

Governo Brasileiro
Comitê Executivo de Governo Eletrônico



e-PING
Padrões de Interoperabilidade
de Governo Eletrônico

Documento de Referência
Minuta Versão 2010
16 de outubro de 2009

SUMÁRIO

APRESENTAÇÃO.....	4
PARTE I – VISÃO GERAL DA E-PING.....	5
1. INTRODUÇÃO.....	6
2. ESCOPO.....	7
2.1. ADESÃO À E-PING.....	7
2.2. FOCO NA INTEROPERABILIDADE.....	8
2.3. ASSUNTOS NÃO ABORDADOS.....	8
3. POLÍTICAS GERAIS.....	9
4. SEGMENTAÇÃO.....	11
4.1. INTERCONEXÃO.....	11
4.2. SEGURANÇA.....	11
4.3. MEIOS DE ACESSO.....	11
4.4. ORGANIZAÇÃO E INTERCÂMBIO DE INFORMAÇÕES.....	12
4.5. ÁREAS DE INTEGRAÇÃO PARA GOVERNO ELETRÔNICO.....	12
5. GESTÃO DA E-PING.....	13
5.1. HISTÓRICO.....	13
5.2. ESTRATÉGIA DE IMPLANTAÇÃO.....	13
5.3. MODELO DE GESTÃO.....	14
5.3.1. Atribuições.....	14
5.3.2. Responsabilidades.....	15
5.4. ATIVIDADES ADICIONAIS.....	16
5.4.1. Seleção e Homologação de Padrões Tecnológicos.....	16
5.4.2. Auditoria de Conformidade.....	17
5.4.3. Criação e Manutenção do Sítio.....	17
5.4.4. Acompanhamento Legal e Institucional.....	18
5.4.5. Divulgação.....	18
5.4.6. Capacitação.....	18
5.5. RELACIONAMENTO COM GOVERNO E SOCIEDADE.....	18
5.5.1. Organizações do Governo Federal – Poder Executivo.....	18
5.5.2. Outras Instâncias de Governo (outros Poderes Federais, Governos Estaduais e Municipais).....	19
5.5.3. Organizações do Setor Privado e do Terceiro Setor.....	19
5.5.4. Cidadão.....	19

PARTE II – ESPECIFICAÇÃO TÉCNICA DOS COMPONENTES DA E-PING.....	20
6. INTERCONEXÃO.....	21
6.1. INTERCONEXÃO: POLÍTICAS TÉCNICAS.....	21
6.2. INTERCONEXÃO: ESPECIFICAÇÕES TÉCNICAS.....	21
6.3. MENSAGEM ELETRÔNICA (E-MAIL).....	24
6.4. VPN.....	24
6.5. REDES PEER-TO-PEER.....	25
7. SEGURANÇA.....	26
7.1. SEGURANÇA: POLÍTICAS TÉCNICAS.....	26
7.2. SEGURANÇA: ESPECIFICAÇÕES TÉCNICAS.....	27
8. MEIOS DE ACESSO.....	33
8.1. MEIOS DE ACESSO: POLÍTICAS TÉCNICAS.....	33
8.2. MEIOS DE ACESSO: ESPECIFICAÇÕES TÉCNICAS PARA ESTAÇÕES DE TRABALHO.....	34
8.3. MEIOS DE ACESSO: ESPECIFICAÇÕES TÉCNICAS PARA TOKENS, CARTÕES INTELIGENTES E CARTÕES EM GERAL.....	38
8.4. MEIOS DE ACESSO: ESPECIFICAÇÕES TÉCNICAS PARA MOBILIDADE.....	46
8.5. MEIOS DE ACESSO: ESPECIFICAÇÕES TÉCNICAS PARA TV DIGITAL.....	47
9. ORGANIZAÇÃO E INTERCÂMBIO DE INFORMAÇÕES.....	50
9.1. ORGANIZAÇÃO E INTERCÂMBIO DE INFORMAÇÕES: POLÍTICAS TÉCNICAS.....	50
9.2. ORGANIZAÇÃO E INTERCÂMBIO DE INFORMAÇÕES: ESPECIFICAÇÕES TÉCNICAS.....	50
9.3. NOTAS SOBRE XML E MIDDLEWARE.....	51
9.4. NOTA SOBRE O USO DE UML.....	51
9.5. NOTA SOBRE A LAG.....	51
10. ÁREAS DE INTEGRAÇÃO PARA GOVERNO ELETRÔNICO.....	52
10.1. ÁREAS DE INTEGRAÇÃO PARA GOVERNO ELETRÔNICO: POLÍTICAS TÉCNICAS.....	52
10.2. CATÁLOGO DE INTEROPERABILIDADE.....	52
10.3. MODELOS PARA DOCUMENTAÇÃO DE WEB SERVICES E OUTRAS MODALIDADES DE TROCAS DE DADOS.....	53
10.4. ÁREAS DE INTEGRAÇÃO PARA GOVERNO ELETRÔNICO: NOTA EXPLICATIVA SOBRE OS CATÁLOGOS PADRÃO DE DADOS E XML SCHEMAS.....	53
10.4.1. <i>Considerações Iniciais</i>	53
10.4.2. <i>Propriedade e Responsabilidade</i>	53
10.4.3. <i>Mecanismos de Gestão do Catálogo de XML Schemas</i>	53
10.5. ÁREAS DE INTEGRAÇÃO PARA GOVERNO ELETRÔNICO: ESPECIFICAÇÕES TÉCNICAS.....	54
11. GLOSSÁRIO DE SIGLAS E TERMOS TÉCNICOS.....	57
12. INTEGRANTES.....	63

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.

O conteúdo deste documento é de domínio público, não havendo restrições quanto à sua reprodução nem quanto à utilização das informações nele contidas. A reprodução pode ser realizada em qualquer mídia, sem necessidade de autorização específica. O uso inadequado do material com fins depreciativos será considerado objeto de tratamento jurídico apropriado por parte do governo brasileiro, detentor dos direitos autorais.

É proibida a utilização do todo ou de parte do conteúdo deste documento com fins comerciais.

Parte I – Visão Geral da e-PING

1. Introdução

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

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

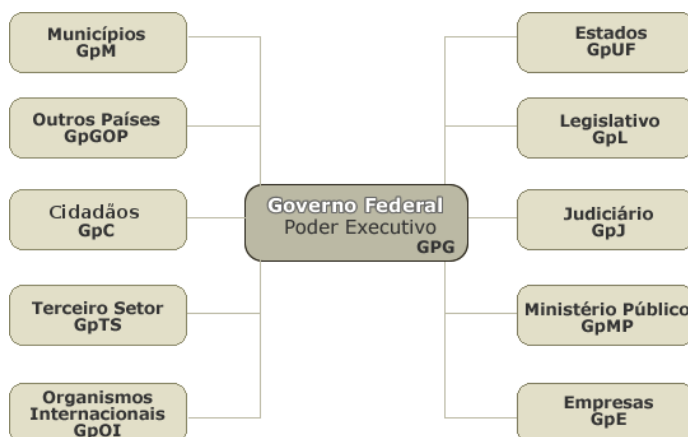


Figura 1 – Relacionamentos do governo federal.

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 elaborado pelo próprio órgão, que considerará a situação da instituição em relação às condições para se adequar às especificações e recomendações da e-PING.

A aferição da situação do órgão quanto ao uso efetivo dos padrões se dará com base no Modelo de Maturidade de Adoção da e-PING – M-PING, atualmente em construção.

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.

Informações sobre diretrizes e políticas relativas à apresentação e acessibilidade dos portais e sítios de governo eletrônico estão disponíveis no portal do governo eletrônico brasileiro (<http://www.governoeletronico.gov.br>).

3. Políticas Gerais

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

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.

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

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>).

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

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.

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

Dimensão técnica:

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.

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.

Dimensão semântica:

Desenvolvimento e manutenção de recursos de organização da informação visando contribuir para a simplificação do acesso a documentos e serviços pelo cidadão brasileiro, tais como vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações.

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

Dimensão organizacional:

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

Promoção da colaboração entre organizações, por meio da integração entre objetivos institucionais e processos de negócio de organizações com estruturas internas e processos internos diferentes.

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

4. Segmentação

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

Os cinco segmentos – “Interconexão”, “Segurança”, “Meios de Acesso”, “Organização e Intercâmbio de Informações” e “Áreas de Integração para Governo Eletrônico” – foram subdivididos em **componentes**, para os quais foram estabelecidas as políticas e as especificações técnicas a serem adotadas pelo governo federal. A seguir 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:

- Mensageria;
- Infraestrutura de Rede;
- Serviços de Rede.

4.2. Segurança

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

- Segurança na Comunicação de Dados;
- Segurança de Correio Eletrônico;
- Criptografia;
- Desenvolvimento de Sistemas;
- Serviços de Rede;
- Redes sem Fio;
- Tratamento e Resposta a Incidentes de Segurança da Informação.

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 as políticas e as especificações para estações de trabalho, cartões inteligentes (*smart-cards*), *tokens* e outros cartões, televisão digital e mobilidade. Em versões futuras, serão tratados outros dispositivos. É formado por quatro subgrupos contemplando 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;

- Programação Estendida (Plugins).

Cartões Inteligentes / Tokens / Outros:

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

Mobilidade:

- Definição;
- Protocolo de transmissão;
- Navegador;
- Padrão de Hipertexto;
- Programação estendida;
- Mensageria;
- Arquivos de Vídeo e Som;
- Arquivos de Imagem;
- Arquivos de Escritório;
- Leitor PDF.

TV Digital:

- Definição;
- Normas da ABNT;
- Especificações de Padrões.

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;
- Vocabulário Controlado do Governo Eletrônico (VCGE);
- Padrão de Metadados do Governo (e-PMG).

4.5. Áreas de Integração para Governo Eletrônico

O segmento estabelece a utilização ou construção de especificações técnicas baseadas no padrão XML para sustentar o intercâmbio de informações em áreas transversais da atuação governamental.

As ferramentas que apoiam a atuação do segmento são:

- Catálogo Padrão de Dados (CPD);
- Catálogo XML *Schemas*;
- Catálogo de Serviços Interoperáveis (*Web Services*).

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 Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (ABEP).

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 minuta da versão 2010.

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 infraestrutura gerencial necessária para sua correta utilização e garantindo sua atualização, considerando: as prioridades e metas de governo, as necessidades da sociedade e a disponibilidade de novas tecnologias maduras e suportadas pelo mercado de TIC;
- 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 infraestrutura 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);
 - Vocabulário Controlado do Governo Eletrônico (VCGE);
 - 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.

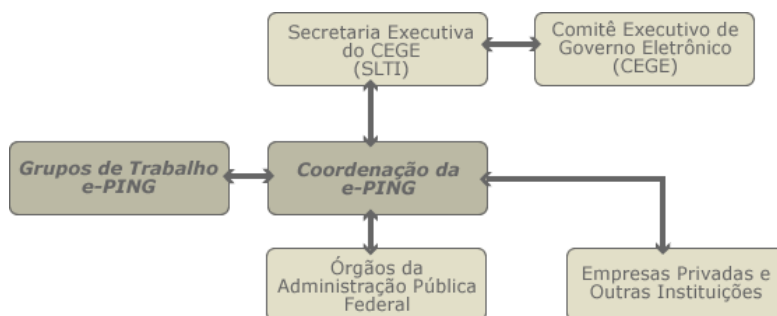


Figura 2 – Administração da e-PING.

A SLTI/MP, por meio 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 específicas, 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 poderá ser enquadrado numa das situações acima, assim que o processo de avaliação estiver concluído;
- **Estudo Futuro (F):** componente ainda não avaliado e que será objeto de estudo posterior.

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 indispensável a avaliação de características físicas de determinados componentes (Cartões Inteligentes, por exemplo) até outros em que sejam requeridos estudos 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. Para tal, foi constituído, por intermédio da Portaria nº 8, de 31 de outubro de 2008, da SLTI/MP, Grupo de Trabalho para estudar, analisar e propor modelo de auditoria quanto à aderência aos padrões da e-PING. Essa proposta também contemplará o modelo de maturidade da e-PING (M-PING).

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 infraestrutura de TIC da organização à arquitetura e-PING;

- Assegurar que sejam de domínio das equipes da instituição, as habilidades para definir e utilizar as especificações requeridas para interoperabilidade, fornecendo suporte de treinamento quando necessário;
- Estabelecer ponto de contato nas instituições, para intercâmbio de informações e de necessidades com a Coordenação da e-PING;
- Alocar e suprir recursos para dar suporte aos seus processos de adequação à e-PING;
- Aproveitar a oportunidade para racionalizar processos (como resultado do aumento da interoperabilidade) de maneira a melhorar a qualidade e reduzir custos de provimento dos serviços de e-gov.

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

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

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

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

5.5.3. 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 equidade 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 preveem 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 obedecer à política de nomeação de domínios do governo federal, estabelecida na Resolução nº 7, que pode ser visualizada no endereço eletrônico

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

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

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

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

6.1.7. A tecnologia de *Web Services* é recomendada como solução de interoperabilidade da e-PING. Recomenda-se a utilização do protocolo *Simple Object Access Protocol* (SOAP) para interconexão em arquiteturas descentralizadas e/ou distribuídas para implementação de serviços em sistemas de qualquer porte. Alternativamente, para serviços web de pequeno porte, considera-se possível a utilização do RESTful, que utiliza o protocolo HTTP.

6.2. Interconexão: Especificações Técnicas

Tabela 1 – Especificações para Interconexão – Mensageria²

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Endereços de caixa postal eletrônica	As regras para definição dos nomes das caixas postais de correio eletrônico deverão seguir ao estabelecido no documento “Caixas Postais Individuais-Funcionais no governo federal”, disponível no endereço eletrônico http://www.e.gov.br/correios/cp_individ.htm	A	

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

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

Componente	Especificação	SIT	Observações
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 3676; RFC 2047; RFC 2231 (atualização das RFCs 2045, 2047 e 2183); RFC 2183; RFC 4288; RFC 4289; RFC 3023 e RFC 2049.	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. RFC correlacionada: RFC 1939 (atualizada pela RFC 1957 e RFC 2449).	T	
	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 2342; RFC 2910 (atualizada pela RFC 3510); RFC 2971; RFC 3501; RFC 3502 e RFC 3503.	R	
Mensageria em Tempo Real	O modelo e requisitos para <i>Instant Messaging and Presence Protocol</i> (IMPP) são definidos pela RFC 2778 e RFC 2779.	T	
	O modelo e requisitos para <i>Extensible Messaging and Presence Protocol</i> (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	

Tabela 2 – Especificações para Interconexão – Infraestrutura de Rede

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Transporte	TCP (RFC 793)	A	
	UDP (RFC 768) quando necessário, sujeito às limitações de segurança.	A	
Intercomunicação LAN/WAN	IPv4 (RFC 791)	A	
	IPv6 (RFC 2460)	E	
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.	A	
Qualidade de serviço	Adoção de uma arquitetura para serviços diferenciados pelo uso do Diffserv (RFC 2475).	E	

Componente	Especificação	SIT	Observações
Rede metropolitana sem fio	IEEE 802.16, em conformidade com as determinações do <i>WiMax Forum</i> (http://www.wimaxforum.org) e com as normas da Anatel (http://www.anatel.gov.br).	E	
Rede local sem fio	IEEE 802.11 b/g, em conformidade com as determinações do <i>Wi-Fi Alliance</i> (http://www.wi-fi.org) e com as normas da Anatel (http://www.anatel.gov.br).	R	
Rede de acesso por cabeamento elétrico	<i>Power Line Communication</i> (PLC), segundo as normas da Anatel (http://www.anatel.gov.br) e da Aneel (http://www.aneel.gov.br).	F	

Tabela 3 – Especificações para Interconexão – Serviços de Rede

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1 (RFC 2616).	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	
Diretório	LDAP v3 deverá ser utilizado para acesso geral ao diretório, conforme RFC 4510.	A	
Sincronismo de tempo	RFC 1305 IETF - <i>Network Time Protocol</i> - NTP version 3.0. RFC 4330 IETF - <i>Simple Network Time Protocol</i> - SNTP version 4.0.	R	
Serviços de Nomeação de Domínio	O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035. Por sua vez, as diretivas de nomeação de domínio do governo brasileiro são encontradas na Resolução N° 7 do Comitê Executivo do Governo Eletrônico, no endereço eletrônico https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm Além dessas diretivas, por decisão do Comitê Gestor da Internet no Brasil, a nomeação de domínios obedece às orientações do Ministério do Planejamento, Orçamento e Gestão, a quem compete gerenciar os domínios .GOV.BR. As particularidades de outros níveis de governo, como por exemplo, os domínios dos governos das Unidades da Federação, que incluem a sigla da UF na composição dos endereços, são abordadas no endereço eletrônico http://registro.br/faq/faq1.html#12 .	A	
Protocolos de sinalização	Uso do Protocolo de Inicialização de Sessão (SIP), definido pela RFC 3261, como protocolo de controle	R	

Componente	Especificação	SIT	Observações
	na camada de aplicação (sinalização) para criar, modificar e terminar sessões com um ou mais participantes.		
Protocolos de gerenciamento de rede	Uso do protocolo SNMP, definido pelas RFCs 3411 e 3418, como protocolo de gerência de rede.	T	Versão 2
		R	Versão 3
Protocolo de troca de informações estruturadas em plataforma descentralizada e/ou distribuída	SOAP v1.2, como definido pelo W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/	A	
	Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/		
Protocolo de análise de tráfego de rede	IPFix	F	

6.3. Mensagem Eletrônica (E-mail)

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

Transporte de Mensagem Eletrônica

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

Acesso à caixa postal

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

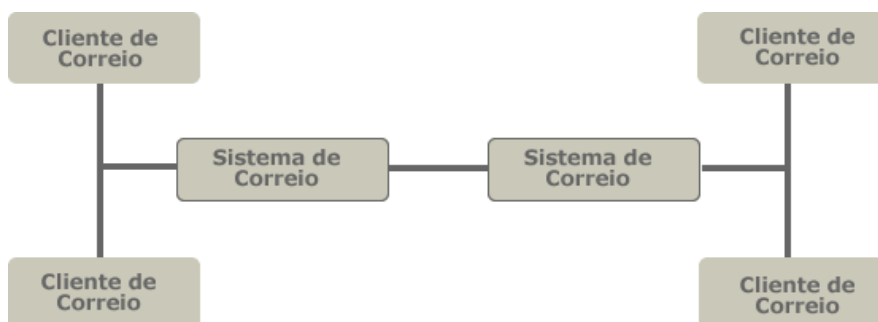


Figura 3 – Interfaces entre sistemas e clientes de Correio.

6.4. VPN

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

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

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

Os dispositivos responsáveis pelo gerenciamento da VPN devem ser capazes de garantir

privacidade, integridade e autenticidade dos dados.

As especificações sobre VPN estão apresentadas no segmento de segurança.

6.5. Redes *peer-to-peer*

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

Embora sistemas P2P possam contribuir para compartilhamento de recursos e colaboração em larga escala, com controle descentralizado e baixo acoplamento, ainda estão suscetíveis a diversos problemas de segurança, 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, disponibilidade e autenticidade.

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

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

7.1.4. Os requisitos de segurança da informação, dos serviços e de infraestrutura devem ser identificados e tratados de acordo com a classificação da informação, níveis de serviço definidos e 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 materiais, 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, mantendo-se grau de sigilo compatível.

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 as normas NBR ISO/IEC 27002:2005 – código de prática para a gestão da segurança da informação; NBR ISO/IEC 27001:2006 – sistemas de gestão de segurança da informação; NBR 15999-1:2007 e 15999-2:2008 – gestão de continuidade de negócios; NBR ISO/IEC 27005:2008 – gestão de riscos de segurança da informação; Instrução Normativa nº 01/2000, Norma Complementar nº 02/2009, 04/2009 e 05/2009.

7.2. Segurança: Especificações Técnicas

Tabela 4 – Especificações para Segurança – Comunicação de dados

Componente	Especificação	SIT	Observações
	<p>A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro</p>		
Transferência de dados em redes inseguras pelos protocolos HTTP, LDAP, IMAP, POP3, Telnet.	<p>TLS – <i>Transport Layer Security</i>, RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.</p> <p>HTTP sobre TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Podendo implementar os seguintes algoritmos criptográficos:</p> <ul style="list-style-type: none"> - Algoritmos para troca de chaves de sessão, durante o <i>handshake</i>: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - Algoritmos para definição de chave de cifração: RC4, IDEA, 3DES e AES; - Algoritmos que implementam a função de <i>hash</i> para definição do MAC: SHA-256 ou SHA-512. - Tipo de Certificado Digital - X.509 v3 - ICP-Brasil, http://www.iti.gov.br <p>SASL - <i>Simple Authentication and Security Layer</i>, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt).</p>	R	
Segurança de redes IPv4	<p>IPSec <i>Authentication Header</i> RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) e RFC 4835 (http://www.ietf.org/rfc/rfc4835.txt) para autenticação de cabeçalho do IP.</p> <p>IKE – <i>Internet Key Exchange</i>, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento.</p> <p>ESP – <i>Encapsulating Security Payload</i>, RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) Requisito para VPN – Virtual Private Network.</p>	A	
Segurança de redes IPv4 para protocolos de aplicação	<p>O S/MIME v3 ,RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.</p>	A	

Componente	Especificação	SIT	Observações
Segurança de redes IPv6 na camada de rede	O IPv6 definido na RFC 2460 (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 (<i>Authentication Header</i>) RFC 4302 (http://www.ietf.org/rfc/rfc4302.txt) ou autenticação IP, e a segurança do encapsulamento IP, ESP (<i>Encrypted Security Payload</i>) RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt).	R	

Tabela 5 – Especificações para Segurança – Correio Eletrônico

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Acesso a caixas postais	O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado, considerando as facilidades de segurança nativas do cliente. Quando não for possível utilizar o cliente específico ou for necessário acessar a caixa postal através de redes não seguras (por exemplo: Internet) deve-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), que trata da utilização do TLS com IMAP, POP3 e ACAP.	A	
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), RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt) e RFC 3852 (http://www.ietf.org/rfc/rfc3852.txt).	A	
Transporte de e-mail	Utilizar SPF (<i>Sender Policy Framework</i>) nos termos da RFC 4408 (http://www.ietf.org/rfc/rfc4408.txt).	R	
Assinatura	Utilizar certificado padrão ICP-Brasil para assinatura de e-mail, quando exigido. Em conformidade com o disposto na Medida Provisória nº 2.200-2, de 24/08/2001 e Decreto nº 3.996 de 31/10/2001.	A	Ver Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil

Tabela 6 – Especificações para Segurança – Criptografia

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Algoritmo de cifração	3DES ou AES	R	
Algoritmo para assinatura/hasing	SHA-256 ou SHA-512	R	Os sistemas devem ter suporte para o algoritmo de <i>hash</i> MD5 com RSA, para garantir compatibilidade com implementações anteriores.
Algoritmos para assinatura/hasing	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	A	
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (rfc 5480 – http://www.ietf.org/rfc/rfc5480.txt).	A	ECDSA, para assinaturas digitais, e ECIES para cifração e transporte seguro de chaves criptográficas.
	ECIES 256 e ECIES 512 (Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil).		Consultar errata para a RFC 5480 em http://rfc-editor.org/errata_search.php?rfc=5480 .
	ECMQV e ECDH, ambos para acordo de chaves, conforme RFC 3278. (http://www.ietf.org/rfc/rfc3278.txt).	E	

Componente	Especificação	SIT	Observações
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3; FIPS 140-1 e FIPS 140-2.	R	Ver Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil).

Tabela 7 – Especificações para Segurança – Desenvolvimento de Sistemas

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Assinaturas XML	Sintaxe e Processamento de assinatura XML (XMLsig) conforme definido pelo W3C http://www.w3.org/TR/xmlsig-core/	A	
Cifração XML	Sintaxe e Processamento de Cifração XML (XMLenc) conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/	R	
Assinatura e cifração XML	Transformação de decifração para assinatura XML conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt	R	
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XML – <i>Key Management Specification (XKMS 2.0)</i> (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). 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).	R	O componente anterior (SAML) poderá se juntar a este componente após estudos.
Navegadores	Somente utilizar testemunhas de conexão de caráter permanente (<i>cookies</i>) com a concordância do usuário. Resolução n. 7 do Comitê Executivo do Governo Eletrônico (Capítulo II, Art.7º).	A	

Tabela 8 – Especificações para Segurança – Serviços de Rede

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Diretório	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. LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt). LDAP v3 extensão para TLS RFC2830 (http://www.ietf.org/rfc/rfc2830.txt).	R	
DNSSEC	Resolução no. 7 de 29/07/2002 – Comitê Executivo do Governo Eletrônico Práticas de Segurança para Administradores de Redes Internet Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – CERT.BR http://www.cert.br/docs/seg-adm-redes/seg-adm-chklist.pdf Versão 1.2, 16 de maio de 2003.	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	E	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	
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 2030 IETF- <i>Simple Network Time Protocol - SNTP version 4.0</i> (http://www.ietf.org/rfc/rfc2030.txt).	E	
Carimbo de tempo	RFC 3628 TSAs - <i>Policy Requirements for Time-Stamping Authorities</i> (http://www.ietf.org/rfc/rfc3628.txt), <i>Time-Stamp Protocol</i> , RFC 3161 ETSI TS101861 (<i>Time-Stamping Profile</i>) (http://www.ietf.org/rfc/rfc3161.txt).	R	O serviço de carimbo de tempo deverá estar de acordo com a Resolução nº 58, de 28/11/2008 e demais normas da ICP-Brasil.

Tabela 9 – Especificações para Segurança – Redes Sem Fio

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
MAN ³ sem fio 802.16-2004 ⁴ 802.16.2-2004 ⁵ 802.16e ⁶ e 802.16f ⁷	Utilizar PKM-EAP (<i>Privacy Key Management - Extensible Authentication Protocol</i>) com: <ul style="list-style-type: none"> • EAP – TLS ou TTLS; • AES⁸ (Advanced Encryption Standard). 	E	
LAN sem fio 802.11	Utilizar a especificação WPA2 (<i>Wi-Fi Protect Access</i>).	R	

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

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Preservação de registros	<i>Guidelines for Evidence Collection and Archiving</i> , RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt).	R	
Tratamento e resposta a incidentes em redes computacionais	<i>Expectations for Computer Security Incident Response</i> , RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt). Criação de equipes de tratamento e resposta a incidentes em redes computacionais conforme Norma Complementar nº 05/09 (http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf).	R	
Informática Forense	<i>Guide to Integrating Forensic Techniques into Incident Response – NIST - Special Publication 800-86</i> – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	A	

³ O 802.16 é definido pelo IEEE como uma interface tecnológica para redes de acesso sem fio metropolitanas ou WMAN (*Wireless Metropolitan Access Network*).

⁴ <http://standards.ieee.org/getieee802/download/802.16-2004.pdf>.

⁵ <http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf>.

⁶ <http://standards.ieee.org/getieee802/download/802.16e-2005.pdf>.

⁷ <http://standards.ieee.org/getieee802/download/802.16f-2005.pdf>.

⁸ <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;
 - Cartões Inteligentes, *Tokens* e outros Cartões;
 - Mobilidade;
 - TV Digital.

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)⁹.

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 versões mínimas de navegadores que suportam as funcionalidades requeridas pelo serviço

⁹ 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.

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 *web* (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/Resolucao/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 11.

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

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

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

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Navegadores (<i>browsers</i>)	Devem ser aderentes aos padrões W3C e aos itens Adoção de navegadores e Adoção Preferencial de Padrões Abertos em Políticas Gerais.	R	
Conjunto de caracteres e alfabetos	UNICODE <i>standard</i> 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 ⁽¹⁰⁾ .	A	
	XHTML versões 1.0 ou 1.1 (.xhtml), gerado conforme especificações do W3C ⁽¹¹⁾ .	A	
	XML versões 1.0 ou 1.1 (.xml), gerado conforme especificações do W3C ⁽¹²⁾ .	A	
	SHTML (.shtml).	R	
	MHTML (.mhtml ou .mht) ⁽¹³⁾ .	T	
Arquivos do tipo documento	XML versões 1.0 ou 1.1 (.xml), ou com formatação (opcional) XSL (.xsl), gerado conforme especificações do W3C ⁽¹⁴⁾ .	R	
	Open Document (.odt), gerado conforme especificações do padrão ISO/IEC 26300 ⁽¹⁵⁾ .	A	
	Rich Text Format (.rtf).	T	
	PDF (.pdf) gerado em formato até versão 1.3.	T	
	PDF versão aberta PDF/A ⁽¹⁶⁾ .	R	

¹⁰ HTML 4.01 Specification - W3C Recommendation 24 December 1999. Disponível em: <http://www.w3.org/TR/html4/>.

¹¹ 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/>.

¹² 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/>.

¹³ Formato de empacotamento de arquivos web da Microsoft (*Mime Encapsulation of Aggregate HTML Documents*).

¹⁴ Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001. Disponível em: <http://www.w3.org/TR/xsl/>.

¹⁵ Open Document Format for Office Applications (OpenDocument) v1.0 - padrão ISO/IEC 26300. Disponível em: <http://www.iso.org/>.

¹⁶ 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/>.

Componente	Especificação	SIT	Observações
	Texto puro (.txt).	A	
	HTML versão 4.01 (.html ou .htm), gerado conforme especificações do W3C.	R	
Arquivos do tipo planilha	Open Document (.ods), gerado conforme especificações do padrão ABNT NBR ISO/IEC 26300.	A	
Arquivos do tipo apresentação	Open Document (.odp), gerado conforme especificações do padrão ABNT NBR ISO/IEC 26300.	A	
	HTML (.html ou .htm), gerado conforme especificações do W3C.	R	
Arquivos do tipo “banco de dados” para estações de trabalho	XML versões 1.0 ou 1.1 (.xml)	R	Nas opções texto plano (txt) e csv, deve ser incluído obrigatoriamente o leiaute dos campos, de forma a possibilitar seu tratamento.
	MySQL Database (.myd, .myi), gerados nos formatos do MySQL, versão 4.0 ou superior.	R	
	Texto Puro (.txt)	A	
	Texto Puro (.csv) – comma-separated values	A	
	Arquivo do Base (.odb), gerado no formato do BrOffice.org (ou OpenOffice.org) versão 2.0 ou posterior.	R	
Intercâmbio de informações gráficas e imagens estáticas	PNG (.png), gerado conforme especificações do W3C ⁽¹⁷⁾ – ISO/IEC 15948:2003 (E).	A	
	TIFF (.tif) ⁽¹⁸⁾ .	R	
	SVG (.svg), gerado conforme especificações do W3C ⁽¹⁹⁾ .	R	
	JPEG File Interchange Format (.jpeg, .jpg ou .jif) ⁽²⁰⁾ .	R	
	Open Document (.odg), gerado conforme especificações do padrão ABNT NBR ISO/IEC 26300.	A	
	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 ⁽²¹⁾ .	T	
Gráficos vetoriais	SVG (.svg), gerado conforme especificações do W3C.	R	

¹⁷ 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.

¹⁸ Tagged Image File Format (Adobe Systems).

¹⁹ 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.

²⁰ JPEG File Interchange Format (version 1.02) 1 September 1992. Disponível em: <http://www.jpeg.org/public/jfif.pdf>. Acesso em: 7 dez. 2005.

²¹ Graphics Interchange Format (CompuServe/America Online, Inc.).

Componente	Especificação	SIT	Observações
	Open Document (.odg), gerado conforme especificações do padrão ABNT NBR ISO/IEC 26300.	R	
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) ²²	R	
	MIDI (.mid) ²³	R	
	Áudio Ogg Vorbis I (.ogg) ²⁴	R	
	Audio-Video Interleaved (.avi), com codificação Xvid.	R	
	Audio-Video Interleaved (.avi), com codificação divX.	T	
	Áudio MPEG-1, Audio Layer 3 (.mp3) ²⁵	T	
	WAVE (.wav)	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 2.0 ou superior ²⁶ .	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.

²² ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.

²³ 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.

²⁴ Xiph.Org Foundation. Especificação disponível em: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.

²⁵ 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.

²⁶ *Geography Markup Language*. Especificações disponíveis em: <http://www.opengeospatial.org/standards/gml>.

Componente	Especificação	SIT	Observações
	ShapeFile ²⁷ .	A	Indicado para estruturas vetoriais limitadas a linhas, pontos e polígonos, cujos atributos textuais não ultrapassem 256 caracteres. Pode armazenar também as dimensões M e Z.
	GeoTIFF ²⁸ .	A	Indicado para estruturas matriciais limitadas a matrizes de pixel.
	SFS.	E	SFS (<i>Simple Features Interface Standard</i>) é um padrão OGC (http://www.opengeospatial.org/standards/sfa) que define a forma como as aplicações irão armazenar (criar, atualizar e excluir) e acessar feições geográficas em sistemas gerenciadores de banco de dados objetos-relacionais. OpenGIS <i>Simple Features</i> (feições simples) são feições espaciais descritas usando elementos de dados como pontos, linhas e polígonos.
Programação Estendida (Plugins)	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*,

²⁷ ESRI Shapefile Technical Description. Disponível em: <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>.

²⁸ GeoTIFF Format Specification. Disponível em: <http://remotesensing.org/geotiff/geotiff.html>.

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-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 Development 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 12 – Especificações para Meios de Acesso – Cartões Inteligentes, Tokens e Cartões em Geral

Componente	Especificação	SIT	Aplicável a	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo 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 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 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 Parte 2: Funções, mensagens (comandos e respostas), elementos e estruturas de dados.	F	Todos.	
	Sistemas de cartão de identificação BS EN 1546-3 – <i>Inter-sector electronic purse</i> - Parte 3: Elementos e intercâmbio de dados Sistemas de cartão de identificação BS EN 1546-4 – <i>Inter-sector electronic purse</i> - Parte 4: Objetos de dados.	F	Todos.	A atual edição foi publicada em julho de 1999. 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. 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 <i>Registered Application Provider Identifiers</i> (RDIs) (Identificadores de Provedores de Aplicações Registradas) que foi publicada em dezembro de 1996.
	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 <i>Structured Card Query Language</i> (SCQL);	R		
	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 { <i>Vicinity Integrated Circuit(s) Cards</i> (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 frequência de rádio.	R	Cartões de circuito integrado de proximidade.	Esta parte define a interface de frequência 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 { <i>Close Coupling Integrated Circuit(s) Cards</i> (CICC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)}	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 { <i>Vicinity Integrated Circuit(s) Cards</i> (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. 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 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. Parte 2: Processo de transação; ISO 10202-6 Parte 6: Verificação do portador do cartão.	R	Todos.	
	Cartões de identificação ISO/IEC 10536-4 cartões de circuito(s) integrado(s) sem contato { <i>Close Coupling Integrated Circuit(s) Cards</i> (CCIC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)}. 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; localidade e <i>layout</i> de contatos.	Características físicas Cartões de identificação 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 ISO/IEC 7811 , partes 2, 4 e 5: definem as propriedades, posicionamento e codificação (<i>coding</i>) da banda magnética do cartão.	R	Todos os cartões com banda magnética.	
	Cartão de memória ótica ISO/IEC 11693 e 11694.	F	Cartões óticos.	Cartões que suportam o armazenamento de muitos <i>megabytes</i> .
	Cartões de identificação ISO/IEC 7816-1 Parte 1: Características físicas Cartões de identificação ISO/IEC 15693-1 - Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade - Parte 1: Características físicas. Cartões de identificação ISO/IEC 7816-2 – Cartões de circuito(s) integrado(s) com contatos 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. Conforme escolha do GT da ICP-Brasil e Manual de Conduitas Técnicas do ITI – Volume I.
	Cartões de identificação 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 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 ISO/IEC 10536-1 – Cartões de circuito(s) integrado(s) sem contato Parte 1: Características físicas; ISO/IEC 10536-2 Parte 2: Dimensões e localização das áreas de acoplamento.	F	Cartões de circuito(s) integrado(s) de acoplamento forte.	
	Identificadores táteis. 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	<p>Cartões de identificação ISO/IEC 7816-8 – Cartões de circuito(s) integrado(s) com contatos.</p> <p>Parte 8: Comandos de segurança intersetoriais ISO/IEC 7816-9</p> <p>Parte 9: Comandos adicionais intersetoriais e atributos de Segurança.</p> <p>Cartões de identificação ISO/IEC 7816-11 – Cartões de circuito(s) integrado(s) com contatos - Parte 11: Verificação pessoal através de métodos biométricos.</p> <p>Cartões de identificação ISO/IEC 7816-15 – Cartões de circuito(s) integrado(s) com contatos - Parte 15: Informação de dispositivo Criptográfico em cartões CI.</p>	A	Cartões de circuito(s) integrado(s) com contatos.	
	<p>Cartões de transação financeira ISO 10202</p> <p>Arquitetura de segurança de sistemas de transação financeira utilizando cartões de circuito integrado</p> <p>Parte 1: Ciclo de vida do cartão;</p> <p>Parte 2: Princípios e apanhado geral;</p> <p>Parte 3: Relacionamentos de chave criptográfica;</p> <p>Parte 4: Módulos seguros de aplicação;</p> <p>Parte 5: Utilização de algoritmos;</p> <p>Parte 6: Verificação do portador do cartão;</p> <p>Parte 7: Gerenciamento de chave.</p>	F	Todos.	

Componente	Especificação	SIT	Aplicável a	Observações
Infraestrutura do terminal	Sistemas de cartões de identificação EN 1332-3:1999 – Interface Homem-máquina – Parte 3: Teclados.	R	Todos.	
	Padrões PC/SC. Padrões do Consórcio Grupo de Trabalho PC/SC Especificação de Interoperabilidade para ICCs e Sistemas de Computador Pessoal Parte 1. Introdução e Visão Geral da Arquitetura Parte 2. Requisitos de Interface para Cartões Compatíveis com CI e Dispositivos de Interface Parte 3. Requisitos para Dispositivos de Interface Conectados a PC Parte 4. Considerações do projeto IFD e Informação de Referência do Projeto Parte 5. Definição do Gerenciador de Recursos ICC Parte 6. Definição do Interface do Fornecedor de Serviço ICC Parte 7. Considerações do Projeto de Domínio / Desenvolvedor da Aplicação 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.

8.4. Meios de Acesso: Especificações Técnicas para Mobilidade

O número de aparelhos de telefonia móvel já ultrapassou a quantidade de telefonia fixa, tornando-se assim um amplo canal de comunicação com o cidadão. Além disso, a oferta de computadores pessoais com recursos de mobilidade, a preços mais acessíveis ao cidadão, está crescente a cada dia, motivada por incentivos governamentais e redução do custo de produção. Assim, torna-se um grande desafio para o governo possibilitar acesso para a sociedade aos produtos e serviços do governo eletrônico, a partir de dispositivos móveis, em geral portáteis, como *notebooks*, celulares, *smartphones* e similares, almejando o aumento da inclusão digital via mobilidade.

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

Tabela 13 – Especificações para Meios de Acesso – Mobilidade

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Protocolo de Transmissão	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Navegador	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Padrão Hipertexto	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Programação Estendida	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Mensageria	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Arquivos de Vídeo e Som	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Arquivos de Imagem	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Arquivos de Escritório	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	
Leitor PDF	Deve ser aderente aos padrões W3C – <i>Mobile Best Practices</i> 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	R	

8.5. Meios de Acesso: Especificações Técnicas para TV Digital

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

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

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

Para atender as questões técnicas, a Associação Brasileira de Normas Técnicas – ABNT, elaborou diversas normas, conforme listadas na tabela abaixo:

Tabela 14 – Normas ABNT sobre TV Digital

Referência	Título
ABNT NBR15601	Televisão digital terrestre – Sistema de transmissão.
ABNT NBR 15602-1	Televisão digital terrestre – Codificação de vídeo, áudio e multiplexação – Parte 1: Codificação de vídeo.
ABNT NBR 15602-2	Televisão digital terrestre – Codificação de vídeo, áudio e multiplexação – Parte 2: Codificação de áudio.
ABNT NBR 15602-3	Televisão digital terrestre – Codificação de vídeo, áudio e multiplexação – Parte 3: Sistema de Multiplexação de sinais.
ABNT NBR 15603-1	Televisão digital terrestre – Multiplexação e serviços de informação (SI) – Parte 1: Serviços de informação do sistema de radiodifusão.
ABNT NBR 15603-2	Televisão digital terrestre – Multiplexação e serviços de informação (SI) – Parte 2: Sintaxes e definições da informação básica de SI.
ABNT NBR 15603-3	Televisão digital terrestre – Multiplexação e serviços de informação (SI) – Parte 3: Sintaxe e definição da informação estendida do SI.
ABNT NBR 15604	Televisão digital terrestre – Receptores.
ABNT NBR 15605	Televisão digital terrestre – Tópicos de segurança.
ABNT NBR 15606-1	Televisão digital terrestre – Codificação de dados e especificações de transmissão para radiodifusão digital – Parte 1: Codificação de dados.
ABNT NBR 15606-2	Televisão digital terrestre – Codificação de dados e especificações de transmissão para radiodifusão digital – Parte 2: Ginga-NCL para receptores fixos e móveis – Linguagem de aplicação XML para codificação de aplicações.
ABNT NBR 15606-3	Televisão digital terrestre – Codificação de dados e especificações de transmissão para radiodifusão digital – Parte 3: Especificação de transmissão de dados.
ABNT NBR 15606-5	Televisão digital terrestre – Codificação de dados e especificações de transmissão para radiodifusão digital – Parte 5: Ginga-NCL para receptores portáteis – Linguagem de aplicação XML para codificação de aplicações.
ABNT NBR 15607-1	Televisão digital terrestre – Canal de interatividade – Parte 1: Protocolos, interfaces físicas e interfaces de software.
ABNT NBR 15608	Televisão digital terrestre – Guia de elaboração.
ABNT NBR 15609	Televisão digital terrestre – Suíte de testes (em elaboração).
ABNT NBR 15610	Televisão digital terrestre – Ensaios para receptores (em elaboração).

Tabela 15 – Especificações para Meios de Acesso – TV Digital

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Middleware		F	
Codificação de áudio		F	
Codificação de vídeo		F	
Camada de Transporte		F	
Transmissão		F	

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 16 – Especificações para Organização e Intercâmbio de Informações

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Linguagem para intercâmbio de dados	XML (<i>Extensible Markup Language</i>) como definido pelo W3C http://www.w3.org/XML	A	
Transformação de dados	XSL (<i>Extensible Stylesheet Language</i>) como definido pelo W3C http://www.w3.org/TR/xsl XSL <i>Transformation</i> (XSLT) como definido pelo W3C http://www.w3.org/TR/xslt	A	
Definição dos dados para intercâmbio	XML <i>Schema</i> como definido pelo W3C: - XML <i>Schema Part 0: Primer</i> http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ - XML <i>Schema Part 1: Structures</i> http://www.w3.org/TR/xmlschema-1/structures - XML <i>Schema Part 2: Datatypes</i> http://www.w3.org/TR/xmlschema-2/datatypes UML (<i>Unified Modeling Language</i>) como definido pelo OMG http://www.omg.org/gettingstarted/specsandprods.htm/	A	
Descrição de dados	RDF (<i>Resource Description Framework</i>) 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. Conforme definição em http://www.eping.e.gov.br	A	Em 2010 a LAG passará a ser denominado VCGE – Vocabulário Controlado do Governo Eletrônico.

Componente	Especificação	SIT	Observações
Sistema de resolução de Identificadores	<i>Handle system</i> (http://www.handle.net).	E	

9.3. Notas sobre XML e *Middleware*

Nem todos os sistemas necessitam ter capacidade de se comunicar diretamente em XML, como representado na Figura 4. Quando apropriado é aceitável a utilização de *middleware* de acordo com a ilustração da Figura 5.

Embora as configurações abaixo apresentem soluções potenciais, o modelo XML direto (Figura 4) é preferencial, sendo possível a utilização do modelo indireto, apresentado na Figura 5, em casos onde existam razões fundamentais que justifiquem seu uso.



Figura 4 – Modelo XML Direto – Intercâmbio Direto.

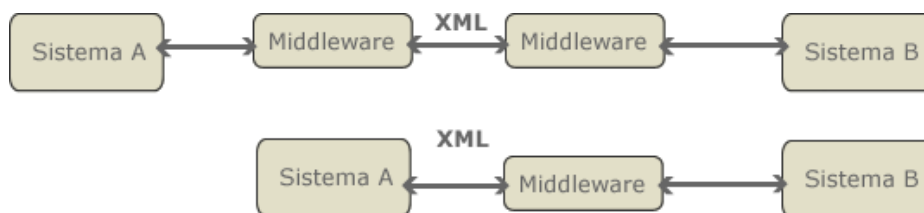


Figura 5 – Intercâmbios via *middleware*.

Em casos específicos como aqueles que necessitam a transferência de grande volume de dados entre sistemas em curto espaço de tempo e nos intercâmbios onde o tempo de resposta é crítico, a adoção do XML como linguagem para intercâmbio poderá ocorrer de forma gradativa.

É importante salientar que o XML é adotado na e-PING como uma linguagem para intercâmbio de dados. Como solução de interoperabilidade (interconexão) observar os itens 6.1.7 e 10.1.12 sobre *Web Services* e *SOAP*.

9.4. Nota sobre o uso de UML

Para a descrição de dados complexos visando melhor explicitação é recomendado, quando cabível, o uso do diagrama de classes da UML.

9.5. Nota sobre a LAG

Em 2010 a LAG passará a ser denominado VCGE – Vocabulário Controlado do Governo Eletrônico.

10. Áreas de Integração para Governo Eletrônico

10.1. Áreas de Integração para Governo Eletrônico: Políticas Técnicas

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

10.1.2. Como diretriz técnica para integração de sistemas de informação recomenda-se a gradual adoção da Arquitetura Orientada a Serviços (SOA), tendo como referência para implementação, a iniciativa “**Arquitetura Referencial de Interoperabilidade dos Sistemas Informatizados de Governo (AR)**”, que é um modelo de Arquitetura Orientada a Serviços, adaptado à realidade dos Sistemas Informatizados do Governo Federal, disponível no sítio <http://www.eping.e.gov.br>.

10.1.3. 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.

10.1.4. Orienta-se o uso de *Web Services* para demandas de integração entre sistemas de informação de governo. De maneira que, independente das tecnologias em que foram implementados, possa-se adotar um padrão de interoperabilidade que garanta escalabilidade, facilidade de uso, além de possibilitar atualização de forma simultânea e em tempo real.

10.1.5. Está disponível, no Portal do Governo Eletrônico, o **Guia de Interoperabilidade de Serviços de Governo** para orientar o uso das ferramentas e tecnologias produzidas pelo segmento.

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

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

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

10.1.9. O **Catálogo de Interoperabilidade** é um elemento central do ambiente de interoperabilidade do Governo Federal. Sua utilização é considerada equivalente à situação Adotado (A).

10.2. Catálogo de Interoperabilidade

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

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

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

10.2.3. A Coordenação da e-PING é responsável pelo Catálogo de Interoperabilidade, em especial pela definição das regras para o gerenciamento dos processos de mudanças e por fomentar que os padrões sejam usados em desenvolvimentos futuros.

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

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

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

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

10.3.4. Solicita-se aos órgãos que utilizarem os Modelos de Documentação que enviem a documentação das interfaces para o email: eping@planejamento.gov.br.

10.4. Áreas de Integração para Governo Eletrônico: Nota explicativa sobre os Catálogos Padrão de Dados e XML Schemas

10.4.1. Considerações Iniciais

Os Catálogos Padrão de Dados e XML Schemas estão disponíveis no portal do Governo Eletrônico no sítio <http://www.governoeletronico.gov.br/>.

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

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

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

O Catálogo XML Schemas 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.

10.4.2. Propriedade e Responsabilidade

A Coordenação da e-PING é responsável por estes Catálogos, em especial pela definição das regras para o 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 apoiem 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 destes Catálogos 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.

10.4.3. 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 Interação 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.

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 testes” 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>.

Para esta versão do documento e-PING, optou-se por disponibilizar o conteúdo do Catálogo XML *Schemas* apenas na ferramenta desenvolvida para a gestão deste, sendo suprimida a publicação no documento das referências aos mesmos. Esta escolha fundamenta-se no objetivo de incentivar o uso e manutenção dos XML *Schemas* na ferramenta apropriada e permitir mais flexibilidade da gestão dos XML *Schemas*.

10.5. Áreas de Integração para Governo Eletrônico: Especificações Técnicas

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

Tabela 17 – Especificações para Áreas de Integração para Governo Eletrônico – Temas Transversais a Áreas de Atuação de Governo

Temas	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
PROCESSOS – Linguagem para Execução de Processos	BPEL4WS V1.1, conforme definido pelo OASIS http://www.oasis-open.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	R	O grupo irá acompanhar a evolução do BPEL4WS versão 2.0. Estudos referentes à orquestração de processos e coreografia serão futuramente conduzidos pelo grupo.

Temas	Especificação	SIT	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	
Troca de Informações Financeiras	XBRL - <i>eXtensible Business Reporting Language</i> http://www.xbrl.org/SpecRecommendations/	F	www.xbrl.org
Legislação, Jurisprudência e Proposições Legislativas	LexML v. 1.0 http://projeto.lexml.gov.br	R	Projeto LexML define recomendações para a identificação e estruturação de documentos legislativos e jurídicos.
Planejamento Estratégico	StratML - <i>Strategy Markup Language</i> http://xml.gov/stratml/index.htm	F	
INFORMAÇÕES GEORREFEREN- CIADAS – 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	
	CSW versão 2.0 ou posterior http://www.opengeospatial.org/standards/cat	A	
	WFS-T versão 1.0 ou posterior http://www.opengeospatial.org/standards/wfs	R	Observar padrões e políticas de segurança indicados pelo GT2, principalmente WS-Security.
	WKT/WKB http://www.opengeospatial.org/standards/sfa	R	Para codificar coordenadas em serviços Web convencionais. As coordenadas devem estar em Lat/Long utilizando o datum SIRGAS2000 ou WGS-84. Usar GML sempre que possível.

Tabela 18 – Especificações para Áreas de Integração para Governo Eletrônico – Web Services²⁹

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Infraestrutura de registro	Especificação UDDI v3.0.2 (<i>Universal Description, Discovery and Integration</i>) definida pela OASIS http://uddi.org/pubs/uddi_v3.htm	R	

²⁹ As questões de segurança relativas a Web Services são abordadas no capítulo 7.

Componente	Especificação	SIT	Observações
	ebXML (<i>Electronic Business using eXtensible Markup Language</i>). A especificação pode ser encontrada em http://www.ebxml.org/specs/index.htm	E	
Linguagem de definição do serviço	WSDL 1.1 (<i>Web Service Description Language</i>) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	A	
	WSDL 2.0 (<i>Web Service Description Language</i>) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl20/	E	
Perfil básico de interoperabilidade	<i>Basic Profile 1.1 Second Edition</i> , como definido pela WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	E	A versão 1.2 do Basic Profile encontra-se como rascunho (<i>Working Draft</i>) em http://www.ws-i.org/Profiles/BasicProfile-1.2.html
<i>Portlets</i> remotos	WSRP 1.0 (<i>Web Services for Remote Portlets</i>) como definido pela OASIS http://www.oasis-open.org/committees/wsrp	E	

11. Glossário de Siglas e Termos Técnicos³⁰

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, resenhas, resenhas 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.

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

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 OGC baseada em 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. 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.

³⁰ Microsoft Press. Dicionário de informática. Tradutor e consultor editorial Fernando Barcellos Ximenes - KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.

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

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

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

IPv4 – Internet Protocol Version 4 (Protocolo de Internet Versão 4): é a versão do protocolo IP mais utilizada atualmente. É formada por um número de 32 bits escrito com quatro octetos no formato decimal, separados por pontos (exemplo: 161.148.1.18). A primeira parte do endereço identifica uma rede específica na inter-rede e a segunda parte identifica um equipamento (host) dentro dessa rede.

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

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

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

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”.

Padrão aberto:

I - possibilita a interoperabilidade entre diversos aplicativos e plataformas, internas e externas;

II - permite aplicação sem quaisquer restrições ou pagamento de royalties;

III - pode ser implementado plena e independentemente por múltiplos fornecedores de programas de computador, em múltiplas plataformas, sem quaisquer ônus relativos à propriedade intelectual para a necessária tecnologia.

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

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 subsequentes que substituem ou elaboram em todas as partes dos RFCs anteriores. RFC também é a abreviação de Remote Function Call (chamada funcional remota).

RSA – Rivest-Shamir-Adleman: cifração de Internet e um sistema de autenticação que utiliza um

algoritmo desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman.

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

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

serviços.

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

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 infraestrutura de uma rede pública de telecomunicações, como a Internet, por exemplo, para a transmissão de informações confidenciais. Os dados transmitidos são encriptados. Sua implementação se dá por meio de túneis virtuais, pelos quais trafegam as informações, protegendo-as do acesso de usuários não autorizados.

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

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

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

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

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

- **WFS Básico (WFS)**: implementa operações somente leitura, que permitem obter os dados espaciais.
- **WFS Transacional (WFS-T)**: implementa as operações transacionais, usadas para manipular os dados remotamente.

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

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

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

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

Agência Nacional de Águas (ANA)
Sérgio Augusto Barbosa

Agência Nacional do Cinema (ANCINE)
Sérgio Augusto S. de Moraes

Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (ABEP)
Dayse Vianna

Banco do Brasil (BB)
Ulisses de Sousa Penna

Caixa Econômica Federal (CAIXA)
Ângela B. Baylo
Paulo Maia da Costa
Rúbia Scrócaro

Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
Humberto Degrazia Campedelli

Ministério da Defesa – Comando do Exército (MD/CEX)
Emerson Magnus de A. Xavier
Jefferson Adelino Lemos Pita

Ministério da Justiça (MJ)
Jorilson da Silva Rodrigues

Ministério da Saúde (MS)
Fábio Lima Cordeiro

Ministério das Relações Exteriores (MRE)
Filipe Carneiro Guimarães

Ministério do Desenvolvimento, Indústria e Comércio Exterior (MDIC)
José Luismar de Campos Larcher

Ministério do Meio Ambiente (MMA)
Maurício Dayriell
Paulo Henrique de Assis Santana

Ministério do Planejamento, Orçamento e Gestão – Secretaria de Logística e Tecnologia da Informação (MP/SLTI)
Nazaré Lopes Bretas (Coordenadora Geral)
Cláudio Muniz Machado Cavalcanti
Cristiano Rocha Heckert
Jorge Arruda
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Lilian Barbara Bender Portugal
Marcelo Martins Villar
Mário Henrique Paes Vieira
Rogério Santanna dos Santos
Yuri Fontes de Oliveira

Nuclebrás Equipamentos Pesados S/A (NUCLEP)
Adilson Custódio
Elizabeth Rodrigues Cunha

Presidência da República (PR)
Macarino Bento Garcia de Freitas

Presidência da República – Instituto Nacional de Tecnologia da Informação (ITI)
Maurício Augusto Coelho

Renato da Silveira Martini

Secretaria da Receita Federal do Brasil (RFB)

Edna Pereira Pinto Fernandes

Secretaria da Administração do Estado da Bahia (SAEB)

Ernani Marques dos Santos

Serviço Federal de Processamento de Dados (SERPRO)

Bruno Pacheco de Paes

Elói Juniti Yamaoka

Grupo de Trabalho Interconexão

Cristiano Rocha Heckert (MP/SLTI) – Coordenador

Carlos Bellone Neto (RFB)

Dijasmó Martins Gomes Junior (ECT)

Filipe Carneiro Guimarães (MRE)

Helio de Araujo Castro (NUCLEP)

Juscelino Kilian (PR/GSI)

Leonardo Boselli da Motta (MP/SLTI)

Luiz Gustavo Lustosa Colombo (IPHAN)

Odilon de Freitas Militao Neto (CAIXA)

Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)

Vanderlei de Jesus dos Santos Marques (ANVISA)

Wellington Luiz Barbosa (MP/SLTI)

Colaboradores

Diogo da Fonseca Tabalipa (MP/SLTI)

Hermógenes Batista Correia (MP/SLTI)

Grupo de Trabalho Segurança

Jorilson da Silva Rodrigues (MJ) – Coordenador

Antônio Acras Filho (SERPRO)

Artur Nobre Mendes (FUNAI)

André Machado Caricatti (ITI)

Cláudio Muniz Machado Cavalcanti (MP/SLTI)

Cristiano Rocha Heckert (MP/SLTI)

Dante de Matos Gomes (PRODEB)

Filipe Carneiro Guimarães (MRE)

Gilberto de Oliveira Netto (SERPRO)

Humberto Degrazia Campedelli (DATAPREV)

Jean Carlo Rodrigues (ITI)

Joel Corrêa (DATAPREV)

José Eduardo Malta de Sá Brandão (IPEA)

José Luiz Povill de Souza (MJ/DPF)

Luiz Gustavo Lustosa Colombo (IPHAN)

Marcos Gomes Figueira (BB)

Marcos J.C. Euzébio (BACEN)

Mario Henrique Paes Vieira (MP/SLTI)

Nazaré Lopes Bretas (MP/SLTI)

Paulo Coelho Ventura Pinto (ANS)

Colaboradores

Anderson Claiton Fernandes (MJ)

Cláudia do Socorro Ferreira Mesquita (MP/SLTI)

Ronaldo Íon Miranda do Nascimento (MJ)

Grupo de Trabalho Meios de Acesso

Paulo Maia da Costa (CAIXA) – Coordenador

Artur Emilio de Rezende (MF)
Bruno Pacheco de Assis (SERPRO)
Carlos Bellone Neto (RFB)
Cláudio Muniz Machado Cavalcanti (MP/SLTI)
Danielle de Menezes Maciel Silva (ANVISA)
Denise Barros de Sousa (MEC)
Eliane Aristoteles moreira (DATAPREV)
Frederico Cabral de Menezes (CONAB)
Geancarlo Noronha Vinhal (SERPRO)
Jacob Batista de Castro Junior (PR/GSI)
Jorge Arruda (MP/CGTI)
Juscelino Kilian (PR/GSI)
Márcio F. Viana M. (ME)
Márcio Humberto M. Cammarota (SERPRO)
Marconi Pereira Sodate (RFB)
Mauro Lemes da Silva (CAIXA)
Pedro Paulo Lemes Machado (ITI)
Reinaldo Silva Simão (PR)
Rubia Scrocaro (CAIXA)
Sonia Regina Rodrigues Motta (MEC)
Viviane Regina Lemos Bertol (ITI)
Wagner Ferreira Carneiro Junior (MF)

Colaboradores

André Luís da Silva Gonçalves (MP/SLTI)

Grupo de Trabalho Organização e Intercâmbio de Informações

Eloi Juniti Yamaoka (SERPRO) – Coordenador
Alisson de Oliveira Rodrigues (MI)
Ângela B. Baylo (CAIXA)
Antonio Celso Xavier de Oliveira (MRE)
Aurélia Dolores Gonçalves Bruner (ELETROBRÁS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Brenda Couto de Brito Rocco (AN-CC)
Cintia de Souza Cinquini (PR)
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (AN-CC)
Eduardo Rafael Miranda Feitoza (MI)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (AN-CC)
Fernanda Hoffmann Lobato (MP/SLTI)
Hilda Pimentel (ANCINE)
João Alberto Lima (Senado Federal)
Ligia Leindorf Bartz Kraemer (UFPR)
Luciana Ferreira Pinto da Silva (INEP)
Márcia Helena Gonçalves Rollemberg (MS)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcio Imamura (IBGE)
Margareth da Silva (AN-CC)
Maria Valéria Lins Tenório (Governo de Pernambuco / ATI)
Neuza Arantes Silva (MAPA)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Sylmara Campos Pinho Garcia (ANCINE)
Vicente de Paula Teixeira (CGU)
Virgílio Dantas Lins Filho (ME)
Vivianne Muniz Veras Barrozo (SERPRO)

Colaboradores

Dalva Clementina Luca (MJ)

Grupo de Trabalho Áreas de Integração para Governo Eletrônico

Cláudio Muniz Machado Cavalcanti (MP/SLTI) – Coordenador
Adelino Fernando Correia (DATASUS)
Aliomar Mariano Rego (EMBRAPA)
Ananda de Medeiros Macias (SERPRO)
Antônio Campos Monteiro (ANEEL)
Bruno Palvarini (MP/SEGES)
Carlos Bellone Neto (RFB)
Carlos Maranhão (ANS)
Ceres Albuquerque (ANS)
Cláudio Manoel Cordeiro (SERPRO)
Ewerton Luciano Martins (ANVISA)
Frederico Duarte Guerra de Macedo (ME)
José Glaucy Rocha (RFB)
Hesley Py (IBGE)
Maurício Dayrell (MMA)
Marcelo Bastos Brandão (ABIN)
Márcio Humberto M. Cammarota (SERPRO)
Márcio Lúcio Vasconcelos Donato (MEC)
Mônica Maria Lucatelli Dória de Araújo (DATAPREV)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo de Lima (INCRA)
Rogério Werneck (PR/DIRTI)
Tatiana Giachini (SERPRO)
Werangge Custódio (ANVISA)
Wilson de Moraes Coelho (DATASUS)

Colaboradores

Cláudia do Socorro Ferreira Mesquita (MP/SLTI)
Luís Carlos Ramos (DATASUS)

Subgrupo: ABEP

Dayse Vianna (Governo do Rio de Janeiro / PRODERJ) – Coordenadora
Tarcísio Quirino Falcao (Governo de Pernambuco / ATI)

Subgrupo: Guia de Interoperabilidade de Serviços de Governo

Cláudia do Socorro Ferreira Mesquita (MP/SLTI) – Coordenadora
Lucio Ribeiro (Governo de Pernambuco / ATI)
Tarcísio Quirino Falcão (Governo de Pernambuco / ATI)
Rodrigo Henriques Medeiros (SERPRO)

Subgrupo: Padrões para Intercâmbio de Informações Espaciais

Emerson Magnus de A. Xavier (MD/CEX/CIGEx) – Coordenador
Cristiane Vaz Domingues (DATAPREV)
Jedson F. Passos (CAIXA)
Linda Soraya Issmael (MD/CEX/DSG)
Marcelo Martins Villar (MP/SLTI)
Moema Augusto (IBGE)
Yoshihisa Kawano (ABIN)
Yuri Fontes de Oliveira (SLTI/MP)

Ilustrações

Hezrai de Souza Cruz (MP/SLTI)