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

gov.br
ePING

Padrões de Interoperabilidade de Governo Eletrônico

Guia de Interoperabilidade
Cartilha Técnica

Versão 2015

BRASIL

Este documento é parte integrante do Guia de Interoperabilidade do Governo Brasileiro, que compreende a Cartilha Técnica de Interoperabilidade e o Manual de Gestão de Interoperabilidade. Este documento foi elaborado pelo Ministério do Planejamento, Orçamento e Gestão com a consultoria da Agência Espanhola de Cooperação para o Desenvolvimento (AECID) e da Fundação Instituto para o Fortalecimento das Capacidades Institucionais (IFCI).

Brasil. Ministério do Planejamento, Orçamento e Gestão
Guia de Interoperabilidade: Cartilha Técnica / Ministério do Planejamento, Orçamento e Gestão. – Brasília: MP, 2015.
90 p.; 30 cm.

Documento técnico do governo brasileiro.

1. Interoperabilidade 2. Governo eletrônico 3.ePING

Presidente da República

Dilma Rousseff

Ministério do Planejamento, Orçamento e Gestão

Miriam Belchior

Secretaria de Logística e Tecnologia da Informação – SLTI

Loreni F. Foresti

Departamento de Governo Eletrônico – DGE

Andrea Thalhofer Ricciardi

Coordenação-Geral de Normas e Padrões de Governo Eletrônico- CGPGE

Fernanda Hoffmann Lobato

ePING

Coordenador: Andrea Thalhofer Ricciardi

GT 1: Marcus Vinícius Paizante

GT 2: Jorilson da Silva Rodrigues

GT 3: Paulo Maia da Costa

GT 4: Carlos Eduardo Araújo Vieira

GT 5: Marcus Vinícius da Costa

Equipe de Elaboração

Ana Paula Pessoa Mello - SLTI/MP

Carlos Eduardo Araújo Vieira - SLTI/MP

Hudson Vinícius Mesquita – SLTI/MP

Roberto Shayer Lyra - SLTI/MP

Agradecimento aos colaboradores

Carlos E. Jiménez Gómez

Cláudia do Socorro F. Mesquita

Daniel Viero – SENADO

Emerson Magnus de A. Xavier – MD/CEX

Gonçalo Teixeira Nunes – IFCI/AECID

Júlio César dos Santos Nunes – SRF/MF

Marcello Alexandre Kill – SERPRO

Patrycia Barros de L. Klavdianos – IFCI/AECID

Rachel Cristina G. M. Domingos – STM

Renata Assunção de Farias – SEP/PR

Yuri Fontes de Oliveira – SLTI/MP

SUMÁRIO

1 INTRODUÇÃO

A Secretaria de Logística e Tecnologia da Informação – SLTI do Ministério do Planejamento, Orçamento e Gestão tem, entre suas atribuições, a competência de planejar, coordenar, supervisionar e orientar, normativamente, as atividades do Sistema de Administração de Recursos de Tecnologia da Informação – SISP, propondo políticas e diretrizes de Tecnologia da Informação, no âmbito da Administração Pública Federal direta, autárquica e fundacional.

A Arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico define um conjunto de premissas, políticas e especificações técnicas que regulamentam sua utilização, com o objetivo maior de possibilitar um nível adequado de interoperabilidade entre os serviços disponibilizados pelo governo eletrônico, tornando-se o marco referencial para as atividades de TIC (Tecnologia da Informação e Comunicação) no Governo. A SLTI é a responsável pela institucionalização e pela definição do formato jurídico da Coordenação da ePING.

O Guia de Interoperabilidade do Governo apresenta orientações para o desenvolvimento de soluções de TIC aderentes à Arquitetura ePING como forma de incentivar a interoperabilidade no Governo Federal e deste com os demais entes da Federação. Ele é organizado em dois volumes: o **Manual do Gestor de Interoperabilidade** e a **Cartilha Técnica de Interoperabilidade**.

O **Manual do Gestor de Interoperabilidade** tem como público-alvo os gestores de TI (Tecnologia da Informação) dos órgãos do Governo. Esse documento possui diretrizes de gestão, assim como indicações de ações promovidas em nosso país com o objetivo de propiciar uma gestão de serviços governamentais direcionada à interoperabilidade.

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

1.1. Assuntos não contemplados

A Cartilha Técnica de Interoperabilidade não pretende guiar os profissionais de TIC no uso de linguagens de programação e técnicas computacionais específicas que envolvam o projeto e a construção de sistemas informatizados. Além disso, não é objetivo deste documento imputar a utilização de ferramentas de trabalho ou de realizar a divulgação de soluções prontas de TIC que tratam de interoperabilidade. Por isso, recomenda-se que os leitores possuam conhecimento adequado dos assuntos tratados em cada um dos capítulos deste documento.

É importante salientar, também, que este documento discorrerá somente sobre o uso dos padrões publicados na ePING como **Adotado** (A) e **Recomendado** (R). Isso porque os demais padrões ou estão em processo de substituição (T – **Em Transição**) ou serão tratados em futuras versões deste documento (E – **Em Estudo**).

2. FUNDAMENTOS DE INTEROPERABILIDADE

2.1. Introdução

O documento de referência da ePING aborda, inicialmente, a importância da TIC no contexto governamental, fornecendo as justificativas para se investir em políticas direcionadas à interoperabilidade governamental.

A ePING surge como documento definidor das políticas e padrões de interoperabilidade aplicáveis, em um primeiro momento, no Governo Federal, mas de uso livre e irrestrito por outros poderes e esferas da Administração Pública dos Estados e Municípios.

A ePING é o marco principal de interoperabilidade do governo brasileiro, e tem como objetivo estabelecer as condições de interação do Poder Executivo com os demais Poderes e esferas de governo e com a sociedade em geral. Para tanto, ela organiza o seu conteúdo em cinco segmentos: (i) Interconexão, (ii) Segurança, (iii) Meios de Acesso, (iv) Organização e Intercâmbio de Informações e (v) Áreas de Integração para Governo Eletrônico.

Entretanto, sendo a ePING um documento de referência, não está entre seus objetivos fornecer respostas aos questionamentos técnicos envolvendo a aplicação dos padrões tecnológicos no contexto de execução dos projetos e das atividades de rotina dos setores de TIC do Governo. Por isso, tornou-se necessário consolidar e aperfeiçoar as ferramentas de apoio à ePING com o objetivo de dar a ela um caráter mais prático.

Este é o enfoque principal deste documento, que recebeu o nome de **Cartilha Técnica de Interoperabilidade** por representar bem o seu objetivo e estrutura interna. Trata-se de uma cartilha que procura utilizar linguagem facilitada para descrever conceitos e ações pertinentes à execução das políticas e práticas de interoperabilidade definidas na ePING. É também um documento técnico, pois embora faça uso de uma linguagem facilitada que permite a melhor compreensão dos conceitos, não deixa de tratar as questões tecnológicas relacionadas ao tema “Interoperabilidade no Governo”.

2.2. Dimensões da Interoperabilidade

A interoperabilidade pode ser organizada em três dimensões que se comunicam e se complementam: organizacional, semântica e técnica.

A Figura 1 ilustra essas três dimensões da interoperabilidade:

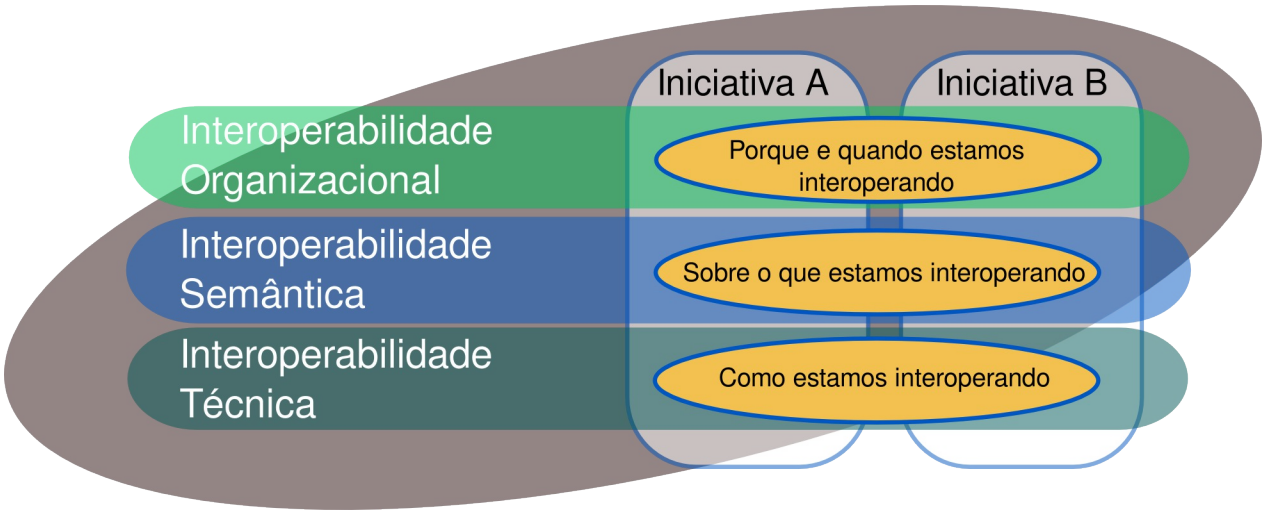


Figura 1: Dimensões da Interoperabilidade

A **interoperabilidade organizacional** diz respeito à colaboração entre organizações que desejam trocar informações mantendo diferentes estruturas internas e processos de negócios variados. Mesmo contando com a padronização de conceitos, as organizações possuem distintos modelos de operação, ou processos de trabalho. Isto quer dizer que elas realizam suas atividades em tempos diferentes e de maneiras diferentes.

Assim, um desafio da interoperabilidade é identificar as vantagens de cada interoperação e em que momentos estas deveriam acontecer. Para isso, as organizações envolvidas na interoperação precisam conhecer mutuamente seus processos de trabalho, e isto só é possível se ambas possuírem processos modelados, e ainda mais, se estes modelos estiverem dentro do mesmo padrão.

A **interoperabilidade semântica** é a capacidade de dois ou mais sistemas heterogêneos e distribuídos trabalharem em conjunto, compartilhando as informações entre eles com entendimento comum de seu significado (Buranarach, 2004). A interoperabilidade semântica garante que os dados trocados tenham seu efetivo significado corretamente interpretado dentro do contexto de uma dada transação ou busca de informação, dentro da cultura, convenções e terminologias adotadas por cada setor ou organização e, assim, compartilhados pelas partes envolvidas.

A **interoperabilidade técnica** trata da ligação entre sistemas e serviços de computação pela utilização de padrões para apresentação, coleta, troca, processamento e transporte de dados. Esses padrões podem abranger *hardware*, *software*, protocolos e processos de negócio. Uma vez que foram estabelecidos vocabulários comuns, e que foram identificados os motivos e os momentos adequados para interoperar, é preciso haver também um padrão para fazer isso, ou seja, para tratar o “como fazer”.

É importante, portanto, que as áreas de Tecnologia busquem utilizar padrões tecnológicos comuns para implementar a interoperabilidade. Alguns destes padrões são encontrados na arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico.

2.3. Interoperabilidade e Conformidade

O termo “conformidade” está associado à ideia de qualidade e tem como objetivo avaliar a semelhança ou correlação entre as coisas. Assim, quando se diz que um produto está em conformidade com um protocolo, por exemplo, significa afirmar que esse produto provê um determinado nível de semelhança aos padrões definidos no protocolo.

No que tange à prática de interoperabilidade no governo brasileiro, a conformidade de produtos e soluções tecnológicas aos padrões definidos na ePING é condição *sine qua non* para se desenvolver as políticas de e-Gov.

Logo, segundo a visão de conformidade da ePING, os padrões tecnológicos a serem aplicados no governo passam por quatro níveis, a saber: Adotado (A), Recomendado (R), Em Transição (T) e Em Estudo (E).

Um padrão identificado como **Adotado (A)** na ePING implica em esforços prioritários, por parte do setor de TI dos órgãos de governo, no sentido de atender à recomendação. Esses padrões foram, de fato, homologados em um processo formal e aprovados pela Coordenação da ePING. Seu uso é obrigatório para os órgãos do Poder Executivo do governo brasileiro.

Um padrão tido como **Recomendado (R)** caracteriza-se por atender às políticas técnicas da ePING, podendo ser utilizado no âmbito das instituições de governo. Entretanto, ainda é necessária a sua homologação e aprovação formais. Geralmente, os padrões identificados como Recomendados (R) são oriundos de práticas de interoperabilidade bem sucedidas e de uso comum, mas que carecem da formalização por parte dos membros da ePING.

Os padrões **Em Transição (T)** correspondem aos itens que o governo não recomenda, seja porque não atendem aos requisitos estabelecidos nas políticas gerais e técnicas da ePING, ou porque se encontram em processo de substituição nas instituições de governo, tendendo à descontinuação de seu uso no futuro. É possível que um item Em Transição (T) passe a ser considerado Recomendado (R). Isso porque as dificuldades em se estabelecer políticas viáveis para sua substituição justificariam a sua permanência. Entretanto, a ePING recomenda enfaticamente evitar-se o uso dos padrões Em Transição (T).

Por fim, os padrões **Em Estudo (E)** são aqueles que ainda estão em avaliação por parte dos membros da ePING e que, por isso, não podem ser classificados em outros níveis de conformidade.

O Guia de Interoperabilidade de Governo, conforme relatado anteriormente, dará ênfase aos padrões **Adotado (A)** e **Recomendado (R)**, por razões óbvias de concordância com as políticas e interesses públicos do governo discutidos durante as reuniões de trabalho da ePING.

3. Especificação Técnica dos Componentes da ePING

3.1. 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.

- **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.
- **Segurança – Segmento 2:** Trata dos aspectos de segurança de TIC que o governo federal deve considerar.
- **Meios de Acesso – Segmento 3:** São explicitadas as questões relativas aos padrões dos dispositivos de acesso aos serviços de governo eletrônico.
- **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.
- **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.

A Tabela 1 descreve os padrões no contexto de cada um dos segmentos mencionados, de modo a fazer referência aos componentes identificados como Adotados (A) e Recomendados (R) pelo governo brasileiro. Inclui-se também nessa tabela a referência às seções da ePING onde se podem localizar os padrões citados.

Tabela 1: Padrões por segmento na ePING

Segmentos da ePING	Componentes da ePING	Referência na ePING
1 – Interconexão	Endereços de caixa postal eletrônica	Tabela 1 – Aplicação
	Transporte de mensagem eletrônica	
	Acesso à caixa postal	
	Mensageria em Tempo Real	
	AntiSpam – Gerenciamento da Porta 25	
	Protocolo de transferência de hipertexto	
	Protocolos de transferência de arquivos	
	Diretório	
	Sincronismo de tempo	
	Serviços de Nomeação de Domínio	
	Protocolos de sinalização	
	Protocolos de gerenciamento de rede	
	Transporte	Tabela 2 – Rede/Transporte
	Intercomunicação LAN/WAN	
	Comutação por Label	
	Qualidade de Serviço	
	Rede local sem fio	Tabela 3 – Enlace/Físico
	Qualidade de Serviço – 802.1p	
	Virtual LAN	
	Resiliência Layer2	
2 – Segurança	Transferência de dados em redes inseguras	Tabela 4 – Comunicação de dados
	Algoritmos para troca de chaves de sessão, durante o handshake	
	Algoritmos para definição de chave de cifração	
	Certificado Digital	
	Hipertexto e transferência de arquivos	
	Transferência de arquivos	
	Segurança de redes IPv4	
	Segurança de redes IPv4 para protocolos de aplicação	
	Segurança de redes IPv6 na camada de rede	
	Acesso a caixas postais	Tabela 5 – Correio Eletrônico
	Conteúdo de e-mail	
	Transporte de e-mail	
	Identificação de e-mail	
	Assinatura	
	Transporte seguro de e-mail	
	Algoritmo de cifração	Tabela 6 – Criptografia
	Algoritmos para assinatura/hashing	
	Algoritmo para transporte de chave criptográfica de conteúdo/sessão	
	Algoritmos criptográficos baseados em curvas elípticas	
	Requisitos de segurança para módulos criptográficos	
	Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	
	Assinaturas XML	Tabela 7 – Desenvolvimento de Sistemas
	Cifração XML	
	Assinatura e cifração XML	
	Principais gerenciamentos XML quando um ambiente PKI é utilizado	
	Autenticação e autorização de acesso XML	

	Intermediação ou Federação de Identidades	
	Navegadores	
	Diretório	Tabela 8 – Serviços de Rede
	DNSSEC	
	Carimbo do tempo	
	LAN sem fio 802.11	Tabela 9 – Redes sem fio
	Preservação de registros	Tabela 10 – Resposta a Incidentes de Segurança da Informação
	Gerenciamento de incidentes em redes computacionais	
	Informática Forense	
	Serviços de tecnologia da informação, conforme definidos no art. 11 da Portaria Interministerial MP/MC/MD nº 141 de 02/05/2014	Tabela 11 – Auditoria em programas e equipamentos
3 – Meios de Acesso	Conjunto de caracteres	Tabela 12 – Meios de Publicação
	Formato de intercâmbio de hipertexto	
	Mobile	
	Arquivos do tipo documento	
	Arquivos do tipo planilha	
	Arquivos do tipo apresentação	
	Arquivos do tipo “banco de dados” para estações de trabalho	
	Intercâmbio de informações gráficas e imagens estáticas	
	Gráficos vetoriais	
	Animação	
	Áudio	
	Vídeo	
	Compactação de arquivos	
	Informações georreferenciadas	
	Transmissão	Tabela 13 – TV Digital
	Codificação	
	Multiplexação	
	Receptores	
	Segurança	
	Middleware	
	Canal de Interatividade	
	Guia de Operações	
	Acessibilidade	
4 – Organização e Intercâmbio de informações	Linguagem para intercâmbio de dados	Tabela 14 – Tratamento e transferência de Dados
	Transformação de dados	
	Definição dos dados para intercâmbio	
	Informações georreferenciadas – catálogo de feições	
	Descrição de recursos	Tabela 15 – Vocabulários e Ontologias
	Especificação de vocabulários para RDF	
	Sistemas de Organização do Conhecimento	
	Linguagem de definição de ontologias na web	

5 – Áreas de Integração para Governo Eletrônico	Linguagem para Execução de Processos	Tabela 16 – Temas Transversais
	Notação de Modelagem de Processos	
	Intercâmbio de Informações Financeiras	
	Legislação, Jurisprudência e Proposições Legislativas	
	Integração de Dados e Processos	
	Interoperabilidade entre sistemas de informação geográfica	
	Infraestrutura de registro	Tabela 17 – *Web Services*
	Linguagem de definição do serviço	
	Protocolo para acesso a *Web Service*	

3.1.1. Interconexão – Segmento 1

3.1.1.1 Especificações para Aplicação

Tabela 2: Aplicação

Componente	Especificação	Situação
Endereços de caixa postal eletrônica	Padrão de Formação de Endereços de Correio Eletrônico - Caixas Postais Individuais	A
Transporte de mensagem eletrônica	Produtos que suportem interfaces em conformidade com SMTP/MIME	A
Acesso à caixa postal	*Internet Message Access Protocol* – IMAP para acesso remoto à caixa postal	A
Mensageria em Tempo Real	Programas de correio eletrônico em conformidade com XMPP	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	A
Protocolos de transferência de arquivos	FTP (com reinicialização e recuperação) e HTTP	A
Diretório	LDAP v3	A
Sincronismo de tempo	RFC 5905 IETF – *Network Time Protocol* – NTP versão 4.0.	A
Serviços de Nomeação de Domínio	DNS. RFC 1035	A
Protocolos de sinalização	Protocolo de Inicialização de Sessão (SIP)	A
Protocolos de gerenciamento de rede	SNMP v3	R

Os nomes das caixas postais de correio eletrônico devem seguir os padrões estabelecidos no documento “Padrão de Formação de Endereços de Correio Eletrônico”, disponível no endereço http://www.eping.e.gov.br. Esse documento estabelece regras para a formação de nomes e composição de endereços eletrônicos (*e-mail*) e têm como base de referência, padrões internacionais definidos pela ITU (*International Telecommunications Union*).

O protocolo SMTP (*Simple Mail Transfer Protocol*) deve ser utilizado por servidores de correio eletrônico e aplicativos de transferência de mensageria para enviar e receber mensagens, enquanto que os aplicativos diretamente acionados pelos usuários finais devem utilizar esse protocolo apenas para enviar as mensagens ao servidor a que estejam diretamente conectados, que então assume a tarefa de dar prosseguimento ao tráfego dessas mensagens, para que cheguem a seu destino final.

Para receber mensagens, os aplicativos de usuários finais devem usar o protocolo IMAP (*Internet Message Access Protocol*), que apresenta inúmeras vantagens quando comparado ao protocolo POP3 (*Post Office Protocol V. 3*), no momento declarado em desuso. Aqui vale lembrar que a ePING restringe a utilização de tecnologias proprietárias para acesso às caixas postais de um servidor de correio eletrônico, embora não vede a utilização de sistemas proprietários para esse fim.

Para mensagens instantâneas, deve-se utilizar o protocolo XMPP (*Extensible Messaging and Presence Protocol*), em substituição ao protocolo IMPP (*Instant Messaging and Presence Protocol*), hoje em obsolescência.

A regulamentação para a troca de mensagens curtas, SMS (*Short Message Service*), que contenham não mais que 160 caracteres é de competência da ANATEL (Agência Nacional de Telecomunicações), cabendo à ePING fomentar serviços governamentais prestados ao cidadão utilizando essa tecnologia, hoje amplamente suportada pelo mercado, e acessível à grande maioria da população.

A gerência de porta 25 é o nome dado ao conjunto de políticas e tecnologias, implantadas em redes de usuários finais ou de caráter residencial, que procura separar as funcionalidades de submissão de mensagens, daquelas de transporte de mensagens entre servidores.

A definição do padrão para o protocolo de submissão é de 1998, sendo sua última revisão de 2011, no documento "**RFC 6409: Message Submission for Mail**". Este protocolo, chamado de "*Message Submission*", fornece um meio para distinguir uma submissão do transporte de mensagens, permitindo assim:

- a aplicação de políticas diferentes para cada tipo de conexão, impedindo *relays* não autorizados ou introdução de *e-mails* não solicitados;
- a implementação de autenticação na submissão, incluindo aquela realizada remotamente por usuários autorizados;
- a possibilidade de implementar, futuramente, melhorias no serviço de submissão.

A adoção do protocolo de *Message Submission* é uma boa prática reforçada na **RFC 5068 / BCP 134: *Email Submission Operations: Access and Accountability Requirements*** e que tem sido recomendada por diversos fóruns de combate ao *spam*, cabendo destacar as seguintes recomendações:

- *Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction* Messaging Anti-Abuse Working Group (MAAWG)
- Tecnologias e Políticas para Combate ao Spam - Comissão de Trabalho Anti-Spam do CGI.br.

Em seu **documento** o **MAAWG** recomenda para redes de caráter residencial, além da adoção de *Message Submission*, as seguintes medidas:

- requerer autenticação para a submissão de mensagens, como recomendado na **RFC 4954**;
- configurar o *software* cliente de *e-mail* para usar a porta 587/TCP e autenticação;

- bloquear acesso de saída para porta 25/TCP a partir de todas as máquinas que não sejam MTAs ou explicitamente autorizadas.

- não interferir no tráfego para a porta 587/TCP;

No primeiro *draft* do SSL v3.0, a Netscape recomendava a utilização da porta 465/TCP para submissão de mensagens via SMTPS. O uso desta porta para submissão de mensagens nunca tornou-se um padrão. Atualmente, a comunidade Internet considera o seu status como "*deprecated*", porém, alguns *softwares* clientes de *e-mail* e alguns servidores de submissão ainda utilizam esta porta.

A porta 465/TCP, segundo registro do IANA, está reservada para o uso do protocolo **URD** (*URL Rendesvous Directory for SSM*). A lista de portas registradas junto ao IANA pode ser econtrada em:**http://www.iana.org/assignments/port-numbers**.

- Resolução CGI.br/RES/2009/001/P – Recomendação para a Adoção de Gerência de Porta 25 em Redes de Caráter Residencial (CGI.br).

Devido a este fato, apesar de não constar explicitamente na recomendação do MAAWG, é importante que também não ocorra interferência no tráfego relacionado com outras portas que possam ser utilizadas para submissão, como a 80/TCP e a 465/TCP.

A figura a seguir ilustra a mudança de cenário em uma rede de caráter residencial, após a implementação de gerência de porta 25, ou seja, após a adoção de *Message Submission* pelos provedores de *e-mail* dos usuários e o bloqueio de tráfego de saída com destino à porta 25/TCP por parte das operadoras de banda larga.

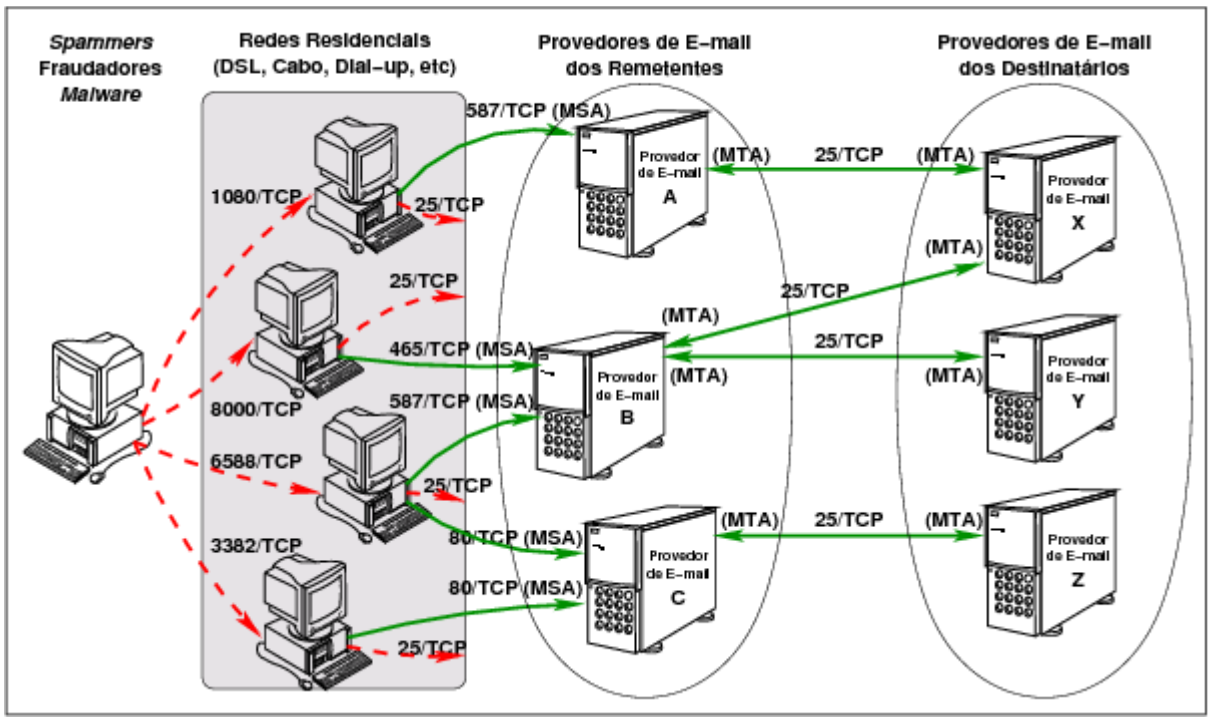


Figura 2: mudança de cenário em uma rede após a implementação de gerência de porta 25

Pode-se ver que o usuário, conectado via uma rede residencial, envia *e-mails* normalmente via *Mail Submission Port* (587/TCP) ou via *Webmail* (80/TCP). Mas, os *spammers*, fraudadores e códigos maliciosos não conseguem mais fazer a entrega direta dos *e-mails* para os provedores de destino, pois a saída de conexões para porta 25/TCP é impedida.

Com este novo cenário os *spammers* e fraudadores, provavelmente, adaptarão suas ferramentas para furtar as credenciais do usuário e se autenticar em seu MSAs (*Mail Submission Agents*) para o envio de*spam*. Mas, mesmo ocorrendo esta mudança para uso das credenciais do usuário, outro reflexo da implementação de *Message Submission* e Gerência de Porta 25 em redes de perfil residencial é que as mensagens abusivas são mais rastreáveis para os provedores de acesso. Pois, além do provedor poder implementar políticas de controle de vazão de *e-mails*, ele poderá identificar mais facilmente máquinas infectadas e usuários abusivos.

O HTTP/1.1 (*Hypertext Transfer Protocol V1.1*) é um protocolo de comunicação utilizado para sistemas de informação de hipermídia distribuídos e colaborativos. Seu uso para viabilizar o compartilhamento de recursos distribuídos a nível planetário levou ao estabelecimento e evolução da rede mundial (*World Wide Web*) como hoje a conhecemos. É natural então que esse seja o protocolo adotado pela ePING para a transferência de hipertexto.

Para a transferência de arquivos, a ePING adotou o próprio protocolo HTTP/1.1, que prevê mecanismos de reinicialização do processo de transferência sem perda dos dados já transmitidos e recebidos, e também de recuperação limitada de dados em caso de erros de comunicação. Também é

aceito o protocolo FTP (*File Transfer Protocol*) desde que utilizado com esses recursos de reinicialização e recuperação.

Para a pesquisa e atualização de diretórios, a ePING determina a utilização do protocolo LDAP (*Lightweight Directory Access Protocol*), versão 3. O termo "diretório" é utilizado para definir uma estrutura que permite o armazenamento sistemático, para posterior localização, de informações sobre organizações, pessoas e outros recursos como arquivos e dispositivos em uma rede, seja na Internet pública ou em uma intranet corporativa.

Outro serviço de rede a ser mencionado é o que trata a intercomunicação, em tempo real, entre computadores em todo o mundo, o que exige um mecanismo de sincronização de relógios que leve em conta os fusos horários, e que possa compensar e corrigir erros de marcação de tempo. Para tanto, foi criado ainda em 1985 o protocolo NTP (*Network Time Protocol*). Hoje em sua versão 4, o NTP pode garantir uma precisão entre relógios da ordem de 10 milissegundos (1/100 s) na rede pública Internet, podendo chegar a 200 microssegundos (1/5000 s) em redes locais. Quando uma precisão dessa ordem não se faz necessária, pode-se utilizar a versão simplificada desse protocolo conhecida com SNTP (*Simple Network Time Protocol*), de mais fácil administração. Os padrões NTP v3.0 e SNTP v4.0 são ambos recomendados pela ePING.

Quanto aos serviços de nomeação de domínio, deve-se seguir a RFC 1035, que descreve os detalhes do sistema de domínio e o respectivo protocolo.

O CGI (Comitê Gestor da Internet no Brasil) é o responsável por coordenar e integrar todas as iniciativas de serviços de Internet no país. No contexto de governo, o CGI definiu o uso das extensões *.gov* e *.mil* para identificar os sítios governamentais e militares, respectivamente. Além disso, ele regulamentou também os procedimentos de registro de domínio sob a raiz *.gov.br* que, além de serem isentos do pagamento de taxas, devem possuir autorização formal do Ministério do Planejamento, Orçamento e Gestão para a sua criação (CGI, 2008).

No caso de serviços de conferências multimídia envolvendo muitos participantes, é necessário que se possa sinalizar o estabelecimento, mudança ou término da sessão de maneira independente do tipo de mídia em utilização, tais como texto, áudio ou vídeo. Além disso, é preciso que seja possível adicionar ou remover participantes dinamicamente numa sessão *multicast*. O SIP (*Session Initiation Protocol*) foi desenvolvido e publicado pela IETF (*Internet Engineering Task Force*) em meados da década de 1990 para atender essas necessidades, em chamadas e conferências através de redes e via protocolo IP. A ePING determina a adoção do SIP como o protocolo de sinalização a ser utilizado nesses casos.

É importante lembrar também que uma rede de computadores precisa ser permanentemente monitorada para a detecção e correção de problemas que possam dificultar, ou mesmo impossibilitar, a comunicação entre os vários pontos que a integram. Com a grande diversidade e heterogeneidade de elementos de hardware e software hoje encontrados, o estabelecimento de um protocolo padrão a ser

seguido pelos programas de gerenciamento de redes é essencial para a eficiência e eficácia desse monitoramento. O SNMP (*Simple Network Management Protocol*) possibilita o intercâmbio de informação entre os diversos dispositivos de rede, como placas e comutadores, permitindo assim aos administradores gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e ainda coletar dados em tempo real que possam ser úteis no planejamento de sua expansão. A ePING recomenda a utilização da versão 3 desse protocolo.

3.1.1.2 Especificações para Rede/Transporte

Tabela 3: Rede/Transporte

Componente	Especificação	Situação
Transporte	TCP e UDP	A
Intercomunicação LAN/WAN	IPv6	A
Comutação por Label	MPLS (pelo menos quatro classes de serviço)	A
Qualidade de Serviço	DiffServ	A

O TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*) formam o núcleo de uma suíte de protocolos conhecida como TCP/IP. Enquanto o TCP normatiza o serviço de troca confiável de dados entre dois servidores, o IP trata do endereçamento e roteamento de mensagens através de uma ou mais redes de comunicação de dados. Com o advento da Internet, que deles faz uso em larga escala, esses protocolos passaram a fazer parte da rotina dos profissionais e dos setores responsáveis pela infraestrutura de TIC.

Praticamente todos os protocolos e aplicativos da Web (páginas web, transferência de arquivo, correio eletrônico etc.) utilizam o TCP como mecanismo de transporte subjacente. Nos casos em que o aplicativo não requeira um serviço confiável de fluxo de dados, o protocolo UDP (*User Datagram Protocol*) pode ser utilizado. O UDP fornece um serviço de datagramas, enfatizando latência sobre confiabilidade.

O IPv4 (*Internet Protocol version 4*) é ainda hoje a versão mais utilizada da suíte de protocolos IP, embora a versão que a sucederá, inicialmente chamada de SIPP (*Simple Internet Protocol Plus*) e agora conhecida simplesmente como IPv6 (*Internet Protocol version 6*), venha ganhando aceitação crescente. A principal diferença entre essas duas versões dizem respeito à estrutura de endereçamento utilizada: endereços de 32 bits no caso do IPv4, e de 128 bits no caso do IPv6.

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

No caso de redes de telecomunicação onde se necessita de alto desempenho, a ePING determina o uso do MPLS (*Multiprotocol Label Switching*), um mecanismo altamente eficiente e escalável para direcionamento e transporte de dados entre duas redes. O MPLS opera com o conceito de CoS (*Class of Service*, ou Classe de Serviço), utilizado para organizar o tráfego de dados em filas de prioridade. A ePING

requer que as implementações do MPLS trabalhem com pelo menos quatro classes de serviço. Por último, cabe ressaltar que a adoção do MPLS preclui a utilização das tecnologias alternativas, como ATM (*Asynchronous Transfer Mode*, ou Modo de Transferência Assíncrona) e *Frame-Relay*.

Nos casos em que não há a necessidade de implementação de MPLS (redes locais, por exemplo), é possível obter Qualidade de Serviço (QoS) com a implementação de DiffServ. Este protocolo permite um melhor aproveitamento do uso das redes através da priorização de pacotes, evitando casos em que uma simples aplicação ou serviço consuma o canal de comunicação e prejudique outros serviços oferecidos por aquela rede.

3.1.1.3 Especificações para Enlace/Físico

Tabela 4: Enlace/Físico

Componente	Especificação	Situação
Rede local sem fio	IEEE 802.11 g	A
	IEEE 802.11 n	R
Qualidade de Serviço – 802.1p		R
Virtual LAN	VLAN (IEEE 802.1Q)	R
Resiliência Layer2	Spanning tree protocol (802.1d, 802.1w, 802.1s)	R

As WLAN (*Wireless Local Area Network*, ou Redes Locais Sem Fio) devem seguir o conjunto de padrões conhecido como IEEE 802.11, na versão “g”, que normatizam a comunicação entre computadores utilizando a frequência de 2.4 GHz. O IEEE é a sigla do *Institute of Electrical and Electronic Engineers*, uma organização internacional dedicada à evolução e à aplicabilidade de tecnologias ligadas à eletricidade de maneira geral, e responsável pela criação e manutenção de um grande número de padrões técnicos.

O padrão IEEE 802.11n que foi criado pelo grupo TGn em 2003 teve sua aprovação no segundo semestre de 2009 e é recomendado pela ePING. As metas iniciais do padrão eram aumentar as taxas de transmissão ao nível das redes locais e assegurar a compatibilidade do novo padrão com os padrões antigos. O 802.11n tem como principal característica o uso de um esquema chamado Multiple-Input Multiple-Output (MIMO), capaz de aumentar consideravelmente as taxas de transferência de dados por meio da combinação de várias vias de transmissão (antenas). Com isso, é possível, por exemplo, usar dois, três ou quatro emissores e receptores para o funcionamento da rede.

Para ser aprovado o padrão IEEE 802.11n, o TGn definiu modos de operações para promover compatibilidade com os padrões 802.11 anteriores. Foram divididos em três modos de operações: HT, Non-HT e HT Mixed Mode.

- Um AP 802.11n usando o modo High Throughput (HT) - também conhecido como modo de Greenfield – assume que não existem estações legadas próximas usando a mesma faixa de frequência. Se estações legadas não existem, elas não podem se comunicar com o AP 802.11n. Modo de HT é opcional.

- Non-HT (Legacy) Mode - um AP 802.11n usando o modo não-HT envia todos os quadros utilizando o antigo formato dos padrões 802.11a / g para que as estações legadas possam entendê-las. Todos os produtos têm de suportar este modo a garantir compatibilidade com versões anteriores. Mas usar um AP 802.11n Non-HT não oferece nenhuma melhora de performance com relação 802.11a / g.

– O HT mixed mode é obrigatório e será o mais comum de funcionamento em APs 802.11n. Nesse modo, melhorias HT podem ser utilizadas simultaneamente com os mecanismos de proteção HT que permitem comunicação com estações legadas. HT modo misto fornece compatibilidade com versões anteriores, mas o padrão 802.11n tem perdas significativas na taxa de transferência em relação ao modo de Greenfield.

A utilização das tecnologias IEEE 802.11g e IEEE 802.11n devem também seguir as determinações do *Wi-Fi Alliance*, uma associação entre fabricantes de equipamentos de WLANs para certificação de produtos que atendam um conjunto de requisitos de interoperabilidade definidos por essa associação. Sempre que aplicáveis, as normas da ANATEL e da ANEEL (Agência Nacional de Energia Elétrica) também devem ser respeitadas.

O protocolo IEEE 802.1p é uma técnica para priorização de tráfego em redes locais, sendo especificado na norma IEEE 802.1D – LAN Bridges. Através dessa técnica, é possível utilizar aplicações sensíveis a tempo em redes locais (LANs).

A norma IEEE 802.1D inclui as extensões 802.1p e 802.1Q, adicionando 4 bytes ao formato do cabeçalho MAC das redes Ethernet e Token Ring. A extensão 802.1Q utiliza dois bytes desse espaço, sendo que 12 bits são reservados para identificação de VLAN (Virtual LAN) e 3 bits são definidos pela norma IEEE 802.1p a fim de determinar a prioridade no nível 2 do modelo OSI, conforme mostra a figura a seguir.

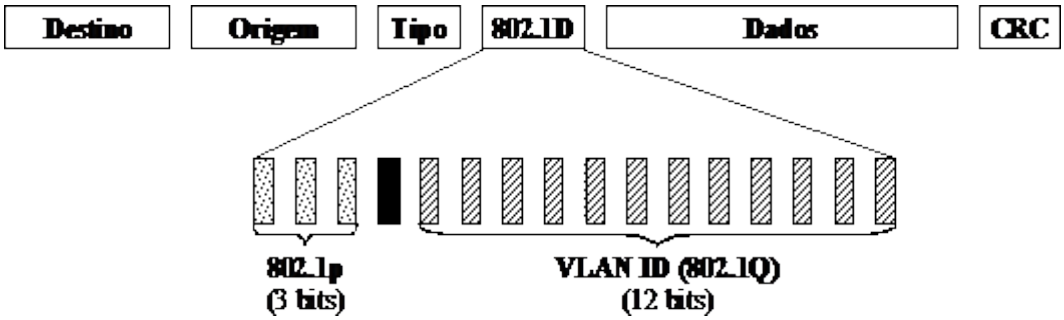


Figura 3: Representação das normas IEEE 802.1D, 802.1p e 802.1Q

Os 3 bits da norma IEEE 802.1p definem 8 classes de tráfego, como mostra a tabela a seguir.

Prioridade	Nome	Características e exemplos
7	Controle da rede	Aplicações críticas (RIP, OSPF, BGP4)
6	Voz interativa	Sensíveis à latência e jitter com baixa banda (Netmeeting, RAT)
5	Multimídia interativa	Sensíveis ao jitter com alta banda (picturetel, indeo)
4	Carga controlada	Aplicações sensíveis à latência (transações SNA)
3	Esforço excelente	Tráfego crítico que tolera atrasos (SAP, SQL)
2	Melhor esforço	Melhor esforço
1	Default	Default
0	Background	Insensíveis à latência (FTP, backups, pointcast)

Um padrão IEEE para provimento de capacidade de LAN virtual em uma rede, usada em conjunto com protocolos de LAN do IEEE, como Ethernet e Token Ring.

A utilização de VLAN (Virtual Local Area Network) permite que uma rede física seja dividida em várias redes lógicas dentro de um Switch. A partir da utilização de VLANs, uma estação não é capaz de comunicar-se com estações que não pertencem a mesma VLAN (para isto, é necessário a utilização de uma sub-rede por VLAN e que o tráfego passe primeiro por um roteador para chegar a outra rede.

A marcação efetuada (chamada de TAG) adiciona aos quadros Ethernet 4 bytes no frame original e calculam um novo valor de checagem de erro para o campo FCS.

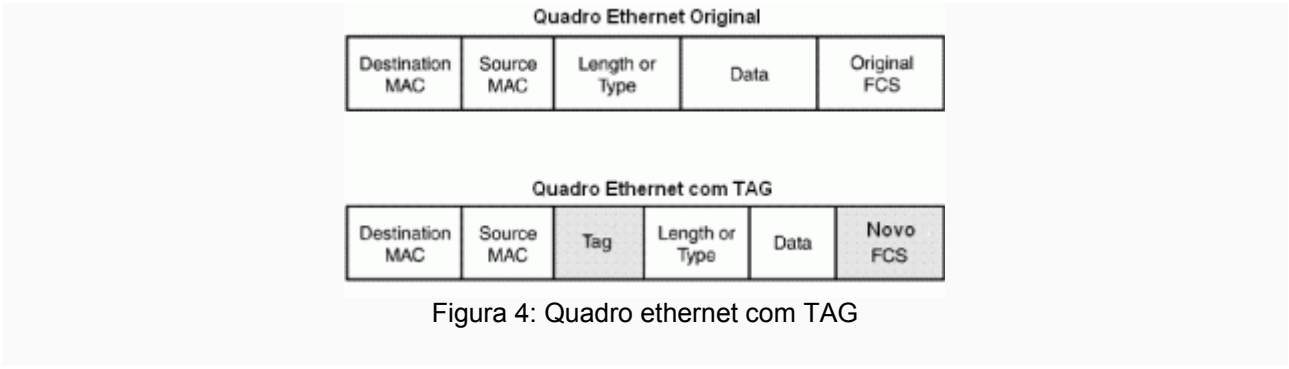


Figura 4: Quadro ethernet com TAG

Dos valores contidos dentro do campo TAG o número da VLAN é adicionado ao campo VLAN id permitindo a identificação da VLAN entre os Switches. Esse mecanismo de VLANs é bastante flexível, e permite organizar os computadores em domínios de broadcast distintos, independentemente de sua conexão física.

O crescimento das redes LANs, associado aos requisitos de qualidade e tolerância a falhas cada vez maiores, culminou em soluções de rede com topologias cada vez mais robustas, como nos casos de redes em anel. Tais implementações, com o intuito de garantir maior disponibilidade para as soluções e serviços, acabam por proporcionar redundância de caminhos de rede e, com isso, a possibilidade de ocorrência de *looping*.

Desse modo, surgiram alguns protocolos com o objetivo de garantir a resiliência na camada 2, além de otimizar a comunicação e os tempos de convergência quando da ocorrência de falhas:

802.11d

Para prevenir os congestionamentos broadcast e outros efeitos colaterais indesejados das ligações em loop, a empresa *Digital Equipment Corporation* criou o protocolo spanning tree (STP), que foi padronizado como a especificação 802.1d pelo IEEE - Institute of Electrical and Electronic Engineers. O protocolo spanning tree utiliza um algoritmo spanning tree (STA), que percebe que o switch tem mais de uma maneira de se comunicar com um nó de destino. Este protocolo determina o melhor caminho e bloqueia os outros (que ficam como caminho alternativo para o caso de falha no caminho principal), de modo a evitar *looping*.

802.11w

Em 2001 foi desenvolvido o Rapid Spanning Tree Protocol (RSTP), norma 802.1w, com a finalidade de acelerar o processo de alteração da árvore de suporte quando há alteração da topologia da rede, de modo que este processo de convergência possa acontecer num tempo muito mais curto, na casa dos milissegundos.

802.11s

O IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), proposto em 2002, é uma evolução do IEEE 802.1d Spanning Tree Protocol (STP). Com o crescente número de problemas associados ao aparecimento constante de esquemas mais complexos para as redes baseadas na camada 2 do modelo de OSI (Open Systems Interconnection), especialmente referentes à redundância e ao balanceamento de carga, foi desenvolvido o MSTP, tendo sempre em vista obter o menor impacto possível em termos de desempenho. Este novo protocolo veio trazer várias vantagens, fazendo uso de vários aspectos de outros protocolos como o Rapid Spanning Tree Protocol (RSTP) e Per-Vlan Spanning Tree (PVST).

Um exemplo representativo da utilização das diretrizes e recomendações da ePING para componentes de infraestrutura de rede pode ser encontrado no processo de aquisição de comutadores (*switches*) pelo Ministério do Planejamento, Orçamento e Gestão, conduzido no sítio do Comprasnet, com a publicação de três especificações de referência para diferentes famílias de dispositivos de comutação (COMPRASNET, 2010).

3.1.2. Segurança – Segmento 2

A ePING estabelece que os dados, informações e sistemas de informação do governo devem ser protegidos contra ameaças de forma a reduzir riscos e garantir sua integridade, confidencialidade, disponibilidade e autenticidade. Para tanto, é indispensável que os dados e informações sejam mantidos com o mesmo nível de proteção, independentemente do meio em que estejam sendo processados e armazenados, ou pelos quais estejam trafegando. Assim, as informações sensíveis que trafegam em redes inseguras, incluindo as redes sem fio, devem ser criptografadas de modo adequado, conforme os componentes de segurança por ela especificados.

A política de segurança da ePING enfatiza a necessidade de que essa questão seja tratada de forma *preventiva* e *global*. Por ser preventiva, a segurança requer a elaboração de planos de continuidade para sistemas que apoiam processos críticos, de forma a garantir níveis mínimos de produção. Por ser global, a segurança deve ser considerada em todas as etapas do ciclo de desenvolvimento de um sistema.

3.1.2.1 Especificações para Comunicação de dados

Tabela 5: Comunicação de Dados

Componente	Especificação	Situação
Transferência de dados em redes inseguras	TLS. 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	R
Hipertexto e transferência de arquivos	RFC 2818 (atualizada pela RFC 5785)	R
Segurança de redes IPv4	Autenticação IPSec, IKE para permutação de chaves, ESP como requisito para VPN	A
Segurança de redes IPv4 para protocolos de aplicação	S/MIME v3	A
Segurança de redes IPv6 na camada de rede	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

Garantir a integridade e confidencialidade dos dados transmitidos por redes de comunicação é, sobretudo, prevenir que terceiros tenham acesso indevido ou falsifiquem esses dados enquanto em trânsito. Para dados que trafegam em redes inseguras como a Internet, é indispensável a utilização de protocolos criptográficos. Esses protocolos tipicamente provêm a privacidade e a integridade dos dados trafegando entre duas ou mais aplicações através de dois mecanismos básicos: (i) autenticação das partes envolvidas, e (ii) cifração dos dados transmitidos entre as partes.

A **autenticação** busca garantir que um agente envolvido em uma interlocução ou troca de mensagens é de fato quem ele diz ser. A **cifração**, com o emprego de algoritmos matemáticos e parâmetros de controle chamados de **chaves criptográficas**, busca tornar a mensagem incompreensível e inútil para todos os efeitos, enquanto não for submetida ao processo inverso de **decifração**. São dois os mecanismos básicos de cifração/decifração hoje em utilização: (i) **criptografia simétrica** (ou de chave secreta), e (ii) **criptografia assimétrica** (ou de chave pública). Os algoritmos simétricos utilizam uma mesma chave tanto na cifração como na decifração, enquanto os algoritmos assimétricos utilizam chaves distintas em cada processo.

O esforço mais bem sucedido de construção de um protocolo criptográfico para a Internet foi o SSL (*Secure Socket Layer*) ou Protocolo Seguro da Camada de *Socket,* que utiliza PKI (*Public Key Infrastructure*) ou ICP (Infraestrutura de Chaves Públicas), um método assimétrico que emprega pares de chaves (uma pública, de acesso universal, e outra privada, de conhecimento exclusivo de seu proprietário) para garantir que (i) apenas o destinatário poderá conhecer o conteúdo da mensagem, e (ii) o destinatário estará seguro de que a mensagem originou-se do emitente declarado.

Com as modificações introduzidas na versão 3.1, o SSL passou a ser chamado de TLS (*Transport Layer Security*) ou Segurança da Camada de Transporte. A ePING recomenda a utilização do TLS v1 com todos os protocolos de transporte subjacentes que se baseiam no protocolo TCP, tais como HTTP, LDAP, IMAP, POP3 e Telnet. Uma vantagem do TLS v1, destacada na ePING, é sua capacidade de emular o SSL v3, útil em situações que requeiram esse nível de compatibilidade.

Quanto aos certificados digitais, a ePING recomenda o padrão X.509 v3, um padrão internacional para a Infraestrutura de Chaves Públicas que garante uma autenticação forte (em outras palavras, uma vinculação segura entre um certificado, seu emitente e seu destinatário). Esses certificados devem ser emitidos por entidades pertencentes à rede de entidades certificadoras conhecida como ICP-Brasil.

Quanto aos mecanismos internos inerentes à utilização do TLS v1, a ePING recomenda múltiplas alternativas de algoritmos, para cada caso: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS e DHE_RSA (definição de chaves de cifração), RC4, IDEA, 3DES e AES (troca de chaves durante o *hand-shake* de uma sessão), SHA-256 ou SHA-512 (implementação de funções de *hash*).

Para a complementação dos serviços oferecidos pelo TLS v1, a ePING recomenda a utilização do SASL (*Simple Authentication and Security Layer*). O SASL possibilita o desacoplamento entre mecanismos de autenticação e protocolos de aplicação, e também viabiliza um procedimento conhecido com *proxy authorization* (um usuário assume a identidade de outro, em um contexto de alta confiabilidade).

A ePING especifica que a segurança de redes IPv4 e IPv6 em suas múltiplas camadas deve ser implementada com os seguintes componentes:

- ***IPSec Authentication Header*** – autenticação de cabeçalhos IP;
- **IKE** (***Internet Key Exchange***) – negociação entre duas entidades para a troca de material de chaveamento;
- **ESP** (***Encapsulating Security Payload***) – implementação de redes privadas virtuais (VPNs) e autenticação e segurança de encapsulamento de pacotes IP;
- **S/MIME** (***Secure/Multipurpose Internet Mail Extensions***) – cifração genérica de mensagens MIME com criptografia de chave pública;
- **AH** (***Authenticaton Header***) – autenticação de cabeçalho com o protocolo Ipv6.

3.1.2.2 Especificações para Correio Eletrônico

Tabela 6: Correio Eletrônico

Componente	Especificação	Situação
Acesso a caixas postais	Cliente específico com mecanismos de segurança nativos ou HTTPS	A
Conteúdo de e-mail	S/MIME v3	A
Transporte de e-mail	SPF	A
Identificação de e-mail	DKIM	R
Assinatura	Padrão ICP-Brasil	A
Transporte seguro de e-mail	SMTP seguro sobre TLS	R

A ePING especifica que o acesso seguro a caixas postais eletrônicas pode ser feito através de dois mecanismos, considerados individualmente ou combinados: (i) utilização de aplicativos-cliente específicos que disponham de mecanismos de segurança nativos, e (ii) utilização do protocolo HTTPS (*HyperText Transfer Protocol Secure*). Esse protocolo permite a criação de um canal seguro na Internet pela combinação dos protocolos HTTP e SSL/TLS, esse último descrito na seção 3.4.1.

As mensagens de correio eletrônico seguro devem ser protegidas através do padrão S/MIME v3. Esse padrão disponibiliza os seguintes serviços de segurança criptográfica: (i) autenticação, (ii) integridade de conteúdo (iii) privacidade e (iv) não-repúdio da origem declarada. Esse último e importante serviço garante que o autor de uma mensagem assim protegida não conseguirá contestar com sucesso a alegada origem dessa mensagem, não podendo assim repudiar sua validade.

Para evitar a falsificação da origem de mensagens de correio eletrônico, a ePING recomenda que o transporte dessas mensagens utilize o sistema de validação conhecido como SPF (*Sender Policy Framework*). O objetivo do SPF é impedir que domínios da internet enviem mensagens personificando outros domínios sem a devida autorização, bloqueando assim uma prática com enorme potencial para fraudes.

Para a assinatura de mensagens seguras, a ePING determina a utilização de certificados digitais no padrão X.509 v3, emitidos por entidades pertencentes à rede certificadora ICP-Brasil.

3.1.2.3 Especificações para Criptografia

Tabela 7: Criptografia

Componente	Especificação	Situação
Algoritmo de cifração	3DES ou AES	R
Algoritmo para assinatura/hashing	SHA-256 ou SHA-512	R
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	A
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 ECIES 256 e ECIES 512	A
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3 FIPS 140-1 e FIPS 140-2	R
Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	Padrões da ICP – Brasil	R

A confiabilidade de um procedimento de cifração depende da qualidade e robustez do algoritmo utilizado. Para a cifração de conteúdo de qualquer natureza, a ePING recomenda a utilização dos algoritmos 3DES *Triple Data Encryption Algorithm*, ou DES Triplo) e AES (*Advanced Encryption Standard*, ou Padrão de Criptografia Avançada).

O 3DES é uma variante mais robusta do DES (*Data Encryption Standard*), um padrão instituído pelo governo americano em 1976. O DES é um mecanismo simétrico de cifração que utiliza chaves de 56 bits, adequadas ao panorama computacional daquela época, mas hoje incapazes de resistir a ataques de força bruta com os recursos de CPU disponíveis até em equipamentos de uso doméstico. Para compensar essa fraqueza, o 3DES usa três chaves em sequência: a informação é encriptada com a primeira chave, decriptada com a segunda, e por fim novamente encriptada com a terceira chave.

O AES (*Advanced Encryption Standard*) foi promulgado como padrão criptográfico do governo americano em 2002, após um longo processo conduzido pelo NIST (*National Institute of Standards and Technology*), que durou cerca de cinco anos, e onde se procurou selecionar através de concurso público um novo algoritmo de chave simétrica para proteger informações do Governo Federal. O AES é considerado pela maioria dos especialistas o estado da arte em algoritmo criptográfico. Ele combina com eficiência as características de segurança, desempenho, facilidade de implementação, flexibilidade e alta resistência a ataques. Além disso, ele demanda pouca memória e CPU, o que o torna adequado para utilização em plataformas de poder computacional relativamente baixo, como *smart cards*, PDAs e telefones celulares.

Em criptografia, uma função *hash* é um procedimento determinístico que recebe um bloco de informação de qualquer comprimento (chamado de *mensagem*), e retorna uma cadeia de caracteres de tamanho fixo (chamado de *digest*). Esse procedimento é útil para garantir a integridade de uma mensagem, uma vez que produzirá um *digest* diferente no evento de qualquer mudança, intencional ou acidental, na

mensagem original. As propriedades consideradas essenciais para esse tipo de procedimento são: (i) facilidade de computação do *digest* para mensagens de qualquer natureza, (ii) impossibilidade prática de obtenção de uma mensagem a partir de um *digest*, (iii) impossibilidade prática de modificação de uma mensagem com a manutenção do mesmo *digest* e (iv) impossibilidade prática de obtenção de duas mensagens distintas com o mesmo *digest*.

O SHA-2 (*Secure Hash Algorithm, version 2*) é uma família de funções *hash* desenvolvidas pela agência do governo norte-americano NSA (*National Security Agency*), com quatro variantes: SHA-224, SHA-256, SHA-384 e SHA-512 (que produzem *digests* de 224, 256, 384 e 512 bits, respectivamente). Enquanto todas essas variantes atendem as propriedades arroladas no parágrafo anterior, a ePING recomenda a utilização das variantes hoje mais usadas, SHA-256 e SHA-512.

Sistemas de criptografia simétricos, tais como 3DES e AES, são muito mais rápidos do que os assimétricos. Na prática, as mensagens são criptadas com um algoritmo simétrico, e as chaves utilizadas, em geral muito mais curtas do que as mensagens, são criptadas com um algoritmo assimétrico, tornando seguro o transporte das chaves entre os interlocutores. A ePING determina a utilização do algoritmo RSA (sigla construída a partir dos sobrenomes de seus inventores, Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman) como mecanismo criptográfico de chaves.

Publicado em 1978, o RSA é até hoje o mais bem sucedido mecanismo de criptografia assimétrica, e é a base para a Infraestrutura de Chaves Públicas. O RSA utiliza pares de chaves de comprimento variável, e quanto maior esse comprimento, maior a segurança proporcionada. Com o aumento de poder dos recursos computacionais disponíveis, e concomitante queda nos custos envolvidos, chaves cada vez maiores são necessárias para o mesmo nível de segurança. Hoje, o RSA é tipicamente utilizado com chaves de comprimento entre 1024 e 2048 bits, enquanto comprimentos inferiores a 512 bits já são considerados inseguros.

Em muitas situações, é necessário que a mesma segurança propiciada por algoritmos como RSA seja obtido com a utilização de números bem menores. Para essas situações, a ePING especifica que: (i) para assinaturas digitais, deve-se utilizar o ECDSA (*Elliptic Curve Digital Signature Algorithm*, ou Algoritmo de Assinatura Digital de Curvas Elípticas), nas variantes ECDSA 256 e ECDSA 512, e (ii) para cifração e transporte seguro de chaves criptográficas, deve-se utilizar o ECIES (*Elliptic Curve Integrated Encryption Scheme*, ou Esquema Integrado de Criptação com Curvas Elípticas), nas variantes ECIES 256 e ECIES 512.

O ECDSA é uma modificação do algoritmo DSA (*Digital Signature Algorithm*, ou Algoritmo de Assinatura Digital), enquanto o ECIES é uma variante do IES (*Integrated Encryption Scheme, ou Esquema Integrado de Criptação*). Tanto o ECDSA quanto o ECIES notabilizam-se por serem implementações da família ECC (*Elliptic Curve Cryptography*, ou Criptografia de Curvas Elípticas), uma área da criptografia que hoje desfruta de intenso interesse acadêmico e comercial.

A ePING recomenda que os módulos criptográficos utilizados, tais como equipamentos e sistemas de certificação digital, atendam os Níveis de Segurança de Homologação 2 e 3 (NSH-2 e NSH-3) da ICP-Brasil (ICP-BRASIL, 2009), ou os requisitos de segurança para módulos criptográficos publicados pelo *National Institute of Standards and Technology* (NIST, 2001).

3.1.2.4 Especificações para Desenvolvimento de Sistemas

Tabela 8: Desenvolvimento de Sistemas

Componente	Especificação	Situação
Assinaturas XML	XMLsig	A
Cifração XML	XMLenc	R
Assinatura e cifração XML	Transformação de decifração para assinatura XML	R
Principais gerenciamentos XML em ambiente PKI	XKMS 2.0	R
Autenticação e autorização de acesso XML	SAML	R
Intermediação ou Federação de Identidades	WS-Security 1.1 WS-Trust 1.4	R
Navegadores	*Cookies* apenas com a concordância do usuário	A

A ePING determina que os seguintes padrões de segurança sejam utilizados no desenvolvimento de sistemas, quando houver envolvimento de componentes XML (*Extensible Markup Language*) e de navegadores:

- **XMLsig** (XML Signature) – na assinatura de documentos e artefatos XML;
- ***Cookies*** – no controle da interação do usuário com o sistema através de navegadores, desde que obtida sua concordância.

A ePING recomenda a utilização dos seguintes padrões de segurança na utilização de documentos e artefatos XML em sistemas de computação:

- **XMLenc** (XML Encryption) – procedimentos a serem observados na criptação de documentos XML;
- **XKMS 2.0** (XML Key Management Specification) – para facilitar a interoperabilidade entre aplicações que fazem o uso da Infraestrutura de Chaves Públicas, através de dois componentes: (i) **XKISS** (*XML Key Information Service Specification*), que diz respeito à gestão da chave pública, e (ii) XKRSS (XML Key Registration Service Specification), que diz respeito à gestão da chave privada;
- **SAML** (Security *Assertion Markup Language*) - para a troca de informação sobre autenticação e autorização entre domínios;
- **WS-Security** 1.1 – para o fornecimento de segurança às mensagens SOAP (*Simple Object Access Protocol*), através da utilização dos padrões **XMLsig** e **XMLenc**;
- **WS-Trust** 1.3 – extensões ao **WS-Security** para a gestão de relacionamentos confiáveis entre os envolvidos na troca de mensagens seguras.

3.1.2.5 Especificações para Serviços de Rede

Tabela 9: Serviços de Rede

Componente	Especificação	Situação
Diretório	LDAP v3 e extensão para TLS	R
DNSSEC	Práticas de Segurança para Administradores de Redes Internet	A
Carimbo de tempo	TSP e TSAs Normas da ICP-Brasil	R

A ePING recomenda que a segurança de diretórios seja implementada com a extensão para TLS do LDAP v3. Para a transferência segura de arquivos, a ePING recomenda o protocolo HTTPS, que permite a criação de um canal seguro na internet pela combinação dos protocolos HTTP e SSL/TLS.

Para a resolução segura de endereços na internet, a ePING determina aos administradores implementar o padrão DNSSEC (*DNS Secure Extensions*, ou Extensões de Segurança do DNS), uma extensão do DNS (*Domain Name System*, ou Sistema de Nomes de Domínios) que reduz o risco de manipulação de dados e de utilização de domínios forjados.

O protocolo TSP (*Time-Stamp Protocol*, ou Protocolo de Carimbo de Tempo) deve ser utilizado sempre que houver a necessidade de se garantir que um artefato eletrônico existia antes de, ou em um momento particular de tempo. Esses carimbos de tempo usam certificados X.509 e a Infraestrutura de Chaves Públicas, e devem ser emitidos por TSAs (*Time-Stamping Authorities*, ou Autoridades Emissoras de Carimbo de Tempo), segundo procedimentos definidos pelo IETF, responsável pela manutenção desses dois padrões. Além disso, devem ser observadas as normas da ICP-Brasil sobre o assunto (ICP-BRASIL, 2008).

3.1.2.6 Especificações para Redes Sem Fio

Tabela 10: Redes Sem Fio

Componente	Especificação	Situação
LAN sem fio 802.11	WPA2	R

A ePING recomenda que a segurança de redes sem fio seja implementada com a utilização do padrão WPA2 (*Wi-Fi Protected Access, version 2*), uma evolução do padrão anterior WPA. O WPA2 requer testes e certificação pelos autores do padrão, a Wi-Fi Alliance, antes que um dispositivo possa se declarar em conformidade com ele.

3.1.2.7 Especificações para Resposta a Incidentes de Segurança da Informação

Tabela 11: Resposta a Incidentes de Segurança da Informação

Componente	Especificação	Situação
Preservação de registros	*Guidelines for Evidence Collection and Archiving*	R
Gerenciamento de incidentes em redes computacionais	*Expectations for Computer Security Incident Response* Norma Complementar Nº. 05/09	A
Informática Forense	*Guide to Integrating Forensic Techniques into Incident Response*	A

Os administradores devem estar preparados a dar respostas adequadas aos incidentes de segurança da informação que possam vir a ocorrer, quaisquer que sejam sua natureza ou origem. Para tanto, a ePING recomenda que sejam seguidas as orientações contidas em textos de referência internacional sobre preservação de registros (IETF, 2002) e informática forense (NIST, 2006), bem como em Normas Complementares específicas editadas pelo Gabinete de Segurança Institucional da Presidência da República (PRESIDÊNCIA DA REPÚBLICA, 2010). Em particular, são destacadas duas linhas de atuação: (i) criação de equipes especializadas no tratamento e resposta a incidentes, e (ii) organização de uma capacidade forênsica para a identificação, coleta, exame e análise de dados, mantendo a integridade da informação e a estrita cadeia de custódia desses dados.

3.1.3. Meios de Acesso – Segmento 3

3.1.3.1 Especificações para Meios de Publicação

Tabela 12: Meios de Publicação

Componentes	Especificação	Situação
Conjunto de caracteres	UNICODE, versão 7.0 e UTF-8	R
Formato de intercâmbio de hipertexto	HTML, versão 5	A
	XML, versões 1.0 e ou 1.1	A
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 (*.txt*)	A
	Open Document (*.odt*)	A
	ODF 1.2	R
	EPUB 3.0.1	R
	PDF	R
	PDF versão aberta PDF/A	R
Arquivos do tipo planilha	*Open Document* (*.ods*)	A
	ODF 1.2	R
Arquivos do tipo apresentação	*Open Document* (*.odp*)	A
	ODF 1.2	R
	HTML *(.htm* ou *.html*)	R
Arquivos do tipo “banco de dados” para estações de trabalho	XML, versões 1.0 ou 1.1 *(.xml*)	R
	MySQL Database (*.myd, .myi*)	R
	Texto puro (*.txt*)	A
	Texto puro (*.csv*)	A
	Arquivo do Base (*.odb*)	R
Intercâmbio de informações gráficas e imagens estáticas	PNG (.png)	A
	SVG (.svg)	R
	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)	R
Gráficos vetoriais	SVG (*.svg*)	R
Animação	SVG (*.svg*)	R
Áudio	Ogg Vorbis (.ogg, .oga)	R
	Ogg FLAC (.ogg, .oga)	R
	FLAC (.flac)	R
Vídeo	Ogg Theora (.ogg, .ogv)	R
	Matroska	R
Compactação de arquivos de uso geral	ZIP (*.zip*)	R
	GNU ZIP (*.gz*)	R
	Pacote TAR (*.tar*)	R
	Pacote TAR compactado (*.tgz ou .tar.gz*)	R
	BZIP2 (.bz2)	R
	Pacote TAR compactado com BZIP2 (*.tar.bz2*)	R

Informações georreferenciadas	GML, versão 2 ou superior	A
	ShapeFile	A
	GeoTIFF	A

3.1.3.1.1 Codificação dos Dados (*encoding*)

A interoperabilidade semântica para meios de publicação envolve, primeiramente, a definição do padrão para a representação e manipulação dos dados de acordo com a língua oficial do país. Neste caso, a ePING recomenda a adoção do padrão UNICODE, em detrimento do padrão ASCII (*American Standard Code for Information Interchange*), que não é mencionado no documento.

O UNICODE, que consiste na definição de pouco mais de 107 mil caracteres, permite a representação de informações em qualquer língua existente no mundo. Além da padronização dos caracteres, o UNICODE define toda uma metodologia para a codificação de caracteres e operações de teclado, por exemplo, operações com as teclas de funções (F1 a F12).

A manutenção do padrão UNICODE é realizada pelo *Unicode Consortium* e conta com a participação da ISO (Organização Internacional para Padronização). A última versão do UNICODE, versão 5.2.0, pode ser consultada no sítio do *Unicode Consortium* (UNICODE CONSORTIUM, 2010).

O UNICODE define dois métodos de mapeamento de caracteres: UCS (*Universal Character Set*) e UTF (*Unicode Transformation Format*). O UCS, conhecido como UCS-2, é um sistema de codificação de largura fixa, suportado apenas em sistemas obsoletos. O UTF, por sua vez, compreende os padrões UTF-7, UTF-8, UTF-16 e UTF-32. Os números (7, 8, 16 e 32) representam a quantidade de *bits* necessários para se codificar uma caracter. No que diz respeito à interoperabilidade semântica, é importante considerar os seguintes pontos:

- UCS-2 é considerado um padrão obsoleto, apenas suportado em sistemas legados.
- UTF-7 é considerado um padrão obsoleto, apenas suportado em sistemas legados.
- Arquivos codificados em UTF-8 com caracteres ASCII equivalem a arquivos em padrão ASCII.
- UTF-16 e UTF-32 são incompatíveis com arquivos codificados em ASCII.
- O UTF-8 é a codificação mais utilizada.

Como recomendação de boas práticas quanto ao uso de UNICODE, sugere-se:

- Para codificação de mensagens de cabeçalho de e-mail:

Content-Type: text/plain; charset="UTF-8"

ou

Content-Type: text/plain; charset="UTF-16"

- Para codificação de páginas HTML:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

ou

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-16">
```

☼ Para codificação de arquivos XML:

```
<?xml version="1.0" encoding="ISO-8859-1"?>

ou

<?xml version="1.0" encoding="UTF-8"?>

ou

<?xml version="1.0" encoding="UTF-16"?>
```

☼ Recomenda-se verificar o tipo de codificação que melhor atenda aos requisitos da informação que se deseja transmitir ou receber. Verifique a presença de acentuação e de caracteres estrangeiros, pois esse requisito pode significar a necessidade de se utilizar um tipo de UNICODE específico.

3.1.3.1.2 Formato de Intercâmbio de hipertexto

Outro aspecto relacionado à interoperabilidade semântica em meios de publicação envolve a transferência de dados em formato de hipertexto. A ePING adota como padrão o HTML (versão 5) e o XML (versões 1.0 e 1.1).

3.1.3.1.3 Especificações para Mobilidade

A ePING entende como um grande desafio para o governo possibilitar à sociedade o acesso aos produtos e serviços do governo eletrônico a partir de dispositivos móveis ou portáteis. A crescente aceitação desses dispositivos os torna canais privilegiados de comunicação com o cidadão, permitindo que se impulsione a inclusão digital via mobilidade. Entre esses dispositivos destacam-se notebooks, smartphones e, sobretudo, os telefones celulares.

O conceito fundamental que deve ser aplicado aos serviços a serem disponibilizados por meio dos dispositivos móveis é o da “web universal”: a internet disponível para todos, em qualquer lugar, independentemente do dispositivo de acesso. Sob essa perspectiva, a ePING recomenda a aderência às melhores práticas de implementação da web móvel definidas pelo Consórcio *World Wide Web* (W3C, 2008).

3.1.3.1.4 Arquivos do tipo documento/ publicação

A interoperabilidade semântica também implica no intercâmbio de arquivos nos mais diferentes formatos. Isso porque a utilização de formatos pouco conhecidos ou de uso não muito frequente dificulta ou impede que a informação seja recebida e decifrada adequadamente.

Nesse contexto, para a troca de arquivos do tipo documento, a ePING referencia como padrões Adotados (A), arquivos no formato de texto puro (*.txt*) e em formato *Open Document* (*.odt*). Adicionalmente, na impossibilidade de utilização desses dois padrões, pode-se optar pelo uso de arquivos XML (versões 1.0 e 1.1), com ou sem formatação baseada em XSL (*Extensible Stylesheet Language*), arquivos HMTL (versão 4.01) e arquivos no padrão PDF (*Portable Document Format*), onde se deve optar por sua versão aberta, PDF 1.4, quando necessária a preservação digital de documentos.

Para o intercâmbio de planilhas eletrônicas e arquivos de apresentação, a ePING Adota (A), respectivamente, os formatos *Open Document* (*.ods* e *.odp*).

Visando o recebimento de arquivos gerados por sistemas de banco de dados, a ePING Adota (A) como padrão obrigatório os formatos de texto puro (*.txt* e *.csv*). Outros formatos mencionados como Recomendados (R) são: XML (versão 1.0 e 1.1), *MySQL Database* (versão 4.0 ou superior) e *Open Office Base* (*.odb*).

No que diz respeito à troca de imagens no setor público, deve-se adotar os padrões PNG (*.png*). Na impossibilidade de uso desses padrões, a ePING recomenda o uso dos formatos SVG (*.svg*) e JPEG (*.jpeg, .jpg ou jfif*).

Para o tratamento de gráficos vetoriais nenhum padrão é definido como Adotado (A) na ePING. Entretanto, há a recomendação pelo uso do formato SVG (*.svg*). A ePING também referencia o formato SVG (*.svg*) como Recomendado (R) para a definição de arquivos de animação.

No que tange ao uso de arquivos de áudio e vídeo, a ePING ainda não define nenhum formato como Adotado (A). No entanto, recomenda o uso dos seguintes padrões: FLAC, Matroska, Ogg Vorbis - formato aberto para *streaming* de áudio (*.oga*) e *Theora (.ogv)*. Os formatos que devem ser evitados, segundo a ePING, são: *Audio-Video Interleaved* (*.avi*) com codificação divX ou Xvid, MPEG-4 e WAVE (*.wav*).

Para o intercâmbio de informações georreferenciadas, deve-se adotar: GML (versão 2.0 ou superior), *ShapeFile* ou *GeoTIFF*.

Por fim, no que diz respeito à compactação de arquivos para envio, recomenda-se todos os principais formatos atualmente em uso, quais sejam: ZIP (*.zip*), GNU ZIP (*.gz*) e pacote TAR (*.tar*, *.tgz*).

3.1.3.2 Especificações para TV Digital

Tabela 13: TV Digital

Componente	Especificação	Situação
Transmissão	Norma ABNT NBR 15601 Parte 1 – Sistema de transmissão	A
Codificação	Norma ABNT NBR 15602 Parte 1 – Codificação de Vídeo Parte 2 – Codificação de Áudio Parte 3 – Sistema de multiplexação de sinais	A
Multiplexação	Norma 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	Norma ABNT NBR 15604 Parte 1 – Receptores	A
Segurança	Norma ABNT NBR 15605 Parte 1 – Tópicos de segurança	A
Middleware	Norma 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 5 – Ginga-NCL para receptores portáteis Linguagem de aplicação XML para codificação de aplicações Parte 6 – Java DTV 1.3 Parte 7 – Ginga-NCL – Diretrizes Operacionais para as ABNT NBR15606-2 e 15606-5	A
Canal de Interatividade	Norma ABNT NBR 15607 Parte 1 – Protocolos, interfaces físicas e interfaces de software	A
Guia de Operação	Norma 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

O SBTVD (Sistema Brasileiro de Televisão Digital), ora em implantação e com cobertura nacional prevista para dezembro de 2016, além de propiciar som e imagem digitais de superior qualidade técnica, permite ao usuário (ou telespectador) interagir com o aparelho de televisão através de seu controle remoto. Isto traz à televisão a possibilidade de torná-la meio de acesso a serviços como compras, acesso a bancos e opções diversas de recreação e lazer. Mais importante ainda, isso a transforma em canal de grande potencial de relacionamento entre governo e sociedade. Atividades como tele-educação, consultas ao FGTS, ao PIS e a outros programas sociais do governo, dentre outras, farão com que os cidadãos passem de uma atividade essencialmente passiva para uma atividade participativa. A ePING adota, às implementações de interatividade para a TV digital, a aderência às normas pertinentes publicadas pela ABNT (Associação Brasileira de Normas Técnicas), o órgão responsável pela normalização técnica no país.

Uma recomendação da ePING na implementação de soluções para a TV digital digna de nota é a do Ginga, um *middleware* aberto para o desenvolvimento de aplicativos para o SBTVD. Ele é constituído por um conjunto de tecnologias padronizadas e de inovações brasileiras, sendo organizado em dois subsistemas: (i) Ginga-J, para aplicações procedurais no ambiente de desenvolvimento Java, e (ii) Ginga-NCL, para aplicações declarativas escritas em NCL (*Nested Context Language*). O Ginga é resultado de projetos de pesquisa coordenados pelo Laboratório de Sistemas Multimídia da PUC-Rio, em conjunto com o Laboratório de Aplicações de Vídeo Digital da Universidade Federal da Paraíba (GINGA, 2006).

3.1.4. Organização e Intercâmbio de Informações – Segmento 4

3.1.4.1 Especificações para Tratamento e Transferência de Dados

Tabela 14: Tratamento e Transferência de Dados

Componentes	Especificação	Situação
Linguagem para intercâmbio de dados	XML	A
	JSON	
Transformação de dados	XSL XSLT	A
Definição dos dados para intercâmbio	XML *Schema*	A
Informações georreferenciadas – catálogo de feições	Estruturação de Dados Geoespaciais Vetoriais (EDGV) como definido pela CONCAR	R

Para a criação da informação que será enviada a outro sistema ou unidade de processamento computacional, a ePING adota, como formato padrão, o XML. Para a verificação das regras de formação dos dados, adota-se o padrão XML *Schema*. Finalmente, para a transformação dos dados com o objetivo de apresentação ao usuário final, adota-se o XLS.

3.1.4.1.1 Linguagem para Intercâmbio de Dados (XML)

O uso de XML como linguagem para representação de dados é uma peça fundamental no contexto da interoperabilidade semântica, pois representa tanto os aspectos conceituais quanto tecnológicos associados a uma arquitetura de software que se preocupa em organizar a informação, ao mesmo tempo em que promove o seu intercâmbio. Entretanto, lidar com essa tecnologia não é tarefa trivial. Pelo contrário, exige planejamento e estratégias de projeto elaboradas pela equipe de arquitetos, projetistas e desenvolvedores de *software*.

Logo, recomendam-se os seguintes passos para o uso adequado de XML nas instituições públicas:

- ☼ Posicione a tecnologia XML no conjunto de componentes da arquitetura de software adotada.
- ☼ Realize a etapa de modelagem dos arquivos XML.
- ☼ Defina padrões para nomear os elementos do arquivo XML.
- ☼ Escolha a API correta (DOM, SAX ou *Data Binding*).

Quanto ao posicionamento da tecnologia XML a uma arquitetura de software definida, sugerem-se quatro abordagens: (i) utilizar XML para o transporte de informações dentro da própria aplicação a ser desenvolvida; (ii) utilizar XML para o transporte de informações entre aplicações; (iii) utilizar XML como conversor de dados no contexto de uma aplicação; e (iv) utilizar XML como conversor de dados no contexto de várias aplicações (ERL, 2004).

Quando o XML é utilizado para o transporte de informações dentro da própria aplicação a ser desenvolvida, é importante que se identifique as camadas da aplicação onde a informação será originada e onde a informação será recepcionada. Com isso, verifica-se a consistência do fluxo de dados dentro da própria aplicação e evita-se o excesso de tráfego de informações desnecessárias. A Figura 5 ilustra esse uso do XML, considerando duas camadas de uma arquitetura MVC (*Model-View-Controller*).

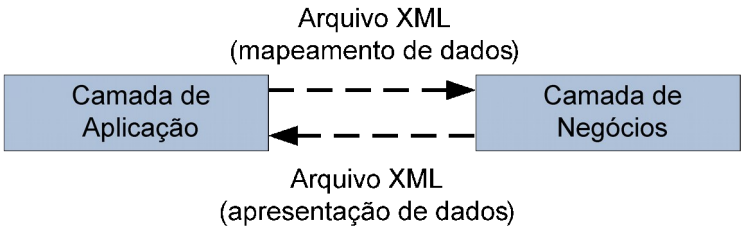


Figura 5: XML utilizado para transportar dados dentro de uma aplicação.

Quando o XML é utilizado para o transporte de informações entre aplicações, a ePING adota como padrão o uso da tecnologia de *Web Services*. Assim, a informação em formato XML é transportada através de mensagens SOAP. Para saber mais sobre *Web Services*, consulte a seção 3.6.4 neste documento, que trata do assunto sob a ótica da interoperabilidade técnica. A Figura 6 ilustra o processo de transporte de um arquivo XML, considerando o uso da tecnologia de *Web Services*.

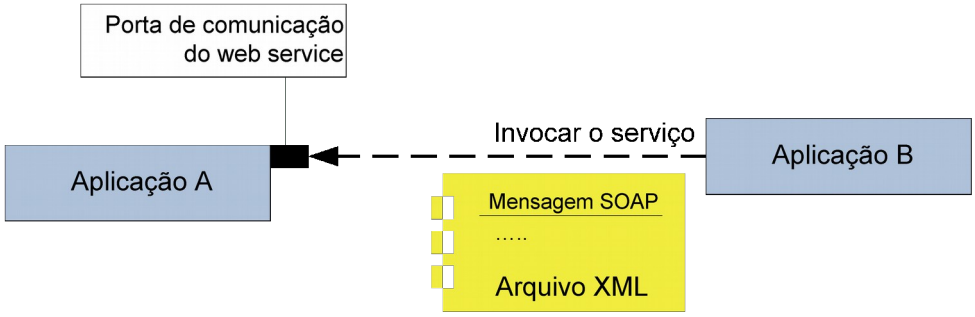


Figura 6: XML utilizado para transportar dados com a tecnologia de *Web Services*.

Quando o XML é utilizado como conversor de dados no contexto de uma aplicação, devem-se utilizar ferramentas específicas para realizar a conversão. A escolha do conversor mais adequado deve considerar o uso de APIs (*Application Programming Interfaces)* específicas para o tratamento de arquivos no formato XML (DOM, SAX ou *Data Binding)*. A Figura 7 ilustra o processo de utilização de XML como conversor de dados no contexto de uma aplicação.

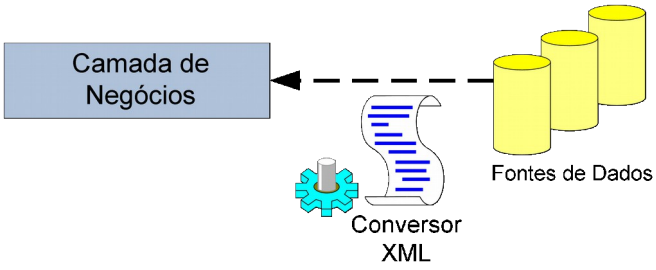


Figura 7: XML utilizado como conversor de dados no contexto de uma aplicação.

Quando o XML é utilizado para consolidar informações de diferentes fontes de dados, uma aplicação (consumidor) invoca o serviço de troca de dados em outra aplicação (provedor) utilizando a tecnologia de *Web Services*. A aplicação de destino, por sua vez, processa a requisição utilizando-se de um conversor de dados XML que pode se comunicar com outras partes do sistema de destino para executar o processamento. A Figura 8 ilustra esse caso de utilização de XML.

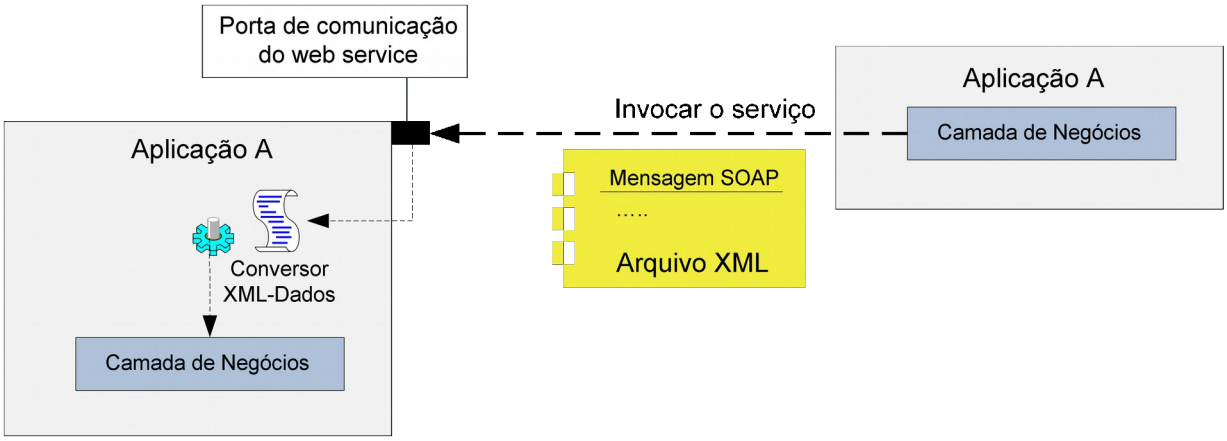


Figura 8: XML utilizado como conversor de dados no contexto de várias aplicações.

Após o posicionamento da tecnologia XML em relação à arquitetura de software utilizada, recomenda-se a realização da modelagem dos arquivos XML. Esta é, sem dúvida, a atividade mais importante para o projeto de sistemas que interoperam através da tecnologia XML, pois é através dela, que se minimizam as chances de alteração da estrutura do arquivo XML no futuro. Logo, os profissionais de TI devem compreender que os arquivos XML são comparáveis às estruturas de bases de dados, no sentido de que também mantêm as informações para uso futuro. Isso implica em dizer que, assim como os bancos de dados necessitam de modelos, a estrutura dos arquivos XML também precisa ser modelada. A Figura 9 fornece uma comparação das estruturas de banco de dados com aquelas em formato XML (ERL, 2004). Como se pode perceber, os esquemas de banco de dados representam o resultado da modelagem de dados no contexto de um SGBD (Sistema Gerenciador de Banco de Dados). Da mesma maneira, os XML *Schemas* representam o resultado da modelagem dos arquivos XML, pois ditam as regras para a validação da estrutura de dados de acordo com os requisitos de negócio que se pretende atender.

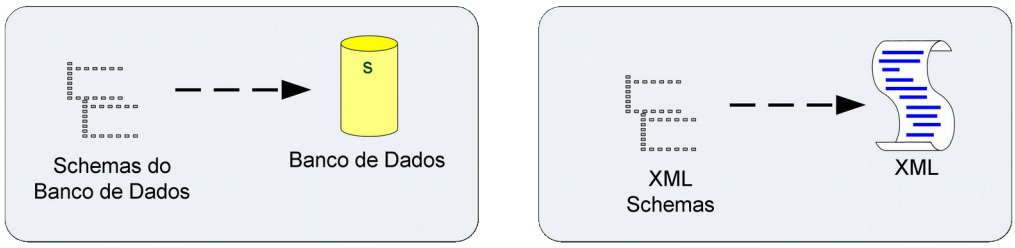


Figura 9: Comparação das tecnologias de Banco de Dados e XML
(Modificado de Erl, 2004)

Um ponto de grande importância a ser observado pelos profissionais de TI durante a modelagem dos arquivos XML diz respeito à nomeação dos elementos que compõem esse arquivo propriamente dito. Este aspecto da modelagem em XML é bastante controverso se o considerarmos sob o ponto de vista da interoperabilidade semântica e dos requisitos técnicos de desempenho dos sistemas. Por um lado, ter um nome de elemento XML mais completo e consequentemente maior é bom para garantir a compreensão daquele item de dado, o que atende ao requisito da interoperabilidade semântica. Por outro lado, modelar elementos XML muito extensos gera arquivos relativamente maiores e que exigem melhor desempenho das aplicações para processá-los, e também maior banda de rede para distribuí-los. Assim, essa Cartilha Técnica sugere as seguintes práticas para lidar com esse tipo de problema:

- Identifique claramente quem serão os consumidores dos arquivos XML a serem modelados. Caso tais arquivos sejam consumidos apenas por sistemas e não por pessoas, considere reduzir o tamanho dos arquivos, utilizando nomes menores para os elementos XML.
- Para atender aos requisitos de interoperabilidade semântica, faça uso de comentários sempre que identificar que alguns elementos foram nomeados de forma muito reduzida.
- Utilize nomes genéricos, evitando incluir nome de departamentos ou do órgão diretamente no nome dos elementos XML.
- Evite redundâncias. Sempre que um elemento XML pertencer a outro elemento-pai, evite repetir o nome do elemento-pai quando nomear o elemento filho. Por exemplo, um elemento NumCodigoItemNotaFiscal seria melhor nomeado como NumItem ou CodItem, pois o mesmo já pertence a um elemento-pai que corresponde aos Itens de uma Nota Fiscal.
- Para distribuir arquivos XML extensos pela rede, considere a utilização de tecnologias de compressão de dados.

Outra questão associada aos elementos XML e que gera muita discussão diz respeito ao uso de atributos no lugar de simples elementos XML. Esse é um problema complexo que pode envolver diversas considerações associadas ao projeto de um sistema de informações. Assim, a recomendação primária dessa Cartilha Técnica é utilizar o bom senso na decisão de se representar uma informação como um atributo ou um elemento XML. Considere, sempre que possível, as seguintes práticas, descritas por ordem de importância:

- ☼ Se a informação é uma parte essencial (importante) para o negócio que se pretende comunicar, represente-a como um elemento XML. Caso contrário, se a informação for periférica ou incidental, puramente utilizada para auxiliar o processamento dos dados, represente-a como um atributo XML. Um exemplo prático é o identificador ou ID. Caso este seja apenas um recurso utilizado para apropriadamente processar a informação, represente-o como um atributo e não como um elemento XML. Lembre-se que: *Dados são representados como elementos e Metadados como atributos*.
- ☼ Se a informação pode sofrer alterações em sua estrutura no futuro, represente-a como um elemento. Caso contrário, se a informação é atômica, não podendo ser desmembrada em diversas estruturas no futuro, considere representá-la como um atributo. Como exemplo, pode-se citar o nome de uma pessoa representado como um atributo. Neste caso, alterações futuras seriam afetadas se fosse necessário representar esse nome como sendo a composição de primeiro nome, nomes intermediários e nome de família.
- ☼ Se a informação que se pretende transmitir será lida por pessoas, represente-a como um elemento. Caso contrário, se a informação for processada unicamente por máquinas, utilize atributos.

Além da modelagem dos arquivos XML, outra atividade importante a ser executada pelos profissionais de TI é a escolha da API a ser utilizada no processamento das informações contidas no arquivo XML. As opções atuais são: DOM (*Document Object Model*), SAX (*Simple API for XML*) e *Data Binding*.

DOM é a interface de programação tradicional favorecida pelo W3C. Uma das características dessa API e também a sua maior desvantagem é que, ao se processar o arquivo XML, todo o seu conteúdo é carregado para a memória do computador. Isso permite o acesso completo em toda a árvore de elementos do XML, mas ao custo de um grande consumo de memória, o que pode significar sérios problemas de desempenho e falta de memória quando do processamento de arquivos XML mais extensos.

Como forma de contornar os problemas causados pelo DOM, surgiu o SAX, uma alternativa mais leve para o processamento de arquivos XML de qualquer tamanho. A API SAX teve origem em um grupo de discussões chamado XML-DEV promovido pelo OASIS (*Organization for the Advancement of Structured Information Standards*) com o objetivo de solucionar problemas de incompatibilidade entre os diferentes *parsers* de XML existentes no mercado. Essa API alcançou uma rápida popularidade por ter sido originalmente criada para atender à comunidade de programadores Java. Entretanto, atualmente já existem várias implementações dessa API em diversas linguagens de programação, incluindo versões *open-source* e proprietárias.

É importante salientar que a especificação e implementação da API SAX são mantidas atualmente por um grupo de programadores independentes. A ideia da API SAX é bem simples, se comparada com o DOM. Enquanto o DOM monta toda a árvore de elementos XML de uma única vez, a API SAX provê uma arquitetura mais dinâmica que permite que os elementos XML sejam encontrados e retornados em resposta a situações predeterminadas. Assim, na arquitetura SAX, em vez de pedir ao *parser* XML que retorne toda a

estrutura do arquivo XML, requisita-se ao *parser* disparar um evento quando a informação de interesse for encontrada. Maiores informações sobre essa API podem ser consultados no sítio http://www.saxproject.org.

Outra abordagem para o processamento de arquivos XML é a utilização de APIs que implementam o conceito de *Data Binding*. Essa nova abordagem surgiu da necessidade de se relacionar automaticamente as informações de um arquivo XML com os elementos representados em campos de tabelas de banco de dados ou em atributos/propriedades de classes implementadas em diversas linguagens de programação. Assim, em vez de utilizar uma abordagem centrada na estrutura do arquivo XML, como é o caso do DOM e SAX, as APIs que utilizam o conceito de *Data Binding* aplicam uma abordagem centrada nos dados e no seu mapeamento adequado. Com isso, pretende-se economizar código de programação, ao mesmo tempo em que se produz soluções mais padronizadas, uma vez que mesmo utilizando DOM e SAX algum tipo de mapeamento de dados deve ser fornecido.

Soluções de processamento de arquivos XML baseadas em *Data Binding* podem fornecer também outras vantagens, como por exemplo, a conversão de dados e a geração em tempo de execução de classes de negócio baseadas nos modelos XML *Schemas* associados ao arquivo XML. Essa abordagem, entretanto, também traz algumas limitações. Dependendo da API utilizada, podem ocorrer problemas tanto na interpretação correta dos elementos do arquivo XML, quanto na geração de arquivos XML como resultado de um processamento.

Como se pode observar, a escolha da melhor abordagem para o processamento de arquivos XML depende de diversos fatores e deve ser uma atividade discutida entre os membros técnicos da equipe de arquitetura. Como forma de direcionar essas discussões, são relacionadas a seguir algumas recomendações práticas envolvendo esse tema (ERL, 2004):

- Utilize DOM:
  - Quando se tratar de arquivos XML de pequeno ou médio porte (com menos de 1000 elementos).
  - Quando houver necessidade de modificar a estrutura do documento XML em tempo de execução.
  - Quando houver necessidade de acesso imediato à toda estrutura do arquivo XML.

- Utilize SAX:
  - Quando se tratar de arquivos XML grandes (com mais de 1000 elementos).
  - Quando o processamento por DOM for muito lento.
  - Quando houver necessidade de acessar apenas parte do conteúdo do arquivo XML.

- Utilize APIs baseadas em *Data Biding*:
  - Quando houver requisitos claros de se construir uma interface orientada a objetos para o processamento de arquivos XML.
  - Quando houver a necessidade de simplificar a lógica de programação para acesso e mapeamento de dados.

☼ Quando a API selecionada não representar problemas no processamento e geração de arquivos XML de acordo com a especificação padrão, sem a adição de extensões proprietárias.

Como se pode observar, trabalhar com arquivos XML requer muito mais do que simplesmente se promover a estruturação da informação no formato de *tags*. É importante considerar todos os aspectos associados a essa nova tecnologia, sejam eles de desempenho, segurança de dados, estratégia de desenvolvimento acelerado e padronizado de software ou da modelagem e estruturação da informação. É importante, antes de tudo, definir um planejamento, organizar os dados e tomar decisões acertadas envolvendo arquitetura de *software* e a utilização de ferramentas de produtividade.

3.1.4.1.2 Linguagem para Intercâmbio de Dados (JSON)

O JSON (*JavaScript Object Notation*) é um padrão baseado em texto, derivado da linguagem *JavaScript*, e que tem como objetivo prover um formato aberto para a troca de dados entre plataformas de *hardware* e *software* heterogêneas. Diferentemente do padrão XML, o JSON se propõe a ser um padrão que seja, ao mesmo tempo, de fácil leitura e escrita para o usuário comum e passível de ser processado por computadores. (JSON.ORG, 2009).

O JSON foi criado por Douglas Crockford por volta de 2001 e em 2002 ele foi divulgado na Internet através do sítio da organização JSON (JSON.ORG, 2009). A partir de 2005 empresas como Yahoo! e Google aderiram ao padrão como meio de promover o intercâmbio de dados e em julho de 2006, após a grande e rápida aceitação do padrão pelo mercado, Douglas Crockford formalizou a especificação do JSON através da RFC 4627 (CROCKFORD, 2006).

O JSON tem sido bastante utilizado para transmitir dados entre um servidor e uma aplicação *Web*, servindo assim como uma alternativa ao padrão XML. Ele difere, no entanto, do XML, principalmente porque é um padrão muito simplificado e não baseado na estrutura de *tags*, o que também limita a sua utilização em casos onde a semântica da informação deve ser garantida. Em contrapartida, a limitação apresentada quanto à semântica se traduz em ganho na representação mais reduzida da informação que se pretende transmitir. Alguns adeptos desse padrão acreditam que um documento JSON apresenta tamanho 30% menor que o mesmo arquivo representado em XML (JSON.ORG, 2009).

Um arquivo JSON possui a extensão .json e é referenciado pelos protocolos de Internet através do MIME *type* application/json. Os tipos de dados básicos suportados pelo JSON são: (i) números (*integer* ou *real*), (ii) texto (*string*), (iii) valor lógico (*boolean*), (iv) sequência de valores (*array*), (v) coleção de dados, definidos por pares do tipo chave e valor (*object*), (vi) tipos de dados vazio ou nulo (*null*). A Figura 10 ilustra um exemplo de descrição dos dados de uma pessoa no padrão JSON.

```
{
    "primeiroNome": "Maria",
    "ultimoNome": "Silva",
    "endereco":
    {
        "logradouro": "Rua 11 de Novembro",
        "cidade": "Sao Paulo",
        "estado": "SP",
    }
}
```

Figura 10: Exemplo de um arquivo JSON

3.1.4.1.3 Transformação de Dados (XSL)

Outro padrão da família XML é o XSL, utilizado para criar folhas de estilo e, com isso, formatar um documento XML para apresentação. A ideia de aplicação do XSL é bastante simples: um programa processador de XSL, também chamado de *engine* XSL, transforma o documento XML em outro tipo documento, pronto para exibição. Neste novo documento, a informação é associada com diferentes tipos de formatação, cores e leiautes atrativos.

Um ponto de discussão bastante interessante associado à tecnologia de XSL é a sua diferenciação de outro padrão, também da família XML, denominado XSLT (*Extensible Stylesheet Language Transformations*). O padrão XSL puro, como é conhecido, compreende o uso de dois padrões: XSLT e o XSL-FO (XSL *Formatting Objects*). O XSLT define uma linguagem para a conversão de um documento XML em outro formato de documento. O XSL-FO, por sua vez, define uma linguagem para formatar um documento XML para exibição ou impressão independentemente de plataforma. Isso pode ser um pouco confuso de se compreender, pois os dois padrões constituem o XSL, porém, é importante entender que cada padrão pode ser utilizado de forma independente.

Uma aplicação XSL clássica é aquela que utiliza XSLT para ler um arquivo XML e, a partir dele, criar um documento do tipo XSL-FO. Em seguida, esse arquivo XSL-FO é tratado por um *engine* específico para tratamento de arquivos XSL que gera, como resultado final do processamento, um arquivo formatado para impressão ou para visualização, por exemplo, em formato PDF. Como as etapas deste processo são independentes, é possível que o documento XSL-FO seja criado através de outro método, e não pela utilização de XSLT. Alternativamente, é possível também utilizar XSLT para a criação de outros tipos de documentos, não necessariamente de arquivos XSL-FO. Essa última alternativa é mais comumente utilizada, principalmente para a geração de documentos do tipo HTML, texto simples e outros formatos como o SVG (*Scalable Vector Graphics*) e WML (*Wireless Markup Language*).

Como o uso de XSLT tem sido bastante difundido e a tecnologia tem provado ser madura o suficiente para justificar sua adesão por parte dos profissionais de TI, seu uso no desenvolvimento de aplicações governamentais é recomendado, seja para a conversão de um formato de documento em outro, ou para padronizar a forma de apresentação das informações.

As Figuras 11 e 12 apresentam respectivamente um exemplo de documento XML e XSL. A Figura 13 ilustra o resultado final da transformação XSL sobre a informação contida no documento XML.

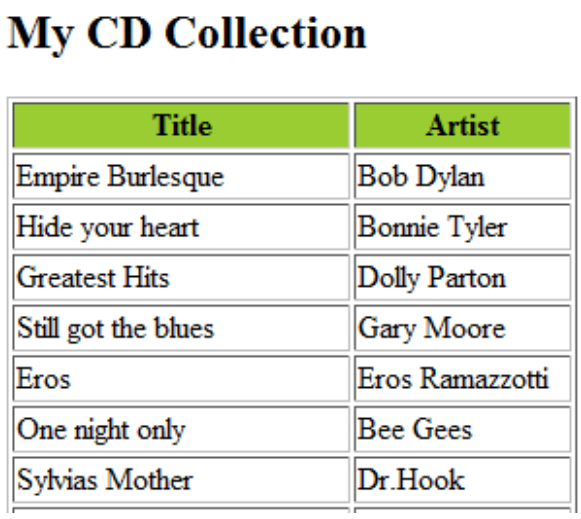
```
<?xml version="1.0" encoding="iso-8859-1"?>
<catalog>
  <cd>
    <title>Empire Burlesque</title>
    <artist>Bob Dylan</artist>
    <country>USA</country>
    <company>Columbia</company>
    <price>10.90</price>
    <year>1985</year>
  </cd>
  <cd>
    <title>Hide your heart</title>
    <artist>Bonnie Tyler</artist>
    <country>UK</country>
    <company>CBS Records</company>
    <price>9.90</price>
    <year>1988</year>
  </cd>
  <cd>
    <title>Greatest Hits</title>
    <artist>Dolly Parton</artist>
    <country>USA</country>
    <company>RCA</company>
    <price>9.90</price>
    <year>1982</year>
  </cd>
  <cd>
    <title>Still got the blues</title>
    <artist>Gary Moore</artist>
    <country>UK</country>
    <company>Virgin records</company>
    <price>10.20</price>
    <year>1990</year>
  </cd>
  <cd>
    <title>Eros</title>
    <artist>Eros Ramazzotti</artist>
    <country>EU</country>
    <company>BMG</company>
    <price>9.90</price>
    <year>1997</year>
  </cd>
  <cd>
    <title>One night only</title>
    <artist>Bee Gees</artist>
    <country>UK</country>
    <company>Polydor</company>
    <price>10.90</price>
    <year>1998</year>
  </cd>
  <cd>
    <title>Sylvias Mother</title>
    <artist>Dr.Hook</artist>
    <country>UK</country>
```

```
    <company>CBS</company>
    <price>8.10</price>
    <year>1973</year>
  </cd>
</catalog>
```

Figura 11: Exemplo de um documento XML
(Fonte: W3Schools)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:template match="/">
    <html>
      <body>
        <h2>My CD Collection</h2>
        <table border="1">
          <tr bgcolor="#9acd32">
            <th>Title</th>
            <th>Artist</th>
          </tr>
          <xsl:for-each select="catalog/cd">
            <tr>
              <td>
                <xsl:value-of select="title"/>
              </td>
              <td>
                <xsl:value-of select="artist"/>
              </td>
            </tr>
          </xsl:for-each>
        </table>
      </body>
    </html>
  </xsl:template>
</xsl:stylesheet>
```

Figura 12: Exemplo de um documento XSL



My CD Collection

Title	Artist
Empire Burlesque	Bob Dylan
Hide your heart	Bonnie Tyler
Greatest Hits	Dolly Parton
Still got the blues	Gary Moore
Eros	Eros Ramazzotti
One night only	Bee Gees
Sylvias Mother	Dr.Hook

Figura 13: Resultado final da transformação XSL
(Fonte: W3Schools)

3.1.4.1.4 Definição de Dados para intercâmbio (*XML Schemas*)

A tecnologia de XML permite a criação de vocabulários que podem ser utilizados pelas organizações públicas para trocar informações de maneira padronizada. Alternativamente, os documentos no formato XML podem ser transformados em outros tipos de documento de modo a facilitar a sua exibição ou impressão, o que é de responsabilidade das tecnologias XSL. Outra tecnologia da família XML que merece destaque e é bastante utilizada no intercâmbio de dados é a tecnologia de XML *Schemas*.

Essa tecnologia permite a criação de documentos, denominados *schemas*, que tem por objetivo validar os documentos XML. A validação em questão é baseada na estrutura modelada para o documento XML, o que envolve o atendimento às regras de negócio, tipos de dados, relacionamentos entre os elementos XML e restrições aplicadas aos dados. Em outras palavras, a tecnologia de XML *Schemas* define o que pode ser incluído ou não em um arquivo XML. Logo, da mesma forma que o *schema* de banco de dados define as regras de estruturação dos objetos de um banco de dados, um documento XML *Schema* define as regras de estruturação de um arquivo XML.

Neste contexto, é importante saber diferenciar quando um arquivo XML é bem formado (*well-formed*) e quando é válido (*valid*). De um modo geral, um arquivo XML é dito “bem formado” quando ele atende aos requisitos de estruturação de qualquer documento XML, requisitos estes definidos pelo W3C. Uma breve lista de verificação quanto à formação de documentos XML é fornecida a seguir:

- Toda *tag* deve ser fechada; admite-se o fechamento abreviado de *tags* vazias.
- *Tags* não podem se sobrepor, mas devem ser perfeitamente aninhadas.
- Documentos XML só podem ter uma única raiz.
- Nomes de elementos XML devem obedecer às convenções de nomeação definida pelo W3C.
- XML é um documento *case-sensitive*.
- Espaços são mantidos em documentos XML.

Os documentos XML são ditos válidos quando atendem às regras de estruturação definidas em um documento XML *Schema*. Logo, enquanto a formação do documento XML é dada pelo atendimento às regras básicas de criação de qualquer documento XML, a validade é verificada de acordo com regras de negócio definidas pela equipe técnica durante a etapa de modelagem do documento XML. A lista a seguir fornece os tipos de validações que podem ser elaboradas com o uso de XML *Schemas*:

- Define quais elementos e atributos podem aparecer no documento XML.
- Define a relação entre elementos (pai-filho).
- Define a ordem em que os elementos filhos devem aparecer no documento XML e total de elementos filhos permitidos.
- Define se um elemento XML pode estar vazio ou deve incluir algum valor.
- Define tipos de dados para os elementos e atributos XML.
- Define valores padrão ou fixo para elementos e atributos XML.

Entretanto, o padrão XML *Schema* também possui algumas limitações, e conhecê-las é essencial para criar soluções de intercâmbio de dados mais eficientes, além de abrir a possibilidade de elaboração de estratégias adicionais para contornar possíveis problemas de validação de dados. A lista abaixo relaciona as mais conhecidas limitações de validação do XML *Schema*. Entretanto, é importante lembrar que não é escopo desta Cartilha Técnica discutir ou elaborar soluções técnicas para contornar os problemas resultantes destas limitações.

- Não trata restrições condicionais.
- Não possibilita a definição de dependências entre elementos distintos.
- Não provê mecanismos para validação cruzada de documentos XML distintos.
- Não permite a definição de valores "nulos" para atributos.
- Não provê mecanismos para validação de valores numéricos grandes.
- Exige grande esforço para manter um código relativamente complexo, o que demanda o uso de ferramentas de produtividade.
- Pode gerar problemas de desempenho nas aplicações devido à necessidade de transmitir arquivos relativamente grandes.

Outros padrões para validação de documentos XML têm surgido com o objetivo de contornar as limitações do XML *Schema*, por exemplo: SAF (*Schema Adjunct Framework*), *Schematron*, RELAX and RELAX NG, SOX (*Schema for Object Oriented* XML) e DSDL (*Document Schema Definition Languages – Interoperability Framework*). Entretanto, nenhuma dessas novas tecnologias é recomendada ou adotada pela ePING.

A Figura 14 apresenta um exemplo de um arquivo *XML Schema* enquanto que a Figura 15 ilustra como referenciar esse documento *XML Schema* a partir de um arquivo XML.

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="note">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="to" type="xs:string"/>
        <xs:element name="from" type="xs:string"/>
        <xs:element name="heading" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Figura 14: Exemplo de um XML *Schema*
(Fonte: W3Schools)

```
<?xml version="1.0"?>
<note
xmlns="http://www.w3schools.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.w3schools.com note.xsd">
  <to>Tove</to>
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

Figura 15: Referencia a um XML *Schema* a partir do XML
(Fonte: W3Schools)

3.1.4.1.5 Estruturação de Dados Geoespaciais Vetoriais (EDGV)

A demanda por informação geoespacial na atual sociedade tem crescido exponencialmente. Com a multiplicidade de geotecnologias existentes no mercado, a produção de dados geoespaciais e sua distribuição vêm se tornando cada vez mais ágeis. Portanto, é fundamental que os dados sejam gerados segundo padrões e especificações técnicas para possibilitar a interoperabilidade dos dados. Atenta às necessidades brasileiras, a Comissão Nacional de Cartografia (CONCAR) constituiu um comitê especializado para elaborar um catálogo de feições para o Sistema Cartográfico Nacional (SCN).

Um catálogo de feições é um modelo de dados geoespaciais com o objetivo de obter a interoperabilidade semântica por meio de um padrão de compartilhamento. A EDGV (Estruturação de Dados Geoespaciais Vetoriais) é uma especificação técnica que define um modelo conceitual para dados vetoriais garantindo sua consistência lógica. Esta especificação objetiva padronizar as estruturas de dados geoespaciais de forma a viabilizar o compartilhamento, a interoperabilidade e a racionalização de recursos entre os produtores e consumidores de dados georreferenciados. A EDGV é uma das especificações da Infraestrutura Nacional de Dados Espaciais (INDE).

O modelo da EDGV é composto por um diagrama que contém as classes e seus relacionamentos, e de um dicionário de dados, que apresenta em detalhes a estrutura e atributos de cada uma das classes que compõem o modelo. Estas classes estão divididas atualmente em treze categorias: Hidrografia, Relevo, Vegetação, Sistema de transporte, Energia e comunicações, Abastecimento de água e saneamento básico, Educação e cultura, Estrutura econômica, Localidades, Pontos de referência, Limites, Administração pública, Saúde e serviço social.

A EDGV se destina a desenvolvedores de sistemas de informações geográficas (SIG), produtores e usuários de dados geoespaciais. Seu modelo para dados geoespaciais vetoriais de referência, também conhecidos como cartografia básica, permite o uso de uma interface comum tanto para produtores como para usuários. A adoção deste modelo é essencial para o sucesso da INDE.

Maiores informações sobre a EDGV podem ser encontradas no Portal SIG Brasil em http://www.inde.gov.br.

3.1.4.2 Especificações para Vocabulários e Ontologias

Tabela 15: Vocabulários e Ontologias

Componentes	Especificação	Situação
Descrição de recursos	RDF	R
Especificação de vocabulários para RDF Resource Description Framework (RDF) Schema	Resource Description Framework (RDF) Schema	R
Sistemas de Organização do Conhecimento	SKOS (*Simple Knowledge Organization System*)	R
Linguagem de definição de ontologias na web	OWL (*Web Ontology Language*)	R

3.1.4.2.1 Descrição de Recursos (RDF)

O RDF (*Resource Description Framework*) é um conjunto de especificações desenvolvidas pelo W3C com o objetivo de representar e intercambiar informações na *Web*. Sua característica principal é a de facilitar a combinação de diferentes metadados, permitindo assim, a evolução natural e facilitada das informações ao longo do tempo (W3C, 2010).

O fundamento básico do RDF é a linguagem XML, que lhe fornece a sintaxe necessária para a definição da especificação em um padrão aberto. O W3C publicou a primeira especificação do RDF em 1999, e em 2004 essa versão foi atualizada para o que o W3C denomina de “recomendações” e que, na verdade, representa um conjunto de especificações que se constitui a família RDF. A Tabela 17 descreve o conjunto de especificações ou recomendações que compõem toda a estrutura RDF:

Tabela 16: Estrutura do RDF (W3C, 2010)

Especificação	Descrição
RDF: *Concepts and Abstract Syntax*	Descreve os conceitos básicos do RDF e define uma sintaxe abstrata no qual o padrão é definido.
RDF *Semantics*	Define precisamente a semântica do RDF.
RDF *Primer*	Descreve uma linguagem para a representação de informações a respeito de recursos encontrados na *Web*. Descreve como o RDF pode ser utilizado e como se pode construir um vocabulário baseado neste padrão.
RDF *Vocabulary Description Language* 1.0: RDF *Schema*	Define uma linguagem de propósito geral para representar tipos diversos de informações na *Web.* Permite a definição de recursos da *Web* através de classes, propriedades e valores.
RDF/XML *Syntax Specification*	Define a sintaxe XML utilizada para descrever o RDF.
RDF *Test Cases*	Descreve os casos de testes desenvolvidos pelo grupo de trabalho do W3C.

Os padrões XML e RDF são considerados a fundação básica da *Web* Semântica que, por sua vez, compreende um grupo de mecanismos e tecnologias que permitirão aos computadores “compreenderem” como as informações se relacionam e se interconectam no ambiente heterogêneo e vasto da *World Wide Web*. Neste contexto, o RDF provê o mecanismo ideal para, formalmente, definir os recursos disponíveis no ambiente da *Web* Semântica.

Através do fornecimento de um método padrão de referência a elementos de metadados e também de conteúdo, o RDF se consolida como um padrão para que as aplicações possam interoperar de maneira mais facilitada. Ele define uma linguagem de metadados para a representação das informações na *Web* e provê também um modelo completo para a descrição e criação de relacionamentos entre os recursos disponíveis. Para o RDF, um *recurso*, também chamado de *subject,* pode ser uma coisa, uma pessoa, uma música ou mesmo uma página inteira da *Web* que é unicamente identificado por uma URI (*Uniform Resource Identifier*). Esses recursos, são associados a objetos (*objects*) que definem o valor ou conteúdo da informação. A Figura 16 ilustra e define os elementos básicos que compõem a especificação RDF.

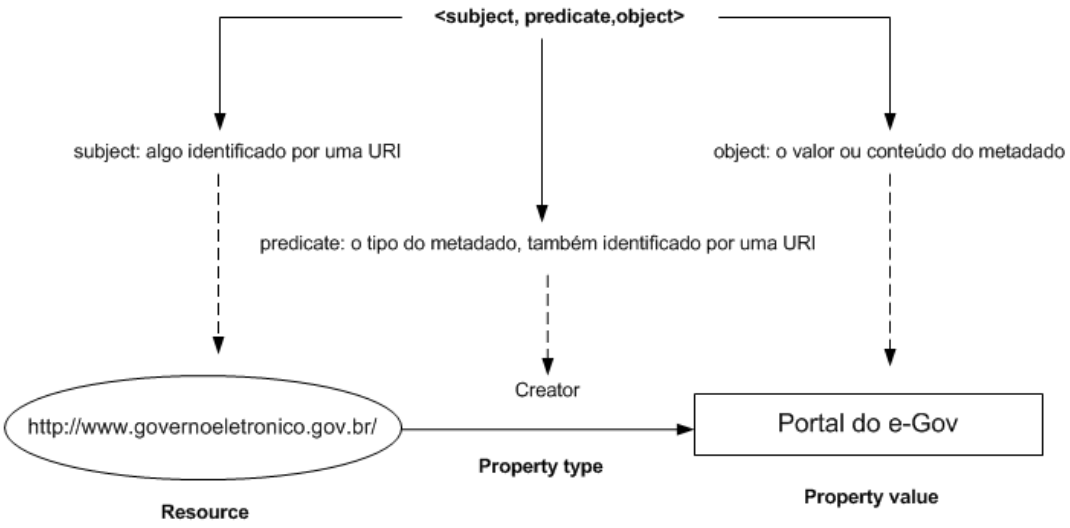


Figura 16: Elementos básicos do RDF

A Figura 17 mostra um exemplo de documento RDF, assim como o seu conteúdo exibido na *Web*.

```
<?xml version="1.0"?>

<rdf:RDF
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:cd="http://www.recshop.fake/cd#">

 <rdf:Description
 rdf:about="http://www.recshop.fake/cd/Empire Burlesque">
  <cd:artist>Bob Dylan</cd:artist>
  <cd:country>USA</cd:country>
  <cd:company>Columbia</cd:company>
  <cd:price>10.90</cd:price>
  <cd:year>1985</cd:year>
 </rdf:Description>

 <rdf:Description
 rdf:about="http://www.recshop.fake/cd/Hide your heart">
  <cd:artist>Bonnie Tyler</cd:artist>
  <cd:country>UK</cd:country>
  <cd:company>CBS Records</cd:company>
  <cd:price>9.90</cd:price>
  <cd:year>1988</cd:year>
 </rdf:Description>
 .
 .
 .
```

Title	Artist	Country	Company	Price	Year
Empire Burlesque	Bob Dylan	USA	Columbia	10.90	1985
Hide your heart	Bonnie Tyler	UK	CBS Records	9.90	1988

Figura 17: Exemplo de um documento RDF
(Fonte: W3Schools)

3.1.4.2.2 Resource Description Framework Schema

Uma ontologia define (especifica) os conceitos, relacionamentos e outras especificidades que são relevantes para modelar um domínio. Essa definição é realizada especificando um vocabulário (classes, relacionamentos e afins), e assim, provendo significado para o mesmo e criando restrições formais para seu uso.

O Resource Description Framework (RDF) é uma linguagem geral para representar informações na Web. O Resource Description Framework Schema (RDFS) é uma linguagem que utiliza o RDF para descrever vocabulários/termos em RDF. Dessa forma o RDFS é uma extensão semântica do RDF.

O RDFS define uma coleção de recursos RDF que podem ser usadas para descrever propriedades de outros recursos RDF em vocabulários RDF específicos. O núcleo do vocabulário é definido no *namespace*

chamado de rdfs[1] e rdf[2] possuindo definições de Classes como: rdfs:Resource, rdfs:Class, rdfs:Literal entre outros e Propriedades como: rdf:type, rdfs:subClassOf, rdfs:comment. A especificação do RDFS utiliza de uma forma abreviada para representar uma URI. Por exemplo um rdf:type deve ser lido como http://www.w3.org/1999/02/22-rdf-syntax-ns#type.

O quadro abaixo mostra um exemplo de utilização do RDFS.

Em português:

Cachorro1 é um animal
Gato1 é um gato
Gatos são animais
Zoologicos abrigam animais
Zoologico1 abriga o Gato2

Em RDF/Turtle:

```
@prefix rdf:   <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs:   <http://www.w3.org/2000/01/rdf-schema#> .
@prefix ex:   <http://example.org/> .
@prefix zoo:   <http://example.org/zoo/> .

ex:cachorro1    rdf:type        ex:animal .
ex:gato1        rdf:type        ex:gato .
ex:gato         rdfs:subClassOf  ex:animal .
zoo:abriga      rdfs:range       ex:animal .
ex:zoo1         zoo:abriga       ex:gato2 .
```

3.1.4.2.3 Sistemas de Organização do Conhecimento (SKOS)

A tecnologia *Simple Knowledge Organization System* (SKOS) é um conjunto de linguagens formais voltado para a representação de conhecimentos de uma organização através de um *thesauri*, taxonomia ou outro tipo de vocabulário controlado. Um dos focos é a interoperabilidade de informações e conceitos de uma forma passível de automação de máquina. Uma leitura recomendada é o do SKOS[3] para entender os conceitos básicos do SKOS e suas aplicações.

É importante ressaltar que o SKOS não representa axiomas e fatos e, portanto, não é uma linguagem que descreve uma ontologia formal.

Como um exemplo da notação formal há o RDF/N3 que é um tipo de notação não baseada em XML que preza a leitura e seu tamanho reduzido. SKOS é utilizado pelo VCGE tanto em sua notação RDF/N3 como na notação RDF/XML, disponível no endereço http://vocab.e.gov.br.

1 http://www.w3.org/2000/01/rdf-schema#

2 http://www.w3.org/1999/02/22-rdf-syntax-ns#

3 http://www.w3.org/2004/02/skos/

Exemplo em RDF/N3

```
@prefix dc: <http://purl.org/dc/terms/> .
@prefix ns1: <http://purl.org/dc/elements/1.1/> .
@prefix skos: <http://www.w3.org/2004/02/skos/core#> .

  <http://vocab.e.gov.br/2011/03/vcge#abastecimento-agua>a
  <http://www.w3.org/2004/02/skos/core#Concept>;
    dc:created "20090312T07:29:42"^^
   <http://www.w3.org/2001/XMLSchema#dateTime>;
    skos:broader
   <http://vocab.e.gov.br/2011/03/vcge#usos-multiplos-recursos-hidricos>;
   skos:inScheme <http://vocab.e.gov.br/2011/03/vcge#esquema>;
   skos:narrower <http://vocab.e.gov.br/2011/03/vcge#abastecimento-agua>;

skos:prefLabel "Abastecimento de água" .

 <http://vocab.e.gov.br/2011/03/vcge#acesso-divulgacao-producao-cientifica>a
 <http://www.w3.org/2004/02/skos/core#Concept>;
    dc:created "2008-09-23T07:02:39"^^
    <http://www.w3.org/2001/XMLSchema#dateTime>;
    skos:broader <http://vocab.e.gov.br/2011/03/vcge#fomento-pos-graduacao>;
    skos:inScheme <http://vocab.e.gov.br/2011/03/vcge#esquema>;
    skos:narrower
    <http://vocab.e.gov.br/2011/03/vcge#acesso-divulgacao-producao-cientifica>;
    skos:prefLabel "Acesso e divulgação da produção cientifica" .
```

Exemplo em RDF/XML

```
<rdf:RDF>
<rdf:Description rdf:about="http://vocab.e.gov.br/2011/03/vcge#abastecimento-agua">
   <rdf:type rdf:resource="http://www.w3.org/2004/02/skos/core#Concept"/>
   <skos:prefLabel>Abastecimento de água</skos:prefLabel>
            <dc:created rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">2009-03-
12T07:29:42</dc:created>
   <skos:inScheme rdf:resource="http://vocab.e.gov.br/2011/03/vcge#esquema"/>
   <skos:broader rdf:resource="http://vocab.e.gov.br/2011/03/vcge#usos-multiplos-recursos-hidricos"/>
   <skos:narrower rdf:resource="http://vocab.e.gov.br/2011/03/vcge#abastecimento-agua"/>
</rdf:Description>

<rdf:Description rdf:about="http://vocab.e.gov.br/2011/03/vcge#acesso-divulgacao-producao-
cientifica">
   <rdf:type rdf:resource="http://www.w3.org/2004/02/skos/core#Concept"/>
   <skos:prefLabel>Acesso e divulgação da produção cientifica</skos:prefLabel>
            <dc:created rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">2008-09-
23T07:02:39</dc:created>
   <skos:inScheme rdf:resource="http://vocab.e.gov.br/2011/03/vcge#esquema"/>
   <skos:broader rdf:resource="http://vocab.e.gov.br/2011/03/vcge#fomento-pos-graduacao"/>
      <skos:narrower rdf:resource="http://vocab.e.gov.br/2011/03/vcge#acesso-divulgacao-producao-
cientifica"/>
</rdf:Description>

</rdf:RDF>
```

3.1.4.2.4 Web Ontology Language

A *Web Ontology Language* (OWL) é uma família de linguagens utilizadas para representar conhecimento através de ontologias. OWL é direcionando quando a informação contida em um documento tem como alvo ser interpretada por aplicações e não somente interpretada por pessoas. OWL pode ser utilizada para representar explicitamente o significado dos termos de um vocabulário e os relacionamentos entre os mesmos[4].

O OWL representa conhecimento utilizando de uma semântica precisa com relacionamento de superclasses e subclasses. Já o SKOS representa uma organização do conhecimento apresentando conceitos e seus relacionamentos através de um vocabulário, *thesauri* ou taxonomia.

4 http://www.w3.org/TR/owl-features/

Exemplo da Ontologia do Orçamento Federal Brasileiro[5]:

```
<?xml version="1.0"?>

<!DOCTYPE rdf:RDF [
   <!ENTITY owl "http://www.w3.org/2002/07/owl#" >
   <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" >
   <!ENTITY owl2xml "http://www.w3.org/2006/12/owl2-xml#" >
   <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" >
   <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
   <!ENTITY siop "http://vocab.e.gov.br/2012/08/loa2012#" >
]>
<rdf:RDF xmlns="http://vocab.e.gov.br/2012/08/loa2012#"
    xml:base="http://vocab.e.gov.br/2012/08/loa2012#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:owl2xml="http://www.w3.org/2006/12/owl2-xml#"
    xmlns:owl="http://www.w3.org/2002/07/owl#"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:siop="http://vocab.e.gov.br/2012/08/loa2012#">
   <owl:Ontology rdf:about=""/>

   <owl:Class rdf:about="#Esfera">
      <rdfs:subClassOf rdf:resource="#Classificador"/>
      <rdfs:comment rdf:datatype="&xsd;string"
         >Classe nomeada cujos elementos representam os tipos de orcamento definidos para o Governo:
orcamento fiscal (10), orcamento da seguridade social (20, e orcamento de investimento
(30).</rdfs:comment>
   </owl:Class>
 <owl:Class rdf:about="#Orgao">
      <rdfs:subClassOf rdf:resource="#Classificador"/>
      <rdfs:comment rdf:datatype="&xsd;string"
         >Os elementos dessa classe referem-se aos orgaos orcamentarios que possuem vinculados a si,
os elementos da classe UnidadeOrcamentaria atraves da propriedade temOrgao. Orgaos nao
correspondem necessariamente a uma estrutura administrativa, como ocorre, por exemplo, com alguns
fundos especiais e com alguns orgaos tais como  (i) Transferencias a Estados, Distrito Federal e
Municipios, (ii) Encargos financeiros da Uniao, (iii) Operacoes oficiais de credito, (iv) Refinanciamento da
divida publica mobiliaria federal, e (v) Reserva de contingencia.</rdfs:comment>
   </owl:Class>



   <owl:Class rdf:about="#Programa">
      <rdfs:subClassOf rdf:resource="#Classificador"/>
      <rdfs:comment rdf:datatype="&xsd;string"
         >Os elementos dessa classe sao programas orientados para a realizacao dos objetivos
estrategicos definidos para o periodo do PPA (Plano Plurianual), ou seja, quatro anos. Programas podem
ser tematicos (que retratam no PPA a agenda de governo e orienta a acao governamental), ou de gestao,
```

5 http://vocab.e.gov.br/

```
manutencao e servicos (instrumentos do PPA que classificam um conjunto de acoes destinadas ao apoio,
gestao e manutencao da atuacao governamental).</rdfs:comment>
   </owl:Class>


   <owl:Class rdf:about="#Projeto">
      <rdfs:subClassOf rdf:resource="#Acao"/>
      <rdfs:comment rdf:datatype="&xsd;string"
         >Os elementos dessa classe sao acoes limitadas no tempo e das quais resulta um produto que
concorre para a expansao ou aperfeicoamento da acao do governo.</rdfs:comment>
   </owl:Class>
</rdf:RDF>
```

3.1.4.2.5 Identificador Uniforme de Recurso (URI)

O Identificador Uniforme de Recurso – URI é um texto que identifica um recurso abstrato ou real que obedece um conjunto de regras para sua formação. O URI prove uma forma simples e extensível de identificar um recurso. Ele abrange tanto o Localizador Uniforme de Recurso - URL como o Nome Uniforme de Recurso - URN podendo pertencer a uma dessas classes ou de ambas, conforme mostra a figura a seguir.

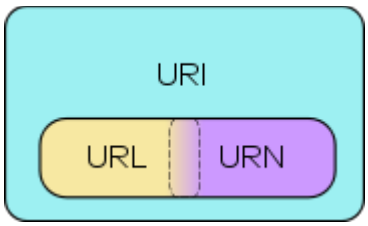


Figura 18: Formação do URI

O URI permite que diferentes identificadores sejam usados no mesmo contexto inclusive com diferentes mecanismos de acesso. Permite também a inclusão de outros identificadores sem que os novos interfiram com os identificadores já existentes. No contexto de URI um recurso pode ser qualquer coisa identificável por uma URI. Inclusive objetos físicos, uma pessoa, livros, e abstratos como um relacionamento de empregador-empregado.

O conjunto de regras que define um schema URI é de responsabilidade da equipe envolvida com a representação dos recursos. É desejável que as URIs sejam perenes durante um tempo e seja possível seu acesso nesse período. Exemplos de URI podem ser:

mailto:joao.da.silva@exemplo.com

tel:+55-99-9999-9999

http://localhost/

urn:oasis:names:specification:docbook:dtd:xml:4.1.2

Onde o primeiro identifica o email de joao.da.silva na rede exemplo.com, o segundo informa um telefone no Brasil, o terceiro informa o endereço do localhost e a sua forma de acesso (HTTP) e o último é uma URN para uma especificação Oasis.

No governo federal brasileiro há o conjunto de regras para publicação de Dados Abertos chamado “Política de URIs para Publicação de Dados no Governo” disponível em: http://www.governoeletronico.gov.br/biblioteca/arquivos/Politica-URIs-Publicacao-Dados-Governo.

Alguns exemplos de URIs no governo federal brasileiro são:

http://vocab.e.gov.br/2011/03/vcge#agricultura-extrativismo-pesca – Que identifica o termo 'Agricultura Extrativismo e Pesca' do VCGE

http://vocab.e.gov.br/2013/09/loa – Que identifica o modelo ontológico da LOA de 2013

3.1.5. Áreas de Integração para Governo Eletrônico – Segmento 5

3.1.5.1 Especificações para Temas Transversais às Áreas de Atuação de Governo

Tabela 17: Temas Transversais às Áreas de Atuação de Governo

Componente	Especificação	Situação
Linguagem para Execução de Processos	BPEL4WS v1.1	R
Notação de Modelagem de Processos	BPMN 1.0	A
Intercâmbio de Informações Financeiras	XBRL	A
Legislação, Jurisprudência e Proposições Legislativas	LexML 1.0	R
Integração de Dados e Processos	MGD	A
Interoperabilidade entre sistemas de informação geográfica	WMS, WFS, WCS, CSW e Filter Encoding versão 1.0 ou posterior	A
	WFS-T, WKT	R

3.1.5.1.1 Linguagem para Execução de Processos (BPEL4WS);

O BPEL4WS (*Business Process Execution Language for Web Services*), também conhecido simplesmente como BPEL, é uma linguagem para a definição e execução de processos de negócio baseada no conceito de orquestração de serviços. Embora não seja a única linguagem com essa finalidade, é sem dúvida a mais utilizada atualmente.

Existem duas formas de representar processos de negócio, quais sejam: a forma notacional ou gráfica, voltada para comunicação entre pessoas, e utilizando-se XML (*Extensible Markup Language*), voltada para processamento ou execução automatizada. A forma notacional ou gráfica é definida pela especificação BPMN (*Business Process Modeling Notation*). A representação de processos utilizando XML, por sua vez, é de responsabilidade da especificação BPEL4WS que possui, neste campo de atuação, alguns competidores como, por exemplo, BPML (*Business Process Modeling Language*) e XPDL (XML *Process Definition Language*). A versão 2.0 do BPMN, cujo estudo está sendo iniciado, também define a representação de processos de negócio em XML.

A especificação BPEL é considerada uma extensão dos padrões existentes para a tecnologia de *Web Services*. Isso porque antigamente, os *Web Services* eram limitados a interações do tipo *stateless*, o que significa dizer que o estado de comunicação entre consumidor e provedor não era mantido durante as transações. Nas chamadas de serviços *stateless*, cada transação é única, o que dificulta o aproveitamento de dados e o uso de mecanismos de controle de transação entre duas ou mais invocações do mesmo serviço. Com o advento do BPEL e outras tecnologias de orquestração e coreografia de processos, a conversação entre processos pôde ser desenvolvida utilizando a tecnologia de *Web Services* ao mesmo tempo em que se faz uso dos mecanismos de chamada de serviços do tipo *stateful*, o que permite preservar o estado atual do processo entre as diversas chamadas. Assim, pode-se definir BPEL como sendo uma

linguagem rigorosa, baseada na tecnologia de *Web Services*, e que possibilita a interação entre processos utilizando chamadas do tipo *stateful*.

A definição completa de processos baseada em BPEL utiliza dois tipos de arquivos: WSDL (*Web Services Description Language*) e BPEL. Os arquivos WSDL especificam as interfaces de serviços. Maiores detalhamentos envolvendo WSDL são fornecidos na seção 3.6 que trata de serviços baseados na tecnologia de *Web Services*. Os arquivos BPEL, como descritos anteriormente, contêm a especificação do processo para execução, incluindo a descrição de execução de suas atividades, variáveis, eventos, tratamentos de exceção, detalhamento de rotas de decisão, etc. Assim, quando o BPEL é combinado com o WSDL, gera como resultado um completo fluxo de controle do processo de negócio que pode ser invocado através de uma interface bem definida e padronizada como um serviço. Outro ponto importante em relação a essa tecnologia é que um processo, representado em BPEL, necessita para ser executado de um *engine* BPEL, um *software* capaz de entender a especificação e fazer o processo de negócio executar passo-a-passo.

Alguns fornecedores de solução para modelagem de processos disponibilizam, em seus produtos, uma interface visual para que os profissionais modelem um processo diretamente em BPEL. Entretanto, a notação neste caso não deve ser confundida com a notação BPMN. A notação BPMN representa o processo de forma que o usuário ou o "dono" do negócio possa compreender. O BPEL, por sua vez, sendo provido por interface visual ou não, gera documentos no formato XML e em conformidade com a linguagem BPEL, que representam a execução do processo em um nível de detalhamento que os usuários comuns geralmente não compreendem. Para um maior detalhamento envolvendo BPMN, consulte a seção 5.1.3 neste documento.

Outro ponto de confusão entre os profissionais de TI, usuários e vendedores de ferramentas de produtividade, diz respeito à etapa de transição do modelo BPMN para o modelo BPEL. É importante salientar que embora a especificação BPMN forneça mecanismos de mapeamento com BPEL, essa atividade em nada irá substituir o trabalho de engenharia de software que deve ser executado pelos profissionais de TI. Isso significa dizer que ter apenas uma equipe de analistas de processos e uma boa ferramenta BPMN-BPEL não é garantia de gerar um sistema completo ao final da etapa da modelagem.

É verdade que as novas tecnologias associadas à gestão por processos tenham diminuído a distância entre a área de TI e a área de negócios. Entretanto, os esforços de ambos os lados para o desenvolvimento de sistemas mais robustos e eficientes é imprescindível e, com certeza, é a diferença entre a obtenção de bons resultados e resultados pobres ou mesmo indesejáveis.

3.1.5.1.2 Notação de Modelagem de Processos (BPMN)

O tema envolvendo modelagem de processos não é novo, mas tem recebido muita atenção por parte da comunidade de TI nos últimos anos. Isso porque a idéia de se construir sistemas compatíveis, ou até mesmo que imitem a maneira que os processos de trabalho são executados, promete ganhos em

desempenho, redução do retrabalho e a eliminação de atividades desnecessárias. Mas, para se construir sistemas baseados em processos de negócio é necessário, inicialmente, se modelar o processo de forma a representá-lo e descrevê-lo de maneira padronizada. Neste cenário, o padrão BPMN (*Business Process Modeling Notation*) fornece a sua contribuição.

O BPMN é uma especificação que define uma notação gráfica padronizada a ser utilizada pelos analistas de processos para modelar processos. A modelagem de processos pode ser realizada em diferentes níveis de abstração, também chamados de níveis de granularidade. A literatura atual define genericamente três possíveis níveis de granularidade: modelagem descritiva, modelagem analítica e modelagem para execução de processos.

A modelagem descritiva de processos é aquela que define a visão mais genérica da execução das atividades de trabalho. Geralmente neste tipo de modelagem são ignoradas regras e validações de dados em um nível mais detalhado. O objetivo é simplesmente comunicar o que é executado, para quem, quando e onde. A forma de execução das atividades, ou seja, “o como fazer” é descrita pela sequência das atividades, pela presença de alguns subprocessos e também por descrições textuais fornecidas pelo analista de processos.

A modelagem analítica de processos é mais detalhada do que a modelagem descritiva no sentido de que já contempla a inclusão de regras de negócio simples, além da capacidade de simular a execução do processo utilizando cenários de negócio definidos pelo analista de processos. Entretanto, ainda se encontra bastante longe de atender aos requisitos para a construção de um sistema informatizado.

A modelagem para execução dos processos, por sua vez, fornece a visão mais completa de todas, pois além de contemplar todos os recursos das abordagens anteriores, também possui a capacidade de tratar eventos, exceções, entrada de dados, processamento de dados, enfim, praticamente todas as preocupações inerentes à implementação de um sistema informatizado completo.

Teoricamente, o BPMN pode ser utilizado para modelar quaisquer dos três níveis de granularidade e, por isso, obteve tanta aceitação por parte da comunidade de profissionais do setor de processos. Entretanto, devido às complexidades existentes na modelagem para execução de processos, o BPMN por si só não é suficiente, o que levou a criação de um novo padrão denominado BPEL4WS, discutido na seção 3.5.1.

A especificação BPMN foi originalmente desenvolvida pelo BPMI (*Business Process Management Initiative*) e atualmente é mantida pelo OMG (*Object Management Group*). O BPMN é baseado na notação de fluxograma, embora forneça vários novos elementos, principalmente para a representação de eventos, regras de negócio e mensagens. A versão 2.0 do BPMN, cujo estudo já foi iniciado, traz evoluções para fortalecer o BPMN neste e em outros aspectos.

O principal elemento do BPMN é o BPD (*Business Process Diagram*) que pode conter diversos elementos gráficos, tais como: atividades, eventos, decisão, indicador de sequência, indicador de mensagem, entre outros. A Figura 19 ilustra os principais componentes da notação BPMN.

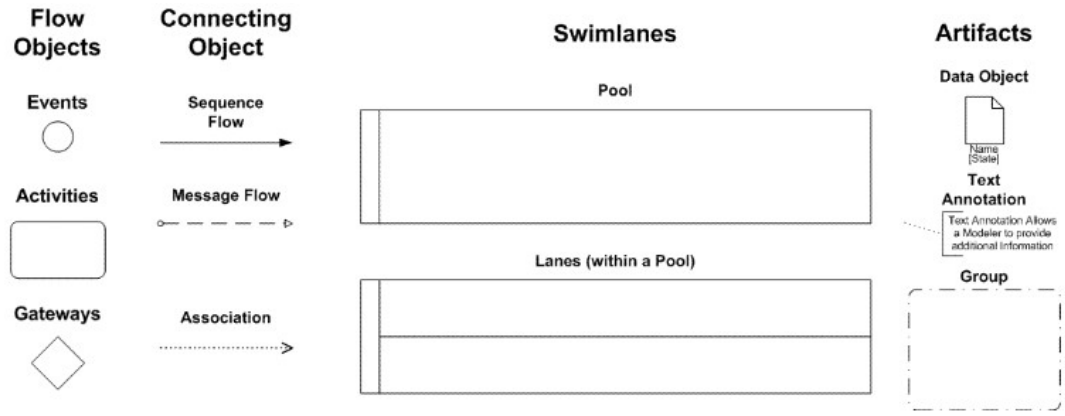


Figura 19: Principais componentes da notação BPMN
(Fonte: OMG, 2005)

Como se pode observar na Figura 19, diversos elementos do BPMN já são conhecidos, o que nos leva à conclusão de que essa especificação tem como meta padronizar a notação utilizada para modelagem de processos entre os diversos fornecedores deste tipo de solução.

Outra vantagem de se utilizar a especificação BPMN é que ela fornece possibilidades para se mapear o processo para o padrão BPEL, propiciando assim a conversão da versão gráfica do processo para uma versão executável. A Figura 20 ilustra um processo de negócio do governo, mapeado em BPMN.

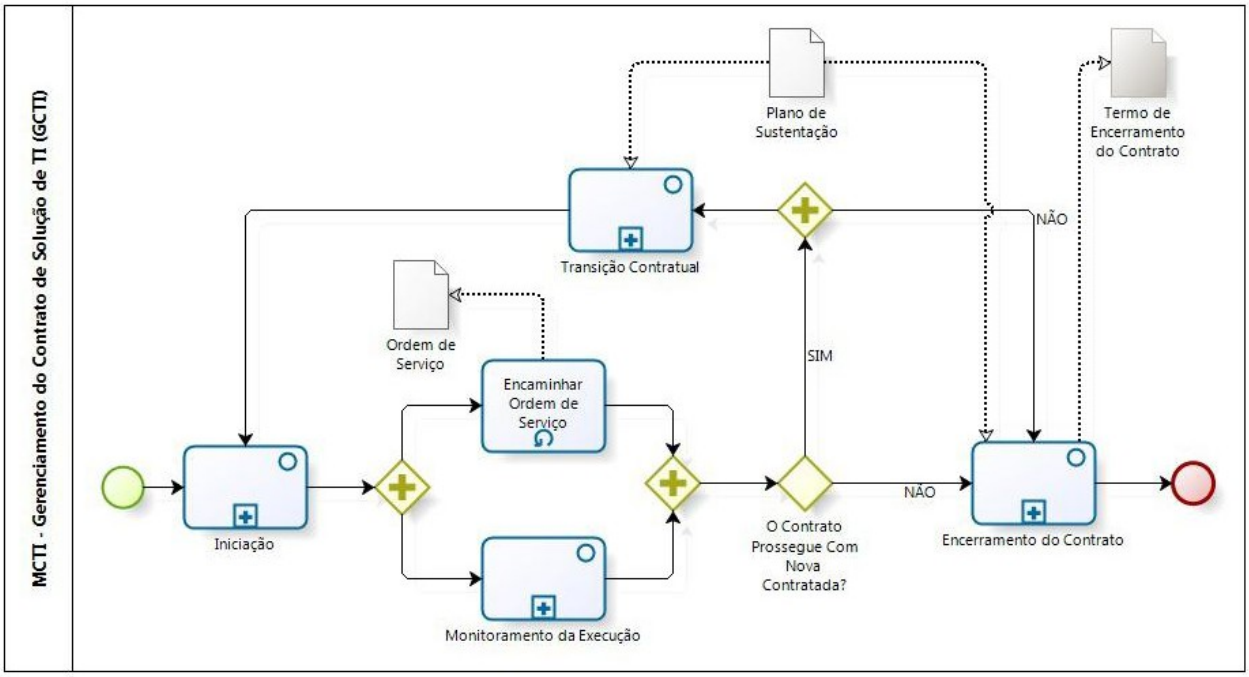


Figura 20: Exemplo de um processo de negócio mapeado em BPMN.

3.1.5.1.3 XBRL

XBRL (*eXtensible Business Reporting Language*) é um padrão baseado no XML para comunicar dados financeiros a partir de um conjunto de metadados estabelecidos nas taxonomias. Uma taxonomia XBRL é um dicionário estruturado que explica o conjunto de conceitos utilizados por um país (ex. EUA), um grupo de países (ex. União Europeia) ou um domínio particular (bancos, seguradoras, bolsa de valores). Estas taxonomias permitem criar os documentos XBRL, as *instâncias*, que contêm *factos* (os dados contábeis-financeiros) que são assim trocados pelas empresas e as organizações envolvidas (bancos, bolsas, seguradoras, organismos de controle financeiros e organizações estatísticas).

A primeira taxonomia XBRL para o governo brasileiro foi criada no ano de 2014 pela Secretaria do Tesouro Nacional, para ser utilizada no Sistema de Informações Contábeis e Fiscais do Setor Público Brasileiro (Siconfi), e está disponível para download no Portal Siconfi (siconfi.tesouro.gov.br).

3.1.5.1.4 LexML

O LexML é um portal especializado em informação jurídica e legislativa, cujo objetivo é reunir leis, decretos, acórdãos, súmulas, projetos de leis e outros documentos das esferas federal, estadual e municipal, dos Poderes Executivo, Legislativo e Judiciário de todo o Brasil. O LexML pode ser considerado como uma rede de informações legislativas e jurídicas que visa organizar, integrar e dar acesso às informações disponibilizadas nos diversos portais de órgãos do governo na Internet (TICONTROLE, 2010).

Para os profissionais de TI que trabalham no fornecimento de soluções informatizadas, o LexML pode ser utilizado para se referenciar, em páginas *Web*, documentos jurídicos armazenados em sua base de dados. A vantagem de se utilizar o endereçamento do LexML está no fato de que ele fornece uma identificação padronizada dos documentos jurídicos, evitando-se assim, a ocorrência do chamado "*link* quebrado". O "*link* quebrado" é identificado pelo retorno do erro HTTP 404 no navegador do usuário, e é consequência da referência a uma página na Internet que não mais se encontra disponível. Muitas vezes, o que ocorre realmente é que o endereço de referência mudou, mas o *hiperlink* na página *Web* não foi atualizado (TICONTROLE, 2010).

Com o uso do LexML esse problema pode ser contornado, uma vez que os documentos jurídicos são referenciados e descritos através de uma metodologia semântica para catalogação de dados e de uma identificação dos documentos por uso de URN (*Uniform Resource Name*, ou Nome Uniforme de Recurso). A catalogação de documentos do LexML é baseada em vocabulário controlado, utilizado para classificação, e XML *Schemas* utilizados para validação das regras de formação dos documentos armazenados. A identificação dos documentos no LexML, por sua vez, utiliza o recurso de URN, recomendado pelo W3C.

Assim, um desenvolvedor de sistemas que queira referenciar a Lei nº. 8.666 em uma página da *Web*, poderia utilizar-se do seguinte endereço fornecido pelo LexML (TICONTROLE, 2010):

http://www.lexml.gov.br/urn/urn:lex:br:federal:lei:1993-06-21;8666

Observe que o endereço do documento jurídico é formado pela junção de uma URL padrão da Internet, no caso http://www.lexml.gov.br/, acrescida de uma URN, urn:lex:br:federal:lei:1993-06-21;8666, que identifica a Lei a que se deseja fazer referência. Da mesma maneira, um usuário de Internet poderia copiar e colar o endereço acima na caixa de endereços do *browser* para ter acesso ao documento citado. A Figura 21 mostra o resultado da consulta ao documento, na página de referência do LexML.

Figura 21: Referência a documentos jurídicos no LexML
(Fonte: TICONTROLE, 2010)

Outra forma de se consultar o LexML é através da sua interface gráfica (Figura 22), disponível no endereço http://www.lexml.gov.br/.

Figura 22: Interface de consulta do LexML
(Fonte: TICONTROLE, 2010)

3.1.5.1.5 Modelo Global de Dados - MGD

O Modelo Global de Dados (MGD) é uma iniciativa do Ministério do Planejamento, Orçamento e Gestão (MP), Ministério da Fazenda (MF) e SERPRO que surgiu para simplificar e melhorar a Gestão dos Dados do Macroprocesso de Planejamento, Orçamento e Finanças. Este modelo tem como objetivo identificar o

contexto atual e as ações necessárias para a integração, modernização e desenvolvimento de soluções que suportem a operação e a tomada de decisão deste Macroprocesso.

O MP, MF e SERPRO compõem o Comitê do Macroprocesso de Planejamento, Orçamento e Finanças (MPOF). Este Comitê é composto de dois Grupos de Trabalho Interministerial (GTIs) e quatro outros Grupos de Trabalho onde destes destacamos o GTI2 que trata da Simplificação e Gestão da Informação do MPOF. Dentro deste GTI, o SERPRO coordena a parte que trata a Simplificação e Gestão da Informação dos Dados deste Macroprocesso.

O MGD é uma inciativa de interoperabilidade técnica porque é um modelo de dados do tipo entidade-relacionamentos, semântica porque objetiva harmonizar dados num significado comum ou interoperável e organizacional porque traz, em sua visão de negócio, um modelo de processos que leva a um entendimento comum dos processos executados pelos órgãos de governo.

A medida em que foi modelando os dados do MP, percebeu-se a necessidade de deixar de ser um modelo baseado apenas nos sistemas de informação e se alinhar ao negocio a partir da visão de processos. Desta forma o Modelo é baseado em 3 etapas: Modelagem dos Dados, Refinamento dos Dados e levantamento da visão de negócio (Processos). A visão de negócio permite ao MGD apontar os possíveis Gestores da Informação que serão os donos da informação de Governo como também mapear dados que servem ao processo e que não existem nos atuais sistemas de informação. Como consequência é possível compreender mais rapidamente qual o órgão do governo é responsável por disponibilizar informações afetas a sua competência e quais os órgãos estão interessados em seu consumo, visto sua relevância para o seu negócio, desonerando-os assim dos custos de manter informações que não estão sob sua outorga.

O MGD possui as seguintes metas:

- Mapear os dados (Entidades) utilizados pelo Macroprocesso, as integrações atuais e as possíveis integrações;
- Associar dados a processos (Visão de Negócio), favorecendo sua normalização;
- Consolidar conceitos sobre a definição dos dados entre os diferentes envolvidos;
- Permitir uma visão integrada dos dados e sua utilização nos diferentes contextos;
- Minimizar impactos de mudanças nos dados que se encontram dentro dos Sistemas de Gestão Administrativa (Estruturadores);
- Sistematizar e aperfeiçoar a construção de novas soluções, a partir do uso de padrões focados na interoperabilidade;
- Permitir a prospecção de novas estruturas de dados com o objetivo de melhorar a qualidade da informação;
- Contribuir para a uma melhor Gestão Publica por meio de soluções mais eficientes, capazes de prover informações mais confiáveis e precisas para a tomada de decisão;
- Promover o reuso dos dados, evitando assim possíveis redundâncias;
- Favorecer a implementação de Modelos Corporativos de Dados.

O que o MGD conseguiu demonstrar para o Macroprocesso de Planejamento, Orçamento e Finanças sobre a ótica de Dados, e mais tarde sobre a visão de processos, serviu para que ele fosse incorporado à ePING em Dezembro de 2010 com um objetivo maior: Ampliar a visão integrada e detalhada dos dados e processos que suportam os macroprocessos de Governo. Desta forma foi colocado na ePING como a arquitetura de interoperabilidade de dados e processos.

Atualmente o MGD é operacionalizado pelo SERPRO, que a cada etapa de evolução do modelo publica um compêndio que apresenta as informações necessárias ao entendimento do negócio, as entidades relacionadas ao negócio e também os principais processos de negócio. Assim, o MGD gera como resultado uma documentação direcionada ao negócio e aos profissionais de TIC responsáveis pela construção de soluções integradas envolvendo os Macroprocessos do Governo Federal.

Cabe aos órgãos fazer uso do MGD como uma ferramenta que auxilie a definição de demandas de evolução dos sistemas de informação permitindo que os Gestores dos Sistemas busquem a não replicação das informações no Governo Federal fortalecendo a interoperabilidade e a capacidade de integração dos sistemas. Desta forma o Governo passa a contar com uma capacidade maior de gerar sistemas e soluções que forneçam informações úteis para a tomada de decisão dos órgãos da Administração Pública Federal melhorando a Gestão Pública.

Mais informações sobre o projeto MGD podem ser consultadas no sítio http://modeloglobaldados.serpro.gov.br.

3.1.6.1.6 Interoperabilidade entre sistemas de informação geográfica

O *Open Geospatial Consortium* (OGC) é um consórcio internacional formado por mais de 450 empresas, universidades e agências governamentais. Seu objetivo é promover o desenvolvimento de tecnologias que promovam a interoperabilidade entre sistemas que utilizam a informação geográfica. Nesta subseção são apresentadas seis especificações publicadas pelo OGC e que constam no documento de referência da ePING. São adotados na arquitetura os padrões de serviços WMS (*Web Map Service*), WFS (*Web Feature Service*), WCS (*Web Coverage Service*) e CSW (*Catalogue Services for the Web*). Constam como recomendados os padrões WFS-T (*Web Feature Service Transactional*) e WKT (Well-Known Text).

O WMS é um serviço Web que permite obter mapas (dados geográficos editados) ou imagens na Internet. Este serviço resolve a principal demanda de informação geográfica: “quero ver o mapa”. Esta especificação é também o padrão internacional ISO 19128:2005.

O WFS é um serviço Web que permite obter as feições geográficas (dados vetoriais) de acordo com um conjunto de parâmetros. As consultas podem envolver predicados escalares (booleanos, de comparação etc.) e/ou geométricos (toca, cruza etc.). O WFS-T é um WFS básico com métodos que permitem alterar os dados via Web, com operações do tipo INSERT e DELETE. O WFS (básico e transactional) é também o padrão internacional ISO 19142:2010.

O propósito do serviço WCS é prover informação geoespacial que tem valores definidos em todo o espaço, também conhecida como dado matricial. Uma imagem de satélite ou uma fotografia aérea são exemplos de dados matriciais que podem ser publicados num servidor WCS.

O CSW é um serviço que define uma interface para publicar, acessar, navegar e consultar metadados sobre informações georreferenciadas na Internet, via HTTP. A partir desta interface os produtores de dados geoespaciais podem publicar seus produtos e os usuários podem encontrá-los. Um servidor CSW faz o papel de um diretório UDDI (*Universal Description, Discovery and Integration*), usado em serviços Web convencionais.

Para que serviços não-geográficos possam trafegar coordenadas geográficas via serviços convencionais, o formato WKT segue recomendado na arquitetura ePING para suprir essa necessidade. Este formato faz parte da especificação OGC Simple Features Access (SFA).

No contexto de serviços Web geográficos, um usuário desses sistemas pode acessar um serviço CSW e descobrir a informação geográfica de seu interesse por meio de uma consulta aos metadados publicados. Este usuário pode navegar pelos mapas disponíveis utilizando o serviço WMS para visualização. Após encontrar algum geodado que seja do seu interesse, o usuário pode obter as feições a partir de uma consulta a um serviço WFS. Caso esta informação seja uma imagem, este usuário pode baixá-la por meio de uma consulta a um serviço WCS.

3.1.5.2 Especificações para *Web Services*

Tabela 18: *Web Services*

Componente	Especificação	Situação
Infraestrutura de registro	UDDI v3.0.2	R
Linguagem de definição do serviço	WSDL 1.1	A
Protocolo para acesso a *Web Services*	SOAP v1.2	A
	HTTP/1.1 (REST)	

3.1.5.2.1 Arquitetura de Software e Interoperabilidade Técnica

A interoperabilidade entre sistemas diferentes é a chave para a comunicação envolvendo ambientes de *hardware* e *software* heterogêneos. Entretanto, como não se pode mudar o *hardware* a todo o momento, modifica-se o software e seus componentes internos, o que requer que este *software* seja construído com base em uma arquitetura que favoreça a interoperabilidade desejada.

A arquitetura de *software* define a estrutura de um sistema ou programa de computador de modo a ressaltar seus elementos, os relacionamentos entre eles e as interfaces de comunicação do sistema com o mundo exterior (BASS, CLEMENTS e KAZMAN, 2003). No padrão IEEE 12207.0-1996 que define os processos da Engenharia de *Software*, o tema “Arquitetura de *Software*” é utilizado para se descrever a estrutura de alto nível dos componentes do sistema computacional, o que implica em dizer que as interfaces de comunicação internas e externas devem ser enfatizadas. Como se pode perceber através dessas duas

definições, definir uma arquitetura de software adequada é o primeiro passo para se atingir a interoperabilidade entre sistemas.

A ePING enfatiza o uso da tecnologia de *Web Services* para propiciar a interoperabilidade entre sistemas heterogêneos o que implica também na busca por uma arquitetura de software mais alinhada aos conceitos de serviços em ambientes distribuídos. Nesse contexto, a Arquitetura Orientada a Serviços ou simplesmente SOA (*Service-Oriented Architecture*) oferece diversas vantagens à aderência aos padrões tecnológicos propostos pela ePING.

3.1.5.2.2 Arquitetura SOA

Um sistema distribuído é aquele que executa processos em um conjunto de máquinas sem memória compartilhada, que representam um único computador para seus usuários (TANEMBAUM, 2003). Além disso, seus componentes de *hardware* e *software* localizados em computadores em rede comunicam-se e coordenam suas ações através de troca de mensagens. Nesse contexto, SOA representa um conceito importante no âmbito dos sistemas distribuídos, pois é um paradigma para a realização e manutenção de processos de negócio que são suportados por sistemas distribuídos complexos (JOSUTTIS, 2007).

O ambiente distribuído de sistemas geralmente contempla sistemas legados que representam estabilidade e operacionalização segura, bem como vários anos de investimento em pessoas, infraestrutura, *softwares*, etc. (POTTS e KOPACK, 2003). Além disso, cada organização opta por diferentes fornecedores, delineando ambientes que contemplam linguagens de programação, bancos de dados, tecnologias e paradigmas de programação bem distintos.

Ao longo do tempo, a indústria de TI disponibilizou algumas alternativas como solução para o problema de interoperabilidade entre diferentes ambientes tecnológicos e de negócios cada vez mais integrados com parceiros comerciais e consumidores. Como exemplos de tais soluções podem ser citados: (i) CORBA (*Common Object Request Broker Architecture*), (ii) RMI (*Remote Method Invocation*), (iii) DCOM (*Distributed Common Object Model*), e (iv) *Servlets*/JSP (*Java Server Pages*).

Esses padrões ainda podem estar sendo utilizados, mas apresentam desvantagens no que diz respeito aos requisitos técnicos associados ao desenvolvimento de sistemas distribuídos mais complexos. Algumas das dificuldades encontradas com o uso de tais padrões são: (i) a falta de padronização de dados e interfaces, (ii) a dificuldade na localização e reuso dos objetos, (iii) necessidade de uso de portas especiais para a comunicação adequada entre cliente e servidor (CORBA e RMI), (iv) restrição de linguagem (RMI e Servlets/JSP apenas utilizam a linguagem Java), (v) restrição de plataforma (DCOM apenas funciona sob plataforma Microsoft), (vi) uso de padrões muito específicos (CORBA possui uma linguagem própria, a IDL (I*nterface Definition Language*)) e (vii) dificuldade de reuso na forma de serviço interoperável (falta de registro ou diretório para localizar Servlets/JSP e de especificações de interface para comunicação com os Servlets/JSP) (POTTS e KOPACK, 2003).

Nesse cenário, SOA surge como uma nova abordagem para se projetar softwares mais fortemente reutilizáveis e aderentes aos processos de negócio das organizações.

No intuito de definir SOA, diversos autores consideram diferentes dimensões ou pontos de vista, tais como: (i) uma evolução da arquitetura baseada em componentes e orientação a objetos, (ii) um conjunto de melhores práticas, princípios e padrões relacionados aos serviços das instituições e no contexto de aplicação da computação distribuída, ou (iii) como um estilo arquitetural que busca o alinhamento entre negócios e TI.

Sob o ponto de vista de evolução da arquitetura, SOA introduz o conceito de serviços como uma unidade executável que encapsula aspectos técnicos e negociais, e que permite que tais serviços sejam acessados de várias máquinas, pela Internet ou Intranet, através de interfaces consistentes e publicadas em consonância com padrões abertos.

Como um conjunto de melhores práticas, princípios e padrões, SOA é um modelo de arquitetura orientada a serviços que tem sido apontado como uma alternativa de sucesso para o alcance da interoperabilidade entre sistemas e agilidade nas práticas de negócio das instituições (LEWIS, MORRIS, *et al.*, 2007). Tal desafio é reflexo do mundo atual, cada vez mais globalizado e exigente quanto à evolução dos processos e dos sistemas institucionais. De acordo com este novo paradigma, esses dois elementos devem evoluir em um conjunto, o que muitas vezes resulta em um complexo e intrincado conjunto de sistemas distribuídos e interoperáveis.

Sob o ponto de vista do alinhamento estratégico que envolve os objetivos das instituições públicas e da TI adotada por elas, SOA provê a capacidade dos processos de negócios conduzirem o desenvolvimento de soluções informatizadas através de serviços flexíveis e de mecanismos que gerenciam e divulgam os serviços das organizações (ZHAO, 2006).

3.1.5.2.2.1 Serviços

O desenvolvimento de software é baseado na abstração do mundo real, ou seja, cada elemento da realidade é observado e analisado sob determinados pontos de vista. Segundo Josuttis (2007), SOA baseia-se na abstração de um problema do ponto de vista do negócio das organizações e o serviço é um conceito essencial nessa abordagem.

Serviços representam funcionalidades ou partes de uma ou mais funcionalidades que podem ser descobertas e utilizadas por outras aplicações ou outros serviços. Os serviços são independentes de plataformas e linguagens de programação, o que garante a sua plena utilização em ambientes de *software* e *hardware* heterogêneos.

3.1.5.2.3 Opção por *Web Services*

Web Services são tipicamente APIs baseadas em tecnologias de Internet. Essas APIs são acionadas através de HTTP ou, menos frequentemente, através do protocolo SMTP. *Web Services* podem ser classificados em dois grupos: (i) *Web Services* baseados no protocolo SOAP (*Simple Object Access Protocol*), e (ii) *Web Services* em conformidade com a arquitetura REST (*Representational State Transfer*).

A ePING recomenda tanto a utilização de *Web Services* que usam mensagens XML seguindo o padrão SOAP, quanto a utilização do protocolo HTTP para projetos baseados em REST. Em sistemas dessa natureza, a descrição das operações do serviço é feita em arquivo WSDL, de modo que possa ser lida e tratada diretamente pelos aplicativos com quem vai interagir. Independentemente da tecnologia utilizada (SOAP ou REST), é indispensável que cada *Web Service* implementado seja documentado com precisão e clareza.

Antes do advento da tecnologia de *Web Services*, a comunicação entre sistemas pela Internet baseava-se na troca de informação através de *brokers* centralizados ou conectores desenvolvidos para a troca de dados entre aplicações específicas. Isso dificultava, ou mesmo inviabilizava, o crescimento de atividades como o comércio eletrônico, uma vez que soluções particulares, circunscritas a um domínio limitado, precisavam ser desenvolvidas cada vez que duas ou mais empresas necessitavam trocar dados eletronicamente.

A tecnologia de *Web Services* representou, então, o estado da arte em tecnologia de sistemas distribuídos, uma vez que permitia a troca de informações através de aplicativos modulares, reutilizáveis, baseados em padrões abertos e acessíveis pela Internet. A tecnologia de *Web Services* tem a vantagem de permitir a construção de aplicativos em qualquer plataforma, utilizando-se de qualquer paradigma de desenvolvimento de software e linguagem de programação, e possibilitando a qualquer sistema comunicar-se com outros sistemas através de mensageria baseada em XML.

Essa é a questão fundamental envolvendo *Web Services*: o advento de uma gramática comum, não-proprietária e universalmente aceita que significou, por si só, uma enorme mudança na maneira como aplicativos distintos conversam entre si através de uma rede de comunicação de dados. Entre os principais ganhos a serem auferidos com a utilização de *Web Services* como solução de interoperabilidade, pode-se enumerar:

- **Longevidade** — o fato de operarem através de redes públicas e não-proprietárias, aliado ao seu caráter ecumênico no que tange a paradigmas de desenvolvimento, ambientes e linguagens de programação, garante que os serviços desenvolvidos com *Web Services* tenham vida longa, muito além das soluções proprietárias com que hoje dividem o cenário de interoperabilidade de TIC;
- **Facilidade** — *Web Services* permitem que a lógica negocial de qualquer sistema possa ser expostas na *Web*. Analistas de negócio e desenvolvedores podem construir soluções para situações particulares combinando os *Web Services* adequados e utilizando, nesse processo, não

apenas suas linguagens de programação prediletas, mas também a estratégia de implementação de sua escolha. Com *Web Services*, o compartilhamento de funcionalidades através da *Web* pode ser feita sem qualquer conhecimento de detalhes operacionais específicos dos sistemas envolvidos, sendo necessária apenas a aderência aos padrões publicados;

- **Reuso** — o modelo baseado em *Web Services* garante a reutilização sempre que necessário. Esse modelo viabiliza ainda que o código legado possa ser estendido e exposto na Internet, sem o caráter de intratabilidade comum a esses casos;
- **Universalidade** – a tecnologia de *Web Services* foi desenvolvida para ser facilmente acessível tanto a seres humanos (através, por exemplo, de um aplicativo *Web*) como a computadores (através, por exemplo, de uma API). Sua aderência ao ambiente de Internet e aos padrões abertos para comunicação entre sistemas distribuídos, garantem que eles possam ser acessados praticamente de qualquer lugar, utilizando infraestrutura já existente e respeitando sistemas de segurança já instalados, como *firewalls* e filtros.

3.1.5.2.4 Papel do SOAP (*Simple Object Access Protocol*)

SOAP é um protocolo que define uma maneira uniforme para o trânsito de dados codificados como documentos XML. SOAP define também um modo de execução de RPCs (*Remote Procedure Calls*), quase sempre se utilizando de HTTP como mecanismo de comunicação subjacente. Embora venha sofrendo forte concorrência da arquitetura REST, é ainda hoje o mecanismo de preferência no desenvolvimento e invocação de *Web Services*. As mensagens SOAP são documentos XML, e como tal, devem aderir à especificação formal dessa linguagem.

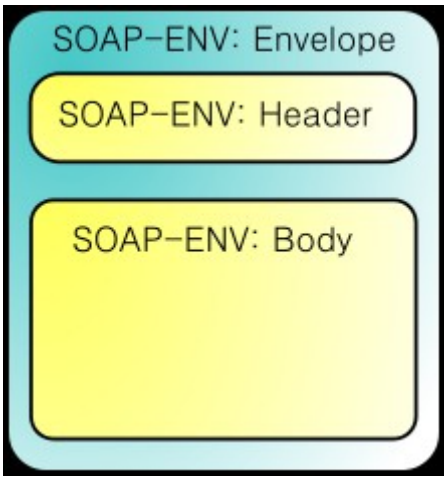


Figura 23: Estrutura do SOAP
(Fonte: Wikipedia)

Vale ressaltar que não se trata de um protocolo de acesso a objetos, razão pela qual a utilização do nome SOAP como acrônimo encontra-se em desuso. Atualmente, a manutenção e evolução desse padrão são de responsabilidade do grupo da W3C chamado de *XML Protocols Working Group*. Isso garante ao padrão SOAP um grau satisfatório de confiabilidade, uma vez que, como parte do largo espectro de padrões W3C, ele permanece estável e inalterado até a publicação de uma nova revisão dessa especificação por aquele grupo.

A especificação SOAP define um *framework* de mensageria consistindo dos seguintes elementos:

- **Modelo de processamento** – define as regras para o processamento de uma mensagem SOAP;

- **Modelo de extensibilidade** – define os conceitos e módulos SOAP;
- **Protocolo subjacente de enlace** – descreve as regras para o enlace com protocolos de transporte subjacente a serem usados na troca de mensagens entre nós SOAP;
- **Modelo de mensagem** – define a estrutura de uma mensagem SOAP.

Desses elementos, o mais relevante é o modelo de processamento, que descreve um modelo distribuído, seus participantes e também como uma mensagem SOAP deve ser processada. Esse modelo de processamento define os seguintes nós:

- **SOAP *sender*** – um nó que transmite uma mensagem SOAP;
- **SOAP *receiver*** – um nó que aceita uma mensagem SOAP;
- **SOAP *message path*** – o conjunto de nós através dos quais trafega uma mensagem SOAP;
- **SOAP *originator*** – o remetente de origem de uma mensagem (o ponto de início de um **SOAP *message path***);
- **SOAP *intermediary*** – endereçável de dentro de uma mensagem SOAP, pode ser tanto um **SOAP *receiver*** como um **SOAP *sender***. Processa os blocos de cabeçalho que se destinam a ele e retransmite a mensagem para que possa chegar a seu destinatário final;
- ***Ultimate* SOAP *receiver*** – destinatário final de uma mensagem SOAP, é responsável pelo processamento do corpo da mensagem e dos blocos de cabeçalho a ele endereçados.

As Figuras 24 e 25 apresentam, respectivamente, exemplos de requisição e resposta SOAP.

```
POST /InStock HTTP/1.1
Host: www.example.org
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPrice>
      <m:StockName>IBM</m:StockName>
    </m:GetStockPrice>
  </soap:Body>

</soap:Envelope>
```

Figura 24: Exemplo de uma requisição SOAP
(Fonte: W3Schools)

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPriceResponse>
      <m:Price>34.5</m:Price>
    </m:GetStockPriceResponse>
  </soap:Body>

</soap:Envelope>
```

Figura 25: Exemplo de uma resposta SOAP
(Fonte: W3Schools)

3.1.5.2.5 Papel do REST (*Representational State Transfer*)

A expressão “Transferência de Estado Representacional” foi criada e definida em 2000 por Roy Fielding, um dos arquitetos da versão 1.1 do protocolo HTTP, em uma dissertação para seu título de PhD. Ao contrário do SOAP, REST é uma arquitetura, e não um protocolo. Os *Web Services* construídos em conformidade com essa arquitetura são chamados de *RESTful*. Também diferentemente do SOAP, não há um padrão oficial para *RESTful Web Services*.

Para que um serviço seja considerado *RESTful*, é preciso que se submeta a um conjunto de seis restrições, e siga um conjunto de quatro princípios. A discussão dessas restrições e princípios merece um capítulo específico, e foge ao escopo do presente documento. Em seu lugar, uma visão útil, embora simplificada, da arquitetura REST é apresentada nos parágrafos seguintes.

O padrão de arquitetura REST consiste de clientes e servidores: clientes fazem solicitações a servidores; servidores processam solicitações de clientes e retornam a resposta apropriada. Solicitações e respostas são construídas tendo em vista a transferência de “representações de recursos". Um “recurso”, ou elemento de informação, é qualquer conceito coerente e significativo que possa ser referido no processo. A “representação de um recurso” é tipicamente um documento que captura o estado atual ou pretendido desse recurso.

Em qualquer momento definido no tempo da interação, um cliente pode estar em “transição” entre estados, ou “em repouso” (*at rest*). O cliente começa a enviar solicitações quando está pronto para fazer a transição para um novo estado. Enquanto uma ou mais solicitações estiverem pendentes, o cliente é considerado como em transição. A representação de cada estado contém *links* que podem ser utilizados na próxima vez que o cliente decida iniciar uma nova transição de estado.

Um *RESTful Web Service*, também chamado de um *RESTful Web API*, é um simples serviço *Web* implementado utilizando-se HTTP e os princípios e restrições do REST. Consiste em uma coleção de recursos, com três aspectos muito bem definidos:

- a ***URI* base** para o *Web Service* (por exemplo, http://www.exemplo.com/recursos/);
- o ***MIME type*** do dado suportado pelo *Web Service* (pode ser XML ou qualquer outro *MIME type* válido);
- o **Conjunto de Operações** suportado pelo *Web Service*, representados por verbos padronizados (*List, Retrieve, Replace, Update, Create, Delete*), utilizando necessariamente os métodos HTTP (*POST, GET, PUT, DELETE*).

A Tabela 19 ilustra como os verbos e métodos HTTP são usados na implementação de um *RESTful Web Service*:

Tabela 19: *RESTful Web Services* - métodos e verbos HTTP

Recurso	GET	PUT	POST	DELETE
Coleção de elementos URI (http:/exemplo.com/recursos/)	Lista (***List***) dados dos elementos da coleção	Substitui (***Replace***) a coleção inteira por outra	Cria (***Create***) um novo elemento na coleção	Destrói (***Delete***) a coleção
Elemento URI individual (http:/exemplo.com/recursos/123)	Obtém (***Retrieve***) a representação do elemento especificado, expresso em um *MIME type* apropriado	Atualiza (***Update***) o elemento especificado ou, se inexistente, cria (***Create***) um novo elemento	Trata o elemento especificado como uma coleção e cria (***Create***) nela um novo elemento	Remove (***Delete***) da coleção o elemento especificado

3.1.5.2.6 Papel do WSDL (*Web Services Description Language*)

A especificação WSDL define um formato XML para documentos onde serviços e mensagens são descritos de maneira abstrata, independente de seu uso ou implementação.

Essas definições estão livres para serem reutilizadas em situações e contextos distintos. Documentos WSDL referem-se a serviços, que são descritos como uma coleção de pontos (*endpoints* ou, na versão inicial, *ports*) em uma rede de computação distribuída.

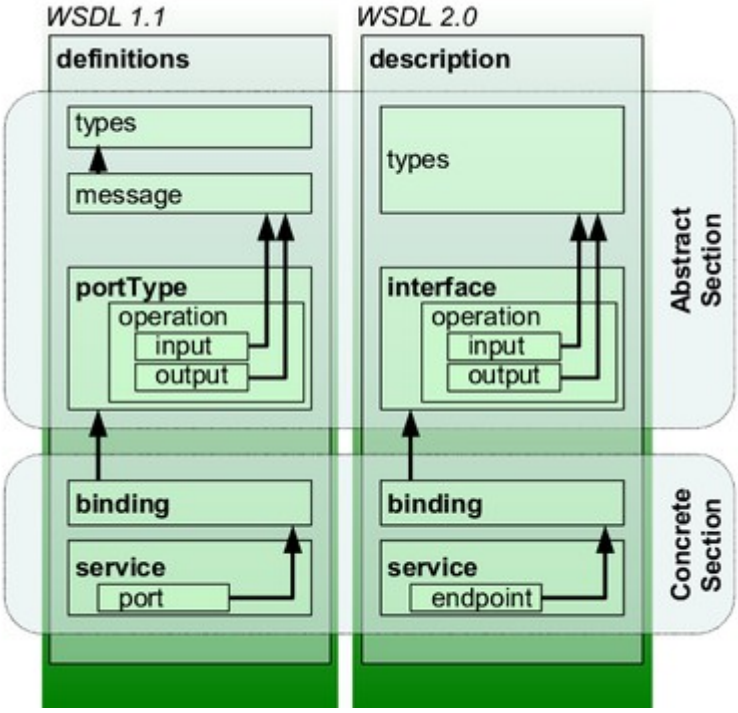


Figura 26: Conceitos definidos nas WSDL 1.0 e 2.0
(Fonte: Wikipedia)

Um *port* consiste na associação entre um endereço na rede e um mecanismo de enlace reutilizável (*binding*), enquanto coleções de *ports* definem serviços. Mensagens (*messages*) são descrições abstratas dos dados sendo transmitidos, e *interfaces* (na versão inicial, *port types*) são coleções abstratas das operações suportadas. O protocolo concreto e o formato da mensagem para um *port type* em particular constituem um enlace reutilizável, que promove a ligação entre o *port type* e as mensagens e operações. É através dessas abstrações que o WSDL descreve a *interface* pública de um *Web Service*.

Uma mensagem WSDL contém a informação necessária à execução de uma operação, e consiste logicamente de uma ou mais partes. Cada parte é associada a um atributo que tipifica a mensagem, podendo ser entendida com uma descrição lógica do conteúdo da mensagem, ou mesmo representar um parâmetro na mensagem. As mensagens foram excluídas na versão mais recente, que determina que, na definição de corpos de *inputs* e *outputs*, se faça uma referência direta a um documento XML *Schema*.

Em 2007, o WSDL 2.0 tornou-se uma recomendação oficial do W3C. Os objetos que fazem parte da versão atual dessa especificação são:

1. ***service*** – um *service* pode ser entendido como um recipiente para um conjunto de funções de um sistema que foram expostas aos protocolos da *Web*;
2. ***endpoint*** – define o endereço ou ponto de conexão para um *Web Service*, sendo tipicamente representado por uma simples *url*;

3. ***binding*** - especifica a *interface* e define o estilo do enlace SOAP, o tipo de transporte (protocolo SOAP) e as operações pertinentes;
4. ***interface*** – o elemento <*interface*> define um *Web Service*, as operações que podem ser executadas e as mensagens a serem utilizadas na execução das operações;
5. ***operation*** – uma operação pode ser comparada a um método, procedimento ou função de uma linguagem de programação;
6. ***types*** – são usados para a descrição dos dados, por meio de um *XML Schema*.

A importância do WSDL na prática tem a ver com a possibilidade de se construir aplicativos a partir da integração ou montagem de serviços de terceiros através da Internet. Antes, esses aplicativos eram necessariamente construídos, por assim dizer, “a partir do zero”. Para essa montagem se tornar possível, é necessário que os desenvolvedores obtenham algumas informações sobre esses serviços, tais como assinatura dos métodos a serem invocados, argumentos de entrada e saída, protocolos a serem utilizados, endereço do serviço na rede e formato dos dados. São essas as informações que a linguagem WSDL define em formato XML.

3.1.5.2.7 Infraestrutura de registro (UDDI)

O uso extensivo da tecnologia de *Web Services* para implementar serviços de negócio gerou a necessidade de se estruturar mecanismos para o seu gerenciamento, consolidando assim, a ideia de que os serviços são também ativos computacionais existentes nas organizações. Sendo um ativo computacional, da mesma forma que a organização mantém o registro do seu patrimônio (produtos, equipamentos, etc.), ela também deve manter o registro sobre os serviços que disponibiliza. Assim, em 2001 surgiram as primeiras publicações para se definir padrões de registro, localização e recuperação de serviços eletrônicos a partir de um catálogo ou diretório centralizado. Essas publicações deram origem a duas especificações que se tornaram padrão de mercado, conhecidas como UDDI (*Universal Description, Discovery and Integration*) e ebXML (*Electronic Business using Extensible Markup Language*).

A especificação UDDI é mais difundida por se tratar de um padrão simplificado que disponibiliza um conjunto restrito de metadados sobre o serviço, além de fornecer diversas APIs que facilitam a publicação e busca automática dos serviços. O objetivo do UDDI é servir como um serviço de diretório centralizado onde é possível publicar informações técnicas e de descrição dos *Web Services* que se deseja divulgar.

Através de serviços de registro UDDI, as partes interessadas em obter serviços pela Internet podem descobrir, comparar, contratar e invocar serviços, baseados em critérios técnicos e negociais tais como *interfaces* do serviço, níveis de disponibilidade, direitos autorais, custos, etc. O serviço de repositório do UDDI, por outro lado, se presta a ser interrogado por mensagens SOAP, provendo acesso a documentos WSDL que descrevem protocolos e formatos exigidos para a utilização dos serviços listados no diretório.

3.1.5.2.8 *Enterprise Service Bus* (ESB)

Um ESB (*Enterprise Service Bus*) é uma infraestrutura de software que facilita a interoperabilidade entre aplicações heterogêneas. O ESB é uma peça importante na implantação da SOA, pois provê a troca facilitada de mensagens, executa e controla transações complexas, orquestra serviços, e fornece recursos de notificação baseado no modelo *publish-subscribe*, além de outras facilidades.

A tecnologia de ESB foi desenvolvida para atender as demandas de integração entre aplicações distribuídas e em plataforma heterogênea de *hardware* e *software*, de modo a se evitar os problemas inerentes às plataformas de integração baseadas na tecnologia de EAI (*Enterprise Application Integration*). No modelo mais comum de EAI, conhecido como *hub and spoke*, as aplicações trabalham através de um único e centralizado *broker*, que constitui o canal de comunicação entre elas. Esse único *broker* ou *middleware*, como também é conhecido, embora apresente uma arquitetura mais simplificada e fácil de manter, também representa um único ponto de falha para toda a arquitetura. O ESB, por outro lado, introduziu a capacidade de distribuição do *middleware* provendo a possibilidade de se elaborar diversificadas configurações do ambiente tecnológico que passou a ser composto por diversos *brokers* interconectados. Outra diferença entre a tecnologia de ESB e a EAI consiste no fato de que o primeiro facilita o desacoplamento dos sistemas e o uso de padrões abertos para interoperabilidade, nem sempre atendidos pelos produtos baseados no último.

Essa Cartilha Técnica apresenta na Tabela 20 uma descrição das principais funcionalidades encontradas em arquiteturas ESB de pequeno, médio e grande porte.

Tabela 20: Funcionalidades do ESB

Funcionalidade	Descrição	Observação
Invocação	Suporte a protocolos síncronos e assíncronos, além do recurso de mapeamento de serviços (*locating* e *binding*)	Deve estar presente nas configurações básicas de ESB.
Roteamento	Endereçamento e roteamento de mensagens através das técnicas de roteamento estático, baseado em conteúdo, baseado em regras e baseado em políticas de uso.	Deve estar presente nas configurações básicas de ESB.
Mediação	Uso de adaptadores e protocolos específicos para a troca de dados, com ou sem recurso de transformação dos dados.	O recurso de adaptadores para comunicação com sistemas legados pode nem sempre estar disponível. Alguns ESB também podem não fornecer recursos para transformação de dados.
Mensageria	Processamento, transformação e tratamento das mensagens.	Deve estar presente nas configurações básicas de ESB.
Coreografia de Processos	Implementação de processos de negócio.	Este recurso geralmente não está presente no ESB, mas ele deve prover um mecanismo de acionamento dos processos de negócio implementados em outras ferramentas.

Orquestração de Serviços	Coordenação de serviços.	Este recurso pode ou não estar presente no ESB. Algumas configurações de ESB proveem o mecanismo de comunicação com ferramentas especializadas em orquestrar serviços.
Processamento Complexo de Eventos	Processamento de Eventos	Este recurso pode ou não estar presente no ESB. Algumas configurações de ESB proveem o mecanismo de comunicação com ferramentas especializadas em processamento complexo de eventos.
QoS (Qualidade de Serviço)	Segurança, gerenciamento de transações, controle de qualidade dos serviços publicados no ESB	Deve estar presente nas configurações básicas de ESB.
Gerenciamento	Monitoramento, auditoria, logging e console de administração.	Deve estar presente nas configurações básicas de ESB.

4. Ferramentas de apoio à interoperabilidade

4.1. Catálogo de Interoperabilidade

Como forma de promoção da interoperabilidade, a ePING disponibiliza aos órgãos de governo o Catálogo de Interoperabilidade, que é uma ferramenta composta pelo Catálogo de Serviços Interoperáveis e pelo Catálogo Padrão de Dados (CPD).

O Catálogo de Serviços Interoperáveis tem por objetivo tornar públicas as *interfaces* (pontos de integração) de sistemas que apoiem a oferta de serviços de Governo Eletrônico (E-PING, 2014). Quem deseja se conectar a um sistema, ou dele obter informações, deve consultar o catálogo no sitio http://catalogo.governoeletronico.gov.br, onde encontram-se registrados tanto *Web Services* como FTPs e outras modalidades de troca de informações.

Já o CPD tem por objetivo estabelecer padrões de tipos e itens de dados que se aplicam às interfaces dos sistemas que fazem parte do setor público.

O objetivo da ePING com essas duas iniciativas é a divulgação dos serviços de governo, assim como dos padrões das informações fornecidas e consumidas pelas instituições públicas. A Figura 27 mostra o Catálogo de Serviços Interoperáveis.

Serviço	Órgão	Sistema	Base Oficial?	Data Inclusão	Data Alteração	Documentação
Consulta a Títulos do Tesouro	STN - Secretaria do Tesouro Nacional	Títulos – Títulos do Tesouro	✗	27/09/2010	27/09/2010	(61 KB)
Consultar Tabelas Administrativas	STN - Secretaria do Tesouro Nacional	Novo SIAFI - Sistema Integrado de Administração Financeira do Governo Federal	✗	20/11/2013	16/01/2014	(290 KB)
Exportação SIGPlan	SPI - Secretaria de Planejamento e Investimentos Estratégicos	SIGPLAN - Sistema de Informações Gerenciais e Planejamento	✗	27/09/2010	27/09/2010	(264 KB)
Extrator de Dados	SEGEP - Secretaria de Gestão Pública	SIAPE - Sistema de Administração de Pessoal	✓	27/07/2011	12/11/2012	121 KB)
Fornecimento de Informações Cadastrais	RFB - Receita Federal do Brasil	InfoConv - Sistema de Informações para Convenentes	✓	03/06/2013	03/06/2013	(220 KB)
Importação de Dados - Submissão Batch	STN - Secretaria do Tesouro Nacional	Novo SIAFI - Sistema Integrado de Administração Financeira do Governo Federal	✗	20/11/2013	16/01/2014	(403 KB)
Infrasig SIGPLAN	SPI - Secretaria de Planejamento e Investimentos Estratégicos	SIGPLAN - Sistema de Informações Gerenciais e Planejamento	✗	13/09/2010	27/09/2010	(86 KB)
Manter Contas a Pagar e Receber	STN - Secretaria do Tesouro Nacional	Novo SIAFI - Sistema Integrado de Administração Financeira do Governo Federal	✗	20/11/2013	16/01/2014	(461 KB)
Manter Programação Financeira	STN - Secretaria do Tesouro Nacional	Novo SIAFI - Sistema Integrado de Administração Financeira do Governo Federal	✗	16/01/2014	16/01/2014	(331 KB)
SIAPE - Fita Espelho	SEGEP - Secretaria de Gestão Pública	SIAPE - Sistema de Administração de Pessoal	✓	09/05/2011	12/11/2012	122 KB)
SIAPE - Web Service	SEGEP - Secretaria de Gestão Pública	SIAPE - Sistema de Administração de Pessoal	✓	13/09/2010	12/11/2012	123 KB)

Figura 27: Busca no Catálogo de Serviços Interoperáveis

4.2. Padrão de Metadados para o Governo Eletrônico (ePMG)

O ePMG (Padrão de Metadados para o Governo Eletrônico) estabelece um conjunto mínimo de elementos que contêm dados necessários para a recuperação e gerenciamento de informações. Cada elemento contém informações relacionadas a um aspecto específico do recurso, como por exemplo, “Título” ou “Criador”.

O objetivo do ePMG é assegurar que as pessoas que pesquisam as informações do governo brasileiro na Web tenham acesso rápido e eficiente nas descrições dos recursos. Os elementos do ePMG têm o propósito de facilitar as pessoas localizarem os recursos que precisam, mesmo sem possuir conhecimento detalhado da localização ou da entidade responsável pelos mesmos.

O ePMG foi desenvolvido com base no Padrão Dublin Core (DC) do Dublin Core Metadata Initiative (DCMI), uma organização engajada no desenvolvimento de um padrão de metadados interoperável. O núcleo do DC é um conjunto mínimo de elementos para descrever recursos eletrônicos, composto por 15 elementos principais com as suas respectivas definições.

O conjunto de elementos do ePMG consiste em 20 elementos: 15 elementos do DC e 5 elementos adicionais identificados como necessários para o contexto do governo eletrônico brasileiro.

O ePMG difere do padrão DC em outros pontos importantes:

- pode ser utilizado para descrever tanto recursos eletrônicos (por exemplo, páginas web, arquivos ou outros objetos digitais) quanto recursos não eletrônicos (por exemplo, livros, acervos de museu, pinturas, documentos impressos etc.);
- pretende descrever mais do que recursos informacionais, podendo descrever serviços disponíveis na *Web*;
- a adoção de qualificadores adicionais; e
- diferentes critérios na obrigatoriedade ou não do uso de elementos e qualificadores.

Os órgãos do governo precisam avaliar os seus principais objetivos e o público-alvo a fim de decidir quais os recursos que devem ser descritos prioritariamente com o uso do ePMG. Recomenda-se a identificação dos recursos com maior frequência de utilização para que estes também sejam prioritariamente descritos.

Para cada elemento do ePMG haverá os seguintes dados:

- **Nome**: Termo atribuído ao elemento em português
- **Identificador**: Termo atribuído ao elemento de acordo com o padrão originário.

- **Definição**: Uma descrição do que se trata o elemento.
- **Obrigatoriedade**: Define o grau de uso do elemento, divididos em:
    - obrigatório: este elemento deve obrigatoriamente ter um valor;
    - obrigatório se aplicável: a este elemento deve ser fornecido um valor se o tipo de recurso assim o requerer;
    - opcional: a este elemento pode ser fornecido um valor se o dado estiver disponível e apropriado ao recurso.

    A obrigatoriedade aplica-se ao elemento e a seus qualificadores quando for o caso.
- **Objetivo:** Fornece a informação essencial sobre a aplicabilidade do elemento.
- **Comentários:** Informação adicional para a compreensão e utilização do elemento ou dos qualificadores do elemento.
- **Não confundir com:** Fornece informações comparativas com elementos que eventualmente possam gerar dúvidas ou semelhanças no nome e suscitar uso inadequado.
- **Qualificadores:** Usado para tornar o significado de um elemento mais específico, podendo ser utilizado para informação adicional de um recurso.
- **Exemplos:** Indica como os elementos podem ser acrescentados para diferentes situações. Os exemplos são fictícios, pois são destinados somente para demonstrar a forma de utilização do elemento ou qualificador.
- **Sintaxe de HTML:** Usualmente os metadados aparecem em forma de tag em um arquivo HTML. Este campo visa facilitar a forma de uso dos elementos ePMG para páginas da Web. Por exemplo: <meta name=“dc.element” content="valor">.
- **Esquemas:** Os esquemas indicam a fonte que especifica a forma ou informa os valores possíveis para um elemento. Incluem vocabulários controlados, normas brasileiras e internacionais.
- **Mapeamento:** Correlação com elementos de outros padrões de metadados como:

    e-GMS: Government Metadata Standard;

    AGLS: Australian Government Locator Service;

    GILS: Government Locator Service;

FGDC: Federal Geographic Data Committee (FGDC) Metadata;

MARC: MAchine-Readable Cataloging; etc.

Para mais informações, acesse a página do ePMG no sítio do governo eletrônico: http://governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/padrao-de-metadados-do-governo-eletronico-e-pmg.

4.3. Vocabulário Controlado de Governo Eletrônico (VCGE)

Uma informação pode ser definida e descrita de diversas formas, sendo a área de estudo desse tema denominada de “Representação do Conhecimento”. Um dos métodos mais básicos utilizados pelo ser humano para descrever os objetos ao seu redor é, sem dúvida, a classificação. Classificar objetos, coisas ou mesmo conceitos, consiste em agrupá-los de acordo com suas similaridades.

O VCGE (Vocabulário Controlado do Governo Eletrônico) é um vocabulário controlado organizado como uma taxonomia criado pelo governo brasileiro com o objetivo de organizar assuntos do governo. A primeira versão da taxonomia ficou conhecida como LCG (Lista de Categorias de Governo), que passou a ser a LAG (Lista de Assuntos do Governo), e agora é denominada VCGE que, além de associar os elementos taxonômicos com o ePMG (Padrão de Metadados do Governo Eletrônico), tem o foco no cidadão e, por isso, apresenta um esquema mais intuitivo e abrangente.

O VCGE é composto de dois níveis e representam as áreas de atuação do governo. Ele possui informações como termos incluídos, códigos numéricos e outros campos. Os termos e a quantidade de níveis, termos incluídos podem mudar e evoluir, afinal o VCGE é um vocabulário e precisa se adaptar as necessidades de evolução dos órgãos. A Figura a seguir exibe um trecho do VCGE e o detalhamento de um item do primeiro nível.

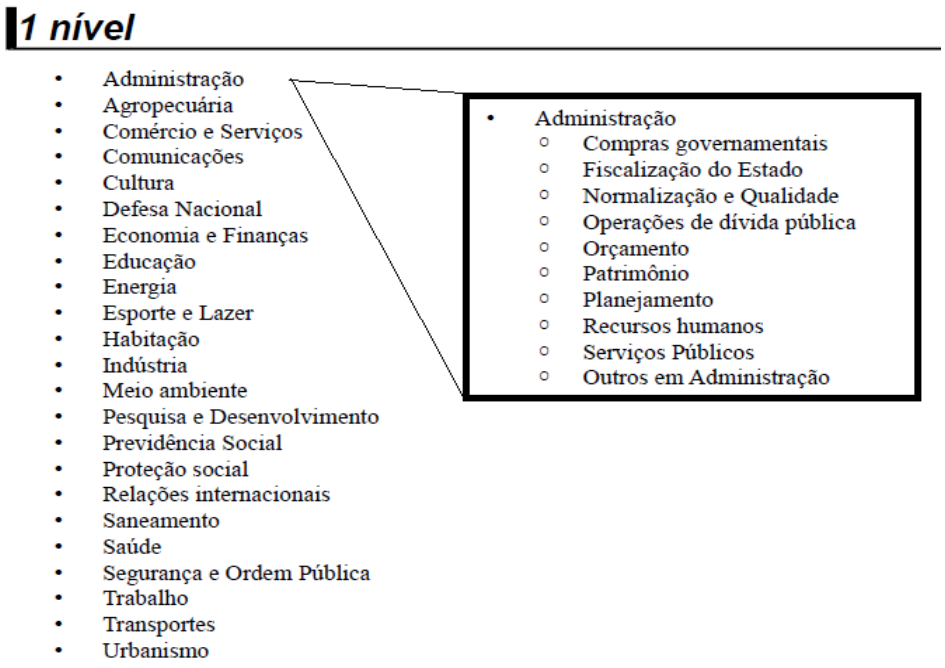


Figura 28: Estrutura do VCGE

O VCGE tem como meta principal auxiliar na organização das informações governamentais de modo a beneficiar o cidadão que necessita realizar, por exemplo, consultas aos sítios e portais informatizados do governo. Por isso, a ePING adota o VCGE como padrão taxonômico para a organização de informações

eletrônicas, principalmente nos casos em que a informação é direcionada ao cidadão através de portais na Internet.

O VCGE está disponível em diversos formatos incluindo documentos PDF, SQL, JSON, SKOS e CSV. Novos formatos podem vir a ser incorporados. Um dos arquivos PDF é o VCGE Detalhado que contém descrições completas da história, propósitos e características do VCGE.

Para mais informações, acesse a página do ePMG no sítio do governo eletrônico: http://governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/vcge.

REFERÊNCIAS BIBLIOGRÁFICAS

ARMS, W. Y. Thoughts about Interoperability in the NSDL. Cornell University. [S.l.]. 2000.

BAIRD, S. A. Government Role and the Interoperability Ecosystem. ICEGOV2007, Macao, Dezembro 2007. 219-290.

BASS, L.; CLEMENTS, P.; KAZMAN, R. Software architecture in practice. 2. ed. Boston, MA: Pearson Education, Inc, 2003.

CGI. Resolução CGI.br No. 08, 28 de novembro de 2008. CGI, 2008. Disponível em: <http://www.cgi.br/regulamentacao/resolucao2008-008.htm>. Acesso em: 2 de Maio de 2014.

COMPRASNET. Especificação de Referência - Switches de Borda e Central Médio e Pequeno. Portal de Compras de TIC, 2010. Disponível em: <https://www.comprasnet.gov.br/PortalCompras/portais/tic/livre/download_espec_switch.asp>. Acesso em: 2 de Maio de 2014.

CROCKFORD, D. Network Working Group. RFC 4627, 2006. Disponível em: <http://tools.ietf.org/html/rfc4627>. Acesso em: 2 de Maio de 2014.

E-PING. ePING: Programa de Governo Eletrônico Brasileiro. Governo Eletrônico, 2014. Disponível em: <http://www.eping.e.gov.br>. Acesso em: 2 de Dezembro de 2014.

ERL, T. Service-Oriented Architecture: A field Guide to Integrating XML and Web Services. New Jersey: Prentice Hall PTR, 2004.

GINGA. TV Interativa. Ginga Digital TV Middleware, 2006. Disponível em: <http://www.ginga.org.br/>. Acesso em: 2 de Maio de 2014 .

ICP-BRASIL. Resolução Nº 58. Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil, 2008. Disponível em: <http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/Resolucao_58.pdf>. Acesso em: 2 de Maio de 2014.

ICP-BRASIL. Resolução Nº 65. Padrões e Algoritmos Criptográficos da ICP-Brasil, 2009. Disponível em: <http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/resolucao65.pdf>. Acesso em: 2 de Maio de 2014.

IETF. RFC 3277: Guidelines for Evidence Collection and Archiving. Network Working Group, 2002. Disponível em: <http://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 2 de Maio de 2014.

JOSUTTIS, N. M. SOA In Pratice. [S.l.]: O'Reilly, 2007.

JSON.ORG. JSON, 2009. Disponível em: <http://json.org/>. Acesso em: 2 de Maio de 2014.

LEWIS, G. A. et al. Common misconception about Service-Oriented Architecture. Sixth International IEEE Conference on Commercial off the shelf Based Software Systems. [S.l.]: [s.n.]. 2007.

MCGOVERN, J. et al. Enterprise Service Oriented Architectures: concepts, challenges, recommendations. [S.l.]: Springer, 2006.

NEWCOMER, E.; LOMOW, G. Understanding SOA with Web Services. Massachusetts: Addison Wesley, 2005.

NIST. FIPS 140-1/2: Security Requirements For Cryptographic Modules. National Institute of Standards and Technology, 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips1401.htm, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Acesso em: 2 de Maio de 2014.

NIST. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology - Special Publication 800-86, 2006. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: 2 de Maio de 2014.

OASIS. Reference Model for Service Oriented Architecture 1.0. OASIS SOA Reference Model TC, 2006. Disponível em: <http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf>. Acesso em: 2 de Maio de 2014.

OMG. BPMN Graphical Elements. BPMN Core Elements, 2005. Disponível em: <http://www.omg.org/bpmn/Samples/Elements/Core_BPMN_Elements.htm>. Acesso em: 2 de Maio de 2014.

PAPAZOGLOU, T. A.; RIBBERS, P. M. A. E-business: Organizational and technical foundation. West Sussex, UK: John Wiley & Sons, 2006.

POTTS, S.; KOPACK, M. Web Services in 24 hours. [S.l.]: Sams Publishing, 2003.

PRESIDÊNCIA DA REPÚBLICA. Resolução 07. Resolução no. 07, julho de 2002, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm>. Acesso em: 2 de Maio de 2014.

PRESIDÊNCIA DA REPÚBLICA. Normas Complementares N° 4 a 7, 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf; http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf; http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf; http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf>. Acesso em: 2 de Maio de 2014.

GOVERNO ELETRÔNICO. Regra de Formação de Nomes para a composição dos endereços eletrônicos (e-mail) 2011, ISSN S/N. Disponível em: <http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade/arquivo>. Acesso em: 2 de Maio de 2014.

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO, MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Portal Brasileiro de Dados Abertos. Portal Brasileiro de Dados Abertos, 2014. Disponível em: <http://dados.gov.br/>. Acesso em: 2 de Maio de 2014.

TANEMBAUM, A. S. Sistemas Operacionais Modernos. [S.l.]: Prentice Hall, 2003.

TEECE, D. J.; PISANO, G.; SHUEN, A. Dynamic Capabilities and Strategic Management. Strategic Management Journal, v. 17, Agosto 1997. ISSN 7.

TICONTROLE. Rede de Informação Legislativa e Jurídica: Projeto LexML Brasil. LexML, 2010. Disponível em: <http://projeto.lexml.gov.br/>. Acesso em: 2 de Maio de 2014.

TRIPATHI, R.; GUPTA, M. P.; BHATTACHARYA, J. Selected Aspects of Interoperability in One-Stop Government Portal of India. Computer Society of India, New Delli, India, 2008. 1-11.

UNICODE CONSORTIUM. UNICODE 4.2.0. Padrão UNICODE, 2010. Disponível em: <http://www.unicode.org/versions/Unicode5.2.0/>. Acesso em: 2 de Maio de 2014.

W3C. Mobile Web Best Practices. W3C Recommendation, 2008. Disponível em: <http://www.w3.org/TR/mobile-bp/>. Acesso em: 2 de Maio de 2014.

W3C. Semantic Web Standards. RDF, 2010. Disponível em: <http://www.w3.org/RDF/>. Acesso em: 2 de Maio de 2014.

ZHAO, Y. Enterprise Service Oriented Architecture (ESOA) Adoption Reference. IEEE International Conference on Services Computing. Washington, DC: [s.n.]. 2006.

Ministério do
Planejamento

gov.br
ePING