Lucas Silveira

MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO: APERFEIÇOAMENTO QUANTO À SEGURANÇA E INTEROPERABILIDADE DOS DADOS

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do Grau de mestre em Ciência da Computação.
Orientador: Prof. Dr. Raul Sidnei Wazlawick
Coorientador: Prof. Dr. Aires José Rover

Florianópolis (SC)
2015

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Silveira, Lucas
MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO : APERFEIÇOAMENTO QUANTO À SEGURANÇA E INTEROPERABILIDADE DOS DADOS / Lucas Silveira ; orientador, Raul Sidnei Wazlawick ; coorientador, Aires José Rover. - Florianópolis, SC, 2015.
92 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Modelo Nacional de Interoperabilidade do Judiciário. 3. Padrão Brasileiro de Assinatura Digital. 4. Interoperabilidade de Dados. 5. Segurança da Informação. I. Wazlawick, Raul Sidnei . II. Rover, Aires José. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. IV. Titulo.

Lucas Silveira

MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO: APERFEIÇOAMENTO QUANTO À SEGURANÇA E INTEROPERABILIDADE DOS DADOS

Esta Dissertação foi julgada adequada para obtenção do Título de "Mestre", e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina.

Florianópolis, 4 de março de 2015.

_____
Prof. Ronaldo dos Santos Mello, Dr.
Coordenador do Curso

_____
Prof. Raul Sidnei Wazlawick, Dr.
Orientador
Universidade Federal de Santa Catarina

_____
Prof. Aires José Rover, Dr.
Coorientador
Universidade Federal de Santa Catarina

Banca Examinadora:

_____
Prof. Denilson Sell, Dr.
Universidade do Estado de Santa Catarina

_____
Prof. Orides Mezzaroba, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Carlos Becker Westphall, Dr.
Universidade Federal de Santa Catarina

Este trabalho é dedicado aos meus pais, que me deram toda educação, amor, e incentivo, não medindo esforços para tornar possível a concretização deste momento.

AGRADECIMENTOS

Agradeço primeiramente a minha família. A meu pai, Osnildo Osmar Silveira, minha mãe, Maria Aparecida Bessa Silveira, minha irmã, Tamara Silveira, e minha vó, Mercedes E. Bessa. Sem vocês, a realização deste trabalho não seria possível. Obrigado pelos incentivos, carinhos e pelas batalhas realizadas para a construção deste trabalho.

Agradeço aos meus parceiros de pesquisa do Grupo de Governo Eletrônico da Universidade Federal de Santa Catarina, que trabalham unidos em busca dos melhores resultados para o desenvolvimento da pesquisa científica no Brasil e no mundo.

Obrigado aos meus orientadores, prof. Raul Wazlawick, e prof. Aires José Rover, e todos aqueles que participaram efetivamente para a conclusão de mais esta etapa.

Gostaria de agradecer à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), o apoio concedido através do Projeto "CNJ Acadêmico", Edital n. 020/201/CAPES/CNJ, Área Temática 5, que proporcionou o pagamento da minha bolsa de mestrado, auxiliando de forma direta na realização deste trabalho.

Acredite que você pode, assim você já está no meio do caminho.

(Theodore Roosevelt)

RESUMO

Esta dissertação de mestrado apresenta como resultado uma análise crítica para o aperfeiçoamento quanto à segurança e a interoperabilidade dos dados do Modelo Nacional de Interoperabilidade do Poder Judiciário Brasileiro (MNI) (CNJ, 2013). Uma breve apresentação da estrutura judiciária brasileira é realizada, expondo a importância da interoperabilidade nesse contexto. Outros modelos de interoperabilidade de dados em utilização no Brasil e no mundo, como o e-PING e o e-CODEX, são sucintamente exibidos. Os resultados apresentados neste trabalho são baseados no Padrão Brasileiro de Assinatura Digital (ITI, 2012), no *framework* de Ray (2011), e no *European Interoperability Framework* (EIF) (ISA, 2010). Através do *framework* de Ray, identificam-se problemas no MNI como: a falta de definição de políticas básicas, de gerenciamento e de conformidade, ausência de um ciclo de vida para gestão do modelo, entre outros. O PBAD é apresentado e utilizado como meio de agregar mais segurança ao MNI, sendo indicado neste trabalho como ferramenta obrigatória para controle de acesso do MNI e dos documentos eletrônicos, para prover interoperabilidade, não-repúdio, unicidade, temporalidade, integridade e autenticidade aos dados. Além disto, o trabalho determina o nível de interoperabilidade que o MNI atinge, conforme a categorização de interoperabilidade definida pelo *European Interoperability Framework* (EIF) (ISA, 2010). Soluções para que níveis mais altos de interoperabilidade possam ser atingidos são apresentadas, além da identificação de problemas em níveis mais básicos, como falta de definição de protocolos de comunicação para o nível de interoperabilidade técnica.

Palavras-chave: Interoperabilidade. MNI. Judiciário. PBAD.

ABSTRACT

This dissertation presents as a result an assessment on the improvement of security and interoperability for the Brazilian e-Justice Interoperability Model (MNI) (CNJ, 2013). A brief presentation of the judicial structure in Brazil is presented with a focus on highlighting the importance of interoperability in this context. Additionally, other data interoperability models that are used in Brazil and around the world, such as e-PING and e-CODEX, are introduced in this text. The results are based on the Digital Signature Brazilian Standard (ITI, 2012), considering Ray's framework (2011), and the European Interoperability Framework (EIF) (ISA, 2010). Through Ray's framework, it was observed a lack of basic, management, and compliance policies in the MNI, as well as a lack of a life cycle model, among other improvement opportunities. The PBAD is presented and used as a way to add more security to the MNI and it is indicated in this paper as a mandatory tool for MNI access control and to provide interoperability, non-repudiation, uniqueness, timeliness, integrity, and authenticity to the electronic documents. In addition, this paper determines the level of interoperability that the MNI reaches, through the EIF interoperability categorization. It also presents solutions to achieve higher interoperability levels, and it identifies problems in the lower levels, such as a lack of communication protocols for the level of technical interoperability.

Keywords: Interoperability. Brazilian e-Justice Interoperability Model. Judiciary. Digital Signature Brazilian Standard.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

PBAD – Padrão Brasileiro de Assinatura Digital
EIF – *European Interoperability Framework*
ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira
MNI – Modelo Nacional de Interoperabilidade do Judiciário
SGPJE – Sistemas de Gestão de Processos Judiciais Eletrônicos
CNJ – Conselho Nacional de Justiça
CNMP – Conselho Nacional do Ministério Público
MNI – Modelo Nacional de Interoperabilidade do Judiciário
TIC – Tecnologia de Informação e Comunicação
E-Gov – Governo Eletrônico
E-*Justice* – Justiça Electrônica
STF – Supremo Tribunal Federal
XML – *eXtensible Markup Language*
E-Ping – Arquitetura de Padrões de Interoperabilidade de Governo Eletrônico do Brasil
e-PMG – Padrão de Metadados de Governo Eletrônico do Brasil
ITI – Instituto Nacional de Tecnologia da Informação
AC – Autoridade Certificadora
LCR – Lista de Certificados Revogados
OCSP – *Online Certificate Status Protocol*
CAdES – *CMS Advanced Electronic Signatures*
XAdES – *XML-DSig Advanced Electronic Signatures*
ASN.1 – *Abstract Syntax Notation One*
PA – Política de Assinatura
AD-RB – Assinatura Digital com Referência Básica
AD-RT – Assinatura Digital com Referência do Tempo
AD-RC – Assinatura Digital com Referências Completa
AD-RV – Assinatura Digital com Referências para Validação
AD-RA – Assinatura Digital com Referências para Arquivamento
LPA – Lista de Políticas Aprovadas
NSA – Agência Nacional de Segurança Americana

1. INTRODUÇÃO

A implantação da Lei nº 11.419, de dezembro de 2006, que dispõe sobre a informatização do processo judicial eletrônico no Brasil (BRASIL, 2006), e a Medida Provisória 2.200-2, que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (BRASIL, 2001), garantem validade jurídica, autenticidade, e integridade, aos processos judiciais eletrônicos que tramitam no Poder Judiciário deste país.

A estrutura judiciária brasileira é composta por um conjunto de 91 tribunais e demais órgãos de administração da justiça. Grande parte destes tribunais utilizam Sistemas de Gestão de Processos Judiciais Eletrônicos (SGPJE). Esses sistemas são utilizados para prover celeridade e dinamismo aos processos eletrônicos do judiciário. A utilização desses sistemas fornece uma velocidade bastante superior ao processo em papel, além de agregar outros benefícios para a sociedade como a preservação ambiental (CONCEIÇÃO, 2011).

Um processo judicial eletrônico pode tramitar por diferentes tribunais e instâncias, sendo que, qualquer tribunal e toda instância, tem autonomia para escolher o sistema de gestão que lhe convém. Dessa forma, diversos e diferentes sistemas são utilizados dentro da justiça brasileira. Observando pela ótica da tecnologia da informação, esse fato agrega segurança para o poder judiciário, pois a variedade de sistemas dificulta a busca de agentes maliciosos por falhas, diminuindo o risco de um possível comprometimento desses sistemas. A utilização de um sistema único poderia ser potencialmente prejudicial para a segurança das informações judiciárias.

Devido ao fato dos processos judiciais serem manuseados por diferentes partes (pessoas e órgãos integrantes no processo), e por tramitarem em diferentes tribunais e instâncias, seria ideal que esses processos pudessem ser acessados e modificados independentemente de sistema. Para que isso ocorra, é necessário que os diversos sistemas eletrônicos de gestão se comuniquem, permitindo troca de informação entre eles. Essa comunicação entre sistemas heterogêneos chama-se interoperabilidade (IEEE, 1991). Desta maneira, o processo tornar-se-ia interoperável, podendo estar disponível eletronicamente para acesso independente do SGPJE utilizado, não precisando ser acessado pelo mesmo SGPJE em que foi criado.

Em geral, nos SGPJE da justiça brasileira, a interoperabilidade ainda não é considerada e planejada. Os sistemas não trocam

informações, portanto, não são capazes de criar processos interoperáveis. Este fato afeta o bom funcionamento do sistema como um todo. No decorrer do trabalho, problemas gerados pela falta de interoperabilidade são apresentados.

Com o propósito de resolver esta questão, o Conselho Nacional de Justiça Brasileiro (CNJ), em parceria com o Conselho Nacional do Ministério Público (CNMP), instituiu o Modelo Nacional de Interoperabilidade do Judiciário (MNI). Por meio da Resolução Conjunta Nº 3, estes órgãos determinaram um prazo máximo, que se encerra em abril de 2015, para que todos os tribunais de justiça do país utilizem ao menos um sistema que implemente o MNI (CNJ, 2013). Essa decisão comprova a preocupação com a interoperabilidade nos sistemas de gestão da justiça.

Nesse sentido, na busca do aperfeiçoamento deste modelo, este trabalho apresenta uma análise cientifica, até o momento inexistente, sobre o MNI, levando em consideração a segurança e a interoperabilidade dos dados tramitados por meio do MNI. Outros aspectos, que não sejam relacionados à segurança da informação e interoperabilidade dos dados, estão fora do escopo deste trabalho. A análise apresentada é baseada no Padrão Brasileiro de Assinatura Digital (PBAD) (ITI, 2012), no *framework* de Ray (2011), no *European Interoperability Framework* (EIF) (ISA, 2010), e nas implicações técnicas advindas da implantação de um sistema de gestão único para tramitação dos processos judiciais eletrônicos (CONJUR, 2013).

Os resultados deste trabalho visam produzir recomendações para o aprimoramento do MNI, para que este modelo possa proporcionar interoperabilidade real e segura entre os tribunais e os demais órgãos de gestão da justiça, desobstruindo e produzindo maior celeridade na tramitação dos processos judiciais.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O objetivo deste trabalho é realizar uma análise crítica sobre o MNI, sob a ótica da segurança da informação e da interoperabilidade de dados, a fim de identificar problemas existentes e oportunidades de melhorias.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Compreender e apresentar a importância da interoperabilidade no cenário da justiça eletrônica brasileira;
- Buscar e identificar problemas/falhas no MNI em todos os níveis de interoperabilidade categorizados pelo EIF;
- Categorizar o MNI dentro de um dos níveis de interoperabilidade definidos pelo EIF;
- Avaliar a importância do PBAD para a segurança e interoperabilidade do MNI;
- Analisar sob a ótica da segurança da informação e da interoperabilidade de dados a iniciativa do CNJ de implantar um SGPJE único na justiça brasileira;
- Utilizar o framework de Ray para realizar uma análise qualitativa sobre o contexto, o conteúdo, e o processo do MNI;
- Apresentar recomendações de melhorias para solucionar os problemas encontrados;
- Apresentar recomendações para ampliar o nível de interoperabilidade do MNI caso seja possível;

1.2 JUSTIFICATIVA

A partir de abril de 2015, todos os tribunais e demais órgãos da justiça devem ter, pelo menos, um sistema em execução no qual o MNI esteja implantado (CNJ 2013c). Para minimizar futuros problemas com a implementação deste modelo, é necessário uma análise científica que identifique possíveis problemas e apresente melhorias para um uso mais eficaz do MNI, contribuindo para o avanço tecnológico do processo judicial eletrônico como um todo, beneficiando a sociedade e o judiciário.

A justiça eletrônica brasileira carece de trabalhos científicos que tenham como objetivo aprimorar o MNI e qualquer outra iniciativa de prover interoperabilidade na tramitação dos processos judiciais eletrônicos. Este fato gera custos, em tempo e financeiros, para o governo. A inexistência de interoperabilidade entre os SGPJE promove falta de coordenação entre tribunais e demais órgãos de administração da justiça, gerando altos custos operacionais e de manutenção em sistemas heterogêneos, redundância e inconsistência de dados.

A pesquisa realizada sobre o Modelo Nacional de Interoperabilidade do Judiciário (MNI), que resulta nesta dissertação de mestrado e em outros três artigos científicos, é relevante para prover cooperação, intercambio, compartilhamento, e reuso das informações entre os órgãos de justiça. As recomendações aqui expostas servem para benefício dos cidadãos e empresas deste país, visto que buscam o aumento da eficiência dos processos jurisdicionais, assim como a diminuição da burocracia existente. Isto propicia uma maior eficácia na prestação dos serviços públicos e na redução de custos para o estado, os cidadãos, e as organizações, proporcionando maior acesso à informação, desobstrução da justiça, e celeridade no trâmite dos processos judiciais.

Nenhum outro trabalho científico, que tratasse o MNI, foi encontrado. Este trabalho é desbravador neste sentido, buscando uma melhora tecnológica para este modelo, baseada em padrões que podem prover maior interoperabilidade e segurança ao processo, como é o caso do Padrão Brasileiro de Assinatura Digital (PBAD).

Assim sendo, a justificativa para criação deste trabalho é o aprimoramento do Poder Judiciário, através da utilização das tecnologias de informação e comunicação (TICs), na busca da identificação de falhas que podem comprometer a interoperabilidade proporcionada pelo MNI, e prover maior confiabilidade a este modelo por meio do PBAD. As sugestões de melhorias destacadas neste trabalho são significativas para o aperfeiçoamento do modelo, acarretando na qualidade dos serviços oferecidos pela justiça a todas as partes envolvidas neste cenário.

1.3 PROCEDIMENTOS METODOLÓGICOS

O método de pesquisa utilizado neste trabalho é o dedutivo, ou seja, do geral para o particular. As pesquisas são baseadas nas características gerais do MNI e de outros modelos de interoperabilidade pelo mundo, para identificar características específicas que possam ser exploradas, e/ou modificadas, para que promovam interoperabilidade entre os sistemas.

Os procedimentos adotados são: a) revisão bibliográfica, em periódicos científicos e bases de dados, buscando autores renomados na área de governo eletrônico, processo judicial eletrônico, informatização do judiciário; b) pesquisa documental, investigando normas e padrões reconhecidos na área de interoperabilidade, governo eletrônico, e poder judiciário; c) análise documental de sistemas de gestão de processos

eletrônicos judiciais e ferramentas de análise de interoperabilidade a fim de identificar aspectos relevantes para prover interoperabilidade.

As análises apresentadas são compostas por quatro módulos: o *European Interoperability Framework* (EIF) (ISA, 2010), utilizado como base para identificar o nível de interoperabilidade que o MNI atinge; o *framework* de Ray (2011), que é dividido em oito camadas que identificam as características necessárias para a criação de um modelo de interoperabilidade em governo eletrônico de qualidade; o PBAD, que permite prover uma análise sobre aspectos de segurança viabilizados pelo MNI; e uma análise sobre a iniciativa do CNJ em implementar um SGPJE único em todo o sistema judiciário Brasileiro. As análises são realizadas de forma qualitativa.

1.4 ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado em cinco seções temáticas. A estruturação e divisão dessas seções são classificadas e expostas da seguinte forma:

Poder Judiciário e Processo Judicial eletrônico: Uma visão geral sobre a estrutura judiciária brasileira, apresentando o funcionamento e os principais componentes do Poder Judiciário. O conceito de governo eletrônico é apresentado, assim como o processo judicial eletrônico e seus principais artefatos.

Interoperabilidade: Uma revisão bibliográfica é apresentada sobre a interoperabilidade, expondo o conceito e os níveis de interoperabilidade existentes. Tecnologias para prover interoperabilidade e guarnecer os níveis existentes também são apresentadas.

Modelo Nacional de Interoperabilidade: O MNI é apresentado, mostrando seus principais elementos de comunicação, e requisitos de segurança. Outros modelos de interoperabilidade em governo eletrônico e justiça eletrônica, do Brasil e do mundo, são apresentados.

Padrão Brasileiro de Assinatura Digital: Aqui são expostos mecanismos de segurança envolvidos no processo de assinatura digital, bem como o PBAD e seus principais atores.

Avalição e Resultados: Por fim, esta seção é responsável por apresentar as análises realizadas e as recomendações de melhorias.

2. PODER JUDICIÁRIO E PROCESSO JUDICIAL ELETRÔNICO

Tem-se como objetivo, nesta seção, apresentar os aspectos gerais relacionados à estrutura judiciária brasileira, suas ramificações, funcionamento e elementos chaves para o andamento do processo judicial eletrônico. Aqui, é possível entender como funciona a estrutura judiciária brasileira e a função do processo judicial eletrônico neste contexto.

Inserido no âmbito do Poder Judiciário, está a Justiça Eletrônica (e-*Justice*). Ela visa à modernização dos serviços prestados pela justiça à comunidade, contribuindo para melhor atender os cidadãos que acedem ao mesmo através dos processos judiciais. Essa modernização acontece através da aplicação das TICs nos órgãos de justiça.

Os sistemas responsáveis por gerenciar o funcionamento dos processos judiciais eletrônicos são conhecidos como Sistemas de Gestão de Processos Judicias Eletrônicos (SGPJE). Esses sistemas visam atender a condução desses processos que, na sua maioria, ainda circulam em papel, mas que aos poucos se transformam em processos judiciais eletrônicos. Neste ponto, a interoperabilidade se faz importante, como exposto na subseção 2.6.

2.1 ESTRUTURA JUDICIÁRIA BRASILEIRA (VISÃO GERAL)

Para conhecer melhor o processo judicial eletrônico e a importância da interoperabilidade neste meio, exibe-se aqui uma visão geral sobre Poder Judiciário e sua estrutura.

A função do Poder Judiciário é assegurar os direitos individuais, coletivos e sociais dos cidadãos, e aplicar a Justiça através do emprego das leis vigentes aos casos concretos que chegam ao mesmo. (BRASIL, 2009). Desta forma, estes casos são responsáveis pela geração dos processos judiciais.

Para organização e julgamento desses processos, a justiça brasileira é dividida em cinco áreas de competência (BRASIL, 2009):

a) Justiça Estadual: procura a resolução de conflitos que possam existir entre pessoas, empresas, e instituições, nos campos: Civil, Tributário, Consumidor e Penal;
   Matéria: Justiça Comum.

b) Justiça Federal: julga casos de interesse da União, das autarquias ou das empresas públicas;
Matéria: Justiça Comum.

c) Justiça do Trabalho: procura a resolução de conflitos entre empregadores e trabalhadores;
Matéria: Justiça Especializada.

d) Justiça Eleitoral: busca reger e resolver conflitos eleitorais;
Matéria: Justiça Especializada.

e) Justiça Militar: tem como missão processar e julgar crimes militares.
Matéria: Justiça Especializada.

A divisão hierárquica da justiça no Brasil é baseada em quatro graus (BRASIL, 1999):

- Primeira Instância: Responsável pela primeira análise e sentença do processo, normalmente comandada por juízes. Caso uma das partes não concorde com a decisão tomada em primeira instância, ela pode pedir uma reavaliação do processo na instância superior;

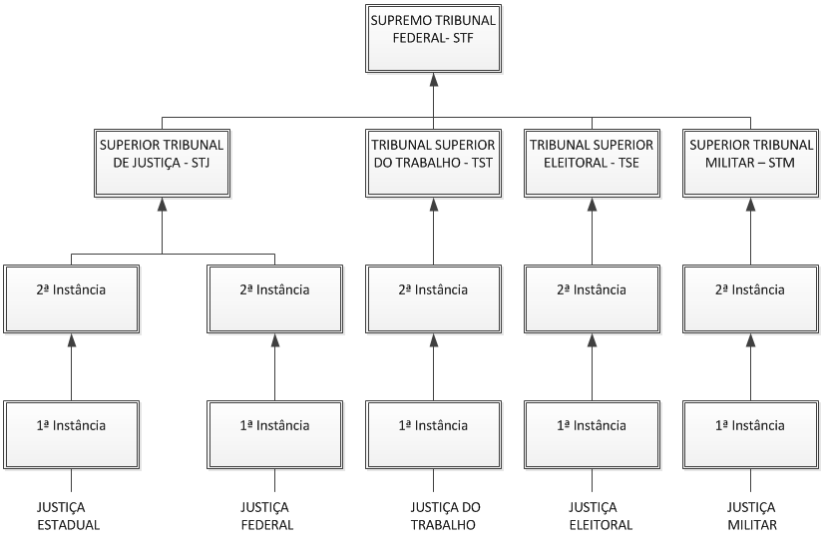
- Segunda Instância: Os processos em que houve requisição de reavaliação são novamente julgados, agora em segunda instância. Estas instâncias na justiça comum são representadas pelos Tribunais de Justiça, e são coordenadas pelos desembargadores, com poderes para manter ou revogar a decisão tomada em primeira instância. O equivalente ocorre nas demais justiças;

- Terceira instância: Em caso de nova contestação, a ação pode ser encaminhada ao terceiro grau, responsável por decretar a sentença final, a qual não permite mais recursos. Este grau é comandado por ministros e é representado pelos tribunais superiores, tendo por objetivo fazer com que a lei seja executada de igual forma em todo o país.

- Quarta instância: A mais alta corte Judicial, representada pelo Supremo Tribunal Federal (STF). Este é responsável por garantir que a Constituição Federal seja cumprida, além de julgar os políticos que desempenham funções federais: presidente, senadores, e deputados da república.

Esta divisão hierárquica é ilustrada através de um organograma representado pela Figura 1.

Figura 1 - Organograma da Estrutura Judiciária Brasileira.



Além dessa atuação jurisdicional precípua, cada órgão tem atribuições administrativas autônomas. Para a administração de toda essa estrutura, o Conselho Nacional de Justiça foi fundado (CNJ).

2.2 CONSELHO NACIONAL DE JUSTIÇA (CNJ)

Criado em 31 de dezembro de 2004 (Emenda Constitucional nº 45/2004) e instalado em 14 de junho de 2005, o Conselho Nacional de Justiça (CNJ) é instituído como órgão superior para gestão e aprimoramento da justiça. Este órgão tem como missão contribuir para construção de um serviço jurisdicional cada vez melhor, cooperando na busca pela eficiência, transparência e modernização dos serviços prestados à sociedade (CNJ, 2013a).

Para o CNJ alcançar estes objetivos, avançar com o processo judicial eletrônico é fundamental, gerando altos ganhos em produtividade para o sistema judiciário (CONCEIÇÃO, 2011).

O CNJ se define da seguinte forma: *"Uma instituição pública que visa aperfeiçoar o trabalho do sistema judiciário brasileiro, principalmente no que diz respeito ao controle e à transparência administrativa e processual."* (CNJ, 2013a).

Determinado pela Constituição Federal de 1988 (BRASIL, 1988), o CNJ possui funções específicas nas áreas destacadas abaixo:

- Política Judiciária: *"zelar pela autonomia do Poder Judiciário e pelo cumprimento do Estatuto da Magistratura, expedindo atos normativos e recomendações."* (CNJ, 2013a).
- Gestão: *"definir o planejamento estratégico, os planos de metas e os programas de avaliação institucional do Poder Judiciário."* (CNJ, 2013a).
- Prestação de Serviços ao Cidadão: *"receber reclamações, petições eletrônicas e representações contra membros ou órgãos do Judiciário, inclusive contra seus serviços auxiliares, serventias e órgãos prestadores de serviços notariais e de registro que atuem por delegação do poder público ou oficializado."* (CNJ, 2013a).
- Moralidade: *"julgar processos disciplinares, assegurada ampla defesa, podendo determinar a remoção, a disponibilidade ou a aposentadoria com subsídios ou proventos proporcionais ao tempo de serviço e aplicar outras sanções administrativas."* (CNJ, 2013a).
- Eficiência dos Serviços Judiciais: *"melhores práticas e celeridade: elaborar e publicar semestralmente relatório estatístico sobre movimentação processual e outros indicadores pertinentes à atividade jurisdicional em todo o País."* (CNJ, 2013a).

Assim, pode-se destacar como atribuições do CNJ a gestão de toda a estrutura judiciária brasileira e das partes envolvidas, através de planejamento e planos de metas, contribuindo para a autonomia do Poder Judiciário, para fazer com que o cidadão seja bem atendido e tenha seus direitos garantidos, colaborando para uma melhora contínua no sistema judiciário, cooperando na busca pela eficiência, transparência e modernização dos serviços prestados à sociedade.

2.3 GOVERNO ELETRÔNICO

Quando se fala em modernização do Poder Judiciário, é importante entender o que é o Governo Eletrônico (e-Gov), e qual a

relação dele com a informatização judiciária. Assim, esta subseção apresenta os conceitos envolvidos neste plano.

Os termos e-*Justice* e e-Gov estão completamente entrelaçados, sendo que e-*Justice*, é o próprio Governo Eletrônico, porém aplicado especificamente ao ramo judicial. Logo, o entendimento de e-Gov satisfaz as condições necessárias para a compreensão da Justiça Eletrônica.

O e-Gov é a aplicação das TICs nos órgãos públicos, visando à melhoria dos serviços de administração pública e o atendimento ao cidadão. O e-Gov é responsável por formar uma infraestrutura única de comunicação entre os diferentes órgãos públicos, tendo como objetivo principal ampliar a participação popular e manter clareza nas operações executadas (ROVER; MEZZAROBA, 2011).

Existem duas maneiras de enxergar o governo eletrônico, uma por meio da visão do estado e outra através da ótica da sociedade. O estado entende o governo eletrônico como uma ferramenta para auxiliar nos serviços públicos prestados aos cidadãos e nas funções do Estado (Poder Judiciário, Legislativo, e Executivo). Já a sociedade entende o governo eletrônico como uma forma de cumprimento dos fins estabelecidos pelo Estado Democrático de Direito, por intermédio das TICs, como instrumento de diálogo com a sociedade (ROVER; MEZZAROBA, 2011).

Segundo Rover e Mezzaroba (2011), o governo eletrônico pode ser dividido em três diferentes categorias, as quais podem ser igualmente representadas pela justiça eletrônica:

- G2G: Trata as transações entre governos (compras, contratos, etc);
- G2B: Trata as transações entre governo e fornecedores;
- G2C: Trata as transações entre governo e sociedade (cidadãos);

Dentro deste entendimento está o Processo Judicial Eletrônico, que entre outros aspectos, visa à modernização e ao dinamismo do poder judiciário, para uma prestação jurisdicional mais célere, moderna, e efetiva aos cidadãos.

2.4 PROCESSO JUDICIAL ELETRÔNICO

A Lei que regulamenta o processo judicial eletrônico no país é a de Nº 11.419, de 19 de dezembro de 2006, dando respaldo jurídico à mudança que iniciou mesmo antes dessa lei (BRASIL, 2006). De forma sucinta e geral, permite o uso de TI no âmbito do processo judicial e dá liberdade aos tribunais para fazê-lo. Define regras gerais de segurança e remete para outras normas específicas a validade jurídica dos documentos eletrônicos (BRASIL, 2001).

Segundo Rover (2013), o processo judicial eletrônico nada mais é do que a informatização de ações e documentos em fluxos, garantindo autenticidade, integridade, e temporalidade aos processos. Esses princípios são garantidos através da utilização segura dos documentos eletrônicos. Estes princípios são conceituados da seguinte forma:

- Autenticidade: responsável por identificar a autoria dos documentos;
- Integridade: corresponde à inalterabilidade do conteúdo do documento;
- Temporalidade: representa a verificação e certificação dos momentos de criação e alteração do documento.

A informatização do poder judiciário, através do processo judicial eletrônico, permite agilidade para os integrantes do processo (autores, juízes, advogados, réus, assistentes processuais), aumentando a celeridade e eficiência da justiça. Para exemplificar esta afirmação, verificou-se que a implantação de um sistema de gestão de processo judicial eletrônico, em um determinado tribunal, reduziu em 51% o tempo médio de tramitação dos seus processos (CNJ, 2014), diminuindo o tempo de tramitação em mais da metade do tempo do que ocorria na execução do processo judicial em papel.

Algumas razões para a celeridade no tempo de tramitação dos processos são apresentadas abaixo, evidenciando este e outros benefícios trazidos ao judiciário e à sociedade:

- Acessibilidade (pode ser acessado a qualquer hora e em qualquer lugar);
- Arquivamento de documentos (todo o material é arquivado em formato digital);
- Minimização acentuada de papel (alto impacto na preservação ambiental);

- Otimização de tarefas (pesquisas por processos, montagem, arquivamento);
- Redução de espaços físicos (os processos físicos utilizam espaços imensos para armazenamento de todo o sistema judiciário);
- Desobstrução da Justiça (andamento e finalização mais rápida dos processos);
- Redução de custos (aluguel de salas para arquivamento de processos, extinção de mão de obra para realizar tarefas básicas);
- Segurança: Possibilidade de utilização de certificação e assinatura digital, criptografia de dados, provendo privacidade, autenticidade, e integridade aos documentos eletrônicos.

Um fator que merece destaque, quanto à velocidade para a tramitação dos processos, é a forma de organização em meio digital. Tarefas que poderiam durar horas, ou dias, no processo em papel, podem ser realizadas em segundos no processo eletrônico.

Um exemplo básico para esta afirmação é o momento de busca por um processo. No meio eletrônico basta alguns cliques e pronto, o processo está a sua disposição, com todas as informações necessárias para investigação ou tomada de decisão. No processo físico, em papel, é necessário um responsável para este serviço, tendo que procurar o processo em meio uma pilha de documentos e arquivos, tornando o processo lento. Além disto, o responsável deve estar presente no local onde o processo foi arquivado fisicamente, fato que não acontece em meio eletrônico, no qual o processo pode ser acessado em qualquer parte do mundo. Esse simples exemplo demonstra características que produzem celeridade no trâmite processual.

Outro fator interessante advindo do uso dos processos eletrônicos é a preservação ambiental. A utilização de papel no processo judicial eletrônico é mínima, reduzindo absurdamente a quantidade de papel utilizada, consequentemente, o desmatamento de nossas florestas (CONCEIÇÃO, 2011).

Para o funcionamento de toda essa estrutura, o documento eletrônico é imprescindível. Por este motivo ele é apresentado abaixo.

2.4.1 Documento Eletrônico

O documento eletrônico é parte fundamental dentro do processo judicial eletrônico. Sem ele, o processo judicial eletrônico não existe. Assim, procura-se esclarecer o conceito de documento eletrônico para evidenciar sua importância dentro deste processo.

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 (MARCACINI, 1999).

> O documento físico consiste em algum meio tangível, onde a informação está inscrita, normalmente o papel. É comum que instrumentos sejam feitos em um maior número de vias, distribuídas entre os signatários. Estes conceitos, de documento original, ou de vias de um mesmo documento, são inexistentes no meio eletrônico. 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. É o caso até de dizermos que não existe um original e não existem cópias nem vias do documento eletrônico, enquanto ele for mantido nesta forma (MARCACINI, 1999).

Como visto, o documento eletrônico tem a mesma propriedade fundamental do documento em papel, que é registrar acontecimentos. Porém, a sua vantagem é a acessibilidade proporcionada. Permite acesso e manipulação dos dados não importando a localização dos envolvidos.

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.

Os mecanismos que promovem segurança aos documentos eletrônicos e consequentemente, ao processo judicial eletrônico, são apresentados na seção 5. Esses documentos tramitam e são armazenados por meio dos SGPJE.

Os dois principais SGPJE da justiça brasileira, levando em consideração a quantidade de processos que tramitam na justiça e a quantidade de tribunais que os utilizam, são o Sistema de Automação da Justiça (SAJ), e o Processo Judicial eletrônico (PJe).

2.4.2 Sistema de Automação da Justiça (SAJ)

O SAJ foi desenvolvido em parceria com sete tribunais de justiça estaduais que representam a maior parte dos processos que tramitam na justiça estadual brasileira, ou seja, mais de 60%. Segundo a empresa Softplan (2013), o SAJ é responsável por contribuir para uma prestação jurisdicional mais efetiva, aproximando o cidadão e judiciário (SOFTPLAN, 2013).

"O SAJ incorpora facilidades para a automatização das rotinas jurisdicionais e administrativas que asseguram excepcionais ganhos de produtividade e otimização dos recursos de Tribunais de Justiça, Ministério Público e Procuradorias." (SOFTPLAN, 2013).

O SAJ, hoje, conta com cinco soluções de sistemas, são eles: SAJ Judiciário Primeiro Grau, SAJ Judiciário Segundo Grau, e-SAJ, SAJ Procuradorias, SAJ Ministério Público, e SAJ Gestão administrativa.

2.4.3 Processo Judicial eletrônico (PJe)

O PJe é o sistema para a automação de processos judiciais desenvolvido pelo CNJ em parceria com tribunais. Lançado no dia 21 de julho de 2011, tem por objetivo a prática de atos processuais, assim como o acompanhamento de processos judiciais (CNJ, 2013b).

> O objetivo principal do CNJ é manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais pelos magistrados, servidores e demais participantes da relação processual diretamente no sistema, assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na

> Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho. (BRASIL, 2013b).

Por meio deste objetivo, o PJe foi construído com o intuito de ser uma solução única, gratuita, interoperável e segura aos tribunais brasileiros, visando a redução de gastos dos próprios tribunais com o desenvolvido e/ou aquisição de software para gestão de processos eletrônicos, podendo, assim, utilizar esses recursos financeiros em atividades próprias aos objetivos do judiciário (CNJ, 2013b).

Pode-se observar que estes dois sistemas, PJe e SAJ, têm o mesmo foco e possuem o mesmo objetivo; o que os diferencia é a forma de implementação, ou seja, o meio, e não o fim. O SAJ e PJe, assim como os demais SGPJE ainda não são interoperáveis, o que é um retrocesso para a celeridade e modernização dos processos eletrônicos em trâmite na justiça brasileira.

3. INTEROPERABILIDADE

Conforme visto acima, a interoperabilidade é tema fundamental quando se fala em intercomunicação de dados entre sistemas heterogêneos. Mas o que realmente é interoperabilidade, e quais os níveis de interoperabilidade se pode alcançar durante a troca de informações entre sistemas? Para responder estas perguntas, esta seção trata o conceito e os níveis de categorização de interoperabilidade existentes.

Conforme Diallo (2011), interoperabilidade é a troca de informações úteis entre sistemas heterogêneos, ou unidades heterogêneas de sistemas. O sistema que recebe a informação deve reconhecer a informação que necessita e utilizá-la, assim como desprezar a informação desnecessária. Os requisitos necessários para obtenção da interoperabilidade são a troca e o uso da informação. Isso quer dizer que o fato de trocar informações entre sistemas diferentes não produz interoperabilidade, as informações trocadas precisam ser utilizadas.

Isto posto, pode-se dizer que a interoperabilidade é a tecnologia que promove facilidades para a comunicação entre diferentes sistemas, ou partes distintas de um mesmo sistema. Deste modo, a falta de interoperabilidade entre sistemas pode ocasionar problemas. De acordo com Beaumaster (2002), evidenciam-se alguns destes problemas na lista abaixo:

- Redundância de dados;
- Inconsistência de dados;
- Falhas na qualidade e integridade de dados;
- Falhas para compartilhar informações;
- Falhas para compartilhar serviços e funcionalidades;
- Falta de conectividade;
- Falta de coordenação entre departamentos;
- Alto custo operacional de sistemas heterogêneos;
- Alto custo para manutenção de sistemas heterogêneos;

Além dos problemas gerados pela falta de interoperabilidade, destacam-se, também, alguns benefícios trazidos pela utilização desta tecnologia no âmbito de e-Gov (ISA, 2010):

- **Cooperação** entre administrações públicas que visam estabelecer serviços públicos;
- **Câmbio de informações** entre administrações públicas para cumprir requisitos legais ou compromissos políticos;
- **Compartilhamento e reuso da informação** entre administrações públicas para aumentar a eficiência administrativa e diminuir a burocracia para os cidadãos e empresas.

Ainda, conforme o ISA (2010), esses benefícios provêm como resultados:

- **Melhora na prestação do serviço público** aos cidadãos e empresas facilitando a entrega dos serviços públicos;
- **Redução de Custos** para administração pública, empresas, e cidadãos, devido à eficiência na prestação dos serviços públicos.

Como posto anteriormente, para se obter a interoperabilidade não basta somente trocar informações entre sistemas heterogêneos, precisa-se, também, identificar a informação utilizável. Para prover um contexto que permita identificar essas informações, é necessário definir níveis de interoperabilidade. Estes níveis podem ser compreendidos como um modelo de maturidade. Assim, para alcançar o próximo nível é preciso ter cumprido as exigências do nível anterior.

Neste trabalho, adotou-se a categorização apresentada no EIF (ISA, 2010). O EIF é um *framework* que define, entre outros aspectos, a interoperabilidade em níveis. Esta definição é baseada em quatro níveis: técnico, semântico, organizacional, e legal. Aqui, evidencia-se o nível sintático, que no EIF é categorizado dentro do nível semântico. As definições de cada um destes níveis, por ordem crescente de complexidade (do mais básico ao mais complexo), são apresentadas abaixo.

3.1 INTEROPERABILIDADE TÉCNICA

Interoperabilidade técnica é o nível mais básico de interoperabilidade. Trata as questões técnicas de conexão para a comunicação (troca de mensagens) entre os sistemas de computadores.

Nesse conceito, estão incluídos padrões de conexão de rede, protocolos de comunicação, tais como: TCP/IP, HTTP, HTTPS, SSH.

Esse nível permite que haja troca de dados confiável entre sistemas, porém não permite que ocorra entendimento dos dados trocados. Para obter essa compreensão, é preciso alcançar outros níveis de interoperabilidade (MISURACA, 2011).

Padrões que levam em consideração apenas a interoperabilidade técnica, podem falhar no seu objetivo que é obter troca de informação entre sistemas. Desta forma, necessitarão de novas iniciativas no futuro para alcançar maiores níveis de interoperabilidade, e assim resolver essas questões. (RAY, 2011).

A interoperabilidade técnica está se tornando cada vez mais fácil de ser atingida, a ênfase agora está em atingir maiores níveis de interoperabilidade, embora o conhecimento ainda seja limitado para alcançar alguns níveis (KUBICEK E CIMANDER, 2009).

3.2 INTEROPERABILIDADE SINTÁTICA

O nível sintático é categorizado no EIF dentro do nível de interoperabilidade semântica. Porém, são duas dimensões distintas, pois possuem objetos, objetivos, soluções tecnológicas, estado da arte, conceitos e características diferentes (ver Quadro 1). Por essas razões, optou-se por separá-las neste trabalho, para melhor compreensão de ambas.

A interoperabilidade sintática se preocupa em descrever o exato formato do dado que é trocado, considerando a gramática, e os esquemas (ISA, 2010), para que a aplicação que está recebendo os dados possa processá-los com sucesso (KUBICEK, CIMANDER, e SCHOLL, 2011).

Neste nível, o objeto de transporte são os dados (KUBICEK E CIMANDER, 2009). Tecnologias para alcançar este estágio já existem, tais como: XML, (para definição da sintaxe), WSDL, SOAP (para padrões de troca de mensagens).

3.3 INTEROPERABILIDADE SEMÂNTICA

Aqui o entendimento dos dados começa a ser considerado. O objetivo neste nível é garantir que o significado dos dados trocados seja compreendido pela aplicação receptora (SAEKOW e BOONMEE,

2009). Desta forma, neste nível, o objeto de transporte é a informação (KUBICEK E CIMANDER, 2009).

Para o entendimento das informações que estão sendo trocadas, é necessário o desenvolvimento de vocabulários controlados de dados, para assim, garantir que o significado dos dados seja compreendido da mesma forma por ambas as partes (ISA, 2010). É possível expressar neste nível o real significado da informação, permitindo que a mesma seja compreendida e executada entre diferentes sistemas. (CARBONI e VELICOGNA, 2012).

Para atingir o nível semântico, existem conceitos e métodos disponíveis, porém, ainda não padronizados. Algumas soluções existentes: diretórios comuns, *data keys*, e ontologias (KUBICEK E CIMANDER, 2009).

3.4 INTEROPERABILIDADE ORGANIZACIONAL

O nível de interoperabilidade organizacional trata a coordenação e o alinhamento entre os processos e a arquitetura de informação dos diferentes sistemas (SAEKOW e BOONMEE, 2009). O objeto de transporte são os processos e os serviços (KUBICEK, CIMANDER, e SCHOLL, 2011).

Conforme Ray (2011), iniciativas para alcançar a interoperabilidade organizacional deveriam levar em consideração a abordagem arquitetural das organizações e cobrir os seguintes itens, entre outros:

- Princípios de cooperação entre departamentos de governo sobre diferentes níveis;
- Política para coleta, compartilhamento, e propriedade de dados;
- Definição dos processos de negócio;
- Identificação do escopo no qual possa haver compartilhamento através das fronteiras das organizações;
- Visão arquitetural, proporcionada através de modelos de arquitetura. Exemplo: Arquitetura Orientada a Serviços (SOA).

O estado da arte deste nível ainda possui falta de clareza em sua conceituação, com diversas possibilidades de interpretação. Apesar da

importância deste nível, a cobertura desse domínio ainda é limitada (KUBICEK, CIMANDER, e SCHOLL, 2011).

3.5 INTEROPERABILIDADE LEGAL

Aqui é contemplada a validade legal da troca de informações. Levam-se em consideração os métodos legais determinados pelos governos. A troca de informação deve ser harmonizada e efetuada de acordo com as leis vigentes.

Normalmente, as regulamentações legais já existem para atingir este nível, porém a dificuldade está em combinar as leis com as disposições técnicas (KUBICEK, CIMANDER, e SCHOLL, 2011).

3.6 TECNOLOGIAS PARA PROVER INTEROPERABILIDADE

Esta subseção tem o objetivo de apresentar, através de uma tabela (Quadro 1), o estado da arte com relação às tecnologias de interoperabilidade existentes para atingir os diferentes níveis de interoperabilidade.

Quadro 1 – Comparação entre Níveis de Interoperabilidade

Nível	Conteúdo	Objetivo	Soluções	Algumas Tecnologias Existentes
Técnica	Sinais	Conexão entre computadores	Protocolos de comunicação	HTTPS, SSH, TCP/IP, S/MIME.
Sintática	Dados	Formatação e Processamento de Dados	Padrões de sintaxe e troca de dados	XML, ASN.1, WSDL
Semântica	Informação	Interpretação de dados	Vocabulários de informação	XML Schemes, Ontologias
Organizacional	Processos	Interconexão entre processos	Modelos de Arquitetura	SOA

O quadro 1 é baseado nas propostas apresentadas por Kubicek (2011), e pelo ISA (2010). Neste quadro, mostram-se, de forma clara, as diferenças entre os níveis técnico, sintático, semântico e organizacional de interoperabilidade, usando como variáveis o conteúdo, o objetivo, a solução e a tecnologia referente a cada nível.

4. MODELO NACIONAL DE INTEROPERABILIDADE DO JUDICIÁRIO

O Modelo Nacional de Interoperabilidade de dados do Poder Judiciário e órgãos de administração da justiça (MNI) foi instituído por meio da Resolução Conjunta Nº 3, de 16 de abril de 2013. Esta resolução evidencia a necessidade da interoperabilidade e determina que os órgãos do Poder Judiciário e do Ministério Público implementem o MNI até o prazo final, definido para o dia 16 de abril de 2015. (CNJ, 2013c).

O objetivo principal da construção do MNI é proporcionar o intercâmbio de informações entre os mais variados SGPJE em execução no Poder Judiciário. A cooperação que poderá ser agregada entre os sistemas de gestão dos órgãos judiciais, através deste modelo, proporcionará uma prestação do serviço jurisdicional mais clara, acessível e menos burocrática aos cidadãos e organizações. Outros fatos são as informações que o MNI define, que podem servir de base para auxiliar os desenvolvedores a implementar e conhecer as funcionalidades vinculadas aos SGPJEs (CNJ, 2014a).

Os resultados esperados através da implementação do MNI são maior celeridade, dinamismo e reuso dos sistemas judiciais, por conseguinte, reproduzindo redução de custos (financeiros, e em tempo) na tramitação de processos judiciais eletrônicos, contribuindo para a desobstrução do Poder Judiciário.

Para a realização do intercâmbio de informações entre diferentes sistemas, algumas estruturas e tecnologias são definidas pelo MNI. Na subseção abaixo, os principais elementos envolvidos neste processo são apresentados:

4.1 ELEMENTOS DE COMUNIÇÃO DO MNI

O MNI apresenta um conjunto de elementos de comunicação para prover interoperabilidade entre os SGPJEs. Neste modelo, esses elementos são implementados através da linguagem XML (*eXtensible Markup* Language), definidos por esquemas XML (subseção 4.1.1), e um serviço web responsável por enviar e receber dados (*web services* – subseção 4.1.2).

4.1.1 Esquemas XML

Os esquemas XML são uma estrutura de dados que definem vocabulários compartilhados e possibilitam que as máquinas exerçam as regras concebidas pelas pessoas. O significado dos dados é fornecido através da definição da estrutura, índice e semântica dos documentos XML. Esses documentos XML também são conhecidos como documentos de instância, quando estão de acordo com um esquema particular. Os esquemas XML disponibilizam uma linguagem abundante para definição da estrutura do documento XML. A sintaxe desses esquemas é baseada na própria linguagem XML, permitindo reutilização desta tecnologia. O reuso e refinamento de esquemas é admitido através da extensão ou restrição de elementos já definidos (W3C, 2008).

A estrutura do MNI é composta por dois Esquemas XML principais. Esses dois esquemas são responsáveis por definir a descrição de cada elemento envolvido no trâmite do processo judicial eletrônico. Assim, todo e qualquer sistema que implementar o MNI terá de gerar processos que contenham compatibilidade com os elementos definidos pelo MNI, para prover o intercâmbio de informações. Isso quer dizer, em outras palavras, gerar documentos XML que possam ser validados por intermédio dos esquemas XML definidos pelo MNI. Neste caso, os documentos XML são os próprios processos judiciais eletrônicos.

Desta forma, o sistema receptor (responsável por receber os dados do sistema emissor) consegue entender o contexto e o significado daqueles dados, podendo, assim, interpretá-los. Da mesma forma, a aplicação emissora sempre sabe como definir as informações, para que a aplicação na outra ponta entenda seu significado. Modelos que se utilizam destes esquemas, quando bem elaborados, podem atingir o nível de interoperabilidade semântica, isto é, se não falhar em nenhum nível de interoperabilidade anterior.

Abaixo, uma descrição geral sobre estes dois esquemas, para apontar a responsabilidade de cada um:

Intercomunicacao-2.2.2.xsd: Define os objetos básicos para troca de informações processuais. Entre esses elementos constam: assuntos, classes, polos processuais, partes do processo, documentos, tipos de documentos. Este esquema permite a utilização dos seus elementos por meio de serviços oferecidos por sistemas externos (CNJ, 2014b).

Tipos-servico-intercomunicacao-2.2.2.xsd: Este esquema define os elementos utilizados pelo serviço web (*web service*) definido no MNI. Neste esquema, existe não só a definição de novos elementos, como também o encapsulamento dos elementos definidos no esquema anterior. Desta forma, o esquema intercomunicação-2.2.2.xsd é um complemento a este esquema (CNJ, 2014b).

4.1.2 Web Service

A intercomunicação entre os sistemas heterogêneos é realizada através da utilização da tecnologia de *web services* (WSDL). Os *web services* são tecnologias que permitem compartilhar informações distintas através de uma rede de dados, normalmente a internet. A maior vantagem do uso de *web services* é a capacidade de intercomunicar sistemas distintos, independente da linguagem ou plataforma em que é executado. Ou seja, a maior característica dos *web service* é prover interoperabilidade, aplicar a interação da aplicação diretamente com outra aplicação, sem a intervenção humana (ROVARIS, 2007).

O *web service* definido pelo MNI tem como proposta representar os serviços de comunicação processuais oferecidos por um tribunal. O conjunto dos esquemas para comunicação apresentados acima constituem este *web service*. Entre outros, os serviços ofertados por este web service são: consulta, alteração, recebimento de processos e entrega de manifestação processual.

4.1.3 Requisitos de Segurança

O MNI determina como meio preferencial para autenticação de acesso aos seus serviços a utilização de certificados ICP-Brasil. Caso o tribunal não implemente o uso de certificados ICP-Brasil, determina-se, então, o uso de login e senha, desde que a autenticação entre as partes seja feita por meio de um canal seguro, mediante protocolo de comunicação HTTPS.

A comunicação entre tribunais deve conter os códigos identificadores de acordo com a Resolução CNJ Nº 65, que dispõe sobre a uniformização dos números dos processos nos órgãos do Poder Judiciário (CNJ, 2008).

O MNI conta com uma categorização em níveis para autorização de acesso aos serviços que oferece. Os níveis são definidos conforme Quadro 2, adaptado do documento que descreve o MNI (CNJ, 2014b).

Quadro 2. – Níveis de acesso ao MNI.

Nível	Nome	Quem acessa
Zero	Público	Servidores do judiciário e dos demais órgãos públicos de administração da justiça e Advogados.
Um	Segredo	Servidores do judiciário e dos demais órgãos públicos de administração da justiça e as partes (integrantes) do processo.
Dois	Sigilo mínimo	Servidores do judiciário e dos demais órgãos públicos de administração da justiça
Três	Sigilo médio	Servidores do órgão no qual tramita o processo, as partes que provocaram o incidente, e aqueles que forem expressamente incluídos.
Quatro	Sigilo intenso	Servidores qualificados (magistrado, diretor de secretaria/escrivão, oficial de gabinete/assessor) do órgão no qual tramita o processo, as partes que provocaram o incidente e aqueles que forem expressamente incluídos.
Cinco	Sigilo absoluto	Apenas o magistrado do órgão em que tramita, os servidores e demais usuários por ele indicado e as partes que provocaram o incidente.

A responsabilidade em assegurar que os níveis de sigilo sejam respeitados é dos tribunais.

4.2 MODELOS DE INTEROPERABILIDADE EM E-GOV

Assim como o MNI, outros modelos de interoperabilidade, relacionados a e-Gov e e-Justice, estão em aplicação ou em desenvolvimento no Brasil e no mundo. Desta maneira, esta seção procura apresentar sucintamente alguns modelos existentes nesta área, podendo, inclusive, servir como objetos de comparação para com o MNI em trabalhos futuros.

4.2.1 e-PING

A arquitetura de Padrões de Interoperabilidade de Governo Eletrônico do Brasil (E-Ping) é baseada em um conjunto mínimo de regras, que estabelecem padrões para a utilização da TIC no governo

federal, criando condições para uma intercomunicação mais efetiva entre governo e sociedade, e entre os próprios órgãos do governo (BRASIL, 2014).

Para as instâncias do governo federal (Poder Executivo Brasileiro), a utilização da arquitetura E-Ping é obrigatória (Portaria SLTI/MP nº 5, de 14 de julho de 2005). O governo federal sugere a utilização do E-Ping a quem desejar interoperar com as entidades fora do governo federal. Desta forma, a aplicação deste padrão acontece de forma voluntária para os demais poderes e órgãos que não compõem o quadro do governo federal (BRASIL, 2014).

Áreas de cobertura do E-Ping:

- Interconexão;
- Segurança;
- Meios de Acesso;
- Organização e Intercâmbio de Informações;
- Áreas de Integração para Governo Eletrônico.

O objetivo do E-Ping é conceder de maneira mais fácil e segura o intercâmbio de informações entre governo e sociedade, entre as diferentes instâncias do governo e também, entre governo brasileiro e entidades estrangeiras (outros governos, multinacionais) (BRASIL, 2014).

4.2.2 e-PMG

O Padrão de Metadados de Governo Eletrônico (e-PMG) é incorporado dentro da arquitetura e-PING. Tem por objetivo facilitar o acesso dos cidadãos que buscam por informações do governo federal na web através da descrição dos recursos. O e-PMG é baseado no Padrão Dublin Core (DC), desenvolvido pelo *Dublin Core Metadata Initiative* (DCMI), que trabalha no desenvolvimento de padrões de metadados interoperáveis (BRASIL, 2014a).

O e-PMG em parceria com o e-PING, são padrões que buscam prover interoperabilidade semântica ao governo federal. Este padrão é formado por um conjunto de 20 elementos: 15 baseados no DC, e 5 elementos novos considerados importantes dentro do âmbito de e-*gov* no Brasil (BRASIL, 2014a).

4.2.3 e-CODEX

O e-CODEX é um projeto de larga escala que visa melhorar o acesso dos cidadãos e das empresas à justiça entre os países da Europa, bem como melhorar a interoperabilidade dos órgãos da justiça entre os países membros da União Europeia (EUROPEAN UNION, 2014).

Carboni e Velicogna (2012) apresentam a infraestrutura do e-CODEX e produzem uma análise, avaliando questões de interoperabilidade, governança, e valores públicos. O trabalho é focado no projeto e-CODEX e não faz menção a outros modelos.

4.2.4 GRP

Jimenez (2012) apresenta o GRP (Gestão de Requisições Policiais). O GRP é um módulo de interoperabilidade de software introduzido nos sistemas dos órgãos da administração da justiça Catalã. O GRP visa gerar uma intercomunicação eficaz entre o sistema de gestão da polícia e do judiciário, através da adoção de padrões de interoperabilidade.

O trabalho mostra que a adoção do GRP foi um sucesso, trazendo mais celeridade e eficiência à justiça Catalã, ganhando o prêmio *Quality in Justice*, em 2010, pelo Conselho Geral do Judiciário Espanhol. A análise de Jimenez demonstra que a interoperabilidade pode ser fator primordial para a celeridade do sistema judiciário.

O artigo não aborda as tecnologias, os padrões e modelos utilizados no desenvolvimento do GRP. O ponto principal do artigo é apontar como resultado a importância da interoperabilidade no âmbito da justiça eletrônica.

4.3 FRAMEWORK DE RAY

Ray (2011) apresenta um *framework* desenvolvido para realizar análises de padrões de interoperabilidade em e-government. Esse *framework* é baseado em três áreas: Contexto (1), Conteúdo (2), e Processo (3); subdivididas em oito camadas: *background* and escopo (1); políticas de interoperabilidade básicas, critérios para seleção de padrões, definição de padrões abertos e padrões de tecnologia (2); padrões de ciclo de vida e políticas de gerenciamento e conformidade (3). Essas camadas são os critérios considerados por Ray significativos para avaliar modelos de interoperabilidade em e-gov.

Ray avaliou um conjunto de 21 modelos de interoperabilidade em e-Gov, englobando países de todos os continentes. Por meio deste *framework*, foi produzido um conjunto de recomendações para a construção de novos modelos de interoperabilidade em e-*government*, destacando-se os seguintes: definir níveis de interoperabilidade e como atingi-los; apresentar fundamentos jurídicos, metas e objetivos; ter políticas bem definidas; evidenciar o uso de padrões abertos na política de aplicações; contar com mecanismo para gerenciar o ciclo de vida (podendo atualizar, e modificar de maneira simples e planejada). Neste trabalho, nenhum modelo de interoperabilidade em e-*Justice* é analisado. Ray não apresenta recomendações de melhorias aos modelos analisados, apenas define as oito camadas de análise e verifica se os modelos cumprem ou não os requisitos inerentes a cada camada.

Outros trabalhos relevantes, que fazem análises sobre padrões de interoperabilidade em governo eletrônico, são discutidos e apresentados em Gartner (2007), UNDP (2007), e Guijarro (2009). Todos fazem análises comparativas sobre padrões de interoperabilidade em e-gov, porém variam em termos de camadas de análise, e da conceituação dada aos níveis de interoperabilidade. Nenhum desses trabalhos realiza análise crítica ou comparativa sobre padrões de interoperabilidade no âmbito judicial.

5. PADRÃO BRASILEIRO DE ASSINATURA DIGITAL

A tecnologia responsável por prover segurança aos documentos eletrônicos, assegurando autenticidade, integridade e não repúdio é a assinatura digital. Essa tecnologia é factível através da utilização de mecanismos criptográficos (MENEZES, OORSCHOT, e VANSTONE, 2001).

Para compreender o funcionamento dessa tecnologia, é fundamental o entendimento de outros conceitos que estão inseridos neste contexto. Além da segurança proporcionada aos documentos eletrônicos, a assinatura digital pode prover interoperabilidade aos processos eletrônicos que tramitam no judiciário, por meio da utilização do PBAD.

Assim, o objetivo nesta seção é apresentar os conceitos relacionados à assinatura digital e ao PBAD definido pelo Instituto Brasileiro de Tecnologia da Informação (ITI), para apresentar o estado da arte da assinatura digital no país, e poder mostrar uma relação direta dessa tecnologia com o MNI, identificando na seção de avaliação e resultados de que forma o PBAD pode beneficiar o MNI e o processo judicial eletrônico como um todo.

5.1 RESUMO CRIPTOGRÁFICO

O resumo criptográfico é a tecnologia responsável por calcular o resumo de uma mensagem. Este resumo é uma pequena sequência de bytes de tamanho fixo. Para uma determinada mensagem, o resumo criptográfico pode ser como uma impressão digital da mesma, ou seja, uma forma única de representação da mensagem. (PAAR; PELZL; 2009). A troca de um único bit da mensagem já é o necessário para causar a alteração do resultado de uma função de resumo criptográfico.

São diversos os usos de funções de resumo criptográfico. Eles são uma parte essencial dos esquemas de assinatura digital e de autenticações de mensagem. São bastante utilizados, também, em outros serviços, como armazenamento de senhas e derivação de chaves (PAAR; PELZL; 2009).

Resumos criptográficos também podem ser utilizados para verificar a integridade de informações, ou seja, verificar se a informação não foi alterada. Devido ao resumo criptográfico prover uma forma única de representação da informação, qualquer alteração pode ser identificada através desta tecnologia. (FERGUSON; SCHNEIER; KOHNO, 2011).

5.2 INFRAESTRUTURA DE CHAVES PÚBLICAS (ICP)

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).

Esta infraestrutura assume que a identidade do receptor pode ser assegurada através de certificados digitais e algoritmos assimétricos. Portanto, a 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 (HARRIS, 2010).

Qualquer pessoa que deseja participar de uma 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 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.

Uma ICP provê suporte a serviços de autenticidade, confidencialidade, não repúdio, e integridade.

5.2.1 Infraestrutura de Chaves Públicas Brasileira

Por meio da implantação 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 Padrão Brasileiro de Assinatura Digital (PBAD) (ITI, 2012).

5.2.2 Certificado Digital

O certificado digital é um dos pontos mais importantes dentro de uma 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).

O padrão que a AC utiliza para criar certificados é o X.509, que determina os diferentes campos utilizados no certificado e os valores que podem ser populados nestes campos. Atualmente, este padrão está na versão 4, que é frequentemente denotada como x.509v4. Muitos protocolos criptográficos utilizam este tipo de certificado, incluindo o SSL (HARRIS, 2010).

As principais informações encontradas nos certificados digitais são: número serial, número da versão, informações de identidade do titular, informações de algoritmos, data de emissão e expiração, e uma assinatura da autoridade emissora (HARRIS, 2010).

A ICP-Brasil hoje conta 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).

De acordo com o Quadro 3, os tipos de certificados A1 e S1 exigem regras menos rígidas, e os tipos A4, S4, e T4 exigem regras mais rigorosas, consequentemente, provendo maior nível de segurança. Os certificados tipo A e T são utilizados para assinaturas digitais, e os de tipo S são utilizados para sigilo. Sendo que, os de tipo A e S são utilizados por pessoas físicas, pessoas jurídicas, equipamentos ou programas, e os de tipo T podem ser utilizados unicamente por equipamentos das Autoridades de Carimbo de Tempo (ACTs) (ITI, 2014). O Quadro 3 é adaptado de ITI (2014) e apresenta as diferenças principais entre esses certificados.

Duas formas de checar se o certificado digital correspondente a um determinado signatário é válido, é via utilização das Listas de Certificados Revogados (LCRs), ou através do *Online Certificate Status Protocol* (OCSP).

Quadro 3- Tipos de Certificados Digitais

Tipo do Certificado	Geração da Chave Privada	Armazenamento da Chave Privada
A1 e S1	Software	Repositório protegido por senha e/ou identificação biométrica
A2 e S2	Software	Cartão Inteligente ou Token
A3 e S3	Hardware	Cartão Inteligente ou Token
A4 e S4	Hardware	Hardware criptográfico homologado junto à ICP-Brasil
T3 e T4	Hardware	Hardware criptográfico homologado junto à ICP-Brasil

5.2.3 Lista de Certificados Revogados (LCR)

A LCR, como o próprio nome sugere, é uma base de dados que contém uma lista de certificados revogados. O indivíduo que pretende verificar a validade de um certificado digital deve verificar a LCR para constatar se o certificado em questão é valido ou já foi revogado. Isto se a ICP ao qual o certificado pertence utilizar este tipo de tecnologia para revogação dos certificados.

Uma vez que um certificado é adicionado à LCR, transações envolvendo o mesmo não serão mais autorizadas. Revogação é muito confiável, e não existe um limite de quantos certificados podem ser revogados (FERGUSON; SCHNEIER; KOHNO, 2011).

5.2.4 Online Certificate Status Protocol

Outra forma de verificar a revogação dos certificados é a verificação online de certificados. Esta é baseada no *Online Certificate Status Protocol* (OCSP).

Para verificar um certificado, por exemplo, Alice consulta uma parte confiável, como uma Autoridade Certificadora ou uma outra parte

delegada, com o número serial do certificado em questão. A parte confiável verifica o estado do certificado em sua própria base de dados e então, envia uma resposta assinada para Alice. Alice conhece a chave pública da parte confiável e com isso pode verificar a assinatura da resposta obtida. Se a parte confiável diz que o certificado é válido, Alice agora é capaz de saber que o mesmo não está revogado (FERGUSON; SCHNEIER; KOHNO, 2011).

5.3 PADRÃO BRASILEIRO DE ASSINATURA DIGITAL (PBAD)

O Padrão Brasileiro de Assinatura Digital (PBAD) é definido pela ICP-Brasil, e tem como objetivo impor as regras de validação e criação de assinaturas digitais no âmbito da ICP-Brasil. Esse padrão é descrito através do conjunto normativo DOC-ICP-15 (ITI, 2012), sendo composto por quatro documentos. São eles:

DOC-ICP-15: Visão Geral sobre Assinaturas Digitais na ICP-Brasil;

DOC-ICP-15.01: Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil;

DOC-ICP-15.02: Perfil de uso geral para assinaturas digitais na ICP-Brasil;

DOC-ICP-15.03 Requisitos das políticas de assinatura digital na ICP-Brasil.

Nestes documentos é encontrada toda e qualquer informação sobre como gerar e verificar uma assinatura digital no contexto do PBAD. Através da compreensão e interpretação destes documentos é possível reconhecer 10 diferentes perfis de assinaturas digitais (5 em formato CAdES e 5 em formato XAdES).

5.3.1 Formatos de Assinatura Digital

Toda assinatura digital possui um formato. Este formato representa a codificação na qual a assinatura é desenvolvida. No PBAD os formatos utilizados são dois: CAdES (*CMS Advanced Electronic Signatures*) e XAdES (*XML-DSig Advanced Electronic Signatures*).

Uma assinatura eletrônica, criada através da utilização desses dois formatos, pode ser aplicada para decisões, em casos de disputas entre o signatário e o verificador, que podem ocorrer em um momento futuro, mesmo anos mais tarde.

Abaixo, é apresentada a definição destes formatos:

CAdES: Este formato pode ser considerado uma extensão da RFC 3852 e RFC 2634. É um formato de assinatura eletrônica que pode permanecer válida por longos períodos, incluindo evidências sobre sua validade, mesmo se as partes interessadas tentarem negar a validade da assinatura (PINKAS; POPE; ROSS, 2008). Este formato utiliza a codificação ASN.1 (*Abstract Syntax Notation One*).

XAdES: Estende o formato definido em *XML-DSig* dentro do contexto de assinaturas eletrônicas que permanecem válidas por longos períodos. Este formato inclui evidências sobre a validade da assinatura mesmo se o signatário ou verificador tentar negar (repudiar) a sua validade. (EASTLAKE, 2002). A codificação utilizada é XML (*eXtensible Markup Language*).

5.3.2 Perfis de Assinatura Digital

Para a construção de cada perfil é necessário uma Política de Assinatura (PA) diferente, buscando adaptar as regras de acordo com os campos de aplicação de cada PA. Todos os perfis existentes no PBAD e seus respectivos campos de aplicação são destacados abaixo. É importante ressaltar que cada perfil apresentado se equivale para CAdES e XAdES, sendo a única diferença o formato da assinatura.

a) Assinatura Digital com Referência Básica (AD-RB): Este perfil de assinatura deve ser utilizado em processos em que o período de validação dos dados seja executado durante o prazo de validade dos certificados dos signatários (ITI, 2012a).

b) Assinatura Digital com Referência do Tempo (AD-RT): Este perfil de assinatura deve ser utilizado em processos que necessitam de segurança quanto à irretratabilidade do momento da assinatura. Este perfil deve ser utilizado quando as referências e os dados para validação da assinatura puderem ser obtidos por meios externos, de maneira inequívoca (ITI, 2012a).

c) Assinatura Digital com Referências para Validação (AD-RV): Este perfil contém no corpo da assinatura as referências para validação. Deve ser utilizado em processos nos quais a

assinatura possa ser verificada a qualquer momento e os dados necessários para validação (cadeia de certificação e estado de revogação) possam ser recuperados por meio externo ao corpo da assinatura. Além de prover segurança quanto à irretratabilidade do momento de assinatura, permite que ocorra verificação da assinatura quando o certificado da AC que emitiu o certificado do signatário seja comprometido, desde que tenha sido utilizado um carimbo de tempo sobre as referências de validação antes do período de comprometimento (ITI, 2012a).

d) Assinatura Digital com Referências Completas (AD-RC): Este perfil contém no corpo da assinatura, além das referências para validação, a cadeia de certificação e o estado de revogação do certificado do signatário no corpo da assinatura. Deve ser utilizado em negócios nos quais a validação da assinatura deva ser realizada a qualquer momento, devido ao fato de todos os dados necessários para validação estarem autocontidos na própria assinatura. Provê segurança quanto à irretratabilidade do momento de assinatura e também permite que ocorra validação da assinatura quando o certificado da AC que emitiu o certificado do signatário seja revogado, desde que exista um carimbo de tempo sobre as referências de validação antes deste comprometimento (ITI, 2012a).

e) Assinatura Digital com Referências para Arquivamento (AD-RA): Este perfil deve ser utilizado em processos que precisam ter o conteúdo digital assinado arquivado por longos períodos. Provê segurança contra a fraqueza dos algoritmos, funções de resumo, e tamanho de chaves criptográficas ao longo do tempo, mas para isso carimbos do tempo de arquivamento devem ser aplicados tempestivamente. Provê segurança quanto à irretratabilidade do momento de assinatura e também permite que ocorra validação da assinatura quando o certificado da AC que emitiu o certificado do signatário seja revogado, desde que exista um carimbo de tempo sobre as referências de validação antes deste comprometimento (ITI, 2012a).

5.3.3 Política de Assinatura (PA)

Segundo Ross (2001), uma PA é um conjunto de regras impostas para a criação e verificação de assinaturas eletrônicas, para que a validade da assinatura possa ser verificada.

Uma PA deve existir em formato textual (compreensível por ser humano) e em formato de máquina. O objetivo de uma PA em formato textual é tornar viável a avaliação das suas exigências legais e o contexto contratual no qual a mesma está sendo aplicada. Já para as PAs em formato de máquina, o objetivo é permitir a automação do processo de uma assinatura eletrônica (tanto para criação, quanto para verificação).

Os principais campos dentro de uma PA são:

- Identificador da Política de Assinatura;
- Data de Emissão;
- Nome da Entidade Emissora da Política de Assinatura;
- Campo de Aplicação;
- Política de Validação da Assinatura (inclui as regras de validação/verificação da PA);
- Informações Adicionais sobre a Política de Assinatura;

A forma de identificação de uma PA é feita através de uma referência global única, que pode ser um identificador único da política (*object identifier*), seu próprio resumo criptográfico, ou outra forma existente de representá-la unicamente. Essa referência é adicionada dentro da estrutura da assinatura, para posterior identificação da PA no momento de validação.

No PBAD existem 10 PAs, cada uma corresponde a um perfil de assinatura apresentado acima, sendo que cada um desses perfis são definidos por duas políticas, uma que define o uso do formato CAdES e outra que determina o uso do formato XAdES. No contexto da ICP-Brasil a PA é parte essencial no processo de assinatura digital, seus requisitos devem ser obrigatoriamente cumpridos, para gerar assinaturas válidas, e poder verificá-las corretamente.

O acesso às PAs é fundamental para gerar e verificar as assinaturas digitais. Assim, o ITI desenvolveu a Lista de Políticas de Assinaturas Aprovadas (LPA), responsável por conter todas as PAs existentes. O acesso a essa lista é disponibilizado pelo próprio ITI, e sua definição consta no conjunto normativo DOC-ICP-15 (ITI, 2012a).

5.3.4 Algoritmos de Resumo Criptográfico

Apenas alguns algoritmos de resumo criptográfico e de assinatura digital podem ser utilizados dentro do PBAD. Os algoritmos de resumo criptográfico permitidos são SHA-1, SHA-256, e SHA-512.

Os algoritmos de assinatura digital aceitos para os certificados de usuários finais são: sha1WithRSAEncryption, sha256WithRSAEncryption, sha256WithECDSAEncryption, sha512WithRSAEncryption, e sha512WithECDSAEncryption.

Qualquer assinatura gerada que não utilize algum desses algoritmos não se enquadra dentro do PBAD, comprometendo, assim, a validade da assinatura.

5.3.5 Encapsulamento da Assinatura Digital

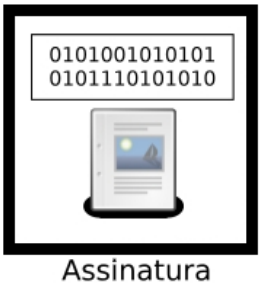
Encapsulamento da assinatura digital é o conceito que determina se o conteúdo assinado está inserido no mesmo documento (arquivo) da assinatura, ou se o conteúdo assinado e a assinatura estão em documentos (arquivos) separados.

Este segundo caso, pode ser utilizado, por exemplo, havendo a necessidade de se transferir o arquivo de assinatura via rede e os recursos para transmissão sejam limitados, possibilitando, assim, que o tamanho do arquivo que contém a assinatura possa ser reduzido (em bytes) significantemente, viabilizando a transmissão do arquivo assinado. Assim, o documento (arquivo com conteúdo assinado) não precisará ser necessariamente transferido com o arquivo de assinatura, podendo ser obtido de qualquer outra forma, e a validação desta assinatura poderá ser feita sem problemas consequentes da separação das partes.

Através da utilização deste conceito, podemos ter diferentes tipos de encapsulamento para as assinaturas digitais. Atualmente, no PBAD, têm-se quatro tipos de encapsulamento diferentes, são eles:

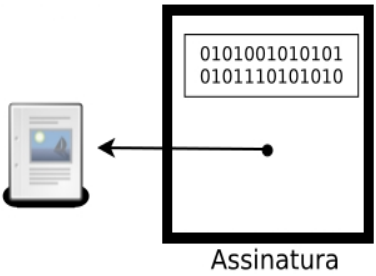
Assinatura Anexada: o conteúdo assinado está dentro da estrutura da assinatura. Utilizada apenas para assinaturas no formato CAdES.

Figura 2 - Assinatura Anexada



Assinatura Destacada: o conteúdo assinado está fora da estrutura da assinatura. Utilizada em ambos os formatos, CAdES e XAdES.

Figura 3 - Assinatura Destacada



Assinatura Encapsuladora: o conteúdo está dentro da estrutura da assinatura. É semelhante, conceitualmente, ao tipo anexada, porém estruturalmente são bastante diferentes. Utilizada apenas para assinaturas no formato XAdES.

Figura 4 - Assinatura Encapsuladora

Assinaturas Embarcadas: a assinatura está incluída na estrutura do documento que foi assinado. Esse tipo de assinatura só existe para documentos XML. Utilizada apenas para assinaturas no formato XAdES.

Figura 5 - Assinatura Embarcada

5.3.6 Processo de Assinatura Digital

A assinatura digital é o processo de criptografar um resumo criptográfico com uma chave criptográfica privada. (HARRIS, 2010). Para compreender este processo é apresentado aqui o funcionamento da assinatura digital, através do exemplo abaixo e da Figura 2, que esclarecem os conceitos e procedimentos envolvidos na etapa de criação e verificação criptográfica da assinatura.

Esclarecendo o Procedimento Criptográfico de Assinatura Digital, apresentado na Figura 6, no qual o remetente é Lucas e o receptor Laura:

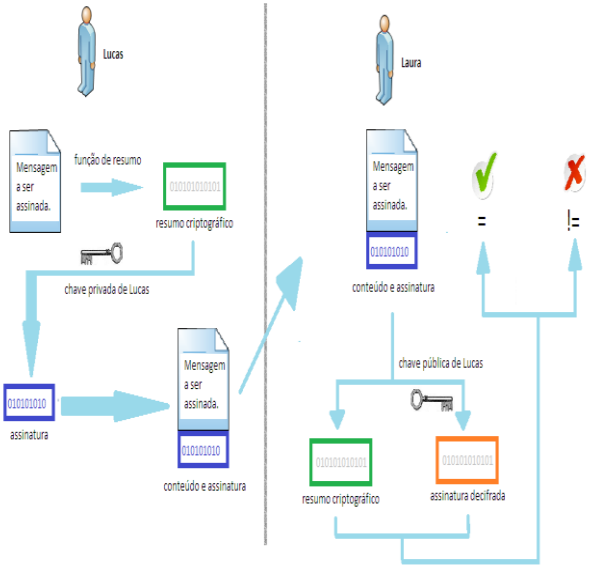
Lucas deseja enviar uma mensagem para Laura e quer garantir que a mensagem não seja modificada e que Laura tenha certeza que a mensagem foi enviada realmente por ele. Para isto, Lucas pode assinar digitalmente esta mensagem. Isso significa que uma função de resumo criptográfico deve ser aplicada à mensagem, e o seu resultado deve ser cifrado com a chave privada de Lucas. Como visto, essa chave criptográfica é disponibilizada pela ICP a qual os dois são membros, e é

de uso único e exclusivo de Lucas. Após a assinatura ser feita, Lucas pode enviar a mensagem à Laura.

No momento em que Laura for verificar a mensagem recebida, ela deverá utilizar a mesma função de resumo criptográfico que Lucas utilizou e armazenar esta informação. Após essa operação, Laura deverá decifrar o valor da assinatura digital realizada por Lucas, utilizando a chave pública dele, que é conhecida por todos os membros da ICP, através do certificado digital de Lucas. Ela deve comparar o valor do resumo criptográfico obtido nesta operação com o valor do resumo criptográfico que ela tem armazenado. Se os valores forem os mesmos ela pode ter certeza que a mensagem não foi alterada durante o processo de transmissão e que realmente foi enviada por Lucas (SILVEIRA, 2011). Essa verificação garante a validade por meio dos mecanismos criptográficos presentes na assinatura.

Para esta assinatura ser válida no âmbito do PBAD só isto não é suficiente. Além desta verificação, é preciso validar a Política de Assinatura utilizada pelo signatário, para ter certeza que as tecnologias e os procedimentos utilizados estão de acordo com os determinados pela ICP-Brasil. Dentro destas regras estão envolvidos, protocolos de criptografia, algoritmos de hash, período de validade da política, entre outros.

Figura 6 - Processo Criptográfico de uma Assinatura Digital.



O grande benefício para a verificação da PA ser parte integrante da validação da assinatura, além de obrigar o uso de tecnologias atuais e conforme os padrões estabelecidos pela ICP-Brasil, é o fato de prover interoperabilidade. Por seguir uma PA, e consequentemente um conjunto de regras de geração e validação de assinaturas, todos os sistemas devem estar de acordo com esta PA para operar dentro do PBAD. Desta maneira, todo sistema conforme com o PBAD saberá reconhecer a semântica das assinaturas, e desta forma, validá-las independente do sistema em que a assinatura é gerada e verificada.

6. AVALIAÇÃO DO MODELO NACIONAL DE INTEROPERABILIDADE DE DADOS DO PODER JUDICIÁRIO

A análise proposta e os resultados gerados neste trabalho são apresentados em quatro etapas distintas. A primeira etapa, apresentada na subseção 6.1, faz uma análise crítica expondo argumentos técnicos sobre a iniciativa o CNJ em impor a utilização de um SGPJE único no poder judiciário.

A segunda etapa, manifestada na subseção 6.2, realiza uma avaliação sobre os mecanismos de controle de acesso do MNI, apontando como resultado que seja imposto como requisito obrigatório a utilização do PBAD no MNI para autenticação dos serviços prestados, para prover maior segurança e interoperabilidade ao acesso dos dados.

A etapa três (seção 6.3) é baseada no *framework* de Ray (2011). Esse *framework* produz critérios de avaliação que permitem realizar análises qualitativas sobre modelos de interoperabilidade em e-government. Todos os critérios de avaliação definidos neste framework são utilizados nesta análise. Os resultados gerados nesta etapa são apresentados através de sugestões de melhorias para cada um dos critérios avaliados.

Por fim, a quarta etapa é apresentada. Esta avaliação utiliza a categorização de níveis de interoperabilidade definida neste trabalho (seção 4), baseada no *European Interoperability Framework* (EIF) (ISA, 2010). Por meio desta categorização, o resultado obtido nesta análise é a identificação do nível de interoperabilidade que o MNI atinge.

6.1 ANÁLISE SOBRE SGPJE ÚNICO

Como visto, para que os processos judiciais sejam executados em meio eletrônico, eles precisam rodar sobre algum tipo de software. No Brasil, estes softwares são conhecidos como Sistemas de Gestão de Processo Judicial Eletrônico (SGPJE), e têm por objetivo viabilizar a prática de atos processuais, bem como o acompanhamento de ações judiciais de forma segura, proporcionando o gerenciamento dos documentos eletrônicos envolvidos no processo.

As instituições do sistema judiciário brasileiro, instâncias, tribunais, e demais órgãos gestores, têm autonomia para utilizar o SGPJE que acreditam ser o mais adequado e eficaz para cumprir suas determinações políticas e técnicas. Desta forma, uma grande variedade de SGPJE estão em execução na justiça brasileira. Por um lado, a

diversidade de SGPJE provê maior segurança às informações eletrônicas do judiciário, por outro, não proporciona intercomunicação sistêmica entre os órgãos de justiça, criando um gap na tramitação dos processos.

O CNJ, por meio de algumas medidas, procura tornar o PJe um SGPJE único dentro do sistema judiciário brasileiro (CONJUR, 2013). O fato da obrigação de todos os órgãos judiciais trabalharem com um SGPJE único pode acarretar alguns problemas técnicos advindos dessa imposição. Esses problemas precisam ser levados em consideração para poder melhor avaliar os impactos dessa medida. Assim, esta seção traz uma análise sobre estes fatos, apresentando pontos de vista diferentes sobre esta situação.

O fato dos SGPJE serem heterogêneos, implementados de forma independente por meio de tecnologias diversificadas, dificulta o comprometimento das informações judiciais por intermédio de agentes maliciosos (hackers), sendo este um excelente benefício em termos de segurança computacional. Além disto, a variedade sistêmica proporciona aos tribunais, e demais órgãos da justiça, optar pelo sistema que melhor atende seus requisitos de negócio, como: segurança, processamento de dados, portabilidade, e outros.

Analisando sob outra ótica, essa diversidade acarreta alguns problemas. Conforme apresentado na seção 2, a estrutura judiciária brasileira possui 3 graus, os quais necessitam comunicar-se para que a tramitação dos processos ocorra de forma automatizada. Este fato, aliado ao grande número de sistemas, tem gerado transtornos. A falta de comunicação entre os órgãos do judiciário e a diversidade de interfaces para os usuários vêm causando descontinuidades e retrabalho.

Em alguns casos, é necessário imprimir todos os documentos envolvidos no processo eletrônico para papel, para assim poder submeter a uma esfera superior e, a partir disto, digitalizar novamente o processo em um novo sistema. Este fato faz com que a celeridade e a segurança do processo sejam comprometidas, não sendo a maneira mais eficiente de conduzir o processo.

Para solucionar esta questão, muitos defendem a ideia da utilização de um sistema único. Porém, este não é o melhor caminho. Como dito anteriormente, possíveis falhas em um sistema único poderiam deixar todo o sistema judiciário vulnerável a ataques, comprometendo as informações inerentes aos processos judiciais. Além disso, todo um retrabalho que deve ser feito e o custo disso, em tempo e dinheiro.

Sendo assim, há um impasse: A diversidade de sistemas é benéfica para a segurança da informação, mas não para a comunicação.

A adoção de um sistema único é o inverso. Para resolver esta questão, a interoperabilidade é fundamental. Ela pode solucionar os problemas de comunicação entre os sistemas heterogêneos e manter os benefícios proporcionados pela diversidade. Por conta disto, a utilização do MNI é fundamental para o aperfeiçoamento do processo judicial eletrônico no Brasil.

Um outro fato que deve ser observado é que mesmo com a implementação de um sistema único a interoperabilidade não é garantida. O SGPJE que o CNJ tenta impor como único é o PJe e por este ser um sistema livre (open source), permite que os órgãos encarregados de sua utilização promovam novas atualizações e alterações no sistema por conta própria, para adequar o modelo ao seu plano de gestão. O problema é que essas alterações e atualizações por vezes não seguem um modelo específico de interoperabilidade, ocasionando falta de interoperabilidade entre o próprio PJe.

Com isso, o MNI não seria exclusivamente para aplicar a interoperabilidade aos diferentes SGPJE, mas também entre os mesmos SGPJE que sofreram possíveis modificações. Com esta análise, identifica-se que o MNI é essencial mesmo em casos que os órgãos da justiça operem com o mesmo SGPJE.

6.2 AVALIACAO E RESULTADOS BASEADOS NO PBAD

O PBAD pode prover diversos melhoramentos com relação à segurança e à interoperabilidade dos sistemas processuais. Aqui são apresentados diversos benefícios advindos com a possível aderência deste modelo. Problemas ocasionados pela falta de utilização deste padrão na justiça eletrônica também são identificados.

Como exposto anteriormente, na seção 4, o MNI permite o controle de acesso às informações judiciais de duas maneiras: certificação digital ICP-Brasil, ou seja, através do PBAD; ou por meio de *login* e senha. A autenticação via *login* e senha não produz a mesma segurança informacional aos processos eletrônicos que o PBAD.

Atente-se para o fato de que para o método de *login* e senha ser aplicado é necessário existir um banco de dados que contenha as informações de todos os usuários, incluindo seus *logins* e suas respectivas senhas. Caso contrário, não é possível fazer autenticação no sistema.

Sabendo disto, se eventualmente um *hacker* (usuário malicioso com grandes conhecimentos) invadir esse banco de dados e obter as senhas dos usuários, pode conectar-se indeterminadamente ao sistema,

inclusive, propagando essas informações a terceiros. Caso as evidências dessa invasão sejam completamente apagadas pelo hacker, o que é possível computacionalmente, os usuários e gestores do sistema não terão conhecimento sobre esta invasão. Assim, este *hacker* terá livre acesso para manipular o sistema, podendo, inclusive, decretar sentenças, alterar informações sensíveis, entre outros abusos.

Na verdade, ninguém pode garantir que isto já não aconteceu. Esse fato proporciona a espionagem e manipulação de outros governos sobre as informações que tramitam no sistema judiciário brasileiro. Para evidenciar esta constatação, as denúncias de espionagem da Agência Nacional de Segurança dos Estados Unidos (NSA) sobre informações confidenciais do governo brasileiro alertam para a falta de segurança na proteção dos dados no país, servindo de motivação para o melhoramento destes procedimentos (Portal G1, 2013).

Na autenticação realizada através do PBAD, as senhas não podem ser capturadas tão facilmente. Aqui, a chave privada do signatário (usuário) corresponde à senha no método anterior. Nos níveis mais altos de segurança providos pela ICP-Brasil, é possível que a chave privada seja gerada e armazenada apenas dentro de dispositivos criptográficos, que podem ser cartões inteligentes (*smart cards*), ou *tokens USB* (*pen drives*). Para isto, é indispensável a utilização de certificados digitais A3 ou A4, emitidos pela ICP-Brasil.

Esses dispositivos criptográficos são mídias físicas (*hardwares)*, portanto, não estão disponíveis na internet, ou qualquer outra rede de computadores que possa ser acessada por *hackers* e ter os dados comprometidos. Para obter sucesso no acesso às informações processuais ligadas ao MNI, é preciso ter posse da chave privada do usuário. Esta chave é armazenada em uma única mídia, sob posse apenas do usuário (proprietário e responsável pelo certificado digital), tornando o processo para obtenção da chave mais seguro.

Outros pontos que proveem mais segurança e benefícios em relação à utilização exclusiva do PBAD para controle de acesso no MNI são:

Existem **mecanismos criptográficos** para proteção das informações contidas nesses dispositivos. Algoritmos de hash e algoritmos de criptografia, sempre atualizados através das políticas de certificação digital da ICP-Brasil;

A **liberação de uso da chave privada** contida no dispositivo só é realizada mediante confirmação de senha, que pode ser uma sequência de símbolos (*bytes*) definidos no momento de geração da chave privada. Essa senha permanece armazenada apenas dentro do dispositivo. Essa

liberação também pode ser executada através do uso de biometria, dependendo da política de segurança de cada órgão.

A **emissão do certificado e da chave privada** é realizada por uma parte confiável dentro da ICP, uma Autoridade Certificadora credenciada pela ICP-Brasil.

As informações ligadas aos dispositivos criptográficos são únicas. Os mecanismos de criptografia asseguram que nenhum outro dispositivo criptográfico portará a mesma chave privada contida em um dispositivo em funcionamento.

A **unicidade** é garantida. Conforme as determinações de uma ICP, o cartão (ou token) é único e intransferível. Necessariamente, o usuário deve ter posse do seu dispositivo criptográfico no momento em que tentar acessar o sistema. Assim, duas pessoas não poderão acessar este sistema ao mesmo tempo por meio de um único nome usuário. Tentativas para violar este cartão e obter a chave privada são detectáveis. A unicidade dificulta a forja de identidade no acesso ao sistema e, consequentemente, o acesso de intrusos.

Revogação de certificado: Caso o cartão seja perdido, ou roubado, facilmente este certificado pode ser revogado, bloqueando o acesso de qualquer pessoa que pretenda utilizar este cartão sem autorização. Isso prova **não-repúdio**, aumentando ainda mais o nível de confiança do sistema. O não-repúdio impede que ações tomadas sejam negadas em um tempo posterior.

Temporalidade: Através da utilização de determinados perfis de assinatura do PBAD, a temporalidade é garantida. Os perfis do PBAD que têm por objetivo a irretratabilidade do momento de geração da assinatura são: AD-RT, AD-RV, AD-RC, e AD-RA. Cada perfil possui um grau diferente de segurança, conforme apresentado na subseção 5.3.2.

Interoperabilidade: Além de todos os benefícios apresentados advindos da utilização exclusiva do PBAD para autenticação dos serviços do MNI, o PBAD proporciona interoperabilidade entre as assinaturas digitais no âmbito da ICP-Brasil. Desta forma, a interoperabilidade no controle de acesso aos sistemas que implementam o MNI seria garantida. Em outras palavras, é possível identificar em qualquer SGPJE se o sistema terá mecanismos suficientes para reconhecer o usuário, sem problemas de compatibilidade. O PBAD provê interoperabilidade semântica aos sistemas de gestão de assinatura digital que o implementam. Segundo Silveira (2011), o maior ganho com a implementação desse padrão é a interoperabilidade.

Integridade e Autenticidade: Caso algum documento seja alterado é possível perceber. Assim como ter conhecimento de quem fez a alteração.

O método de *login* e senha, permitido pelo MNI, não garantem unicidade, não repúdio, temporalidade, integridade, autenticidade, e interoperabilidade dos dados. Por meio das fragilidades desse método, o *hacker* tem o seu "serviço" facilitado, podendo de forma menos complexa consultar e controlar processos judiciais eletrônicos, alterar resultados de sentenças, apagar informações importantes de processos, e diversas outras ações obscuras.

Deste modo, considerando as argumentações feitas, recomenda-se a utilização única e exclusiva do PBAD para controle de acesso do MNI, assim como a aplicação deste padrão em todos os documentos eletrônicos que tramitam no judiciário, salvo aqueles que não têm significância suficiente para tal nível de segurança. De modo consequente, sugere-se a abolição do método de *login* e senha para controle de acesso.

Ressalta-se que a determinação de uso obrigatório do PBAD para controle de acesso às informações que são operadas através do MNI não garantem que os SGPJE não poderão ser invadidos, mas tornarão este processo mais difícil, elevando o nível de proteção dos dados, para reduzir os riscos de comprometimento dos processos judiciais eletrônicos.

6.3 AVALIACAO E RESULTADOS BASEADOS NO FRAMEWORK DE RAY

O framework de Ray é uma importante ferramenta para analisar modelos de interoperabilidade em governo eletrônico. Optou-se pelo modelo de Ray por considerar que ele cobre um conjunto de definições de interoperabilidade em e-gov mais amplo. Todos os outros trabalhos citados na subseção 4.4 identificam critérios de avaliação de interoperabilidade em e-gov, porém nenhum deles consegue abordar todos os quesitos apresentados por Ray. O framework de Ray consegue cobrir todos os critérios apresentados nos demais trabalhos mencionados anteriormente.

As subseções abaixo são tituladas conforme as camadas/critérios de avaliação identificados por Ray. Esses critérios permitem executar uma avaliação qualitativa do MNI. Todas as subseções identificam o contexto no qual o critério está inserido, a avalição desenvolvida, e uma sugestão de melhoria, caso seja aplicável.

6.3.1 Background

A camada de *background* não leva em consideração requisitos técnicos, mas sim os aspectos legais e institucionais envolvidos na iniciativa de implantação de um novo modelo de interoperabilidade em e-gov.

Avaliação: Com relação a estes aspectos o MNI está bem amparado. A Resolução Conjunta Nº 3 (CNJ, 2013c), e o termo de cooperação técnica número 58 (CNJ, 2009), tratam as questões legais e institucionais relacionadas à criação e implementação deste modelo.

Sugestão de Melhoria: Não se aplica, dado que o MNI cumpre os requisitos inerentes a esta camada.

6.3.2 Escopo

A camada de escopo é responsável por apresentar a identificação do tipo de interação do modelo com o governo. Essas interações podem ser: Governo para Governo (G2G), Governo para Cidadão (G2C), Governo para Empresas (G2B), Governo para Empregados (G2E), Governo para Governo de Outros Países (GO).

Avaliação: O MNI não apresenta de forma explícita o seu escopo. Desta forma, não é claro o tipo de interação com o governo que ele propõe. Através de uma avaliação documental do modelo, identifica-se que o MNI trabalha com o tipo de interação G2G, já que as interações que acontecerão entre tribunais e outros órgãos de administração da justiça são evidentes. Outros tipos de interações com o governo não são claras; exemplo: a interação com o cidadão (G2C) e demais instituições privadas (G2B) não se pode afirmar se existem. Diferentes interpretações podem ser dadas para essas interações. Neste aspecto o MNI deixa a desejar.

Sugestão de Melhoria: Definir uma seção específica para descrever o escopo do MNI. Desta forma é possível conhecer em quais áreas a implantação do modelo irá impactar. Isso torna possível a realização de um planejamento das instituições e dos cidadãos que serão afetados pela implantação do MNI, diminuindo o impacto gerado pelas mudanças, aumentando a aceitação do modelo perante os órgãos de interação. Esta identificação pode ser adicionada como uma seção no documento: Modelo de Interoperabilidade de Dados do Poder Judiciário e Órgãos de Administração da Justiça (CNJ, 2013).

6.3.3 Políticas de Interoperabilidade Básicas

Acredita-se que esta é uma das camadas mais importantes dentro de um modelo de interoperabilidade. Aqui são definidas as políticas básicas de uso do modelo. Seguir as políticas de uso do modelo é fundamental para que a interoperabilidade seja alcançada.

Essas políticas são as diretrizes que os desenvolvedores e analistas devem seguir para que o modelo seja implementado de forma padrão por todas as partes envolvidas. Caso essas políticas não sejam definidas, dificilmente as implementações terão compatibilidade de dados.

Avaliação: Os arquivos/documentos do MNI são expostos pelo CNJ através de uma página *web* disponível no Portal CNJ (CNJ, 2014b). Em nenhum desses documentos é definida uma política de uso para o MNI. Esses documentos apresentam algumas tecnologias como requisitos para implementação do modelo, porém não existe uma determinação para as tecnologias, protocolos, e abordagens que podem, devem, ou não podem, não devem ser utilizadas para implantação do modelo.

Este fato afeta diretamente os desenvolvedores dos sistemas que, sem uma política definida, não têm um guia confiável para implementar o MNI. Possíveis problemas de interoperabilidade podem ser ocasionados por este motivo, dado que, para diminuir o risco de incompatibilidades de implementação, a presença das políticas básicas é essencial.

Sugestão de Melhoria: Implementar um documento específico que defina as políticas de uso e implementação do modelo, de forma emergencial. Essas políticas devem ser desenvolvidas em formato textual, para entendimento dos desenvolvedores, e também em linguagem de máquina, para que as validações das políticas possam ser automatizadas, para certificar que as implementações estão realmente de acordo com as definições estabelecidas nas políticas, diminuindo o risco de incompatibilidades sistêmicas. Um exemplo a ser seguido é o PBAD, que define políticas de uso concisas, em forma de texto e de máquina, sendo esta uma importante peça no processo de interoperabilidade.

6.3.4 Critérios para Seleção de Padrões

Esta etapa não é tão importante para prover interoperabilidade ao MNI, mas é interessante para futuras atualizações do MNI. Ela envolve

o processo de seleção dos padrões a serem utilizados no modelo, e pode ser útil para manter o MNI moderno.

O objetivo aqui não é a definição dos padrões empregados no MNI, mas sim a identificação dos critérios adotados para seleção desses padrões.

Avaliação: Com o passar dos anos, as tecnologias e protocolos de comunicação vão se depreciando. Alguns dos critérios utilizados para a definição de um padrão podem não ser mais suportados pelo mesmo. Nestes casos, uma análise sobre esta camada facilita a tomada de decisão dos gestores do MNI, para substituir padrões depreciados que estão em vigência. O MNI não define o processo e os critérios utilizados na definição dos padrões adotados, porém, como dito acima, a adoção deste procedimento pode auxiliar na manutenção do modelo.

Sugestão de Melhoria: Desenvolver uma seção dentro do documento que trata o MNI (CNJ, 2013) para abordar os critérios envolvidos no processo de seleção dos padrões.

6.3.5 Definição de Padrões Abertos

Nesta camada é tratada a definição de padrões abertos. Os padrões abertos têm o objetivo de prover interoperabilidade entre sistemas, sem cobrança de taxas de uso (*royalties*). Desta forma, a definição destes padrões é valorosa para o desenvolvimento de um modelo de interoperabilidade em e-gov.

Avaliação: O MNI define como padrão aberto para comunicação de dados a linguagem XML, através de esquemas XML e *webservices*. A linguagem XML foi desenvolvida para prover interoperabilidade. É uma tecnologia madura, extensível, publicamente acessível, e gratuita. Essas características fazem com que o MNI cumpra os requisitos dessa camada para a comunicação dos dados. Contudo, o MNI não define padrões abertos para obter interoperabilidade em outras áreas relevantes. Cita-se como exemplo os padrões para definição de usabilidade, segurança, disponibilidade, armazenamento e gerenciamento dos dados. As definições desses padrões agregam qualidade ao MNI, aumentando o nível de integração entre os SGPJE.

Sugestão de Melhoria: Definir mais padrões abertos para obter interoperabilidade nas áreas mencionadas acima. Essas definições devem ser aplicadas ao documento do MNI (CNJ, 2013), e também às políticas de uso, sugeridas na seção 6.2.5, em formato textual e de máquina.

6.3.6 Padrões de Tecnologia

Os padrões de tecnologias definidos aqui são constituídos por um conjunto mínimo de normas técnicas que devem estar em conformidade com as políticas adotadas pelo modelo. Deve abranger todos os níveis interoperáveis do modelo.

Avaliação: Este é mais um quesito em que o MNI falha. Para começar, o MNI não adota políticas de uso, não podendo relacionar estes padrões com a política. Além disto, não é apresentado através dos arquivos do MNI, disponível no Portal CNJ (CNJ, 2014), nenhum documento que especifique um conjunto mínimo de regras para o desenvolvimento e implementação do MNI. Sem esta documentação fica complicado para os desenvolvedores trabalharem para construir um sistema interoperável. Isto abre portas para cada desenvolvedor optar por padrões tecnológicos distintos, o que pode afetar a interoperabilidade dos sistemas.

Sugestão de Melhoria: Deve-se construir um conjunto de políticas que tratem este assunto (conforme descrito no item 6.1.3), e posteriormente, criar um documento que aponte o conjunto mínimo de normas técnicas a serem seguidas pelos desenvolvedores, para que assim uma parte da interoperabilidade seja alcançada. Sem a definição explícita de um conjunto de requisitos técnicos, a interoperabilidade pode ser comprometida. Exemplo: Esta documentação pode ser exposta através de uma tabela, que define os padrões tecnológicos que devem, não devem, podem, e não podem ser utilizados. Isso ajudaria bastante os desenvolvedores no momento de criação e manutenção dos sistemas.

6.3.7 Padrões de Ciclo de Vida

Os padrões de ciclo de vida são significativos para tornar mais claro e eficiente o processo de criação e aprimoramento contínuo do modelo. Esses padrões são importantes para manter o nível de qualidade, auxiliando, por exemplo, na identificação e resolução de falhas.

Avaliação: O MNI não define nenhum padrão de ciclo de vida. A ausência deste padrão prejudica os desenvolvedores e analistas a executar tarefas de manutenção e atualização do MNI. Sem a presença deste padrão, o planejamento para aprimoramento do modelo será custoso.

Sugestão de Melhoria: É necessário que esta documentação seja criada. Indica-se utilizar um padrão de ciclo de vida para sistemas de

grande porte, devido ao fato do MNI ser um modelo robusto. Os ciclos deste padrão auxiliaram para melhora do MNI, permitindo que haja um processo de manutenção contínua do MNI. Exemplo: Inserção de novas tecnologias e remoção das tecnologias ultrapassadas.

6.3.8 Políticas de Gerenciamento e Conformidade

As políticas de gerenciamento e conformidade são utilizadas para garantir que o modelo seja revisado e atualizado regularmente, através da definição de uma estrutura para realização destas tarefas. Nesta estrutura, também devem estar dispostas as tecnologias e infraestruturas compatíveis/conformes com o modelo.

Avaliação: Essas políticas estão diretamente ligadas aos objetivos propostos pelos padrões de tecnologias e de ciclo de vida. Elas têm por objetivo o aprimoramento contínuo do MNI. Uma política de gestão e conformidade deve existir para garantir a durabilidade do modelo, assim como auxiliar os desenvolvedores na implementação do MNI, esclarecendo aspectos obrigatórios e recomendáveis para a implantação correta do modelo. Novamente, o MNI não cumpre os requisitos de mais uma camada.

Sugestão de Melhoria: Devem-se criar estruturas para definição destas políticas. É necessário que a política seja definida em formato compreensível por humanos e máquina. No primeiro caso, para que sirva de guia para os programadores interpretarem os requisitos da política e, no segundo, para que seja possível validar os requisitos de forma automatizada, através de um XML esquema por exemplo. Desta forma, o processo de desenvolvimento dos sistemas seria mais simples, tendo certeza que os requisitos obrigatórios estão implementados, para prover maior amadurecimento ao MNI.

6.4 ANÁLISE PARA IDENTIFICAÇÃO DO NÍVEL DE INTEROPERABILIDADE DO MNI

A identificação do nível de interoperabilidade do MNI é uma proposta inovadora. Nenhum outro trabalho foi identificado neste sentido, assim como as demais subseções de análise apresentadas neste capítulo.

Nesta subseção, é realizada uma análise que identifica o nível de interoperabilidade que o MNI atinge. A análise é baseada nas definições de níveis de interoperabilidade do *European Interoperability Framework* (ISA, 2010), conforme adaptação apresentada na seção

quatro. Assim, a classificação dos níveis de interoperabilidade é composta pelos níveis: técnico, sintático, semântico, organizacional, e legal, respectivamente.

Como visto, os níveis de interoperabilidade podem ser reconhecidos como um modelo de maturidade. Deste modo, é necessário atingir, primeiramente, o nível mais básico para alcançar o próximo nível. Abaixo são apresentadas as análises realizadas em cada nível. A última subseção apresentada (6.6.6) expõe a identificação do nível do MNI.

6.4.1 Interoperabilidade Técnica

A interoperabilidade técnica é comprometida no MNI, devido ao fato da indefinição de diversos protocolos para comunicação dos dados. Esse problema pode gerar incompatibilidades entre a comunicação dos SGPJE.

Algumas indefinições quanto a protocolos que afetam diretamente o alcance deste nível:

- Protocolo de gerenciamento de rede;
- Protocolo para transferência de arquivos;
- Protocolo para acesso a caixa postal (email);
- Protocolo para mensagens instantâneas;
- Protocolos de segurança de dados;
- Protocolo para sincronismo de tempo.

Um caminho para resolução desta questão é a implementação das políticas de interoperabilidade básicas, englobando a definição destes protocolos. Com uma boa política para determinar esses protocolos, os riscos de incompatibilidades nesse nível são mínimos.

As falhas apresentadas neste nível comprometem o alcance da interoperabilidade em todos os demais.

6.4.2 Interoperabilidade Sintática

O MNI implementa os componentes necessários para o alcance deste nível. O MNI utiliza, para o alcance deste nível, a linguagem XML para uniformização da sintaxe de dados, e um *webservice* para a troca de mensagens entre os sistemas. Esses componentes são identificados na seção quatro (4).

A falta de políticas básicas pode ocasionar problemas neste nível, devido ao fato dos requisitos obrigatórios e proibidos não serem identificados de maneira formal. A criação das políticas básicas podem gerar mudanças no código do *webservice*, para que o mesmo seja adaptado às políticas impostas. Assim, sem a criação dessas políticas não se pode atestar que os *webservices* cumprem as normas estabelecidas pelo MNI para prover interoperabilidade sintática.

Outra constatação são os problemas apresentados no nível técnico. Essas adversidades interferem diretamente neste nível, fazendo com que a interoperabilidade sintática não seja atingida.

6.4.3 Interoperabilidade Semântica

O nível semântico seria alcançado no MNI através da utilização dos esquemas XML propostos, denominados: intercomunicacao-2.2.2.xsd e tipos-servico-intercomunicacao-2.2.2.xsd. Esses esquemas permitem que o significado dos dados trocados sejam compreendidos pela aplicação que os está recebendo, garantindo que a informação seja trocada e, consequentemente, que o nível semântico seja atingido.

Porém, o mesmo problema que ocorre no nível sintático acontece aqui. Será necessária uma estruturação das políticas do modelo e das lacunas apresentadas no nível técnico, para assim evoluir e obter a interoperabilidade semântica.

Austrália, Brasil, Canada, Nova Zelândia, e Reino Unido, são países que têm iniciativas para prover interoperabilidade semântica em governo eletrônico. Eles definem metadados e controle de vocabulário. Para desenvolver soluções para este nível é interessante seguir a abordagem utilizada por esses países (RAY, 2011). A utilização de vocabulários controlados de dados, como o uso de ontologias, é uma alternativa para desenvolvimento deste nível.

O e-PMG e o e-PING podem ser analisados e levados em consideração para servirem como referência para o aprimoramento do MNI.

6.4.4 Interoperabilidade Organizacional

A interoperabilidade organizacional ainda está longe de ser alcançada pelo MNI. Nenhuma iniciativa ou proposta de atingir este nível é mencionada pelo modelo. É importante ressaltar, conforme esclarecido na seção 4.4, que a cobertura deste nível ainda é limitada em todo o mundo.

Austrália e Alemanha são países que se destacam pelas iniciativas de prover interoperabilidade organizacional nos seus governos, sendo alternativas de pesquisas para atingir a interoperabilidade organizacional (RAY, 2011).

6.4.5 Interoperabilidade Legal

Esse nível também está longe de ser alcançado pelo MNI. Conforme o item 4.5, conhecimento jurídico para atingir este nível já existe, porém a dificuldade está em alinhar as tecnologias com as leis. Diferente dos outros, este nível ainda está em um grau pouco explorado de pesquisas por todo o mundo. Não foram encontrados modelos e trabalhos de referências que poderiam ser utilizados como exemplos.

6.4.6 Identificação do Nível de Interoperabilidade

Conforme as análises realizadas, constatou-se que o MNI não está pronto para atingir nenhum nível de interoperabilidade. O nível mais básico de todos (nível técnico) apresenta falhas, como evidenciado na subseção 6.2.1.

O MNI contém as estruturas necessárias para alcançar os níveis sintático e semântico, porém necessita corrigir os problemas encontrados no primeiro nível, assim como aplicar as sugestões de melhorias apresentadas na subseção 6.2, para poder gerar interoperabilidade de fato. Sem corrigir estes problemas, as lacunas existentes podem ser fatais para a promoção de interoperabilidade entre os SGPJE.

7. CONCLUSÃO E TRABALHOS FUTUROS

Os esforços realizados para implementação deste trabalho compreenderam o levantamento do estado da arte para conceituação e classificação da interoperabilidade, em conjunto com a identificação do funcionamento da estrutura judiciária brasileira, para determinar a importância da implantação da interoperabilidade na justiça eletrônica, mais especificamente, nos SGPJE. Desta forma, mostrou-se que através da interoperabilidade e do aprimoramento do MNI pode-se obter grandes melhorias com relação a celeridade e eficiência na tramitação dos processos judiciais eletrônicos.

Para constatação dos problemas apresentados pelo MNI, utilizou-se o *Framework* de Ray (2011), evidenciando, através desta análise, que o MNI precisa ser aprimorado em muitos aspectos. Sendo os principais a falta de políticas básicas e políticas de gerenciamento e conformidade do MNI, para servirem como um guia de implementação aos desenvolvedores e de validação das tecnologias permitidas como modelo, a definição de um padrão de ciclo de vida para manutenção e aperfeiçoamento do MNI, e a definição de tecnologias e padrões abertos para prover interoperabilidade em áreas como segurança, armazenamento e gerenciamento dos dados. Para todos os problemas detectados, recomendações de melhorias foram apresentadas.

Como uma proposta inovadora, este trabalho identificou, por meio das análises apresentadas, o nível de interoperabilidade que o MNI atinge e, na verdade, foi constatado que o MNI apresenta problemas no nível técnico, o mais básico, comprometendo, assim, o alcance dos demais níveis. Desta maneira, pode-se dizer que o MNI não atinge nenhum nível de interoperabilidade. Quando corrigido os problemas evidenciados no primeiro nível, possivelmente o MNI atingirá o nível semântico, por ter definido e implementado as estruturas necessárias para o alcance deste nível, desde que também siga as recomendações de melhorias apresentadas através do *framework* de Ray.

O Padrão Brasileiro de Assinatura Digital (PBAD) foi apresentado. A importância deste padrão para prover maior segurança ao processo judicial eletrônico, assim como os benefícios de interoperabilidade agregados por meio da utilização do PBAD também foram identificados. É recomendado que a utilização deste padrão seja obrigatória, e o método de *login* e senha seja abolido como meio de autenticação no MNI, para assegurar o não-repúdio, temporalidade, unicidade, integridade, e autenticidade ao acesso e manutenção dos processos interligados ao MNI.

Fundado na iniciativa do CNJ em determinar a utilização de um SGPJE único através da e-*Justice*, uma análise expondo riscos relacionados ao comprometimento dos documentos judiciais eletrônicos é exposta, informando de maneira clara que a diversidade sistêmica é relevante para segurança do processo, além de mostrar que um sistema único pode não prover interoperabilidade ao judiciário.

Contudo, acredita-se que este trabalho é relevante para o aprimoramento do MNI, que de fato, não provê interoperabilidade. Medidas de aperfeiçoamento devem ser tomadas, para que após a implantação deste modelo não ocorram problemas. As recomendações de melhorias propostas nesta dissertação, assim como as análises qualitativas expostas, são informações importantes que devem ser utilizadas para composição de um modelo de interoperabilidade mais robusto e eficiente.

Acredita-se que o caminho para a e-*Justice* no Brasil é a interoperabilidade, provendo o destravamento da justiça e dando celeridade aos processos, aproximando a sociedade do Poder Judiciário. É importante ressaltar que os cuidados com a segurança dos dados são fundamentais para evitar o comprometimento de informações sensíveis, sendo um requisito que deve ser sempre lembrado e dado a devida importância.

7.1 TRABALHOS FUTUROS

Os trabalhos futuros para o aprimoramento dos temas aqui abordados são destacados abaixo:

- Criar um modelo de políticas de interoperabilidade básicas do MNI;
- Criar um modelo de políticas de gerenciamento e conformidade do MNI;
- Definir todos os protocolos de rede necessários para alcance do nível técnico;
- Estudar a possibilidade e os benefícios da aplicação de ontologias no MNI;
- Apresentar métodos para integração do MNI e do MoReq-Jus;
- Investigar possível integração do MNI com o E-Ping e os benefícios dessa integração;

- Apresentar análises comparativas entre o MNI e outros modelos de interoperabilidade (E-Ping, E-PMG, e-CODEX, GRP);
- Investigar a família ISO 27000 para prover outras recomendações de segurança.

REFERÊNCIAS

BEAUMASTER, Suzanne. **Local government IT implementation issues**: a challenge for public administration. In System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii Inter-national Conference on (pp. 1725-1734). IEEE.

BRASIL. Comitê Executivo de Governo Eletrônico. **e-PING - Padrões de Interoperabilidade de Governo Eletrônico.** Brasília, 2014. Disponível em: <http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em: 12 abr. de 2014.

BRASIL. Comitê Executivo de Governo Eletrônico. **e-PMG - Padrão de Metadados do Governo Eletrônico. Comitê Executivo de Governo Eletrônico.** Brasília, 2014a. Disponível em: <http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/padrao-de-metadados-do-governo-eletronico-e-pmg>. Acesso em: 12 abr. de 2014.

BRASIL. Presidência da República. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 out. 2014.

BRASIL. Presidência da República. **Lei nº 11.419**. Brasília, 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm>. Acesso em: 30 jun. 2014.

BRASIL. 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: 05 jun. 2013.

BRASIL. Presidência da República. **Conheça os órgãos que formam o judiciário.** Brasília, 2009. Disponível em: <http://www.brasil.gov.br/governo/2009/11/conheca-os-orgaos-que-formam-o-poder-judiciario>. Acesso em: 15 mar. 2015.

BRASIL. Presidência da República. **Evolução Histórica da Estrutura Judiciária Brasileira.** Brasília, 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/revista/Rev_05/evol_historica.htm>. Acesso em: 15 mar. 2015.

CARBONI, Nadia; VELICOGNA, Marco. **Electronic data exchange within European Justice:** a good opportunity?. International Journal for Court Administration, v. 4, n. 3, p. 104-120, 2012.

CNJ. Portal CNJ. **TRT4 comemora celeridade nos processos com a implantação do PJe.** Brasília, 2014. Disponível em: <http://www.cnj.jus.br/noticias/cnj/29442-trt-4-comemora-celeridade-nos-processos-com-a-implantacao-do-pje>. Acesso em: 07 jun. de 2014.

CNJ. Portal CNJ. **Modelo Nacional de Interoperabilidade.** Brasília, 2014a. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/eficiencia-modernizacao-e-transparencia/comite-nacional-da-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade>. Acesso em: 10 jul. de 2014.

CNJ. Portal CNJ. **Arquivos do Modelo Nacional de Interoperabilidade, version 2.2.2.** Brasília, 2014b. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/eficiencia-modernizacao-e-transparencia/comite-nacional-da-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade/arquivos-do-modelo-nacional-de-interoperabilidade>. Acesso em: 10 jul. de 2014.

CNJ. Portal CNJ. **Modelo de Interoperabilidade de Dados do Poder Judiciário e Órgãos de Administração da Justiça, version 2.2.2.** Brasília, 2013. Disponível em: <http://www.cnj.jus.br/images/dti/Comite_Gestao_TIC/Modelo_Nacional_Interoperabilidade/interoperabilidade_2.2.2.pdf>. Acesso em: 10 jul. de 2014.

CNJ. Portal CNJ. **Sobre o CNJ.** Brasília, 2013a. Disponível em: <http://www.cnj.jus.br/sobre-o-cnj>. Acesso em: 02 ago. de 2013.

CNJ. Portal CNJ. **Entenda o PJe.** Brasília, 2013b. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicial-eletronico-pje>. Acesso em: 09 set. de 2013.

CNJ. **Resolução Conjunta Nº 3**. Brasília, 2013c. Disponível em: <http://www.cnj.jus.br/atos-administrativos/atos-da-presidencia/567-resolucoes-conjuntas/24343-resolucao-conjunta-n-3-de-16-de-abril-de-2013>. Acesso em: 21 jul. de 2014.

CNJ. **Termo de Acordo de Cooperação Técnica Nº 58/2009.** Brasília, 2009. Disponível em: http://www.cnj.jus.br/images/Modelo_Nacional_Interoperabilidade/ACOT_058_2009.pdf Acesso em: 21 July 2014).

CNJ. **Resolução CNJ Nº 65.** Brasília, 2008. Disponível em: <http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/rescnj_65.pdf>. Acesso em: 21 jul. de 2014.

CONCEIÇÃO, Rodrigo da Silva. **A informática jurídica no auxílio à acessibilidade da justiça: processo eletrônico.** 2011. 98 f. Monografia - Curso de Direito, Departamento de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2011.

CONJUR. **CNJ estuda impor sistema único de processo eletrônico.** 2013. Disponível em: <http://www.conjur.com.br/2013-out-30/cnj-estuda-impor-aos-tribunais-troca-sistemas-pje-ainda-instavel>. Acesso em: 21 de set. 2014.

DIALLO, Saikou Y. et al. **Understanding interoperability.** In: Proceedings of the 2011 Emerging M&S Applications in Industry and Academia Symposium. Society for Computer Simulation International, 2011. p. 84-91.

EASTLAKE, D. **XML-Signature Syntax and Processing.** 2002. Disponível em: <http://www.w3.org/TR/2002/RECxmldsig-core-20020212/>. Acesso em: 25 abr. 2013.

EUROPEAN UNION. **e-CODEX (e-Justice Communication via Online Data Exchange).** European Commision, 2014. Disponível em: <ec.europa.eu/justice/criminal/european-e-justice/e-codex/index_en.htm>. Acesso em: 9 jul. 2014.

FERGUSON, Niels; SCHNEIER, Bruce; KOHNO, Tadayoshi. **Cryptography Engineering: Design Principles and Practical Applications: Design Principles and Practical Applications.** John Wiley & Sons, 2011.

GARTNER. **A Report for European Commission, Director General of Informatics.** NIFO Project – Final Report. European Commision, 2009. Disponível em: http://ec.europa.eu/idabc/servlets/Doc79da.pdf?id=32120 Acesso em: 15 June 2014).

GUIJARRO, Luis. **Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States.** Government Information Quarterly, v. 24, n. 1, p. 89-101, 2007.

HARRIS, Shon. **CISSP All-in-One Exam Guide**. 5. Ed: McGraw-Hill., 2010.

IEEE. **IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries**. New York, Standard. 1991.

ISA. **European Interoperability Framework (EIF) for European public services,** version 2.0. European Commission, 2010. Disponível em: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf. Acesso em: 22 July 2014).

ITI. **Requisitos mínimos para as políticas de certificado na ICP-Brasil.** Brasília, 2014. Disponível em: <http://www.iti.gov.br/images/legislacao/Docicp/DOC-ICP-04_-_Versao_5.3_-_REQ._MIN._PARA_AS_PCs_NA_ICP-BRASIL_29.04.2014.pdf>. Acesso em: 20 out. de 2014.

ITI. **Visão geral sobre assinaturas digitais na ICP-Brasil.** Brasília, 2012. Disponível em: < http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-15_-_Versao_2.1_VISAO_GERAL_SOBRE_ASSIN_DIG_NA_ICP-BRASIL_13-08-2012.pdf>. Acesso em: 20 mar. 2013.

ITI. **Requisitos das Políticas de Assinatura Digital na ICP-Brasil - DOC-ICP-15.03.** Brasília, 2012a. Disponível em:

<http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/docs 13082012/DOC-ICP-15.03_-_Versao_6.1_2.pdf>. Acesso em: 05 jun. 2014.

JIMÉNEZ, Carlos E. **Implementing Interoperability in E-Justice's Criminal Area**. Effectius Newsletter, n. 17, 2012.

KUBICEK, Herbert; CIMANDER, Ralf. **Three dimensions of organizational interoperability.** European Journal of ePractice, v. 6, 2009.

KUBICEK, Herbert; CIMANDER, Ralf; SCHOLL, Hans Jochen. **Organizational interoperability in e-government:** lessons from 77 European good-practice cases. Springer Science & Business Media, 2011.

LALLANA, Emmanuel C. **e-Government Interoperability:** A Review of Government Interoperability Frameworks in Selected Countries. United Nations Development Programme, Bangkok, Thailand, New York, NY, 2007.

ROVARIS, Felipe Machado. **AUTOMATIZAÇÃO NA COTAÇÃO DE LIVROS UTILIZANDO WEB SERVICE**. Florianópolis, 2007. Disponível em: < https://projetos.inf.ufsc.br/arquivos_projetos/projeto_583/TCC%20FELIPE%20pronto.pdf>. Acesso em: 21 de jul. 2014.

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: 09 jun. 2013.

MENEZES, A. J.; OORSCHOT, P. C. van; VANSTONE, S. A. **Handbook of Applied Cryptography**. 5. Ed: CRC Press, 2001

MISURACA, Gianluca; REID, Alasdair; DEAKIN, Mark. **Exploring emerging ICT-enabled governance models in European cities.** Analysis of the Mapping Survey to identify the key city governance policy areas most impacted by ICTs, EU European Commission Joint Research Centre Institute for Prospective Technological Studies, 2011.

PAAR, Christof; PELZL, Jan. **Understanding cryptography: a textbook for students and practitioners.** Springer Science & Business Media, 2009.

PINKAS, D.; POPE, N.; ROSS, J. **CMS Advanced Electronic Signatures (CAdES).** RFC 5126 (Informational). (Request for Comments, 5126). IETF, 2008. Disponível em: <http://www.ietf.org/rfc/rfc5126.txt>. Acesso em: 25 abr. 2013.

Portal G1. **Documentos da NSA apontam Dilma Rousseff como alvo de espionagem.** 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html>. Acessado em: 06 jun. 2014.

RAY, Dibakar et al. **A critical survey of selected government interoperability frameworks.** Transforming Government: People, Process and Policy, v. 5, n. 2, p. 114-142, 2011.

ROSS, J.; PINKAS, D.; POPE, N. **Electronic Signature Policies**. IETF, 2001. RFC 3125 (Experimental). (Request for Comments, 3125). Disponível em: <http://www.ietf.org/rfc/rfc3125.txt>. Acesso em: 20 abr. 2013.

ROVER, Aires J.; MEZZAROBA, O. **Novas tecnologias: o governo eletrônico na perspectiva da governança.** In: (Org.) Vladimir Oliveira da Silveira e Orides Mezzaroba. Empresa, sustentabilidade e funcionalização do Direto. - São Paulo: Editora Revista dos Tribunais, 2011. -(coleção Justiça, Empresa e Sustentabilidade; v.2).

ROVER, Aires José; **Definindo o processo eletrônico.** Disponível em: <http://www.egov.ufsc.br/portal/conteudo/publicação-definindo-o-termo-processo-eletrônico>. Acesso em: 05 jun. 2013.

SAEKOW, Apitep; BOONMEE, Choompol. **Towards a Practical Approach for Electronic Government Interoperability Framework (e-GIF).** In: System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on. IEEE, 2009. p. 1-9.

SILVEIRA, Lucas. **Implementação do Padrão Brasileiro de Assinatura Digital.** Florianópolis, 2011. Disponível em:

<https://projetos.inf.ufsc.br/arquivos_projetos/projeto_1187/Lucas-Silveira-tcc-versao-final.pdf>. Acesso em: 20 jan. 2013.

SOFTPLAN (Brasil). **SAJ Tour.** Disponível em: <http://www.softplan.com.br/saj/saj_tour.jsf>. Acesso em: 12 jun. 2013.

W3C. W3C Recommendation. **XML Schema Part 0: Primer Second Edition.** 2008. Disponível em: <https://www.ocf.berkeley.edu/~ttv/cmpe276/XMLSchema.pdf>. Acesso em: 13 jul. de 2014.