - Plenário
>
> _ 2.1. Estude a possibilidade de implementar, a médio prazo, no âmbito do seu plano de contingência, uma solução alternativa para o caso de perda total das instalações da Filial São Paulo, nas quais se opera o processamento da Arrecadação Federal, para que o tratamento das informações essenciais não sofra solução de continuidade no caso de ocorrência de sinistro de grandes proporções;
>
> Decisão nº. 445/1998 - Plenário
>
> _ 3.7.1. Disciplinar de forma rígida o acesso de pessoas aos andares do prédio onde a Gerência Executiva de Tecnologia [...] se encontra instalada;
>
> _ 3.7.2. Definir, oficialmente, junto aos gestores responsáveis, uma sistemática de "back-up" para os sistemas existentes;
>
> _ 3.7.5. Definir regras que regulamentem o acesso de usuários externos ao ambiente computacional;
>
> Acórdão n.º 2.023/2005-Plenário - Determinações
>
> _ defina uma Política de Segurança da Informação, nos termos das orientações contidas no item 3 da NBR ISO/IEC 17799:2001, que estabeleça os princípios norteadores da gestão da segurança da informação no Ministério e que esteja integrada à visão, à missão, ao negócio e às metas institucionais, observando a regulamentação ou as recomendações porventura feitas pelo Comitê Gestor de Segurança da Informação instituído pelo Decreto n. 3.505/2000 e pelo Gabinete de Segurança Institucional da Presidência da República, conforme Decreto n. 5.408, de 1º/04/2005;
>
> Acórdão nº. 2.023/2005-Plenário - Determinações
>
> _ estabeleça institucionalmente as atribuições relativas à segurança da informação, conforme preceituam os itens 4.1.1, 4.1.2 e 4.1.3 da NBR ISO/IEC 17779:2001;
>
> _ não assuma responsabilidades inerentes às áreas de negócio, como a inserção, alteração e exclusão de informações em bases de dados;
>
> _ crie critérios de classificação das informações;
>
> _ crie mecanismos para que as políticas e normas se tornem conhecidas, acessíveis e observadas;
>
> _ o acesso ao ambiente de produção deve ser feito de forma controlada pelos gestores dos sistemas;
>
> Acórdão n.º 2.023/2005-Plenário – Determinações defina uma Política de Controle de Acesso aos ativos de informação que contenha, no mínimo:
>
> 9.1.3.1. Regras de concessão, de controle e de direitos de acesso para cada usuário e/ou grupo de usuários [...], conforme preceitua o item 9.1.1 da NBR ISO/IEC 17799:2001;
>
> 9.1.3.2. Responsabilidades dos gestores de negócios sobre os seus sistemas, bem como a obrigação deles [...] fazerem a revisão periódica, com

> intervalos de tempo previamente definidos, dos direitos de acesso dos usuários, conforme preveem os itens 9.2.1, incisos h e i, e 9.2.4 da NBR ISO/IEC 17799:2001;
>
> _ Acórdão n.º 1.092/2007-TCU-Plenário – Determinações _ inventarie os ativos de informação e estabeleça critérios para a classificação desses ativos;
>
> _ implante a gestão de continuidade do negócio e elabore o Plano de Continuidade do Negócio (PCN);
>
> _ implante e divulgue sua Metodologia de Desenvolvimento de Sistemas (MDS) em toda a Empresa, à semelhança das orientações contidas nos itens PO 8.3 e AI 2.7 do COBIT 4.0.
>
> Ademais, estabeleça os requisitos mínimos de documentação que todos os sistemas devem apresentar, inclusive os sistemas legados, e defina um prazo para que todos os sistemas estejam adequados à nova MDS.

Toda essa preocupação com a Segurança de Informação na Administração Pública é relevante, falhas de segurança nas informações do setor público geram repercussão negativa e prejuízos consideráveis, pois o sistema público atende toda a sociedade. Segurança da Informação na Administração Pública é algo essencial na atual conjuntura.

3 A LEI 11.419/2006 – INFORMATIZAÇÃO DO PROCESSO JUDICIAL BRASILEIRO

A informatização do processo judicial no Brasil surgiu com o advento da Lei n° 11.419/06, cujo projeto tramitou no Congresso Nacional por mais de cinco anos (ALMEIDA FILHO, 2010)

O Projeto de Lei nº 5828, cujo relator foi o Deputado José Eduardo Cardozo, percorreu um longo caminho até originar a Lei 11.419/06. Primeiramente foi originado de uma iniciativa popular encaminhado pela Associação de Juízes Federais do Brasil (AJUFE). Após ter sido acolhida e ratificada pela Comissão de Participação da Câmara, obteve parecer favorável do Deputado Federal Ney Lopes (ALMEIDA FILHO, 2010)

No ano de 2002, o projeto foi recebido pela Comissão de Constituição e Justiça e Cidadania e foi designado relator do projeto o Deputado Federal Roberto Batochio, o qual apresentou parecer favorável pela constitucionalidade e sua

aprovação. Dessa forma, o projeto foi aprovado à unanimidade na Comissão em 11/06/2002(ALVARES, 2011)

A tramitação do projeto ainda demorou alguns anos entre debates e ajustes, e em 30 de novembro de 2006 o substitutivo do Senado Federal foi aprovado pela Câmara dos Deputados, surgindo a lei nº 11.419/2006 (ALVARES, 2011)

O Presidente da República sancionou a Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, e altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil. Pelas regras trazidas com a legislação, os procedimentos judiciais nas áreas civil, penal e trabalhista poderão ser feitos por meio eletrônico (GUIMARÂES, 2008)

A Lei nº 11.419 está dividida em quatro capítulos, a saber:

I – Da informatização do processo judicial;

II – Da comunicação eletrônica dos atos processuais;

III – Do processo eletrônico e

IV – Disposições finais

Rodrigo e Flores (2014) entendem que as inovações tecnológicas precisam ser absorvidas no âmbito processual, e a integridade sistêmica do Direito deve ser preservada. Para isso, as balizas para tal renovação e avanço do procedimento judicial têm sido expressas na Lei n.º 11.419/2006. Essa Lei estabelece diretrizes a todas as instâncias do país para a informatização do processo e tem vistas à redução de despesas, à minimização do tempo de trâmite e à eliminação do papel como meio físico.

De acordo com Atheniense (2010, p.25):

> Ainda que, *a priori*, tal dispositivo legal estabeleça caráter meramente autorizativo quanto ao uso do processo eletrônico pelos tribunais, entendemos que este é um caminho que, em poucos anos, se tornará obrigatório, não somente pela necessidade de evolução tecnológica do judiciário, mas, principalmente, pelo agravamento de sua incapacidade de absorver a crescente demanda pela prestação jurisdicional, que acarreta excessiva e danosa morosidade na resolução dos litígios judiciais.

Rodrigues e Flores (2014) acreditam que nesse sentido, com a Lei n.º 11.419/2006 servindo como base para uma nova perspectiva de processo judicial,

cabe aos órgãos competentes do Poder Judiciário desenvolver sistemas e soluções informáticas que venham ao encontro dos fundamentos arquivísticos e promovam uma grande mudança cultural, de modo a minimizar os impactos e consolidar de maneira positiva a implementação dessa nova tecnologia, que é uma ferramenta a serviço do instrumento processual. Portanto, sua incorporação deve ser feita resguardando-se os princípios do processo e os seus objetivos

3.1 A UTILIZAÇÃO DA INFORMÁTICA PELO PODER JUDICIÁRIO

A informatização da justiça brasileira já dura mais de três décadas, e atualmente aponta para a importância da formulação de uma política pública para acesso por meios eletrônicos aos serviços prestados pelos órgãos judiciários (ZAMUR FILHO, 2011)

Andrade (2011) discorre sobre os estágios de informatização da justiça brasileira, podendo ser resumido da seguinte forma:

- Em meados dos anos 80, a arquitetura dos sistemas computacionais era suportada por grandes computadores centrais, aos quais se conectavam, por cabo, terminais de digitação, com propriedades telemáticas limitadas. Naquele contexto, a informatização de cada tribunal estava restrita ao controle da distribuição e localização dos processos, ao registro das fases processuais e ao cadastro das partes. Em muitos casos, os graus de jurisdição possuíam soluções diversas, que não contemplavam a comunicação entre si (este fato podia ser observado até pouco tempo atrás, tanto na no sistema de justiça federal quanto nos tribunais estaduais). Este período é o da “pré-informatização”.

- No início dos anos 90, houve a informatização institucional dos tribunais, com a implantação de sistemas informáticos para controle do andamento e impulso processual e outros, de caráter administrativo, mas que não seguiram as diretivas de padronização e integração previstas, pertinentes ao planejamento de sistemas computacionais

- A partir de 1995, com a disseminação dos microcomputadores e das redes locais operando sobre ambiente multitarefa (notadamente com a predominância do *Microsoft Windows*) se buscou informatizar as áreas administrativas e seus fluxos de trabalho, que anteriormente realizavam suas operações baseadas em terminais de sistemas de grande porte, com poucos sistemas informatizados disponíveis e ainda amparados em controles manuais. Ainda assim, continuava a perspectiva insular, e cada tribunal e suas equipes de desenvolvimento de sistemas trabalhavam em soluções e projetos locais.

- No início dos anos 2000, houve um esforço de integração dos Tribunais Superiores e respectivos Tribunais Regionais no sistema de justiça federal. Na Justiça Federal, sob a coordenação do Conselho da Justiça Federal, realizou-se o exercício programado de comparações (*benchmarking*) entre os sistemas desenvolvidos por cada Tribunal Regional, em especial os administrativos, e o acompanhamento da implantação do sistema virtual dos JEFs da 3ª Região. Na Justiça do Trabalho houve interação dos Tribunais Regionais, inclusive com definição de sistemas prioritários e divisão das responsabilidades quanto ao desenvolvimento das soluções para utilização comum. Os Tribunais de Justiça estaduais ainda se informatizavam autonomamente, com apoio nas companhias estaduais de processamento de dados ou pela contratação de empresas especializadas.

- Após a vigência das leis nº 11.280/06 e nº 11.419/06, houve uma aceleração da informatização dos tribunais, com suas administrações mais atentas ao uso dos meios eletrônicos na tramitação dos processos e na comunicação dos atos processuais. A Lei nº 11.419/06, ao permitir o desenvolvimento descentralizado dos sistemas de processamento eletrônico pelos tribunais (art. 8º), prorrogou a total autonomia dos tribunais no desenvolvimento de sistemas, o que levou a uma grande redundância de esforços e investimentos por uns, e da impossibilidade de realização por outros, tamanha a disparidade entre as estruturas dos tribunais estaduais e o distanciamento, no sistema de justiça federal, entre a jurisdição comum e as especializadas

Zamur Filho (2011) esclarece que o cenário começou a se alterar a partir de uma postura mais ativa do Conselho Nacional de Justiça, que primeiramente se comprometeu a desenvolver e implantar nos tribunais estaduais o sistema Projudi, a partir de 2006. Em continuidade, e dentro de uma visão sistêmica da Justiça, vem assumindo a primazia da formulação estratégica do desenvolvimento das TICs aplicadas pelo Poder Judiciário, com o objetivo de implantação do PJE em todos os órgãos jurisdicionais

3.2 INOVAÇÕES DA LEI 11.419/2006

a) **A ciência presumida**

A Inovação trazida pela Lei 11.419/2006 no sentido de considerar realizada a comunicação após dez dias da inclusão no site está contida no parágrafo 3º do artigo 5º da lei 11.419/06.

> Art. 5º. As intimações serão feitas por meio eletrônico em portal próprio aos que se cadastrarem na forma do art. 2o desta Lei, dispensando-se a publicação no órgão oficial, inclusive eletrônico.
>
> § 1º Considerar-se-á realizada a intimação no dia em que o intimando efetivar a consulta eletrônica ao teor da intimação, certificando-se nos autos a sua realização.
>
> § 2º Na hipótese do § 1o deste artigo, nos casos em que a consulta se dê em dia não útil, a intimação será considerada como realizada no primeiro dia útil seguinte.
>
> § 3º A consulta referida nos §§ 1o e 2o deste artigo deverá ser feita em até 10 (dez) dias corridos contados da data do envio da intimação, sob pena de considerar-se a intimação automaticamente realizada na data do término desse prazo.

O compromisso firmado pelo usuário no momento do cadastramento serve para dar um limite temporal à boa vontade do usuário. A essa forma estabelecida pela lei deu-se o nome de ciência presumida (SANTOS, 2010)

b) **Vista pessoal eletrônica aos autos**

O artigo 9º, parágrafo primeiro da lei 11.419/2006 traz uma questão interessante:

> Art. 9º No processo eletrônico, todas as citações, intimações e notificações, inclusive da Fazenda Pública, serão feitas por meio eletrônico, na forma desta Lei.
>
> § 1º As citações, intimações, notificações e remessas que viabilizem o acesso à íntegra do processo correspondente serão consideradas vista pessoal do interessado para todos os efeitos legais.

Com o recebimento do ato citatório na via eletrônica, ter-se-á acesso a todo o processo proposto. Isso derruba a necessidade de o demandado ou o seu procurador deslocar-se até o cartório competente para ter vista aos autos. Esta e a grande diferença em relação ao procedimento tradicional.

Abrão (2009) destaca que, para se considerar válido o ato por si só, a parte interessada necessitará ter plena capacidade de acessar os dados, ficando, consequentemente, registrados no próprio encaminhamento eletrônico do procedimento.

c) **Comunicação entre tribunais de diferentes jurisdições**

Para que um órgão judiciário se comunique oficialmente ou solicite atos processuais a outro que não esteja sob os limites territoriais da comarca, fazem-se necessárias as seguintes cartas: rogatória, de ordem e precatória. A primeira é dirigida a um juiz subordinado ao tribunal remetente, a segunda a uma autoridade judiciária estrangeira e a terceira para os demais casos, ou seja, a um juiz por outro sem que entre os dois não haja nenhum tipo de subordinação. Fazem-se necessários, ainda, a realização de acordos para que a interoperabilidade se possibilite, isso dentro do território nacional, já nas relações internacionais necessita-se de tratados que estabeleçam a forma de cumprimento das cartas (SANTOS, 2010).

A adoção do procedimento eletrônico nos órgãos judiciais vai alterar a rotina de serviços dos auxiliares da justiça. Não mais será necessária a autuação de processo, anotações manuais e outros atos que tomavam o tempo dos servidores. Desta forma a sequência dos autos poderá ser realizada de forma mais organizada e ágil (ABRÃO, 2009).

Santos (2010) enfatiza que esta situação exigirá adaptações, mudanças de hábitos e da mentalidade. É comum a dificuldade na adaptação a certas mudanças.

Nesse caso apesar de causar algum ou outro contratempo, é uma mudança irreversível e necessária.

Além disso, até mesmo a saúde não correrá o risco de contaminação com bactérias contidas em autos que receberam umidade excessiva (CINTRA, 2009). Isso não é algo tão incomum ao se considerar que em muitas repartições judiciárias a estrutura existente no armazenamento dos documentos é precária.

3.3 OS JUIZADOS ESPECIAIS CÍVEIS E O PROCESSO ELETRÔNICO

Com o advento da Lei nº 11.419 de 19 de dezembro de 2006 foi possível vislumbrar ideias inovadoras em relação ao processo uma vez ser este viabilizado por meio eletrônico sendo definido pelo próprio estatuto legal como “qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais” (artigo 1º, parágrafo 2º, inciso I).

Assim, muitas características positivas serão proporcionadas através do processo informatizado, tendo como uma delas a celeridade processual, algo que na sociedade em que se vive é muito prezado. Além disso, efetivando alguns princípios constitucionais que constam apenas em um rol no qual o cidadão não consegue de fato ter garantido, como no caso de um processo célere, implica diretamente no direito de acesso à justiça, ou seja, o acesso à justiça se torna mais “palpável” para todos quando se tem de forma definitiva, efetiva e segura, assegurado o direito que se pleiteia (PEREZ; CORONA, 2010)

Os Juizados Especiais virtuais surgiram, além de outros, com objetivo de promover um mais amplo, célere e efetivo acesso à justiça.

Perez e Corona (2010) discorrem que a princípio, os Juizados Especiais foram instalados para trabalhar com autos físicos, o que já constituiu um grande avanço, dada a rapidez de procedimento. Entretanto, tão logo instaladas as primeiras unidades dessa justiça especializada, percebeu-se que a simples criação de um rito procedimental mais célere e pautado em princípios como a oralidade e a conciliação

não seria suficiente para o escopo de imprimir a celeridade e a eficiência almejadas ao serviço judiciário.

De acordo com Carvalho (2006, p. 459):

> Diante do assombroso quadro de lentidão da máquina jurídica, corroborado também por um jurássico gerenciamento das atividades cartorárias, cujo estado de agonia é revelado pelo abarrotamento das secretarias judiciárias, que já não dispõem sequer de espaço físico para o armazenamento de autos processuais, sem falar no tempo dispensado pelos servidores no atendimento ao público, advogados e juntada de documentos, acreditou-se que a solução do problema passaria necessariamente pela informatização de todo o sistema, desde o ajuizamento da petição até a satisfação da pretensão.

Em iniciativa pioneira, no âmbito da Justiça Estadual, a 10ª Vara do Juizado Especial da Comarca de Campo Grande, criada especialmente pelo Tribunal de Justiça do Mato Grosso do Sul, para implantar o processo virtual no Estado, implantou em janeiro de 2005 o sistema de tramitação de processos integralmente eletrônico, eliminando o uso do papel nos processos, e descontinuando os autos físicos e os tradicionais arquivos. Nessa pioneira experiência, foram observados os seguintes benefícios, conforme quadro 1.

Quadro 2: Benefícios do processo virtual

AUMENTA	REDUZ
Celeridade na tramitação processual	Sobrecarga dos cartórios
Qualidade da prestação jurisdicional	Tempo de atendimento ao público
Economia de recursos e tempo	Custos diversos
Produtividade e eficiência das tarefas	Fluxo de advogados no setor de distribuição e nos cartórios
Disponibilidade da informação	Espera na obtenção de informações
Integração entre justiça e jurisdicionado	Volume de papel e materiais de expediente
Reaproveitamento de informações	Perda de páginas ou documentos

Agilidade e padronização das rotinas cartorárias	Redigitação de dados no setor de cadastro e distribuição
Manipulação de lotes de processos em fluxos de trabalho	Diferenças procedimentais e desvios no andamento do processo
Organização e planejamento das atividades	Trabalhos repetitivos e manuais
Praticidade na consulta de processos	Cargas de processos
Comodidade do jurisdicionado	Necessidade de deslocamento até o tribunal

Fonte: Carvalho (2006, p. 463)

A Justiça virtual, portanto, além de trocar o papel pelo armazenamento dos autos em meio digital, evita uma série de derivações causadoras de morosidade na justiça

Fontes (2013) enfatiza que os atos praticados nos processos virtuais recebem as chamadas assinaturas virtuais, também conhecidas como certificação digital ou assinatura eletrônica.

Desta forma, a Lei nº. 11.419, de 19 de dezembro de 2006, chamada de lei de informatização do judiciário, prevê o uso de meio eletrônico para a tramitação de processos judiciais, a comunicação de atos e a transmissão de peças processuais.

A utilização está prevista para os processos civis, penais e trabalhistas, além daqueles da competência dos juizados especiais. O sistema operacional atual é o Projudi que permite a tramitação totalmente eletrônica de processos judiciais, via internet. Ele foi desenvolvido em software livre pelo Conselho Nacional de Justiça e distribuído gratuitamente a todos os órgãos da justiça interessados. O sistema Projudi foi implantado com a finalidade de permitir à ampliação do acesso à justiça e imprimir celeridade aos processos no rito do juizado especial (FONTES, 2013).

O processo virtual é uma realidade, já que estão em pleno funcionamento nos Juizados Especiais, com autos e procedimento totalmente virtuais, e porque foram

ungidos com objetivo de promover mais amplo, célere e efetivo acesso à justiça. Na transição do processo tradicional para o eletrônico, destacam--se os seguintes estágios: a informatização das rotinas internas de acompanhamento processual; a disponibilidade *on-line* de atos processuais; a prática de atos processuais por meios eletrônicos (CARVALHO, 2006)

3.4 REFLEXOS DO PROCESSO JUDICIAL ELETRÔNICO

Refletir sobre o alcance do Processo Judicial Eletrônico(PJE), entendido no sentido da abrangência e aderência dos meios eletrônicos em sentido amplo (mídia, telemática, certificação e outros de seus elementos formadores) ao direito processual, e de sua efetividade, enquanto capacidade de produzir resultados reais implica em encontrar referenciais úteis sobre as modificações que ocorrem nos direitos e deveres processuais e no atingimento dos múltiplos escopos processuais quando da transição do processo-papel para o processo eletrônico(ZAMUR FILHO, 2011)

> É importante entender que a distinção entre o que o direito processual civil moderno pode esperar do processo, que foi condicionado, secularmente à sua representação por meio dos autos, e aquela que advirá da ampliação do Processo Judicial Eletrônico (PJE) a todos os tribunais e de sua interoperabilidade com outros sistemas de governo eletrônico e com a Internet, é a de sua aproximação e conexão com o mundo. O processo já não estará dependente de seu meio físico, e nem mesmo estará, aqui ou ali: permanecerá conectado, pois será um arquivo disponibilizado na Internet (ZAMUR FILHO, 2011, p.117)

O Processo Judicial Eletrônico(PJE) potencializa a conexão imediata dos sujeitos processuais com a lide, e desta com o mundo: corrobora tal fato as regras esculpidas pela Lei nº 11.382/06, ao inserir o art. 655-A no CPC (que permite a penhora on-line) e pela própria Lei nº 11.419/06, que em seu art. 13 prevê a possibilidade, por determinação judicial, de consulta a cadastros públicos (entendidos como bases de dados públicas e privadas) e da transmissão eletrônica de documentos para a instrução do processo (CHAVES JÙNIOR, 2010)

Zamur Filho (2011) explica que se antes, dentro do modelo liberal, o juiz esteve vinculado ao que constava nos autos para decidir, a partir da constatação da

natureza publicista do processo, este já não estava mais adstrito à verdade formal, mas lhe faltavam meios: recursos, tempo e auxiliares para realizar suas diligências. Com a conexão permitida pelo PJE (Processo Judicial Eletrônico) e a instrução processual pelo ciberespaço já admitida por lei processual especial, a livre investigação das provas não é mais uma faculdade potencial, pois é dinamizada sobremaneira com a instantaneidade e a quase gratuidade da informação.

Zamur Filho (2011) entende que a efetividade do Processo Judicial Eletrônico (PJE) como instrumento processual está relacionada ao incremento que possa conferir aos escopos do processo. Tais acréscimos podem se referenciar à eficiência do método (do rendimento e aceleração que proporciona à resolução dos conflitos), e à eficácia da prestação jurisdicional (da garantia de acesso à justiça e ao direito reconhecido em juízo).

No Processo Judicial Eletrônico (PJE) os “autos” não tem representação física que os encerre. Em sentido inverso, já não necessitam de “representação”, pois são formados logicamente no universo digital, consolidados num arquivo acessível pela Internet, ainda que estejam suportados pela mídia conveniente nos equipamentos servidores dos tribunais, que permitem ou não acesso aos conteúdos conforme as regras estabelecidas. Este contrassenso aparente se deve aos paradigmas atuais do direito processual, calcados ainda na materialização dos autos (CHAVES JÚNIOR, 2010).

Desta afirmação decorre um dos princípios do PJE (Processo Judicial Eletrônico). O princípio da imaterialidade, que aproximam o sentido de autos e atos processuais, bem como os de processo e procedimento, pois no PJE o sentido que resta é o de fluxo, de impulso. O PJE é puro movimento que tende a informar e a se comunicar: informa sobre os direitos materiais requeridos e os direitos e deveres processuais a serem observados, e facilita a comunicação das partes pelo contraditório (ZAMUR FILHO, 2011)

São vários os fatores decorrentes do princípio da imaterialidade que levam o PJE a ser mais eficiente como método adequado à pacificação social, mas basta destacar que permite a ampliação do contraditório e que, em si, leva à orientação da atividade jurisdicional: “distribuídos” automaticamente os autos, nos termos do art.

10 da Lei nº 11.419/06, a apreciação da petição inicial é imediata. Aceita sem emendas, procede-se à citação por meios eletrônicos. Se contestada com observação dos comandos legais, estarão configurados os autos virtuais, e daí decorrerão os atos subsequentes de forma proativa (CHAVES JÚNIOR, 2010)

Outros fatores que distinguem a eficiência do PJE também decorrem de princípios que lhe são próprios, Chaves Júnior (2010) destaca alguns:

O princípio da intermidialidade: pelo qual o PJE permite o registro da verdade real em diversas mídias, com destaque para o registro de audiências em vídeo, o que ao mesmo tempo permite melhorar a percepção do juiz sobre a verdade real, além de eficientemente tornar desnecessária a atividade da degravação e transposição escrita das audiências. Por este mesmo princípio, outros modos de realização do processo podem ser registrados, quer seja por videoconferências, interrogatórios e oitiva de testemunhas à distância, acelerando o a prestação jurisdicional sem prejuízo ao devido processo legal

O princípio da hiper-realidade: que radicaliza o princípio da oralidade, ao permitir o registro das audiências de modo instantâneo e com representação quase idêntica à realidade (pois depende ainda de enquadramento, iluminação, qualidade sonora etc. tanto quanto uma obra cinematográfica).

O princípio da interação: que decorre das outras possibilidades do PJE em rede, consubstanciando no meio eletrônico uma oportunidade de participação efetiva, em tempo real, de um contraditório que não será mais linear e formal, pois já não basta garantir a paridade pelo procedimento de se ouvir as partes, a colaboração das partes com o juiz é fundamental na visão mais publicista e social do processo.

O princípio da desterritorialização: que se sintetiza na transcendência da jurisdição, e que permite prover eficácia ao processo de modo nunca experimentado pelo processo-papel, pois este sempre era dependente de um sistema de aplicação local da jurisdição, com a remessa, cumprimento e devolução de cartas precatórias, de ordem ou rogatórias. Com as extensões do PJE pelas facilidades de justiça eletrônica (Bacen Jud, RenaJud e Infojud) já se pode observar a eficácia possível

das decisões judiciais em meios eletrônicos. Basta que as partes estejam previamente cadastradas para que a citação ocorra ainda que ausentes os réus

Existe porém um sério problema a ser resolvido com a implantação do Processo Judicial Eletrônico (PJE), é a de exclusão digital. Zamur Filho (2011) discorre que enquanto as políticas públicas inclusivas não atingirem resultados sólidos, avaliados sobre seus aspectos quantitativos (número de cidadãos com acesso à Internet em banda larga) e qualitativos (capacitação para a operacionalização de transações eletrônicas e de requisição de serviços de governo eletrônico), o Processo Judicial Eletrônico (PJE) pode significar mais uma barreira ao exercício de cidadania, mais uma assimetria de informações a redundar em exclusão social. Compete ao CNJ (Conselho Nacional de Justiça), como órgão central de planejamento judiciário, acompanhar o resultado de tais políticas e definir estratégias próprias para a inclusão digital dos jurisdicionados.

4 A SEGURANÇA DA INFORMAÇÃO NA PRESERVAÇÃO E INTEGRIDADE DOS DOCUMENTOS DIGITAIS

4.1 DOCUMENTO E ASSINATURA ELETRÔNICA

O documento eletrônico é parte fundamental dentro do processo judicial eletrônico. O processo judicial eletrônico inexiste sem ele. Desta forma, torna-se importante esclarecer o conceito de documento eletrônico para evidenciar a sua importância (SILVEIRA, 2015)

Marcacini (1999) explica que o documento eletrônico é uma sequência de *bits* que, interpretada por intermédio de um programa computacional, representa um determinado acontecimento. Os documentos eletrônicos podem conter diferentes

tipos de dados, como vídeos, textos escritos, imagens, sons e tudo aquilo que seja capaz de representar um acontecimento através de uma sequência de *bits*.

O documento eletrônico é a sequência de *bits* e, onde quer que esteja gravado, em qualquer quantidade de cópias, mas desde que seja reproduzida exatamente a mesma sequência, teremos sempre o mesmo documento. Dado o fato de que o documento eletrônico pode ser copiado infinitas vezes, mantendo-se exatamente igual à matriz, é impossível falar-se em original, em cópia, ou em número de vias do documento eletrônico. Toda "cópia" do documento eletrônico terá sempre as mesmas características do "original" e, por isso, deve ser assim considerada. (MARCACINI, 1999).

De acordo com Silveira (2015, p.39):

> Os documentos eletrônicos são capazes de garantir confiabilidade para utilização nos mais altos níveis de significância. As TICs proporcionam mecanismos de segurança informacional suficientes para prover os princípios necessários para integridade, autenticidade, não repúdio, e privacidade.

A Assinatura Eletrônica é a tecnologia responsável por prover segurança aos documentos eletrônicos, assegurando autenticidade e integridade. Essa tecnologia é factível através da utilização de mecanismos criptográficos (SILVEIRA, 2015).

No entender de Nobre (2009) a utilização do Padrão Brasileiro de Assinatura Digital (PBAD), propicia aos processos eletrônicos que tramitam no judiciário brasileiro, interoperabilidade, que é a capacidade de um sistema (informatizado ou não) de se comunicar de forma transparente (ou o mais próximo disso) com outro sistema (semelhante ou não).

Pereira (2011) explica que a assinatura digital é análoga à manuscrita com a vantagem de que o documento assinado digitalmente pode ser guardado em um meio eletrônico sem a necessidade de impressão, e ainda pode ser transmitido de um computador para outro, via internet. Porém, segundo o mesmo autor, algumas questões devem ser consideradas a respeito do uso de uma assinatura digital em relação à manuscrita, quais sejam:

> Primeiro, a assinatura convencional é uma parte física do documento. Quando uma assinatura é feita em papel, passa a fazer parte desse documento. Não é possível removê-la sem causar danos ao documento. Já

> a assinatura digital não é anexada fisicamente ao documento, existe um algoritmo criptográfico que de alguma forma vincula a assinatura digital ao documento.
>
> Segundo o mesmo autor, a verificação de uma assinatura convencional em um documento é feita por comparação a outras assinaturas autênticas. Esse método não é muito seguro, pois nem todos são peritos grafotécnicos e dispõem de recursos para garantir a semelhança entre as assinaturas.
>
> Também, deve-se considerar a possibilidade de alguém forjar uma assinatura e se passar por outra pessoa. A assinatura digital pode ser verificada utilizando algoritmos públicos de verificação baseados em conceitos matemáticos conhecidos, o que impossibilita a fraude.
>
> Terceiro, a cópia de uma assinatura convencional pode apresentar imperfeições, enquanto a assinatura digital é idêntica ao original.

A assinatura digital é um protocolo criptográfico de autenticação de um documento. Stallings (2007) *apud* Pereira (2011, p.25-26) sugere algumas características importantes no processo de assinatura eletrônica:

- Deve-se verificar o remetente, a data e a hora da assinatura;
- Deve-se autenticar o conteúdo no momento da assinatura;
- Deve ser verificável por terceiros.
- Com base nessas propriedades, Stallings (2007(define os seguintes requisitos para uma assinatura digital:
- Ela precisa ser um padrão de *bits* que dependa da mensagem que será assinada;
- Precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação;
- Deve ser relativamente fácil produzi-la;
- Deve ser computacionalmente inviável falsificá-la, seja construindo uma nova mensagem para uma assinatura digital existente, seja construindo uma assinatura digital fraudulenta para determinada mensagem;
- Deve ser prático armazenar uma cópia da assinatura digital.

Diante dos requisitos citados, se faz necessário a certificação digital, a mesma garantirá a identificação do proprietário de uma assinatura digital (PEREIRA, 2011).

4. 2 A CRIPTOGRAFIA

Uma das mais frequentes formas de se implementar segurança em um sistema computacional é conhecida como criptografia. Em resumo, a criptografia pode ser entendida como um conjunto de métodos e técnicas para criptografar (cifrar ou codificar) informações legíveis por meio de um algoritmo de criptografia parametrizado por uma chave, convertendo um texto original, denominado texto aberto (texto claro ou texto simples), em um texto ilegível, denominado texto cifrado (cifra ou texto código). Posteriormente, é possível para o receptor decriptar este texto cifrado, ou seja, efetuar o processo reverso e recuperar as informações originais (Moreno et al., 2005).

Conforme Nakamura e Geus (2003), a criptografia é uma ciência que tem importância fundamental para a segurança da informação, ao servir de base para diversas tecnologias e protocolos. A criptografia possibilita a integridade, a autenticidade, o não-repúdio e o sigilo da informação.

Diversos fatores devem ser analisados para a proteção adequada da informação. Entre os principais estão: geração das chaves, mecanismos de troca das chaves, taxa de troca das chaves, tamanho das chaves, qualidade do algoritmo e sua correta implementação (BERNSTEIN, 1997).

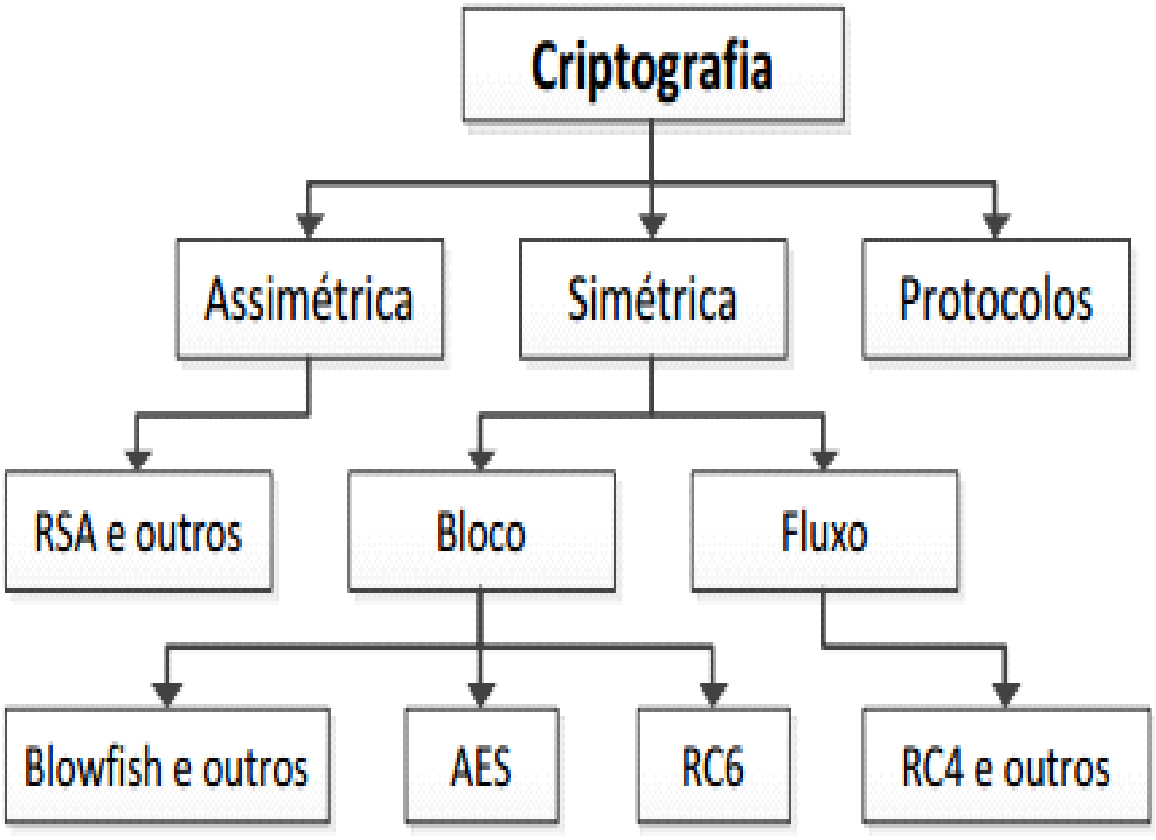
De acordo Dumont (2006, p. 43):

> Um algoritmo criptográfico é considerado eficiente se não existirem facilidades que permitam que se recuperem as informações sem a utilização de ataques de força bruta e se o número de chaves possíveis for suficientemente grande para fazer com que os ataques de força bruta se tornem impraticáveis. Com o aumento exponencial da capacidade de processamento e o avanço da computação distribuída, é essencial considerar o tempo durante o qual a informação deverá ficar protegida, para que seja utilizado o tamanho ideal de chave.

Jang (2003), é possível ativar a criptografia em diferentes níveis de segurança, como, em senhas, serviços e sistemas. Entre os tipos de criptografia para sistemas estão: Senhas MD5, *Shadow Password Suite*, GNU *Privacy Guard*, RSA e DSA.

A criptografia pode ser utilizada para tornar a comunicação em uma rede mais segura, através da criação de túneis criptografados. Vários serviços podem ser tunelados utilizando protocolos seguros, como o SSL ou SSH. Os protocolos seguros possibilitam a encriptação, autenticação e integridade dos dados, possibilitando proteger a informação mesmo quando transferida através de redes públicas inseguras

Figura 1: Classificações da criptografia



Fonte: Pigatto (2012, p. 16)

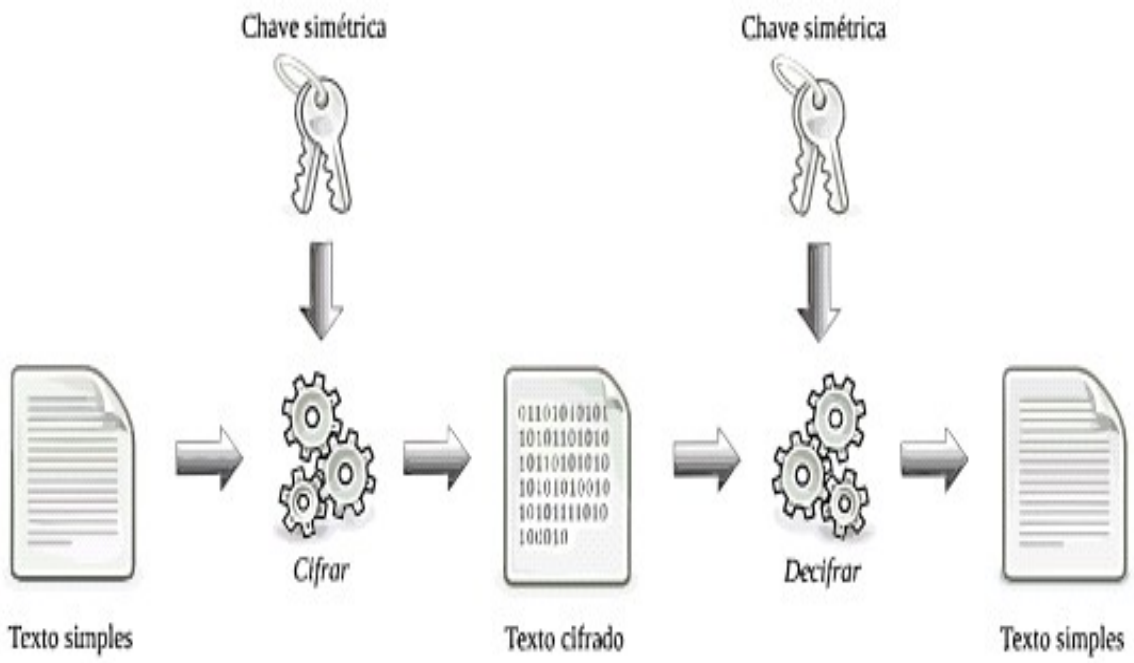
Tanenbaum (2003) explica que novos algoritmos são divulgados à comunidade à medida em que vão sendo desenvolvidos e o sigilo das informações é assegurado pela chave, a qual deve ser mantida em segredo e oferecida apenas às entidades pertinentes. Desta forma, o tamanho da chave é muito importante, já que quanto maior seu comprimento, mais segura torna-se a criptografia.

As criptografias simétrica e assimétrica são largamente utilizadas na construção de sistemas seguros.

- Criptografia Simétrica

A criptografia de chave simétrica (ou criptografia de chave privada) possui este nome porque os processos de criptografia e decriptografia são realizados com uma única chave, ou seja, tanto o emissor quanto o receptor detêm a mesma chave e esta deve ser mantida em segredo para que se possa garantir a confidencialidade das mensagens ou da comunicação. A principal vantagem da criptografia de chave simétrica é que os algoritmos deste tipo são rápidos e podem operar em tamanhos arbitrários de mensagens. Em contrapartida, a desvantagem está na dificuldade de gerenciamento da chave compartilhada, a qual deve ser enviada de modo seguro a todos os usuários autorizados antes que as mensagens possam ser trocadas e ainda deve ser mantida em segredo (Moreno et al., 2005).

Figura 2: Processo da criptografia simétrica



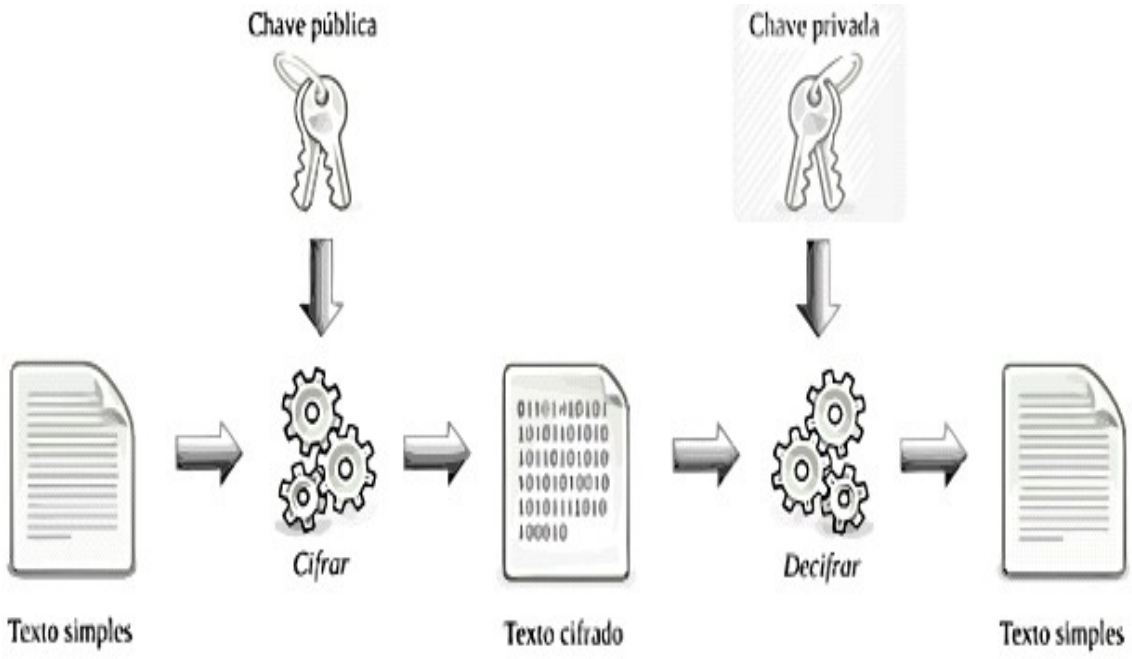
Fonte: Pigatto (2012, p. 17)

- Criptografia Assimétrica

A criptografia assimétrica, mais conhecida como criptografia de chave pública, utiliza um par de chaves denominadas chave privada e chave pública. Qualquer uma

das chaves pode ser utilizada para criptografar os dados, porém a mesma não pode ser utilizada para decriptografá-los, isto é, se a criptografia for realizada com a chave pública, somente a respectiva chave privada poderá realizar a decriptografia, ou vice-versa. Para que este tipo de criptografia obtenha sucesso é fundamental que a chave privada seja mantida em segredo, enquanto a chave pública pode, e deve, ser divulgada a outros usuários que desejam se comunicar (STALLINGS, 2008).

Figura 3: Processo da criptografia assimétrica



Fonte: Pigatto (2012, p. 19)

4.3 INFRAESTRUTURA DE CHAVES PÚBLICAS (ICP)

Através da Medida Provisória 2200-2, de 24 de agosto de 2001, o governo brasileiro instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil (BRASIL, 2001).

A ICP-Brasil é composta por uma cadeia de certificação digital hierárquica, vinculada ao ITI. Essa cadeia possibilita a emissão de certificados digitais e chaves criptográficas (públicas e privadas) para a identificação do cidadão em meio eletrônico. Por meio dessa infraestrutura, os documentos eletrônicos podem ser

assinados digitalmente através do PBAD - Padrão Brasileiro de Assinatura Digital (ITI, 2012).

A Infraestrutura de Chaves Públicas (ICP) é formada por programas, formatos de dados, procedimentos, protocolos de comunicação, políticas de segurança e mecanismos de criptografia de chave pública que trabalham em conjunto para possibilitar que pessoas se comuniquem de forma segura. Em outras palavras, uma ICP é responsável por estabelecer o nível de confiança em um ambiente (HARRIS, 2010).

Conforme Harris (2010) esta infraestrutura assume que a identidade do receptor pode ser assegurada através de certificados digitais e algoritmos assimétricos. O ICP contém as peças necessárias para identificar usuários, criar e distribuir certificados, manter e revogar certificados, distribuir e manter as chaves de criptografia, e todas as tecnologias necessárias para se alcançar o objetivo da comunicação criptografada e autêntica

Os que desejam participar de uma Infraestrutura de Chaves Públicas (ICP) deve requisitar um certificado digital, que nada mais é do que uma credencial que contém a chave criptográfica pública daquele indivíduo, juntamente com outras informações de identificação. O certificado é criado e assinado por uma terceira parte confiável, conhecida como Autoridade Certificadora (AC). Quando a Autoridade Certificadora (AC) assina um certificado, vincula-se a identidade do proprietário a uma chave criptográfica pública, e a AC assume a responsabilidade pela autenticidade do indivíduo. Essa terceira parte confiável (AC) permite a comunicação entre pessoas, em uma rede, de forma segura, para isso, basta que as partes envolvidas na comunicação confiem na mesma AC (SILVEIRA, 2015).

Uma Infraestrutura de Chaves Públicas (ICP) provê suporte a serviços de autenticidade, confidencialidade, não repúdio, e integridade.

4.4 CERTIFICAÇÃO DIGITAL

O certificado digital é um dos pontos mais importantes dentro de uma Infraestrutura de Chaves Públicas (ICP). Ele é o mecanismo usado para associar uma chave criptográfica pública com uma coleção de componentes de maneira suficiente para identificar o proprietário (HARRIS, 2010).

A ICP-Brasil conta atualmente com um conjunto de 10 tipos diferentes de certificados digitais permitidos para usuários finais, sendo 6 aplicados a assinaturas digitais, e 4 para sigilo. Esses certificados apresentam diferenças que produzem distintos níveis de segurança (ITI, 2014).

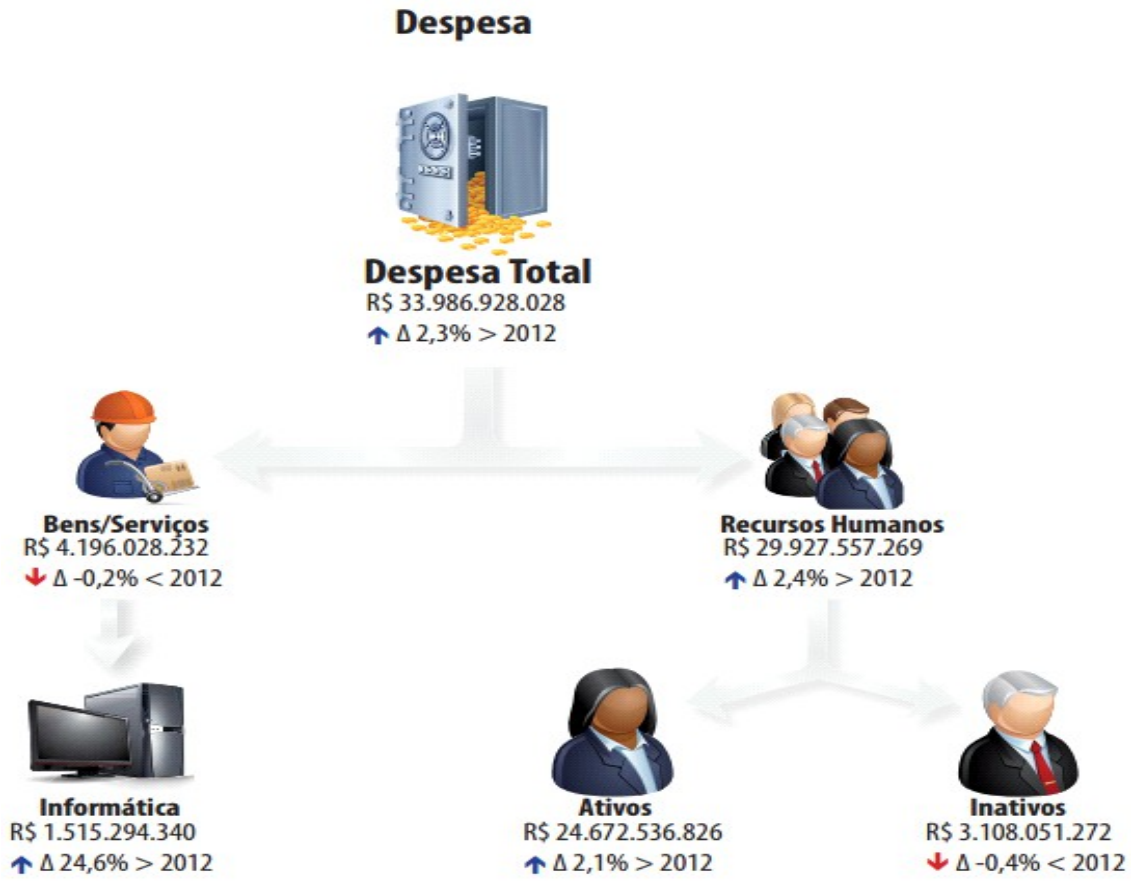
O Certificado Digital (CD) funciona como uma carteira de identidade virtual. ITI (2014) diz que o Certificado Digital (CD) é um documento eletrônico que contém diversos dados sobre o emissor, a Autoridade Certificadora (AC) e o titular do certificado, como: nome do titular, identificação do algoritmo de assinatura, assinatura digital do emissor, validade do certificado e dois números denominados chave pública e privada. A chave privada é que garante o sigilo dos dados do titular que assina a mensagem. A pública permite que ele compartilhe com outras pessoas a informação protegida por criptografia.

Ramiro (2008) pontua que a Certificação Digital permite a assinatura eletrônica, tornando mais segura a prática de atividades online, dentre algumas: uso de Internet banking, compras online e declaração de Imposto de Renda. Nas transações bancárias, o banco terá a certeza de que quem está acessando sua conta corrente é o cliente portador do certificado digital, evitando fraudes. No entanto, ao contrário do RG, a certificação digital tem validade. O prazo de vigência do documento eletrônico varia em função do tipo de certificado.

5 DISCUSSÃO SOBRE SEGURANÇA DA INFORMAÇÃO NA PROTEÇÃO DE DADOS PROCESSUAIS NO PODER JUDICIÁRIO

O Judiciário brasileiro tem investido valores cada vez maiores na área de informática dos tribunais. Existe uma demanda cada vez maior na ampliação, segurança e informatização do processo de gestão da informação do judiciário. O Conselho Nacional de Justiça (CNJ) vem divulgado dados que possibilitam compreender os gastos do judiciário em cada esfera. Um dos últimos relatórios foi divulgado em 2014, referente a gestão judiciária de 2013 e comparados a 2012. Com estes dados podemos compreender melhor os gastos na área de informática, que em resumo seria a área responsável pelo armazenamento, transmissão e processamento de informações. Nas figuras 4 a 8 esses números são apresentados.

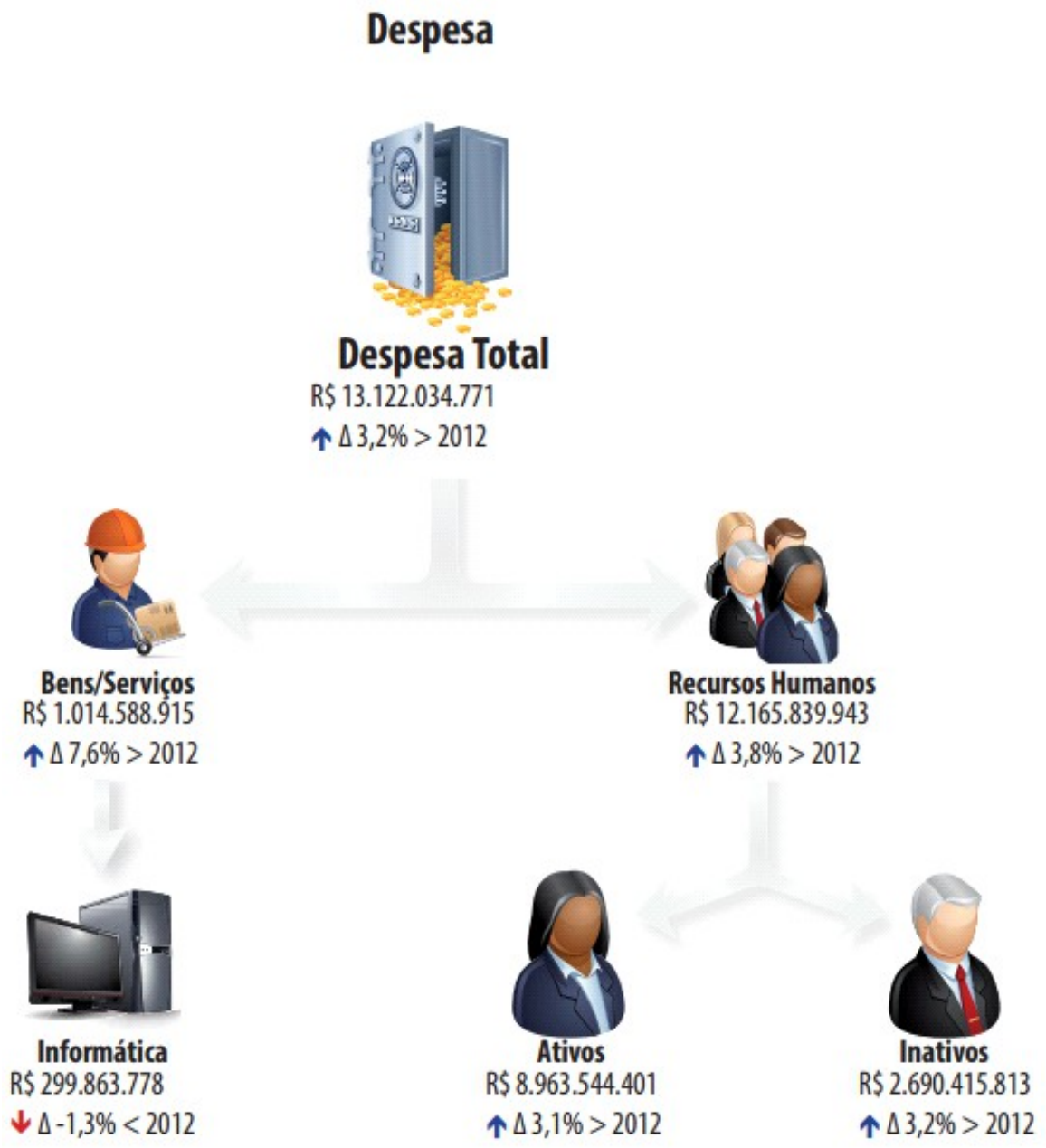
Figura 4: Despesas Justiça Estadual -2013



Fonte: CNJ (2014, p.80)

A Justiça Estadual no ano de 2013 aumentou em 24,6% seus gastos com informática, significou um aumento percentual considerável nesta área.

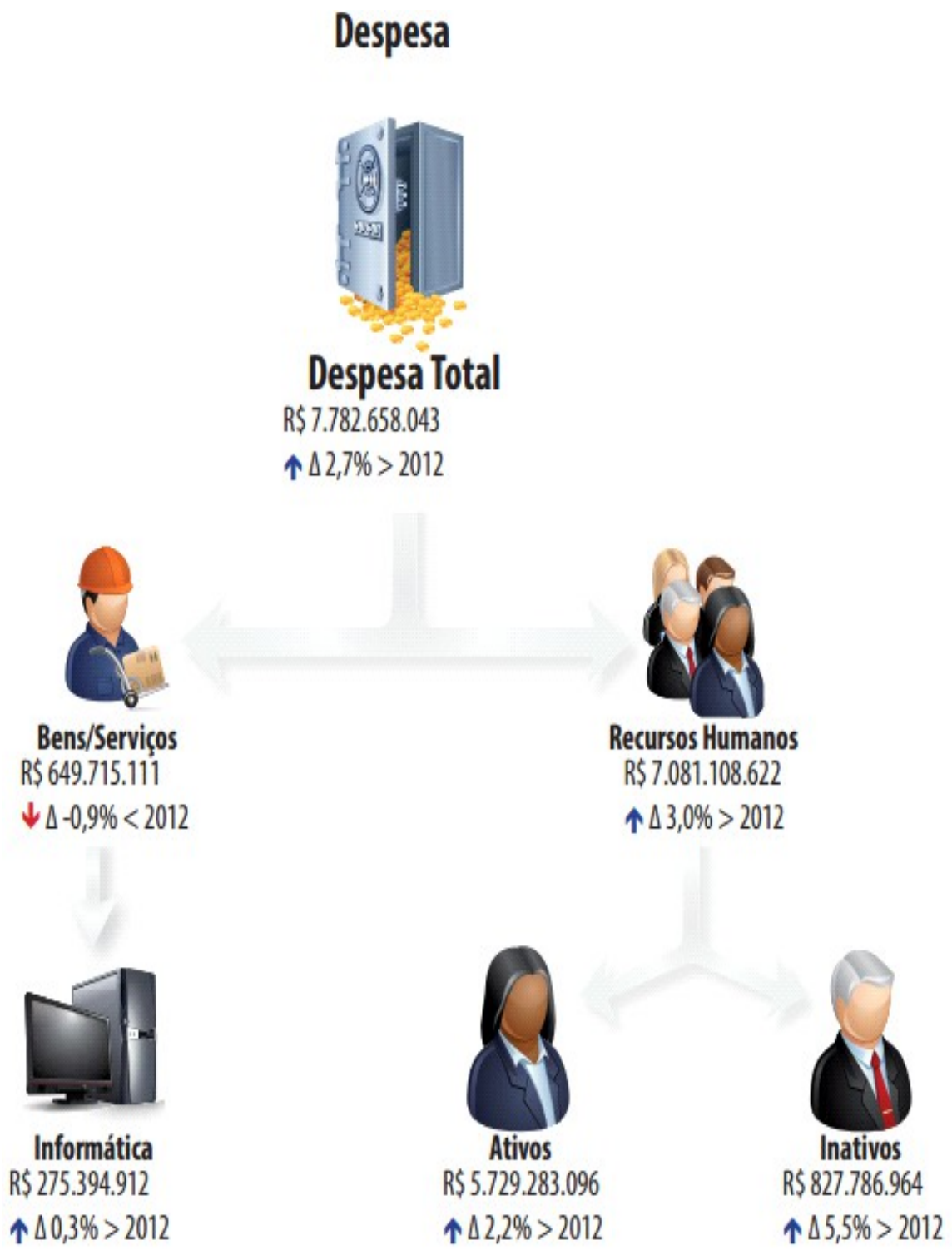
Figura 5: Despesas Justiça do Trabalho-2013



Fonte: CNJ (2014, p. 178)

A Justiça do trabalho em 2013 teve 1,3% a menos de gastos com informática se comparado a 2012. No relatório do Conselho Nacional de Justiça (CNJ) não é informado o motivo.

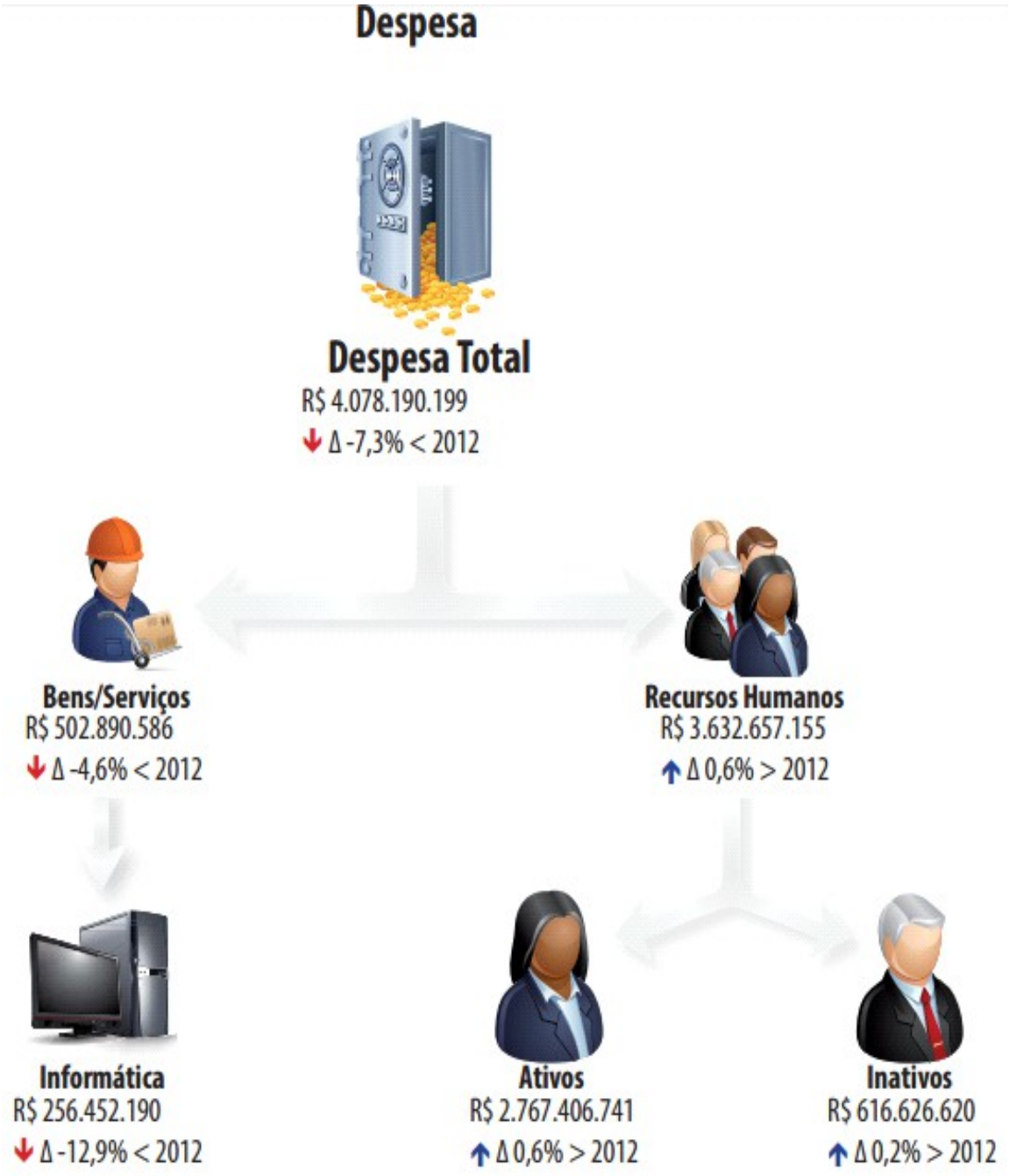
Figura 6: Despesas Justiça Federal-2013



Fonte: CNJ (2014, p. 260)

A Justiça Federal teve pequeno aumento de gastos com informática em 2013 (0,3%) em relação a 2012.

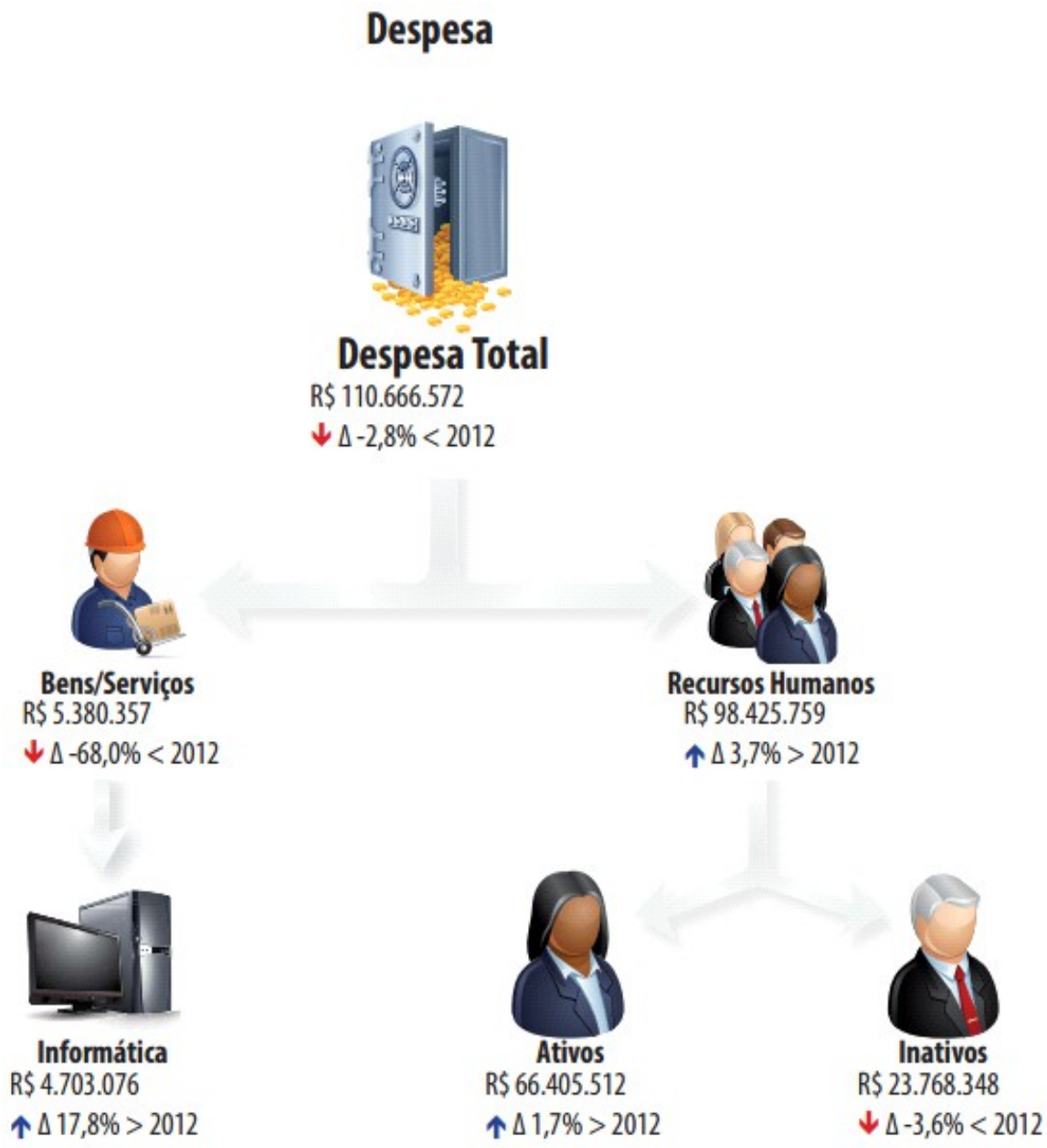
Figura 7: Despesas Justiça Eleitoral - 2013



Fonte: CNJ (2014, p.292)

A Justiça Eleitoral teve uma queda de gastos considerável na área de informática (12,9%) em 2013. A explicação mais plausível é que em 2012 houve eleições municipais, período em que naturalmente os gastos da Justiça Eleitoral nessa área tende a aumentar consideravelmente.

Figura 8: Despesas Justiça Militar Estadual -2013



Fonte: CNJ (2014, p. 362)

A Justiça Militar Estadual, apesar de ter diminuído o total de suas despesas em 2013, em relação a 2012, não o fez com a área de informática que teve um aumento de gastos de 17,8%.

O que se pode concluir com as figuras expostas, é que a informática vem sendo tratada como uma área essencial dentre as despesas do judiciário, sendo

destacada em separado. A maioria das instâncias apresentadas tiveram um aumento nos gastos com informática no ano de 2013. A análise geral é que independente do gasto ser maior ou menor, tem-se investido muito na informatização e no aperfeiçoamento dos processos virtuais nos últimos anos.

Atualmente a questão da segurança é algo tão imprescindível que não se pode sequer pensar em desconsiderá-la, principalmente em um judiciário onde a demanda aumenta a cada dia.

Com o judiciário precisando se adequar à nova realidade, necessita de um sistema de informação ágil, mas ao mesmo tempo seguro, principalmente fazendo com que os arquivos processuais e as informações neles contidas sejam as mais fiéis possíveis.

Nesse sentido, a Segurança da Informação se torna fundamental, pois está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização, além da proteção dos sistemas em si.

CONCLUSÃO

O Direito, ciência que estuda as relações sociais, a elas intervindo por meio das normas jurídicas, sofreu mudanças por conta de uma das grandes revoluções pelas quais passou a sociedade: a revolução da informática. Por outro lado, o poder judiciário, função estatal que detém o poder e dever de exercer a jurisdição precisa há algum tempo de cuidados efetivos na gestão desse poder. Esses cuidados são defendidos como ações que viabilizem o acesso à justiça.

O Processo Judicial Eletrônico é uma realidade irreversível no cenário jurídico brasileiro. Essa nova modalidade está possibilitando o descongestionamento do Poder Judiciário e permitindo uma revisão do modelo de processo tradicional, já obsoleto.

O novo modelo de processo desempenhará papel-chave na sociedade, com o encurtamento da distância e diminuição do tempo entre as etapas do processo e a eliminação da possibilidade de extravio ou falta de pessoal para fazer as juntadas de documentos nos autos.

Nesse sentido, pode-se verificar que a Lei n.º 11.419/2006 veio para suprir e eliminar a deficiência processual brasileira, tendo em vista a aptidão das vias eletrônicas para a tramitação de documentos jurídicos e observando determinados critérios.

Contudo, alguns problemas ainda existem e merecem atenção, como a indefinição de padrões para o envio de arquivos para o processo eletrônico, tendo cada tribunal as suas particularidades em relação às ferramentas usadas na tramitação dos documentos.

A tecnologia definitivamente chegou ao direito. Um dos seus benefícios foi a possibilidade de criação de meios eficientes e eficazes na busca da justiça.

A Lei 11.419/06 trata de uma norma permissiva, restando aos órgãos judiciais regulamentarem o seu uso, o que já vem sendo feito em larga escala, na medida dos recursos disponíveis. É preciso vontade de mudar conceitos, paradigmas, quebrar resistências ao novo.

Nesse cenário apresentado, a Segurança da Informação entra como um importante ator, capaz de garantir ao judiciário um sistema informatizado capaz de atender as novas demandas de forma segura e ágil.

Sem a Segurança da Informação os dados judiciais em rede poderiam sofrer ataques virtuais que prejudicariam a fidelidade das informações, prejudicando os cidadãos e criando dúvidas quanto à credibilidade da justiça. Cabe a Segurança da Informação garantir proteção aos sistemas disponíveis, possibilitando eficiência e agilidade ao judiciário nas demandas virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Associação Brasileira de Normas Técnicas ABNT**: Norma NBR 27002:2013**. Disponível em: <http://pt.slideshare.net/FabioMartins12/iso-270022013?related=1> Acesso em: 24 fev. 2016.

ABRÃO, Carlos Henrique. Processo eletrônico: Lei 11.419 de 19 de dezembro de 2006. 2ª ed. rev. atual. Ampl. São Paulo: **Revista dos Tribunais**, 2009.

ALMEIDA FILHO, José Carlos de Araújo. **Processo eletrônico e teoria geral do processo eletrônico: a informatização judicial no Brasil**. 3.ed.Rio de Janeiro: Forense, 2010.

ALVARES, Nathalia Oliveira. **A informatização do processo judicial e o acesso à justiça**. Brasília: Uniceub, 2011.

ANDRADE, André. **Porque a Justiça não se comunica? Um problema de estrutura organizacional.** 2011. Disponível em: < http://www.egov.ufsc.br/portal/conteudo/porque-justi%C3%A7a-n%C3%A3o-se-comunica-um-problema-de-estrutura-organizacional> Acesso em: 14 fev. 2016.

ATHENIENSE, A. **Comentários à Lei 11.419/06 e as práticas processuais por meio eletrônico nos tribunais brasileiros**. Curitiba: Juruá, 2010.

BERNSTEIN, Terry. **Segurança na internet**. Rio de Janeiro: Campus, 1997. BRASIL. **Lei 11.419 de 19 de dezembro de 2006**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm> Acesso em 14 fev. 2016.

_____. Presidência da República. **Medida Provisória nº 2.200-2**. Brasília, 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 25 fev. 2016.

_____. **Decreto n.º 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 24 fev. 2016.

_____. **Instrução Normativa Nº 1 de 13.06.2008**. Gabinete de Segurança Institucional da Presidência da República, Brasília, 2008. Disponível em:

<http://www.mct.gov.br/index.php/content/view/72703.html>. Acesso em: 24 fev. 2016.

CARVALHO, Juan Pablo Couto de. A era virtual no processo judicial: a experiência dos juizados especiais virtuais e o projeto de lei de informatização do processo. **Revista Direito e Liberdade** – Mossoró – v. 3, n. 2, p. 453 – 484 – set, 2006

CHAVES JÚNIOR, José Eduardo Resende (coord.). **Comentários à lei do processo eletrônico**. São Paulo: LTr, 2010.

CINTRA, Erickson Brener de Carvalho**. A informatização do processo judicial e seus reflexos no Superior Tribunal de Justiça**. Brasília: UnB, 2009.

CNJ. Conselho Nacional de Justiça. **Entenda o PJe**. Brasília, 2013b. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicialeletronico-pje>. Acesso em: 25 fev. 2016.

_____.. **Justiça em números 2014: ano-base 2013**. Brasília: CNJ, 2014. Disponível em: <ftp://ftp.cnj.jus.br/Justica_em_Numeros/relatorio_jn2014.pdf> Acesso em: 05 mar. 2016.

DUMONT, Carlos Eduardo Silva. **Segurança computacional: segurança em servidores linux em camadas.** Especialização em Administração de Redes Linux. Lavras: UFLA, 2006.

FONTES, Nicolau Otto dos Anjos. Uma análise histórico-jurídica da virtualização do processo judicial. **Revista *Juris Rationis***, ano 6, n. 1 - out. 2012/mar. 2013. Natal, 2013. Disponível em:<https://repositorio.unp.br/index.php/juris/article/view/298/243> Acesso em: 13 fev. 2016.

GIL, Antonio Carlos **Métodos e técnicas de pesquisa social.** 6ª ed. São Paulo: Atlas, 2008.

HARRIS, Shon. **Cissp all-in-one exam guide**. 5. Ed: McGraw-Hill, 2010.

ITI. **Visão geral sobre assinaturas digitais na ICP-Brasil**. Brasília, 2012. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOCICP-15_-_Versao_2.1_VISAO_GERAL_SOBRE_ASSIN_DIG_NA_ICPBRASIL_13-08-2012.pdf> Acesso em: 03 mar. 2016.

JANG, Michael. **Dominando *red hat linux* 9**. Rio de Janeiro: Ciência Moderna, 2003.

LACERDA, Eduardo Azambuja. **Processo eletrônico: alterações na legislação e relação com o justo processo legal**. Porto Alegre: UFRGS, 2014.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**.5ª. ed. São Paulo: Atlas 2003.

LAUREANO, M. A. P. **Gestão de segurança da informação**. Disponível em: <http://www.laureano.eti.br/ensino/puc/gst/gestao_da_seguranca_da_informacaov20.pdf#search=%22laureano%20A%20pr%C3%B3xima%20figura%20demonstra%2C% 20do%20ponto%20de%20vista%20estrat%C3%A9gico%2C%22>. Acesso em: 25 fev. 2016.

LOUREIRO, Silvana Crispim. **Segurança da informação preservação das informações estratégicas com foco em sua segurança.** Brasília: UNB, 2008.

MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. São Paulo, 1999. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/13948-13949-1-PB.htm#21>. Acesso em: 24 fev. 2016.

MIRANDA, S.V; STREIT, R.E. **O processo de gestão da informação em organizações públicas**. ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, 2007. Florianópolis: ANPAD, 2007.

MORENO, E. D; CHIARAMONTE, F. D; PEREIRA, R. B. **Criptografia em *software* e *hardware*.** São Paulo: Novatec, 2005.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes: em ambientes cooperativos**. 2. ed. São Paulo: Futura, 2003

NOBRE, Anna Cláudia dos Santos. **Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação: um estudo com gestores públicos estaduais no Brasil.** Dissertação (Mestrado em Administração). Natal: UFRN, 2009.

PEREIRA, Winicius. **Protocolo para emissão de assinatura digital utilizando compartilhamento de segredo.** Dissertação (Mestrado) -Uberlândia: Universidade Federal de Uberlândia, 2011.

PEREZ, Ana Carolina Fonseca Martinez; CORONA, Roberto Brocanelli. O processo eletrônico como efetivação do direito fundamental de acesso à justiça. **Revista Estudos Jurídicos**. UNESP, Franca, A. 14 n.19, p. 01-404, 2010. Disponível em:<http://seer.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/233/282 > Acesso em: 13 fev. 2016.

PIGATTO, Daniel Fernando. **Segurança em sistemas embarcados críticos - utilização de criptografia para comunicação segura**. São Carlos: USP, 2012.

PLANO EDITORIAL. **Anuário da Revista TI & Governo 2005**. Porto Alegre: Plano Editorial, 2005.

RAMIRO, Marcelo Lepsch. **Gestão da segurança da informação: certificação digital**. Dissertação (Mestrado). Rio de Janeiro: FGV, 2008.

SANTOS, Leilson Mascarenhas. **O processo eletrônico e o acesso à justiça**. Palmas: ULBRA, 2010.

SILVEIRA, Lucas. **Modelo nacional de interoperabilidade do poder judiciário: aperfeiçoamento quanto à segurança e interoperabilidade dos dados**. Dissertação (Mestrado). Florianópolis: UFSC, 2015.

STALLINGS, W. **Criptografia e segurança de redes**. 4º ed. São Paulo: Person, 2007.

_____. **Criptografia e segurança de redes: princípios e práticas**. PRENTICE HALL BRASIL, 2008.

TANENBAUM, A. S. **Redes de computadores**. Rio de Janeiro: Campus, 2003.

ZAMUR FILHO, Jamil Zamur. **Processo judicial eletrônico: alcance e efetividade sob a égide da Lei nº 11.419, de 19.12.2006**. São Paulo: USP, 2011.