Governo Brasileiro

Comitê Executivo de Governo Eletrônico

e-PING
Padrões de Interoperabilidade de Governo Eletrônico

Documento de Referência

Versão 2014

SUMÁRIO

Apresentação

A arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico – define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

As áreas cobertas pela e-PING estão segmentadas em:

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

Para cada um desses segmentos foram especificados componentes, para os quais são estabelecidos padrões.

Todo o conteúdo deste documento de referência está em consonância com as diretrizes do Comitê Executivo de Governo Eletrônico, criado pelo Decreto de 18 de outubro de 2000, e está publicado em sítio específico na Internet (http://www.eping.e.gov.br), garantindo acesso público às informações de interesse geral e transparência intrínseca à iniciativa. O governo brasileiro está comprometido em assegurar que estas políticas e especificações permaneçam alinhadas com as necessidades da sociedade e com a evolução do mercado e da tecnologia.

O documento de referência da e-PING contém:

- os fundamentos de concepção, implantação e administração da e-PING, relacionando os benefícios esperados com o trabalho, definindo os limites da abrangência da arquitetura e-PING e destacando as premissas consideradas e as políticas estabelecidas;
- o modelo de gestão da e-PING, discriminando atividades e responsabilidades, gestão de mudanças, divulgação e orientação para capacitação;
- as políticas e as especificações técnicas estabelecidas para todos os componentes de cada um dos segmentos da e-PING;
- glossário de termos técnicos referenciados;
- relação dos integrantes e colaboradores da presente versão deste documento.

Parte I – Visão Geral da e-PING

1. Introdução

A base para o fornecimento de melhores serviços, adequados às necessidades dos cidadãos e dos negócios, a custos mais baixos, é a existência de uma infraestrutura de Tecnologia da Informação e Comunicação (TIC) que se preste como alicerce para a criação desses serviços. Um governo moderno, integrado e eficiente exige sistemas igualmente modernos, integrados e interoperáveis, trabalhando de forma íntegra, segura e coerente em todo o setor público.

Nesse contexto, a interoperabilidade de tecnologia, processos, informação e dados é condição vital para o provimento de serviços de qualidade, tornando-se premissa para governos em todo o mundo, como fundamento para os conceitos de governo eletrônico, o *e-gov*. A interoperabilidade permite racionalizar investimentos em TIC, por meio do compartilhamento, reuso e intercâmbio de recursos tecnológicos.

Governos como o norte-americano, o canadense, o britânico, o australiano e o neozelandês investem fortemente no desenvolvimento de políticas e processos e no estabelecimento de padrões em TIC, montando estruturas dedicadas para obter a interoperabilidade, com o objetivo de prover serviços de melhor qualidade a custos reduzidos.

O governo brasileiro vem consolidando a arquitetura e-PING – "Padrões de Interoperabilidade de Governo Eletrônico", que tem como propósito ser o paradigma para o estabelecimento de políticas e especificações técnicas que permitam a prestação de serviços eletrônicos de qualidade à sociedade.

O que é Interoperabilidade?

Para o estabelecimento dos objetivos da e-PING, é fundamental que se defina claramente o que se entende por *Interoperabilidade*. A seguir são apresentados quatro conceitos que fundamentaram o entendimento do governo brasileiro a respeito do assunto:

"Intercâmbio coerente de informações e serviços entre sistemas. Deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema." (governo do Reino Unido);

"Habilidade de transferir e utilizar informações de maneira uniforme e eficiente entre várias organizações e sistemas de informação." (governo da Austrália);

"Habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, software e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados." (ISO);

"Interoperabilidade define se dois componentes de um sistema, desenvolvidos com ferramentas diferentes, de fornecedores diferentes, podem ou não atuar em conjunto." (Lichun Wang, Instituto Europeu de Informática – CORBA Workshops);

Interoperabilidade não é somente Integração de Sistemas, não é somente Integração de Redes. Não referencia unicamente troca de dados entre sistemas. Não contempla simplesmente definição de tecnologia.

É, na verdade, a soma de todos esses fatores, considerando, também, a existência de um legado de sistemas, de plataformas de Hardware e Software instaladas. Parte de princípios que tratam da diversidade de componentes, com a utilização de produtos diversos de fornecedores distintos. Tem por meta a consideração de todos os fatores para que os sistemas possam atuar cooperativamente, fixando as normas, as políticas e os padrões necessários para consecução desses objetivos.

Para que se conquiste a interoperabilidade, as pessoas devem estar engajadas num esforço contínuo para assegurar que sistemas, processos e culturas de uma organização sejam gerenciados e direcionados para maximizar oportunidades de troca e reuso de informações.

2. Escopo

Políticas e especificações claramente definidas para interoperabilidade e gerenciamento de informações são fundamentais para propiciar a conexão do governo, tanto no âmbito interno como no contato com a sociedade e, em maior nível de abrangência, com o resto do mundo – outros governos e empresas atuantes no mercado mundial. A e-PING é concebida como uma estrutura básica para a estratégia de governo eletrônico, aplicada inicialmente ao governo federal – Poder Executivo, não restringindo a participação, por adesão voluntária, de outros Poderes e esferas de governo.

Os recursos de informação do governo constituem valiosos ativos econômicos. Ao garantir que a informação governamental possa ser rapidamente localizada e intercambiada entre o setor público e a sociedade, mantidas as obrigações de privacidade e segurança, o governo auxilia no aproveitamento máximo deste ativo, impulsionando e estimulando a economia do país.

A arquitetura e-PING cobre o intercâmbio de informações entre os sistemas do governo federal – Poder Executivo e as interações com:

- Cidadãos;
- Outras esferas de governo (estadual e municipal);
- Outros Poderes (Legislativo, Judiciário) e Ministério Público Federal;
- Organismos Internacionais;
- Governos de outros países;
- Empresas (no Brasil e no mundo);
- Terceiro Setor.

2.1. Adesão à e-PING

A adoção dos padrões e políticas contidos na e-PING não pode ser imposta aos cidadãos e às diversas instâncias de governo, dentro e fora do país. O governo brasileiro, no entanto, estabelece essas especificações como o padrão por ele selecionado e aceito, ou seja, estes são os padrões em que deseja interoperar com as entidades fora do governo federal – Poder Executivo brasileiro. A adesão dessas entidades dar-se-á de forma voluntária e sem qualquer ingerência por parte da Coordenação da e-PING.

Para os órgãos do governo federal – Poder Executivo brasileiro a adoção dos padrões e políticas contidos na e-PING é obrigatória (Portaria SLTI/MP nº 5, de 14 de julho de 2005).

O governo federal – Poder Executivo brasileiro inclui:

- os órgãos da Administração Direta: Ministérios, Secretarias e outras entidades governamentais de mesma natureza jurídica, ligados direta ou indiretamente à Presidência da República do Brasil;
- as autarquias e fundações.

No âmbito das entidades supramencionadas, são obrigatórias as especificações contidas na e-PING para:

- todos os novos sistemas de informação que vierem a ser desenvolvidos e implantados no governo federal e que se enquadram no escopo de interação, dentro do governo federal e com a sociedade em geral;
- sistemas de informação legados que sejam objeto de implementações que envolvam provimento de serviços de governo eletrônico ou interação entre sistemas;
- outros sistemas que façam parte dos objetivos de disponibilizar os serviços de governo eletrônico.

A adesão ocorrerá de maneira gradativa, a partir da definição do Plano Diretor de Tecnologia da Informação – PDTI do órgão.

A aferição da situação de cada órgão quanto ao uso efetivo dos padrões se dará com os mecanismos descritos no item 5.3.2 Auditoria de Conformidade.

Para os sistemas de informação de governo que estiverem fora do escopo de obrigatoriedade delimitado, é recomendável que os responsáveis considerem a adequação aos padrões da e-PING

sempre que forem planejados esforços significativos de atualização.

Todas as compras e contratações do governo federal – Poder Executivo direcionadas para desenvolvimento de serviços de governo eletrônico e para atualizações de sistemas legados devem estar em consonância com as especificações e políticas contidas neste documento.

A e-PING incentiva a participação de todas as partes interessadas no desenvolvimento e atualização contínua das especificações e recomendações integrantes da arquitetura. A gestão da e-PING prevê essa participação, com utilização da Internet (http://www.eping.e.gov.br) como meio preferencial para o contato entre os gestores da e-PING e a sociedade.

2.2. Foco na interoperabilidade

A e-PING não terá como foco de trabalho todos os assuntos da área de Tecnologia da Informação e Comunicação (TIC). Serão tratadas apenas especificações que forem relevantes para garantir a interconectividade de sistemas, integração de dados, acesso a serviço de governo eletrônico e gerenciamento de conteúdo. A e-PING envolve os assuntos compreendidos na segmentação, descrita no item 4 deste documento.

2.3. Assuntos não abordados

A e-PING não tem por objetivo recomendar ferramentas. Os órgãos tem liberdade de escolha, devendo observar a adoção dos padrões da e-PING.

A e-PING também não tem por objetivo padronizar a forma de apresentação das informações dos serviços de governo eletrônico, restringindo-se à definição dos requisitos de intercâmbio de dados e das condições de disponibilidade desses dados para os dispositivos de acesso.

Estão disponíveis no portal do governo eletrônico brasileiro (http://www.governoeletronico.gov.br) as informações sobre diretrizes e políticas relativas à apresentação dos portais e sítios de governo eletrônico, que são abordados pelos Padrões Web e-GOV (e-PWG), assim como as informações sobre diretrizes e políticas relativas à acessibilidade dos portais e sítios de governo eletrônico, que são abordados pelo Modelo de Acessibilidade de Governo Eletrônico (e-MAG).

3. Políticas Gerais

Relacionam-se a seguir as políticas gerais utilizadas na construção da e-PING e que fundamentam as políticas e especificações técnicas de cada segmento:

3.1. Adoção Preferencial de Padrões Abertos

A e-PING define que, sempre que possível, serão adotados padrões abertos nas especificações técnicas. Padrões proprietários são aceitos, de forma transitória, mantendo-se as perspectivas de substituição assim que houver condições de migração. Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações.

3.2. Software Público e/ou Software Livre

A implementação dos padrões de interoperabilidade deve priorizar o uso de software público e/ou software livre, em conformidade com diretrizes do Comitê Executivo de Governo Eletrônico e normas definidas no âmbito do SISP.

A lista de softwares públicos está disponível no Portal do Software Público Brasileiro (http://www.softwarepublico.gov.br).

3.3. Transparência

Os documentos da e-PING estarão à disposição da sociedade, via Internet, sendo previstos mecanismos de divulgação, recebimento e avaliação de sugestões.

3.4. Segurança

A interoperabilidade na prestação dos serviços de governo eletrônico deve considerar o nível de segurança requerido pelo serviço, com a máxima transparência.

3.5. Suporte de mercado

Todas as especificações contidas na e-PING contemplam soluções amplamente utilizadas pelo mercado. O objetivo a ser alcançado é a redução dos custos e dos riscos na concepção e produção de serviços nos sistemas de informações governamentais.

3.6. Dimensões

A e-PING considera que a interoperabilidade envolve elementos técnicos, semânticos e organizacionais, sendo políticas gerais direcionadoras dessas dimensões:

3.6.1. Dimensão Técnica

3.6.1.1. Alinhamento com a INTERNET

Todos os sistemas de informação da administração pública deverão estar alinhados com as principais especificações usadas na Internet e com a *World Wide Web*.

3.6.1.2. Adoção de navegadores (*browsers*)

Como principal meio de acesso, todos os sistemas de informação de governo deverão ser acessíveis, preferencialmente, por meio de tecnologia baseada em *browser.* Outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores.

3.6.1.3. Escalabilidade

As especificações selecionadas deverão ter a capacidade de atender alterações de demanda no sistema, tais como, mudanças em volumes de dados, quantidade de transações ou quantidade de usuários. Os padrões estabelecidos não poderão ser fator restritivo, devendo ser capazes de fundamentar o desenvolvimento de serviços que atendam desde necessidades mais localizadas, envolvendo pequenos volumes de transações e de usuários, até demandas de abrangência nacional, com tratamento de grande quantidade de informações e envolvimento de um elevado contingente de usuários.

3.6.2. Dimensão Semântica

3.6.2.1. Desenvolvimento e manutenção de ontologias e outros recursos de organização da informação

Visando facilitar o cruzamento de dados de diferentes fontes de informação, quando da sua utilização por outras organizações integrantes da administração pública, por organizações da sociedade civil ou pelo cidadão, devem ser utilizados recursos tais como vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações.

Tais recursos podem ser desenvolvidos colaborativamente por pessoas com conhecimento na área específica e/ou em metodologias de modelagem específicas, e os resultados devem ser compartilhados, reaproveitados e disponibilizados em um repositório de vocabulários e ontologias de Governo Eletrônico.

3.6.2.2. Desenvolvimento e adoção de um padrão de modelagem de dados para Governo

Baseada em notação simples, objetiva e facilmente utilizável, a modelagem deve: evidenciar as integrações atuais e as integrações necessárias entre os dados; apoiar as interações do governo em suas diversas secretarias e órgãos; apoiar o alinhamento com os processos de negócios governamentais; promover a melhoria na gestão pública; e servir como arquitetura de interoperabilidade para o Governo.

3.6.2.3. Desenvolvimento e adoção de uma política de disseminação de dados e informações

Baseada em experiências internacionais de abertura de dados governamentais (OpenData), a política consiste em uma série de ações coordenadas para orientar a incorporação de processos de disponibilização dos dados públicos para permitir seu melhor uso pela sociedade, alinhada com a diretriz da e-PING de adoção de padrões abertos na interação do governo federal com a sociedade.

3.6.3. Dimensão Organizacional

3.6.3.1. Simplificação administrativa

A aplicação da e-PING visa contribuir para que as interações do governo com a sociedade sejam realizadas de forma simples e direta, sem prejuízo da legislação vigente.

3.6.3.2. Promoção da colaboração entre organizações

Por meio da integração entre objetivos institucionais e processos de negócio de organizações com estruturas internas e processos internos diferentes.

3.6.3.3. Garantia à privacidade de informação

Todos os órgãos responsáveis pelo oferecimento de serviços de governo eletrônico devem garantir as condições de preservação da privacidade das informações do cidadão, empresas e órgãos de governo, respeitando e cumprindo a legislação que define as restrições de acesso e divulgação.

4. Segmentação

A arquitetura e-PING foi segmentada em cinco partes, com a finalidade de organizar as definições dos padrões. Para cada um dos **segmentos**, foi criado um grupo de trabalho, composto por profissionais atuantes em órgãos dos governos federal, estadual e municipal, especialistas em cada assunto. Esses grupos foram responsáveis pela elaboração desta versão da arquitetura, base para o estabelecimento dos padrões de interoperabilidade do governo brasileiro.

Os cinco segmentos – “Interconexão”, “Segurança”, “Meios de Acesso”, ”Organização e Intercâmbio de Informações” e “Áreas de Integração para Governo Eletrônico” – foram subdivididos em **componentes**, para os quais foram estabelecidas as políticas e as especificações técnicas a serem adotadas pelo governo federal. A seguir, uma breve descrição dos segmentos. Os componentes serão tratados a partir do capítulo 6.

4.1. Interconexão – GT1

Estabelece as condições para que os órgãos de governo se interconectem, além de fixar as condições de interoperação entre o governo e a sociedade.

4.2. Segurança – GT2

Trata dos aspectos de segurança de TIC que o governo federal deve considerar.

4.3. Meios de Acesso – GT3

São explicitadas as questões relativas aos padrões dos dispositivos de acesso aos serviços de governo eletrônico. Nesta versão são abordadas as políticas e as especificações para estações de trabalho, televisão digital e mobilidade.

4.4. Organização e Intercâmbio de informações – GT4

Aborda os aspectos relativos ao tratamento e à transferência de informações nos serviços de governo eletrônico. Inclui padrão de vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações.

4.5. Áreas de Integração para Governo Eletrônico – GT5

Estabelece a utilização ou construção de especificações técnicas para sustentar o intercâmbio de informações em áreas transversais da atuação governamental, cuja padronização seja relevante para a interoperabilidade de serviços de Governo Eletrônico, tais como Dados e Processos, Informações Contábeis e Informações Geográficas, entre outras.

5. Gestão da e-PING

Neste item são tratados os aspectos de gestão da arquitetura e-PING, especificando a forma pela qual o governo brasileiro pretende consolidar a implantação das políticas e especificações técnicas como padrões efetivos adotados tanto internamente, pelos órgãos que compõem a Administração Pública Federal, como na interoperabilidade com as entidades externas, representadas por outras instâncias de governo, pela iniciativa privada, por instituições atuantes no terceiro setor e pelo cidadão.

5.1. Histórico

A arquitetura e-PING tem por finalidade ser o paradigma de interoperabilidade para o governo federal, inicialmente no âmbito do Poder Executivo, onde seu uso é obrigatório. A iniciativa de montagem da arquitetura coube a três órgãos da esfera federal:

- Ministério do Planejamento, Orçamento e Gestão, por meio da sua Secretaria de Logística e Tecnologia da Informação (SLTI/MP);
- Instituto Nacional de Tecnologia da Informação, da Presidência da República (ITI);
- Serviço Federal de Processamento de Dados (SERPRO), empresa pública ligada ao Ministério da Fazenda.

Os trabalhos foram iniciados em 2003 com a visita do Secretário da SLTI ao Governo Britânico para conhecer o modelo britânico de interoperabilidade (e-GIF). Ainda em 2003, esses três órgãos organizaram um Seminário, com participação de entidades do governo federal, no âmbito do Poder Executivo, tendo como objetivo a formação de um comitê interórgãos – denominado Comitê Constituinte – para conduzir os trabalhos iniciais de montagem da arquitetura. Após a sua institucionalização, por intermédio da Portaria Normativa nº 5, de 14 de julho de 2005, este Comitê Constituinte passou a ser denominado Coordenação da e-PING.

5.2. Estratégia de Atualização

A divulgação dos padrões e especificações estabelecidos pelo governo brasileiro segue o esquema de versionamento. É prevista a elaboração de uma versão anual, com publicação intermediária de atualizações, sempre que existirem modificações significativas.

A presente versão consolidou o trabalho dos grupos montados para os cinco segmentos definidos. Todo seu conteúdo foi disponibilizado para Consulta Pública, com o objetivo de obter contribuições às propostas de padrões publicados na minuta da versão 2014.

5.3. Modelo de Governança e Gestão

O modelo se baseia nos conceitos de Governança, que trata das estruturas e processos necessários para se fazer a gestão e controle da arquitetura, e ainda nos conceitos de Gestão, que trata das ações que visam garantir a utilização e atualização da arquitetura e-PING. O modelo contempla as principais atribuições, papéis, responsabilidades dos integrantes e a forma de implementação dessas atividades na organização estrutural do governo.

A estrutura de governo criada para administração da e-PING é apresentada no esquema simplificado a seguir:

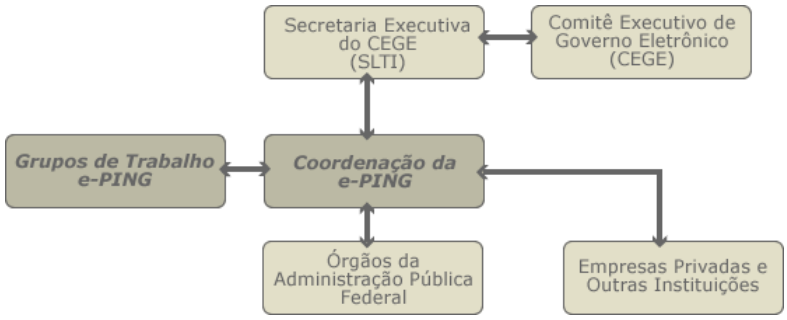

Figura 1 – Administração da e-PING.

Para operacionalizar a evolução da e-PING foi definido o modelo de Governança, baseado em papéis, responsabilidades e atividades, que tem como objetivo garantir a manutenção e evolução dos padrões de interoperabilidade. Os papéis e responsabilidades definidos para o modelo de governança seguem abaixo:

- Coordenação Geral e-PING
  - Estabelecer os objetivos estratégicos e de gestão de governo para o estabelecimento de padrões de interoperabilidade;
  - Administrar a arquitetura de interoperabilidade do governo brasileiro, provendo a infraestrutura gerencial necessária para sua correta utilização e garantindo sua atualização, considerando: as prioridades e metas de governo, as necessidades da sociedade e a disponibilidade de novas tecnologias maduras e suportadas pelo mercado de TIC;
  - Atualização da arquitetura e-PING, providenciando as atividades necessárias para consolidação da versão atual e dinâmica da sua evolução;
  - Gestão da arquitetura e-PING;
  - Estabelecimento e gestão das normas e dos instrumentos institucionais e legais que garantam a efetividade das recomendações e especificações da e-PING;
  - Administração dos padrões considerados na e-PING;
  - Garantia de manutenção da atualização dos diversos catálogos da e-PING;
  - Gestão dos processos de Comunicação e Divulgação dos padrões, das decisões e das atividades da e-PING, incluindo a publicação de novas versões e das atualizações intermediárias;
  - Centralizar as sugestões de padrões dos órgãos da Administração Pública Federal nas diversas áreas de interesse da e-PING;
  - Administração dos Grupos de Trabalhos (GTs), definindo sua composição e determinando as diretrizes de trabalho, baseadas nas políticas técnicas, gerais e especificas, nas necessidades de governo e na monitoração do cenário tecnológico;
  - Gerenciar a interação com iniciativas de mesmo propósito, conduzidas por outros governos, no país e no exterior;
  - Gerenciar a interação com organismos de especificação (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Institutos Normativos de segmentos específicos, como ABNT, INMETRO, ISO, NIST, etc). Estes organismos serão escolhidos a critério da coordenação da e-PING levando em consideração o seu notório reconhecimento internacional, competência em sua área de atuação e o estabelecimento de padrões abertos;
  - Gerenciar a interação com órgãos de fomento nacionais e internacionais, para canalizar recursos, visando atender as necessidades de criação de infraestrutura da e-PING e promover a pesquisa e desenvolvimento;
  - Gerenciar o processo de homologação dos padrões a serem estabelecidos para o governo;
  - Gerenciar processos de auditoria realizados com a finalidade de verificar o nível de adesão às recomendações e especificações da e-PING;
  - Atuar cooperativamente, como apoio aos órgãos de governo, na realização dos processos necessários para adequação aos padrões e-PING;

- Avaliar a possibilidade de patrocinar programas abrangentes que promovam a utilização intensiva dos padrões propostos;
- Gerenciar e operacionalizar a divulgação dos padrões da e-PING;
- Administrar sítio da e-PING na internet (http://www.eping.e.gov.br);
- Estabelecimento dos pontos de contato com os diversos órgãos da Administração Pública Federal;

➢ **Coordenação dos Grupos de Trabalhos (GTs)**
- Realizar o planejamento anual do GT baseado nas diretrizes da Coordenação Geral;
- Agrupar metas e ações por temas;
- Criar subgrupos e designar coordenadores, se necessário;
- Direcionar ações e corrigir rotas de planejamento;
- Consolidar os padrões dos subgrupos/integrantes.

➢ **Coordenação dos Subgrupos**
- Definir metas e ações do subgrupo;
- Divulgar as metas e ações;
- Direcionar análises e estudos dos padrões;
- Monitorar/coordenador as ações dos subgrupos;
- Consolidar os padrões dos subgrupos.

➢ **Integrantes dos Subgrupos**
- Estudar e avaliar padrões;
- Executar as ações definidas pelo Coordenador do GT ou subgrupo.

➢ **Domínio de Informação (Órgãos de Governo)**
- Prospecção e uso dos padrões;
- Sinalizar tecnologias que atendam suas necessidades específicas para que sejam estudadas mais profundamente;
- Utilizar os padrões em suas aplicações.

A SLTI/MP, por meio do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), instituído pelo Decreto nº 7.579, de 11 de outubro de 2011, é a responsável pela institucionalização e pela definição do formato jurídico da Coordenação da e-PING.

Estes papéis atuam a partir de um processo padronizado conforme figura 2. Cabe destacar que o diagrama apresentado faz uso do padrão de Notação de Modelagem de Processo de Negócio (BPMN) definido pela e-PING.

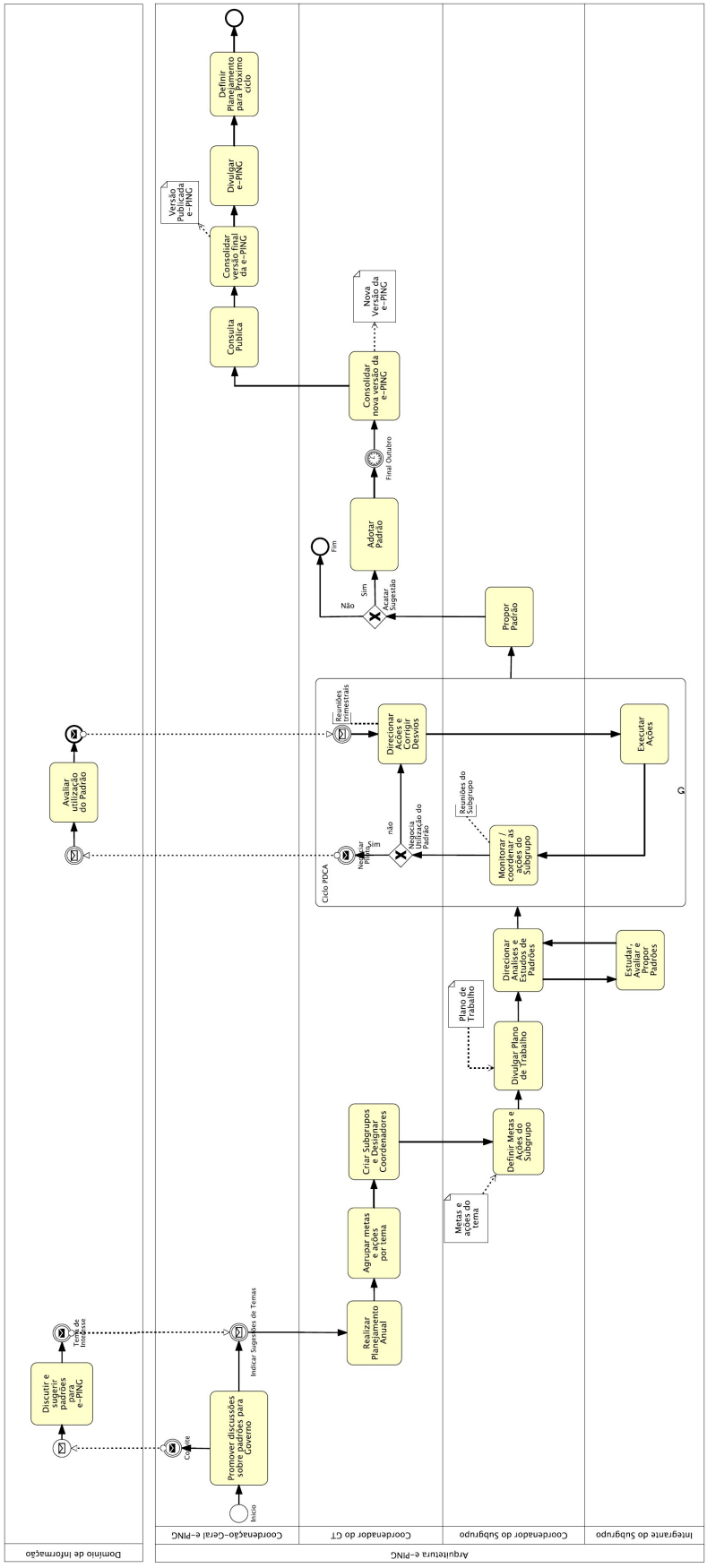

Figura 2 – Gestão da e-PING.

5.3.1. Descrição das Atividades

Esse processo tem o objetivo de descrever o modelo de governança e gestão da arquitetura e-PING, relacionando as principais atribuições e formas de implementações destas atividades na organização estrutural do governo.

- **Promover Discussões sobre Padrões para Governo**
  Monitorar sistematicamente o mercado com o objetivo de detectar novas tecnologias que atendam as necessidades de atualização tecnológica das políticas e especificações técnicas sugerindo padrões a serem analisados e possivelmente adotados pela e-PING, bem como promover discussões sobre a substituição de padrões adotados por outros mais atuais.
  Responsável: Coordenadores dos GTs

- **Discutir e Sugerir Padrões para a e-PING**
  Identificar e sugerir padrões tecnológicos que atendam as necessidades especificamente para os segmentos sob sua responsabilidade e que possam ser adotados pela e-PING.
  Responsável: Domínios de Informação

- **Realizar Planejamento Anual**
  Com base nas discussões levantadas na atividade anterior, e na evolução contínua da e-PING, serão definidos os objetivos estratégicos e de gestão previstos a serem executadas no ano corrente.
  Responsável: Coordenadores dos GTs

- **Agrupar Metas e Ações por Tema**
  Agrupar metas e ações por tema, facilitando a organização dos padrões para serem analisados e estudados por grupos de trabalhos específicos.
  Responsável: Coordenadores dos GTs

- **Criar Subgrupos e Designar Coordenadores**
  Criar subgrupos de trabalhos para atuar sobre padrões específicos bem como designar o coordenador responsável por gerir os integrantes do subgrupo nas atividades de pesquisas e estudos sobre o tema ou padrão sob sua responsabilidade, proporcionando maior agilidade e rapidez na condução dos trabalhos.
  Responsável: Coordenadores dos GTs

- **Definir metas e Ações do Subgrupo**
  Definir as metas e ações do subgrupo que irá atuar sobre uma tecnologia ou padrão específico, planejando as ações necessárias para a efetiva realização das atividades previstas, consolidando essas informações em um plano de trabalho.
  Responsável: Coordenador do Subgrupo

- **Divulgar Plano de Trabalho**
  Definir e divulgar a forma de condução dos trabalhos de pesquisas específicos sobre o padrão a ser prospectado, bem como o cronograma das atividades previstas para o ano.
  Responsável: Coordenador do Subgrupo

- **Direcionar Análises e Estudos de Padrões**
  Direcionar a equipe do subgrupo nos estudos e pesquisas dos padrões previstos sobre sua responsabilidade.
  Responsável: Coordenador do Subgrupo

- **Estudar, Avaliar e Propor Padrões**
  Executar as ações definidas no plano de trabalho, focada nas pesquisas e estudos das tecnologias, com intuito de avaliar e identificar oportunidades e ganhos possíveis com o padrão estudado, caso ele venha a ser adotado pela e-PING.
  Responsável: Integrantes do Subgrupo

- **Ciclo PDCA**
  Ciclo de desenvolvimento que tem foco na melhoria contínua, tanto dos trabalhos e padrões estudados quanto das iterações com entes envolvidos nas atividades evolutivas da arquitetura e-PING que fazem uso dos padrões propostos.

  - **Executar as Ações**
    Realizar estudos e pesquisas sobre determinadas tecnologias e padrões previstos no plano de trabalho do subgrupo.
    Responsável: Integrantes do Subgrupo

  - **Monitorar / Coordenar as Ações do Subgrupo**
    Acompanhar as atividades e ações previstas no plano de trabalho.
    Responsável: Coordenador do Subgrupo

  - **Direcionar Ações e Corrigir Desvios**
    Corrigir desvios, movimentando a equipe com intuito de acelerar ou motivar pesquisas, caso algum padrão seja sinalizado como não aplicável. Permite ao subgrupo sugerir novo tema de pesquisa, revendo plano de trabalho permitindo agilidade ao subgrupo nos estudos e sugestões de novos padrões de mercado.
    Responsável: Coordenadores dos GTs

  - **Avaliar a Utilização do Padrão**
    Utilizar o padrão estudado em um caso prático que possa validar o padrão estudado. O governo poderá estabelecer convênios ou credenciar instituições para elaboração de testes de conformidade, sempre definindo quais componentes devem ser submetidos a processos de homologação, quais os critérios de avaliação dos resultados e quais as condições de realização dos procedimentos.
    Responsável: Domínios de Informação

- **Propor Padrão**
  Após pesquisas e estudos da viabilidade de uso do padrão estudado é formalizada a proposta e direcionada ao Coordenador do GT a qual o subgrupo está vinculado, para que a tecnologia analisada seja adotada e incorporada à nova versão da e-PING.
  Responsável: Coordenador do Subgrupo

- **Adotar Padrão**
  Analisar os padrões candidatos a integrar a arquitetura. Esse processo abrange a seleção, a homologação e a classificação das especificações selecionadas em cinco níveis de situações que caracterizam o grau de aderência às políticas técnicas gerais e específicas de cada segmento.
  Esses cinco níveis são os seguintes:

  Adotado (A): item adotado pelo governo como padrão na arquitetura e-PING, tendo sido submetido a um processo formal de homologação realizado por parte de uma instituição do governo ou por uma outra instituição com delegação formal para realizar o processo. Também é considerado homologado quando baseado em uma proposição devidamente fundamentada pela coordenação do segmento, publicada no sítio e aprovado pela Coordenação da e-PING. Os componentes com padrão nível Adotado devem ser obrigatoriamente adotados em novos produtos/projetos de TI;

  Recomendado (R): item que atende às políticas técnicas da e-PING, é reconhecido como um item que deve ser utilizado no âmbito das instituições de governo, mas ainda não foi submetido a um processo formal de homologação. Os componentes de nível Recomendados não são obrigatórios, porém sugeridos para adoção em novos produtos/projetos de TI;

  Em Transição (T): item que o governo não recomenda, por não atender a um ou mais requisitos estabelecidos nas políticas gerais e técnicas da arquitetura; é incluído na e-PING em razão de seu uso significativo em instituições de governo, tendendo a ser desativado assim que algum outro componente, em uma das duas situações anteriores venha a apresentar condições totais de substituí-lo. Pode vir a ser considerado um componente “recomendado” caso venha a se adequar a todas

as políticas técnicas estabelecidas. Convém salientar que o desenvolvimento de novos serviços ou a reconstrução de partes significativas dos já existentes deve evitar o uso de componentes classificados como transitórios;
Em Estudo (E): componente que está em avaliação e poderá ser enquadrado numa das situações acima, assim que o processo de avaliação estiver concluído;
Estudo Futuro (F): componente ainda não avaliado e que será objeto de estudo posterior.

A homologação, por sua vez, deverá ser objeto de estudo mais aprofundado por parte dos gestores da e-PING. Em virtude da grande variedade de componentes tratados pela arquitetura, será necessário elaborar uma sistemática de homologação. Tal instrumento contemplará desde processos em que será indispensável a validação de características físicas de determinados componentes (ex: "cartões inteligentes") até outros em que sejam requeridos estudos de aspectos que envolvam o uso do componente no desenvolvimento e construção de serviços (ex: organização e intercâmbio de informações e segurança).

Responsável: Coordenadores dos GTs

- **Consolidar Nova Versão da e-PING**

  Ao final de cada ano são consolidados em nova versão da e-PING, todos os padrões estudados e aprovados, juntamente com os demais padrões vigentes na e-PING.

  Responsável: Coordenadores dos GTs

  - **Consulta Pública**

    Colocar a nova versão da e-PING em consulta pública, para receber contribuições e sugestões sobre os padrões e tecnologias propostas, bem como o documento como um todo. A disponibilização de versões para consulta pública será efetuada pela Internet no endereço http://www.eping.e.gov.br.

    Responsável: Coordenação-Geral da e-PING

  - **Consolidar Versão Final da e-PING**

    Após findar o prazo da consulta pública, todas as contribuições recebidas são analisadas e consolidadas na versão final da e-PING para o próximo ano.

    Responsável: Coordenação-Geral da e-PING

  - **Divulgar e-PING**

    Contempla toda atividade de divulgação da e-PING tanto as realizadas por meio do sitio como:

    - Divulgação completa da documentação relativa à arquitetura: versões oficiais e respectivas atualizações, versões para consultas públicas, documentação técnica de apoio, documentação legal e institucional correlata;
    - Disponibilidade das recomendações, determinações, especificações técnicas e políticas para validação, homologação e recebimento de comentários e sugestões por parte da sociedade;
    - Publicação de solicitação de comentários relativos à especificação de componentes para a arquitetura;
    - Realização de eventos específicos de divulgação como Seminários, *Workshops* e apresentações em geral;
    - Participação em eventos governamentais na área de TIC e correlatas;
    - Participação em eventos direcionados a públicos específicos;
    - Intercâmbio com outras esferas e outros Poderes de governo como instituições públicas, privadas e do terceiro setor e com governos de outros países.

    Responsável: Coordenação-Geral da e-PING

  - **Definir Planejamento para o Próximo Ciclo**

    Atividade no qual é realizado o planejamento inicial a ser tratado no próximo ciclo da e-PING.

    Responsável: Coordenação-Geral da e-PING

5.3.2. Auditoria de Conformidade

O cumprimento das especificações e recomendações por parte dos órgãos do governo federal – Poder Executivo, é fator crítico de sucesso na implantação e consolidação da e-PING. Os gestores da e-PING recomendarão a realização de processos de auditoria para verificação do atendimento às especificações e políticas da arquitetura.

Poderá haver delegação de responsabilidade para equipes especialmente montadas para essa finalidade, compostas por técnicos de governo com experiência em procedimentos dessa natureza.

A forma preferencial de realização desse tipo de procedimento, entretanto, será a utilização das estruturas próprias nos órgãos responsáveis por auditoria de sistemas. A Coordenação da e-PING atuará no sentido de sugerir os critérios básicos a serem seguidos pelos órgãos.

Outra questão a ser considerada será a colaboração de órgãos de governo atuantes na área, prevendo-se contatos com instituições de outros Poderes e esferas de governo.

5.3.3. Acompanhamento Legal e Institucional

A e-PING terá apoio constante da equipe da Assessoria Jurídica do Ministério do Planejamento, Orçamento e Gestão para garantir a aderência do conteúdo dos documentos que compõem a arquitetura às normas e instrumentos legais vigentes no país.

A Coordenação da e-PING poderá atuar no sentido de estabelecer uma forma de colaboração com algum outro órgão de governo que tenha condições de fornecer sua estrutura de apoio jurídico para realização dessa atividade.

5.3.4. Capacitação

Farão parte da agenda de implantação e gestão da e-PING eventos direcionados para fomentar e promover a capacitação.

Os Grupos de Trabalho da e-PING irão avaliar a necessidade e propor treinamentos relacionados aos padrões de cada segmento.

Cada órgão de governo deverá observar as definições de padrão da e-PING na montagem de seus planos particulares de capacitação, garantindo o fornecimento de treinamento adequado para os componentes de suas equipes técnicas.

5.4. Relacionamento com Governo e Sociedade

Neste item são tratadas as formas de relacionamento da e-PING com as entidades que compõem o governo e a sociedade.

5.4.1. Organizações do Governo Federal – Poder Executivo

No âmbito do Poder Executivo, a participação de todos os níveis hierárquicos da Administração Pública Federal, suas agências e organismos reguladores e as empresas e instituições públicas é essencial para a promoção e consolidação da interoperabilidade no setor público.

Embora as diretrizes gerais sejam geridas pela Coordenação da e-PING, cada instituição em particular terá sua responsabilidade na gestão e garantia de uso dos padrões e-PING. Dentre as atribuições dessa natureza, destacam-se:

- Contribuir para o desenvolvimento e melhoria contínua da e-PING;
- Garantir que suas estratégias organizacionais de TIC considerem que os sistemas integrantes de serviços de governo eletrônico sob sua responsabilidade estejam adequados às recomendações da e-PING;
- Dispor de um plano de implementação e adequação da infraestrutura de TIC da organização à arquitetura e-PING;
- Assegurar que sejam de domínio das equipes da instituição, as habilidades para definir e utilizar as especificações requeridas para interoperabilidade, fornecendo suporte de treinamento quando necessário;

- Estabelecer ponto de contato nas instituições, para intercâmbio de informações e de necessidades com a Coordenação da e-PING;
- Alocar e suprir recursos para dar suporte aos seus processos de adequação à e-PING;
- Aproveitar a oportunidade para racionalizar processos (como resultado do aumento da interoperabilidade) de maneira a melhorar a qualidade e reduzir custos de provimento dos serviços de e-gov.

5.4.2. Outras Instâncias de Governo (outros Poderes Federais, Governos Estaduais e Municipais)

A adoção da e-PING é obrigatória para os órgãos e entidades do governo federal – Poder Executivo. Aos outros Poderes (Judiciário, Legislativo) e outras esferas de governo (estadual e municipal) a adoção é facultativa.

A coordenação da e-PING atua proativamente visando a adoção da e-PING pelos entes integrantes de outras esferas e Poderes, dada a relevância do intercâmbio de informações entre esferas e Poderes para a eficiência, eficácia e efetividade da atuação governamental e para a construção de serviços de governo eletrônico orientados à sociedade, em especial, ao cidadão.

Para facilitar a adoção da e-PING pelos governos estaduais, a ABEP participa da coordenação da e-PING, atuando em colaboração com a coordenação da e-PING na construção de uma matriz de interesses federativos para troca de informações.

5.4.3. Organizações do Setor Privado e do Terceiro Setor

A e-PING prevê a interação com o Setor Privado e com o Terceiro Setor por meio dos mecanismos de Consulta Pública, Solicitação de Comentários e Recebimento de Sugestões.

Todas as entidades dessa natureza que participarem de processos de licitação para fornecimento de produtos e serviços para o Poder Executivo Federal deverão atender às especificações e recomendações da e-PING.

Outras formas de participação dessas instituições na e-PING podem ser consideradas, estabelecendo-se critérios que garantam a transparência e equidade de oportunidades.

5.4.4. Cidadão

Governo eletrônico significa, essencialmente, o governo servir melhor às necessidades do cidadão utilizando os recursos de Tecnologia, Informação e Comunicação. A arquitetura e-PING possibilita a integração e torna disponíveis serviços de forma íntegra, segura e coerente, permitindo obter melhores níveis de eficiência no governo.

O governo deve incentivar a sociedade a opinar, comentar, e contribuir com sugestões de inovações que possam ajudá-lo a melhorar o acesso à informação e a prestação de seus serviços. Todos os processos de divulgação e de inter-relacionamento da e-PING preveem a participação ativa do cidadão e da sociedade em geral, no processo de construção e gestão da arquitetura.

5.5. Documentos de suporte à Interoperabilidade

5.5.1. Guia de Interoperabilidade

Está disponível no sítio da e-PING (http://www.eping.e.gov.br) o Guia de Interoperabilidade do Governo, composto pelo Manual do Gestor e pela Cartilha Técnica.

O Manual do Gestor tem como público-alvo os gestores de Tecnologia da Informação dos órgãos do Governo. Esse documento traz uma visão para o gestor da importância da interoperabilidade, o papel da e-PING e apresenta um roteiro com orientações para o Gestor realizar a troca de informações com outros órgãos.

A Cartilha Técnica tem como público-alvo os profissionais técnicos que atuam na área de Tecnologia da Informação. A Cartilha Técnica apresenta os requisitos técnicos e indica melhores usos de tecnologias de mercado, que proporcionam a melhoria da interoperabilidade governamental, sua melhor qualidade e abrangência.

Parte II – Especificação Técnica dos Componentes da e-PING

6. Interconexão

6.1. Interconexão: Políticas Técnicas

As políticas técnicas para interconexão são:

6.1.1 Devido ao esgotamento da oferta de endereços IPv4 públicos, os órgãos da APF deverão planejar sua futura migração para IPv6. Novas contratações e atualizações de redes interoperávies deverão implementar ambos os protocolos IPv4 e IPv6.

6.1.2 Os sistemas de e-mail devem utilizar SMTP/MIME para o transporte de mensagens. Para acesso às mensagens, devem ser utilizados os protocolos POP3 e/ou IMAP, sendo encorajado o uso de interfaces *web* para correio eletrônico, observados os aspectos de segurança.

6.1.3 Os órgãos da APF devem obedecer à política de nomeação de domínios do governo federal, estabelecida na Resolução nº 7, que pode ser visualizada no endereço eletrônico https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm.

6.1.4 O DNS deve ser utilizado para resolução de nomes de domínios Internet, convertendo-os em endereços IP e, inversamente, convertendo IPs em nomes de domínios, através da manutenção dos mapas direto e reverso, respectivamente.

6.1.5 Os protocolos FTP e/ou HTTP devem ser utilizados para transferência de arquivos, observando suas funcionalidades para recuperação de interrupções e segurança. O HTTP deve ser priorizado para transferências de arquivos originários de páginas de sítios da Internet.

6.1.6 Sempre que possível[1], deve ser utilizada tecnologia baseada na *web* em aplicações que utilizaram Emulação de Terminal anteriormente.

6.2. Interconexão: Especificações Técnicas

Tabela 1 – Especificações para Interconexão – Aplicação[2]

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Endereços de caixa postal eletrônica	As regras para definição dos nomes das caixas postais de correio eletrônico deverão seguir ao estabelecido no documento “Caixas Postais Individuais-Funcionais no governo federal”, disponível no endereço eletrônico http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/arquivo	**A**	
Transporte de mensagem eletrônica	Utilizar produtos de mensageria eletrônica que suportam interfaces em conformidade com SMTP/MIME para transferência de mensagens. RFC correlacionadas: RFC 5321, RFC 5322, RFC 2045, RFC 2046, RFC 3676, RFC 2047, RFC 2231 (atualização das RFC 2045, 2047 e 2183), RFC	**A**	

[1] Existem produtos que podem fornecer acesso pelo *browser* aos sistemas legados, sem necessidade de mudar esses sistemas; tipicamente estes produtos podem fornecer acesso direto às telas de legado ou serem substituídas por interfaces gráficas (GUIs). Deve-se prestar atenção a qualquer implicação de segurança em relação a seu uso.

[2] As RFCs podem ser acessadas em http://www.ietf.org/rfc.html

Componente	Especificação	SIT	Observações
	2183, RFC 4288, RFC 4289, RFC 3023 e RFC 2049.		
Acesso à caixa postal	*Post Office Protocol* – POP3 para acesso remoto a caixa postal. RFC correlacionada: RFC 1939 (atualizada pela RFC 1957 e RFC 2449).	**T**	
	Internet Message Access Protocol – IMAP para acesso remoto à caixa postal. RFCs correlacionadas: RFC 2342 (atualizada pela RFC 4466), RFC 2910 (atualizada pela RFC 3380, RFC 3381, RFC 3382, RFC 3510 e RFC 3995), RFC 2971, RFC 3501, RFC 3502 e RFC 3503.	**A**	
Mensageria em Tempo Real	O modelo e requisitos para *Instant Messaging and Presence Protocol* (IMPP) são definidos pela RFC 2778 e RFC 2779.	**T**	
	O modelo e requisitos para *Extensible Messaging and Presence Protocol* (XMPP) são definidos pela RFC 6120 e atualizada pela RFC 6122.	**A**	
AntiSpam – Gerenciamento da Porta 25	Implementar submissão de e-mail via porta 587/TCP com autenticação, reservando a porta 25/TCP apenas para transporte entre servidores SMTP, conforme recomendação CGI / Cert.br http://www.cert.br/	**R**	
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1 (RFC 2616, atualizada pelas RFCs 2817, 5785, 6266 e 6585).	**A**	
Protocolos de transferência de arquivos	FTP (com re-inicialização e recuperação) conforme RFC 959 (atualizada pela RFC 2228, RFC 2640, RFC 2773, RFC 3659 e RFC 5797) e HTTP conforme RFC 2616 (atualizada pelas RFCs 2817, 5785, 6266 e 6585) para transferência de arquivos.	**A**	
Diretório	LDAP v3 deverá ser utilizado para acesso geral ao diretório, conforme RFC 4510.	**A**	
Sincronismo de tempo	RFC 5905 IETF - *Network Time Protocol* - NTP version 4.0.	**A**	O Simple Network Time Protocol – SNTP version 4.0 está definido na seção 14 da RFC 5905.
Serviços de Nomeação de Domínio	O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035 (atualizada pela RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 1101, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966 e RFC 6604). Por sua vez, as diretivas de nomeação de domínio do governo brasileiro são encontradas na Resolução nº 7 do Comitê Executivo do Governo Eletrônico, no endereço eletrônico https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm Além dessas diretivas, por decisão do Comitê Gestor da Internet no Brasil, a nomeação de domínios obedece às orientações do Ministério do Planejamento, Orçamento e Gestão, a quem	**A**	

Componente	Especificação	SIT	Observações
	compete gerenciar os domínios .GOV.BR. As particularidades de outros níveis de governo, como por exemplo, os domínios dos governos das Unidades da Federação, que incluem a sigla da UF na composição dos endereços, são abordadas no endereço eletrônico http://registro.br/faq/faq1.html#12		
Protocolos de sinalização	Uso do Protocolo de Inicialização de Sessão (SIP), definido pela RFC 3261 (atualizada pela RFC , RFC3265, RFC4320, RFC4916, RFC5393, RFC5621, RFC5626, RFC5630, RFC5922, RFC5954 e RFC6026), como protocolo de controle na camada de aplicação (sinalização) para criar, modificar e terminar sessões com um ou mais participantes.	**A**	
	Uso do protocolo H.323 em sistemas de comunicação multimídia baseado em pacotes, definido pela ITU-T (*International Telecommunication Union Telecommunication Standardization sector*).	**T**	
Protocolos de gerenciamento de rede	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede.	**T**	Versão 2
		R	Versão 3
Protocolo de troca de informações estruturadas em plataforma descentralizada e/ou distribuída	Vide Tabela 17 – Especificações para Áreas de Integração para Governo Eletrônico – *Web Services* na pág. 48		
Protocolo de análise de fluxo de rede	IPFix, conforme RFC 5101, sFlown(RFC 3176)	**E**	

Tabela 2 – Especificações para Interconexão – Rede/Transporte

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Transporte	TCP (RFC 793)	**A**	
	UDP (RFC 768) quando necessário, sujeito às limitações de segurança.	**A**	
Intercomunicação LAN/WAN	IPv4 conforme RFC 791 (atualizada pela RFC 1349).	**A**	
	IPv6 conforme RFC 2460 (atualizada pela RFC 5095, RFC 5722 e RFC 5871).	**R**	
Comutação por Label	Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço.	**A**	
Qualidade de serviço	Adoção de uma arquitetura para serviços diferenciados pelo uso do Diffserv (RFC 2475, atualizada pela RFC 3260).	**A**	

Tabela 3 – Especificações para Interconexão – Enlace/Físico

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Rede local sem fio	IEEE 802.11 b, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org) e com as normas da Anatel (http://www.anatel.gov.br).	**T**	
	IEEE 802.11 g, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org) e com as normas da Anatel (http://www.anatel.gov.br).	**A**	
	IEEE 802.11 n, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org) e com as normas da Anatel (http://www.anatel.gov.br).	**R**	
	IEEE 802.11ac	**E**	
Rede de acesso por cabeamento elétrico	*Power Line Communication* (PLC), segundo as normas da Anatel (http://www.anatel.gov.br) e da Aneel (http://www.aneel.gov.br).	**F**	
Qualidade de Serviço – 802.1p		**R**	
Virtual LAN	VLAN (IEEE 802.1Q)	**R**	
Resiliência Layer2	Spanning tree protocol (802.1d, 802.1w, 802.1s)	**R**	
	Shortest Path Bridging	**E**	
	DCB - Data Center Bridging	**E**	

6.3. Mensagem Eletrônica (E-mail)

Para efeito de clareza, a e-PING utilizará os seguintes conceitos:

Transporte de Mensagem Eletrônica

O transporte de mensagem eletrônica é definido como a interface entre dois sistemas de correio.

Acesso à caixa postal

Acesso à caixa postal é definido como a interface entre um cliente de correio e um sistema de correio.

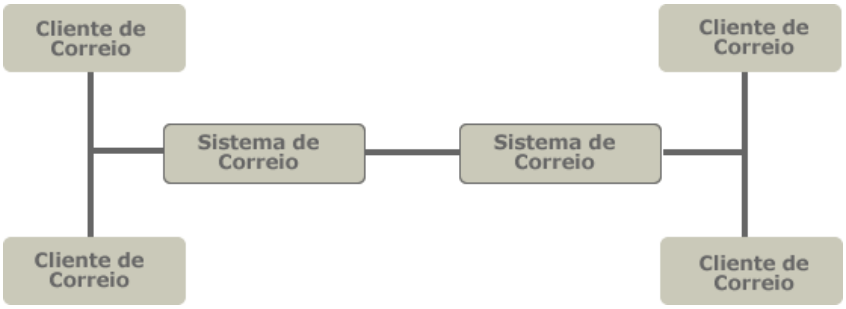

Figura 3 – Interfaces entre sistemas e clientes de Correio.

6.4. VPN

Virtual Private Network (VPN), ou Rede Privada Virtual, é um túnel virtual privativo construído sobre a infraestrutura de uma rede pública ou privada. Em vez de se utilizar circuitos dedicados para conectar redes remotas, utiliza-se usualmente a infraestrutura da Internet.

Tal utilização, como infraestrutura de conexão entre *hosts* da rede privada, é uma boa solução em termos de custos, mas não em termos de privacidade, pois os dados em trânsito podem ser lidos por qualquer equipamento, sendo necessário o uso de VPN.

Os túneis virtuais trafegam dados criptografados sobre redes pública ou privadas, formando um canal virtual seguro através dessas redes. Para tanto, são utilizados protocolos de tunelamento.

Os dispositivos responsáveis pelo gerenciamento da VPN devem ser capazes de garantir confidencialidade, integridade e autenticidade dos dados.

As especificações sobre VPN estão apresentadas no segmento de segurança.

6.5. Redes peer-to-peer

Sistemas *Peer-to-Peer* (P2P) são sistemas distribuídos que consistem de nodos interconectados, com capacidade de se auto-organizarem em topologias de rede, com o objetivo de compartilhar recursos como processamento, armazenamento e largura de banda, capazes de se adaptar a falhas e acomodar populações transientes de nodos, enquanto mantêm conectividade e performance aceitáveis, sem depender da intermediação ou suporte de uma autoridade (servidor) central.

Embora sistemas P2P possam contribuir para compartilhamento de recursos e colaboração em larga escala, com controle descentralizado e baixo acoplamento, ainda estão suscetíveis a diversos problemas de segurança. Este assunto será abordado em momento futuro.

6.6. Serviço SMS (*Short Message Service*)

Serviço de mensagem de texto que habilita mensagens curtas que contenham não mais que 160 caracteres de tamanho. O enfoque da e-PING em relação a essa especificação deve ser adstrito a fomentar serviços governamentais prestados ao cidadão utilizando a tecnologia descrita, que é amplamente suportada pelo mercado e é acessível à grande maioria da população. Não é enfoque da e-PING regulamentar essa tecnologia, sendo esta uma competência da ANATEL.

7. Segurança

7.1. Segurança: Políticas Técnicas

7.1.1 Os dados, informações e sistemas de informação do governo devem ser protegidos contra ameaças, de forma a reduzir riscos e garantir a integridade, confidencialidade, disponibilidade e autenticidade, observando-se as normas do governo federal referentes a Política de Segurança da Informação e Comunicações, favorecendo assim, a interoperabilidade.

7.1.2 Os dados e informações devem ser mantidos com o mesmo nível de proteção, independentemente do meio em que estejam sendo processados, armazenados ou trafegando.

7.1.3 As informações classificadas e sensíveis que trafegam em redes inseguras, incluindo as sem fio, devem ser criptografadas de modo adequado, conforme os componentes de segurança especificados neste documento.

7.1.4 Os requisitos de segurança da informação dos serviços e de infraestrutura devem ser identificados e tratados de acordo com a classificação da informação, níveis de serviço definidos e com o resultado da análise de riscos.

7.1.5 A segurança deve ser tratada de forma preventiva. Para os sistemas que apoiam processos críticos, devem ser elaborados planos de continuidade, nos quais serão tratados os riscos residuais, visando atender aos níveis mínimos de produção.

7.1.6 A segurança é um processo que deve estar inserido em todas as etapas do ciclo de desenvolvimento de um sistema.

7.1.7 Os sistemas devem possuir registros históricos (*logs*) para permitir auditorias e provas materiais, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado, bem como a utilização de mecanismos que garantam a autenticidade dos registros armazenados, se possível, com assinatura digital.

7.1.8 Nas redes sem fio metropolitanas recomenda-se a adoção de valores aleatórios nas associações de segurança, diferentes identificadores para cada serviço e a limitação do tempo de vida das chaves de autorização.

7.1.9 O uso de criptografia e certificação digital, para a proteção do tráfego, armazenamento de dados, controle de acesso, assinatura digital e assinatura de código deve estar em conformidade com as regras da ICP-Brasil.

7.1.10 A documentação dos sistemas, dos controles de segurança e das topologias dos ambientes deve ser mantida atualizada e protegida, mantendo-se grau de sigilo compatível.

7.1.11 Os usuários devem conhecer suas responsabilidades com relação à segurança e devem estar capacitados para a realização de suas tarefas e utilização correta dos meios de acesso.

7.1.12 Os órgãos da APF, visando a melhoria da segurança, devem ter como referência: Decreto nº 3.505/2000; Decreto nº 7.845/2002; a Instrução Normativa nº 01/2008 – GSI/PR e suas Normas Complementares; a Instrução Normativa nº 02/2013 – GSI/PR; a Instrução Normativa nº 3/2013 – GSI/PR; e as normas NBR ISO/IEC 27001:2006 – sistemas de gestão de segurança da informação; NBR ISO/IEC 27002:2005 – código de prática para a gestão da segurança da informação; NBR ISO/IEC 27003:2011 – diretrizes para implantação de um sistema de gestão da segurança da informação; NBR ISO/IEC 27004:2010 – medição ; NBR ISO/IEC 27005:2008 - Gestão de riscos de segurança da informação NBR ISO/IEC 27011:2008 – diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002; e NBR 15999-1:2007 e 15999-2:2008 – gestão de continuidade de negócios.

7.1.13 Para especificações sobre cartões inteligentes e *tokens*, deverão ser adotados os requisitos contidos nos normativos que tratam da homologação de equipamentos e sistemas no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (http://www.iti.gov.br). Estes requisitos, observados por produtos homologados na ICP-Brasil, tais como mídias que armazenam os certificados digitais e respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, estabelecem padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por

eles utilizados. É importante observar que não deve haver impedimento de acesso à dado armazenado em um cartão, como possíveis restrições impostas por licenciamento de uso de interface de software (middleware) para que seja garantida a interoperabilidade.

7.2. Segurança: Especificações Técnicas

Tabela 4 – Especificações para Segurança – Comunicação de dados

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Transferência de dados em redes inseguras	TLS – *Transport Layer Security*, RFC 5246[3] (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.	**R**	
Algoritmos para troca de chaves de sessão, durante o *handshake*	RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;	**R**	
Algoritmos para definição de chave de cifração	RC4, IDEA, 3DES e AES	**R**	
Certificado Digital	X.509 v3 – ICP-Brasil, SASL - *Simple Authentication and Security Layer*, RFC 4422	**R**	
Hipertexto e transferência de arquivos	RFC 2818 (atualizada pela RFC 5785)	**R**	
Transferência de arquivos	SSH FTP	**E**	Os documentos ainda estão no formato de rascunhos.
	Securing FTP with TLS, RFC 4217	**E**	
Segurança de redes IPv4	*IPSec Authentication Header* RFC 4303 e RFC 4835 para autenticação de cabeçalho do IP. IKE – *Internet Key Exchange*, RFC 4306 (atualizada pela RFC5282), deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento. ESP – *Encapsulating Security Payload,* RFC 4303 Requisito para VPN – Virtual Private Network.	**A**	Consultar errata para RFC 4303 e RFC 4306.
Segurança de redes IPv4 para protocolos de aplicação	O S/MIME v3, RFC 5751 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.	**A**	Consultar errata para RFC 5751.

[3] As RFCs podem ser acessadas em http://www.ietf.org/rfc.html

Componente	Especificação	SIT	Observações
Segurança de redes IPv6 na camada de rede	O IPv6 definido na RFC 2460 (atualizada pela RFC 5095), RFC 5722 e RFC 5871 apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*) RFC 4302 ou autenticação IP, e a segurança do encapsulamento IP, ESP (*Encrypted Security Payload*) RFC 4303.	**R**	Consultar errata para RFC 4302 e RFC 4303.

Tabela 5 – Especificações para Segurança – Correio Eletrônico

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Acesso a caixas postais	O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado, considerando as facilidades de segurança nativas do cliente. Quando não for possível utilizar o cliente específico ou for necessário acessar a caixa postal através de redes não seguras (por exemplo: Internet) deve-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595 (atualizada pela RFC 4616), que trata da utilização do TLS com IMAP, POP3 e ACAP.	**A**	Consultar errata para a RFC 2595.
Conteúdo de e-mail	O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 5652, RFC 3370 (atualizada pela RFC 5754), RFC 2631, RFC 5750, RFC 5751 e RFC 5652.	**A**	Consultar errata para RFC 5652, RFC 3370, RFC 5754, RFC 2631, RFC 5751 e RFC 5652.
Transporte de e-mail	Utilizar SPF (Sender Policy Framework) nos termos da RFC 4408, e reservar a porta 25, do protocolo SMTP, exclusivamente para transporte de mensagens entre MTAs; para comunicação entre MUAs e MTAs, utilizar a porta 587 (Submission), nos termos das RFCs 4409 e 5068	**A**	Consultar errata para RFC 4408.
Identificação de e-mail	Utilizar DKIM (*DomainKey Identified Mail*) nos termos da RFC 6376 http://datatracker.ietf.org/doc/rfc6376/ Recomendações do Comitê Gestor da Internet no Brasil. http://antispam.br/admin/dkim/	**R**	Consultar errata para RFC 4871.
Assinatura	Utilizar certificado padrão ICP-Brasil para assinatura de e-mail, quando exigido. Em conformidade com o disposto na Medida Provisória nº 2.200-2, de 24/08/2001 e Decreto nº 3.996 de 31/10/2001.	**A**	O serviço de assinatura deverá estar de acordo com as normas da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil

Componente	Especificação	SIT	Observações
Transporte seguro de e-mail	Usar SMTP seguro sobre TLS para transporte de e-mails entre MTA's nos termos da RFC 3207 e SMTP AUTH nos termos da RFC 4954.	**E**	Ver http://www.ietf.org/rfc/rfc3207.txt e http://www.ietf.org/rfc/rfc4954.txt

Tabela 6 – Especificações para Segurança – Criptografia

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Algoritmo de cifração	3DES ou AES	**R**	
Algoritmos para assinatura/hashing	SHA-256 ou SHA-512	**R**	i) Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil. ii) Os sistemas devem ter suporte para o algoritmo de *hash* MD5 com RSA, para garantir compatibilidade com implementações anteriores.
	SHA-224 ou SHA-238	**E**	Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	**A**	
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (RFC 5480). ECIES 256 e ECIES 512 .	**A**	ECDSA, para assinaturas digitais, e ECIES (Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil)para cifração e transporte seguro de chaves criptográficas.

Componente	Especificação	SIT	Observações
	ECMQV e ECDH, ambos para acordo de chaves, conforme RFC 5753.	**E**	
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3; FIPS 140-1 e FIPS 140-2.	**R**	Ver Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil).
Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	Devem ser aderentes aos padrões da ICP – Brasil.	**R**	Os certificados da AC-raiz devem ser instalados nos navegadores e visualizadores de arquivos conforme recomendado na IN nº 5/2009/ITI.

Tabela 7 – Especificações para Segurança – Desenvolvimento de Sistemas

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Assinaturas XML	Sintaxe e Processamento de assinatura XML (XMLsig) conforme definido pelo W3C http://www.w3.org/TR/xmldsig-core/	**A**	
Cifração XML	Sintaxe e Processamento de Cifração XML (XMLenc) conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/	**R**	
Assinatura e cifração XML	Transformação de decifração para assinatura XML conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificações de Gerenciamento de Chave XML) conforme definido pelo W3C http://www.w3.org/TR/xkms2/	**R**	
Autenticação e autorização de acesso XML	SAML – conforme definido pelo OASIS quando um ambiente ICP é utilizado http://www.oasis-open.org/committees/security/index.shtml	**R**	
Intermediação ou Federação de Identidades	WS-Security 1.1 - arcabouço de padrões para garantir integridade e confidencialidade em mensagens SOAP. (http://www.oasis-open.org/standards#wssv1.1. WS-Trust 1.4 - extensões para o padrão WS-Security, definindo o uso de credenciais de segurança e gerência de confiança distribuída. (http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf).	**R**	O componente anterior (SAML) poderá se juntar a este componente após estudos.

Componente	Especificação	SIT	Observações
Navegadores	Somente utilizar testemunhas de conexão de caráter permanente (*cookies*) com a concordância do usuário. .	**A**	Resolução nº 7 do Comitê Executivo do Governo Eletrônico (Capítulo II, Art.7º)

Tabela 8 – Especificações para Segurança – Serviços de Rede

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Diretório	LDAPv3 RFC 4510, RFC 4511, RFC 4512 e RFC 4513 . LDAP v3 extensão para TLS RFC 4510, RFC 4511 e RFC 4513.	**R**	i) Portaria Normativa nº 2, de 3 de outubro de 2002 - Publicada no D.O. do dia 4 de outubro de 2002. Seção 1, página 85. ii) Consultar errata para RFC 4511 e RFC 4512.
DNSSEC	Resolução nº 7 de 29/07/2002 – Comitê Executivo do Governo Eletrônico Práticas de Segurança para Administradores de Redes Internet Registro de Domínios para Internet no Brasil – registro.br http://registro.br/suporte/tutoriais/dnssec.html	**A**	
Mensagem instantânea	RFC 2778, RFC 3261 (atualizada pela RFC 3265, RFC 3853, RFC 4320, RFC 4916, RFC 5393, RFC 5621, RFC 5626, RFC 5630, RFC 5922), RFC 3262, RFC 3263, RFC 3264 e RFC 3265 (Atualizada pela RFC 5367 e RFC 5727)	**E**	Consultar errata para RFC 3261, RFC 3262, RFC 3264, RFC 3265 e RFC 5727.
Carimbo do tempo	RFC 3628 TSAs – *Policy Requirements for Time-Stamping Authorities*, *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (atualizada pela RFC 5816).	**R**	O serviço de carimbo do tempo deverá estar de acordo com as normas da ICP-Brasil. Consultar errata para RFC 3161.
Prevenção de DDoS	Usar métodos para inibir o uso de *IP spoofing* em ataques de DDoS nos termos do RFC 2827.	**E**	Ver http://www.ietf.org/rfc/rfc2827.txt

Tabela 9 – Especificações para Segurança – Redes Sem Fio

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
MAN[4] sem fio 802.16-2004[5] 802.16.2-2004[6] 802.16e[7] e 802.16f[8]	Utilizar PKM-EAP (*Privacy Key Management - Extensible Autentication Protocol*) com: • EAP – TLS ou TTLS; • AES[9] (Advanced Encryption Standard).	**E**	
LAN sem fio 802.11	Usar a especificação WPA2 (Wi-Fi *Protect Access*) com criptografia AES	**R**	

Tabela 10 – Especificações para Segurança – Resposta a Incidentes de Segurança da Informação

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Preservação de registros	*Guidelines for Evidence Collection and Archiving*, RFC 3227.	**R**	
Gerenciamento de incidentes em redes computacionais	*Expectations for Computer Security Incident Response*, RFC 2350. Criação de equipes de tratamento e resposta a incidentes em redes computacionais conforme Norma Complementar nº 05/09 (http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf). Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal conforme Norma Complementar nº 08/2010 (http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf)	**A**	

[4] O 802.16 é definido pelo IEEE como uma interface tecnológica para redes de acesso sem fio metropolitanas ou WMAN (*Wireless Metropolitan Access Network*).
[5] http://standards.ieee.org/getieee802/download/802.16-2004.pdf.
[6] http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf.
[7] http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.
[8] http://standards.ieee.org/getieee802/download/802.16f-2005.pdf.
[9] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Componente	Especificação	SIT	Observações
Informática Forense	*Guide to Integrating Forensic Techniques into Incident Response* – NIST - *Special Publication* 800-86 – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	**A**	
Comunicação entre Equipes e entre Centros de tratamento e resposta a incidentes	Representação para o compartilhamento de informações entre Equipes e entre Centros de Resposta a Incidentes de Segurança em Redes de Computadores: Incident Object Description Exchange Format (IODEF) – RFC 5070 **http://datatracker.ietf.org/doc/rfc5070/** http://datatracker.ietf.org/doc/rfc5070/ Extensão do formato IODEF para suportar a comunicação de eventos do tipo “phishing”. http://datatracker.ietf.org/doc/rfc5901/ Guia para a extensão do formato IODEF. http://datatracker.ietf.org/doc/rfc6684/	**E**	Deverão ser realizados estudo a respeito de procedimentos e Ferramentas para a possível adoção deste padrão.
Comunicação entre Sistemas de detecção e resposta a intrusão	Formato para compartilhamento de dados entre sistemas de detecção e resposta a incidentes de segurança computacionais: *Intrusion Detection Message Exchange Format* (IDMEF) – RFC 4765 http://datatracker.ietf.org/doc/rfc4765/	**E**	Deverão ser realizados estudo a respeito de procedimentos e Ferramentas para a possível adoção deste padrão.

8. Meios de Acesso

8.1. Meios de Acesso: Políticas Técnicas

As políticas técnicas para permitir o acesso aos serviços eletrônicos do governo federal para a sociedade em geral – cidadãos, outras esferas de governo, outros Poderes, servidores públicos, empresas privadas e outras instituições – são:

8.1.1 Os sistemas de informação do governo devem ser projetados de maneira a respeitar a legislação brasileira, fornecendo recursos de acessibilidade aos cidadãos portadores de necessidades especiais, a grupos étnicos minoritários e àqueles sob risco de exclusão social ou digital. O atendimento via balcão de prestação de serviços deve ser considerado em toda a sua abrangência, de forma a possibilitar que os benefícios decorrentes do uso dos serviços de governo eletrônico venham a ser estendidos à camada da população que não pode ter acesso direto a esses serviços por meio dos dispositivos previstos.

8.1.2 Sistemas de informação do governo que fornecem serviços de governo eletrônico:

- quando utilizarem a Internet como meio de comunicação e estações de trabalho como dispositivo de acesso, serão preferencialmente projetados para fornecer acesso a suas informações com uso de tecnologias e protocolos de comunicação da web baseados em navegadores (browsers);
- quando utilizarem outros dispositivos de acesso, como, por exemplo, telefones celulares e televisão digital, poderão fazer uso de outras interfaces além dos navegadores *web*;
- deverão ser projetados para disponibilizar aos usuários serviços de governo eletrônico por intermédio de vários meios de acesso.

8.1.3 Os sistemas de informação do governo, construídos para suportar um determinado dispositivo de acesso, devem seguir, obrigatoriamente, as especificações publicadas na e-PING para aquele dispositivo.

8.1.4 Todos os sistemas de informação do governo que forneçam serviços eletrônicos devem ser capazes de utilizar a Internet como meio de comunicação, seja diretamente ou por meio de serviços de terceiros.

8.1.5 O desenvolvimento dos serviços de governo eletrônico deve ser direcionado de modo a prover atendimento aos usuários que não tenham acesso às tecnologias mais recentes disponíveis no mercado. Por outro lado, também deve ser considerada a necessidade de atendimento àqueles usuários portadores de necessidades especiais, requisito que envolve a utilização de recursos mais sofisticados e de uso específico. De modo a conciliar essas necessidades, deverão ser observadas as recomendações do Modelo de Acessibilidade em Governo Eletrônico (e-MAG)[10].

8.1.6 Quando a Internet for usada como meio de comunicação, os sistemas de informação do governo devem ser projetados de maneira que sejam aderentes às especificações da seção 8.2. Complementarmente, a e-PING recomenda que todo serviço de governo eletrônico especifique, com clareza e, de preferência, na sua página inicial, as versões mínimas de navegadores que suportam as funcionalidades requeridas pelo serviço associado.

No atendimento ao padrão mínimo supramencionado, devem ser consideradas as exceções que envolvam questões de segurança no tratamento de informações.

8.1.7 Quando a Internet for utilizada como meio de comunicação, *middleware* ou *plug-ins* adicionais poderão ser utilizados, se não houver alternativa tecnicamente viável, para otimizar a funcionalidade do navegador nas estações de trabalho. Neste caso, esse software adicional deverá ser oferecido sem o pagamento de taxa de licença e deverá estar em conformidade com todas as especificações técnicas correspondentes discriminadas na e-PING. Além disso, deverá ser disponibilizado em repositório seguro mantido pelo órgão governamental responsável pela aplicação.

[10] BRASIL. Ministério do Planejamento, Orçamento e Gestão. Modelo de Acessibilidade em Governo Eletrônico. Versão 3.0. Brasília, 2011. Disponível em: (http://www.governoeletronico.gov.br/emag/). Acessado em: 26/09/2011.

8.1.8 Os serviços de governo eletrônico devem ser projetados de maneira a garantir aos usuários a autenticidade do conteúdo por meio de emissão de certificado digital, conforme padrões preconizados pela ICP – Brasil (http://www.iti.gov.br). Nesse sentido, todos os sítios *web* deverão obrigatoriamente utilizar "https" ao invés de "http".

8.1.9 A necessidade da sociedade aliada à possibilidade do governo desenvolver e implantar serviços eletrônicos fundamentará a definição das especificações técnicas exigidas pelos meios de acesso disponíveis. Técnicas de gerenciamento de conteúdo e tecnologias que possibilitem adaptação dos dispositivos para suportar os serviços de governo eletrônico poderão ser usadas para facilitar o acesso por meio do padrão mínimo de navegador w*eb* (conforme item 3. Políticas Gerais) e para tornar viável o uso de quiosques públicos, de balcões de atendimento e de Centrais de Atendimento ao cidadão (como, por exemplo, Telecentros).

8.1.10 Os sistemas de informação do governo federal devem prever, quando necessário e quando técnica e economicamente viável, a construção de adaptadores que permitam o acesso às informações dos serviços eletrônicos em *web* para uma diversidade de ambientes, apresentando tempos de resposta aceitáveis e custos reduzidos.

Esses adaptadores podem ser utilizados para filtrar, converter e reformatar, dinamicamente, o conteúdo *web*, de modo a se adaptar às exigências e às capacidades de exibição do dispositivo de acesso. Podem, ainda, possibilitar a modificação do conteúdo de uma página *web*, com base em protocolos de dados (XML, XSL), preferências de usuário e parametrização de rede e de dispositivos de acesso.

Esses adaptadores também poderão ser utilizados como forma alternativa de possibilitar o acesso a minorias étnicas, a portadores de deficiência visual (por exemplo: pela utilização de tradutores de textos, fontes e gráficos maiores, áudio, etc.). Tais aspectos são abordados pela Resolução n.º 7 do Comitê Executivo de Governo Eletrônico, disponível em: https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm

8.1.11 Serão considerados preferenciais aqueles tipos de arquivo que têm como padrão de representação o formato XML, de forma a facilitar a interoperabilidade entre os serviços de governo eletrônico.

8.1.12 Os serviços de governo eletrônico que disponibilizem documentos aos seus usuários deverão fazê-lo empregando no próprio link de acesso ao documento informação clara quanto a sua proveniência, versão, data de publicação e formato. Por data de publicação entende-se aquela em que o documento foi publicado em diário oficial, para os casos em que esta medida seja exigida, ou a data da disponibilização no sítio, para os demais casos. Outras informações sobre o documento, tais como, autor, redator, emissor, data tópica ou outras relevantes para a sua precisa caracterização, deverão constar no campo propriedades do próprio documento.

8.2. Meios de Acesso: Especificações Técnicas para Estações de Trabalho

Para elaboração de minutas de documentos ou trabalhos que necessitem ser criados colaborativamente por mais de uma pessoa e/ou órgão, podem ser utilizados os formatos previstos na Tabela 11.

Já para a elaboração da versão final de documentos, deve ser enviada a outros órgãos ou mesmo arquivada digitalmente, recomenda-se a utilização do formato pdf/a. Documentos que necessitem de garantia de integridade e/ou autoria, além de estarem em formato pdf/a, devem ser assinados digitalmente pelo seu autor, utilizando certificado ICP-Brasil.

A menção aos produtos que geram os formatos de arquivos citados na Tabela 11 tem como objetivo único a identificação de uma referência mínima a partir da qual os serviços de e-gov devem intercambiar informações, estando aptos a receber ou enviar arquivos em versões iguais ou posteriores às mencionadas.

Tabela 11 – Especificações para Meios de Acesso – Estações de Trabalho

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Navegadores (*browsers*)	Devem ser aderentes aos padrões W3C e aos itens Adoção de navegadores e Adoção Preferencial de Padrões Abertos em Políticas Gerais.	**A**	
Conjunto de caracteres e alfabetos	UNICODE *standard* versão 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	**R**	
Formato de intercâmbio de hipertexto	HTML versão 4.01 (.html ou .htm), gerado conforme especificações do W3C[11].	**A**	
	XHTML versões 1.0 ou 1.1 (.xhtml), gerado conforme especificações do W3C[12].	**R**	
	XML versões 1.0 ou 1.1 (.xml), gerado conforme especificações do W3C[13].	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl ou .mht)[14].	**T**	
	HTML 5 conforme especificações do W3C[15].	**E**	

[11] *HTML 4.01 Specification - W3C Recommendation 24 December 1999*. Disponível em: http://www.w3.org/TR/html4/.
[12] *XHTML 1.0 The Extensible HyperText Markup Language (Second Edition): A Reformulation of HTML 4 in XML 1.0 - W3C Recommendation 26 January 2000, revised 1 August 2002*. Disponível em: http://www.w3.org/TR/xhtml1/.
[13] *Extensible Markup Language (XML) 1.0 (Third Edition) - W3C Recommendation 04 February 2004*. Disponível em: http://www.w3.org/TR/2004/REC-xml-20040204/.
Extensible Markup Language (XML) 1.1 - W3C Recommendation 04 February 2004, edited in place 15 April 2004. Disponível em: http://www.w3.org/TR/2004/REC-xml11-20040204/.
[14] Formato de empacotamento de arquivos *web* da Microsoft (*Mime Enscapsulation of Aggregate HTML Documents*).
[15] HTML 5 (http://www.w3.org/TR/html5/).

Componente	Especificação	SIT	Observações
Arquivos do tipo documento	XML versões 1.0 ou 1.1 (.xml), ou com formatação (opcional) XSL (.xsl), gerado conforme especificações do W3C[16].	**R**	
	Open Document (.odt), gerado conforme especificações do padrão NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 conforme especificação OASIS[17].	**E**	
	Rich Text Format (.rtf).	**T**	
	PDF (.pdf).	**T**	
	PDF versão aberta PDF/A[18].	**R**	
	Texto puro (.txt).	**A**	
	HTML versão 4.01 (.html ou .htm), gerado conforme especificações do W3C.	**R**	
	HTML 5 conforme especificações do W3C[19].	**E**	
Arquivos do tipo planilha	Open Document (.ods), gerado conforme especificações do padrão NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 conforme especificação OASIS[20]	**E**	
Arquivos do tipo apresentação	Open Document (.odp), gerado conforme especificações do padrão NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 conforme especificação OASIS[20]	**E**	
	HTML (.html ou .htm), gerado conforme especificações do W3C.	**R**	
Arquivos do tipo “banco de dados” para estações de trabalho	XML versões 1.0 ou 1.1 (.xml).	**R**	Nas opções texto plano (txt) e csv, deve ser incluído obrigatoriamente o leiaute dos campos, de forma a possibilitar seu tratamento.
	MySQL Database (.myd, .myi), gerados nos formatos do MySQL, versão 4.0 ou superior.	**R**	
	Texto Puro (.txt).	**A**	
	Texto Puro (.csv) – comma-separated values	**A**	
	Arquivo do Base (.odb), gerado conforme especificações do padrão NBR ISO/IEC	**R**	

[16] *Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001*. Disponível em: http://www.w3.org/TR/xsl/.
[17] Disponível em: docs.oasis-open.org/office/v1.2/cs01/OpenDocumentv1.2-cs01.html
[18] *Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A -1)* - padrão ISO 19005-1:2005. Disponível em: http://www.iso.org/.
[19] HTML 5 (http://www.w3.org/TR/html5/).
[20] Disponível em: docs.oasis-open.org/office/v1.2/cs01/OpenDocumentv1.2-cs01.html

Componente	Especificação	SIT	Observações
	26.300:2008.		
Intercâmbio de informações gráficas e imagens estáticas	PNG (.png), gerado conforme especificações do W3C[21] – ISO/IEC 15948:2003 (E).	**A**	
	TIFF (.tif)[22].	**R**	
	SVG (.svg), gerado conforme especificações do W3C[23].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)[24].	**R**	
	BMP (.bmp).	**T**	
	GIF (.gif), gerado conforme as especificações GIF87a e GIF89a[25].	**T**	
Gráficos vetoriais	SVG (.svg), gerado conforme especificações do W3C.	**R**	
Especificação de padrões de animação	SVG (.svg), gerado conforme especificações do W3C.	**R**	
	GIF (.gif), gerado conforme a especificação GIF89a.	**T**	
Arquivos do tipo áudio e do tipo vídeo	Áudio e vídeo MPEG-4, Part 14 (.mp4)[26].	**T**	
	MIDI (.mid)[27].	**R**	
	Áudio Ogg Vorbis I (.ogg)[28].	**R**	
	Audio-Video Interleaved (.avi), com codificação Xvid.	**T**	
	Audio-Video Interleaved (.avi), com codificação divX.	**T**	
	WAVE (.wav).	**T**	
	Theora (.ogv)[29].	**R**	
	WebM[30].	**E**	
Compactação de arquivos de uso geral	ZIP (.zip).	**R**	
	GNU ZIP (.gz).	**R**	

[21] *Portable Network Graphics (PNG) Specification (Second Edition). W3C Recommendation 10 November 2003.*
ISO/IEC 15948:2003 (E) - Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification. Disponível em: http://www.w3.org/TR/2003/REC-PNG-20031110/. Acesso em: 7 dez 2005.
[22] *Tagged Image File Format (Adobe Systems).*
[23] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponível em: http://www.w3.org/TR/2003/REC-SVG11-20030114/*. Acesso em: 7 dez. 2005.
[24] *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponível em: http://www.jpeg.org/public/jfif.pdf*. Acesso em: 7 dez. 2005.
[25] *Graphics Interchange Format (CompuServe/America Online, Inc.).*
[26] *ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.*
[27] Musical Instrument Digital Interface, conforme a especificação *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., nov. 2001. Disponível em: http://www.midi.org/about-midi/specinfo.shtml. Acesso em: 30 mai. 2007.
[28] Xiph.Org Foundation. Especificação disponível em: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.
[29] Theora. Especificação disponível em: http://www.theora.org/.
[30] WebM. Especificação disponível em http://www.webmproject.org/.

Componente	Especificação	SIT	Observações
	Pacote TAR (.tar).	**R**	
	Pacote TAR compactado (.tgz ou .tar.gz).	**R**	
	BZIP2 (.bz2).	**R**	
	Pacote TAR compactado com BZIP2 (.tar.bz2).	**R**	
	MS Cabinet (.cab).	**T**	
Informações georreferenciadas – padrões de arquivos para intercâmbio entre estações de trabalho	GML versão 2.0 ou superior[31].	**A**	Indicado para estruturas vetoriais complexas, envolvendo primitivas geográficas como polígonos, pontos, linhas, superfícies, coleções, e atributos numéricos ou textuais sem limites de número de caracteres.
	ShapeFile[32].	**A**	Indicado para estruturas vetoriais limitadas a linhas, pontos e polígonos, cujos atributos textuais não ultrapassem 256 caracteres. Pode armazenar também as dimensões M e Z.
	GeoTIFF[33].	**A**	Indicado para estruturas matriciais limitadas a
Programação Estendida (Plug-ins)	Assunto para consideração futura.	**F**	

8.3. Meios de Acesso: Especificações Técnicas para Mobilidade

O número de aparelhos de telefonia móvel já ultrapassou a quantidade de telefonia fixa. Em agosto de 2011 já eram 224 milhões de aparelhos celulares habilitados no país (TELECO, 2011). Além disso, a oferta de computadores pessoais com recursos de mobilidade, a preços mais acessíveis ao cidadão, cresce a cada dia, motivada por incentivos governamentais e redução do custo de produção. Assim, torna-se um grande desafio para o governo possibilitar à sociedade acesso aos produtos e serviços do governo eletrônico, por intermédio de dispositivos móveis, em geral portáteis, como *notebooks*, celulares, *smartphones* e similares, almejando assim o aumento da inclusão digital via mobilidade.

Um conceito que vem se consolidando para a interface de aplicações aos usuários, é o de “web universal”, que seja para todos, em qualquer lugar, em qualquer momento, independente do dispositivo de acesso. Conceito este que deve ser aplicado aos serviços a serem disponibilizados por meio dos dispositivos móveis, o chamado Governo Móvel (m-Gov).

Tabela 12 – Especificações para Meios de Acesso – Mobilidade

[31] *Geography Markup Language*. Especificações disponíveis em: http://www.opengeospatial.org/standards/gml.
[32] *ESRI Shapefile Technical Description*. Disponível em: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.
[33] *GeoTIFF Format Especification*. Disponível em: http://remotesensing.org/geotiff/geotiff.html.

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Todos os Componentes	Deve ser aderente aos padrões W3C – *Mobile Web application Best Practices*, disponíveis no endereço eletrônico: http://www.w3.org/TR/2010/PR-mwabp-20101021/	**R**	

8.4. Meios de Acesso: Especificações Técnicas para TV Digital

Tendo em vista o alto nível da presença de aparelhos receptores de sinais de televisão nos lares brasileiros e a implantação do Sistema Brasileiro de TV Digital, que permite interação com os telespectadores, este se transforma em canal de grande potencial de relacionamento entre governo e sociedade. Assim surgem novas possibilidades de acesso aos produtos e serviços do governo eletrônico, a partir dos novos aparelhos de TV Digital.

Sua utilização oferece muito mais que um sinal de qualidade, proporciona interatividade e acessibilidade com serviços comerciais como: compras, jogos e acesso à bancos, e também serviços sociais, tais como: consultas ao FGTS, PIS, programas sociais do governo, tele-educação dentre outros, fazendo com que os cidadãos passem de uma atividade essencialmente passiva para uma atividade participativa.

A TV Digital torna-se um padrão de comunicação em diferentes perspectivas como: a tecnológica, com a migração do sistema analógico para o digital; a econômica, com a migração de novas possibilidades de serviços e negócios; a social, com oferta de diversidade de conteúdos e inclusão digital ao utilizar Internet através do aparelho de TV; a política, com a possibilidade de estimular a discussão de um novo marco regulatório e a comportamental, com a possibilidade de participação ativa das audiências através do uso de diferentes níveis de interatividade na TV Digital.

Para atender às questões técnicas, o Fórum do Sistema Brasileiro de TV Digital Terrestre – SBTVD, publicado junto à Associação Brasileira de Normas Técnicas – ABNT, agrupa diversas normas no sítio: http://www.forumsbtvd.org.br/materias.asp?id=112, onde está referenciado um conjunto de especificações, padronizado e livre de royalties, denominado GINGA.

Tabela 13 – Especificações para Meios de Acesso – TV Digital

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Transmissão	**ABNT NBR 15601** Parte 1 – Sistema de transmissão.	**A**	
Codificação	**ABNT NBR 15602** Parte 1 – Codificação de Video. Parte 2 – Codificação de Áudio. Parte 3 – Sistema de multiplexação de sinais.	**A**	

Multiplexação	**ABNT NBR 15603** Parte 1 – Serviços de informação do sistema de radiodifusão. Parte 2 – Sintaxes e definições da informação básica de SI. Parte 3 – Sintaxe e definição da informação estendida do SI.	**A**	
Receptores	**ABNT NBR 15604** Parte 1 – Receptores.	**A**	
Segurança	**ABNT NBR 15605** Parte 1 – Tópicos de segurança.	**A**	
Middleware	**ABNT NBR 15606** Parte 1 – Codificação de dados. Parte 2 – Ginga-NCL para receptores fixos e móveis – Linguagem de aplicação XML para codificação de aplicações. Parte 3 – Especificação de transmissão de dados. Parte 4 – Ginga-J – Ambiente para a execução de aplicações procedurais. Parte 5 – Ginga-NCL para receptores portáteis – Linguagem de aplicação XML para codificação de aplicações. Parte 6 – Java DTV 1.3. Parte 7 – Ginga-NCL – Diretrizes Operacionais para as ABNT NBR15606-2 e 15606-5	**A**	
Canal de Interatividade	**ABNT NBR 15607** Parte 1 – Protocolos, interfaces físicas e interfaces de software.	**A**	
Guia de Operações	**ABNT NBR 15608** Parte 1 – Sistema de Transmissão – Guia para implementação da ABNT NBR 15601. Parte 2 – Codificação de vídeo, áudio e multiplexação – Guia para implementação da ABNT NBR 15602. Parte 3 – Multiplexação e serviço de informação (SI) – Guia de implementação da ABNT NBR 15603.	**A**	

9. Organização e Intercâmbio de Informações

9.1. Organização e Intercâmbio de informações: Políticas Técnicas

As políticas técnicas para sistemas de organização e intercâmbio de informações e dados são:

9.1.1 Uso de XML ou JSON para intercâmbio de dados.

9.1.2 Uso de XML *Schema* para definição dos dados para intercâmbio.

9.1.3 Uso de XSL para transformação de dados.

9.1.4 Uso de Vocabulários e Ontologias do Governo Eletrônico (e-VOG) para a interoperabilidade semântica.

9.1.5 Uso de URIs conforme definido no documento "Política de URIs para Publicação de Dados no Governo", disponível em http://www.eping.e.gov.br.

9.2. Organização e Intercâmbio de Informações: Especificações Técnicas

Tabela 14 – Especificações para Organização e Intercâmbio de Informações - Tratamento e transferência de Dados

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Linguagem para intercâmbio de dados	XML (Extensible Markup Language) como definido pelo W3C http://www.w3.org/XML	**A**	
	JSON (Javascript Object Notation) Como definido pela IETC http://www.ietf.org/rfc/rfc4627.txt	**A**	
	YAML A'int Markup Language, como definido em http://www.yaml.org/	**F**	
Transformação de dados	XSL (*Extensible Stylesheet Language*) como definido pelo W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) como definido pelo W3C http://www.w3.org/TR/xslt	**A**	
Definição dos dados para intercâmbio	XML *Schema* como definido pelo W3C: - XML *Schema Part 0: Primer* http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ - XML *Schema Part 1: Structures* http://www.w3.org/TR/xmlschema-1/structures - XML *Schema Part 2: Datatypes* http://www.w3.org/TR/xmlschema-2/datatypes	**A**	
Informações georreferenciadas – catálogo de feições	Estruturação de Dados Geoespaciais Vetoriais (EDGV) como definido pela CONCAR	**R**	Para dados geoespaciais vetoriais de referência (cartografia básica)

Componente	Especificação	SIT	Observações
Metadados para informações georreferenciadas	Perfil de Metadados Geoespaciais do Brasil (Perfil MGB) como definido pela CONCAR	**E**	Conjunto básico de elementos comum a todos os tipos de produtos geoespaciais
Formato para intercâmbio de dados geoespaciais	GeoJSON, como definido em http://www.geojson.org/geojson-spec.html	**E**	
Especificação para informações de transporte público	GTFS (General Transit Feed Specification) como definido em https://developers.google.com/transit/gtfs/	**E**	

9.3. Organização e Intercâmbio de Informações: Especificações Técnicas para Vocabulários e Ontologias

A utilização de vocabulários e ontologias possibilita amplo entendimento e controle dos domínios de informação relacionados aos sistemas governamentais. A abordagem de utilização de ontologias como modelos conceituais de alto nível proporcionam maior gerência sobre os sistemas, artefato essencial na implementação de soluções de software com qualidade.

O e-VoG (Vocabulários e Ontologias do Governo Eletrônico) é um conjunto de padrões, ferramentas e metodologias para possibilitar: o intercâmbio de informações com acordo semântico, de forma a viabilizar o pronto cruzamento de dados de diversas fontes; o uso de metodologias de modelagem conceitual como forma de elicitação do conhecimento tácito das áreas de negócio de governo; o uso de ontologias como ferramenta para explicitar conhecimentos de maneira formal e coerente; o alinhamento conceitual das diversas áreas do conhecimento do governo.

As ontologias desenvolvidas no âmbito do e-VoG farão referência a conceitos externos definidos em ontologias que tenham ampla utilização nacional e internacional, de forma a aumentar o potencial para o cruzamento de dados.

Além da adoção de vocabulários e ontologias de referência na e-PING, também estão previstos os seguintes produtos para o e-VoG:

- Capacitação em ontologias;
- Conjunto de vocabulários e ontologias de domínio;
- Manual de boas práticas e processo de engenharia de ontologias;
- Repositório persistente de ontologias (vocab.e.gov.br);
- Política de URIs para Publicação de Dados no Governo.

Tabela 15 – Especificações para Organização e Intercâmbio de Informações – Vocabulários e Ontologias

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Descrição de recursos	RDF (*Resource Description Framework*) Como definido pela W3C.	**R**	

Componente	Especificação	SIT	Observações
Especificação de vocabulários para RDF	Resource Description Framework (RDF) Schema, como definido pelo W3C em http://www.w3.org/TR/rdf-schema/	**R**	Recomenda-se usar RDF Schema em situações em que o poder de processamento disponível for limitado ou onde não for necessária para descrever os dados toda a expressividade da linguagem OWL.
Elementos de Metadados para gestão de conteúdos	e-PMG – Padrão de Metadados para o Governo Eletrônico. Conforme definição em http://www.eping.e.gov.br	**R**	
Sistemas de Organização do Conhecimento	SKOS (*Simple Knowledge Organization System*) como definido pelo W3C http://www.w3.org/2004/02/skos/	**R**	
Linguagem de definição de ontologias na web	OWL (*Web Ontology Language*) Como definido pelo W3C	**R**	
Linguagem de consulta semântica	SPARQL (*Sparql Protocol and RDF Query Language*) Como definido pelo W3C	**E**	
Taxonomia para navegação	VCGE – Vocabulário Controlado do Governo Eletrônico. Conforme definição em http://www.eping.e.gov.br	**A**	
Sistema de resolução de Identificadores	*Handle system* (http://www.handle.net).	**E**	
Definição de URIs para publicação de Dados	Conforme definido nas Política de URIs para Publicação de Dados no Governo, disponível em http://governoeletronico.gov.br/biblioteca/arquivos/Politica-URIs-Publicacao-Dados-Governo	**R**	

9.3.1. Nota sobre a LAG

Em 2010 a LAG (Lista de Assuntos do Governo) passou a ser denominada VCGE – Vocabulário Controlado do Governo Eletrônico.

10. Áreas de Integração para Governo Eletrônico

10.1. Áreas de Integração para Governo Eletrônico: Políticas Técnicas

10.1.1 Neste segmento, são tratados componentes relacionados a temas transversais às Áreas de Atuação de Governo, cuja padronização seja relevante para a interoperabilidade de serviços de Governo Eletrônico, tais como Processos e Informações Geográficas, entre outras.

10.1.2 O Modelo Global de Dados (MGD) foi adotado como a Arquitetura de Interoperabilidade para o Governo, sendo a utilização de sua metodologia e notação requeridas para a construção de modelos de dados de alto nível, possibilitando o compartilhamento de informações relativas a integrações atuais e futuras de dados atreladas a uma visão de negócio, macroprocessos e dimensões de governo. Sua utilização possibilita a evolução ordenada de sistemas estruturantes de governo (legado) e o desenvolvimento de novos com maior nível de reusabilidade e interoperabilidade, além da integração à soluções estratégicas nos diversos níveis e esferas de governo. O expansão do padrão nos diversos órgãos possibilita o tratamento do modelo, através das dimensões sintática e semântica, integrando os variados MGDs e suas estruturas, viabilizando a compreensão dos modelos de dados das diversas instituições públicas e a identificação de estruturas semelhantes entre os diversos órgãos inerentes a Administração Pública. O MGD está disponível no sitio: http://modeloglobaldados.serpro.gov.br.

10.1.3 O Guia de Gestão de Processos de Governo (GGPG) tem como objetivo conduzir os diferentes órgãos da Administração Pública Federal a trabalhar padronizadamente com a Gestão de Processos. Este guia define o vocabulário comum da área de gestão de processos para governo federal, esclarece aos órgãos a importância da gestão de processos, sugere padrões de notação e artefatos necessários a modelagem de processos e com isso proporciona uma melhor troca de informações referentes aos processos de negócio entre os órgãos da Administração Pública. O GGPG está disponível em http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/guia-de-gestao-de-processos-de-governo.

10.1.4 Como diretriz técnica para integração de sistemas de informação recomenda-se a gradual adoção da Arquitetura Orientada a Serviços (SOA).

10.1.5 A tecnologia de *Web Services* é recomendada como solução de interoperabilidade da e-PING. De maneira que, independente das tecnologias em que foram implementados, possa-se adotar um padrão de interoperabilidade que garanta escalabilidade, facilidade de uso, além de possibilitar atualização de forma simultânea e em tempo real. Recomenda-se a utilização do protocolo *Simple Object Access Protocol* (SOAP) para interconexão em arquiteturas descentralizadas e/ou distribuídas para implementação de serviços em sistemas de qualquer porte. Alternativamente, recomenda-se o desenvolvimento de projetos baseados em REST, que utiliza o protocolo HTTP.

10.1.6 Para disponibilização de dados em formato aberto devem ser observadas as políticas definidas pela Infraestrutura Nacional de Dados Abertos (INDA), conforme descrito em http://wiki.gtinda.ibge.gov.br, que mantém alinhamento incondicional às premissas, politicas e especificações técnicas que regulamentam a utilização da TIC na interoperabilidade de serviços de Governo Eletrônico, estabelecidos na e-PING.

10.1.7 O segmento atuará buscando a identificação, acompanhamento da produção e análise de padrões de dados de interesse geral da Administração Pública, em articulação com grupos representativos do governo e da sociedade, reportando-se a instâncias competentes no que tange à priorização.

10.1.8 O formato dos Dados de interesse geral do governo devem ser disponibilizados no **Catálogo de Interoperabilidade**, segundo as regras de utilização desta ferramenta.

10.2. Catálogo de Interoperabilidade

10.2.1 O Catálogo de Interoperabilidade está disponível no sítio http://catalogo.governoeletronico.gov.br, sendo composto pelo Catálogo Padrão de Dados (CPD) e pelo Catálogo de Serviços Interoperáveis.

10.2.2 O Catálogo Padrão de Dados (CPD) tem por objetivo estabelecer padrões de tipos e itens de dados que se aplicam às interfaces dos sistemas que fazem parte do setor público, estando dividido em dois documentos:

- Volume 1, que estabelece os princípios gerais, isto é, as razões, abordagem e regras para a aplicação dos padrões de Tipo e Itens de Dados; e
- Volume 2, que apresenta os Tipos e Item de Dados padronizados.

10.2.3 Os Serviços Interoperáveis de interesse geral devem ser disponibilizados no **Catálogo de Interoperabilidade**, porém, há necessidade de se observar regras de utilização dos serviços de acesso restrito definidas pelos respectivos órgãos.

10.2.4 O **Catálogo de Interoperabilidade** é um elemento central do ambiente de interoperabilidade do governo federal. Sua utilização é considerada equivalente à situação Adotado (A).

10.3. Modelos para documentação de *Web Services* e outras modalidades de trocas de dados

10.3.1 Como forma de documentar os serviços interoperáveis, é recomendado o uso, em cada caso, do modelo de documentação para *Web Services* e do modelo de documentação para serviços de modo geral (não *Web Services*), como troca de arquivos, FTP, etc. Esses modelos estão disponíveis no sítio do Catálogo de Interoperabilidade.

10.3.2 A adoção dos modelos de documentação tem status equivalente à situação Recomendada (R).

10.4. Áreas de Integração para Governo Eletrônico: Especificações Técnicas

Tabela 16 – Especificações para Áreas de Integração para Governo Eletrônico – Temas Transversais a Áreas de Atuação de Governo

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
PROCESSOS – Linguagem para Execução de Processos	BPEL4WS V1.1, conforme definido pelo OASIS http://www.oasis-open.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	**R**	O grupo irá acompanhar a evolução do BPEL4WS versão 2.0. Estudos referentes à orquestração de processos e coreografia serão futuramente conduzidos pelo grupo.
PROCESSOS – Notação de Modelagem de Processos	BPMN – Business Process Model and Notation versão 1.2, definido pelo OMG http://www.omg.org/spec/BPMN/1.2/	**A**	A atualização para versão 2.0 do padrão está em estudo.
Intercâmbio de Informações Financeiras	XBRL – *eXtensible Business Reporting Language* http://www.xbrl.org/SpecRecommendations/	**R**	www.xbrl.org

Componente	Especificação	SIT	Observações
Legislação, Jurisprudência e Proposições Legislativas	LexML v. 1.0 http://projeto.lexml.gov.br	**A**	Projeto LexML define recomendações para a identificação e estruturação de documentos legislativos e jurídicos.
Planejamento Estratégico	StratML - *Strategy Markup Language* http://xml.gov/stratml/index.htm	**F**	
Integração de Dados e Processos	MGD http://modeloglobaldados.serpro.gov.br	**A**	
Informações Georreferenciadas – -Interoperabilidade entre sistemas de informação geográfica	WMS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	WFS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	WCS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	CSW versão 2.0 ou posterior http://www.opengeospatial.org/standards/cat	**A**	
	WFS-T versão 1.0 ou posterior http://www.opengeospatial.org/standards/wfs	**R**	Observar padrões e políticas de segurança indicados pelo GT2, principalmente WS-Security.
	WKT http://www.opengeospatial.org/standards/sfa	**R**	Para codificar coordenadas em serviços Web convencionais. As coordenadas devem estar em Lat/Long utilizando o datum SIRGAS2000 (EPSG:4674) ou WGS-84 (EPSG:4326). Usar GML sempre que possível.
	Filter Encoding versão 1.0 ou posterior http://www.opengeospatial.org/standards/filter	**A**	Especificação acessória para codificar expressões de filtro
	Symbology Encoding versão 1.1.0 ou posterior http://www.opengeospatial.org/standards/se	**E**	Para codificar estilos em mapas
Intercâmbio de Dados Estatísticos	SDMX – Statistical Data and Metadata Exchange http://sdmx.org/wp-content/uploads/2011/04/SDMX_2-1_SECTION_1_Framework.pdf	**E**	http://sdmx.org/

Tabela 17 – Especificações para Áreas de Integração para Governo Eletrônico – *Web Services*[34]

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Infraestrutura de registro	Especificação UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida pela OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	
	ebXML (*Electronic Business using eXtensible Markup Language*). A especificação pode ser encontrada em http://www.ebxml.org/specs/index.htm	**E**	
Linguagem de definição do serviço	WSDL 1.1 (*Web Service Description Language*) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (*Web Service Description Language*) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl20/	**E**	
Protocolo para acesso a Web Service	SOAP v1.2, como definido pelo W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/	**A**	
	HTTP/1.1 (RFC 2616)	**A**	Utilizado para desenvolvimento de projetos baseados em REST, conforme item 10.1.5
Perfil básico de interoperabilidade	*Basic Profile 1.1 Second Edition*, como definido pela WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	A versão 1.2 do Basic Profile encontra-se como rascunho (*Working Draft*) em http://www.ws-i.org/Profiles/BasicProfile-1.2.html
Portlets remotos	WSRP 1.0 (Web Services for Remote Portlets) como definido pela OASIS http://www.oasis-open.org/committees/wsrp	**E**	
Descoberta de Web Services Governamentais	DWSG, conforme especificação em http://www.eping.e.gov.br	**E**	

[34] As questões de segurança relativas a *Web Services* são abordadas no capítulo 7.

11. Glossário de Siglas e Termos Técnicos[35]

Neste item são apresentados os significados dos principais termos técnicos utilizados na e-PING.

ABNT – Associação Brasileira de Normas Técnicas: publica normas que orientam sobre a preparação e compilação de referências de material utilizado para a produção de documentos e para inclusão em bibliografias, resumos, resenhas, recensões e outros.

ACAP – *Application Configuration Access Protocol* (Protocolo de Acesso a Configuração de Aplicação): protocolo Internet para acesso a opções de programa cliente, configurações e informações preferenciais remotamente. É uma solução para o problema de mobilidade de cliente na Internet.

APF – Administração Pública Federal: reúne órgãos da administração direta (serviços integrados na estrutura administrativa da Presidência da República e dos Ministérios) e indireta (Autarquias, Empresas Públicas, Sociedades de Economia Mista e Fundações Públicas) do Poder Executivo. https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm.

BPM - *Business Process Management*: Visão dos processos de negócio de uma organização como fluxo de serviços utilizando padrões de representação de notação, execução e coordenação em XML, cujo rigor semântico permite sua interoperabilidade entre sistemas de plataformas diferentes, sendo assim um fundamento para a implementação de soluções baseada em arquitetura orientada a serviços. Quando a coordenação da execução dos serviços é realizada com subordinação a um processo mestre, em geral, intra-organização, é denominada essa coordenação como Orquestração. Quando, a coordenação se dá sem a subordinação a um processo mestre, em geral, interorganização, denomina-se Coreografia.

CONCAR – Comissão Nacional de Cartografia: órgão colegiado do Ministério do Planejamento, Orçamento e Gestão, com as atribuições de assessorar o Ministro de Estado na supervisão do Sistema Cartográfico Nacional (SCN), de coordenar a execução da política cartográfica nacional e de exercer outras atribuições nos termos da legislação pertinente.

Criptografia: Técnica de proteção de informação que consiste em cifrar o conteúdo de uma mensagem ou um sinal, transformando-o em um texto ilegível, por meio da utilização de algoritmos matemáticos complexos.

CSW – *Catalogue Services for the Web*: especificação OGC que define interfaces para publicar, acessar, navegar e consultar metadados sobre informações georreferenciadas na Internet (HTTP).

Diretório – Serviço que armazena e organiza informações sobre os recursos e os usuários de uma rede de computadores, e que permite os administradores de rede gerenciar o acesso de usuários e sistemas a esses recursos. Além disso, serviço de diretório podem atuar como uma camada de abstração entre os usuários e esses recursos." no item 11 - "Glossário de Siglas e Termos Técnicos.

DNS – *Domain Name System* (Sistema de Nomes de Domínio): forma como os nomes de domínio são encontrados e traduzidos no endereço de protocolo da Internet. Um nome de domínio é um recurso fácil de ser lembrado quando referenciado como um endereço na Internet.

EDGV – Estruturação de Dados Geoespaciais Vetoriais: as Especificações Técnicas para Estruturação de Dados Geoespaciais Vetoriais (ET-EDGV) são um componente da estruturação de dados cartográficos da Infraestrutura Nacional de Dados Espaciais (INDE). Seu objetivo é padronizar estruturas de dados que viabilizem o compartilhamento e a interoperabilidade para dados geoespaciais vetoriais de referência (cartografia básica).

Filter Encoding: Especificação OGC usada para codificar expressões de filtro em consultas. É uma especificação de uso geral que serve de acessório para outras, notadamente o WFS e o

[35] Microsoft Press. Dicionário de informática. Tradutor e consultor editorial Fernando Barcellos Ximenes – KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.

Thing, Lowell (ed.). Dicionário de Tecnologia. Tradução de Bazán Tecnologia e Linguística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

CSW.

FTP – *File Transfer Protocol* (Protocolo de Transferência de Arquivo): é um protocolo aplicativo que utiliza os protocolos TCP/IP da Internet, sendo a maneira mais simples de trocar arquivos entre computadores na Internet.

GeoJSON: Formato para codificar várias estruturas de dados geográficas, baseado na JavaScript Object Notation (JSON). Um objeto GeoJSON pode representar uma geometria, uma feição geográfica ou uma coleção de feições.

GML – *Geography Markup Language*: especificação OGC baseada em XML desenvolvida para permitir o transporte e armazenamento de informações geográficas/espaciais.

GTFS – General Transit Feed Specification: Define um formato comum para tabelas de horário de transporte público e de informações geográficas associadas. O "feed" GTFS permite que as agências de transporte público publiquem seus dados e que desenvolvedores escrevam aplicações que consomem esses dados em um modo interoperável.

Handshake: Em uma comunicação via telefone, troca de informações entre dois modems e o resultante acordo sobre que protocolo utilizar antes de cada conexão telefônica.

Hashing: É a transformação de uma cadeia de caracteres em um valor de tamanho fixo normalmente menor ou em uma chave que representa a cadeia original. É utilizada para indexar e recuperar itens em um banco de dados, porque é mais rápido encontrar o item utilizando a menor chave transformada do que o valor original. Também é utilizada em algoritmos de criptografia.

HTTP – *Hyper Text Transfer Protocol* (Protocolo de Transferência de Hipertexto): conjunto de regras para permuta de arquivos (texto, imagens gráficas, som, vídeo e outros arquivos multimídia) na *World Wide Web*.

HTTPS – *Secure Hyper Text Transfer Protocol* (Protocolo de Transferência de Hipertexto Seguro): protocolo *web* desenvolvido pela Netscape e acoplado ao navegador. Criptografa e criptoanalisa solicitações e retornos de páginas retornadas pelo servidor *web*. O HTTPS é apenas o uso do SSL (*Secure Sockets Layer*) do Netscape como uma subcamada sob a organização normal dos programas das aplicações HTTP.

ICP – Brasil: conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. http://www.iti.gov.br.

IEEE – *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Elétricos e Eletrônicos): fomenta o desenvolvimento de padrões e normas que frequentemente se tornam nacionais e internacionais.

IETF – *Internet Engineering Task Force* (Força Tarefa de Engenharia da Internet): entidade que define protocolos operacionais padrão da Internet, como o TCP/IP.

IMAP – *Internet Message Access Protocol* (Protocolo de Acesso a Mensagem na Internet): protocolo padrão para acessar e-mail a partir do servidor local. IMAP é um protocolo cliente-servidor em que o e-mail é recebido e guardado pelo servidor de Internet.

IP – *Internet Protocol* (Protocolo de Internet): protocolo que permite a comunicação entre dispositivos na rede. De forma genérica, pode ser considerado como um conjunto de números que representa o local de um determinado equipamento (normalmente computadores) em uma rede privada ou pública.

IPSec – *Internet Protocol Security* (Segurança de Protocolo de Internet): padrão de desenvolvimento relativo à segurança na camada da rede ou do processamento de pacotes da comunicação em rede. Uma grande vantagem do IPsec é que as disposições de segurança podem ser manipuladas sem exigir mudanças nos computadores de usuários individuais. O IPsec fornece duas opções de serviços de segurança: *Authentication Header* (AH), que essencialmente permite a autenticação do remetente de dados, e *Encapsulating Security Payload* (ESP), que suporta tanto a autenticação do remetente quanto a codificação criptográfica de dados.

IPv4 – *Internet Protocol Version 4* (Protocolo de Internet Versão 4): é a versão do protocolo IP mais utilizada atualmente. É formada por um número de 32 bits escrito com quatro octetos no formato decimal, separados por pontos (exemplo: 161.148.1.18). A primeira parte do endereço

identifica uma rede específica na inter-rede e a segunda parte identifica um equipamento (host) dentro dessa rede.

IPv6 – *Internet Protocol Version 6* (Protocolo de Internet Versão 6): é a versão mais atual do protocolo IP. É formada por um número de 128 bits escrito em oito campos de quatro dígitos hexadecimais, separados por dois pontos (exemplo: 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344); e inclui prefixo de rede e sufixo de host. Ele está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "pilha dupla", por algum tempo. A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de 4 bilhões (4 x 109) de endereços, contra cerca de 3,4 x 1038 endereços do novo protocolo.

JSON – *Javascript Object Notation*: um formato de troca de dados leve, baseado em texto e de fácil representação. Embora seja baseado em Javascript, o formato é independente de linguagem. Ele define um pequeno conjunto de regras de formatação para a representação portável dos dados: estruturas de dados baseadas em vetores, apresentadas também como objetos.

LAN – *Local Area Network* (Rede Local): grupo de computadores e dispositivos associados que compartilham uma mesma linha de comunicação e normalmente os recursos de um único processador ou servidor em uma pequena área geográfica. Normalmente, o servidor possui aplicações e armazenamento de dados compartilhados por vários usuários em diferentes computadores.

LDAP – *Lightweight Directory Access Protocol* (Protocolo Leve de Acesso a Diretório): protocolo de software para permitir a localização de organizações, de pessoas e de outros recursos como arquivos e dispositivos em uma rede, seja na Internet pública ou em uma intranet corporativa.

Mensageria em Tempo Real ou Mensagem Instantânea: É um tipo de comunicação que permite que um usuário troque mensagens em tempo real com outro usuário também conectado à rede.

Metadados: Conhecido como “dados sobre dados” metadados são utilizados para registrar atributos sobre um recurso informacional visando facilitar a recuperação, a gestão, a interoperabilidade, dar suporte à identificação digital e dar suporte ao arquivamento e preservação.

Middleware: *É* um termo geral que serve para mediar dois programas separados e normalmente já existentes. Aplicações diferentes podem comunicar-se através do serviço de *Messaging*, proporcionado por programas *middleware*.

MGD - Modelo Global de Dados: É um macromodelo integrado e dinâmico que se destina a ser usado como referência para a manutenção e para o desenvolvimento de novas versões dos sistemas estruturantes e soluções que requeiram integração de dados em outros sistemas.

OGC – *Open Geospatial Consortium* (consórcio internacional *Open Geospatial*): possui a missão de “desenvolver especificações para interfaces espaciais que serão disponibilizadas livremente para uso geral”.

Ontologia: Na filosofia, ontologia é o estudo da existência ou do ser enquanto ser, ou seja, a maneira de compreender as identidades e grupos de identidades. Na ciência da computação, é um modelo de dados que representa um conjunto de conceitos sob um domínio e seus relacionamentos, ou, mais formalmente, especifica uma conceitualização dele.

Padrão Aberto:

I - possibilita a interoperabilidade entre diversos aplicativos e plataformas, internas e externas;
II - permite aplicação sem quaisquer restrições ou pagamento de royalties;
III - pode ser implementado plena e independentemente por múltiplos fornecedores de programas de computador, em múltiplas plataformas, sem quaisquer ônus relativos à propriedade intelectual para a necessária tecnologia.

Padrão de Metadados: um padrão de metadados estabelece um conjunto de elementos de metadados para uma comunidade, incluindo a especificação de cada elemento e esquemas de codificação para permitir a interoperabilidade entre os sistemas que utilizam o padrão.

PDCA – *Plan-Do-Check-Act* (Planejar-Executar-Verificar-Agir): Ferramenta de gestão da qualidade com foco na melhoria contínua de processos.

Perfil MGB – Perfil de Metadados Geoespaciais do Brasil: conjunto básico e necessário de elementos que caracterizam os produtos geoespaciais conforme definido pela CONCAR. Perfil

baseado na norma internacional ISO 19115:2003 (Geographic information – Metadata).

Plug-in: Um programa acessório que adiciona capacidades ao programa principal. Normalmente, em aplicações *web*, são programas que podem ser facilmente instalados e usados como parte do navegador. Uma aplicação de plug-in é reconhecida automaticamente pelo navegador e a função é integrada à página HTML que está sendo apresentada.

POP3 – *Post Office Protocol* 3 (Protocolo dos Correios 3): versão mais recente do protocolo padrão para recuperar e-mails. O POP3 é um protocolo de cliente/servidor no qual o e-mail é recebido e guardado pelo servidor de Internet.

Portal: Sítio na Internet que agrega serviços, notícias e grande volume de conteúdo informativo e/ou de entretenimento.

REST: *Representational State Transfer* (Transferência de Estado Representacional). Técnica de engenharia de software para sistemas hipermídia distribuídos.

RFC – *Request for Comments* (Solicitação de Comentários): documento formal da IETF, resultante de modelos e revisões de partes interessadas. A versão final do RFC tornou-se um padrão em que nem comentários nem alterações são permitidos. As alterações podem ocorrer, porém, por meio de RFCs subsequentes que substituem ou elaboram em todas as partes dos RFCs anteriores. RFC também é a abreviação de Remote Function Call (chamada funcional remota).

RSA – *Rivest-Shamir-Adleman*: cifração de Internet e um sistema de autenticação que utiliza um algoritmo desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman.

SE – Symbology Encoding: especificação OGC usada para codificar estilos de apresentação para dados geoespaciais vetoriais e matriciais. Em suas primeiras versões fazia parte do perfil Styled Layer Descriptor (SLD) do WMS, até ser separada em outra parte que possibilita seu uso por demais serviços ou formatos.

Sistemas de Organização do Conhecimento: No padrão SKOS (*Simple Knowledge Organization System*), segundo o documento de referência do W3C, são considerados sistemas de organização do conhecimento os tesauros, esquemas de classificação, listas de assuntos, taxonomias, e outros tipos de vocabulários controlados.

S/MIME – *Secure Multi-Purpose Internet Mail Extensions* (Extensões de Correio de Internet Multipropósito Seguras): método seguro de enviar e-mail que usa o sistema de cifração RSA (Rivest-Shamir-Adleman). S/MIME descreve como informações encriptadas e um certificado digital podem ser incluídos como parte do corpo da mensagem.

SMTP/MIME – *Simple Mail Transfer Protocol/Multi-purpose Internet Mail Extensions* (Protocolo de Transferência de Mensagem Simples/Extensões de Correio de Internet Multipropósito): SMTP é um protocolo TCP/IP usado no envio e recepção de e-mails. MIME é uma extensão de protocolo de e-mail original da Internet que possibilita a troca de diferentes tipos de arquivos de dados pela Internet.

SOA - *Service Oriented Architecture* (Arquitetura Orientada a Serviços): é um paradigma para organização e utilização de competências distribuídas que estão sob controle de diferentes domínios proprietários. A arquitetura SOA é utilizada para interoperabilidade de sistemas por meio de conjunto de interfaces de serviços fracamente acoplados (*loosely coupled*), onde os serviços não necessitam de detalhes técnicos da plataforma dos outros serviços para a troca de informações ser realizada.

SOAP – *Simple Object Access Protocol* (Protocolo Simples para Acesso a Objetos): descreve um modelo para o empacotamento de perguntas e respostas XML.O envio de mensagens SOAP é utilizado para permitir o intercâmbio de uma variedade de informações XML. A norma de SOAP assume a tarefa de transmitir pedidos e respostas sobre serviços entre usuários e fornecedores de serviços.

Software Livre: Programa de computador disponível através de seu código-fonte e com a permissão para qualquer um usá-lo, copiá-lo e distribuí-lo, seja na sua forma original ou com modificações, seja gratuitamente ou com custo. O software livre é necessariamente não proprietário, mas é importante não confundir software livre com software grátis.

SSL – *Secure Sockets Layer* (Camada de Soquetes Segura): é um protocolo comumente usado

para gerenciar a segurança de uma transmissão de mensagem na Internet.

Taxonomia para Navegação: É um vocabulário controlado de termos e frases, organizado e estruturado hierarquicamente, de acordo com relações naturais ou presumidas, objetivando facilitar aos usuários de sítios e portais da Internet a descoberta de informação através da navegação.

TCP – *Transmission Control Protocol* (Protocolo de Controle de Transmissão): conjunto de regras usadas com o IP para enviar dados na forma de unidades de mensagem entre computadores pela Internet. Enquanto o IP lida com a entrega real dos dados, o TCP controla as unidades individuais dos dados em que uma mensagem é dividida para roteamento eficiente através da Internet.

TIC: Tecnologia da Informação e Comunicação

TLS – *Transport Layer Security* (Segurança de Nível de Transporte): protocolo que garante a privacidade entre os aplicativos de comunicação e seus usuários na Internet. Quando um servidor e o cliente se comunicam, o TLS garante que nenhuma outra parte poderá ver ou apanhar a mensagem.

Token: Um objeto de dados estruturado ou uma mensagem que circula continuamente entre os nós de uma rede *token ring* e descreve o estado atual da rede.

UDDI – *Universal Description Discovery and Integration* (Descrição, Descoberta e Integração Universais): é o repositório no qual os desenvolvedores registram os *Web Services* disponíveis que permitem aos clientes a descoberta e a utilização dos serviços alocados em Extranets e Intranets.

UDP – *User Datagram Protocol* (Protocolo de Datagrama de Usuários): protocolo de comunicação que oferece uma quantidade limitada de serviço quando as mensagens são trocadas entre computadores em uma rede que usa o IP. O UDP é uma alternativa para o TCP e, com o IP, é referido como UDP/IP. Assim como o TCP, o UDP usa o IP para levar uma unidade de dados de um computador para outro. Diferentemente do TCP, o UDP não fornece o serviço de dividir uma mensagem em pacotes e remontá-la na outra extremidade. O UDP não fornece a sequência dos pacotes em que os dados chegam. Isso significa que o programa de aplicativo que usa o UDP deve garantir que a mensagem inteira chegou e está em ordem. Os aplicativos de rede que querem poupar o tempo de processamento porque têm unidades muito pequenas de dados para trocar podem preferir o UDP em vez do TCP.

URI – *Uniform Resource Identifier* (Identificador Único de Recurso): padrão de codificação de nomes e endereços na Internet. Uma URI é composta por um nome (ex.: file, http, ftp, news, mailto, gopher), seguido por dois pontos, e por fim, um caminho, padronizado por uma lista de esquemas que segue a RFC 1630. A URI agrupa os conceitos URNs e URLs.

VPN – *Virtual Private Networks* (Rede Privada Virtual): Rede particular, que se utiliza da infraestrutura de uma rede pública de telecomunicações, como a Internet, por exemplo, para a transmissão de informações confidenciais. Os dados transmitidos são encriptados. Sua implementação se dá por meio de túneis virtuais, pelos quais trafegam as informações, protegendo-as do acesso de usuários não autorizados.

W3C – *World Wide Web Consortium* (Consórcio da Rede Mundial *Web*): associação de indústrias que visa promover padrões para a evolução da *web* e interoperabilidade entre produtos para WWW produzindo softwares de especificação e referência.

WAN – *Wide Area Network* (Rede de Grande Área): Rede de computadores que abrange extensas áreas geográficas como um estado, um país ou um continente.

WCS – *Web Coverage Service*: especificação OGC que define a interface de um serviço para acessar informações georreferenciadas que possuem valores em todo o espaço considerado, sem fronteiras bem definidas (geo-campos).

Web Services: Aplicação lógica, programável que torna compatíveis entre si os mais diferentes aplicativos, independentemente do sistema operacional, permitindo a comunicação e intercâmbio de dados entre diferentes redes.

WFS – *Web Feature Service*: especificação OGC que define a interface de um serviço que permite acessar e manipular dados geográficos codificados em GML na Internet (HTTP). Duas classes de serviços podem ser definidas:

- **WFS Básico (WFS):** implementa operações somente leitura, que permitem obter os

dados espaciais.

- **WFS Transacional (WFS-T):** implementa as operações transacionais, usadas para manipular os dados remotamente.

WMS – *Web Map Service*: especificação OGC que define a interface de um serviço para disponibilizar mapas (dados geográficos editados) ou imagens na Internet (HTTP).

WSDL – *Web Services Definition Language* (Linguagem para definição de Serviços *Web*): é um formato XML para descrição de serviços *web* e suas informações para acesso. Ela descreve as funcionalidades dos serviços oferecidos pelo provedor de serviços, bem como sua localização e forma de acesso.

XML – *eXtensible Markup Language* (Linguagem Markup Estensível): maneira flexível para criar formatos de informações comuns e compartilhar ambos os formatos e os dados na *World Wide Web*, nas intranets e em qualquer lugar. O XML é extensível porque, diferentemente do HTML, os símbolos markup são ilimitados e se autodefinem.

XML *Schemas:* São documentos XML, encontrados também num sitio Internet, que especificam a estrutura, número de ocorrências de cada elemento, valores permitidos, unidades, etc, ou seja, a sintaxe do documento. Os Esquemas de um conjunto de documentos XML, de um mesmo tipo, ficam disponíveis publicamente num sitio Internet, para que programas possam ter acesso a eles para validar os documentos XML deste conjunto.

XMPP – *eXtensible Messaging and Presence Protocol* (Protocolo de Mensageria em Tempo Real): Protocolo aberto, baseado em XML para mensagens em tempo real.

XSL – *eXtensible Stylesheet Language*: linguagem de criação de planilhas que descreve como um dado é mandado por meio da *web*, usando o XML, e é apresentado ao usuário. O XSL é uma linguagem para formatar um documento XML.

XSLT – *eXtensible Stylesheet Language Transformations*: jeito padrão de descrever como mudar a estrutura de um documento XML em um outro documento XML com outra estrutura. O XSLT pode ser pensado como uma extensão do XSL. O XSLT mostra como o documento XSL deve ser reorganizado em uma outra estrutura de dados (que pode ser apresentado seguindo uma planilha do XSL).

YAML – Ain't Markup Language: Formato de serialização de dados legível por humanos que utiliza conceitos de linguagens de programação como C, Perl, e Python, e ideias do XML e o formato de dados do correio eletrônico (RFC 2822).

12. Integrantes

Coordenação da e-PING

Advocacia-Geral da União (AGU)
Márcio Gonçalves

Agência Nacional de Águas (ANA)
Sérgio Augusto Barbosa
Takaharu Uchino

Agência Nacional de Aviação Civil (ANAC)
Alexandre Fraga Almeida

Agência Nacional do Cinema (ANCINE)
Hime Aguiar e Oliveira Júnior

Agência Nacional de Energia Elétrica (ANEEL)
Wilson Delgado Pinto
Antônio Campos Monteiro Neto

Agência Nacional de Saúde Suplementar (ANS)
Sérgio Oliveira Costa Júnior
Márcia Elizabeth Marinho da Silva

Banco do Brasil (BB)
Kraucer FernandesMazuco
Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)
Paulo Maia da Costa

Empresa de Correios e Telégrafos (ECT)
Eloy Arnaud Duque

Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
Adriano dos Santos Vieira

Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN)
Carlos Augusto Pessoa Machado
Delson Pereira da Silva

Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP)
Everton Batista dos Santos
Ramon Moreno de Matos Vieira

Instituto Nacional de Tecnologia da Informação (ITI/PR)
Antônio Sérgio Borba Cangiano
Ruy César Ramos Filho

Ministério da Ciência, Tecnologia e Inovação (MCTI)
George Hideyuki Kuroki Junior
Anivaldo Soares Vale

Ministério da Justiça (MJ)
Márcio Lopes de Freitas Filho
Guilherme Augusto F. De Moraes-Rego

Ministério da Justiça/Polícia Federal (MJ/DPF)
Jorilson da Silva Rodrigues

Ministério da Pesca e Aquicultura (MPA)
Alexandre Palhares Ribeiro
Thiago Augusto dos Santos Silva

Ministério da Saúde (MS)
Augusto Cesar Gadelha Vieira
Maurício Bucciolli Guernelli

Ministério do Desenvolvimento Agrário (MDA)
Vitor Carneiro Soares
Geraldo de Paula Martins

Ministério do Planejamento, Orçamento e Gestão – Secretaria de Logística e Tecnologia da Informação (MP/SLTI)
João Batista Ferri (Coordenador Geral)
Ana Paula Pessoa Mello
Carlos Eduardo Araújo Vieira
Everson Lopes de Aguiar
Fernanda Hoffmann Lobato
Hermógenes Batista Correia
Hudson Vinícius Mesquita
Leandro Vieira Rodrigues
Rachel Cristina Guimarães Monteiro Domingos

Ministério do Turismo (MTur)
Sumaid Andrade de Alburqueque
Maria Aparecida Gomes

Nuclebrás Equipamentos Pesados S/A (NUCLEP)
Adilson Custódio
Helio de Araújo e Castro

Receita Federal do Brasil (RFB)
Edna Pereira Pinto Fernandes
Carlos Maurício Farjoun

Secretaria de Administração (SA/PR)
Maurício Theodosio Marques Mattos
Inálio de Sena Correa

Secretaria de Direitos Humanos (SDH/PR)
Daniel Miranda Rogério
Wesley Rodrigo Couto Lira

Secretaria Nacional de Juventude (SNJ/PR)
Carla de Paiva

Serviço Federal de Processamento de Dados (SERPRO)
José Maria Leocádio
Marcus Vinícius da Costa

Tribunal de Contas da União (TCU)
Mauricio Ramos e Silva
Geraldo Magela Lopes de Freitas

Grupo de Trabalho Interconexão – GT1

Leandro Vieira Rodrigues (MP) – Coordenador
André Gustavo de Andrade Moreira (ANEEL)
Augusto Ewerton Dias Ferreira (MF)
Carino Andrade Rodrigues (BB)
David Fagundes Cordeiro Junior (MP)
Filipe Carneiro Guimarães (IPEA)
Hermógenes Ramos Batista Correia (MP)
Joaquim Eudes Mendes Gomide (BB)
Jorilson da Silva Rodirgues (MJ)
Loriza Andrade Vaz de Melo (MP)
Marcos Fernandes Albuquerque Lima (MC)
Roberto Sefan Fernandes de Aguiar (ANEEL)
Sérgio Tadeu Neiva Carvalho (CGU)

Grupo de Trabalho Segurança – GT2

Jorilson da Silva Rodirgues (DPF) – Coordenador
Adelino F. S. Correia (MS)
Ana Lúcia Basilio de Oliveira Silva (MS)
Antônio Acras Filho (SERPRO)
André Machado Caricatti (ITI)
Augusto Ewerton Dias Ferreira (MF)
Dante de Matos Gomes (PRODEB)
Elane Coelho Lima (MPA)
Filipe Carneiro Guimarães (IPEA)
Gilberto de Oliveira Netto (SERPRO)
Hélio Marçola Jr (PRODASEN)
Humberto Degrazia Campedelli (DATAPREV)
Jean Carlo Rodrigues (ITI)
Joel Corrêa (DATAPREV)
José Eduardo Malta de Sá Brandão (IPEA)
José Ney de Oliveira Lima (MP)
Luiz Gustavo Lustosa Colombo (IPHAN)
Marcos Cícero S. Wanderlei (Correios)
Marcos Fernandes (MC)
Marcos Gomes Figueira (BB)
Marcos J.C. Euzébio (BACEN)
Mario Henrique Paes Vieira (MP)
Paulo Coelho Ventura Pinto (ANS)
Sandro Herman Pereira Rehem (MP)
Sérgio Soares da Silva (INEP)
Silvio Correia Filho (SERPRO)

Grupo de Trabalho Meios de Acesso – GT3

Paulo Maia da Costa (CAIXA) – Coordenador
Adriano César de Oliveira (MP)
Artur Emílio de Rezende (MF)
Bruno Pacheco de Assis (SERPRO)
Carlos Bellone Neto (RFB)
Cláudio Muniz Machado Cavalcanti (MP)
Danielle de Menezes Maciel Silva (ANVISA)
Denise Barros de Sousa (MEC)
Eliane Aristóteles Moreira (DATAPREV)
Frederico Cabral de Menezes (CONAB)
Geancarlo Noronha Vinhal (SERPRO)
Helius Tavares de Oliveira (SERPRO)
Jacob Batista de Castro Junior (MP)
Jorge Arruda (MP)
Jorge L. S. Oliveira (ECT)

Juscelino Kilian (PR/GSI)
Márcio F. Viana M. (ME)
Márcio Humberto M. Cammarota (SERPRO)
Marconi Pereira Sodate (RFB)
Marcos Gomes Figueira (BB)
Mauro Lemes da Silva (CAIXA)
Murilo Dantas Barreto (BB)
Pedro Paulo Lemes Machado (ITI)
Reinaldo Silva Simão (PR)
Rubia Scrocaro (CAIXA)
Sônia Regina Rodrigues Motta (MEC)
Viviane Regina Lemos Bertol (ITI)
Wagner Ferreira Carneiro Junior (MF)
Wesley Gomes de Sousa (SERPRO)

Grupo de Trabalho Organização e Intercâmbio de Informações – GT4

Carlos Eduardo Araújo Vieira (MP) – Coordenador

Sub-Grupo: Vocabulários e Ontologias de Governo Eletrônico (e-VOG)

Carlos Eduardo Araújo Vieira (MP) – Coordenador
Ana Paula Mello (MP)
Angela Baylo (CAIXA)
Augusto Herrmann (MP)
Christian Moryah Contiero Miranda (MP)
Emerson Xavier (MD/CEX)
Helio Kuramoto (IBICT)
Hudson Vinícius Mesquita (MP)
João Alberto de Oliveira Lima (RFB)
Neuza Arantes Silva (MAPA)
Nitai Bezerra da Silva (MP)
Rachel Cristina Guimarães Monteiro Domingos (MP)
Ramón Martins S da Fonseca (IBICT)
Roberto Lyra (MP)
Rommel Novaes Carvalho (CGU)
Sandra Paula de Brito Aguiar(Força Aérea Brasileira)
Siomara Zgiet (MS)

Sub-Grupo: Vocabulário Controlado do Governo Eletrônico (VCGE)

Roberto Lyra (MP) – Coordenador
Aline Borges (ICMBio)
Augusto Herrman (SLTI/MP)
Bárbara R. B. Sallaberry (CODIN/MP)
Caio Braga Vilas Boas (ANEEL)
Christian R.C. Miranda (SLTI/MP)
Cristine C Marcial Pinheiro (CODIN/MP)
Daniel Aguiar (SOF/MP)
Eleidimar Odilia da Silva (SLTI/MP)
Elias Ribeiro da Silva (PGR)
Everson Lopes Aguiar (SLTI/MP)
Fabiola Marques Ferigato (Câmara)
Fernanda Hoffmann Lobato (SLTI/MP)
Idalécio José de Aquino (ANEEL)
Janaína Ruivo dos Santos (Arquivo Nacional)
João Alberto de Oliveira Lima (PRODASEN)
Livia Cristina O de Souza (ANEEL)
Lucia Elande da Silva dos Santos (MAPA)
Lucia Helena C Valverde (SOF/MP)
Lucia Taira Miyazak (MAPA)

Luis Sergio de Oliveira Araujo (SOF/MP)
Marcia Pachaly (SECOM/PR)
Maria de Fátima Jaegger (Senado)
Mônea Maria Caetano Trindade (MDIC)
Neuza Arantes Silva (MAPA)
Nitai Bezerra da Silva (SLTI/MP)
Osmar Arouck (Senado)
Otávio Moreira de Castro Neves (CGU)
Paulo Cesar Viana Maline (DATASUS)
Rafael Melo (ICMBio)
Rejane Rodrigues de Carvalho (SPI/MP)
Roberta Penha e Silva Marins (ANEEL)
Roberto Kodama (CGU)
Sergio Roberto Guedes Reis (CGU)
Sergio Santos (MAPA)

Grupo de Trabalho Áreas de Integração para Governo Eletrônico – GT5

Marcus Vinícius da Costa (SERPRO) – Coordenador

Subgrupo: ABEP – Associação Brasileira de Entidades Estaduais de TIC

Romero Guimarães (ATI / PE) – Coordenador
Dayse Vianna (PRODERJ – ABEP) – Coordenadora Suplente
Everson Lopes de Aguiar (MP)
Marcus Vinicius Costa (SERPRO)
Quédima Sales (INFRAERO)
Reni Elisa da Silva Pontes (FMT)
Roberto Kodama (CGU)
Rômulo Santos (ETICE/CE)
Verlaynne Rocha (Governo de Pernambuco / ATI)
Welson de Marino Vianna (SERPRO)

Subgrupo: Padrão INDE – Intercâmbio de Informações Espaciais

Emerson Magnus de A. Xavier (MD/CEX/CIGEx) – Coordenador
Luciana Campos Mota (SERPRO) – Coordenadora Suplente
Hesley Py (IBGE)
Moema José de Carvalho Augusto (IBGE)
Rodrigo Hjort (SERPRO)
Wesley Silva Fernandes (IBGE)

Subgrupo: Padrão BPM – Business Process Management

Daniel Viero (BACEN) – Coordenador
Pilade Baiocchi Neto (MCT) – Coordenador Suplente
Adelnei Felix (ATI / PE)
André Luiz Matos Rodrigues da Silva (Inmetro)
Claudia Cappelli (UNIRIO)
Cristiane Bueno Mariani (Exército Brasileiro)
Debora Reis (MP)
Dualceu Davis (Ministério da Defesa)
Eduardo Moraes (MP)
Eleidimar Odília Isaque da Silva (MP)
Eliel Martins (Exército Brasileiro)
Everson Lopes de Aguiar (MP)
Fernando Escobar (ENAP)
Gustavo Felhberg (MP)
Igor Takenami (PRODEB)
Jennifer Staar Hamilton (PRODEB)
Jones Madruga (ELO Group)
José Benjamim Borges (SERPRO)

Joseilson de Assis Costa (ICMBio)
Julio Cezar de Oliveira Maltez (PRODEB)
Kalina Porto (MF)
Lidia Cristina Bueno Chamelete (BB)
Luciana Carla Lins e Silva (PRODEB)
Luciana Mota (SERPRO)
Luciano Antonio Costa (CAIXA)
Marcello Alexandre Kill (SERPRO)
Marcio André Dell Aglio Frick (UFSM)
Marcos Fernandes Albuquerque Lima (MinCon)
Marcos Vinícius Amorim Ferreira Guimarães (MP)
Marcus Vinicius Costa (SERPRO)
Nayara Barreto Matos (PRODEB)
Nelson Nóbrega Júnior (BACEN)
Nicir Maria Gomes Chaves (MPS)
Pedro Borges Mourão (MP / RJ)
Raul Antunes (DATAPREV)
Regina Silva (MP / RJ)
Reni Elisa da Silva Pontes (IFMT)
Rosana de Souza Ribeiro Freitas (IBAMA)
Sidney Batista Filho (SERPRO)
Talita Arantes (INFRAERO)
Tânia Miranda (PRODEB)
Valter Camargo (BACEN)
Walcir Fontanini (CTI)

Subgrupo: Padrão MGD – Modelo Global de Dados

Luciana Campos Mota (SERPRO) – Coordenadora
Quédima Sales (Infraero) – Coordenadora Suplente
Augusto Herrmann (MP)
Cristiane Bueno Mariani (Exército Brasileiro)
Daniel Viero (Bacen)
Eduardo Arend Leao (Infraero)
Everson Lopes de Aguiar (MP)
Flávio Horácio Vieira (Infraero)
Jorge Maciel Pereira (Dataprev)
Joseilson de Assis Costa (ICMBio)
Luciano Antonio Costa (CEF)
Marcello Alexandre Kill (SERPRO)
Marcus Vinicius Costa (SERPRO)
Pedro Borges Mourão (MP-RJ)
Pilade Baiocchi Neto (MCTI)
Ronie Peterson de Oliveira Aguiar dos Santos (Infraero)
Sidney Batista Filho (SERPRO)
Talita Arantes (Infraero)
Vinicius Silva (MP)
Welson de Marino Vianna (SERPRO)

Subgrupo: Padrões WEB – *Web Services*

Paulo Gladson Ximenes Pinheiro (SERPRO) – Coordenador
Clovis Lemes Ferreira Junior (SERPRO) – Coordenador Suplente
Ádria Ferreira (SERPRO)
Adriana Teles (PRODEPA)
Alysson Magalhaes da Costa (SERPRO)
Érica Viana Cruz (ANAC)
Carlos Roberto Gonçalves Viana (PRODERJ)
Clovis Lemes Ferreira Junior (SERPRO)
Daiane Vaz Lima (SERPRO)
Daniel goulart crosara (SERPRO)
Evandro Paes (PRODEPA)

Everson Lopes de Aguiar (MP)
Fabiano Sardenberg kuss (SERPRO)
Fernando Fernandes da Silva Caldeira (IPLANRIO)
Hudson Mesquita (MP)
Janaina Breda Leite (SERPRO)
José Luiz Moreira (INPE)
marcus vinicius costa (SERPRO)
Michel Antunes (DATAPREV)
Paulo Gimenez (IBGE)
Rômulo Santos (ETICE)
Regina Silva (MPE-RJ)
Renato Cardoso (MP-BA)
Thiago Soares (PRODEPA)
Victor Torres (STN)
Vinicius Natividade Campos (SERPRO)

Subgrupo: Padrão XBRL – eXtensible Business Reporting Language

Fabiano Castro Pereira (SERPRO) – Coordenador
Amanda Nascimento (SERPRO) – Coordenadora Suplente
Adriano Taves Sobreiro (SERPRO)
Ana Maria Mallmann (SERPRO)
Augusto Ewerton Dias Ferreira (MF)
Carla Marques (SERPRO)
Carlos Bon (RFB)
Divino Lisboa (SERPRO)
Everson Lopes de Aguiar (MP)
Fernando Almeida Barbalho (MF)
Gustavo Assis Chaves (SERPRO)
Marcello Alexandre Kill (SERPRO)
Marcus Vinicius Costa (SERPRO)
Roberto Kodama (CGU)
Thais Crhistine Oliveira Machado Arraes (SERPRO)
Vinicius Silva (MP)