

Governo Brasileiro
Comitê Executivo de Governo Eletrônico



e-PING
Padrões de Interoperabilidade
de Governo Eletrônico

Documento de Referência

Versão 1.0

13 de julho 2005



SUMÁRIO

	Página
Apresentação	4
PARTE I – VISÃO GERAL DA e-PING	
1. Introdução	6
2. Escopo	8
3. Políticas Gerais	10
4. Segmentação	12
4.1. Interconexão	12
4.2. Segurança	12
4.3. Meios de Acesso	12
4.4. Organização e Intercâmbio de Informações	13
4.5. Áreas de Integração para Governo Eletrônico	13
5. Gestão da e-PING	14
5.1. Histórico	14
5.2. Estratégia de Implantação	14
5.3. Modelo de Gestão	15
5.3.1. Atribuições	15
5.3.2. Responsabilidades	16
5.4. Atividades Adicionais	17
5.4.1. Seleção e Homologação de Padrões Tecnológicos	17
5.4.2. Auditoria de Conformidade	18
5.4.3. Criação e Manutenção do Sítio	18
5.4.4. Acompanhamento Legal e Institucional	18
5.4.5. Divulgação	19
5.4.6. Capacitação	19
5.5. Relacionamento com Governo e Sociedade	19
5.5.1. Organizações do Governo Federal – Poder Executivo	19
5.5.2. Outras Instâncias de Governo	20
5.5.3. Organizações do Setor Privado e do Terceiro Setor	20
5.5.4. Cidadão	20

PARTE II – ESPECIFICAÇÃO DOS COMPONENTES DA e-PING

6. Interconexão	22
6.1. Interconexão: Políticas Técnicas	22
6.2. Interconexão: Especificações Técnicas	22
6.3. Web Services	24
6.4. Mensagens Eletrônicas	25
6.5. Migração para IPv6	26
6.6. LAN Sem Fio	26
6.7. Mensageria em Tempo Real	26
6.8. VPN	26
7. Segurança	27
7.1. Segurança: Políticas Técnicas	27
7.2. Segurança: Especificações Técnicas	27
8. Meios de Acesso	32
8.1. Meios de Acesso: Políticas Técnicas	32
8.2. Meios de Acesso: Especificações Técnicas para Estações de Trabalho	34
8.3. Meios de Acesso: Especificações Técnicas para Smart Cards, Tokens e Cartões em Geral	37
9. Organização e Intercâmbio de Informações	47
9.1. Organização e Intercâmbio de Informações: Políticas Técnicas	47
9.2. Organização e Intercâmbio de Informações: Especificações Técnicas	47
9.3. Notas sobre XML e Middleware	47
9.4. Notas sobre Assuntos em Estudo e Elaboração	48
10. Áreas de Integração para Governo Eletrônico	51
10.1 Áreas de Integração para Governo Eletrônico: Políticas Técnicas	51
10.2 Áreas de Integração para Governo Eletrônico: Especificações Técnicas	53
11. Glossário de Termos Técnicos	54
12. Créditos	60

Documento de Referência da e-PING – Versão 1.0

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 e está publicado em sítio específico na Internet (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;
- Créditos – Relação dos 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

O documento que define as políticas de gestão do governo brasileiro – Gestão Pública para um Brasil de todos (www.gestaopublica.gov.br) – destaca a “necessidade de significativas transformações nas instituições públicas”, tendo como diretriz “a consideração do cidadão como foco da ação pública”.

A implementação dessas políticas requer “o desenvolvimento de sistemas contínuos de monitoramento e avaliação”, “a otimização dos processos de trabalho, incorporando inovações tecnológicas e gerenciais que permitam redimensionar, quantitativa e qualitativamente, os recursos humanos, orçamentários, financeiros e logísticos” e “o aprimoramento do atendimento ao cidadão, mediante a facilitação do acesso aos serviços públicos e o aprimoramento dos sistemas de informação”.

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

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

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

Utilizando como referência a experiência de outros países, o governo brasileiro dá início a esse processo com a implantação da 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.

Documento de Referência da e-PING – Versão 1.0

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

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

2. Escopo

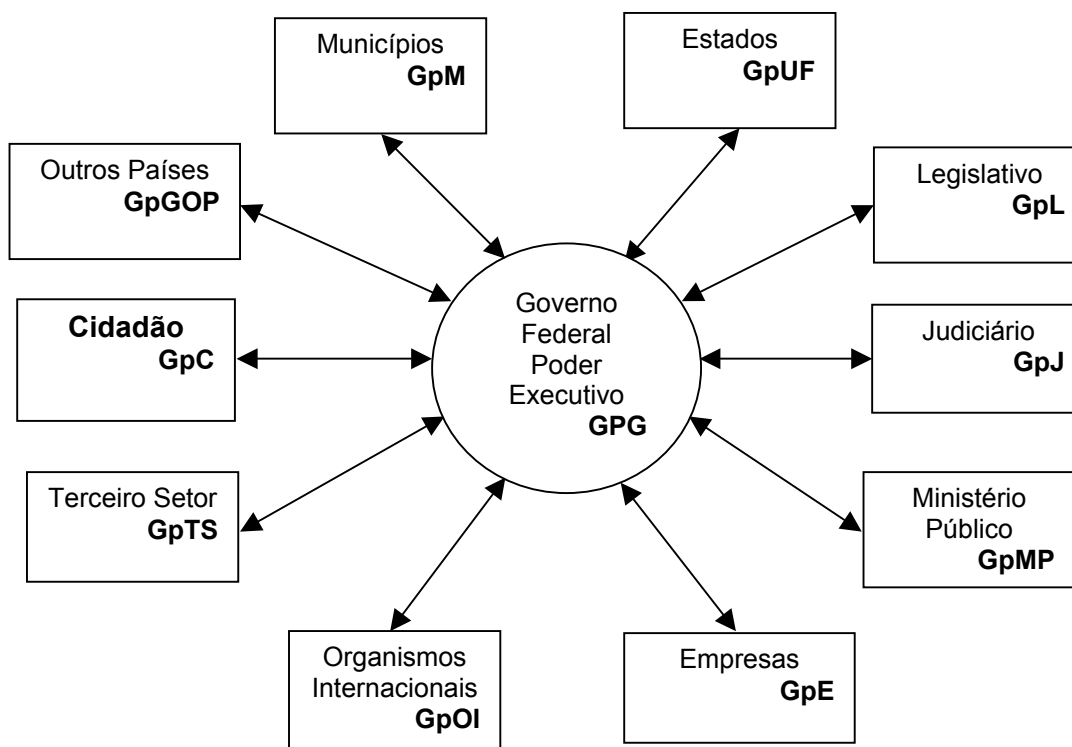
Políticas e especificações claramente definidas para interoperabilidade e gerenciamento de informações são fundamentais para propiciar a conexão do governo, tanto no âmbito interno como no contato com a sociedade e, em maior nível de abrangência, com o resto do mundo – outros governos e empresas atuantes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



Documento de Referência da e-PING – Versão 1.0

A adoção dos padrões e políticas contidos na e-PING não pode ser imposta aos cidadãos e às diversas instâncias de governo referenciadas, dentro e fora do país. O governo brasileiro, no entanto, estabelece essas especificações como o padrão por ele selecionado e aceito.

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.

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 sistemática da Internet (www.eping.e.gov.br) como meio preferencial para o contato entre os gestores da e-PING e a sociedade em geral.

3. Políticas Gerais

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

Alinhamento com a INTERNET: todos os sistemas de informação da administração pública deverão estar alinhados com as principais especificações usadas na Internet e com a World Wide Web.

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

Adoção de navegadores ("browsers") como principal meio de acesso: todos os sistemas de informação de governo deverão ser acessíveis, preferencialmente, por meio de tecnologia baseada em "browser"; outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores.

Seguindo a política governamental de inclusão digital, a e-PING deverá adotar um padrão mínimo referencial de browser, estabelecido para direcionar o desenvolvimento dos serviços de governo eletrônico, considerando-se os princípios de 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.

Tendo por objetivo a conciliação desses dois princípios fundamentais, esta versão ainda não trata da especificação completa desse padrão mínimo de navegador. Essa definição está sendo objeto de estudo, conduzido prioritariamente, que será incorporado à e-PING tão logo os resultados estejam disponíveis.

A e-PING recomenda que todo serviço de governo eletrônico especifique, com clareza e, de preferência, na sua página inicial, as versões mínimas de navegadores que suportam as funcionalidades requeridas pelo serviço associado.

Adoção de metadados para os recursos de informação do governo.

Desenvolvimento e adoção de um Padrão de Metadados do Governo Eletrônico – e-PMG, baseado em modelo aberto e internacional.

Desenvolvimento e manutenção da Lista de Assuntos do Governo: Taxonomia de Navegação (LAG), que contemple, numa estrutura de diretório, todos os assuntos relacionados com a atuação de governo.

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

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

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

Adoção Preferencial de Padrões Abertos: a e-PING define que, sempre que possível, serão adotados padrões abertos nas especificações técnicas. Padrões proprietários são aceitos, de

Documento de Referência da e-PING – Versão 1.0

forma transitória, mantendo-se as perspectivas de substituição assim que houver condições de migração. Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações. Quando disponíveis, soluções em Software Livre são consideradas preferenciais.

A e-PING mantém total compatibilidade com as iniciativas de governo na área de TIC. Um exemplo a ser mencionado é o Guia de Migração de Software Livre do Governo Brasileiro, objeto de publicação recente.

Adesão à e-PING: nos limites estabelecidos por este documento, a adesão à e-PING é obrigatória para todos os órgãos do Poder Executivo do governo federal do Brasil, conforme definição contida no item 2 – Escopo da e-PING.

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

Para contato com entidades externas, cuja interação encontra-se discriminada no mesmo item 2, o governo federal não pretende impor o uso dessas especificações mas estabelece que esses são os padrões em que deseja interoperar com essas entidades.

A adesão para entidades fora do governo federal – Poder Executivo dar-se-á de forma voluntária e sem qualquer ingerência por parte da Coordenação da e-PING.

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

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.

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. O estabelecimento da forma de apresentação ficará a cargo de cada equipe de construção da interface com o usuário, no âmbito das instituições responsáveis pelos serviços de e-gov oferecidos.

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 específico, composto por profissionais atuantes em órgãos dos governos federal, estadual e municipal, especialistas em cada assunto. Esses grupos foram responsáveis pela elaboração desta versão da arquitetura, base para o estabelecimento dos padrões de interoperabilidade do governo brasileiro.

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

4.1. Interconexão

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

Neste segmento, são estabelecidas as especificações para:

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

4.2. Segurança

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

- Segurança de IP
- Segurança de Correio Eletrônico
- Criptografia
- Desenvolvimento de Sistemas
- Serviços de Rede

4.3. Meios de Acesso

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

Padrões para acesso via estações de trabalho

- Navegadores (*browsers*)
- Conjunto de Caracteres e Alfabetos
- Formato de Intercâmbio de Hipertexto

Documento de Referência da e-PING – Versão 1.0

- 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
- Georreferenciamento: padrões de arquivos para estações de trabalho

Cartões Inteligentes / Tokens / Outros

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

4.4. Organização e Intercâmbio de Informações

Aborda os aspectos relativos ao tratamento e à transferência de informações nos serviços de governo eletrônico. Inclui a padronização da estrutura de assuntos de governo para uso em portais e tratamento de metadados, compreendendo os seguintes componentes:

- Linguagem para intercâmbio de dados;
- Linguagem para transformação de dados;
- Modelagem dos dados para intercâmbio;
- Catálogo de Dados de Uso Comum;
- Lista de Assuntos do Governo: Taxonomia para Navegação (LAG);
- Padrão de Metadados do Governo – e-PMG.

4.5. Áreas de Integração para Governo Eletrônico

As metas de análise e proposição deste segmento são:

- os processos que, nas áreas de atuação do governo, demandam integração e intercâmbio de informações;
- os atores envolvidos com esses processos;
- o catálogo de referência de Esquemas XML.

Esse trabalho permitirá o estabelecimento e a publicação dos padrões e das políticas técnicas que tornarão possível a oferta de serviços de e-gov para o governo e para a sociedade.

Serão mencionadas as áreas prioritárias, sempre considerando os benefícios diretos e indiretos para a sociedade. Em cada área serão selecionados processos para os quais serão estabelecidos padrões de unidades de informação intercambiadas, representados principalmente por Esquemas XML, definidos e administrados de forma a possibilitar sua utilização compartilhada.

É apresentada uma metodologia inicial para estabelecimento e manutenção dos padrões de interoperabilidade por processo selecionado. Para cada processo selecionado para estudo, a metodologia prevê, dentre outros, a identificação:

- da área temática (área de atuação de governo) à qual o processo está relacionado;
- dos tipos de relacionamento do governo existentes;
- das entidades envolvidas (atores), inclusive com o gestor ou responsável;
- dos resultados esperados do processo de integração.

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/PR;
- 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 inter-órgãos – denominado Comitê Constituinte – para conduzir os trabalhos iniciais de montagem da arquitetura. Além dos três organizadores, participaram desse grupo os seguintes órgãos: DATAPREV, Banco do Brasil, Ministério das Comunicações, Caixa Econômica Federal, DATASUS e ABEP - Associação Brasileira de Empresas Estaduais de Processamento de Dados.

O Comitê estabeleceu o seguinte programa de trabalho:

- Definição da forma inicial de elaboração e gestão da arquitetura e-PING;
- Definição da segmentação dos assuntos a serem cobertos pela e-PING;
- Criação de cinco grupos de trabalho responsáveis pelas definições iniciais de políticas e especificações técnicas para cada um dos segmentos;
- Estabelecimento de um cronograma de trabalho com o objetivo de construção e divulgação da versão inicial da arquitetura, denominada versão 0;
- Realização de consulta pública e audiências públicas em RS, SP, DF, RJ, MG e PE, de modo a colher contribuições, da sociedade em geral, sobre o conteúdo proposto na versão 0;
- Publicação da versão 1, juntamente com a resolução de institucionalização da e-PING no âmbito da APF – Poder Executivo.

Foram pesquisadas experiências semelhantes desenvolvidas por governos de outros países. 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 seguirá o esquema de versionamento. É prevista a elaboração de uma versão anual, com publicação intermediária de atualizações, sempre que existirem modificações significativas.

Este documento consolida o trabalho inicial dos grupos montados para os cinco segmentos definidos. Todo seu conteúdo foi disponibilizado para Consulta Pública, com o objetivo de obter contribuições às propostas de padrões publicados na versão 0.

Documento de Referência da e-PING – Versão 1.0

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 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 (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 atuantes no 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, responsáveis pelo estabelecimento de padrões reconhecidos internacionalmente (W3C, OASIS, IETF, Institutos Normativos de segmentos específicos, como ABNT, INMETRO, ISO, NIST, etc.);
- Gerenciar a interação com órgãos de fomento nacionais e internacionais, para canalizar recursos, visando atender as necessidades de criação de infra-estrutura da e-PING e promover a pesquisa e desenvolvimento;
- Viabilizar a implantação e gerenciar o processo de homologação dos padrões a serem estabelecidos para o governo;
- Viabilizar a implantação e gerenciar processos de auditoria realizados com a finalidade de verificar o nível de adesão às recomendações e especificações da e-PING;
- Atuar cooperativamente, como apoio aos órgãos de governo, na realização dos processos necessários para adequação aos padrões e-PING; avaliar a possibilidade de patrocinar programas abrangentes que promovam a utilização intensiva dos padrões propostos.

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

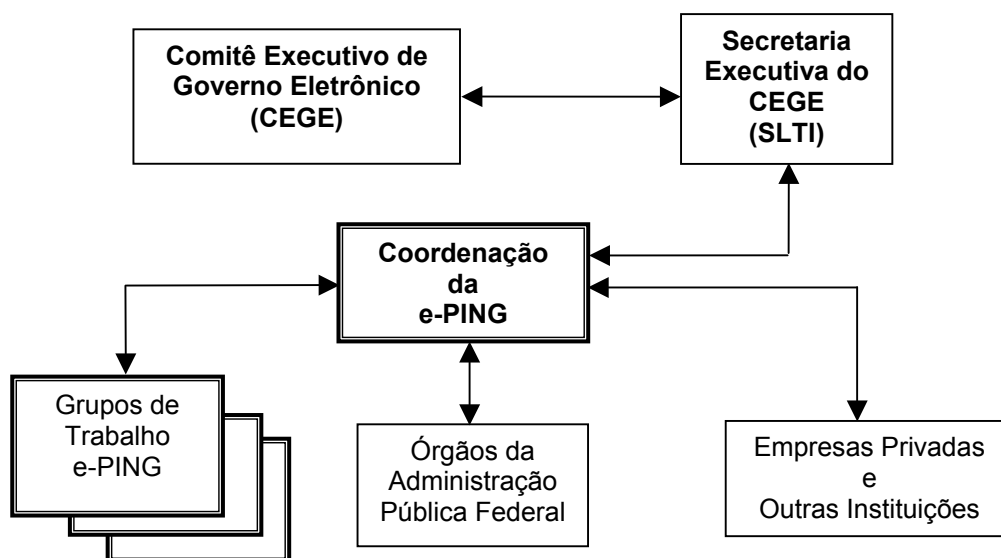
- Estabelecer as formas de elaboração e de manutenção das políticas e especificações técnicas que compõem a e-PING, considerando:
 - Identificação, criação e gestão de grupos de trabalho específicos;
 - Estabelecimento de convênios e definição de instituições de governo como responsáveis pelas políticas e especificações técnicas de componentes específicos dos segmentos de interoperabilidade;

Documento de Referência da e-PING – Versão 1.0

- Identificação e implementação de formas alternativas de gerenciamento técnico dos assuntos contemplados na abrangência de atuação da e-PING;
- Coordenar o desenvolvimento e manutenção, no âmbito do governo federal – Poder Executivo, de:
 - Padrão de Metadados de Governo – e-PMG;
 - Lista de Assuntos do Governo: Taxonomia para Navegação (LAG);
 - Catálogo de Dados de Uso Comum;
 - Catálogo de Referência dos Esquemas XML;
 - 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 a ser criada para administração da e-PING é apresentada no esquema simplificado a seguir.



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

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

- Implantação da arquitetura e-PING, providenciando as atividades necessárias para consolidação da versão inicial 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;

Documento de Referência da e-PING – Versão 1.0

- 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;
- **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 técnicas; é incluído na e-PING em razão de seu uso significativo em instituições de governo, tendendo a ser desativado assim que algum outro componente, em uma das duas situações anteriores venha a apresentar condições totais de substituí-lo. Pode vir a ser considerado um componente “recomendado” caso venha a se adequar a todas as políticas técnicas estabelecidas. Convém salientar que o desenvolvimento de novos serviços ou a reconstrução de partes significativas dos já existentes deve evitar o uso de componentes classificados como transitórios;
- **Em Estudo (E):** componente que está em avaliação e será enquadrado numa das situações acima, assim que o processo de avaliação estiver concluído;
- **Estudo Futuro (F):** componente ainda não avaliado e que será objeto de estudo posterior.

O processo de seleção dos componentes adotados pela e-PING e sua conseqüente classificação nas situações acima indicadas, é de responsabilidade dos Grupos de Trabalho compostos por

Documento de Referência da e-PING – Versão 1.0

profissionais especialistas com atuação no governo e em instituições com as quais seja estabelecido algum tipo de convênio ou contrato especificamente para essa finalidade.

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

Nesse caso, o governo deverá estabelecer convênios ou credenciar instituições para elaboração de testes de conformidade, sempre definindo quais componentes devem ser submetidos a processos de homologação, quais os critérios de avaliação dos resultados e quais as condições de realização dos procedimentos.

A definição completa do processo de seleção e homologação ficará a cargo da Coordenação da e-PING e será incluída em publicações futuras da e-PING.

5.4.2. Auditoria de Conformidade

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

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

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

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

5.4.3. Criação e Manutenção do Sítio

Todo o processo de troca de informações sobre a e-PING com usuários, colaboradores e interessados é realizado, preferencialmente, pela Internet, no endereço 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 para garantir a aderência do conteúdo dos documentos que compõem a arquitetura às normas e instrumentos legais vigentes no país.

Documento de Referência da e-PING – Versão 1.0

Adicionalmente, essa Assessoria terá ainda a responsabilidade de preparar toda a parte institucional necessária para garantir que as adequações e recomendações da e-PING venham a compor o conjunto de instrumentos legais de TIC no país.

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

5.4.5. Divulgação

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

- Realização de eventos específicos de divulgação, como Seminários, Workshops e apresentações em geral;
- Participação em eventos governamentais na área de TIC e correlatas;
- Participação em eventos direcionados a públicos específicos;
- Publicação de todas as versões da e-PING e das atualizações intermediárias;
- Intercâmbio com outras esferas e outros Poderes de governo, com instituições públicas, privadas e do terceiro setor e com governos de outros países.

5.4.6. Capacitação

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

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

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

5.5. Relacionamento com Governo e Sociedade

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

5.5.1. Organizações do Governo Federal – Poder Executivo

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

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

- Contribuir para o desenvolvimento e melhoria contínua da e-PING;
- Garantir que suas estratégias organizacionais de TIC considerem que os sistemas integrantes de serviços de governo eletrônico sob sua responsabilidade estejam adequados às recomendações da e-PING;
- Dispor de um plano de implementação e adequação da infra-estrutura de TIC da organização à arquitetura e-PING;
- Assegurar que sejam de domínio das equipes da instituição, as habilidades para definir e utilizar as especificações requeridas para interoperabilidade, fornecendo suporte de treinamento quando necessário;
- Estabelecer ponto de contato nas instituições, para intercâmbio de informações e de necessidades com a Coordenação da e-PING;
- Alocar e suprir recursos para dar suporte aos seus processos de adequação à e-PING;

Documento de Referência da e-PING – Versão 1.0

- Aproveitar a oportunidade para racionalizar processos (como resultado do aumento da interoperabilidade) de maneira a melhorar a qualidade e reduzir custos de provimento dos serviços de e-gov.

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

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

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

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

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

5.5.3. Organizações do Setor Privado e do Terceiro Setor

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

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

Outras formas de participação dessas instituições na e-PING podem ser consideradas, estabelecendo-se critérios que garantam a transparência e 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 prevêem a participação ativa do cidadão e da sociedade em geral, no processo de construção e gestão da arquitetura.

Parte II – Especificação Técnica dos Componentes da e-PING

6. Interconexão

6.1. Interconexão: Políticas Técnicas

As políticas técnicas para interconexão são:

6.1.1. Os órgãos da APF deverão se interconectar utilizando IPv4 e planejar sua futura migração para IPv6. Veja nota sobre migração para IPv6, item 6.5.

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. Para envio de mensagens seguras deve ser utilizado S/MIME v3, a menos que exigências de segurança imponham outra forma.

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

6.1.4. Os órgãos da APF devem obedecer à política de nomeação de domínios da Rede Governo, estabelecidos na Resolução n.º 7, que pode ser visualizada no endereço eletrônico http://www.governoeletronico.e.gov.br/governoeletronico/publicacao/down_anexo.wsp?tmp.arquivo=E15_223resolucao_n7_sitios_oficiais2562002.pdf.

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

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

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

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

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

6.1.10. O protocolo SOAP é recomendado para comunicação entre os clientes e os Web Services e a especificação do serviço deverá utilizar a linguagem WSDL.

6.2. Interconexão: Especificações Técnicas

Tabela 6.1 – Especificações para Interconectividade

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) e/ou HTTPS (RFC 2660).	R	

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.

Documento de Referência da e-PING – Versão 1.0

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 2646; RFC 2047; RFC 2231; RFC 2048; RFC 3023; RFC 2049.	R	Os anexos de mensagens eletrônicas devem estar de acordo com os tipos de arquivo para navegadores e visualizadores, como definido para o canal de envio específico.
Segurança de conteúdo de mensagem eletrônica	O S/MIME v3 deverá ser utilizado quando for apropriado para segurança de conteúdo de mensagens gerais do governo, a menos que os requisitos de segurança determinem outra forma. RFCs correlacionadas: RFC 3369, RFC 2631, RFC 2632 e RFC 2633.	R	
Acesso à Caixa Postal	A menos que as exigências de segurança determinem de outra forma, programas de correio que fornecem facilidades de acesso a correspondência deverão, no mínimo, estar de acordo com POP3 para acesso remoto a caixa postal. RFCs correlacionadas: RFC 1939, RFC 1957 e RFC 2449. Onde facilidades adicionais forem necessárias, a menos que requisitos de segurança estabeleçam de forma contrária, os programas de correio que fornecem facilidades avançadas de acesso à correspondência, deverão estar de acordo com IMAP para acesso remoto à caixa postal. RFCs correlacionadas: RFC 3501, RFC 2342, RFC 2971, RFC 3502, RFC 3503 e RFC 3510.	R	
Acesso seguro à caixa postal	O acesso à caixa postal, através de redes não seguras, deverá usar HTTPS, de acordo com os padrões de segurança no transporte. RFCs correlacionadas: RFC 2595 quando estiver sendo usado TLS com IMAP e POP3 para acesso à caixa postal.	R	
Diretório	Usar o esquema do diretório central, conforme definido no endereço eletrônico: http://www.e.gov.br/correios/dir_redegoverno.htm . LDAP v3 deverá ser utilizado para acesso geral de usuários do diretório.	R	
Serviços de Nomeação de Domínio	DNS (RFC 1035) As diretivas de nomeação de domínio do governo brasileiro são encontradas na Resolução N° 7 do Comitê Executivo do Governo Eletrônico http://www.governoeletronico.e.gov.br/governoeletronico/publicacao/down_anexo.wsp?tmp.arquivo=E15_223resolucao_n7_sitios_oficiais2562002.pdf . Além dessas diretivas, por decisão do Comitê Gestor da Internet no Brasil, a nomeação de	R	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
	<p>domínios obedece às orientações do Ministério do Planejamento, a quem compete gerenciar os domínios .GOV.BR”.</p> <p>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</p>		
Endereços de caixa postal eletrônica	<p>As regras para definição dos nomes das caixas postais de correio eletrônico deverão seguir ao estabelecido no documento “Caixas Postais Individuais-Funcionais na Rede Governo”, disponível no endereço eletrônico http://www.e.gov.br/correios/cp_individ.htm</p>	R	
Protocolos de transferência de arquivos	<p>FTP (RFC 959 e RFC 2228) (com re-inicialização e recuperação) e HTTP (RFC 2616) para transferência de arquivos.</p>	R	
Intercomunicação LAN/WAN	<p>IPv4 (RFC 791)</p>	R	
Transporte	<p>TCP (RFC 793)</p> <p>UDP (RFC 768) quando necessário, sujeito às limitações de segurança.</p>	R	

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

6.3. Web Services

Os Web Services são aplicações de software, identificadas por uma URI (Uniform Resource Identifier), cujas interfaces e ligações são capazes de serem definidas, descritas e descobertas por artefatos baseados em XML. Além disso, possuem suporte para integração direta com outras aplicações de software, utilizando, como padrão de interoperabilidade, mensagens escritas em XML e encapsuladas em protocolos de aplicação padrão da Internet.

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

A tecnologia de Web Services é adequada para atender tais necessidades, além de ser independente em relação aos Sistemas Operacionais e às Linguagens de Programação.

Uma das suas características mais relevantes se refere ao nível de abstração, superior ao conceito de componentes de software. Desde um formulário pertencente a uma página web, até um componente de software, que encapsula uma complexa regra de negócio, podem ser transformados em Web Services, o que torna seu uso bastante flexível.

O uso de Web Services contempla tanto transferências de documentos entre Instituições quanto solicitações para execução de serviços remotos.

As estruturas de documentos XML serão descritas através de Esquemas XML, como forma de validação dos tipos de dados pertencentes às linhas de negócio.

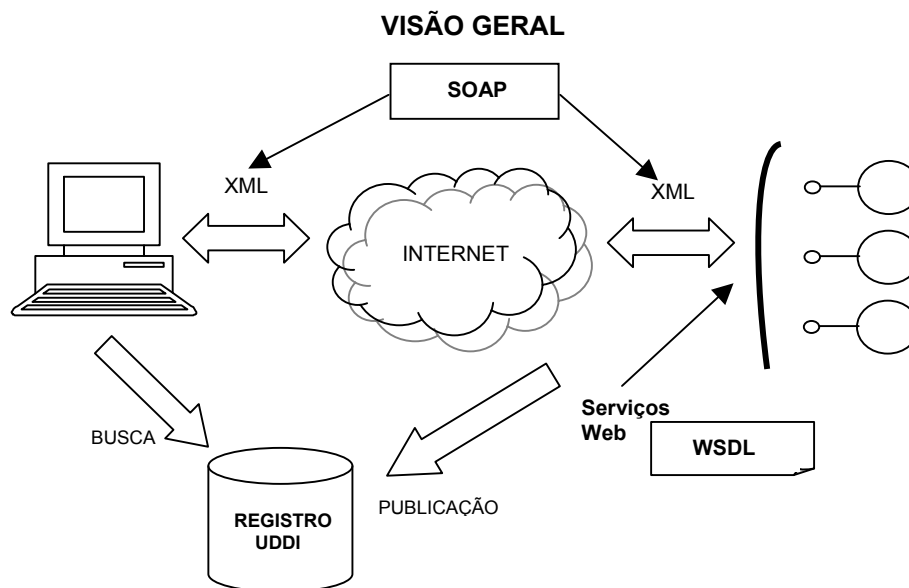


Tabela 6.2 – Especificações para Web Services

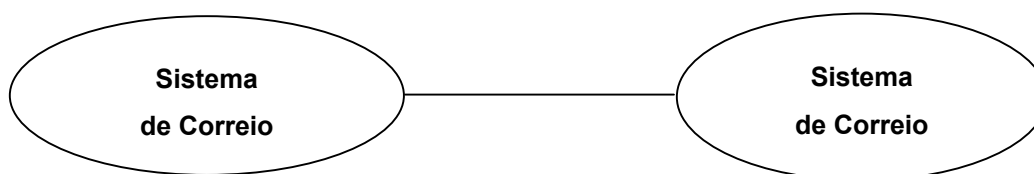
Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Protocolo de troca de informações	SOAP v1.2, como definido pelo W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/	R	
Infra-estrutura de registro	Especificação UDDI v3.0 (Universal Description, Discovery and Integration) definida pela OASIS http://www.uddi.org/specification.html	R	
Linguagem de definição do serviço	WSDL 1.1 (Web Service Description Language) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	R	

6.4. Mensagem Eletrônica (E-mail)

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

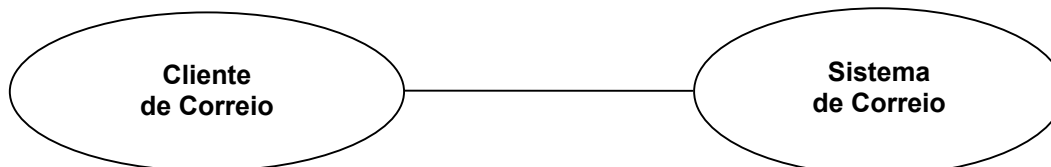
Transporte de Mensagem Eletrônica

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



Acesso à caixa postal

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



6.5. Migração para IPv6

A política da e-PING inclui a migração gradual para o IPv6, mantendo uma coexistência com o IPv4. Novas contratações e atualizações de redes devem prever suporte à coexistência dos protocolos IPv4 e IPv6 e a produtos que suportem os protocolos IPv4 e IPv6.

6.6. LAN Sem Fio

Existe uma crescente necessidade de computação móvel dentro do governo para permitir padrões de trabalho mais flexíveis. As soluções LAN sem fio, baseadas nas séries de padrão IEEE 802.11, são bem aceitas pelo mercado. Recomenda-se observar as especificações sobre segurança, contidas no capítulo 7 deste documento.

6.7. Mensageria em Tempo Real

Os padrões para mensageria em tempo real ainda estão surgindo. Quando a utilização de mensageria em tempo real for necessária, a orientação é adaptá-la ao Extensible Messaging and Presence Protocol (xmpp), como definido pelo IETF, RFC 2778, RFC 2779 e outras RFCs em desenvolvimento.

6.8. VPN

“Virtual Private Network” - VPN ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a Internet. Em vez de se utilizar links dedicados ou redes de pacotes para conectar redes remotas, utiliza-se a infra-estrutura da Internet.

A utilização da Internet, como infra-estrutura de conexão entre hosts da rede privada, é uma boa solução em termos de custos, mas não em termos de privacidade, pois a Internet é uma rede pública, onde os dados em trânsito podem ser lidos por qualquer equipamento.

Os túneis virtuais habilitam o tráfego de dados criptografados pela Internet e esses dispositivos são capazes de entender os dados criptografados, formando uma rede virtual segura sobre a Internet.

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.

7. Segurança

7.1. Segurança: Políticas Técnicas

7.1.1. Os dados, informações e sistemas de informação do governo devem ser protegidos contra ameaças de forma a reduzir riscos e garantir a integridade, confidencialidade e disponibilidade.

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

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

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

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

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

7.1.7. Os sistemas devem possuir registros históricos (logs) para permitir auditorias e provas forenses, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado.

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

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

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

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

7.1.12. Os Órgãos da APF, visando a melhoria da segurança, devem ter como referência a norma NBR ISO/IEC 17799 editada pela ABNT.

7.2. Segurança: Especificações Técnicas

Tabela 7.1 – Especificações Técnicas para Segurança de IP

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Transferência de dados em redes inseguras pelos protocolos HTTP, LDAP, IMAP, POP3, Telnet sempre que possível. – Segurança de	TLS - Transport Layer Security (RFC2246), disponível em http://www.cis.ohio-state.edu/htbin/rfc/rfc2246.html ou http://www.ietf.org/html.charters/tls-charter.html), caso seja necessário, o TLS v1 pode emular o SSL v3. HTTP sobre TLS (RFC 2818) http://www.ietf.org/rfc/rfc2818.txt	R	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
redes IPv4 na camada de transporte	<p>Podendo implementar os seguintes algoritmos criptográficos:</p> <ul style="list-style-type: none"> - Algoritmos para troca de chaves de sessão, durante o handshake: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA - Algoritmos para definição de chave de cifração: RC4, IDEA, 3DES - Algoritmos que implementam a função de Hash para definição do MAC: SHA, MD5 - Tipo de Certificado Digital - X.509 v3 - ICP-Brasil, http://www.iti.gov.br 		
Segurança de redes IPv4	<p>IPSec Authentication Header (RFCs 2402/2404) para autenticação de cabeçalho do IP.</p> <p>IKE – Internet Key Exchange (RFC 2409), 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 2406]) Requisito para VPN – Virtual Private Network.</p>	R	
Segurança de redes IPv4 para protocolos de aplicação	<p>O S/MIME v3 (RFC2633) deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.</p>	R	
Segurança de redes IPv6 na camada de rede	<p>O IPv6 (RFC 2460) apresenta implementações de segurança nativa no protocolo conforme texto abaixo.</p> <p>As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho (authentication header, [RFC 1826]) ou autenticação IP, e a segurança do encapsulamento IP (encrypted security payload, [RFC 1827]).</p> <p>A autenticação de cabeçalho assegura ao destinatário que os dados IP são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações. A autenticação utiliza um algoritmo chamado MD5 (Message Digest 5), especificado em [RFC 1828].</p> <p>A segurança do encapsulamento IP permite a autenticação dos dados encapsulados no pacote IP, através do algoritmo de criptografia DES (Data Encryption Standard) com chaves de 56 bits, definida em [RFC 1829].</p> <p>Os algoritmos de autenticação e criptografia citados acima utilizam o conceito de associação de segurança entre o transmissor e o receptor. Assim, o transmissor e o receptor devem concordar com uma</p>	R	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
	<p>chave secreta e com outros parâmetros relacionados a segurança, conhecidos apenas pelos membros da associação.</p> <p>Estes dois métodos podem ser utilizados em conjunto, a fim de fornecer tanto autenticidade quanto privacidade.</p>		
LAN sem fio	802.11g	R	O uso da nova especificação WPA (Wi-Fi Protect Access) com o padrão 802.11g deve ser incentivado, uma vez que a proteção oferecida pelo padrão WEP (Wired Equivalent Privacy) apresenta vulnerabilidades.

Tabela 7.2 – Especificações Técnicas para Segurança de 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 que trata da utilização do TLS com IMAP, POP3 e ACAP.	R	
Conteúdo de e-mail	O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 3369, RFC 2631, RFC 2632 e RFC 2633.	R	
Transporte de e-mail	Verificar se o reverso confere com o nome no HELO, para garantia da origem da mensagem e minimizar SPAM.	F(2)	
Assinatura	Utilizar padrão ICP-Brasil para a assinatura de e-mail, quando exigido. Em conformidade com o disposto no Decreto 3.996 de 31 de outubro de 2001.	R	

² Possível implicação na performance; possível descarte de mensagens válidas; impossibilidade de tratar múltiplos domínios.

Documento de Referência da e-PING – Versão 1.0

Tabela 7.3 – Especificações Técnicas para Segurança – Criptografia

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Algoritmo de cifração	3DES, AES	R	
Algoritmo de cifração	IDEA, SAFER+	T	
Algoritmo para assinatura	SHA-1 com RSA, MD5 com RSA e SHA-1 com DSA	R	
Algoritmo para hashing	MD5, SHA-1	R	
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	R	

Tabela 7.4 – Especificações Técnicas 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/2002/REC-xmlsig-core-20020212	R	
Cifração XML	Sintaxe e Processamento de Cifração XML (XMLenc) conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/	R	
Assinatura e cifração XML	Transformação de decifração para assinatura XML conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt	R	
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XML-Key Management Specification (XKMS 2.0) (Especificações de Gerenciamento de Chave XML) conforme definido pelo W3C http://www.w3.org/TR/xkms2/	R	
Autenticação e autorização de acesso XML	(SAML) conforme definido pelo OASIS quando um ambiente ICP é utilizado http://www.oasis-open.org/committees/security/index.shtml	R	
Navegadores	Somente utilizar testemunhas de conexão de caráter permanente (cookies) com a concordância do usuário. Resolução n. 7 do Comitê Executivo do Governo Eletrônico (Capítulo II, Art.7°).	A	

Tabela 7.5 – Especificações Técnicas 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. RFC 2251 (LDAP)	R	
DNS	Resolução no. 7 de 29/07/2002 – Comitê Executivo do Governo Eletrônico Práticas de Segurança para Administradores de Redes Internet NIC BR Security Office http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-chklist.pdf Versão 1.2 16 de maio de 2003 Securing an internet name server, CERT – ago/2002	R	
Transferência de arquivos de forma segura	FTP (RFC 959 e RFC 2228) HTTPS (RFC 2818)	R	
Newsgroup		F	
Mensagem instantânea	RFC 2778, RFC 3261, RFC 3261, RFC 3262, RFC 3263, RFC 3264 e RFC 3265.	E	
Sincronismo de tempo	Uso de informações do Observatório Nacional Protocolo descrito no documento “draft-ietf-stime- ntpauth-04.txt”: http://www.ietf.org/proceedings/03mar/I-D/draft-ietf-stime-ntpauth-04.txt	E	
Carimbo de tempo	Uso de informações do Observatório Nacional, Autoridades de Carimbo de Tempo (TSA) e protocolo descrito no documento “draft-ietf-stime-ntpauth- 04.txt”. RFC 3268 (Policy Requirements for Time-Stamping Authorities (TSAs), RFC 3161 (Time-Stamp Protocol), ETSI TS101861 (Time-Stamping Profile).	E	

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 deverão 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 deverá 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;
- deverão prever a substituição gradativa da sistemática de “login/senha” por mecanismos seguros de autenticação e de identificação dos usuários dos serviços do governo eletrônico, acrescentando preferencialmente a esses mecanismos um sistema de cartões inteligentes;
- deverão ser projetados de maneira que as informações essenciais de um serviço estejam acessíveis ao cidadão, mesmo quando do uso de meios de acesso com capacidade limitada, prevendo o uso de tecnologias que tornem esse acesso viável. No escopo deste documento, entende-se por meios de acesso com capacidade limitada⁽³⁾ aqueles que apresentem quaisquer das seguintes características: acesso com baixa velocidade de transmissão/recepção (mínimo aceitável – 28,8 kbps), estações de trabalho com capacidade reduzida (ciclo mínimo de processador aceitável – 233 MHz), memória RAM mínima de 128 MBytes, versões de navegadores web definidas como padrão mínimo no item “3. Políticas” e sistemas operacionais desatualizados ou de utilização específica;
- em sua versão inicial, a e-PING trata apenas dos seguintes meios de acesso:
 - estações de trabalho, considerando acesso aos usuários de forma direta ou indireta, por meio da prestação de serviços via balcão de atendimento;
 - cartões inteligentes, tokens e outros cartões;
- outros meios de acesso, como telefones celulares, hand-helds e televisão digital serão objeto de estudo futuro para determinação dos padrões aceitos pelo governo federal.

8.1.3. Os sistemas de informação do governo, construídos para suportar um determinado dispositivo de acesso, deverão 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 deverão ser capazes de utilizar a Internet como meio de comunicação, seja diretamente ou por meio de serviços de terceiros.

8.1.5. Quando a Internet for usada como meio de comunicação, os sistemas de informação do governo serão projetados de maneira que o máximo de informações possa ser trabalhado a partir do padrão mínimo de navegador (cf. item 3. Políticas), considerando-se as exceções que envolvam questões de segurança no tratamento de informações.

³ A definição de meios de acesso com capacidade limitada leva em consideração a realidade do país em relação ao uso dos recursos de TIC. Será atualizada a cada nova versão da e-PING. Em versões futuras serão incluídos padrões internacionalmente utilizados e aceitos como referência.

Documento de Referência da e-PING – Versão 1.0

8.1.6. 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.

8.1.7. Os serviços de governo eletrônico deverão 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/>

8.1.8. 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 (cf. item 3.Políticas) e para tornar viável o uso de quiosques públicos, de balcões de atendimento e de Centrais de Atendimento ao cidadão (como, por exemplo, Telecentros).

8.1.9. 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: http://www.governoeletronico.e.gov.br/arquivos/Resolucao_N_7_Diretrizes_para_Sitios_Internet.pdf

8.1.10. 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.

8.1.11. As especificações iniciais sobre cartões inteligentes, apresentadas neste trabalho, receberam como acréscimo o trabalho construído pelo 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). 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.

8.1.12. 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.

8.1.13. 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.

Documento de Referência da e-PING – Versão 1.0

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

Tabela 8.1 – Especificações Técnicas – Estação de Trabalho(4)

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Navegadores (<i>browsers</i>)	Ver item 3. Políticas	E	
Conjunto de caracteres e alfabetos	UNICODE standard versão 4.0, latin-1, UTF8, ISBN 0-321-18578-1	R	
Formato de intercâmbio de hipertexto	.html/.htm, incluindo os arquivos tipo “htm” gerados por servidores específicos, independente de suas extensões	R	
	.xhtm	R	
	.shtm	R	
	.xml	R	
	.mht	T	
Arquivos do tipo documento	.xml, com formatação (opcional) xsl	R	
	.sxw, gerado no formato do Open Office, versão 1.0 ou superior	R	
	.rtf	R	
	.pdf, gerado no formato do Adobe Acrobat, versão 4 ou superior	R	
	.txt	R	
	.htm/.html	R	
	.doc, gerado no formato do MS Office, versão 97 ou superior	T	
	.sdw, gerado no formato do Star Office, versão 5.2 ou superior	T	
Arquivos do tipo planilha	.sxc, gerado no formato do Open Office, versão 1.0 ou superior	R	
	.sdc, gerado no formato do Star Office, versão 5.2 ou superior	T	
	.xls, gerado no formato do MS Office, versão 97 ou superior	T	
Arquivos do tipo apresentação	.sxi, gerado no formato do Open Office, versão 1.0 ou superior	R	

⁴ A menção aos produtos que geram os formatos de arquivos citados 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.

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
	.htm/.html	R	
	.sdd, gerado no formato do Star Office, versão 5.2 ou superior	T	
	.ppt /.pps, gerado no formato do MS Office, versão 97 ou superior	T	
Arquivos do tipo “banco de dados” para estação de trabalho	.xml	R	Nas opções texto plano (txt) e csv, deve ser incluído obrigatoriamente o leiaute dos campos, de forma a possibilitar seu tratamento.
	.myd, .myi, gerados nos formatos do MySQL, versão 4.0 ou superior	R	
	.txt	R	
	.csv	R	
	.sdb, gerado no formato do Star Office, versão 5.2 ou superior	T	
	.mdb, gerado no formato do MS Office, versão 97 ou superior	T	
Intercâmbio de informações gráficas e imagens estáticas	.png	R	
	.tif	R	
	.svg	R	
	.jpg, versão 1 ou superior	R	
	.sxd, gerado no formato do Open Office, versão 1.0 ou superior	R	
	.xcf, gerado no formato do GIMP, versão 1 ou superior	R	
	.bmp	T	
	.gif	T	
	.cpt, gerado no formato da suíte Corel Draw, versão 7 ou superior	T	
	.psd, gerado no formato do Adobe Photoshop, versão 4 ou superior	T	
Gráficos vetoriais	.sxd, gerado no formato do Open Office, versão 1.0 ou superior	R	
	.svg, gerado no formato do Sodipodi, versão 1 ou superior	R	
	.cdr, gerado no formato da suíte Corel Draw, versão 7 ou superior	T	
	.msx, gerado no formato da suíte Corel Draw, versão 7 ou superior	T	
	.vss, .vsd, gerados no formato do Visio, versão 97 ou superior	T	
	.wmf	T	
Especificação de padrões de animação	.svg	R	
	.gif (gif animada – formato 89A)	T	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
	.swf, gerado no formato do Macromedia Flash, versão 4 ou superior, ou pelo Macromedia Shockwave, versão 1 ou superior	T	
Arquivos do tipo áudio e do tipo vídeo	.mpg	R	
	.mp4	R	
	.mid	R	
	.ogg	R	
	.avi, com codificação Xvid	R	
	.avi, com codificação divX	T	
	.mp3	T	
	.rm, gerado no formato dos aplicativos Real Audio Media Player, versão 8 ou superior	T	
	.ra, gerado no formato dos aplicativos Real Audio Media Player, versão 8 ou superior	T	
	.ram, gerado no formato dos aplicativos Real Audio Media Player, versão 8 ou superior	T	
	.rmm, gerado no formato dos aplicativos Real Audio Media Player, versão 8 ou superior	T	
	.avi	T	
	.wav	T	
	.swf, gerado no formato do Macromedia Flash, versão 4 ou superior ou pelo Macromedia Shockwave, versão 1 ou superior	T	
	.wmv, gerado no formato do Windows Media Player, versão 6.4 ou superior	T	
	.wma, gerado no formato do Windows Media Player, versão 6.4 ou superior	T	
	.mov, gerado no formato do Apple Quicktime, versão 6 ou superior	T	
	.qt, gerado no formato do Apple Quicktime, versão 6 ou superior	T	
Compactação de arquivos de uso geral	.zip	R	
	.tgz	R	
	.gz	R	
	.tar	R	
	.cab	T	
Georreferenciamento-padrões de arquivos para estações de trabalho	Assunto em estudo	E	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Observações
Programação Estendida (Plug-ins)	Assunto para consideração futura	F	

8.3. Meios de Acesso: Especificações Técnicas para Smart Cards, Tokens e Cartões em Geral

Tabela 8.2 – Especificações para Meios de Acesso – Smart Cards (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	Definições – Grupo de Trabalho da ICP-Brasil, coordenado pelo Instituto Nacional de Tecnologia da Informação/Casa Civil: http://www.iti.br/twiki/bin/view/Main/ConsultaPublicaPadroesHardware	A	Todos os cartões e tokens que manejam certificados digitais	Após ser submetido à Consulta Pública, a versão atual será 1.1
	Cartões de identificação ISO/IEC 7816-6 Cartões de Circuito(s) Integrado(s) com contatos Parte 6: Elementos de dados inter-setorial	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 – Inter-sector electronic purse - Parte 3: Elementos e intercâmbio de dados Sistemas de cartão de identificação BS EN 1546-4 – Inter-sector electronic purse - Parte 4: Objetos de dados	F	Todos	A atual edição foi publicada em julho de 1999 A atual edição foi publicada em agosto de 1999

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	Dispositivos do tipo Token: especificados no GT da ICP-Brasil item 2.2 (a, b e c).	A	Dispositivos Tokens	
Aplicações incluindo multi-aplicações	Cartões de identificação ISO/IEC 7816-4 Parte 4: Comandos inter-setoriais para intercâmbio	A	Cartões de Circuito(s) Integrado(s) com contatos	<p>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.</p> <p>Conforme escolha do GT da ICP-Brasil.</p> <p>A atual edição foi publicada em junho de 1994. Existe também uma alteração ISO/IEC 7816-5/AM1 Registered Application Provider Identifiers (RDIs) (Identificadores de Provedores de Aplicações Registradas) que foi publicada em dezembro de 1996</p>
	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 inter-setoriais para Structured Card Query Language (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	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	<p>Cartões de identificação ISO/IEC 15693-4 Cartões de circuito(s) integrado(s) sem contato, Cartões de proximidade {Vicinity Integrated Circuit(s) Cards (VICC) (Cartões de Circuito(s) Integrado(s) de Proximidade}</p> <p>Parte 4: Registro de aplicações/emissores</p>	R	Cartões de circuito integrado de proximidade	
	<p>Sistemas de cartão de identificação EN 1332-1:1999 – Interface homem-máquina - Parte 1: Princípios de projeto para interface de usuário</p> <p>Sistemas de cartão de identificação EN 1332-4:1999 – Interface Homem-máquina - Parte 4: Codificação de exigências de usuário para pessoas com necessidades especiais.</p>	R	Todos	
Elétrico	<p>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.</p> <p>ISO/IEC 7816—12</p> <p>Parte 12: Interface USB</p>	R	Cartões de circuito(s) integrado(s) com contatos	
	<p>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</p>	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.

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	<p>Cartões de identificação ISO/IEC 10536-3 Cartões de circuito(s) integrado(s) sem contato {Close Coupling Integrated Circuit(s) Cards (CICC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)}</p> <p>Parte 3: Procedimento de sinais eletrônicos e reinicialização.</p>	F	Cartões de circuito(s) integrado(s) de acoplamento forte	
	<p>Cartões de identificação ISO/IEC 15693-2 Cartões de circuito(s) integrado(s) sem contato.</p> <p>Cartões de Proximidade {Vicinity Integrated Circuit(s) Cards (VICC) (Cartões de Circuito(s) Integrado(s) de Proximidade):</p> <p>Parte 2: Interface e inicialização pelo ar;</p>	R	Cartões de circuito(s) integrado(s) de proximidade sem contato	
Protocolos de comunicações	<p>Cartões de identificação ISO/IEC 7816-3 Parte 3: Protocolos de sinais e transmissões eletrônicas.</p>	R	Cartões de circuito(s) integrado(s) com contatos	Conforme escolha do GT da ICP-Brasil
	<p>Cartões de identificação ISO/IEC 14443-3 - Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade – Parte 3: Inicialização e anti-colisão.</p> <p>Cartões de identificação ISO/IEC 14443-4 - Cartões de circuito(s) integrado(s) sem contato- cartões de proximidade – Parte 4: Protocolos de transmissão.</p>	R	Cartões de circuito(s) integrado(s) de proximidade	<p>Esta parte dá continuidade ao duopólio dos Tipos A e B, definindo procedimentos de inicialização e anti-colisão de cartões e protocolos básicos de comunicações. Os procedimentos de anti-colisão são métodos utilizados para identificar e selecionar um cartão quando vários cartões estiverem ativos dentro do campo RF do terminal.</p> <p>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.</p>

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	Cartões de identificação ISO/IEC 15693-3 , - Cartões de circuito(s) integrado(s) sem contato – cartões de proximidade – Parte 3: Protocolo de anti-colisão 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 {Close Coupling Integrated Circuit(s) Cards (CCIC) (Cartões de Circuito(s) Integrado(s) de Acoplamento Forte)}	F	Cartões de circuito(s) integrado(s) de acoplamento forte	
	Parte 4: Resposta a protocolos de reinicialização e transmissão.			
Os Padrões de físico/físico e de interface cobrem as dimensões do cartão;	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.

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
localidade e layout de contatos.	<p>Cartão Magnético</p> <p>ISO/IEC 7811, partes 2, 4 e 5: definem as propriedades, posicionamento e codificação (coding) da banda magnética do cartão.</p>	R	Todos os cartões com banda magnética	
	<p>Cartão de memória ótica</p> <p>ISO/IEC 11693 e 11694</p>	F	Cartões óticos	Cartões que suportam o armazenamento de muitos megabytes
	<p>Cartões de identificação ISO/IEC 7816-1</p> <p>Parte 1: Características físicas</p> <p>Cartões de identificação ISO/IEC 15693-1 - Cartões de circuito(s) integrado(s) sem contato – Cartões de proximidade - Parte 1: Características físicas. Esta part</p> <p>Cartões de identificação ISO/IEC 7816-2 Cartões de circuito(s) integrado(s) com contatos</p> <p>Parte 2: Dimensões e localização dos contatos</p>	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.
	<p>Cartões de identificação ISO/IEC 14443-1 - Cartões de circuito(s) integrado(s) sem contatos – Cartões de proximidade - Parte 1: Características físicas</p>	R	Cartões de circuito integrado de proximidade	Esta parte suplementa as características físicas definidas no ISO/IEC 7810
	<p>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</p>	R	Cartões de circuito(s) integrado(s) de proximidade sem contato	Esta parte do ISO/IEC 15693 foi publicada em 15-07-2000

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	<p>Cartões de identificação ISO/IEC 10536-1 Cartões de circuito(s) integrado(s) sem contato</p> <p>Parte 1: Características físicas;</p> <p>ISO/IEC 10536-2</p> <p>Parte 2: Dimensões e localização das áreas de acoplamento</p>	F	Cartões de circuito(s) integrado(s) de acoplamento forte	
	<p>Identificadores táteis</p> <p>Sistemas de Cartões de identificação BS EN 1332-2 – Interface homem-máquina</p> <p>Parte 2: Dimensões e localização - um identificador tátil para cartões ID-1</p>	F	Quando a gravação em relevo não é 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.	Alguns equipamentos de personalização de cartões, a menos que modificados, 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 inter-setoriais</p> <p>ISO/IEC 7816-9</p> <p>Parte 9: Comandos adicionais inter-setoriais e atributos de Segurança</p> <p>Cartões de identificação ISO/IEC 7816-11</p> <p>- Cartões de circuito(s) integrado(s) com contatos</p> <p>- 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	.

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	<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	
Infra-estrutura do terminal	<p>Sistemas de cartões de identificação EN 1332-3:1999 – Interface Homem-máquina - Parte 3: Teclados</p>	R	Todos	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	<p>Padrões PC/SC</p> <p>Padrões do Consórcio</p> <p>Grupo de Trabalho PC/SC</p> <p>Especificação de Interoperabilidade para ICCs e Sistemas de Computador Pessoal</p> <p>Parte 1. Introdução e Visão Geral da Arquitetura</p> <p>Parte 2. Requisitos de Interface para Cartões Compatíveis com CI e Dispositivos de Interface</p> <p>Parte 3. Requisitos para Dispositivos de Interface Conectados a PC</p> <p>Parte 4. Considerações do projeto IFD e Informação de Referência do Projeto</p> <p>Parte 5. Definição do Gerenciador de Recursos ICC</p> <p>Parte 6. Definição do Interface do Fornecedor de Serviço ICC</p> <p>Parte 7. Considerações do Projeto de Domínio / Desenvolvedor da Aplicação</p> <p>Parte 8. Recomendação para a Implementação de Dispositivos de Segurança e Privacidade ICC.</p>	A	Todos	Para uso geral em PCs.
	<p>GT da ICP-Brasil. Itens 5, 6 e 7:</p> <p>Item 5: Geração de Chaves.</p> <p>Item 6: Segurança na Utilização das Chaves</p> <p>Item 7: Padrões de Armazenamento</p>	A	Cartões com capacidade de gerenciamento de certificados digitais	

Documento de Referência da e-PING – Versão 1.0

Componente	Especificação	SIT	Aplicável a	Observações
	Padrão FIPS-140-1 e 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. Seguir no mínimo as regras estabelecidas para o nível 2 de segurança para verificação de violação do hardware.
Cartões tipo Java Card®	<p>API (<i>Application Programming Interface</i>) para a plataforma de cartões Java Card.</p> <p>Especificação para o ambiente de execução (<i>runtime environment</i>) para a plataforma Java Card.</p> <p>Especificação para a máquina virtual para a plataforma Java Card.</p>	A	<p>Esta API define um conjunto de classes a partir das quais a tecnologia Java Card baseada em <i>applets</i> pode ser construída.</p> <p>Esta especificação descreve o ambiente requerido para a execução de <i>applets</i> baseado em cartões Java Card.</p> <p>Esta especificação define a configuração requerida para a máquina virtual do cartão.</p>	<p>Versão geral para a tecnologia Java Card é 2.2.1 (outubro de 2003), http://java.sun.com/products/javacard/.</p>

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 e Esquemas XML para intercâmbio de dados.

9.1.2. Uso de UML para modelagem 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 9.1 – Especificações para Organização e Intercâmbio de Informações

Componente	Especificação	ST	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Linguagem para intercâmbio de dados	XML (Extensible Markup Language) como definido pelo W3C http://www.w3.org/XML	R	
Transformação de dados	XSL (Extensible Stylesheet Language) como definido pelo W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) como definido pelo W3C http://www.w3.org/TR/xslt	R	
Modelagem dos dados para intercâmbio	UML (Unified Modeling Language) conforme definido pelo OMG http://www.omg.org/gettingstarted/specsandprods.htm/	R	
Descrição de dados	RDF (Research Description Framework) Conforme 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	E	
Definição de dados	Catálogo de Dados de Uso Comum	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 9.1. Quando apropriado, é aceitável a utilização de middleware de acordo com a ilustração da Figura 9.2.

Documento de Referência da e-PING – Versão 1.0

Embora as configurações abaixo apresentem soluções potenciais, o modelo XML direto (Figura 9.1) é preferencial, sendo possível a utilização do modelo indireto, apresentado na Figura 9.2, em casos onde existam razões fundamentais que justifiquem seu uso.

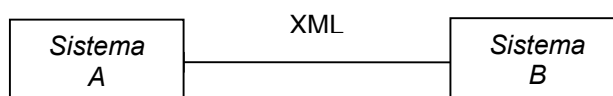


Figura 9.1 – Modelo XML Direto - Intercâmbio Direto

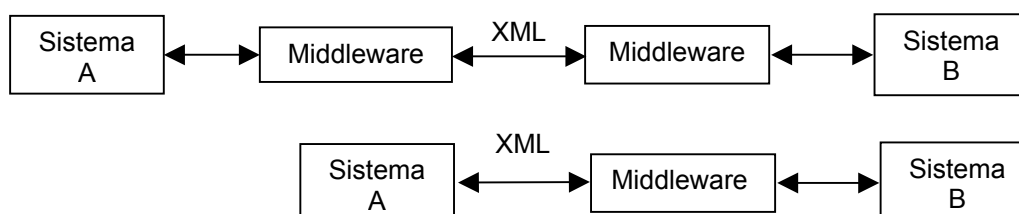


Figura 9.2 – Intercâmbios via middleware

9.4. Notas sobre Assuntos em Estudo e Elaboração

Catálogo de Dados de Uso Comum

A construção de um Catálogo de Dados de Uso Comum do Governo Brasileiro, elegendo e definindo os elementos estruturais para a viabilização da interoperabilidade do governo na sua relação dentro do governo e com a sociedade (cidadãos e empresas), será fundamental no desenvolvimento de Esquemas XML e outros processos de intercâmbio de dados.

A definição e padronização de dados de uso comum permitirá compartilhar conceitos, remover ambigüidades e inconsistências no uso dos dados governamentais.

O Catálogo será composto de 2 volumes:

- o volume 1 que apresentará os princípios gerais para estabelecimento dos dados de uso comum; e
- o volume 2 que será propriamente o catálogo de dados de uso comum, com as descrições dos dados aceitos como padrão.

Cada Dado eleito deverá ser documentado de acordo com um gabarito, como o exemplo abaixo. O gabarito será definido quando da elaboração do volume 1:

Metadados	Especificação
Faz parte de	
Tem partes	
Versão	
Status	
Data de aceitação	

Descrição	
Tipo de elemento	
Formato lógico	
Esquema XML	
Validação	
Valores	
Valor pré-definido	
Proprietário	
Baseado em	
Verificação	
Comentários	
Data de Publicação	

Documento de Referência da e-PING – Versão 1.0

Lista de Assuntos do Governo: Taxonomia para Navegação (LAG)

Órgãos do governo disponibilizam informações e serviços em portais e sítios da web, porém a complexidade da estrutura governamental pode tornar a localização da informação uma tarefa árdua.

A Lista de Assuntos do Governo: Taxonomia para Navegação (LAG), está sendo criada para ajudar pessoas a encontrar informações independente do conhecimento da estrutura do governo ou de qual órgão é responsável pelo assunto.

Os mecanismos utilizados nos populares diretórios da Internet são os mais conhecidos exemplos de listas de categorias.

O foco da LAG é o CIDADÃO. O objetivo da lista é facilitar ao cidadão a busca dos assuntos do seu interesse na larga faixa de informações do setor público. Portanto, a LAG:

- Prefere a linguagem do leigo ao jargão do Serviço Público ou aos termos técnicos;
- Não assume que o cidadão tenha conhecimento prévio das responsabilidades de cada nível ou órgão governamental. Tenta ser independente da estrutura governamental, devendo sobreviver às mudanças de estrutura e organogramas;
- Considera que o uso freqüente é mais importante do que precisão acadêmica.

O Grupo de Trabalho do segmento Organização e Intercâmbio de Informação da e-PING estabeleceu uma metodologia para construção e manutenção da LAG e está elaborando uma proposta de sua versão inicial a qual será publicada no sítio da e-PING em documento separado deste Documento de Referência.

A LAG completa prevê o detalhamento até o quarto nível. A título de exemplo, apresentamos abaixo, os termos de primeiro nível:

LAG - Termos de Primeiro Nível

1. Pessoa, Família e Comunidade
2. População e Sociedade
3. Educação
4. Ciência, Informação e Comunicação
5. Trabalho
6. Direito, Justiça e Leis
7. Política
8. Saúde, Higiene e Nutrição
9. Cultura, Lazer e Esporte
10. Habitação, Saneamento e Urbanismo
11. Meio Ambiente
12. Agricultura, Extrativismo e Pesca
13. Indústria
14. Comércio e Serviços
15. Transportes e Telecomunicações
16. Economia e Finanças
17. Segurança
18. Relações Internacionais
19. Administração Pública

Padrão de Metadados para o Governo Eletrônico (e-PMG)

A simplificação da busca por informações deve ser uma meta primordial dos governos desta Era da Informação. Esta constatação estimula a criação de um Padrão de Metadados para o Governo Eletrônico (e-PMG), ainda em estudo.

Documento de Referência da e-PING – Versão 1.0

Metadados são dados relativos a outros dados, isto é, dados estruturados e codificados que descrevem e permitem encontrar, gerenciar, compreender e preservar outros dados ao longo do tempo.

O e-PMG será baseado no modelo Internacional Dublin Core (ISO 15836) e em outros modelos internacionalmente aceitos.

10. Áreas de Integração para Governo Eletrônico

Este segmento da e-PING busca identificar, nas áreas de atuação do governo, os processos que demandam integração e intercâmbio de informações e os atores envolvidos, para o posterior estabelecimento e publicação de padrões e políticas técnicas que viabilizem a oferta de serviços de e-gov para o governo e a sociedade.

10.1 Áreas de Integração para Governo Eletrônico: Políticas Técnicas

Serão mapeados e priorizados os processos que permitam o desenvolvimento de serviços que requeiram a participação de diversos órgãos e entidades.

As diretrizes para o segmento são:

- A identificação de áreas, processos ou serviços que tragam benefícios diretos ou indiretos ao cidadão - são considerados benefícios indiretos aqueles que tragam melhoria à máquina administrativa do governo federal;
- O alinhamento dos padrões de cada área aos padrões internacionais, com atenção especial àqueles que permitirão a interoperabilidade entre órgãos, no escopo de relacionamento de governo definido no item deste documento.

Para cada uma das áreas, processos ou serviços considerados prioritários e essenciais para a interoperabilidade do governo, serão estabelecidos padrões, representados principalmente por Esquemas XML definidos e administrados de forma a possibilitar sua divulgação centralizada e utilização compartilhada.

Esses esquemas serão definidos e construídos por especialistas em cada processo, sob coordenação do órgão gestor de respectivo processo. A construção dos padrões deverá acompanhar as ações e especificações dos vários organismos nacionais e internacionais de padronização, comunidades de negócio e outros grupos, objetivando atender às políticas definidas para a e-PING, como por exemplo, o alinhamento com a Internet, o suporte de mercado e a escalabilidade.

O fator essencial na produção de um esquema XML é o adequado tratamento dos requisitos do processo tratado. Estes estabelecem, de uma perspectiva de negócios - dos processos - as requisições e as respostas de dados que o esquema XML necessita suportar.

Os trabalhos decorrentes deste segmento da e-PING possibilitarão identificar oportunidades para racionalizar processos e tratamento de dados, na busca contínua de maior benefício para o cidadão e do aprimoramento dos processos administrativos do governo.

Iniciativas existentes que contemplem total ou parcialmente os padrões da e-PING, serão objeto de investigação junto aos respectivos gestores visando análise das condições para formalização no âmbito do presente segmento.

Como proposta para identificação de processos, serviços, sistemas e seus atores, para o estabelecimento e publicação de normas e padrões de intercâmbio de informações, apresenta-se a seguinte relação das Áreas Temáticas de Atuação do Governo:

- SOCIAL
- SAÚDE, HIGIENE E NUTRIÇÃO
- SEGURANÇA PÚBLICA
- EDUCAÇÃO
- ADMINISTRAÇÃO E GESTÃO
- HABITAÇÃO
- CIÊNCIA E TECNOLOGIA
- TURISMO
- COMÉRCIO EXTERIOR
- DEFESA NACIONAL
- ECONOMIA E FINANÇAS

Documento de Referência da e-PING – Versão 1.0

- CULTURA
- MEIO AMBIENTE
- PREVIDÊNCIA SOCIAL
- TRABALHO
- TRANSPORTES
- ENERGIA
- AGRICULTURA E ORGANIZAÇÃO AGRÁRIA
- COMUNICAÇÃO
- DIREITO, JUSTIÇA E LEIS

Essa relação de áreas tem caráter estritamente informativo, fornecendo um parâmetro de enquadramento para os processos de integração identificados como prioritários para estudo.

Na identificação e explicitação dos processos que demandam a integração e intercâmbio de informações, serão identificados e relacionados entidades e atores envolvidos, de modo aderente aos relacionamentos existentes na prestação do serviço de e-gov.

A identificação e priorização dos processos contemplados e instituídos no âmbito das áreas temáticas de atuação de e-gov, deverão ser feitas juntamente com os Comitês Técnicos de Governo Eletrônico vinculados ao CEGE - Comitê Executivo de Governo Eletrônico.

Caberá aos representantes dos Ministérios, Comitês Técnicos, e outros segmentos interessados, identificar as iniciativas afetas à sua área de atuação setorial, bem como indicar as entidades e os órgãos envolvidos (atores).

Metodologia para o estabelecimento e manutenção dos padrões de interoperabilidade no âmbito do presente segmento e-PING

Para cada área temática de atuação governamental, em consonância com prioridades de governo e considerados os tipos de relacionamento, proceder-se-á às seguintes etapas:

- 1. Identificar** a partir do levantamento dos processos que demandam padrões de interoperabilidade, os seguintes itens:
 - Unidades de Informação que sejam usadas em intercâmbio;
 - Áreas Temáticas de Atuação de e-gov;
 - Tipos de relacionamentos envolvidos (GpG, GpC, GpE etc.);
 - Entidades Envolvidas no estabelecimento dos padrões;
 - Entidade Responsável ou Gestora de cada processo;
 - Principais resultados esperados do processo de integração, e
 - Situação da iniciativa (avaliação de abertura de projeto, projeto em andamento etc).
- 2. Apontar** serviços, projetos, processos de negócio, eventos, transações, fluxos de informações e comunidades de usuários, que sejam pertinentes ao processo identificado.
- 3. Criar e supervisionar** Grupos de Trabalho para atuação em cada processo identificado.
- 4. Submeter** os padrões propostos ao processo de homologação definido pela e-PING, para posterior publicação e manutenção evolutiva.

A relação das Áreas Temáticas de Atuação de Governo e dos respectivos processos prioritários bem como informações levantadas ao longo da aplicação da metodologia proposta pode ser consultada no endereço www.eping.e.gov.br/areaseprocessos.

Documento de Referência da e-PING – Versão 1.0

É recomendável que as iniciativas de integração contemplem os seguintes aspectos:

- Especificação de infra-estrutura de integração, em conformidade com os demais segmentos da e-PING;
- Documentação dos processos de integração referentes à área temática, considerando o emprego de linguagens para modelagem de processos de negócio;
- Diagramas UML para modelagem dos dados correlatos aos eventos de integração;
- Esquemas XML, para documentar intercâmbios de dados;
- Documentos XSL e/ou XSLT para representar as transformações de dados no âmbito dos eventos de integração;

Os padrões referidos nos itens (c) a (e) devem estar em conformidade com as políticas e especificações técnicas apontadas no Segmento Organização e Intercâmbio de Informações da e-PING.

Além dos documentos referidos, os dados que forem identificados na implementação da integração das iniciativas prioritárias como de interesse comum do governo, devem ser encaminhados para fazerem parte do Catálogo de Dados de Uso Comum.

10.2 Áreas de Integração para Governo Eletrônico: Especificações Técnicas

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

Tabela 10.1 – Especificações para Áreas de Integração para Governo Eletrônico

Componente	Especificação	ST	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo F = Estudo Futuro		
Linguagens para Modelagem de Processos e Execução de Processos	Assunto em estudo.	E	Será feita a avaliação dos diversos padrões de linguagens de modelagem de processos e linguagens de execução de processos para web services que tenham suporte de mercado
Padrão de Linguagem para Intercâmbio de informações geográficas – georreferenciamento	Assunto em estudo.	E	Serão utilizados como base as recomendações do Open Geospatial Consortium, Inc. (OGC) - http://www.opengis.org . Será realizado levantamento no âmbito do governo com objetivo de definir as necessidades dos órgãos que já utilizam serviços com esta tecnologia.

11. Glossário de Termos Técnicos

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

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 Esquemas XML: diretório de informações sobre os Esquemas XML.

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.

Dispositivo: componente físico (estação de trabalho, telefone celular, cartão inteligente, handheld, 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.

Esquemas XML: 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>

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.

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.

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.

Documento de Referência da e-PING – Versão 1.0

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

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

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

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

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

IP – Internet Protocol (Protocolo de Internet): método ou protocolo através dos quais os dados são enviados de um computador a outro na Internet. Cada computador, na Internet, possui pelo menos um endereço IP que o identifica unicamente em relação a todos os outros computadores da Internet.

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

IPv4 – Internet Protocol Version 4 (Protocolo de Internet Versão 4): ver “IPv6”.

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

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

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

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

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

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

Documento de Referência da e-PING – Versão 1.0

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.

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

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

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

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

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

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

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

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

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

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

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

1. Prestação eletrônica de informações e serviços.
2. Regulamentação das redes de informação, envolvendo principalmente governança, certificação e tributação.
3. Prestação de contas públicas, transparência e monitoramento da execução orçamentária.
4. Ensino à distância, alfabetização digital e manutenção de bibliotecas virtuais.
5. Difusão cultural com ênfase nas identidades locais, fomento e preservação de culturas locais.

Documento de Referência da e-PING – Versão 1.0

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 infra-estrutura (transporte, comunicações, energia, administração de recursos naturais), Agricultura, Saúde, Educação, etc.

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

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 Multi-propósito 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 Multi-propósito): 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.

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 usa-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, organizada e estruturada hierarquicamente, de acordo com relações naturais ou presumidas, objetivando facilitar os 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.

Documento de Referência da e-PING – Versão 1.0

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 remonta-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): anotação padrão do modelo de objetos do mundo real como o primeiro passo no desenvolvimento de uma metodologia de design orientado a objetos.

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.

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.

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 Extensível): 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.

Documento de Referência da e-PING – Versão 1.0

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).

Referências bibliográficas:

Dicionário de tecnologia / editado por Lowell Thing;
[tradução Bazán Tecnologia e Linguística e Texto Digital]
São Paulo: Futura, 2003.
ISBN 85-7413-138-5

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

Câmara Técnica de Implementação do Software Livre
Planejamento Estratégico 2003–2004
Diretrizes, Objetivos e Ações Prioritárias

12. Créditos

Comitê Constituinte e-PING

Associação Brasileira de Empresas Estaduais de Processamento de Dados (ABEP)

Paulo Cezar Coelho

Banco do Brasil (BB)

José Maria Cyrineu Martins
Marco Aurélio Mota Loureiro

Caixa Econômica Federal (CAIXA)

Luiz Antônio dos Santos

DATAPREV

Carlos Alberto Jacques de Castro
Humberto Degrazia Campedelli
José Porphirio Araújo de Miranda

DATASUS

André Amaro Toffanello

Ministério das Comunicações (MC)

Roberto Bernardino Azevedo

Ministério do Planejamento – Secretaria de Logística e Tecnologia da Informação (MP/SLTI)

José Ney de Oliveira Lima
Leonardo Boselli da Motta
Nazaré Lopes Bretas
Rogério Machado Xavier (Coordenador Geral)
Rogério Santanna dos Santos
Sílvio César Damasceno Ferreira

Presidência da República – Instituto Nacional de Tecnologia da Informação – ITI/PR

Renato da Silveira Martini
Sérgio Amadeu

SERPRO

Ana Lúcia d'Aguiar
Antônio Sérgio Borba Cangiano
Elói Juniti Yamaoka
Luiz Gonzaga da Costa
Paulo César Czarnewski
Severino Lucchetti Neto

Grupo de Trabalho Interconexão

Luiz Gonzaga Costa (SERPRO) – Coordenador
Alexandre Hirle de Freitas (MEC)
Anderson Jardim Pereira (SERPRO)
Ângela Patrício de Lima (IBGE)
Carlos Alberto Carvalho Monteiro (CENSIPAM)
Carlos Alves Fernandes (DNIT)
Carlos Bellone Neto (SRF)
Daniel Bispo de Jesus (CODESP)
Diego Figueiredo Costa Viegas (MP)
Eder Manoel de Abreu (EMBRAPA)
Gilberto Parrine Sant'Ana (MP)
Hadib Gabriel Alves Itapá (MT)
Jailson Vieira Dantas (MI)

Documento de Referência da e-PING – Versão 1.0

Jorge Koury Bechara (PRODEPA-PA)
José Euclides da Silva Júnior (DATAPREV)
José Guilherme Barreto Ávila (PR)
José Sarto Mendes Carneiro Junior (SERPRO)
Kátia Bernardo Esteves (MC)
Lilian Amoyr de S. Khenayfis (ANCINE)
Luis Carlos de Paula Barcellos (MI)
Luiz Arthur Sampaio de Mesquita (ELETROBRÁS)
Marcelo Henrique Rios dos Reis (MT)
Moisés de Miranda Barreto (SERPRO)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Rosana da Silva Bulad (CGU)
Ruben César Macedo (CELEPAR-PR)
Salatiel Robson B. Oliveira (CGU)
Télio Luiz Pacheco (CAIXA)
Ulisses de Sousa Penna (BB)

Grupo de Trabalho Segurança

Humberto Degrazia Campedelli (DATAPREV) – Coordenador
Alerrandro Luís Augusto Caetano Corrêa (MEC)
Alexandre Almeida Lima (SEORI)
Alexandre Braga (CPqD)
Carlos Eduardo de Santos Souza (CENSIPAM)
Catarina da Matta (ELETROBRÁS)
Clari Dorça Stacciarini (CGU)
Cristiano Sakai (PR)
Daniel Bispo de Jesus (CODESP)
Ernandes Lopes Bezerra (MP/SLTI)
Etienne César Ribeiro de Oliveira (IBGE)
Joana D'arc Felipe dos Santos (MI)
João Carlos Levy Argel (FUNARTE)
Jorilson da Silva Rodrigues (MJ)
José Ney de Oliveira Lima (MP/SLTI)
Jovino Francisco Filho (MC)
Luiz Augusto Vieira de Melo (ANCINE)
Marco Aurélio Bonato (CELEPAR)
Marcos Allemand Lopes (SERPRO)
Marcos José da Silva (DATAPREV)
Nilson Carlos de M. Pontes (IBGE)
Renato Navajas (MDIC)
Ruy Siqueira de Moura (MRE)
Sérgio Carreira dos Santos (IPHAN)
Silvio Márcio Santos Nery (CGU)

Grupo de Trabalho Meios de Acesso

Renato da Silveira Martini (ITI) – Coordenador
Severino Lucchetti Neto (SERPRO) – Coordenador
Alessander Florindo da Silva (MS)
Ana Júlia Freitas Pinheiro (MI)
Ângela Cristina do Nascimento Gomes (IBGE)
Antônio Francisco Vieira (MRE)
Camila Alcântara Ribeiro (ITI)
Edgar Ladeira da Fonseca (CGU)
Eliane Aristóteles Moreira (DATAPREV)
Elias Nagib David (MC)
Fernando Coutinho Leite (ANCINE)
Gerson Mizuta Weiss (CPqD)

Documento de Referência da e-PING – Versão 1.0

Jefferson Willian Wagner Silva (ECT)
João Carlos Levy Argel (FUNARTE)
José Olímpio da Silva (VALEC)
Josilson Lopes de Souza (SRF)
Kleber Alves Carneiro (SERPRO)
Leonardo Guillén (MP/SLTI)
Leonardo R. Mello (MP/SLTI)
Luís Artur Monteiro de Carvalho (MF)
Luiz Antônio Patta Melão (MS)
Marcelo Augusto Santiago (Eletrobrás)
Márcio Haruzo Otta (CGU)
Márcio Lúcio Vasconcelos Donato (MI)
Odilon de Freitas Militão Neto (CAIXA)
Paulo Édison de Souza (MEC)
Ruy Siqueira de Moura (MRE)
Daniel Bispo de Jesus (CODESP)
Sônia Vasques Nogueira (IBGE)
Walmiro Muzzi (ITI)

Grupo de Trabalho Organização e Intercâmbio de Informações

Eloi Juniti Yamaoka (SERPRO) – Coordenador
Ana Lúcia D`Aguiar Vicente (SERPRO)
Ana Lúcia de Medeiros (CORREIOS)
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Cláudia Carvalho Masset Lacombe Rocha (ARQUIVO NACIONAL)
Cláudia Piovesan Macedo (CPqD)
Cláudio João de Faria Brito (MRE)
Daniel Bispo de Jesus (CODESP)
Gaetano Lo Mônaco (INEP)
Guilherme Luiz Melecchi (DATAPREV)
Hilda Guilherme Pimentel (ANCINE)
Jorge Luiz Caetano Lopes (CODOMAR)
José Euclides Júnior (DATAPREV)
José Gabriel Medef Filho (CGU)
Leonardo José Franca Silva (ANCINE)
Luciana Cabral de Carvalho (MJ)
Luciano Mendonça Menezes (MJ)
Luiz Antonio dos Santos (CAIXA)
Luiz Antônio Nery de Oliveira (DATAPREV)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Marcio Imamura (IBGE)
Marcos Augusto Francisco Borges (CPqD)
Margareth da Silva (ARQUIVO NACIONAL)
Maria Alice Barros (SRF)
Maria Célia Pelisson Jacon (IBGE)
Maria das Graças Comaru de Oliveira (SERPRO)
Neuza Arantes Silva (MAPA)
Paulo Cezar Czarnewski (SERPRO)
Paulo Henrique de Assis Santana (MMA)
Sérgio Silva dos Santos (MAPA)
Valéria Esther Nigri Musafir (SERPRO)
Vicente de Paula Teixeira (CGU)
Vivianne Veras Barrozo (SERPRO)

Documento de Referência da e-PING – Versão 1.0

Grupo de Trabalho Áreas de Integração para Governo Eletrônico

Nazaré Lopes Bretas (MP/SLTI) – Coordenadora
Ana Lúcia D' Aguiar Vicente (SERPRO)
Alexandre Vitor F. de Freitas (MI)
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)
Carlos Fernando de Mattos Barcellos (CODESA)
Celso Ricardo Hottum Meira (MRE)
Cláudio Thomé de Souza (BB)
Corinto Meffe (MP/SLTI)
Edgard de Souza Barros (ANTAQ)
Efraim Soares dos Santos (CAIXA)
Felipe Andrés Leon Garcia (MJ)
Gabriela Miglio do Carmo (CDP)
Gina Maria de Souza (MI)
José Antônio Soares Borba (MP/SLTI)
José Roberto Pereira Gomes (ANCINE)
Marcos Gonçalves (FRANAVE)
Maria Cecília Pullen Parente Badauy (ANTAQ)
Maria Cláudia Paiva (SERPRO)
Paulo César M. Simões (IBGE)
Paulo César Pereira Soares (FUNART)
Paulo Emerson de Oliveira Pereira (MP/SLTI)
Reneide Pereira dos Santos Garcia (CODERN)
Ricardo Sigaud (ELETROBRÁS)
Rosângela Villela Pedro (SRF)
Rubia Maria Pereira (EMBRAPA)
Sérgio Rodrigues Simões (CD/RJ)
Ubiramar Mendonça (DATAPREV)
Valéria Esther Nieri Musafir (SERPRO)
Wagner Garausi Guarizo (PR)