Governo Brasileiro

Comitê Executivo de Governo Eletrônico


# e-PING
# Padrões de Interoperabilidade de Governo Eletrônico

**Documento de Referência**

**Versão 3.0**

14 de dezembro de 2007

## 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 responsabilidades, critérios de verificação de conformidade, 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 infra-estrutura 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, reúso 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 reúso 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;
- Outros níveis 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.

A figura a seguir representa esse relacionamento.

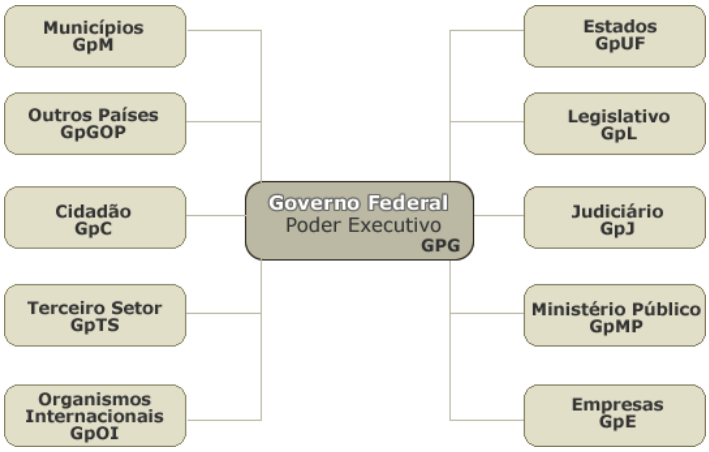


**Figura 1 – Relacionamentos do governo federal.**

### 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

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, de acordo com plano de implementação, que considerará a situação de cada uma dessas instituições em relação à possibilidade de se adequar às especificações e recomendações da e-PING.

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 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.

# 3. Políticas Gerais

Cada um dos segmentos da e-PING contém um conjunto de políticas técnicas que norteia o estabelecimento das especificações dos seus componentes. Esses conjuntos específicos de cada segmento estão fundamentados nas seguintes políticas gerais:

**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*.

**Adoção do XML** como padrão primário de intercâmbio de dados para todos os sistemas do setor público.

**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.

**Adoção de metadados** para os recursos de informação do governo.

**Desenvolvimento e adoção de um Padrão de Metadados do Governo Eletrônico – e-PMG**, baseado em padrões internacionalmente aceitos (http://www.eping.e.gov.br).

**Desenvolvimento e manutenção da Lista de Assuntos do Governo:** Taxonomia de Navegação (LAG), que contemple, numa estrutura de diretório, os assuntos relacionados com a atuação de governo (http://www.eping.e.gov.br).

**Suporte de mercado:** todas as especificações contidas na e-PING contemplam soluções amplamente apoiadas 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.

**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.

**Transparência:** os documentos da e-PING estarão à disposição da sociedade, via Internet, sendo previstos mecanismos de divulgação, recebimento e avaliação de sugestões. Nesse sentido, serão definidos – e divulgados para amplo conhecimento – prazos e compromissos para implantação e gestão de sítio dedicado na Internet (http://www.eping.e.gov.br).

**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. Quando disponíveis, soluções em Software Livre são consideradas preferenciais, conforme política definida pelo Comitê Executivo de Governo Eletrônico (CEGE).

A e-PING mantém total compatibilidade com as iniciativas de governo na área de TIC. Um exemplo a ser mencionado é o Guia de Migração de Software Livre do Governo Brasileiro (http://www.governoeletronico.gov.br).

**Garantia à privacidade de informação:** todos os órgãos responsáveis pelo oferecimento de serviços de e-gov 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 são relacionados os componentes que constituem cada um dos cinco segmentos.

### 4.1. Interconexão

O segmento "Interconexão" estabelece as condições para que os órgãos de governo se interconectem, além de fixar as condições de interoperação entre o governo e a sociedade.

Neste segmento, são estabelecidas as especificações para:

- Protocolo de Transferência de Hipertexto;
- Transporte de Mensagem Eletrônica;
- Segurança de Conteúdo de Mensagem Eletrônica;
- Acesso à Caixa Postal;
- Acesso Seguro à Caixa Postal;
- Diretório;
- Serviços de Nomeação de Domínio;
- Endereços de Caixa Postal Eletrônica;
- Protocolo de Transferência de Arquivos;
- Intercomunicação LAN / WAN;
- Transporte;
- *Web Services*: SOAP, UDDI e WSDL.

### 4.2. Segurança

Este segmento trata dos aspectos de segurança de TIC que o governo federal deve considerar. São tratados os padrões para:

- Segurança de IP;
- Segurança de Correio Eletrônico;
- Criptografia;
- Desenvolvimento de Sistemas;
- Serviços de Rede;
- Coleta e arquivamento de evidências.

### 4.3. Meios de Acesso

No segmento "Meios de Acesso", são explicitadas as questões relativas aos padrões dos dispositivos de acesso aos serviços de governo eletrônico. Nesta versão são abordadas, apenas, as políticas e as especificações para estações de trabalho, cartões inteligentes (*smart cards*), *tokens* e outros cartões. Em versões futuras, serão tratados outros dispositivos, tais como telefone celular, *hand-helds* e televisão digital. É formado por dois subgrupos, com os seguintes componentes:

Padrões para acesso via estações de trabalho:

- Navegadores (*browsers*);
- Conjunto de Caracteres e Alfabetos;
- Formato de Intercâmbio de Hipertexto;
- Arquivos do Tipo Documento;

- Arquivos do Tipo Planilha;
- Arquivos do Tipo Apresentação;
- Arquivos do Tipo Banco de Dados para Estações de Trabalho;
- Especificação de Intercâmbio de Informações Gráficas e Imagens Estáticas;
- Gráficos Vetoriais;
- Especificação de Padrões de Animação;
- Arquivos do Tipo Áudio e do Tipo Vídeo;
- Compactação de Arquivos de Uso Geral;
- Arquivos para georreferenciamento.

Cartões Inteligentes / *Tokens* / Outros:

- Definição de Dados;
- Aplicações (inclusive multi-aplicações);
- Componentes Elétricos;
- Protocolos de Comunicação;
- Padrões de Interface Físico;
- Segurança;
- Infra-estrutura do Terminal.

### 4.4. Organização e Intercâmbio de informações

Aborda os aspectos relativos ao tratamento e à transferência de informações nos serviços de governo eletrônico. Inclui padrão de estrutura de assuntos de governo e de metadados, compreendendo os seguintes componentes:

- Linguagem para intercâmbio de dados;
- Linguagem para transformação de dados;
- Definição dos dados para intercâmbio;
- Catálogo de Padrões de Dados (CPD);
- Lista de Assuntos do Governo: Taxonomia para Navegação (LAG);
- Padrão de Metadados do Governo (e-PMG).

### 4.5. Áreas de Integração para Governo Eletrônico

As metas de análise e proposição deste segmento são:

- XML *Schemas* referentes a aplicações voltadas a Áreas de Atuação de Governo, que serão organizados na forma de Catálogo, disponível no sítio da e-PING, e apresentado com os conteúdos atuais em tópico a seguir;
- Componentes relacionados a temas transversais a Áreas de Atuação de Governo, cuja padronização seja relevante para a interoperabilidade de serviços de Governo Eletrônico, tais como Processos e Informações Geográficas.

# 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 interoperação 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. 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.

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 se passou a denominar Coordenação da e-PING. Além dos três organizadores, participam desse grupo os seguintes órgãos: Presidência da República, Ministério das Relações Exteriores, , Ministério da Saúde, Banco do Brasil, Caixa Econômica Federal, DATAPREV e ABEP - Associação Brasileira de Empresas Estaduais de Processamento de Dados.

O Comitê estabeleceu o seguinte programa de trabalho:

- Definição da forma inicial de elaboração e gestão da arquitetura e-PING;
- Definição da segmentação dos assuntos a serem cobertos pela e-PING;
- Criação de cinco grupos de trabalho responsáveis pelas definições iniciais de políticas e especificações técnicas para cada um dos segmentos;
- Estabelecimento de um cronograma de trabalho com o objetivo de construção e divulgação da versão inicial da arquitetura, denominada versão 0;
- Realização de consulta pública e audiências públicas em RS, SP, DF, RJ, MG e PE, de modo a colher contribuições, da sociedade em geral, sobre o conteúdo proposto na versão 0;
- Publicação da versão 1, juntamente com a resolução de institucionalização da e-PING no âmbito da APF – Poder Executivo;
- Publicação da versão 1.5, contendo as atualizações e revisão das especificações técnicas e da visão geral da e-PING. As versões 1.1 até 1.4 ficaram em discussão interna aos grupos de trabalho e à coordenação da e-PING;
- Realização de consulta pública e audiências públicas de modo a colher contribuições, da sociedade em geral, a cada nova versão do documento de referência;
- Publicação de versão anual, contendo as atualizações e revisões das especificações técnicas e da visão geral da e-PING.

Experiências semelhantes desenvolvidas por governos de outros países são constantemente pesquisadas. A e-GIF – *Government Interoperability Framework* – do governo britânico foi adotada como base para construção da arquitetura de interoperabilidade do governo brasileiro. A gestão da e-PING está apoiada na forma implementada pelo governo do Reino Unido, em operação desde o ano 2000, e, atualmente, situada num grau de maturidade internacionalmente reconhecido como referência.

## 5.2. Estratégia de Implantação

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 versão 2.9.

### 5.3. Modelo de Gestão

Neste item são especificadas as formas de gestão da arquitetura e-PING, sendo relacionadas as principais atribuições e a forma de implementação dessas atividades na organização estrutural do governo.

#### 5.3.1. Atribuições

A Gestão da e-PING compreende o desempenho de atribuições de ordem administrativa e de ordem técnica.

Dentre as **atribuições de caráter administrativo**, destacam-se:

- Definir os objetivos estratégicos e de gestão de governo para o estabelecimento dos padrões;
- Administrar a arquitetura de interoperabilidade do governo brasileiro, provendo a infra-estrutura 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;
- Atuar como centro de coordenação da arquitetura e-PING, buscando alinhamento dos esforços de interoperabilidade, assegurando a coerência das iniciativas empreendidas pelos órgãos de governo;
- Especificamente para os segmentos de Interoperabilidade, administrar o relacionamento do governo federal – Poder Executivo – com as demais instâncias definidas no item 2 - Escopo;
- Gerenciar e operacionalizar a divulgação dos padrões da e-PING, considerando:
  - Criação e administração de um sítio na Internet para a e-PING (http://www.eping.e.gov.br);
  - Coordenação do processo de consultas públicas;
  - Coordenação do processo de recebimento e avaliação de proposições de alteração e complementação;
  - Coordenação do processo de solicitação de sugestões para a e-PING;
  - Publicação das versões atualizadas da e-PING e das atualizações intermediárias;
- Gerenciar a interação com iniciativas de mesmo propósito, conduzidas por outros governos, no país e no exterior;
- Incentivar a capacitação das equipes do governo federal, atuando em conjunto com os órgãos, tanto na consideração da e-PING nos planos específicos de treinamento de cada um deles como na realização de eventos corporativos direcionados para disseminação dos padrões e-PING;
- Estabelecer, implantar e divulgar indicadores de acompanhamento dos resultados obtidos com a implantação da e-PING;
- 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 infra-estrutura da e-PING e promover a pesquisa e desenvolvimento;
- Viabilizar a implantação e gerenciar o processo de homologação dos padrões a serem estabelecidos para o governo;
- Viabilizar a implantação e 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.

Dentre as **atribuições de caráter técnico**, destacam-se:

- Estabelecer as formas de elaboração e de manutenção das políticas e especificações técnicas que compõem a e-PING, considerando:
  - Identificação, criação e gestão de grupos de trabalho específicos;
  - Estabelecimento de convênios e definição de instituições de governo como responsáveis pelas políticas e especificações técnicas de componentes específicos dos segmentos de interoperabilidade;
  - Identificação e implementação de formas alternativas de gerenciamento técnico dos assuntos contemplados na abrangência de atuação da e-PING;

- Coordenar o desenvolvimento e manutenção, no âmbito do governo federal – Poder Executivo, de:
  - Padrão de Metadados de Governo (e-PMG);
  - Lista de Assuntos do Governo: Taxonomia para Navegação (LAG);
  - Catálogo de Padrões de Dados (CPD);
  - Catálogo de Referência dos XML *Schemas*;
  - Demais padrões de Organização e Intercâmbio de Informações;
  - Padrões de Interconexão;
  - Padrões de Segurança;
  - Padrões de Meios de Acesso a serviços eletrônicos de governo;
  - Padrões de uso de Cartões Inteligentes, *Tokens* e outros tipos de cartão;
- Garantir a unicidade de concepção, conceitos, definições e estabelecimento de padrões por parte dos responsáveis pelos segmentos técnicos definidos para a e-PING.

### 5.3.2. Responsabilidades

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

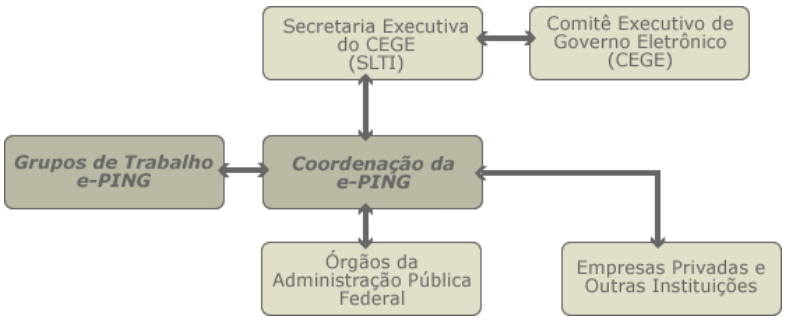


**Figura 2 – Administração da e-PING.**

A Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, através do instrumento do Sistema de Administração dos Recursos de Informação e Informática (SISP), instituído pelo Decreto 1.048, de 21 de janeiro de 1994, é a responsável pela institucionalização e pela definição do formato jurídico da Coordenação da e-PING.

A atuação da Coordenação da e-PING será pautada pelos seguintes pontos:

- Implantação 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;
- Criação de um selo e-PING e administração de processo que certifique a aderência de

determinado serviço ou produto à e-PING;
- Fornecimento de critérios e subsídios para a elaboração da Lei Orçamentária Anual do Governo Federal;
- Gestão dos processos de contratação dos serviços e de estabelecimento de convênios para realização das atribuições necessárias para consolidação dos padrões, como, por exemplo, avaliação de propostas de projetos de e-gov voltados para a Administração Pública Federal, homologação de padrões e verificação de conformidade;
- Estabelecimento dos pontos de contato com os diversos órgãos da Administração Pública Federal;
- Administração dos Grupos de Trabalho – GT, 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.

Os Grupos de Trabalho da e-PING, constituídos por representantes indicados pelos vários órgãos da APF e por representantes de instituições de outras esferas de governos, são responsáveis por:
- Tratar os assuntos que compõem os segmentos da e-PING;
- Monitorar sistematicamente o mercado, especificamente para os segmentos sob sua responsabilidade, com o objetivo de detectar as necessidades de atualização tecnológica das políticas e especificações técnicas;
- Subsidiar a atuação da Coordenação da e-PING, no desempenho de suas atribuições administrativas e técnicas.

Os coordenadores dos Grupos de Trabalho terão assento na Coordenação da e-PING.

### 5.4. Atividades adicionais

Além das atribuições de caráter administrativo e técnico para implantação e manutenção evolutiva da arquitetura e-PING, outras atividades estarão sob responsabilidade da Coordenação da e-PING.

#### 5.4.1. Seleção e Homologação de Padrões Tecnológicos

As políticas técnicas contidas neste documento fundamentam os padrões da e-PING, prestando-se como referência na seleção dos componentes para os quais são estabelecidas as especificações técnicas.

A e-PING prevê um processo de análise dos 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;
- **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;
- **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 será 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.

O processo de seleção dos componentes adotados pela e-PING e sua conseqüente classificação nas situações acima indicadas, é de responsabilidade dos Grupos de Trabalho compostos por profissionais especialistas com atuação no governo e em instituições com as quais seja estabelecido algum tipo de convênio ou contrato especificamente para essa finalidade.

A seleção é feita a partir de sugestões formalizadas, demandas internas dos órgãos do governo federal, Poder Executivo, e pesquisas realizadas pelos Grupos de Trabalho.

Já a homologação deverá ser objeto de estudo mais aprofundado por parte dos gestores da e-PING. Em virtude da grande variedade de componentes tratados pela arquitetura, haverá necessidade de elaboração de uma sistemática de homologação que contemple desde processos em que será necessária a avaliação de características físicas de determinados componentes (Cartões Inteligentes, por exemplo) até outros em que haja necessidade de estudo de aspectos que envolvam o uso do componente no desenvolvimento e construção de serviços (organização e intercâmbio de informações e segurança, por exemplo).

Nesse caso, o governo deverá 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.

A definição completa do processo de seleção e homologação, levando em consideração as especificidades dos segmentos, ficará a cargo da Coordenação da e-PING.

### 5.4.2. 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.

### 5.4.3. Criação e Manutenção do Sítio

Todo o processo de troca de informações sobre a e-PING com usuários, colaboradores e interessados é realizado, preferencialmente, pela Internet, no endereço http://www.eping.e.gov.br Em seu estágio mais avançado de funcionamento, o sítio da e-PING terá, como principais funcionalidades:

- Divulgação completa da documentação relativa à arquitetura: versões oficiais e respectivas atualizações da arquitetura, 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;
- Disponibilidade de meio eletrônico para recebimento de sugestões;
- Disponibilidade de links para documentos, padrões, normas ou qualquer outro tipo de referência constante na e-PING.

### 5.4.4. 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.

Adicionalmente, essa Assessoria terá ainda a responsabilidade de preparar toda a parte institucional necessária para garantir que as adequações e recomendações da e-PING venham a compor o conjunto de instrumentos legais de TIC 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.

### 5.4.5. Divulgação

Será dada total publicidade a todo o conteúdo da e-PING. As principais formas de divulgação previstas, além do sítio na Internet, são:

- 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;
- Publicação de todas as versões da e-PING e das atualizações intermediárias;
- Intercâmbio com outras esferas e outros Poderes de governo, com instituições públicas, privadas e do terceiro setor e com governos de outros países.

### 5.4.6. Capacitação

Farão parte da agenda de implantação e gestão da e-PING eventos direcionados para capacitação. Também é previsto o uso intensivo de Ensino a Distância (EAD).

A Coordenação da e-PING irá elaborar e publicar uma grade mínima de treinamento, de modo que cada órgão da APF tenha subsídios para planejar e estimar investimentos necessários para capacitação dos profissionais envolvidos no processo de adequação às recomendações da e-PING.

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.

## 5.5. 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.

### 5.5.1. 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 infra-estrutura 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.

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

Em sua fase inicial, a e-PING se direciona, basicamente, para o governo federal, Poder Executivo. Outros Poderes (Judiciário, Legislativo e Ministério Público Federal) e outras esferas de governo (estadual e municipal) serão considerados como entidades externas.

Neste caso, vale a orientação de que o governo federal – Poder Executivo não determina a forma como as demais entidades da sociedade devem atuar. Apenas especifica a forma preferencial como pretende interoperar com essas entidades.

A adesão de outras instâncias de governo é incentivada e reconhecida como uma boa estratégia para aprimorar o estabelecimento de padrões e consolidar a e-PING como uma arquitetura de padrões de interoperabilidade do governo brasileiro.

No plano de gestão da e-PING os demais Poderes federais e os governo estaduais e municipais são considerados prioritários. É meta a ser atingida, tão logo sejam estabelecidos e firmados os padrões no âmbito do Poder Executivo Federal, a extensão das discussões aos órgãos e instituições que compõem essas áreas de governo.

### 5.5.3. 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 eqüidade de oportunidades.

### 5.5.4. 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 prevêem a participação ativa do cidadão e da sociedade em geral, no processo de construção e gestão da arquitetura.

# 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.** Os órgãos da APF deverão se interconectar utilizando IPv4 e planejar sua futura migração para IPv6. Novas contratações e atualizações de redes devem prever suporte à coexistência dos protocolos IPv4 e IPv6 e a produtos que suportem ambos os protocolos.

**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 quando necessário os aspectos de segurança.

**6.1.3.** Os órgãos da APF devem usar esquema de Diretório compatível com o do Serviço de Diretório do governo federal, disponível no endereço eletrônico http://www.e.gov.br/correios/dir_redegoverno.htm.

6.1.4. Os órgãos da APF devem obedecer à política de nomeação de domínios do governo federal, estabelecida na Resolução n.º 7, que pode ser visualizada no endereço eletrônico

https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm.

**6.1.5.** 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.

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

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

**6.1.8.** A tecnologia de *Web Services* é recomendada como padrão de interoperabilidade da e-PING.

**6.1.9.** Os *Web Services* deverão ser registrados e estar localizados em estruturas de diretório compatíveis com o padrão UDDI. O protocolo de acesso a essa estrutura deverá ser o HTTP.

**6.1.10.** O protocolo SOAP é recomendado para comunicação entre os clientes e os *Web Services* e a especificação do serviço deverá utilizar a linguagem WSDL. Veja nota sobre *Web Services*, item 6.3.

[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.

### 6.2. Interconexão: Especificações Técnicas

**Tabela 1 – Especificações para Interconectividade[2]**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Protocolo de transferência de hipertexto | Utilizar HTTP/1.1 (RFC 2616) e/ou HTTPS (RFC 2660). | **A** | |
| Transporte de mensagem eletrônica | Utilizar produtos de mensageria eletrônica que suportam interfaces em conformidade com SMTP/MIME para transferência de mensagens. RFCs correlacionadas: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 2646; RFC 2047; RFC 2231; RFC 2183; RFC 2048; RFC 3023 e RFC 2049. | **R** | |
| Segurança de conteúdo de mensagem eletrônica | O S/MIME v3.1 deverá ser utilizado quando for apropriado para segurança de conteúdo de mensagens gerais do governo, a menos que os requisitos de segurança determinem outra forma. RFCs correlacionadas: RFC 3852; RFC 2631; RFC 3850 e RFC 3851. | **R** | |
| Acesso à caixa postal | A menos que as exigências de segurança determinem de outra forma, programas de correio que fornecem facilidades de acesso à correspondência deverão, no mínimo, estar de acordo com POP3 para acesso remoto a caixa postal. RFCs correlacionadas: RFC 1939; RFC 1957 e RFC 2449.<br>Onde facilidades adicionais forem necessárias, a menos que requisitos de segurança estabeleçam de forma contrária, os programas de correio que fornecem facilidades avançadas de acesso à correspondência, deverão estar de acordo com IMAP para acesso remoto à caixa postal. RFCs correlacionadas: RFC 3501; RFC 2342; RFC 2971; RFC 3502; RFC 3503; RFC 3510 e RFC 2910. | **R** | |
| Acesso seguro à caixa postal | O acesso à caixa postal, através de redes não seguras, deverá usar HTTPS, de acordo com os padrões de segurança no transporte. Quando for necessário usar IMAP ou POP, usá-lo através de TLS, conforme RFC 2595. | **R** | |
| Diretório | Usar o esquema do diretório central, conforme definido no endereço eletrônico http://www.e.gov.br/correios/dir_redegoverno.htm<br>LDAP v3 deverá ser utilizado para acesso geral ao diretório. | **R** | |
| Serviços de Nomeação de Domínio | O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035.<br>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 | **A** | |

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

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm<br>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 compete gerenciar os domínios .GOV.BR.<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 | | |
| 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.e.gov.br/correios/cp_individ.htm | **A** | |
| Protocolos de transferência de arquivos | FTP (RFC 959 e RFC 2228) (com re-inicialização e recuperação) e HTTP (RFC 2616) para transferência de arquivos. | **R** | |
| Protocolos de sinalização | Uso do Protocolo de Inicialização de Sessão (SIP), definido pela RFC 3261, como protocolo de controle na camada de aplicação (sinalização) para criar, modificar e terminar sessões com um ou mais participantes. | **R** | |
| 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 3920 e RFC 3921. | **R** | |
| Serviço de Mensagens Curtas | O Serviço de Mensagens Curtas (SMS) deverá utilizar o protocolo SMPP, como definido pelo SMS *Forum* http://www.smsforum.net | **R** | |
| Intercomunicação LAN/WAN | IPv4 (RFC 791) | **A** | |
| | IPv6 (RFC 2460) | **E** | |
| Transporte | TCP (RFC 793)<br>UDP (RFC 768) quando necessário, sujeito às limitações de segurança. | **R** | |
| Tráfego avançado | Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço. | **R** | |
| Rede local sem fio | IEEE 802.11 b/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). | **R** | |
| Rede metropolitana sem fio | IEEE 802.16, em conformidade com as determinações do *WiMax Forum* (http://www.wimaxforum.org) e com as normas da Anatel (http://www.anatel.gov.br). | **E** | |

### 6.3. *Web Services*

Pode-se definir o termo *Web Services*[3] como um serviço disponível na rede (Internet ou Intranet) que utilize um sistema padrão – XML – para troca de mensagens, independente de sistema operacional ou linguagem de programação, com duas propriedades básicas:

(a) possibilitar sua descoberta: ao criar um *Web Service*, deve-se publicá-lo, registrando-o em um catálogo de serviços para que potenciais usuários possam achá-lo. O catálogo pode usar UDDI. Outras formas de repositórios podem ser usadas, entre elas a ebXML – atualmente encontra-se em estudo pela e-PING;

(b) auto-descrição: os *Web Services* fornecem uma descrição completa dos seus serviços e de como os usuários (desenvolvedores) poderão criar aplicações para interagir com eles. Essa descrição é feita através de WSDL.

A Figura 1 apresenta os passos genéricos para se prover e consumir um serviço através de *Web Services*:

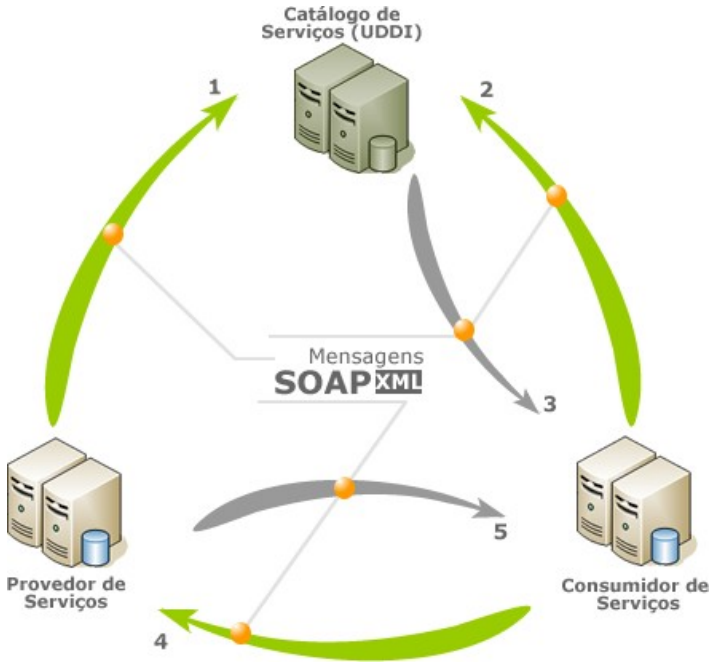


**Figura 3 – Visão geral do funcionamento de *Web Services*[4].**

(1) faz-se o registro do serviço, onde um provedor de serviço descreve seu serviço usando WSDL. Publica-se essa definição em um catálogo de serviços;

(2) o consumidor de serviço faz uma ou mais consultas ao diretório de serviços para localizar um serviço e verificar qual a forma de comunicação com esse serviço;

(3) informações sobre o(s) serviço(s) localizado(s) são enviadas ao consumidor de serviço. Essas informações são parte do WSDL provido pelo provedor de serviços, como, por exemplo, o endereço onde está localizado o serviço solicitado;

(4) e (5) referem-se ao consumo do serviço propriamente dito. Provedor e consumidor trocam mensagens (XML) entre si. Ao receber uma mensagem, o *Web Service* valida-a de acordo com as informações contidas no WSDL. A partir desse momento, o *Web Service* sabe como tratar a mensagem, como processá-la (talvez a enviando para outro programa) e sabe como montar a resposta ao consumidor do serviço.

[3] A definição de Web Services foi adaptada do livro de Ethan Cerami - *Web Services Essentials - Distributed Applications with XML-RPC, SOAP, UDDI & WSDL, 2002. O' Reilly & Associates Inc., Sebastol, CA.*
[4] A figura 1 é uma adaptação da figura disponibilizada pelo W3C Woking Group – http://www.w3.org/TR/ws-arch/#whatis.

A necessidade de integração entre os diversos sistemas de informação de governo, implementados em diferentes tecnologias implica na adoção de um padrão de interoperabilidade que garanta escalabilidade, facilidade de uso, além de possibilitar atualização de forma simultânea e em tempo real.

Diante desse contexto, entende-se que o uso de *Web Services* é adequado a essas necessidades. *Web Services* oferecem uma abordagem dinâmica para integração, na qual os serviços são localizados, determinados e usados automaticamente. A tecnologia de *Web Services* provê uma forma padrão de interoperação entre diferentes aplicações de softwares. Além disso, um *Web Service* pode ter diferentes níveis de granularidade. Tanto um formulário pertencente a uma página *web*, quanto um componente de software, que encapsula uma complexa regra de negócio, podem ser transformados em *Web Services*, o que torna seu uso bastante flexível.

O suporte de Web Services para integração direta com outras aplicações de software utiliza mensagens escritas em XML como padrão de interoperabilidade. Essas mensagens são encapsuladas em protocolos de aplicação padrão da Internet – SOAP. É importante ressaltar que as estruturas de documentos XML serão descritas através de XML Schemas, como forma de validação dos tipos de dados pertencentes às linhas de negócio.

**Tabela 2 – Especificações para *Web Services*[5]**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Protocolo de troca de informações | SOAP v1.2, como definido pelo W3C<br>http://www.w3.org/TR/soap12-part1/<br>http://www.w3.org/TR/soap12-part2/<br>Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/ | **R** | |
| Infra-estrutura de registro | Especificação UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida pela OASIS<br>http://uddi.org/pubs/uddi_v3.htm | **R** | |
| | ebXML (*Electronic Business using eXtensible Markup Language*). A especificação pode ser encontrada em<br>http://www.ebxml.org/specs/index.htm | **E** | |
| Linguagem de definição do serviço | WSDL 1.1 (*Web Service Description Language*) como definido pelo W3C.<br><br>A especificação pode ser encontrada em<br>http://www.w3.org/TR/wsdl | **R** | |
| | WSDL 2.0 (*Web Service Description Language*) como definido pelo W3C.<br><br>A especificação pode ser encontrada em<br>http://www.w3.org/TR/wsdl20/ | **E** | |
| Perfil básico de interoperabilidade | *Basic Profile 1.1 Second Edition*, como definido pela WS-I<br>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 |

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

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| *Portlets* remotos | WSRP 1.0 (Web Services for Remote Portlets) como definido pela OASIS http://www.oasis-open.org/committees/wsrp | **E** | |

### 6.4. 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.

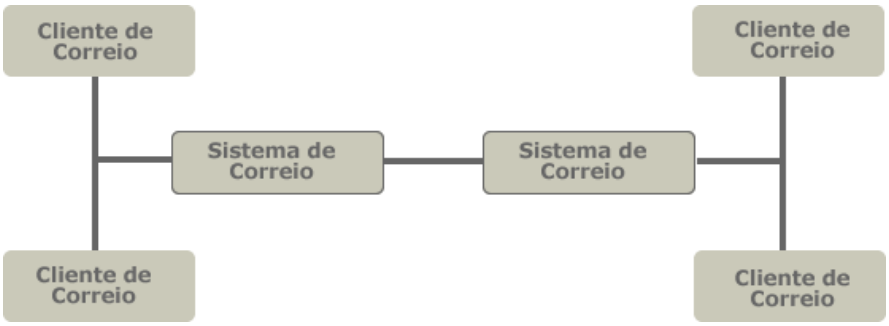


**Figura 4 – Interfaces entre sistemas e clientes de Correio.**

### 6.5. VPN

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

Tal utilização, como infra-estrutura 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 privacidade, integridade e autenticidade dos dados.

As especificações sobre VPN estão apresentadas no segmento de segurança.

### 6.6. 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, impossibilitando o uso sistemático de redes P2P. Este assunto será abordado em momento futuro.

# 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 e disponibilidade.

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

**7.1.3.** As informações que trafegam em redes inseguras, incluindo aquelas sem fio, devem adotar os controles de segurança disponíveis na camada de transporte (IPv4). No caso de LAN sem fio os protocolos de segurança específicos desta tecnologia devem ser usados, quando necessário. Os sistemas de informação do governo devem ser protegidos contra riscos de segurança na conexão com essas redes.

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

**7.1.5.** A segurança deve ser tratada de forma preventiva. Para os sistemas que apóiam processos críticos devem ser elaborados planos de continuidade, nos quais serão tratados os riscos residuais visando atender os 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 forenses, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado, bem como deve-se utilizar mecanismos que garantam a autenticidade dos registros armazenados, se possível com assinatura digital.

**7.1.8.** Os serviços de segurança de XML devem estar em conformidade com as especificações do W3C.

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

**7.1.10.** 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.

**7.1.11.** A documentação dos sistemas, dos controles de segurança e das topologias dos ambientes deve ser mantida atualizada e protegida.

**7.1.12.** 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.

**7.1.13.** Os Órgãos da APF, visando a melhoria da segurança, devem ter como referência a norma NBR ISO/IEC 27002:2005 código de prática para a gestão da segurança da informação e NBR ISO/IEC 27001:2006 sistemas de gestão de segurança da informação, editadas pela ABNT.

### 7.2. Segurança: Especificações Técnicas

**Tabela 3 – Especificações Técnicas para Segurança de IP**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Transferência de dados em redes inseguras pelos protocolos HTTP, LDAP, IMAP, POP3, Telnet sempre que possível. – Segurança de redes IPv4 na camada de transporte | TLS – *Transport Layer Security*, RFC2246 (http://www.ietf.org/rfc/rfc2246.txt). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.<br><br>HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt)<br>Podendo implementar os seguintes algoritmos criptográficos:<br><br>- Algoritmos para troca de chaves de sessão, durante o *handshake*:<br>RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;<br><br>- Algoritmos para definição de chave de cifração:<br>RC4, IDEA, 3DES, AES;<br><br>- Algoritmos que implementam a função de *hash* para definição do MAC:<br>SHA-256 ou SHA-512.<br><br>- Tipo de Certificado Digital - X.509 v3 - ICP-Brasil, http://www.iti.gov.br<br>SASL - *Simple Authentication and Security Layer*, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt). | **R** | |
| Segurança de redes IPv4 | *IPSec Authentication Header* RFC 2402 e RFC 2404 para autenticação de cabeçalho do IP.<br>http://www.ietf.org/rfc/rfc2402.txt<br>http://www.ietf.org/rfc/rfc2404.txt<br><br>IKE – *Internet Key Exchange*, RFC 2409 (http://www.ietf.org/rfc/rfc2409.txt), deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento.<br><br>ESP – *Encapsulating Security Payload,* RFC 2406 (http://www.ietf.org/rfc/rfc2406.txt) Requisito para VPN – Virtual Private Network. | **R** | |
| Segurança de redes IPv4 para protocolos de aplicação | O S/MIME v3 ,RFC2633 (http://www.ietf.org/rfc/rfc2633.txt) deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. | **R** | |

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| Segurança de redes IPv6 na camada de rede | O IPv6 definido na RFC2460 (http://www.ietf.org/rfc/rfc2460.txt) apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*) RFC2402 (http://www.ietf.org/rfc/rfc2402.txt) ou autenticação IP, e a segurança do encapsulamento IP, ESP (*Encrypted Security Payload*) RFC2406 (http://www.ietf.org/rfc/rfc2406.txt). | **R** | |

**Tabela 4 – Especificações Técnicas para Segurança de Correio Eletrônico**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>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 (http://www.ietf.org/rfc/rfc2595.txt), que trata da utilização do TLS com IMAP, POP3 e ACAP. | **R** | |
| Conteúdo de e-mail | O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 3369 (http://www.ietf.org/rfc/rfc3369.txt), RFC 3370 (http://www.ietf.org/rfc/rfc3370.txt), RFC 2631 (http://www.ietf.org/rfc/rfc2631.txt), RFC 3850 (http://www.ietf.org/rfc/rfc3850.txt) e RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt). | **R** | |
| Transporte de e-mail | Verificar se o reverso confere com o nome no HELO, para garantia da origem da mensagem e minimizar SPAM. | **F**[6] | |
| Assinatura | Utilizar padrão ICP-Brasil para a assinatura de e-mail, quando exigido. Em conformidade com o disposto no Decreto 3.996 de 31 de outubro de 2001. | **R** | |

[6] Possível implicação na performance; possível descarte de mensagens válidas; impossibilidade de tratar múltiplos domínios.

**Tabela 5 – Especificações Técnicas para Segurança – Criptografia**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Algoritmo de cifração | 3DES ou AES | **R** | |
| Algoritmo para assinatura/hashing | SHA-256 ou SHA-512 | **R** | Os sistemas devem ter suporte para o algoritmo de *hash* MD5 com RSA, para garantir compatibilidade com implementações anteriores. |
| Algoritmos para assinatura/hashing | SHA-224 ou SHA-238 | **E** | Considerando que foram incluídas no Relatório Final do Grupo de Trabalho de Criptografia I, instituído pelo Gabinete de Segurança Institucional da Presidência da República, porém, ainda não se transformaram em norma na Administração Pública Federal |
| Algoritmo para transporte de chave criptográfica de conteúdo/sessão | RSA | **R** | |
| Algoritmos criptográficos baseados em curvas elípticas | ECMQV e ECDH, ambos para acordo de chaves, ECDSA, para assinaturas digitais, e ECIES para cifração e transporte seguro de chaves criptográficas. O uso destes algoritmos está sujeito a regulamentação e normatização pela ICP-Brasil quanto aos requisitos de segurança. | **E** | |
| Requisitos de segurança para módulos criptográficos | FIPS 140-2 – requisitos mínimos para as soluções de armazenamento de chaves privadas e certificados digitais emitidos no âmbito da ICP – Brasil, que usam dispositivos tanto de *software* como de *hardware* tipo *token* ou *smart card*.<br>Aderência ao padrão:<br>a. Seguir, no mínimo, as regras estabelecidas para o nível 1 ou 2 de segurança do padrão;<br>b. Seguir, no mínimo, as regras estabelecidas para o nível 2 de segurança do padrão FIPS 140-1 ou 2, para verificação de violação no *hardware* (*Tamper Evidence*). | **R** | |

**Tabela 6 – Especificações Técnicas para Segurança – Desenvolvimento de Sistemas**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Assinaturas XML | Sintaxe e Processamento de assinatura XML (XMLsig) conforme definido pelo W3C http://www.w3.org/TR/xmldsig-core/ | **R** | |
| 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://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf).<br>WS-Trust 1.3 - 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/200512). | **E** | O componente anterior (SAML) poderá se juntar a este componente após estudos. |
| Navegadores | Somente utilizar testemunhas de conexão de caráter permanente (*cookies*) com a concordância do usuário. Resolução n. 7 do Comitê Executivo do Governo Eletrônico (Capítulo II, Art.7º). | **A** | |

**Tabela 7 – Especificações Técnicas para Segurança – Serviços de Rede**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Diretório | 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.<br>LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt).<br>LDAP v3 extensão para TLS RFC2830 (http://www.ietf.org/rfc/rfc2830.txt). | **R** | |
| DNS | Resolução no. 7 de 29/07/2002 – Comitê Executivo do Governo Eletrônico<br>Práticas de Segurança para Administradores de Redes Internet<br>NIC BR Security Office<br>http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-chklist.pdf<br>Versão 1.2<br>16 de maio de 2003<br>Securing an internet name server, CERT – ago/2002. | **R** | |
| Transferência de arquivos de forma segura | HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt). | **R** | |
| Transferência de arquivos de forma segura | SSH FTP | **F** | Os documentos ainda estão no formato de rascunhos. |
| Transferência de arquivos de forma segura | Securing FTP with TLS, RFC 4217 http://www.faqs.org/rfcs/rfc4217.html e RFC 2246 http://www.faqs.org/rfcs/rfc2246.html | **E** | |
| Newsgroup | | **F** | |
| Mensagem instantânea | RFC 2778 (http://www.ietf.org/rfc/rfc2778.txt), RFC 3261 (http://www.ietf.org/rfc/rfc3261.txt), RFC 3262 (http://www.ietf.org/rfc/rfc3262.txt), RFC 3263 (http://www.ietf.org/rfc/rfc3263.txt), RFC 3264 (http://www.ietf.org/rfc/rfc3264.txt) e RFC (3265. http://www.ietf.org/rfc/rfc3265.txt). | **E** | |
| Sincronismo de tempo | RFC 1305 IETF-*Network Time Protocol* – NTP *version* 3.0 (http://www.ietf.org/rfc/rfc1305.txt).<br>RFC 2030 IETF- *Simple Network Time Protocol* - SNTP *version* 4.0 (http://www.ietf.org/rfc/rfc2030.txt). | **R** | |

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| Carimbo de tempo | RFC 3628 TSAs - *Policy Requirements for Time-Stamping Authorities* (http://www.ietf.org/rfc/rfc3628.txt), *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (http://www.ietf.org/rfc/rfc3161.txt). | **R** | O serviço de carimbo de tempo deverá estar de acordo com as resoluções e demais normas da ICP-Brasil. |

**Tabela 8 – Especificações Técnicas para Segurança de Redes Sem Fio**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| MAN[7] sem fio 802.16-2004[8] 802.16.2-2004[9] 802.16e[10] e 802.16f[11] | Utilizar PKM-EAP (*Privacy Key Management - Extensible Autentication Protocol*) com:<br>• EAP – TLS ou TTLS;<br>• AES[12] (Advanced Encryption Standard). | **E** | |
| LAN sem fio 802.11 | Utilizar a especificação WPA2 (Wi-Fi *Protect Access*). | **R** | |

**Tabela 9 – Especificações Técnicas para Segurança – Coleta, Tratamento e Arquivamento de Evidências**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Preservação de registros | *Guidelines for Evidence Collection and Archiving*, RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt). | **R** | |
| Resposta a incidentes | *Expectations for Computer Security Incident Response*, RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt). | **R** | |
| Informática Forense | *Guide to Integrating Forensic Techniques into Incident Response* – NIST - *Special Publication* 800-86 (*Draft*) – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf). | **R** | |

[7] O 802.16 é definido pelo IEEE como uma interface tecnológica para redes de acesso sem fio metropolitanas ou WMAN (*Wireless Metropolitan Access Network*).
[8] http://standards.ieee.org/getieee802/download/802.16-2004.pdf.
[9] http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf.
[10] http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.
[11] http://standards.ieee.org/getieee802/download/802.16f-2005.pdf.
[12] http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf.

# 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, televisão digital e cartões inteligentes (*smart cards*), 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;
- devem prever a substituição gradativa da sistemática de "login/senha" por autenticação de usuários com utilização de certificado digital, preferencialmente embarcados em cartões inteligentes ou *tokens*, conforme padrões preconizados pela ICP – Brasil (referência: http://www.icpbrasil.gov.br/);
- novos serviços deverão ser criados já com suporte à autenticação de usuários por meio de certificados digitais ICP-Brasil;
- nesta versão, a e-PING trata dos seguintes meios de acesso:
  - estações de trabalho, considerando acesso aos usuários de forma direta ou indireta, por meio da prestação de serviços via balcão de atendimento;
  - cartões inteligentes, *tokens* e outros cartões;
  - outros meios de acesso, como telefones celulares, *hand-helds* e televisão digital serão objeto de estudo futuro para determinação dos padrões aceitos pelo governo federal.

**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 de Governo Eletrônico (e-MAG)[13].

**8.1.6.** Quando a Internet for usada como meio de comunicação, os sistemas de informação do governo devem ser projetados de maneira que o máximo de informações possa ser trabalhado a partir de navegadores que atendam ao padrão mínimo expresso pelo suporte às especificações técnicas pertinentes previstas na 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

[13] BRASIL. Ministério do Planejamento, Orçamento e Gestão. Recomendações de Acessibilidade para a construção e adaptação de conteúdos do Governo Brasileiro na Internet: modelo de acessibilidade. Versão 2.0. Brasília, 2005. Disponível em: (http://www.governoeletronico.gov.br/emag/). Acessado em: 13/07/2006.

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.

**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. Referência: http://www.icpbrasil.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 de 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. Referência:

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 empacotamento o "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 9.

Já para a elaboração da versão final de documentos, a qual 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 9 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 10 – Especificações Técnicas – Estações de Trabalho**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Navegadores (*browsers*) | Ver item 3. Políticas Gerais. | **E** | |
| 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[14]. | **A** | |
| | XHTML versões 1.0 ou 1.1 (.xhtml), gerado conforme especificações do W3C[15]. | **A** | |
| | XML versões 1.0 ou 1.1 (.xml), gerado conforme especificações do W3C[16]. | **A** | |
| | SHTML (.shtml). | **R** | |
| | MHTML (.mhtl ou .mht)[17]. | **T** | |
| Arquivos do tipo documento | XML versões 1.0 ou 1.1 (.xml), ou com formatação (opcional) XSL (.xsl), gerado conforme especificações do W3C[18]. | **R** | |
| | Open Document (.odt), gerado conforme especificações do padrão ISO/IEC 26300[19]. | **R** | |
| | OpenOffice.org XML (.sxw), gerado no formato do OpenOffice versão 1.0. | **T** | |
| | Rich Text Format (.rtf). | **T** | |
| | PDF (.pdf) gerado em formato até versão 1.3. | **T** | |
| | PDF versão aberta PDF/A[20]. | **R** | |

[14] *HTML 4.01 Specification - W3C Recommendation 24 December 1999*. Disponível em: http://www.w3.org/TR/html4/.
[15] *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/.
[16] *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/.
[17] Formato de empacotamento de arquivos *web* da Microsoft (*Mime Enscapsulation of Aggregate HTML Documents*).
[18] *Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001*. Disponível em: http://www.w3.org/TR/xsl/.
[19] *Open Document Format for Office Applications (OpenDocument)* v1.0 – padrão ISO/IEC 26300. Disponível em: http://www.iso.org/.

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | Texto puro (.txt). | **A** | |
| | HTML versão 4.01 (.html ou .htm), gerado conforme especificações do W3C. | **R** | |
| | Microsoft Word document (.doc), gerado no formato do MS Office até versão 2000. | **T** | |
| Arquivos do tipo planilha | Open Document (.ods), gerado conforme especificações do padrão ISO/IEC 26300. | **R** | |
| | OpenOffice.org XML (.sxc). gerado no formato do Open Office versão 1.0. | **T** | |
| | Planilha MS Excel (.xls), gerado no formato do MS Office até versão 2000. | **T** | |
| Arquivos do tipo apresentação | Open Document (.odp), gerado conforme especificações do padrão ISO/IEC 26300. | **R** | |
| | OpenOffice.org XML (.sxi), gerado no formato do Open Office versão 1.0. | **T** | |
| | HTML (.html ou .htm), gerado conforme especificações do W3C. | **R** | |
| | Apresentação MS Power Point (.ppt), gerado no formato do MS Office até versão 2000. | **T** | |
| 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 no formato do BrOffice.org (ou OpenOffice.org) versão 2.0 ou posterior. | **R** | |
| | Arquivo MS Access (.mdb), gerado no formato do MS Office, até versão 2000. | **T** | |
| 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** | |
| | Open Document (.odg), gerado conforme especificações do padrão ISO/IEC 26300. | **R** | |

[20] *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/.

[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.

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | OpenOffice.org XML (.sxd), gerado no formato do Open Office versão 1.0. | **T** | |
| | XCF (.xcf), gerado no formato do GIMP versão 1.0 ou superior. | **R** | |
| | BMP (.bmp). | **T** | |
| | GIF (.gif), gerado conforme as especificações GIF87a e GIF89a[25]. | **T** | |
| | Imagem Corel Photo-Paint (.cpt), gerado no formato da suíte Corel Draw até versão 7. | **T** | |
| | Imagem Photoshop (.psd), gerado no formato do Adobe Photoshop até versão 4. | **T** | |
| Gráficos vetoriais | SVG (.svg), gerado conforme especificações do W3C. | **R** | |
| | Open Document (.odg), gerado conforme especificações do padrão ISO/IEC 26300. | **R** | |
| | OpenOffice.org XML (.sxd), gerado no formato do Open Office versão 1.0. | **T** | |
| | Gráfico Corel Draw (.cdr), gerado no formato até versão 7. | **T** | |
| | MSX (.msx), gerado no formato da suíte Corel Draw até versão 7. | **T** | |
| | Gráfico MS Visio (.vss ou .vsd), gerados no formato até versão 2000. | **T** | |
| | Windows Metafile (.wmf). | **T** | |
| Especificação de padrões de animação | SVG (.svg), gerado conforme especificações do W3C. | **R** | |
| | GIF (.gif), gerado conforme a especificação GIF89a. | **T** | |
| | Shockwave Flash (.swf), gerado no formato do Macromedia Flash até versão 4, do Macromedia Shockwave versão 1. | **T** | |
| Arquivos do tipo áudio e do tipo vídeo | .mpg | **R** | |
| | Áudio e vídeo MPEG-4, Part 14 (.mp4)[26] | **R** | |
| | MIDI (.mid)[27] | **R** | |
| | Áudio Ogg Vorbis I (.ogg)[28] | **R** | |
| | *Audio-Video Interleaved* (.avi), com codificação Xvid. | **R** | |
| | *Audio-Video Interleaved* (.avi), com codificação divX. | **T** | |
| | Áudio MPEG-1, Audio Layer 3 (.mp3)[29] | **T** | |

[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.

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | *Real Media* (.rm ou .rmm), gerado no formato dos aplicativos Real Audio Media Player, até versão 8. | **T** | |
| | *Real Audio* (.ra ou .ram), gerado no formato dos aplicativos Real Audio Media Player, até versão 8. | **T** | |
| | WAVE (.wav) | **T** | |
| | *Shockwave Flash* (.swf), gerado no formato do Macromedia Flash, até versão 4 ou pelo Macromedia Shockwave, versão 1. | **T** | |
| | *Windows Media Video* (.wmv), gerado no formato do Windows Media Player, até versão 6.4. | **T** | |
| | *Windows Media Audio* (.wma), gerado no formato do Windows Media Player, até versão 6.4. | **T** | |
| | *QuickTime* (.mov), gerado no formato do Apple Quicktime, até versão 6. | **T** | |
| | *QuickTime* (.qt), gerado no formato do Apple Quicktime, até versão 6. | **T** | |
| Compactação de arquivos de uso geral | ZIP (.zip). | **R** | |
| | GNU ZIP (.gz). | **R** | |
| | 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 1.0 ou superior[30]. | **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[31]. | **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. |

[29] *ISO/IEC 11172-3:1993 - Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5Mbit/s - Part 3: Audio.*
*ISO/IEC 11172-3:1993/Cor 1:1996.*
[30] *Geography Markup Language*. Especificações disponíveis em:
http://www.opengeospatial.org/standards.
[31] *ESRI Shapefile Technical Description*. Disponível em:
http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | GeoTIFF[32]. | **A** | Indicado para estruturas matriciais limitadas a matrizes de pixel. |
| | SFS. | **E** | |
| Programação Estendida (Plug-ins) | Assunto para consideração futura. | **F** | |

### 8.3. Meios de Acesso: Especificações Técnicas para *tokens,* Cartões Inteligentes e Cartões em Geral

As especificações iniciais sobre cartões inteligentes e *tokens* receberam como acréscimo as conclusões do Grupo de Trabalho da ICP-Brasil (Portaria nº 33, de 08 de abril de 2003) que usou como linhas básicas a família ISO/IEC (7816 partes 1 a 6).

As conclusões daquele grupo também foram utilizadas para a elaboração dos Manuais de Condutas Técnicas do ITI, documentos que estabelecem os requisitos técnicos a serem observados nos processos de homologação de cartões inteligentes e *tokens* criptográficos no âmbito da ICP-Brasil. As especificações constantes nesses manuais também foram utilizadas para a elaboração deste documento de referência, especificamente para dispositivos criptográficos.

A homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil foi instituída pela Resolução 36 do Comitê Gestor da ICP-Brasil, de 21/10/2004, ficando o Instituto Nacional de Tecnologia da Informação (ITI), como responsável pela condução do processo, enquanto os Laboratórios de Estudos e Auditoria (LEA), criados pela Resolução 36, ficaram responsáveis pelos ensaios de conformidade.

Segundo aquela Resolução, as mídias que armazenam os certificados digitais e respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, deverão obedecer a padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados.

Pelo regulamento são passíveis de homologação mídias como *tokens* criptográficos e *smart cards*, sistemas como de assinatura eletrônica, de autenticação de assinatura, de autoridades certificadoras e de registro, e equipamentos como os de HSM, sincronismo e carimbo de tempo, entre outros. Os produtos homologados por esse processo terão um laudo de conformidade emitido e utilizarão o selo de homologação e seu correspondente número de identificação.

Importante observar que os dados armazenados num determinado cartão inteligente ou *token* não poderão estar protegidos por qualquer tipo de licenciamento que proíba a sua leitura por qualquer outro software que não o do fornecedor daquele cartão inteligente ou *token*.

A padronização desses dispositivos facilitará a inserção do Brasil em acordos internacionais relativos a certificação digital, além de manter a aderência aos Padrões de Interoperabilidade de Governo Eletrônico – e-PING e ajudar a massificar o uso da certificação, pois entre outros aspectos poderá contribuir para o barateamento dessa solução tecnológica.

No contexto da e-PING, foram considerados, também: a ISO/IEC 7810, que define as propriedades físicas tais como flexibilidade, resistência à temperatura e dimensões para três diferentes tipos de formato de cartão (ID-1, ID-2 e ID-3), o padrão PC/SC *Workgroup* e a padronização para segurança de dispositivos FIPS-140, do *National Institute of Standards and Technology* (http://www.nist.gov). Esses padrões fundamentais foram utilizados no Grupo de Trabalho da ICP-Brasil com o objetivo de obter melhor interoperabilidade no universo de dispositivos de acesso do tipo cartões inteligentes e *tokens*, a saber, dispositivos que manejam certificados digitais. Ainda foram incorporadas as normas ISO para cartões magnéticos e cartões óticos, aqueles tradicionais e de baixo custo, estes mais arrojados e de alto custo.

Para as versões futuras da e-PING, será estabelecida uma agenda mínima que deverá revisar todo o quadro de especificações e mapear, no âmbito do governo federal, as ações e planos de governo que usam algum tipo de cartão inteligente e que, por conseguinte, devem ser contemplados. Deverá ser executada uma pesquisa exaustiva que forneça subsídios para a inclusão ou não, na e-

[32] *GeoTIFF Format Especification*. Disponível em: http://remotesensing.org/geotiff/geotiff.html.

PING, dos padrões de cartões efetivamente usados pelos órgãos de governo. Como exemplo dessa situação, podem ser citados os chamados *embossed smart cards* (ISO/IEC 7811), cartões gravados em relevo, que não são contemplados nesta versão. Caso seja constatada, nessa pesquisa, o uso intensivo desse tipo de dispositivo, será analisada a viabilidade de sua inclusão no conjunto de especificações tratadas pela e-PING.

Ainda para as versões futuras, serão analisados em profundidade os padrões tipicamente voltados para a comunidade européia. É o caso do eEurope, o *Open Smart Card Infrastructure for Europe* – versão 2" que assimila a tecnologia de cartões sem contato, presente na ISO/IEC 14443. O mesmo se aplica ao padrão CALYPSO (*Fourth European Research and Technological Devepment Framework Program*) para sistemas de cartões (ou tíquetes) sem contato, voltados para sistemas de transportes públicos. Dever-se-á avaliar as padronizações, sistemas de patentes e licenciamentos que porventura possam existir.

**Tabela 11 – Especificações para Meios de Acesso – Cartões Inteligentes, *tokens* e Cartões em Geral**

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | | |
| Definição de dados | Manuais de Condutas Técnicas do ITI – Volume 1 (http://www.lea.gov.br/). | **A** | Todos os cartões e *tokens* que manejam certificados digitais. | |
| | Cartões de identificação **ISO/IEC 7816-6** Cartões de Circuito(s) Integrado(s) com contatos<br>Parte 6: Elementos de dados intersetorial. | **A** | Todos. | Conforme escolha do GT da ICP-Brasil. |
| | Cartões de identificação **ISO/IEC 7812-1** Identificação dos emissores<br>Parte 1: Sistema de Numeração. | **R** | Todos. | |
| | Cartões de transações financeiras **ISO 9992-2**. Mensagens entre o cartão de circuito integrado e o dispositivo de aceitação do cartão<br>Parte 2: Funções, mensagens (comandos e respostas), elementos e estruturas de dados. | **F** | Todos. | |
| | Sistemas de cartão de identificação **BS EN 1546-3** – *Inter-sector electronic purse* - Parte 3: Elementos e intercâmbio de dados<br><br>Sistemas de cartão de identificação **BS EN 1546-4** – *Inter-sector electronic purse* - Parte 4: Objetos de dados. | **F** | Todos. | A atual edição foi publicada em julho de 1999.<br><br>A atual edição foi publicada em agosto de 1999. |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| Aplicações incluindo multi-aplicações | Cartões de identificação **ISO/IEC 7816-4** Parte 4: Comandos intersetoriais para intercâmbio. | **A** | Cartões de Circuito(s) Integrado(s) com contatos. | Estabelece as estruturas dos arquivos, assegura mensagens para acessar arquivos, inicialização de aplicativos de cartão, e canais lógicos para utilização quando o cartão puder ter mais de um canal virtual de comunicação ativo. Comandos específicos de aplicação não são descritos, e desta forma o padrão trata os códigos de comando como aplicações específicas quando não definidas nesta parte. |
| | Cartões de Identificação **ISO/IEC 7816-5** Parte 5: Sistema de numeração e procedimento de registro para identificadores de aplicação. | **R** | | |
| | **ISO/IEC 7816-7** Parte 7: Comandos intersetoriais para *Structured Card Query Language* (SCQL); | **R** | | Conforme escolha do GT da ICP-Brasil. A atual edição foi publicada em junho de 1994. Existe também uma alteração ISO/IEC 7816-5/AM1 *Registered Application Provider Identifiers* (RDIs) (Identificadores de Provedores de Aplicações Registradas) que foi publicada em dezembro de 1996. |
| | **ISO/IEC 7816-11** Parte 11: Estrutura para o manuseio dinâmico de aplicações múltiplas em cartões de circuitos integrados. | **R** | | |
| | Cartões de identificação **ISO/IEC 7813** – Cartões de transações financeiras. | **R** | Cartões financeiros. | |
| | Cartões de identificação dos emissores **ISO/IEC 7812-2** Parte 2: Procedimentos de aplicação e registro. | **R** | Todos. | |
| | Cartões de identificação **ISO/IEC 15693-4** – Cartões de circuito(s) integrado(s) sem contato, Cartões de proximidade {*Vicinity Integrated Circuit(s) Cards* (VICC) (Cartões de Circuito(s) Integrado(s) de Proximidade} Parte 4: Registro de aplicações/emissores. | **R** | Cartões de circuito integrado de proximidade. | |
| | Sistemas de cartão de identificação **EN 1332-1**:1999 – Interface homem-máquina – Parte 1: Princípios de projeto para interface de usuário Sistemas de cartão de identificação **EN 1332-4:**1999 – Interface Homem-máquina – Parte 4: Codificação de exigências de usuário para pessoas com necessidades especiais. | **R** | Todos. | |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| Elétrico | Cartões de identificação **ISO/IEC 7816-10** – Cartões de circuito(s) Integrado(s) com contatos – Parte 10: Sinais eletrônicos e resposta para reinicialização para cartões síncronos. **ISO/IEC 7816—12** Parte 12: Interface USB. | **R** | Cartões de circuito(s) integrado(s) com contatos. | |
| | Cartões de identificação **ISO/IEC 14443-2** – Cartões de circuito(s) Integrado(s) sem contato – Cartões de proximidade – Parte 2: Interface de potência e sinal de freqüência de rádio. | **R** | Cartões de circuito integrado de proximidade. | Esta parte define a interface de freqüência de rádio, e contém duas técnicas de modulação bem diferentes (Tipos A e B) para a comunicação de dados entre cartão e terminal. O tipo A é baseado na tecnologia Philips Mifare (amplamente licenciada para outros fabricantes). O tipo B é um novo conceito. Estes dois tipos são processados em paralelo nesta parte do padrão e da parte 3. Além disso, alguns itens específicos do Tipo A aparecem na parte 4. |
| | Cartões de identificação **ISO/IEC 10536-3** Cartões de circuito(s) integrado(s) sem contato {*Close Coupling Integrated Circuit(s) Cards* (CICC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)} Parte 3: Procedimento de sinais eletrônicos e reinicialização. | **F** | Cartões de circuito(s) integrado(s) de acoplamento forte. | |
| | Cartões de identificação **ISO/IEC 15693-2** Cartões de circuito(s) integrado(s) sem contato. Cartões de Proximidade {*Vicinity Integrated Circuit(s)* Cards (VICC) (Cartões de Circuito(s) Integrado(s) de Proximidade)}: Parte 2: Interface e inicialização pelo ar; | **R** | Cartões de circuito(s) integrado(s) de proximidade sem contato. | |
| Protocolos de comunicações | Cartões de identificação **ISO/IEC 7816-3** Parte 3: Protocolos de sinais e transmissões eletrônicas. | **R** | Cartões de circuito(s) integrado(s) com contatos. | Conforme escolha do GT da ICP-Brasil |
| | Cartões de identificação **ISO/IEC 14443-3** - Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade – Parte 3: Inicialização e anticolisão. | **R** | Cartões de circuito(s) integrado(s) de proximidade. | Esta parte dá continuidade ao duopólio dos Tipos A e B, definindo procedimentos de inicialização e anticolisão de cartões e protocolos básicos de comunicações. Os procedimentos de anticolisão são métodos utilizados para |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| | Cartões de identificação **ISO/IEC 14443-4** – Cartões de circuito(s) integrado(s) sem contato – cartões de proximidade – Parte 4: Protocolos de transmissão. | | | identificar e selecionar um cartão quando vários cartões estiverem ativos dentro do campo RF do terminal.<br><br>Este contém informações de alto nível (nível de mensagem) de protocolo de transmissão de dados, equivalentes ao protocolo T=1 do ISO/IEC 7816, e é uma ponte sobre o ISO 7816-4. Somente para cartões Tipo A o ISO/IEC 14443-4 inclui um procedimento de inicialização de protocolo. |
| | Cartões de identificação **ISO/IEC 15693-3** – Cartões de circuito(s) integrado(s) sem contato – cartões de proximidade – Parte 3: Protocolo de anticolisão e transmissão. | **R** | Cartões de circuito integrado de proximidade sem contato. | |
| | Mensagem originada de cartão de transação financeira **ISO 8583** – especificação de mensagem de intercâmbio. | **F** | Todos. | |
| | Cartões de transações financeiras **ISO 9992-1** – Mensagens entre o cartão de circuito integrado e o dispositivo de aceitação do cartão – Parte 1: Conceitos e estruturas; ISO 9992-2<br>Parte 2: Funções, mensagens (comandos e respostas), elementos e estruturas de dados. | **F** | Todos. | |
| | Cartões de transações financeiras **ISO 10202-2** Arquitetura de segurança de sistemas transação financeira usando cartões de circuito integrado.<br>Parte 2: Processo de transação; ISO 10202-6<br>**Parte 6: Verificação do portador do cartão.** | **R** | Todos. | |
| | Cartões de identificação **ISO/IEC 10536-4** cartões de circuito(s) integrado(s) sem contato {*Close Coupling Integrated Circuit(s) Cards* (CCIC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)}.<br>Parte 4: Resposta a protocolos de reinicialização e | **F** | Cartões de circuito(s) integrado(s) de acoplamento forte. | |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| | transmissão. | | | |
| Os Padrões de físico/físico e de interface cobrem as dimensões do cartão;<br><br>localidade e *layout* de contatos. | **Características físicas**<br>Cartões de identificação<br>**ISO/IEC 7810** | **R** | Todos os cartões de contato e combinação | Para assegurar que possam ser lidos em leitora padrão, todos os cartões devem seguir o formato ID-1 conforme definido neste padrão. |
| | **Cartão Magnético**<br>**ISO/IEC 7811**, partes 2, 4 e 5: definem as propriedades, posicionamento e codificação (*coding*) da banda magnética do cartão. | **R** | Todos os cartões com banda magnética. | |
| | **Cartão de memória ótica**<br><br>**ISO/IEC 11693** e **11694.** | **F** | Cartões óticos. | Cartões que suportam o armazenamento de muitos *megabytes*. |
| | Cartões de identificação<br>**ISO/IEC 7816-1**<br>Parte 1: Características físicas<br>Cartões de identificação<br>**ISO/IEC 15693-1** - Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade - Parte 1: Características físicas.<br>Cartões de identificação<br>**ISO/IEC 7816-2** – Cartões de circuito(s) integrado(s) com contatos<br>Parte 2: Dimensões e localização dos contatos. | **A** | Cartões de circuito(s) integrado(s) com contatos. | Esta parte suplementa o ISO/IEC 7810, estabelecendo as características físicas particulares dos cartões de CI com contatos.<br><br>Conforme escolha do GT da ICP-Brasil e Manual de Condutas Técnicas do ITI – Volume I. |
| | Cartões de identificação<br>**ISO/IEC 14443-1** – Cartões de circuito(s) integrado(s) sem contatos – Cartões de proximidade - Parte 1: Características físicas. | **R** | Cartões de circuito integrado de proximidade. | Esta parte suplementa as características físicas definidas no ISO/IEC 7810. |
| | Cartões de identificação<br>**ISO/IEC 15693-1** – Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade - Parte 1: Características físicas. Esta parte do **ISO/IEC 15693** foi publicada em 15-07-2000. | **R** | Cartões de circuito(s) integrado(s) de proximidade sem contato. | Esta parte do **ISO/IEC 15693** foi publicada em 15-07-2000. |
| | Cartões de identificação<br>**ISO/IEC 10536-1** – Cartões de circuito(s) integrado(s) sem contato<br>Parte 1: Características físicas;<br>**ISO/IEC 10536-2**<br>Parte 2: Dimensões e localização das áreas de acoplamento. | **F** | Cartões de circuito(s) integrado(s) de acoplamento forte. | |
| | Identificadores táteis.<br><br>Sistemas de Cartões de | **F** | Quando a gravação em relevo não é | Alguns equipamentos de personalização de cartões, a menos que modificados, |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| | identificação **BS EN 1332-2** – Interface homem-máquina Parte 2: Dimensões e localização - um identificador tátil para cartões ID-1. | | utilizada e existe é solicitado ao usuário que introduza o cartão em um determinado sentido, um identificador tátil deverá ser fornecido como auxílio aos deficientes visuais. | poderão ter dificuldade no processamento de cartões com identificadores táteis do tipo '*notch*' ('relevo'). Um acordo, portanto, deve ser realizado junto ao fornecedor do serviço de personalização para a utilização de tais cartões. |
| Segurança | Cartões de identificação **ISO/IEC 7816-8** – Cartões de circuito(s) integrado(s) com contatos.<br><br>Parte 8: Comandos de segurança intersetoriais ISO/IEC 7816-9<br>Parte 9: Comandos adicionais intersetoriais e atributos de Segurança.<br><br>Cartões de identificação **ISO/IEC 7816-11** – Cartões de circuito(s) integrado(s) com contatos<br>- Parte 11: Verificação pessoal através de métodos biométricos.<br><br>Cartões de identificação **ISO/IEC 7816-15** – Cartões de circuito(s) integrado(s) com contatos - Parte 15: Informação de dispositivo Criptográfico em cartões CI. | **A** | Cartões de circuito(s) integrado(s) com contatos. | |
| | Cartões de transação financeira **ISO 10202**<br>Arquitetura de segurança de sistemas de transação financeira utilizando cartões de circuito integrado<br>Parte 1: Ciclo de vida do cartão;<br>Parte 2: Princípios e apanhado geral;<br>Parte 3: Relacionamentos de chave criptográfica;<br>Parte 4: Módulos seguros de aplicação;<br>Parte 5: Utilização de algoritmos;<br>Parte 6: Verificação do portador do cartão;<br>Parte 7: Gerenciamento de chave. | **F** | Todos. | |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| Infra-estrutura do terminal | Sistemas de cartões de identificação EN 1332-3:1999 – Interface Homem-máquina – Parte 3: Teclados. | **R** | Todos. | |
| | Padrões PC/SC.<br><br>Padrões do Consórcio Grupo de Trabalho PC/SC Especificação de Interoperabilidade para ICCs e Sistemas de Computador Pessoal<br>Parte 1. Introdução e Visão Geral da Arquitetura<br>Parte 2. Requisitos de Interface para Cartões Compatíveis com CI e Dispositivos de Interface<br>Parte 3. Requisitos para Dispositivos de Interface Conectados a PC<br>Parte 4. Considerações do projeto IFD e Informação de Referência do Projeto<br>Parte 5. Definição do Gerenciador de Recursos ICC<br>Parte 6. Definição do Interface do Fornecedor de Serviço ICC<br>Parte 7. Considerações do Projeto de Domínio / Desenvolvedor da Aplicação<br>Parte 8. Recomendação para a Implementação de Dispositivos de Segurança e Privacidade ICC. | **A** | Todos. | Para uso geral em PCs. |
| | Manual de Condutas Técnicas do ITI – Volume I. | **A** | Cartões com capacidade de gerenciamento de certificados digitais. | |
| | Padrão FIPS-140-2. | **A** | Todos. | Segundo o item 1 do GT da ICP-Brasil: seguir no mínimo as regras estabelecidas para o nível 1 de segurança do FIPS-140-2. Seguir no mínimo as regras estabelecidas para o nível 2 de segurança para verificação de violação do hardware. |

| Componente | Especificação | SIT | Aplicável a | Observações |
|---|---|---|---|---|
| Cartões tipo **Java Card®** | API (*Application Programming Interface*) para a plataforma de cartões Java Card. | **A** | Esta API define um conjunto de classes a partir das quais a tecnologia Java Card baseada em *applets* pode ser construída. | Versão geral para a tecnologia Java Card é 2.2.1 (outubro de 2003), http://java.sun.com/products/javacard/ |
| | Especificação para o ambiente de execução (*runtime environment*) para a plataforma Java Card. | **A** | Esta especificação descreve o ambiente requerido para a execução de *applets* baseado em cartões Java Card. | |
| | Especificação para a máquina virtual para a plataforma Java Card. | **A** | Esta especificação define a configuração requerida para a máquina virtual do cartão. | |

# 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 para intercâmbio de dados.

**9.1.2.** Uso de XML *Schema* e da UML (quando for o caso) para definição dos dados para intercâmbio.

**9.1.3.** Uso de XSL para transformação de dados.

**9.1.4.** Uso de um padrão de metadados para a gestão de conteúdos eletrônicos.

## 9.2. Organização e Intercâmbio de Informações: Especificações Técnicas

**Tabela 12 – Especificações para Organização e Intercâmbio de Informações**

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>F = Estudo Futuro | | |
| Linguagem para intercâmbio de dados | XML (*Extensible Markup Language*) como definido pelo W3C<br>http://www.w3.org/XML | **R** | |
| Transformação de dados | XSL (*Extensible Stylesheet Language*) como definido pelo W3C http://www.w3.org/TR/xsl<br><br>XSL *Transformation* (XSLT) como definido pelo W3C<br>http://www.w3.org/TR/xslt | **R** | |
| Definição dos dados para intercâmbio | XML *Schema* como definido pelo W3C:<br>- XML *Schema Part 0: Primer*<br>http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/<br>- XML *Schema Part 1: Structures*<br>http://www.w3.org/TR/xmlschema-1/structures<br>- XML *Schema Part 2: Datatypes*<br>http://www.w3.org/TR/xmlschema-2/datatypes<br>UML (*Unified Modeling Language*) como definido pelo OMG<br>http://www.omg.org/gettingstarted/specsandprods.htm/ | **R** | |
| Descrição de dados | RDF (*Resource Description Framework*)<br>Como definido pela W3C. | **F** | |
| Elementos de Metadados para gestão de conteúdos | e-PMG – Padrão de Metadados para o Governo Eletrônico. | **E** | |
| Taxonomia para navegação | LAG - Lista de Assuntos do Governo, Versão 1.0.<br>Conforme definição em http://www.eping.e.gov.br | **A** | |

| Componente | Especificação | SIT | Observações |
|---|---|---|---|
| Definição de dados | CPD - Catálogo de Padrões de Dados, Versão 1.0. Conforme definição em http://www.eping.e.gov.br | **A** | |

### 9.3. Notas sobre XML e *Middleware*

Nem todos os sistemas necessitam ter capacidade de se comunicar diretamente em XML, como representado na Figura 5. Quando apropriado é aceitável a utilização de *middleware* de acordo com a ilustração da Figura 6.

Embora as configurações abaixo apresentem soluções potenciais, o modelo XML direto (Figura 5) é preferencial, sendo possível a utilização do modelo indireto, apresentado na Figura 6, em casos onde existam razões fundamentais que justifiquem seu uso.


**Figura 5 – Modelo XML Direto – Intercâmbio Direto.**

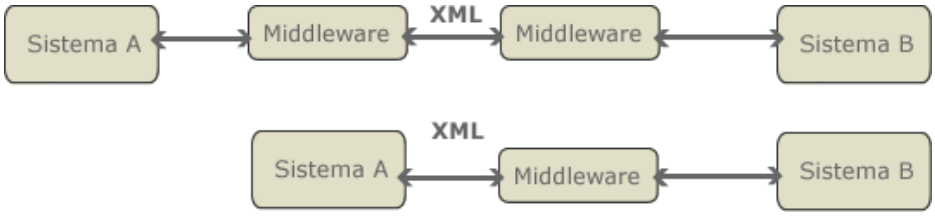


**Figura 6 – Intercâmbios via *middleware.***

# 10. Áreas de Integração para Governo Eletrônico

## 10.1. Áreas de Integração para Governo Eletrônico: Políticas Técnicas

**As diretrizes para o segmento são:**

- As especificações técnicas sob responsabilidade do segmento incluem:
  - XML *Schemas* referentes a aplicações voltadas a Áreas de Atuação de Governo, organizados na forma de Catálogo, disponível no sítio da e-PING e apresentado com os conteúdos atuais em tópico a seguir;
  - 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.
- No que tange a XML *Schemas* referentes a aplicações voltadas a Áreas de Atuação de Governo, o segmento atuará buscando a identificação, acompanhamento da produção e análise de conteúdos de interesse da Administração Pública, em articulação com grupos representativos do governo e da sociedade, reportando-se a instâncias competentes no que tange à priorização;
- As especificações técnicas referentes a XML *Schemas* constantes do Segmento Organização e Intercâmbio de Informações devem ser atendidas pelos proponentes;
- A partir do entendimento de que a materialização do uso de XML *Schemas* se dá através de serviços interoperáveis:
  - Recomenda-se que a Arquitetura Orientada a Serviços (SOA) e as políticas técnicas relacionadas ao Segmento Interconexão sejam observadas no projeto e implementação de aplicações baseadas nos XML *Schemas* referidos;
  - O segmento passa a referenciar a iniciativa "Arquitetura Referencial de Interoperação dos Sistemas Informatizados de Governo (AR)", que é um modelo de Arquitetura Orientada a Serviços, adaptado à realidade dos Sistemas Informatizados de Governo e que, pode ser acessada em http://i3gov.cos.ufrj.br/igov/;
- Existe forte interligação entre o Catálogo de Padrões de Dados e o Catálogo de XML *Schemas* e, consideradas as especificidades dos conteúdos, busca-se manter os princípios gerais e mecanismos de gestão compatíveis.

## 10.2. Áreas de Integração para Governo Eletrônico: Notas sobre Catálogo de XML *Schemas*

### 10.2.1. Considerações Iniciais

A arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico preconiza a adoção do XML e o desenvolvimento de XML *Schemas* como fundamentos para a integração e interoperabilidade eletrônica do governo. Neste sentido, a constituição de repositório que permita a gestores e projetistas de aplicações de Governo Eletrônico consultar XML *Schemas* consolidados, bem como propor a catalogação de esquemas sob sua responsabilidade, tem inegável contribuição para consolidar boas práticas de interoperabilidade no âmbito governamental.

### 10.2.2. Objetivo

O Catálogo tem por objetivo estabelecer padrões de XML *Schemas* que se aplicam às interfaces de sistemas que apóiem a oferta de serviços de Governo Eletrônico.

### 10.2.3. Escopo

O Catálogo contém os padrões aceitos, na forma de XML *Schemas* para intercâmbio de dados envolvendo o setor público. Tais padrões tanto podem constituir-se em um único esquema, quanto

em um conjunto de XML *Schemas*, desde que o conjunto se refira a uma mesma temática dentro da Área de Integração associada.

A publicação de XML *Schemas* não implica automaticamente em garantia de acesso aos conteúdos correspondentes ou serviços associados, para o quê podem ser definidas regras específicas pelo respectivo gestor.

### 10.2.4. Propriedade e Responsabilidade

A Coordenação da e-PING é responsável por este Catálogo, em especial pelo gerenciamento dos processos de mudanças e por fomentar que os padrões sejam usados em desenvolvimentos futuros.

Neste sentido, recomenda-se que o desenvolvimento ou manutenção de sistemas que apóiem a oferta de serviços de Governo Eletrônico correlatos a áreas/sub-áreas de atuação de governo contempladas no Catálogo considerem os XML *Schemas* publicados.

O desenvolvimento e manutenção deste Catálogo são de responsabilidade do Grupo Áreas de Integração para Governo Eletrônico que tem a participação de diferentes segmentos do governo nas esferas federal e estadual.

### 10.2.5. Mecanismos de Gestão do Catálogo de XML *Schemas*

As entradas no Catálogo de XML podem se dar através das seguintes situações:

a) Proposição seguida de aceite de proposta de conteúdo para o Catálogo de Padrões de Dados (CPD);

b) Submissão seguida de aceite de proposta de conteúdo à Arquitetura Referencial de Interoperação dos Sistemas Informatizados de Governo (AR);

c) Submissão, por profissional vinculado ao setor público, de conteúdo diretamente ao Catálogo de XML *Schemas*, através de formulário eletrônico disponível a partir do sítio da e-PING.

Nas situações descritas nos itens (b) e (c) os conteúdos serão encaminhados para análise dos integrantes do Grupo Organização e Intercâmbio de Informações, de forma a avaliar a pertinência de publicar Padrão(ões) de Dado(s) associado(s).

A proposição de cadastro de XML *Schemas* será submetida à análise dos integrantes do Grupo Áreas de Integração para Governo Eletrônico por meio de formulário eletrônico específico, disponível no sítio da e-PING (www.e-ping.e.gov.br). Serão mantidas no Catálogo apenas as proposições aceitas, sendo que as que ainda estiverem em estudo, as rejeitadas, bem como as versões anteriores de XML *Schemas* aceitos serão mantidas em ambiente “de trabalho” a ser oportunamente concebido e implementado.

Os critérios de avaliação empregados incluirão:

- reconhecimento pela comunidade usuária;
- acordo do gestor da área/sub-área (no caso de não ser ele o proponente); e
- aderência aos padrões da e-PING.

Ou seja, a ocorrência de submissões em que o proponente de determinado XML *Schemas* não seja o gestor da área está prevista, mas terá como condição adicional de aceite a concordância do gestor, a partir de interlocução realizada pelo próprio proponente e/ou pelo Grupo Áreas de Integração para Governo Eletrônico.

Solicitações de alteração para XML *Schemas* já publicados serão analisadas preliminarmente pelos integrantes do Grupo Áreas de Integração para Governo Eletrônico. A decisão de aceite caberá à Coordenação Central da e-PING, que poderá adotar as mudanças propostas conforme sua abrangência e impacto ou submetê-las à consulta pública, através do sítio http://www.governoeletronico.gov.br.

A carga inicial do Catálogo, apresentada a seguir, foi constituída por conjuntos de XML *Schemas* relacionados a iniciativas já mapeadas pelos integrantes do Grupo Áreas de Integração para

Governo Eletrônico. O objetivo de publicar estes conteúdos é o de dar visibilidade a casos de uso efetivos de XML *Schemas* por parte da Administração Pública Federal e órgãos parceiros.

Os conteúdos consolidados na carga inicial e as atualizações podem ser consultadas na página da e-PING (www.e-ping.e.gov.br).

### 10.2.6. Gabarito de XML *Schemas*

Cada XML *Schema*, ou agrupamento de XML *Schemas* correlatos, deve ser documentado de acordo com o seguinte gabarito:

**ÓRGÃO PROPONENTE**: Nome do Órgão superior proponente do XML *Schema*. Ex.: Ministério da Agricultura, Ministério da Educação, Ministério do Meio Ambiente etc;

**RESPONSÁVEL**: Nome do profissional responsável pela proposição do XML *Schema*;

**CPF**: CPF do profissional responsável pela proposição do XML *Schema*;

**UNIDADE DE LOTAÇÃO**: Unidade de lotação do responsável pela proposta de cadastro. Indicar a seqüência de unidades até o Órgão superior, por exemplo, GIS/DSI/SLTI/MP;

**E-MAIL**: Endereço eletrônico do profissional responsável pela proposição do XML *Schema*;

**TELEFONE 1**: Número do telefone de contato com profissional responsável pela proposição do XML *Schema*;

**TELEFONE 2**: Número do telefone de contato alternativo com profissional responsável pela proposição do XML *Schema*. Campo de preenchimento opcional;

**INDICADOR DE GESTÃO**: Indicação da situação do proponente em relação à gestão da área/sub-área a que se refere o XML *Schema*. Deve ser preenchido através do assinalamento de uma das opções (Sim ou Não);

**ÓRGÃO GESTOR**: Aquele órgão com atribuições para gerir a área/sub-área à qual se refere o XML *Schema*. Deve ser preenchido apenas quando o indicador de gestão for "Não" e o órgão gestor for de conhecimento do proponente;

**NOME DO XML *SCHEMA***: Denominação usual do agrupamento ou do único XML *Schema* que se propõe catalogar;

**VERSÃO**: Versão do XML *Schema* que se propõe catalogar;

**URL DO XML SCHEMA**: URL em que será encontrado arquivo XSD (Definição de XML *Schema*) e informações detalhadas sobre o (conjunto de) XML *Schema*;

**DESCRIÇÃO**: Breve descrição sobre o (conjunto de) XML *Schema*. E considerações que o proponente considerar pertinente.

**SUB-ÁREA**: Denominação usual dentro da área de atuação de governo à qual o conjunto de XML *Schema* se refere, deve ser informada apenas quando a área não for suficiente para qualificar a temática contemplada pelo XML *Schema*;

**XML *SCHEMAS* COMPONENTES**: Nome dos XML *Schemas* que compõem aquele que está sendo cadastrado.

### 10.2.7. Classificação do Catálogo de XML *Schemas*

O Catálogo de XML *Schemas* será organizado por Áreas Temáticas de Atuação de Governo, na qual serão relacionados XML *Schemas* organizados segundo classificação de 1º nível dada pela Lista de Áreas de Atuação de Governo, que tem como referência o Plano Plurianual (PPA), e é apresentada a seguir:

**Lista de Áreas de Atuação de Governo, baseada no Plano Plurianual – PPA:**

1. Assistência Social;
2. Saúde;

3. Segurança Pública;
4. Educação;
5. Administração;
6. Administração Tributária;
7. Habitação;
8. Ciência e Tecnologia;
9. Comércio e Serviços;
10. Relações Exteriores;
11. Defesa Nacional;
12. Encargos Especiais;
13. Cultura;
14. Gestão Ambiental;
15. Previdência Social;
16. Trabalho;
17. Transporte;
18. Energia;
19. Agricultura;
20. Organização Agrária;
21. Comunicações;
22. Judiciária;
23. Legislativa;
24. Essencial à Justiça;
25. Direitos da Cidadania;
26. Desporto e Lazer;
27. Indústria;
28. Saneamento;
29. Urbanismo.

A versão eletrônica do Catálogo de XML *Schemas* proverá como opção de busca alternativa à classificação por Lista de Áreas de Atuação de Governo, lista alfabética dos XML *Schemas* catalogados.

### 10.3. Áreas de Integração para Governo Eletrônico: Especificações Técnicas

As especificações para as Áreas de Integração para Governo Eletrônico são:

**Tabela 13 – Especificações para Áreas de Integração para Governo Eletrônico – Temas Transversais a Áreas de Atuação de Governo**

| Temas | Especificação | ST | Observações |
|---|---|---|---|
| | A = Adotado<br>R = Recomendado<br>T = Em Transição<br>E = Em Estudo<br>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. |

| Temas | Especificação | ST | Observações |
|---|---|---|---|
| PROCESSOS – Notação de Modelagem de Processos | BPMN 1.0, conforme definido pelo OMG http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf | **R** | |
| INFORMAÇÕES GEORREFERENCIADAS – Interoperabilidade entre sistemas de informação geográfica | WMS versão 1.0 ou posterior http://www.opengeospatial.org/standards | **A** | |
| | WFS versão 1.0 ou posterior http://www.opengeospatial.org/standards | **A** | |
| | WCS versão 1.0 ou posterior http://www.opengeospatial.org/standards | **A** | |
| | CAT | **E** | |
| | WFS-T | **E** | |

**Tabela 14 – Especificações para Áreas de Integração para Governo Eletrônico – Catálogo de XML *Schemas* referentes a Áreas de Atuação de Governo**

| Área/Sub-Área | Especificação | Observações |
|---|---|---|
| ADMINISTRAÇÃO – Compras Governamentais | https://www.comprasnet.gov.br/xml/aviso.xsd<br><br>https://www.comprasnet.gov.br/xml/consultamatserv.xsd<br><br>https://www.comprasnet.gov.br/xml/dispinex.xsd<br><br>https://www.comprasnet.gov.br/xml/contratoent.xsd<br><br>https://www.comprasnet.gov.br/xml/empenho.xsd<br><br>https://www.comprasnet.gov.br/xml/resultado.xsd | XML *Schemas* pelo sistema ComprasNet referentes a Encerramento de Resultado de Licitação, Empenho, Dispensa / Inexigibilidade de Licitação, Consulta de Material via CATMAT, Contrato de entidades não SISG e Aviso de Licitação. |
| ADMINISTRAÇÃO – Estruturas de Governo | http://guialivre.governoeletronico.gov.br/igov/ | Conjunto de XML *Schemas* relacionados aos sistemas de gestão administrativa da Administração Pública Federal. |
| ADMINISTRAÇÃO – Gestão de Redes Locais/CACIC | http://guialivre.governoeletronico.gov.br/cacic/sisp2/invent/Invent.html | Estes *Schemas* fazem parte da solução CACIC, que foi desenvolvida pela Dataprev, e são utilizados para transmissão de dados de inventário de *hardware* e de seus componentes conectados em ambiente de rede.<br>A implementação destes *Schemas* ocorreu em parceria com o Ministério do Meio Ambiente (MMA). |
| ADMINISTRAÇÃO TRIBUTÁRIA – Nota Fiscal Eletrônica | http://200.198.224.29/portal/info/Schemas.htm | *Schema* XML utilizado para emissão da nota fiscal eletrônica, em substituição a de papel e com validade jurídica para todos os fins. Este projeto é coordenado pelo Encontro Nacional dos |

| Área/Sub-Área | Especificação | Observações |
|---|---|---|
| | | Administradores e Coordenadores Tributários Estaduais (ENCAT) e desenvolvido em parceria com a Secretaria da Receita Federal. |
| DIREITOS DA CIDADANIA – Cartórios | http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd | Cabe ao Ministério da Justiça manter o Cadastro Nacional de Cartórios. Este esquema, a partir de um filtro gerado pela unidade da federação e/ou o município e/ou bairro e/ou a atribuição do cartório, consulta o cadastro de cartórios do Brasil devolvendo uma lista dos cartórios que atendem ao filtro. O esquema permite, ainda, entregar o detalhamento de cada cartório listado. |
| DIREITOS DA CIDADANIA – Defesa do Consumidor | http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd | Este esquema permite a consulta à estatística consolidada sobre atendimento nos Procons conveniados ao Sistema Nacional de Informações de Defesa do Consumidor (SINDEC) por unidade da federação ou nome do fornecedor ou o CNPJ, devolvendo as estatísticas de atendimento aderentes aos critérios pesquisados. |
| DIREITOS DA CIDADANIA – Defesa do Consumidor | http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd | Cabe ao Ministério da Justiça formular, promover, supervisionar e coordenar a política de proteção da ordem econômica, nas áreas de concorrência e defesa do consumidor. O procedimento pelo qual o fornecedor informa ao público sobre os defeitos detectados nos produtos ou serviços que colocara no mercado é chamado de *recall*. Os objetivos essenciais desse tipo de procedimento são o de proteger e preservar a vida, saúde, integridade e segurança do consumidor, bem como de evitar ou minimizar quaisquer espécies de prejuízos, quer de ordem material, quer de ordem moral. Este esquema permite |

| Área/Sub-Área | Especificação | Observações |
|---|---|---|
| | | consultar a base de banco de dados de *recall* do Departamento de Proteção e Defesa do Consumidor para conferir se um determinado produto está sendo objeto de *recall.* Para isso, o esquema ao ser acionado retorna a lista de fornecedores/modelos que fizeram *recall*, possibilitando verificar detalhes do *recall* a partir da escolha do produto ou número de série, chassi, lote entre outros. |
| DIREITOS DA CIDADANIA | http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd | Cabe ao Ministério da Justiça exercer a classificação, para efeito indicativo, de diversões públicas e de programas de rádio e televisão.<br>A partir do nome do filme ou programa, este esquema consulta o banco de dados de Classificação Indicativa e devolve uma lista de coincidentes para os quais podem ser exibidos detalhes da classificação indicativa e a justificativa. |
| GESTÃO AMBIENTAL – Licenciamento Ambiental/PNLA | http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_completo.xsd<br><br>http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_simples.xsd<br><br>http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_totalizadores.xsd | Os *Schemas* se aplicam ao âmbito do licenciamento ambiental e são adotados pela plataforma do Portal Nacional de Licenciamento Ambiental (PNLA) do MMA que consolida as informações sobre licenças ambientais de vários estados por meio de *Web Services*.<br><br>Segue abaixo a descrição do propósito de cada esquema:<br><br>•licenciamento_ambiental_completo.xsd – fornece o esquema das informações pertinentes a uma licença ambiental, levando em conta os dados freqüentes nos diversos órgãos licenciadores pesquisados;<br><br>•licenciamento_ambiental_simples.xsd – fornece o esquema para a composição de um relatório contendo um conjunto de licenças com os dados mínimos de sua |

| Área/Sub-Área | Especificação | Observações |
|---|---|---|
| | | identificação. É útil para a navegação preliminar sobre as licenças para um posterior detalhamento que é feito por meio do primeiro esquema;<br><br>•licenciamento_ambiental_totalizadores.xsd – consolida o quantitativo de licenças baseado em um tema arbitrário. |
| JUDICIÁRIO – Serviços de Cartórios Extrajudiciais | www.anoregsp.org.br/arquivos | Os XML *Schemas* referem-se à padronização das consultas aos serviços de cartórios extrajudiciais |

# 11. Glossário de Siglas e Termos Técnicos[33]

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.

***Browser*:** Navegador da *web* – Uma aplicação cliente que permite ao usuário visualizar conteúdos da *World Wide Web* em outra rede ou no computador do usuário, acompanhar os vínculos de hipertexto e transferir arquivos.

**Catálogo de XML *Schemas***: diretório de informações sobre os XML *Schemas*.

**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.

**CAT – *Catalog Service Implementation Specification*:** especificação *OpenGIS* que define interfaces para publicar, acessar, navegar e consultar *metadados* sobre informações georreferenciadas. O termo mais utilizado atualmente para *Calatog Service* é CSW.

**CSW – *Catalog Service Implementation Specification*:** especificação *OpenGIS* que define interfaces para publicar, acessar, navegar e consultar *metadados* sobre informações georreferenciadas.

**Dispositivo**: componente físico (estação de trabalho, telefone celular, cartão inteligente, *hand-held*, televisão digital com acesso à Internet).

**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.

**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.

**GML – *Geography Markup Language***: especificação OpenGIS baseada no XML desenvolvida para permitir o transporte e armazenamento de informações geográficas/espaciais.

***Hand-helds*:** Computador de mão, também conhecido como PDA, pocket PC ou palm top.

[33] 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 Lingüística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

Equipamento portátil desenvolvido para servir como dispositivo de acesso.

***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.

**HELO:** parâmetros que limitam a entrega de e-mail comercial não solicitado. http://www.postfix.org/uce.html.

**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.icpbrasil.gov.br.

**IEEE – *Institute of Electrical and Electronics Engineers*** (Instituto de Engenheiros Elétricos e Eletrônicos): fomenta o desenvolvimento de padrões e normas que freqüentemente 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): método ou protocolo através dos quais os dados são enviados de um computador a outro na Internet. Cada computador, na Internet, possui pelo menos um endereço IP que o identifica unicamente em relação a todos os outros computadores da Internet.

**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): ver “IPv6”.

**IPv6 – *Internet Protocol Version* 6** (Protocolo de Internet Versão 6): último nível do IP, hoje já incluído como parte do suporte IP em muitos produtos, inclusive os principais sistemas operacionais de computadores. Formalmente, IPv6 é um conjunto de especificações da IETF. O IPv6 foi projetado como um conjunto evolutivo de aperfeiçoamentos feitos ao IPv4. O aperfeiçoamento mais significativo do IPv6 em relação ao IPv4 é que os endereços IP são aumentados de 32 bits para 128 bits.

**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.

**Meio de acesso:** conjunto de componentes físicos (dispositivos de acesso) e de não físicos (software básico, aplicativos, etc.) que permite ao usuário o acesso a um serviço de governo eletrônico.

**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:** são informações adicionais necessárias para que os dados se tornem úteis. É informação essencial para que se possa fazer uso dos dados. Em suma, metadados são um conjunto de características sobre os dados que não estão normalmente incluídas nos dados propriamente ditos. http://www.isa.utl.pt/dm/sig/sig20002001/TemaMetadados/trabalho.htm.

***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*.

***Newsgroup*** (Grupo de Notícias): discussão sobre um determinado assunto que consiste em mensagens enviadas a um sítio central na Internet e redistribuídas pela Usenet, uma rede global de grupos de discussão de notícias. Os usuários podem enviar mensagens a grupos de notícias existentes, responder a mensagens anteriores e criar novos grupos de notícias.

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

**OWS - OGC *Web Services*:** refere-se a todas as especificações *OpenGIS* que aplicam geoprocessamento por meio da Web.

**Padrão aberto:** todo o padrão tecnológico estabelecido por órgãos internacionais ou por consórcios de empresas do mercado que desenvolvem especificações que se encontram publicamente disponíveis. O PC (computador pessoal) foi lançado e é desenvolvido com padrão aberto. As especificações da Internet e seu desenvolvimento também. A grande maioria das linguagens de programação também.

**Padrão de Metadados:** Um conjunto de metadados é um padrão, definido por uma comunidade de usuários, que inclui um Vocabulário de elementos descritivos e um Esquema ou regras de codificação destes elementos num meio legível por computador. http://www.uff.br/gdo/htm/tsld013.htm.

***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.

**Rede Governo:** é o portal de entrada para todas as páginas do governo federal na Internet. http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm.

**Resolução nº 7 do Governo Eletrônico:** estabelece regras e diretrizes para os sítios na Internet da Administração Pública Federal (gov.br e mil.br). Dividida em 7 capítulos, a resolução trata da estrutura da informação, do controle e monitoramento, da gestão dos elementos interativos, do modelo organizacional, da identidade visual e da segurança dos sítios governamentais na rede mundial de computadores. http://www.governoeletronico.e.gov.br.

**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 subseqüentes 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.

Serviços Eletrônicos de Governo (*relacionados* Serviços de Governo Eletrônico, Serviços Eletrônicos):

Governo eletrônico pode ser definido pelo uso da tecnologia para aumentar o acesso e melhorar o fornecimento de serviços do governo para cidadãos, fornecedores e servidores. Em linhas gerais, as funções características do governo eletrônico são:

1. Prestação eletrônica de informações e serviços.
2. Regulamentação das redes de informação, envolvendo principalmente governança, certificação e tributação.
3. Prestação de contas públicas, transparência e monitoramento da execução orçamentária.
4. Ensino à distância, alfabetização digital e manutenção de bibliotecas virtuais.
5. Difusão cultural com ênfase nas identidades locais, fomento e preservação de culturas locais.
6. e-procurement, isto é, aquisição de bens e serviços por meio da Internet, como licitações públicas eletrônicas, pregões eletrônicos, bolsas de compras públicas virtuais e outros tipos de mercados digitais para os bens adquiridos pelo governo.
7. Estímulo aos e-negócios, através da criação de ambientes de transações seguras, especialmente para pequenas e médias empresas. http://www.governoeletronico.gov.br/r1.

**Sistemas de Informação do Governo Federal:** sistemas que apóiam as atividades de:

- gestão de governo: Planejamento, Orçamento, Execução Orçamentária, Administração Financeira, Administração de Recursos Humanos, Administração de Serviços Gerais, Gestão de Documentação e Informações, Organização e Modernização Administrativa, Recursos de Informação e Informática e Controle Interno;
- atuação final de governo: atividades finalísticas dos diversos órgãos da estrutura governamental, como infra-estrutura (transporte, comunicações, energia, administração de recursos naturais), Agricultura, Saúde, Educação, etc.

referência: http://www.redegoverno.gov.br/projetos/reg_gestao.asp.

**SFS – *Simple Features Specification for* SQL:** especificação *OpenGIS* que define a padronização do esquema SQL que suporta armazenamento, recuperação, consulta e atualização sobre informações georreferenciadas.

***Smart Cards*:** cartão de plástico, com aproximadamente o tamanho de um cartão de crédito, com um microchip embutido que pode ser carregado com dados, pode ser usado para efetuar chamadas telefônicas, pagamento eletrônicos em dinheiro e outras aplicações. É periodicamente atualizado para receber usos adicionais.

**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): Arquitetura proposta 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.

**SPAM:** e-mail não solicitado na Internet. Do ponto de vista do remetente, essa é uma forma de mensagem em massa, geralmente para uma lista separada de pessoas inscritas a um grupo de discussão Usenet ou obtida por empresas especialistas em criar listas de distribuição de e-mail. Para o destinatário, o *spam* normalmente é considerado como lixo.

**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.

**Telnet**: a maneira de acessar o computador de outra pessoa, assumindo que lhe deram permissão. Mais tecnicamente, Telnet é um comando de usuário e um protocolo subliminar TCP/IP para acessar computadores remotos.

**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 seqüência 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.

**UML – *Unified Modeling Language* (Linguagem de Modelagem Unificada):** A UML é muito mais que a padronização de uma notação, ou seja, ela é uma linguagem-padrão para a elaboração da estrutura de projetos de *software*, incluindo aspectos conceituais tais como processos de negócios e funções do sistema, além de itens concretos como as classes escritas em determinada linguagem de programação, esquemas de banco de dados e componentes de *softwares* reutilizáveis. A UML pode ser empregada para a visualização, a especificação, a construção e a documentação de artefatos de sistemas de *software,* também pode ser utilizada na modelagem de negócios e outros tipos de sistemas e não apenas de *software*.

**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.

**Usenet**: coleção de notas e mensagens submetidas por usuários sobre vários assuntos que são enviados aos servidores em uma rede mundial. Cada coleção de notas enviadas é conhecida como um newsgroup.

**VPN – *Virtual Private Networks*** (Rede Privada Virtual): Rede particular, que se utiliza da infra-estrutura 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 Implementation Specification*:** especificação *OpenGIS* que define interfaces para acessar e manipular operações (*GetCapabilities, DescribeCoverage* e *GetCoverage*) sobre informações georreferenciadas no formato Coverage.

***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 Implementation Specification*:** especificação *OpenGIS* que define interfaces para acessar e manipular operações (*GetCapabilities, DescribeFeaureType, GetFeature, Transaction* e *LockFeature*) sobre informações georreferenciadas, por meio do protocolo HTTP. Baseado nessas operações, duas classes de serviços podem ser definidas:

- **WFS Básico (WFS):** é capaz de implementar apenas as operações: *GetCapabilities, DescribeFeatureType* e *GetFeature*. Por isso, é considerado um serviço WMS somente leitura.
- **WFS Transacional (WFS-T):** é capaz de implementar todas as operações de um WFS básico e operações transacionais. Opcionalmente, poderia implementar também a operação *LockFeature*.

**WMS – *Web Map Service Implementation Specification*:** especificação OpenGIS que define interfaces para acessar e manipular operações (*GetCapabilities, GetMap, GetFeatureInfo*) sobre múltiplas camadas (*layers*) de informações georreferenciadas, contendo vetores e/ou imagens.

**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. http://www.uff.br/gdo/htm/tsld106.htm.

**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).

# 12. Integrantes

## Coordenação da e-PING

Associação Brasileira de Empresas Estaduais de Processamento de Dados (ABEP)
- Dayse Vianna
- Paulo Cezar Coelho

Banco do Brasil (BB)
- Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)
- Ângela B. Baylo

Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
- Humberto Degrazia Campedelli
- José Antônio Borba Soares
- Rodrigo Novais Coutinho

Ministério da Justiça (MJ)
- Jorilson da Silva Rodrigues

Ministério da Saúde (MS)
- Eliane Pereira dos Santos
- Ernani Bento Bandarra
- Márcia Helena Gonçalves Rollemberg

Ministério das Relações Exteriores (MRE)
- Celso Ricardo Hottum Meira

Ministério do Planejamento, Orçamento e Gestão – Secretaria de Logística e Tecnologia da Informação (MP/SLTI)
- Leandro Corte (Coordenador Geral)
- Ednylton Maria Franzosi
- Eduardo Favero
- José Ney de Oliveira Lima
- Leonardo Boselli da Motta
- Leonardo Lanna Guillén
- Nazaré Lopes Bretas
- Rogério Santanna dos Santos
- Sylmara Campos Pinho Garcia

Presidência da República (PR)
- Marcelo André de Barros Oliveira

Presidência da República – Instituto Nacional de Tecnologia da Informação (ITI)
- Mauricio Augusto Coelho
- Renato da Silveira Martini
- Viviane Regina Lemos Bertol

Serviço Federal de Processamento de Dados (SERPRO)
- Antônio Sérgio Borba Cangiano
- Elói Juniti Yamaoka
- Geancarlo Noronha Vinhal
- Paulo Cezar Czarnewski
- Wagner Junqueira Araújo

## Grupo de Trabalho Interconexão

Leonardo Lanna Guillén (MP/SLTI) - Coordenador
Adriano Soriano (CAIXA)
Areno Pires Filho (MC)
Carlos Bellone Neto (RFB)
Daniel Moreira Guilhon (CGU)
Filipe Guimarães (MRE)

Frederico Duarte Guerra de Macedo (ME)
José Rodrigues Gonçalves Júnior (ITI)
Júlio César Japiassu Lyra (MJ)
Leonardo Boselli da Motta (MP/SLTI)
Luciene Pinheiro Capra (ANS)
Odilon de Freitas Militão Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Ruben César Macedo (CELEPAR-PR)
Sérgio de Oliveira Barcellos (MCT)
Sílvia Aparecida da Cunha (MP/CGTI)
Ulisses de Sousa Penna (BB)

**Subgrupo: *Web Services***
Ednylton Maria Franzosi (MP/SLTI) – Coordenador
Bruno Pacheco (SERPRO)
Carlos Falcão Maranhão (MS/ANS)
Cláudio Muniz Machado (MS)
Elaine Fabiano Tocantins (MJ)
Louise Neves (SERPRO)
Mauricio Dayrell (MMA)
Paulo Azevedo (BB)

**Colaboradores**
Claudia do Socorro Ferreira Mesquita (MP/SLTI)
Patrycia Barros de Lima Klaydianos (MP/SLTI)

## Grupo de Trabalho Segurança

Jorilson da Silva Rodirgues (MJ) – Coordenador
Alessandra Silva Moura(ANS)
Dante de Matos Gomes(PRODEB)
Edgar Luciano Morais Martins (MP/SLTI)
Érica Dantas (STJ)
Filipe Carneiro Guimarães (MRE)
Gleyner Martins Novais (SERPRO)
Humberto Degrazia Campedelli (DATAPREV)
Igor Guimarães (MC)
José D'Aleluia Nascimento (MinC)
José Maria Leocádio (SERPRO)
Júlio César de Magalhães (FNDE)
Luiz Augusto Barbosa Mozzer (CGU)
Maisa Netto Ludemer (MC)
Marcelo Henrique Rios dos Reis (MT)
Marco Antônio Reis Henriques (RFB)
Marcos José Cândido Euzébio (BACEN)
Ricardo Luiz Chiacchio (MCidades)
Roberto dos Santos Rodrigues (MCT)
Rodrigo Costa dos Santos (ELETROBRÁS)
Sérgio Carreira dos Santos (IPHAN)

## Grupo de Trabalho Meios de Acesso

Mauricio Augusto Coelho (ITI) – Coordenador
Renato da Silveira Martini (ITI) – Coordenador
Carlos Bellone Neto (RFB)
Cleisson Rodrigues (MTur)
Eduardo Viola (MCT)
Eliane Aristóteles Moreira (DATAPREV)
Eliane Pereira dos Santos (MS)
Ellio Alves de O. Soares (CEF)
Geancarlo Noronha Vinha (SERPRO)

Hilton P. Mendes Sobrinho (MS)
Jean Carlo Rodrigues (ITI)
Paloma Nascimento (MT)
Paulo Édison de Souza (MEC)
Rosane dos Santos Lourenço (MT)
Rubem César Macedo (CELEPAR-PR)
Thimoteo Borges (CGU)
Viviane Regina Lemos Bertol (ITI)

### Grupo de Trabalho Organização e Intercâmbio de Informações

Eloi Juniti Yamaoka (SERPRO) – Coordenador
Aline Ramalho Bezerra (MJ)
Ana Lúcia de Medeiros (CORREIOS)
Ângela B. Baylo (CAIXA)
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Brenda Couto de Brito Rocco (AN-CC)
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)
Dalva Clementina Luca (MJ)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (AN-CC)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (AN-CC)
Fernanda Hoffmann Lobato (MP/SLTI)
Geny Conte Pessoa (SERPRO)
Hilda Pimentel (ANCINE)
João Alberto Lima (Senado Federal)
Ligia Leindorf Bartz Kraemer (UFPR)
Luciana Ferreira Pinto da Silva (INEP)
Luciano Seite Nishikawa (CAIXA)
Marcia Helena Gonçalves Rollemberg (MS)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcia Luzia Albertini (MS)
Márcio Imamura (IBGE)
Marcos Augusto Francisco Borges (CPqD)
Margareth da Silva (AN-CC)
Maria de Fátima Porcaro (IPT)
Maria do Socorro Rodrigo de Medeiros (INEP)
Maria Valéria Lins Tenório (ATI-PE)
Neuza Arantes Silva (MAPA)
Paulo César Pereira Soares (FUNARTE)
Paulo Cezar Czarnewski (SERPRO)
Ricardo Torres Lenzi (INEP)
Rosiane Fonseca (ANCINE)
Samuel Batista dos Santos (IPT)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Taciano Tres (BB)
Vicente de Paula Teixeira (CGU)
Virgilio Dantas Lins Filho (ME)
Vivianne Muniz Veras Barrozo (SERPRO)
Wilson Yociteru Yamaji (AGU)

### Grupo de Trabalho Áreas de Integração para Governo Eletrônico

Nazaré Lopes Bretas (MP/SLTI) – COORDENADORA
Adelino Fernando Correia (DATASUS/MS)
Adriano de Medeiros (INCRA)
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)
Antônio Albuquerque (PR)

Carlos Bellone Neto (RFB)
Ceres Albuquerque (ANS)
Cláudio Manoel Cordeiro (SERPRO)
Frederico Duarte Guerra de Macedo (ESPORTES)
Maurício M. Martinez (MEC)
Mônica Lucatelli (DATAPREV)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo de Lima (INCRA)
Rogério Werneck (DIRTI/PR)
Sylmara Campos Pinho Garcia (MP/SLTI)
Wagner Gardusi Guarizo (PR)

**Colaboradores**
Igor de Freitas (MDS)
Felix de Sousa (MDS)

**Subgrupo: Padrões para Intercâmbio de Informações Espaciais**
Roberto Penido Duque Estrada (DSG/CIGEX) – COORDENADOR
Alex Araújo (CAIXA)
Aramis Mota (GSI/PR)
Christian André H. Govastki (MME/SEE)
Dêner Lima F. Martins (ABIN/PR)
Ellio Alves de O. Soares (CAIXA)
Eneias Roberto Shüller (CAIXA)
Fernando Gibotti (CAIXA)
Gerson Barrey (MEC)
Gilberto Ribeiro Queiroz
Gustavo Araújo (MME)
Hisao Fujimoto (MME)
Jorge D. M. Cerqueira (PR/GSI)
Linda Soraya Issmael (DSG/CIGEX)
Lúbia Vinhas (INPE)
Lúcia Helena Luz (CAIXA)
Moema José de Carvalho Augusto (IBGE)
Mosar Rabelo Júnior (MMA)
Silmara Ramos (PR/GSI)
Silvio Carlos Heitor Jorge (CAIXA)
Tálsia Garcia Meira (DIRTI/CC/PR)
Valdevino S. Campos Neto (ANA)
Zandhor F. S. Cavalli Pradi (MS)

**Colaboradores**
Carlos Brasileiro (MDS)
Edmar Morett (MMA)
Enos Josué Rose (MCIDADES)
Rafael M. Sperb (Univali)
Wilfredo Pacheco (ANA)
Werner Leyh (MS)

## Ilustrações
Hezrai de Souza Cruz (MP/SLTI)