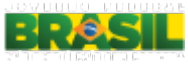
Ministério do Planejamento, Orçamento e Gestão
Secretaria de Logística e Tecnologia da Informação
Departamento de Governo Eletrônico
www.governoeletronico.gov.br

Padrões de Interoperabilidade de Governo Eletrônico

Documento Referência

Versão 2015



SUMÁRIO

Apresentação

A interoperabilidade pode ser entendida como uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.

A arquitetura ePING – 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 ePING estão segmentadas em:

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

Todo o conteúdo deste documento de referência está em consonância com as diretrizes do Comitê Executivo de Governo Eletrônico, criado pelo Decreto de 18 de outubro de 2000, e está publicado em sítio específico na Internet (http://www.governoeletronico.gov.br/eping), garantindo acesso público às informações de interesse geral e transparência intrínseca à iniciativa.

1. Escopo

A ePING é concebida como uma estrutura básica para a estratégia de governo eletrônico, aplicada ao governo federal – Poder Executivo, não restringindo a participação, por adesão voluntária, de outros Poderes e esferas de governo.

Para os órgãos do governo federal, Poder Executivo brasileiro, a adoção dos padrões e políticas contidos na ePING é obrigatória (Portaria SLTI/MP nº 92, de 24 de dezembro de 2014).

No âmbito das entidades supramencionadas, são obrigatórias as especificações contidas na ePING 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; e
- aquisição ou atualização de equipamentos de TIC.

2. Políticas Gerais

Relacionam-se a seguir as políticas gerais utilizadas na construção da ePING e que fundamentam as especificações técnicas de cada segmento, além de orientar os órgãos em suas soluções de interoperabilidade:

1. **Adoção Preferencial de Padrões Abertos**
   A ePING define que, sempre que possível, serão adotados padrões abertos nas especificações técnicas. Padrões proprietários são aceitos nas seguintes condições:
   - de forma transitória, mantendo se as perspectivas de substituição assim que houver condições de migração;
   - quando da inexistência de padrão aberto, na qual poderão ser adotados padrões proprietários até que um padrão aberto esteja disponível.

   Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações.

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

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

3. **Transparência**
   Segundo a Lei de Acesso à Informação (LAI), de novembro de 2011, o acesso é regra e o sigilo constitui uma exceção. A LAI reforça o uso da interoperabilidade na busca pela publicidade dos dados. Com mais informações disponíveis é possível minimizar o número de interações do cidadão com o governo.

4. **Segurança**
   A interoperabilidade na prestação dos serviços de governo eletrônico deve considerar o nível de segurança requerido pelo serviço.

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

2.1. Políticas Gerais nas Dimensões

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

Dimensão Técnica

- **Alinhamento com a INTERNET**

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

- **Adoção de navegadores (*browsers*)**

  Como meio de acesso, todos os sistemas de informação de governo deverão ser acessíveis, preferencialmente, por meio de tecnologia baseada em navegador, quando esta tecnologia se mostrar a mais adequada, dentre as tecnologias disponíveis, ao nível de segurança requerido pelo serviço. Outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores.

- **Escalabilidade**

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

Dimensão Semântica

- **Desenvolvimento e manutenção de ontologias e outros recursos de organização da informação**

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

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

- **Desenvolvimento e adoção de um padrão de modelagem de dados para Governo**

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

- **Desenvolvimento e adoção de uma política de disseminação de dados e informações**

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

Dimensão Organizacional

- **Simplificação administrativa**

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

- **Promoção da colaboração entre organizações**

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

- **Garantia à privacidade de informação**

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

3. Segmentação

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

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

3.1. Interconexão – Segmento 1

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

3.2. Segurança – Segmento 2

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

3.3. Meios de Acesso – Segmento 3

São explicitadas as questões relativas aos padrões dos dispositivos de acesso aos serviços de governo eletrônico.

3.4. Organização e Intercâmbio de informações – Segmento 4

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

3.5. Áreas de Integração para Governo Eletrônico – Segmento 5

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

4. Classificação das especificações técnicas

As especificações técnicas da ePING são classificadas em quatro níveis de situações que caracterizam o grau de aderência às políticas gerais da arquitetura.

Esses quatro níveis são os seguintes:

- **Adotado (A):** item adotado pelo governo como padrão na arquitetura ePING, tendo sido submetido a um processo formal de homologação realizado por parte de uma instituição do governo ou por uma outra instituição com delegação formal para realizar o processo. Também é considerado homologado quando baseado em uma proposição devidamente fundamentada pela coordenação do segmento, publicada no sítio e aprovado pela Comissão de Coordenação da ePING. Os componentes com padrão nível Adotado devem ser obrigatoriamente adotados em novos produtos/projetos de TI;
- **Recomendado (R):** item que atende às políticas técnicas da ePING, é reconhecido como um item que deve ser utilizado no âmbito das instituições de governo, mas ainda não foi submetido a um processo formal de homologação. Os componentes de nível Recomendados não são obrigatórios, porém sugeridos para adoção em novos produtos/projetos de TI;
- **Em Transição (T):** item que o governo não recomenda, por não atender a um ou mais requisitos estabelecidos nas políticas gerais e técnicas da arquitetura; é incluído na ePING em razão de seu uso significativo em instituições de governo, tendendo a ser desativado assim que algum outro componente venha a apresentar condições totais de substituí-lo. 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; e
- **Em Estudo (E):** componente que está em avaliação e poderá ser adotado, assim que o processo de avaliação estiver concluído.

5. Governança e Gestão da ePING

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

5.1. Papéis e responsabilidades

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

Comissão de Coordenação da ePING

- definir as diretrizes da ePING, deliberar sobre as políticas e especificações técnicas, bem como alterações e acréscimos em razão de sua revisão e de sua atualização;
- elaborar e divulgar orientações técnicas, inclusive na forma de manuais e materiais instrucionais;
- definir objetivos, identificar projetos, promover a colaboração entre os órgãos e propor medidas relativas ao planejamento e a implementação da ePING;
- manifestar-se sobre questões técnicas relacionadas com a adoção e a conformidade à ePING por órgãos e entidades integrantes do SISP e outros interessados;
- constituir grupos de trabalho temporários para a elaboração de propostas, diretrizes e especificações técnicas, de acordo com a necessidade;
- definir os temas a serem tratados pelos grupos de trabalho temporários, dentre os temas propostos à Comissão de Coordenação;
- declarar o encerramento de grupo de trabalho temporário;
- promover intercâmbio e cooperação técnica nacional e internacional na área de padrões de interoperabilidade; e
- fomentar iniciativas de divulgação e de capacitação de servidores públicos para a aplicação da ePING, visando a formação da cultura de interoperabilidade na Administração Pública Federal.

Secretaria Executiva da ePING

- prover a infraestrutura administrativa e os recursos orçamentários e financeiros necessários às atividades da ePING;
- apoiar o funcionamento da Comissão de Coordenação da ePING, dos segmentos e dos grupos de trabalho temporários;
- disponibilizar e manter atualizado o arcabouço digital da ePING: páginas, catálogos, gestão de comunidades, respostas às consultas públicas e outros serviços e informações relacionadas à ePING; e
- elaborar e disponibilizar pautas, atas, cronogramas de reuniões, lista de participantes, ofícios e outros documentos oficiais a serem expedidos pela Comissão de Coordenação da ePING.

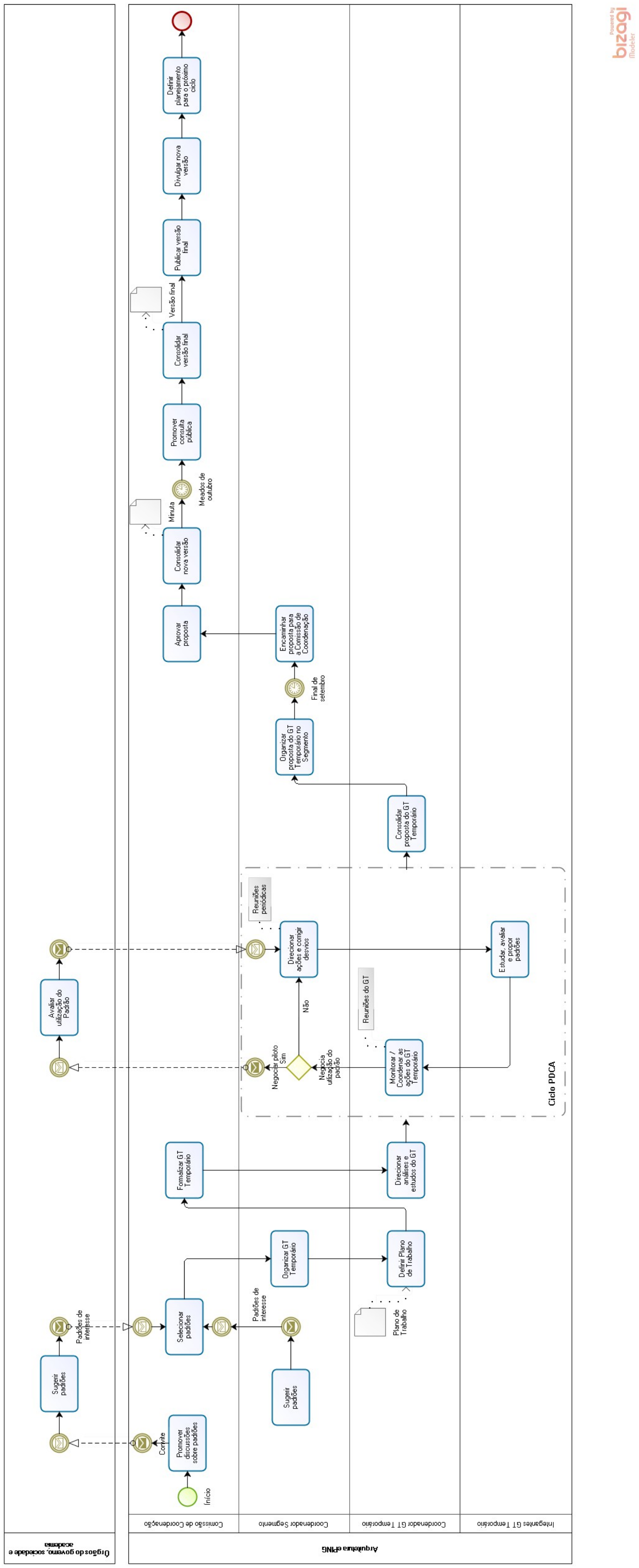
Coordenação dos Segmentos

- convidar especialista ou grupo(s) de especialistas para avaliação de padrões;
- manter comunidades de prática para fomentar a discussão nos assuntos de interesse do segmento;
- dimensionar necessidades e propor capacitação em áreas de interesse do segmento, indicando público-alvo;
- propor grupos de trabalho temporários à Comissão de Coordenação;
- analisar e emitir parecer sobre o(s) produto(s) dos grupos de trabalho temporários como insumo à decisão da Comissão de Coordenação; e
- manter atualizadas as tabelas de padrões do Segmento no Documento de Referência da ePING.

Coordenação dos Grupos de Trabalho Temporários

- Definir entregas e ações do grupo;
- Divulgar as entregas e ações;
- Monitorar/coordenar as ações do grupo; e
- Consolidar os resultados do grupo.

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


Órgãos do governo, sociedade e academia
Arquitetura ePING
Comissão de Coordenação
Coordenador Segmento
Coordenador GT Temporário
Integrantes GT Temporário
Início
Promover discussões sobre padrões
Convite
Sugerir padrões
Padrões de interesse
Selecionar padrões
Sugerir padrões
Padrões de interesse
Organizar GT Temporário
Definir Plano de Trabalho
Plano de Trabalho
Formalizar GT Temporário
Direcionar análises e estudos do GT
Monitorar / Coordenar as ações do GT Temporário
Reuniões do GT
Negocia utilização do padrão
Negocia piloto
Sim
Não
Avaliar utilização do Padrão
Direcionar ações e corrigir desvios
Reuniões periódicas
Estudar, avaliar e propor padrões
Ciclo PDCA
Consolidar proposta do GT Temporário
Organizar proposta do GT Temporário no Segmento
Final de setembro
Encaminhar proposta para Comissão de Coordenação
Aprovar proposta
Consolidar nova versão
Minuta
Meados de outubro
Promover consulta pública
Consolidar versão final
Versão final
Publicar versão final
Divulgar nova versão
Definir planejamento para o próximo ciclo

5.2. Descrição das Atividades

Esse processo tem o objetivo de descrever o modelo de governança e gestão da arquitetura ePING, relacionando as principais atribuições aos papéis que as desempenham.

- **Promover Discussões sobre padrões**
  Monitorar sistematicamente o mercado com o objetivo de detectar novas tecnologias que atendam as necessidades de atualização tecnológica das políticas e especificações técnicas sugerindo padrões a serem analisados pela ePING.

  Responsável: Comissão de Coordenação

- **Sugerir padrões**
  Identificar e sugerir padrões tecnológicos que atendam as necessidades dos responsáveis por essa atividade.

  Responsável: Órgãos do governo, sociedade, academia e coordenador Segmento

- **Selecionar padrões**
  Escolher dentre os padrões sugeridos quais serão estudados.

  Responsável: Comissão de Coordenação

- **Organizar GT Temporário**
  Definir quais segmentos fazem parte do GT Temporário, quem será seu coordenador e seus participantes.

  Responsável: Coordenador Segmento

- **Definir Plano de Trabalho**
  Definir as metas, ações e entregas do GT Temporário, consolidando essas informações em um plano de trabalho.

  Responsável: Coordenador GT Temporário

- **Formalizar GT Temporário**
  Publicar portaria com a criação do GT Temporário, indicando seus representantes, cronograma e entregas.

  Responsável: Comissão de Coordenação

- **Direcionar Análises e Estudos do GT**
  Direcionar a equipe do GT Temporário nos estudos e pesquisas dos padrões previstos sob sua responsabilidade.

  Responsável: Coordenador GT Temporário

- **Ciclo PDCA**
  Ciclo de desenvolvimento que tem foco na melhoria contínua dos trabalhos e padrões estudados.

  - **Monitorar / Coordenar as Ações do GT Temporário**
    Acompanhar as atividades e ações previstas no plano de trabalho.

    Responsável: Coordenador GT Temporário

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

      Responsável: Órgãos do governo, sociedade e academia

- **Direcionar Ações e Corrigir Desvios**
  Corrigir desvios, movimentando a equipe do GT Temporário com intuito de acelerar ou motivar pesquisas visando o cumprimento do plano de trabalho.

  Responsável: Coordenador Segmento

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

  Responsável: Integrantes do GT Temporário

- **Consolidar proposta do GT Temporário**
  Revisar e verificar a aderência do resultado do trabalho ao Plano de Trabalho acordado.

  Responsável: Coordenador GT Temporário

- **Organizar proposta do GT Temporário no segmento**
  Alinhar os trabalhos realizados pelos GT temporários com os conteúdos de cada segmento.

  Responsável: Coordenador Segmento

- **Encaminhar proposta para a Comissão de Coordenação**
  Submeter o resultado do trabalho do GT Temporário à Comissão de Coordenação.

  Responsável: Coordenador Segmento

- **Aprovar proposta**
  Analisar a proposta do GT Temporário e deliberar se será incorporada à nova versão da ePING.

  Responsável: Comissão de Coordenação

- **Consolidar nova versão**
  Atualizar o Documento de Referência com as novas propostas dos GT Temporários para submeter à consulta pública.

  Responsável: Comissão de Coordenação

- **Promover consulta pública**
  Colocar a nova versão da ePING em consulta pública, para receber contribuições e sugestões.

  Responsável: Comissão de Coordenação

- **Consolidar versão final**
  Após findar o prazo da consulta pública, todas as contribuições recebidas serão analisadas e consolidadas na versão final da ePING para o próximo ano.

  Responsável: Comissão de Coordenação

- **Publicar versão final**
  Publicar a nova versão da ePING no sítio do governo eletrônico no endereço http://www.governoeletronico.gov.br/eping.

  Responsável: Comissão de Coordenação

- **Divulgar nova versão**
  Contempla toda atividade de divulgação da ePING tanto as realizadas por meio do sitio como:

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

Responsável: Comissão de Coordenação

- **Definir Planejamento para o Próximo Ciclo**
  Atividade no qual é realizado o planejamento inicial a ser tratado no próximo ciclo da ePING.

  Responsável: Comissão de Coordenação

1. Interconexão

1.1. Especificações Técnicas

Tabela 1 – Aplicação[1]

Componente	Especificação	SIT
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo	
Endereços de caixa postal eletrônica	As regras para definição dos nomes das caixas postais de correio eletrônico deverão seguir ao estabelecido no documento "Padrão de Formação de Endereços de Correio Eletrônico - Caixas Postais Individuais", disponível no endereço eletrônico http://www.governoeletronico.gov.br/eping	**A**
Transporte de mensagem eletrônica	Utilizar produtos de mensageria eletrônica que suportam interfaces em conformidade com SMTP/MIME para transferência de mensagens. RFC correlacionadas: RFC 5321, RFC 5322, RFC 2045, RFC 2046, RFC 3676, RFC 2047, RFC 2231 (atualização das RFC 2045, 2047 e 2183), RFC 2183, RFC 4288, RFC 4289, RFC 3023 e RFC 2049.	**A**
Acesso à caixa postal	*Post Office Protocol* – POP3 para acesso remoto a caixa postal. RFC correlacionada: RFC 1939 (atualizada pela RFC 1957 e RFC 2449).	**T**
	Internet Message Access Protocol – IMAP para acesso remoto à caixa postal. RFCs correlacionadas: RFC 2342 (atualizada pela RFC 4466), RFC 2910 (atualizada pela RFC 3380, RFC 3381, RFC 3382, RFC 3510 e RFC 3995), RFC 2971, RFC 3501, RFC 3502 e RFC 3503.	**A**
Mensageria em Tempo Real	O modelo e requisitos para *Instant Messaging and Presence Protocol* (IMPP) são definidos pela RFC 2778 e RFC 2779.	**T**
	O modelo e requisitos para *Extensible Messaging and Presence Protocol* (XMPP) são definidos pela RFC 6120 e atualizada pela RFC 6122.	**A**
AntiSpam – Gerenciamento da Porta 25	Implementar submissão de e-mail via porta 587/TCP com autenticação, reservando a porta 25/TCP apenas para transporte entre servidores SMTP, conforme recomendação CGI / Cert.br http://www.cert.br/	**R**
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1 (RFC 2616, atualizada pelas RFCs 2817, 5785, 6266 e 6585).	**A**
Protocolos de transferência de arquivos	FTP (com re-inicialização e recuperação) conforme RFC 959 (atualizada pela RFC 2228, RFC 2640, RFC 2773, RFC 3659 e RFC 5797) e HTTP conforme RFC 2616 (atualizada pelas RFCs 2817, 5785, 6266 e 6585) para transferência de arquivos. SFTP (Secure File Transfer Protocol) conforme RFC 913	**A**
Diretório	LDAP v3 deverá ser utilizado para acesso geral ao diretório OpenLDAP, conforme RFC 4510.	**A**
Sincronismo de	RFC 5905 IETF - *Network Time Protocol* - NTP	**A**

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

Componente	Especificação	SIT
tempo	version 4.0[2].	
Serviços de Nomeação de Domínio	O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035 (atualizada pela RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 1101, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966 e RFC 6604). Por sua vez, as diretivas de nomeação de domínio do governo brasileiro são encontradas na Resolução nº 7 do Comitê Executivo do Governo Eletrônico, no endereço eletrônico https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm Além dessas diretivas, por decisão do Comitê Gestor da Internet no Brasil, a nomeação de domínios obedece às orientações do Ministério do Planejamento, Orçamento e Gestão, a quem compete gerenciar os domínios .GOV.BR. As particularidades de outros níveis de governo, como por exemplo, os domínios dos governos das Unidades da Federação, que incluem a sigla da UF na composição dos endereços, são abordadas no endereço eletrônico http://registro.br/faq/faq1.html#12 DNSec (Domain Name System Security Extensions), RFC 4033.	**A**
Protocolos de sinalização	Uso do Protocolo de Inicialização de Sessão (SIP), definido pela RFC 3261 (atualizada pela RFC , RFC3265, RFC4320, RFC4916, RFC5393, RFC5621, RFC5626, RFC5630, RFC5922, RFC5954 e RFC6026), como protocolo de controle na camada de aplicação (sinalização) para criar, modificar e terminar sessões com um ou mais participantes.	**A**
	Uso do protocolo H.323 em sistemas de comunicação multimídia baseado em pacotes, definido pela ITU-T (*International Telecommunication Union Telecommunication Standardization sector*).	**T**
Protocolos de gerenciamento de rede	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 2	**T**
	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 3	**R**
Protocolo de troca de informações estruturadas em plataforma descentralizada e/ou distribuída	Vide Tabela 17 – Especificações para Áreas de Integração para Governo Eletrônico – *Web Services.*	
Protocolo de análise de fluxo de rede	IPFix, conforme RFC 5101, sFlown(RFC 3176)	**E**
Protocolo de Rede Definida por Software	Software-Defined Networking	**E**

[2] O Simple Network Time Protocol – SNTP version 4.0 está definido na seção 14 da RFC 5905.

Tabela 2 – Rede/Transporte

Componente	Especificação	SIT
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo	
Transporte	TCP (RFC 793)	**A**
	UDP (RFC 768) quando necessário, sujeito às limitações de segurança.	**A**
Intercomunicação LAN/WAN	IPv6 conforme RFC 2460 (atualizada pela RFC 5095, RFC 5722 e RFC 5871).	**A**
	IPv4 conforme RFC 791 (atualizada pela RFC 1349).	**T**
Comutação por Label	Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço. No caso de interconexão com a rede pública com comutação por Label, não haverá troca de Label entre a rede privada do governo e a rede pública. Neste caso deve-se adotar interface NNI (Option A) entre a rede do governo e a rede pública.	**A**
Qualidade de serviço	Adoção de uma arquitetura para serviços diferenciados pelo uso do Diffserv (RFC 2475, atualizada pela RFC 3260).	**A**

Tabela 3 – Enlace/Físico

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

2. Segurança

2.1. Políticas Técnicas

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

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

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

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

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

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

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

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

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

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

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

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

7.1.13 Para especificações sobre cartões inteligentes e *tokens*, deverão ser adotados os requisitos contidos nos normativos que tratam da homologação de equipamentos e sistemas no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (http://www.iti.gov.br). Estes requisitos,

observados por produtos homologados na ICP-Brasil, tais como mídias que armazenam os certificados digitais e respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, estabelecem padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados. É importante observar que não deve haver impedimento de acesso a dado armazenado em um cartão, como possíveis restrições impostas por licenciamento de uso de interface de software (middleware) para que seja garantida a interoperabilidade.

2.2.Especificações Técnicas

Tabela 4 – Comunicação de dados

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Transferência de dados em redes inseguras	TLS – *Transport Layer Security*, RFC 5246[3] (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.	**R**	
Algoritmos para troca de chaves de sessão, durante o *handshake*	RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;	**R**	
Algoritmos para definição de chave de cifração	RC4, IDEA, 3DES e AES	**R**	
Certificado Digital	X.509 v3 – ICP-Brasil, SASL - *Simple Authentication and Security Layer*, RFC 4422	**R**	
Hipertexto e transferência de arquivos	RFC 2818 (atualizada pela RFC 5785)	**R**	
Transferência de arquivos	SSH FTP	**R**	
	Securing FTP with TLS, RFC 4217	**R**	
Segurança de redes IPv4	*IPSec Authentication Header* RFC 4303 e RFC 4835 para autenticação de cabeçalho do IP. IKE – *Internet Key Exchange*, RFC 4306 (atualizada pela RFC5282), deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento. ESP – *Encapsulating Security Payload,* RFC 4303 Requisito para VPN – Virtual Private Network.	**A**	Consultar errata para RFC 4303 e RFC 4306.
Segurança de redes IPv4 para protocolos de aplicação	O S/MIME v3, RFC 5751 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.	**A**	Consultar errata para RFC 5751.
Segurança de redes IPv6 na camada de rede	O IPv6 definido na RFC 2460 (atualizada pela RFC 5095), RFC 5722 e RFC 5871 apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*) RFC 4302 ou autenticação IP, e a segurança do encapsulamento IP, ESP (*Encrypted Security Payload*) RFC 4303.	**R**	Consultar errata para RFC 4302 e RFC 4303.

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

Tabela 5 – Correio Eletrônico

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Acesso a caixas postais	O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado, considerando as facilidades de segurança nativas do cliente. Quando não for possível utilizar o cliente específico ou for necessário acessar a caixa postal através de redes não seguras (por exemplo: Internet) deve-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595 (atualizada pela RFC 4616), que trata da utilização do TLS com IMAP, POP3 e ACAP.	**A**	Consultar errata para a RFC 2595.
Conteúdo de e-mail	O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 5652, RFC 3370 (atualizada pela RFC 5754), RFC 2631, RFC 5750, RFC 5751 e RFC 5652.	**A**	Consultar errata para RFC 5652, RFC 3370, RFC 5754, RFC 2631, RFC 5751 e RFC 5652.
Transporte de e-mail	Utilizar SPF (Sender Policy Framework) nos termos da RFC 4408, e reservar a porta 25, do protocolo SMTP, exclusivamente para transporte de mensagens entre MTAs; para comunicação entre MUAs e MTAs, utilizar a porta 587 (Submission), nos termos das RFCs 4409 e 5068	**A**	Consultar errata para RFC 4408.
Identificação de e-mail	Utilizar DKIM (*DomainKey Identified Mail*) nos termos da RFC 6376 http://datatracker.ietf.org/doc/rfc6376/ Recomendações do Comitê Gestor da Internet no Brasil. http://antispam.br/admin/dkim/	**R**	Consultar errata para RFC 4871.
Assinatura	Utilizar certificado padrão ICP-Brasil para assinatura de e-mail, quando exigido. Em conformidade com o disposto na Medida Provisória nº 2.200-2, de 24/08/2001 e Decreto nº 3.996 de 31/10/2001.	**A**	O serviço de assinatura deverá estar de acordo com as normas da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil
Transporte seguro de e-mail	Usar SMTP seguro sobre TLS para transporte de e-mails entre MTA's nos termos da RFC 3207 e SMTP AUTH nos termos da RFC 4954.	**R**	Ver http://www.ietf.org/rfc/rfc3207.txt e http://www.ietf.org/rfc/rfc4954.txt

Tabela 6 – Criptografia

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Algoritmo de cifração	3DES ou AES	**R**	
Algoritmos para assinatura/hashing	SHA-256 ou SHA-512	**R**	i) Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil. ii) Os sistemas devem ter suporte para o algoritmo de *hash* MD5 com RSA, para garantir compatibilidade com implementações anteriores.
	SHA-224 ou SHA-238	**E**	Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	**A**	
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (RFC 5480). ECIES 256 e ECIES 512.	**A**	ECDSA, para assinaturas digitais, e ECIES (Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil)para cifração e transporte seguro de chaves criptográficas.
	ECMQV e ECDH, ambos para acordo de chaves, conforme RFC 5753.	**E**	
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3; FIPS 140-1 e FIPS 140-2.	**R**	Ver Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil).
Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	Devem ser aderentes aos padrões da ICP – Brasil.	**R**	Os certificados da AC-raiz devem ser instalados nos navegadores e visualizadores de arquivos conforme recomendado na IN nº 5/2009/ITI.

Tabela 7 – Desenvolvimento de Sistemas

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Assinaturas XML	Sintaxe e Processamento de assinatura XML (XMLsig) conforme definido pelo W3C http://www.w3.org/TR/xmldsig-core/	**A**	
Cifração XML	Sintaxe e Processamento de Cifração XML (XMLenc) conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/	**R**	
Assinatura e cifração XML	Transformação de decifração para assinatura XML conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificações de Gerenciamento de Chave XML) conforme definido pelo W3C http://www.w3.org/TR/xkms2/	**R**	
Autenticação e autorização de acesso XML	SAML – conforme definido pelo OASIS quando um ambiente ICP é utilizado http://www.oasis-open.org/committees/security/index.shtml	**R**	
Intermediação ou Federação de Identidades	WS-Security 1.1 - arcabouço de padrões para garantir integridade e confidencialidade em mensagens SOAP. (http://www.oasis-open.org/standards#wssv1.1. WS-Trust 1.4 - extensões para o padrão WS-Security, definindo o uso de credenciais de segurança e gerência de confiança distribuída. (http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf).	**R**	O componente anterior (SAML) poderá se juntar a este componente após estudos.
Navegadores	Somente utilizar testemunhas de conexão de caráter permanente (*cookies*) com a concordância do usuário.	**A**	Resolução nº 7 do Comitê Executivo do Governo Eletrônico (Capítulo II, Art.7º)

Tabela 8 – Serviços de Rede

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

Tabela 9 – Redes Sem Fio

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

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

Tabela 10 – Resposta a Incidentes de Segurança da Informação

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Preservação de registros	*Guidelines for Evidence Collection and Archiving*, RFC 3227.	**R**	
Gerenciamento de incidentes em redes computacionais	*Expectations for Computer Security Incident Response*, RFC 2350. Criação de equipes de tratamento e resposta a incidentes em redes computacionais conforme Norma Complementar nº 05/09 (http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf). Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal conforme Norma Complementar nº 08/2010 (http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf)	**A**	
Informática Forense	*Guide to Integrating Forensic Techniques into Incident Response* – NIST - *Special Publication* 800-86 – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	**A**	
Comunicação entre Equipes e entre Centros de tratamento e resposta a incidentes	Representação para o compartilhamento de informações entre Equipes e entre Centros de Resposta a Incidentes de Segurança em Redes de Computadores: Incident Object Description Exchange Format (IODEF) – RFC 5070 **http://datatracker.ietf.org/doc/rfc5070/** http://datatracker.ietf.org/doc/rfc5070/ Extensão do formato IODEF para suportar a comunicação de eventos do tipo “phishing”. http://datatracker.ietf.org/doc/rfc5901/ Guia para a extensão do formato IODEF. http://datatracker.ietf.org/doc/rfc6684/	**E**	Deverão ser realizados estudo a respeito de procedimentos e Ferramentas para a possível adoção deste padrão.
Comunicação entre Sistemas de detecção e resposta a intrusão	Formato para compartilhamento de dados entre sistemas de detecção e resposta a incidentes de segurança computacionais: *Intrusion Detection Message Exchange Format* (IDMEF) – RFC 4765 http://datatracker.ietf.org/doc/rfc4765/	**E**	Deverão ser realizados estudo a respeito de procedimentos e Ferramentas para a possível adoção deste padrão.

Tabela 11 – Auditoria em programas e equipamentos

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Serviços de tecnologia da informação, conforme definidos no art. 11 da Portaria Interministerial MP/MC/MD nº 141 de 02/05/2014	Conforme diretrizes e especificações técnicas definidas em http://www.governoeletronico.gov.br/eping	**A**	

3. Meios de Acesso

3.1. Especificações Técnicas

Tabela 12 – Meios de Publicação

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Conjunto de caracteres	Unicode Standard, Version 7.0.0 Mountain View, CA: The Unicode Consortium, 2014. ISBN 978-1-936213-09-2 http://www.unicode.org/versions/Unicode7.0.0/ UTF-8 ISO/IEC 10646:2014	**R**	
Formato de intercâmbio de hipertexto	W3C XML versões 1.0 ou 1.1 (.xml) http://www.w3.org/TR/xml/	**A**	
	W3C HTML 5 conforme especificações do W3C http://www.w3.org/TR/html5/	**A**	
	W3C HTML versão 4.01 (.html ou .htm) http://www.w3.org/TR/html4/	**T**	
	W3C XHTML versões 1.0 ou 1.1 (.xhtml) http://www.w3.org/TR/xhtml1	**T**	
Mobile	W3C Mobile Web application Best Practices http://www.w3.org/TR/mwabp/	**R**	
	W3C Geolocation API Specification http://www.w3.org/TR/mediaont-api-1.0/	**R**	
	W3C Mobile Web Application Best Practices http://www.w3.org/TR/geolocation-API/	**R**	
Arquivos do tipo documento/ publicação	Texto puro (arquivo .txt)	**A**	
	Open Document (.odt), NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 - especificação OASIS[10]	**R**	
	EPUB 3.0.1 http://idpf.org/epub/301	**R**	
	Portable Document Format - PDF ISO 32000-1:2008	**R**	
	Portable Document Format - PDF/A NBR ISO 19005-1:2009 [11], quando necessária a preservação digital de documentos	**R**	
Arquivos do tipo planilha	Open Document (.ods), NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 - especificação OASIS	**R**	
Arquivos do tipo apresentação	Open Document (.odp), NBR ISO/IEC 26.300:2008.	**A**	
	Open Document ODF 1.2 - especificação OASIS	**R**	
	HTML (.html ou .htm), conforme especificações do W3C.	**R**	
Arquivos do tipo “banco de dados” para estações de trabalho	Texto Puro (.txt).	**A**	No caso de texto plano “txt” e “csv”, deve ser incluído o leiaute dos campos, de
	Texto Puro (.csv) – comma-separated values	**A**	
	XML (.xml), conforme especificações do W3C.	**R**	
	MySQL Database (.myd, .myi), versão 4.0 ou superior.	**R**	

[10] Disponível em: http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html
[11] http://www.pdfa.org/competence-centers/pdfa-competence-center/

Componente	Especificação	SIT	Observações
	Arquivo do Base (.odb), NBR ISO/IEC 26.300:2008.	**R**	forma a possibilitar seu tratamento.
Intercâmbio de informações gráficas e imagens estáticas	W3C PNG (.png), ISO/IEC 15948:2003 (E) http://www.w3.org/TR/PNG/	**A**	
	SVG (.svg), gerado conforme especificações do W3C[12].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)[13]	**R**	
Gráficos vetoriais	SVG (.svg), gerado conforme especificações do W3C.	**R**	
Animação	SVG (.svg), gerado conforme especificações do W3C.	**R**	
Áudio	Ogg Vorbis (.ogg, .oga)[14].	**R**	
	Ogg FLAC (.ogg, .oga)	**R**	
	FLAC (.flac)	**R**	
Vídeo	Ogg Theora (.ogg, .ogv)[15].	**R**	
	Matroska (.mkv)	**R**	
	Áudio e vídeo MPEG-4, Part 14 (.mp4)[16].	**T**	
Compactação de arquivos	ZIP (.zip).	**R**	
	GNU ZIP (.gz).	**R**	
	Pacote TAR (.tar).	**R**	
Informações georreferenciadas	GML versão 2.0 ou superior[17].	**A**	
	ShapeFile[18].	**A**	
	GeoTIFF[19].	**A**	

[12] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponível em: http://www.w3.org/TR/2003/REC-SVG11-20030114/.* Acesso em: 7 dez. 2005.
[13] *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponível em: http://www.jpeg.org/public/jfif.pdf*. Acesso em: 7 dez. 2005.
[14] Xiph.Org Foundation. Especificação disponível em: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.
[15] Theora. Especificação disponível em: http://www.theora.org/.
[16] *ISO/IEC 14496-14:2003 – Information Technology – Coding of audio-visual objects – Part 14: MP4 file format.*
[17] *Geography Markup Language*. Especificações disponíveis em: http://www.opengeospatial.org/standards/gml. Indicado para estruturas vetoriais complexas, envolvendo primitivas geográficas como polígonos, pontos, linhas, superfícies, coleções, e atributos numéricos ou textuais sem limites de número de caracteres.
[18] *ESRI Shapefile Technical Description*. Disponível em: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf. Indicado para estruturas vetoriais limitadas a linhas, pontos e polígonos, cujos atributos textuais não ultrapassem 256 caracteres. Pode armazenar também as dimensões M e Z.
[19] *GeoTIFF Format Especification*. Disponível em: http://remotesensing.org/geotiff/geotiff.html. Indicado para estruturas matriciais limitadas a matrizes de pixel.

Tabela 13 – TV Digital

Para atender às questões técnicas, o Fórum do Sistema Brasileiro de TV Digital Terrestre – SBTVD, publicado junto à Associação Brasileira de Normas Técnicas – ABNT, agrupa diversas normas no sítio: http://forumsbtvd.org.br/acervo-online/normas-brasileiras-de-tv-digital/, onde está referenciado um conjunto de especificações, padronizado e livre de royalties, denominado GINGA.

Componente	Especificação	SIT
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo	
Transmissão	**ABNT NBR 15601** Parte 1 – Sistema de transmissão	**A**
Codificação	**ABNT NBR 15602** Parte 1 – Codificação de video Parte 2 – Codificação de áudio Parte 3 – Sistema de multiplexação de sinais	**A**
Multiplexação	**ABNT NBR 15603** Parte 1 – Serviços de informação do sistema de radiodifusão Parte 2 – Sintaxes e definições da informação básica de SI Parte 3 – Sintaxe e definição da informação estendida do SI	**A**
Receptores	**ABNT NBR 15604** Parte 1 – Receptores	**A**
Segurança	**ABNT NBR 15605** Parte 1 – Tópicos de segurança	**A**
Middleware	**ABNT NBR 15606** Parte 1 – Codificação de dados Parte 2 – Ginga-NCL para receptores fixos e móveis – Linguagem de aplicação XML para codificação de aplicações Parte 3 – Especificação de transmissão de dados Parte 4 – Ginga-J – Ambiente para a execução de aplicações procedurais Parte 5 – Ginga-NCL para receptores portáteis – Linguagem de aplicação XML para codificação de aplicações Parte 6 – Java DTV 1.3 Parte 7 – Ginga-NCL – Diretrizes Operacionais para as ABNT NBR15606-2 e 15606-5 Parte 8 – Ginga-J - Diretrizes operacionais para a ABNT NBR 15606-4 Parte 9 – Diretrizes operacionais para a ABNT NBR 15606-1	**A**
Canal de Interatividade	**ABNT NBR 15607** Parte 1 – Protocolos, interfaces físicas e interfaces de software	**A**
Guia de Operação	**ABNT NBR 15608** Parte 1 – Sistema de Transmissão – Guia para implementação da ABNT NBR 15601 Parte 2 – Codificação de vídeo, áudio e multiplexação – Guia para implementação da ABNT NBR 15602 Parte 3 – Multiplexação e serviço de informação (SI) – Guia de implementação da ABNT NBR 15603	**A**
Acessibilidade	**ABNT NBR 15610** Parte 1 – Ferramentas de texto Parte 2 – Funcionalidades sonoras	**A**

4. Organização e Intercâmbio de Informações

4.1. Especificações Técnicas

Tabela 14 – Tratamento e transferência de Dados

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Linguagem para intercâmbio de dados	XML (Extensible Markup Language) como definido pelo W3C http://www.w3.org/XML	**A**	
	JSON (Javascript Object Notation) Como definido pela IETC http://www.ietf.org/rfc/rfc4627.txt	**A**	
Transformação de dados	XSL (*Extensible Stylesheet Language*) como definido pelo W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) como definido pelo W3C http://www.w3.org/TR/xslt	**A**	
Definição dos dados para intercâmbio	XML *Schema* como definido pelo W3C: - XML *Schema Part 0: Primer* http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ - XML *Schema Part 1: Structures* http://www.w3.org/TR/xmlschema-1/structures - XML *Schema Part 2: Datatypes* http://www.w3.org/TR/xmlschema-2/datatypes	**A**	
Informações georreferenciadas – catálogo de feições	Estruturação de Dados Geoespaciais Vetoriais (EDGV) como definido pela CONCAR	**R**	Para dados geoespaciais vetoriais de referência (cartografia básica)
Metadados para informações georreferenciadas	Perfil de Metadados Geoespaciais do Brasil (Perfil MGB) como definido pela CONCAR	**E**	Conjunto básico de elementos comuns a todos os tipos de produtos geoespaciais
Formato para intercâmbio de dados geoespaciais	GeoJSON, como definido em http://www.geojson.org/geojson-spec.html	**E**	
Especificação para informações de transporte público	GTFS (General Transit Feed Specification) como definido em https://developers.google.com/transit/gtfs/	**E**	

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

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
Descrição de recursos	RDF (*Resource Description Framework*) Como definido pela W3C.	**R**	
Especificação de vocabulários para RDF	Resource Description Framework (RDF) Schema, como definido pelo W3C em http://www.w3.org/TR/rdf-schema/	**R**	Recomenda-se usar RDF Schema em situações em que o poder de processamento disponível for limitado ou onde não for necessária para descrever os dados toda a expressividade da linguagem OWL.
Sistemas de Organização do Conhecimento	SKOS (*Simple Knowledge Organization System*) como definido pelo W3C http://www.w3.org/2004/02/skos/	**R**	
Linguagem de definição de ontologias na web	OWL (*Web Ontology Language*) Como definido pelo W3C	**R**	
Linguagem de consulta semântica	SPARQL (*Sparql Protocol and RDF Query Language*) Como definido pelo W3C	**E**	
Sistema de resolução de Identificadores	*Handle system* (http://www.handle.net).	**E**	

5. Áreas de Integração para Governo Eletrônico

5.1. Especificações Técnicas

Tabela 16 – Temas Transversais às Áreas de Atuação de Governo

Componente	Especificação	SIT	Observações
	A = Adotado R = Recomendado T = Em Transição E = Em Estudo		
PROCESSOS – Linguagem para Execução de Processos	BPEL4WS V1.1, conforme definido pelo OASIS http://www.oasis-open.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	**R**	O grupo acompanhará a evolução do BPEL4WS versão 2.0. Estudos referentes à orquestração de processos e coreografia serão futuramente conduzidos pelo grupo.
PROCESSOS – Notação de Modelagem de Processos	BPMN – Business Process Model and Notation versão 1.2, definido pelo OMG http://www.omg.org/spec/BPMN/1.2/	**A**	A atualização para versão 2.0 do padrão está em estudo.
Intercâmbio de Informações Financeiras	XBRL – *eXtensible Business Reporting Language* http://www.xbrl.org/SpecRecommendations/	**A**	www.xbrl.org
Legislação, Jurisprudência e Proposições Legislativas	LexML v. 1.0 http://projeto.lexml.gov.br	**A**	Projeto LexML define recomendações para a identificação e estruturação de documentos legislativos e jurídicos.
Integração de Dados e Processos	MGD http://modeloglobaldados.serpro.gov.br	**A**	
Informações Georreferenciadas - Interoperabilidade entre sistemas de informação geográfica	WMS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	WFS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	WCS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	**A**	
	CSW versão 2.0 ou posterior http://www.opengeospatial.org/standards/cat	**A**	
	WFS-T versão 1.0 ou posterior http://www.opengeospatial.org/standards/wfs	**R**	Observar padrões e políticas de segurança indicados pelo Segmento Segurança, principalmente WS-Security.

Componente	Especificação	SIT	Observações
	WKT http://www.opengeospatial.org/standards/sfa	**R**	Para codificar coordenadas em serviços Web convencionais. As coordenadas devem estar em Lat/Long utilizando o datum SIRGAS2000 (EPSG:4674) ou WGS-84 (EPSG:4326). Usar GML sempre que possível.
	Filter Encoding versão 1.0 ou posterior http://www.opengeospatial.org/standards/filter	**A**	Especificação acessória para codificar expressões de filtro
	Symbology Encoding versão 1.1.0 ou posterior http://www.opengeospatial.org/standards/se	**E**	Para codificar estilos em mapas
Intercâmbio de Dados Estatísticos	SDMX – Statistical Data and Metadata Exchange http://sdmx.org/wp-content/uploads/2011/04/SDMX_2-1_SECTION_1_Framework.pdf	**E**	http://sdmx.org/

Tabela 17 – *Web Services*[20]

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

[20] As questões de segurança relativas a Web Services são abordadas no capítulo sobre Segurança deste documento.

6. Glossário de Siglas e Termos Técnicos[21]

Neste item são apresentados os significados dos principais termos técnicos utilizados na ePING.

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

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

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

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

Diretório – Serviço que armazena e organiza informações sobre os recursos e os usuários de uma rede de computadores, e que permite os administradores de rede gerenciar o acesso de usuários e sistemas a esses recursos. Além disso, serviço de diretório podem atuar como uma camada de abstração entre os usuários e esses recursos.

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.

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

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

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

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.

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.

[21] Microsoft Press. Dicionário de informática. Tradutor e consultor editorial Fernando Barcellos Ximenes – KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.
Thing, Lowell (ed.). Dicionário de Tecnologia. Tradução de Bazán Tecnologia e Linguística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

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

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

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

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

Padrão Aberto:

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

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

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

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

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

Sistemas de Organização do Conhecimento: Segundo o documento de referência do W3C, são considerados sistemas de organização do conhecimento os tesauros, esquemas de classificação, listas de assuntos, taxonomias, e outros tipos de vocabulários controlados.

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

TIC: Tecnologia da Informação e Comunicação

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.