

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

Secretaria de Logística e Tecnologia da Informação

Departamento de Integração de Sistemas



Padrões de Interoperabilidade de Governo Eletrônico

**Guia de Interoperabilidade
Cartilha Técnica**

**Versão 2011
Junho de 2011**



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).

Impresso no Brasil.

1ª. Edição: Brasília, 13 de junho de 2011.

FICHA CATALOGRÁFICA

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO
Guia de Interoperabilidade: Cartilha Técnica, 2011, 106 páginas, 297 mm. Documento técnico do governo brasileiro.
1. Interoperabilidade
2. Governo eletrônico
3. e-PING

CESSÃO DE DIREITOS

Para a utilização deste documento é necessário seguir as regras da licença Creative Commons Versão 2.5 Brasil. Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para (http://creativecommons.org/licenses/by-nc-sa/2.5/br/deed.pt_BR). Observamos ainda que a responsabilidade pela autoria dos textos e imagens desta obra é exclusivamente dos autores.

Presidente da República

Dilma Rousseff

Ministério do Planejamento, Orçamento e Gestão

Miriam Belchior

Secretaria de Logística e Tecnologia da Informação – SLTI

Delfino Natal de Souza

Departamento de Integração de Sistemas – DSI

Corinto Meffe

Coordenação Geral de Gestão Corporativa – CGGC

Roberto Shayer Lyra

e-PING

Coordenador: Corinto Meffe

GT 1: Diogo Tabalipa

GT 2: Jorilson da Silva Rodrigues

GT 3: Paulo Maia da Costa

GT 4: Roberto Shayer Lyra

GT 5: Marcus Vinícius da Costa

Equipe de Elaboração SLTI

Cláudia do Socorro Ferreira Mesquita

Hudson Vinícius Mesquita

Julio Cesar dos Santos Nunes

Rachel Cristina Guimarães Monteiro Domingos

Yuri Fontes de Oliveira

Equipe de Elaboração IFCI/AECID

Gonçalo Teixeira Nunes

Patrycia Barros de Lima Klavdianos

Revisão Técnica

Carlos E. Jiménez Gómez

SUMÁRIO

LISTA DE TABELAS.....	6
LISTA DE FIGURAS.....	7
LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIACÕES.....	8
APRESENTAÇÃO.....	12
1.INTRODUÇÃO.....	14
1.1.Organização da Cartilha Técnica de Interoperabilidade.....	14
1.2.Assuntos não contemplados.....	15
1.3.Convenções utilizadas.....	15
2.FUNDAMENTOS DE INTEROPERABILIDADE.....	16
2.1.Introdução.....	16
2.2.Dimensões da Interoperabilidade.....	17
2.3.Interoperabilidade e Conformidade.....	19
3.INTEROPERABILIDADE TÉCNICA.....	21
3.1.Interoperabilidade Técnica na e-PING.....	21
3.2.Interoperabilidade Técnica e a Interconexão.....	23
3.2.1.Especificações para Interconexão (Mensageria).....	23
3.2.2.Especificações para Interconexão (Infraestrutura de Rede).....	24
3.2.3.Especificações para Interconexão (Serviços de Rede).....	26
3.3.Interoperabilidade Técnica e a Segurança.....	28
3.3.1.Especificações para Segurança (Comunicação de dados).....	29
3.3.2.Especificações para Segurança (Correio Eletrônico).....	31
3.3.3.Especificações para Segurança (Criptografia).....	32
3.3.4.Especificações para Segurança (Desenvolvimento de Sistemas).....	34
3.3.5.Especificações para Segurança (Serviços de Rede).....	36
3.3.6.Especificações para Segurança (Redes Sem Fio).....	36
3.3.7.Especificações para Segurança (Resposta a Incidentes de Segurança da Informação).....	37
3.4.Interoperabilidade Técnica e Meios de Acesso.....	37
3.4.1.Especificações para Meios de Acesso (Mobilidade).....	38
3.4.2.Especificações para Meios de Acesso (TV Digital).....	38
3.5.Interoperabilidade Técnica e as Áreas de Integração para Governo Eletrônico.....	40
3.5.1.Linguagem para Execução de Processos (BPEL4WS).....	40
3.6.Arquitetura de Software e Interoperabilidade Técnica.....	42
3.6.1.Arquitetura SOA.....	42
3.6.2.Serviços.....	45
3.6.3.Modelo de Referência SOA - OASIS.....	45
3.6.4.Opção por Web Services.....	47

3.6.5.Papel do SOAP (Simple Object Access Protocol).....	49
3.6.6.Papel do REST (Representational State Transfer).....	51
3.6.7.Papel do WSDL (Web Services Description Language).....	53
3.6.8.Utilização de um Web Service.....	58
3.6.9.Enterprise Service Bus (ESB).....	58
4.INTEROPERABILIDADE SEMÂNTICA.....	62
4.1.Interoperabilidade Semântica na e-PING.....	62
4.2.Interoperabilidade Semântica e a Interconexão.....	63
4.3.Interoperabilidade Semântica e Meios de Acesso.....	65
4.3.1.Codificação dos Dados (encoding).....	67
4.3.2.Formato de Intercâmbio de hipertexto.....	68
4.3.3.Intercâmbio de arquivos.....	69
4.4.Interoperabilidade Semântica e a Organização e Intercâmbio de Informações.....	70
4.4.1.Linguagem para Intercâmbio de Dados (XML).....	71
4.4.2.Linguagem para Intercâmbio de Dados (JSON).....	77
4.4.3.Transformação de Dados (XSL).....	78
4.4.4.Definição de Dados para intercâmbio (XML Schemas).....	82
4.4.5.Descrição de Recursos (RDF).....	84
4.4.6.Taxonomia para navegação (VCGE).....	87
4.5.Interoperabilidade Semântica e as Áreas de Integração para Governo Eletrônico.....	89
5.INTEROPERABILIDADE ORGANIZACIONAL.....	92
5.1.Interoperabilidade Organizacional na e-PING.....	92
5.1.1.Catálogo de Interoperabilidade.....	93
5.1.2.Modelo de Documentação de Web Services.....	94
5.1.3.Notação de Modelagem de Processos (BPMN).....	96
5.1.4.Infraestrutura de registro (UDDI).....	98
6.CONCLUSÃO.....	101
REFERÊNCIAS BIBLIOGRÁFICAS.....	102
ÍNDICE REMISSIVO.....	105

LISTA DE TABELAS

Tabela 1: Interoperabilidade Técnica na e-PING.....	22
Tabela 2: Componentes do Segmento de Interconexão (Mensageria)	24
Tabela 3: Componentes do Segmento de Interconexão (Infraestrutura de Rede)	25
Tabela 4: Componentes do Segmento de Interconexão (Serviços de Rede)	26
Tabela 5: Componentes do Segmento de Segurança (Comunicação de Dados)	29
Tabela 6: Componentes do Segmento de Segurança (Correio Eletrônico)	31
Tabela 7: Componente do Segmento de Segurança (Criptografia)	32
Tabela 8: Componentes do Segmento de Segurança (Desenvolvimento de Sistemas)	35
Tabela 9: Componentes do Segmento de Segurança (Serviços de Rede)	36
Tabela 10: Componentes do Segmento de Segurança (Redes Sem Fio)	36
Tabela 11: Componentes do Segmento de Segurança (Resposta a Incidentes de Segurança da Informação)	37
Tabela 12: Componentes do Segmento de Meios de Acesso (Mobilidade).....	38
Tabela 13: Componentes do Segmento de Meios de Acesso (TV Digital).....	38
Tabela 14: Componentes do Segmento de Áreas de Integração para Governo Eletrônico.....	40
Tabela 15: RESTful Web Services - métodos e verbos HTTP.....	53
Tabela 16: Funcionalidades do ESB.....	59
Tabela 17: Interoperabilidade Semântica na e-PING.....	63
Tabela 18: Especificações para o Segmento de Interconexão.....	64
Tabela 19: Especificações para o Segmento de Meios de Acesso.....	66
Tabela 20: Especificações para o Segmento de Organização e Intercâmbio de Informações.....	71
Tabela 21: Estrutura do RDF (W3C, 2010).....	85
Tabela 22: Especificações para o Segmento de Áreas de Integração para Governo Eletrônico (1).....	89
Tabela 23: Especificações para o Segmento de Áreas de Integração para Governo Eletrônico (2).....	92
Tabela 24: Estrutura e funcionalidades de um registro UDDI 2.0 (Modificado do XML.com).....	100

LISTA DE FIGURAS

Figura 1: Dimensões da Interoperabilidade	18
Figura 2: Ciclo dos níveis de conformidade da e-PING.....	19
Figura 3: Modelo Conceitual da SOA (MCGOVERN, SIMS, et al., 2006).....	46
Figura 4: Estrutura do SOAP.....	49
Figura 5: Exemplo de uma requisição SOAP (Fonte: W3Schools).....	51
Figura 6: Exemplo de uma resposta SOAP (Fonte: W3Schools).....	51
Figura 7: Conceitos definidos nas WSDL 1.0 e 2.0.....	53
Figura 8: Descrição de um Web Service com WSDL 2.0.....	57
Figura 9: XML utilizado para transportar dados dentro de uma aplicação.....	72
Figura 10: XML utilizado para transportar dados com a tecnologia de Web Services.....	72
Figura 11: XML utilizado como conversor de dados no contexto de uma aplicação.....	73
Figura 12: XML utilizado como conversor de dados no contexto de várias aplicações.....	73
Figura 13: Comparação das tecnologias de Banco de Dados e XML (Modificado de Erl, 2004).....	74
Figura 14: Exemplo de um arquivo JSON.....	78
Figura 15: Exemplo de um documento XML (Fonte: W3Schools).....	80
Figura 16: Exemplo de um documento XSL.....	81
Figura 17: Resultado final da transformação XSL (Fonte: W3Schools).....	81
Figura 18: Exemplo de um XML Schema (Fonte: W3Schools).....	84
Figura 19: Referência a um XML Schema a partir do XML (Fonte: W3Schools).....	84
Figura 20: Elementos básicos do RDF.....	86
Figura 21: Exemplo de um documento RDF (Fonte: W3Schools).....	86
Figura 22: Estrutura do VCGE.....	88
Figura 23: Exemplo de uso do VCGE.....	89
Figura 24: Referência a documentos jurídicos no LexML (TICONTROLE, 2010).....	91
Figura 25: Interface de consulta do LexML (TICONTROLE, 2010).....	91
Figura 26: Busca no Catálogo Padrão de Dados.....	93
Figura 27: Busca no Catálogo de Serviços Interoperáveis.....	94
Figura 28: Padrão para a descrição dos Web Services de governo.....	94
Figura 29: Principais componentes da notação BPMN (OMG, 2005).....	97
Figura 30: Exemplo de um processo de negócio mapeado em BPMN.....	98

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIações

3DES – *Triple Data Encryption Algorithm*
ABNT – Associação Brasileira de Normas Técnicas
AECID – Agência Espanhola de Cooperação para o Desenvolvimento
AES – *Advanced Encryption Standard*
AH – *Authentication Header*
ANATEL – Agência Nacional de Telecomunicações
ANEEL – Agência Nacional de Energia Elétrica
API – *Application Programming Interfaces*
ASCII – *American Standard Code for Information Interchange*
ATM – *Asynchronous Transfer Mode*
BPEL4WS – *Business Process Execution Language for Web Services*
BPMI – *Business Process Management Initiative*
BPML – *Business Process Modeling Language*
BPMN – *Business Process Modeling Notation*
CGI – Comitê Gestor da Internet no Brasil
CORBA – *Common Object Request Broker Architecture*
CoS – *Class of Service*
CPD – Catálogo Padrão de Dados
DCOM – *Distributed Common Object Model*
DES – *Data Encryption Standard*
DNS – *Domain Name System*
DNSSEC – *Domain Name System Security Extensions*
DOM – *Document Object Model*
DSDL – *Document Schema Definition Languages*
DTD – *Document Type Definition*
EAI – *Enterprise Application Integration*
ebXML – *Electronic Business using Extensible Markup Language*
ECC – *Elliptic Curve Cryptography*
ECDSA – *Elliptic Curve Digital Signature Algorithm*
ECIES – *Elliptic Curve Integrated Encryption Scheme*
e-GIF – *eGovernment Interoperability Framework*
EGTI – Estratégia Geral de Tecnologia da Informação
e-Gov – Governo Eletrônico
e-MAG - Modelo de Acessibilidade de Governo Eletrônico
e-PING – Padrões de Interoperabilidade de Governo Eletrônico

e-PMG – Padrão de Metadados do Governo Eletrônico

ESB – *Enterprise Service Bus*

ESP – *Encapsulating Security Payload*

FTP – *File Transfer Protocol*

G2B – *Government-to-Business*

G2C – *Government-to-Citizen*

G2G – *Government-to-Government*

HTML – *Hyper-Text Markup Language*

HTTP/1.1 – *Hypertext Transfer Protocol V1.1*

ICP – Infraestrutura de Chaves Públicas

IDL – *Interface Definition Language*

IEEE – *Institute of Electrical and Electronic Engineers*

IES – *Integrated Encryption Scheme*

IETF – *Internet Engineering Task Force*

IFCI – Fundação Instituto para o Fortalecimento das Capacidades Institucionais

IKE – *Internet Key Exchange*

IMAP – *Internet Message Access Protocol*

IMPP – *Instant Messaging and Presence Protocol*

IP – *Internet Protocol*

IPv4 – *Internet Protocol version 4*

IPv6 – *Internet Protocol version 6*

ISO – Organização Internacional para Padronização

ITI – Instituto Nacional de Tecnologia da Informação

ITU – *International Telecommunications Union*

JSON – *JavaScript Object Notation*

JSP – *Java Server Pages*

LAG – Lista de Assuntos do Governo

LAN – *Local Area Network*

LDAP – *Lightweight Directory Access Protocol*

MIME – *Multipurpose Internet Mail Extensions*

MIMO – *Multiple-Input, Multiple-Output*

MP – Ministério do Planejamento, Orçamento e Gestão

MPLS – *Multiprotocol Label Switching*

NCL – *Nested Context Language*

NIST – *National Institute of Standards and Technology*

NSA – *National Security Agency*

NSH – Níveis de Segurança de Homologação

NTP – *Network Time Protocol*
OASIS – *Organization for the Advancement of Structured Information Standards*
ORB – *Object Request Broker*
PDF – *Portable Document Format*
PKI – *Public Key Infrastructure*
POP3 – *Post Office Protocol V. 3*
RDF – *Resource Description Framework*
RPC – *Remote Procedure Calls*
REST – *Representational State Transfer*
RMI – *Remote Method Invocation*
RSA – *Rivest, Shamir, & Adleman*
RTF – *Rich Text Format*
SAF – *Schema Adjunct Framework*
SASL – *Simple Authentication and Security Layer*
SAX – *Simple API for XML*
SBTVD – *Sistema Brasileiro de Televisão Digital*
SERPRO – *Serviço Federal de Processamento de Dados*
SAML – *Security Assertion Markup Language*
SHA – *Secure Hash Algorithm*
SHTML – *Server-side HTML*
SIORG – *Sistema de Informações Organizacionais*
SIP – *Session Initiation Protocol*
SIPP – *Simple Internet Protocol Plus*
SISP – *Sistema de Administração dos Recursos de Informação e Informática*
SLTI - *Secretaria de Logística e Tecnologia da Informação*
S/MIME – *Secure/Multipurpose Internet Mail Extensions*
SNMP – *Simple Network Management Protocol*
SMS – *Short Message Service*
SMTP – *Simple Mail Transfer Protocol*
SNTP – *Simple Network Time Protocol*
SOA – *Service-Oriented Architecture*
SOAP – *Simple Object Access Protocol*
SOX – *Schema for Object Oriented XML*
SSL – *Secure Socket Layer*
SVG – *Scalable Vector Graphics*
TCP – *Transmission Control Protocol*
TI – *Tecnologia da Informação*

TIC – Tecnologia da Informação e Comunicação
TLS – *Transport Layer Security*
TSA – *Time-Stamping Authority*
TSP – *Time-Stamp Protocol*
UCS – *Universal Character Set*
UDDI – *Universal Description, Discovery and Integration*
UDP – *User Datagram Protocol*
URI – *Uniform Resource Identifier*
URL - *Uniform Resource Locator*
URN – *Uniform Resource Name*
UTF – *Unicode Transformation Format*
VCGE – Vocabulário Controlado do Governo Eletrônico
XHTML – *Extensible Hypertext Markup Language*
XKMS – *XML Key Management Specification*
XML – *Extensible Markup Language*
XMPP – *Extensible Messaging and Presence Protocol*
XPDL – *XML Process Definition Language*
XSL – *Extensible Stylesheet Language*
XSL-FO – *XSL Formatting Objects*
XSLT – *Extensible Stylesheet Language Transformations*
W3C – *World Wide Web Consortium*
WAN – *Wide Area Network*
WLAN – *Wireless Local Area Network*
WML – *Wireless Markup Language*
WPA – *Wi-Fi Protected Access*
WSDL – *Web Services Description Language*

APRESENTAÇÃO

O Guia de Interoperabilidade do Governo apresenta orientações para o desenvolvimento de soluções de TIC (Tecnologia da Informação e Comunicação) aderentes à arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico) como forma de incentivar a interoperabilidade governamental entre os entes da Federação. Ele é organizado em dois volumes: o **Manual de Gestão de Interoperabilidade** e a **Cartilha Técnica de Interoperabilidade**.

O **Manual de Gestão de Interoperabilidade** tem como público-alvo principal os gestores de TIC dos órgãos do Governo, particularmente aqueles integrantes do SISP (Sistema de Administração dos Recursos de Informação e Informática), enquanto também possa ser útil aos gestores de outras áreas usuárias de serviços de TIC. Esse documento possui diretrizes de gestão aderentes à EGTI (Estratégia Geral de Tecnologia da Informação), para a utilização adequada da e-PING, assim como indicações de ações promovidas em nosso país e em outros países com o objetivo de promover 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 TIC, ou seja: projetistas, analistas, desenvolvedores e pessoal de apoio ou suporte técnico. Esse documento apresenta os requisitos técnicos, descreve práticas de projeto e indica melhores usos de tecnologias de mercado como forma de se atingir interoperabilidade governamental de melhor qualidade e maior abrangência.

Qual é o conteúdo do Guia de Interoperabilidade do Governo?

O Guia de Interoperabilidade do Governo foi elaborado através da visão de utilização dos padrões tecnológicos, semânticos e organizacionais sugeridos na versão 2011 da e-PING, publicado em Dezembro de 2010 (E-PING, 2011). Por isso, não se pretendeu com este documento esgotar em uma única edição todos os aspectos inerentes à interoperabilidade vista à luz das ciências da gestão pública e da tecnologia da informação. O que se pretende é a evolução gradativa e contínua do documento, tal como ocorre hoje com a própria e-PING.

De um modo geral, espera-se que o Guia de Interoperabilidade do Governo resulte em uma contribuição relevante para a melhoria contínua dos processos de trabalho da área de TIC, resultando na utilização correta dos padrões e tecnologias existentes, na redução de custos e no aumento da qualidade dos serviços prestados. Acredita-se que, com isso, os ganhos alcançados deverão convergir em melhores serviços prestados pelo Governo ao cidadão e à sociedade brasileira. Sob este amplo ponto de vista, o Guia de Interoperabilidade do Governo deve ser

compreendido como um documento para aplicação de boas práticas, e consequente execução de ações de melhoria contínua em interoperabilidade governamental. Nesse sentido o Guia necessitará de atualização frequente, acompanhando a evolução da e-PING e de sua aplicação.

Quem deve utilizar o Guia de Interoperabilidade do Governo?

O Guia de Interoperabilidade do Governo segue as recomendações da e-PING quanto à adoção dos padrões para interoperabilidade governamental. Assim, embora o uso deste guia não seja obrigatório no sentido legal, recomenda-se a sua apreciação por parte dos usuários compulsórios da e-PING, que são os órgãos do Poder Executivo do Governo Federal (E-PING, 2011).

Todo o conteúdo deste documento está em consonância com as diretrizes do Comitê Executivo de Governo Eletrônico, criado pelo Decreto de 18 de outubro de 2000 e publicado em sítio específico na Internet (<http://www.eping.e.gov.br>). Isso garante o acesso público às informações aqui publicadas, pois o governo brasileiro está comprometido em assegurar que estas políticas e especificações permaneçam alinhadas com as necessidades da sociedade e com a evolução do mercado e da tecnologia.

Como ler e colaborar com o documento

Este documento pode ser lido da primeira à última página, ou individualmente por seção após a localização, no sumário, dos tópicos de interesse. Ele estará sujeito a revisões anuais, com publicação intermediária de atualizações sempre que existirem modificações significativas, ou ainda quando forem publicadas modificações na própria e-PING que venham a afetar substancialmente documentos auxiliares como este Guia.

Os interessados em contribuir com este documento devem fazê-lo preferencialmente pela Internet, no endereço <http://www.eping.e.gov.br>. Devem também estar atentos aos processos periódicos de consulta pública divulgados naquele endereço

1. INTRODUÇÃO

1.1. Organização da Cartilha Técnica de Interoperabilidade

A Cartilha Técnica de Interoperabilidade está organizada da seguinte forma:

Capítulo 2 – Fundamentos de Interoperabilidade

Introduz o tema “interoperabilidade” e define os conceitos mais relevantes para uma boa compreensão dos capítulos subsequentes. Os tópicos tratados nesse capítulo não são extensos no que se refere ao conteúdo. Assim, havendo a necessidade de um maior detalhamento do assunto, recomenda-se que o leitor considere a bibliografia sugerida ao final deste documento. A partir do capítulo seguinte, o leitor será remetido ao mundo prático da interoperabilidade, em suas três dimensões (técnica, semântica e organizacional).

Capítulo 3 – Interoperabilidade Técnica

O capítulo 3 aprofunda-se nos conceitos associados à interoperabilidade técnica de modo a tratar questões como infraestrutura de TIC, arquitetura de software, projeto, desenvolvimento e manutenção de sistemas computacionais. A interoperabilidade técnica é hoje a dimensão predominante na e-PING, e isso se refletirá naturalmente neste Guia.

Capítulo 4 – Interoperabilidade Semântica

O capítulo 4 fornece uma descrição dos conceitos associados à interoperabilidade semântica e explora os seguintes temas: organização, classificação e distribuição de dados dentro e fora das organizações públicas. Também é foco deste capítulo direcionar o profissional técnico no melhor uso de linguagens de definição e padronização dos esquemas de dados.

Capítulo 5 – Interoperabilidade Organizacional

O capítulo 5 aborda os conceitos associados à interoperabilidade organizacional, que busca superar os obstáculos organizacionais e assegurar a coordenação e o alinhamento dos procedimentos administrativos relevantes ao provimento dos serviços de e-Gov, sobretudo quando esse provimento demanda o envolvimento de duas ou mais agências governamentais.

Capítulo 6 – Conclusão

Ao final da Cartilha Técnica de Interoperabilidade será fornecida uma conclusão do trabalho, além das referências bibliográficas utilizadas no documento e um índice remissivo.

1.2. 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 e-PING 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** e **F- Estudo Futuro**).

1.3. Convenções utilizadas

São poucas as convenções utilizadas neste documento. Além do uso padrão de aspas, itálicos e negritos, merecem destaque as seguintes convenções:

Códigos de Programas: São referenciados através da fonte *Courier New*, tamanho 8 ou 10. Para uma maior ênfase, esses códigos poderão ser inseridos em caixas de texto, conforme o modelo descrito abaixo.

```
<?xml version="1.0" encoding="UTF-8"?>
<description xmlns="http://www.w3.org/ns/wsdl"
  xmlns:tns="http://www.tmsws.com/wsdl20sample"
  targetNamespace="http://www.tmsws.com/wsdl20sample">
  . . .
```

Destques: Destaque a pontos que se relacionam dentro de um contexto específico são formatados conforme o exemplo a seguir:

↪ UCS-2 é considerado um padrão obsoleto, apenas suportado em sistemas legados.

Recomendações: As recomendações técnicas que devem ser consideradas quando da aplicação do padrão da e-PING são identificadas de acordo com exemplo abaixo:

☑ Regra Geral - a identificação da pessoa é formada por PRENOME.SOBRENOME

2. FUNDAMENTOS DE INTEROPERABILIDADE

2.1. Introdução

O texto da e-PING aborda, inicialmente, a importância da TIC no contexto governamental, fornecendo as justificativas para se investir em políticas direcionadas à interoperabilidade governamental. Diz o seguinte:

*“A base para o fornecimento de melhores serviços, adequados às necessidades dos cidadãos e dos negócios, a custos mais baixos, é a existência de uma infraestrutura de Tecnologia da Informação e Comunicação (TIC) que se preste como alicerce para a criação desses serviços. Um governo moderno, integrado e eficiente, exige sistemas igualmente modernos, integrados e interoperáveis, trabalhando de forma íntegra, segura e coerente em todo o setor público. Nesse contexto, a interoperabilidade de tecnologia, processos, informação e dados é condição vital para o provimento de serviços de qualidade, tornando-se premissa para governos em todo o mundo, como fundamento para os conceitos de governo eletrônico, o e-gov. **A interoperabilidade permite racionalizar investimentos em TIC, por meio do compartilhamento, reuso e intercâmbio de recursos tecnológicos.**” (E-PING, 2011)*

A e-PING surge como o 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 preocupação com interoperabilidade no governo brasileiro, que resultou na concepção da e-PING, teve início com uma visita ao Reino Unido por um comitê do Governo Brasileiro em junho de 2003, com o propósito de conhecer a e-GIF (*eGovernment Interoperability Framework*), a arquitetura de interoperabilidade desenvolvida pelo Governo Britânico a partir de 2000. Em novembro daquele mesmo ano foi criado o grupo de coordenação da e-PING, e em seguida os grupos de trabalho formados por profissionais de vários órgãos governamentais.

A e-PING 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. Este último tem dois subgrupos importantes, o de geo-informações e o de processos. Com seis anos de existência, a e-PING está em sua quarta versão e vem colhendo resultados positivos no sentido de promover a padronização

tecnológica no governo, garantir a melhoria contínua dos serviços de TIC dos órgãos públicos e disseminar a importância da interoperabilidade entre os sistemas que apoiam as políticas públicas do País.

Entretanto, sendo a e-PING 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, e considerando-se os bons resultados obtidos desde a sua primeira versão, além de outros oriundos de iniciativas de modernização e otimização dos recursos tecnológicos do Governo, tornou-se necessário consolidar e aperfeiçoar as ferramentas de apoio à e-PING 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 e-PING. 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

William Arms, Professor de Ciência da Computação da Universidade de Cornell, foi um dos primeiros a classificar formalmente os níveis de Interoperabilidade (TRIPATHI, GUPTA e BHATTACHARYA, 2008). No memorando *Thoughts about Interoperability in the NSDL*, ele discorre sobre três dimensões da interoperabilidade: técnica, de conteúdo e organizacional (ARMS, 2000). Segundo Arms (2000), somente a compreensão dessas três dimensões leva a uma melhoria da interoperabilidade nas organizações.

Recentemente, a Comissão Europeia definiu o termo “Ecosistema de Interoperabilidade” que abrange cinco aspectos básicos que os governos têm que se preocupar para promoverem a tão desejada interoperabilidade governamental. São eles: (i) interoperabilidade técnica; (ii) interoperabilidade organizacional; (iii) interoperabilidade legal e de políticas públicas; (iv) interoperabilidade semântica e (v) a avaliação dos impactos político, cultural, social e econômico envolvidos com a interoperabilidade governamental (BAIRD, 2007).

No que diz respeito aos objetivos definidos para a primeira versão do Guia de Interoperabilidade de Governo, foram discutidos apenas os aspectos da interoperabilidade técnica, semântica e organizacional. Os demais aspectos serão temas de versões futuras do documento, como consequência do processo natural de maturidade da prática da interoperabilidade nos órgãos públicos. A Figura 1 ilustra as três dimensões da interoperabilidade tratadas no Guia de Interoperabilidade de Governo.



Figura 1: Dimensões da Interoperabilidade
Fonte: (VIDIGAL, 2011)

A **Interoperabilidade Técnica** cobre as questões técnicas associadas à construção de sistemas computacionais interoperáveis. Isso inclui preocupações com arquiteturas de software, uso de padrões e tecnologias para o projeto e desenvolvimento de sistemas, além do uso correto dos meios de comunicação de dados (redes de computadores).

A **Interoperabilidade Semântica** trata do significado da informação que se deseja transmitir ou utilizar. Assim, questões relacionadas à integridade, representação, formatação, interpretação e segurança dos dados são abordadas pela interoperabilidade semântica.

Por fim, a **Interoperabilidade Organizacional** ocupa-se dos processos de trabalho das organizações públicas, o que envolve o uso otimizado dos recursos materiais e humanos, além da definição de políticas adequadas para a promoção da cooperação e da coordenação dos serviços de governo.

Como forma de controle e monitoramento da interoperabilidade no governo, propõe-se também a implementação de técnicas de **Governança**, que implicam na aplicação de direcionamentos

estratégicos, geralmente levada a efeito através de comitês técnicos e de gestão, com o objetivo de garantir a melhoria contínua das políticas de interoperabilidade adotadas pelo governo.

2.3. Interoperabilidade e Conformidade

O termo “conformidade” está associado à idéia 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 e-PING é condição *sine qua non* para se desenvolver as políticas de e-Gov.

Logo, segundo a visão de conformidade da e-PING, os padrões tecnológicos a serem aplicados no governo passam por cinco níveis, a saber: Adotado (A), Recomendado (R), Em Transição (T), Em Estudo (E) e Estudo Futuro (F). A Figura 2 ilustra o ciclo de transição dos níveis de conformidade dos padrões referenciados na e-PING.

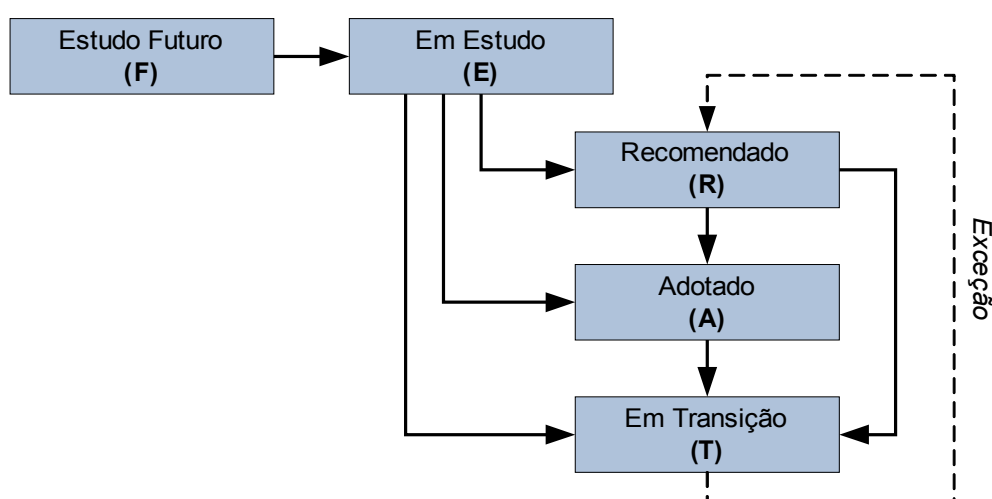


Figura 2: Ciclo dos níveis de conformidade da e-PING

Um padrão identificado como **Adotado (A)** na e-PING 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 e-PING. 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 e-PING, 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 e-PING.

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 e-PING, 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 e-PING recomenda enfaticamente evitar-se o uso dos padrões Em Transição (T).

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

Por fim, os padrões **Estudo Futuro (F)** representam componentes que ainda não foram avaliados, mas que já se tem conhecimento da sua utilização ou do seu interesse de utilização por parte das instituições governamentais.

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 e-PING.

3. INTEROPERABILIDADE TÉCNICA

3.1. Interoperabilidade Técnica na e-PING

A Interoperabilidade Técnica é uma das dimensões cujo entendimento é essencial ao desenvolvimento dos objetivos da e-PING, entre eles o de garantir que a informação produzida no âmbito do Governo Eletrônico possa ser fácil e rapidamente localizada e intercambiada entre os agentes da sociedade interessados nela. Essa dimensão da interoperabilidade cobre as questões técnicas associadas à construção de sistemas computacionais interoperáveis, incluindo preocupações com arquiteturas de software, uso de padrões e tecnologias para o projeto e desenvolvimento de sistemas, além do uso adequado dos meios de comunicação de dados, como redes de computadores e infovias para multimídia.

No contexto da e-PING, a interoperabilidade técnica pode ser considerada como estando presente em todos os seus cinco segmentos. Entretanto, como forma de reforçar a existência e aplicação prática das três dimensões de interoperabilidade, a Cartilha Técnica reserva o segmento de *Organização e Intercâmbio de Informações* para o contexto de aplicação da interoperabilidade semântica. Assim, a interoperabilidade técnica, considerada neste documento, abrange os segmentos de *Interconexão*, *Segurança*, *Meios de Acesso* e *Áreas de Integração para Governo Eletrônico* da e-PING.

O segmento de *Interconexão* estabelece as condições de interoperação entre o governo e a sociedade, definindo as especificações para mensageria, infraestrutura e serviços de rede. O segmento de *Segurança* trata dos aspectos de segurança de TIC que o Governo Federal deve considerar, o que engloba especificações para comunicação de dados, correio eletrônico, criptografia, serviços de rede, redes sem fio, e outros.

A Tabela 1 descreve a interoperabilidade técnica 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 e-PING onde se podem localizar os padrões citados.

Tabela 1: Interoperabilidade Técnica na e-PING

Segmentos da e-PING	Componentes da e-PING	Referência na e-PING
1 – Interconexão	Transporte de mensagem eletrônica	Tabela 1 – Especificações para Interconexão (Mensageria)
	Acesso à caixa postal	
	Mensageria em Tempo Real	
	Transporte	Tabela 2 – Especificações para Interconexão (Infraestrutura de Rede)
	Intercomunicação LAN/WAN	
	Tráfego avançado	
	Rede local sem fio	Tabela 3 – Especificações para Interconexão (Serviços de Rede)
	Protocolo de transferência de hipertexto	
	Protocolos de transferência de arquivos	
	Diretório	
	Sincronismo de tempo	
	Protocolos de sinalização	
	Protocolos de gerenciamento de rede	
	Protocolo de troca de informação estruturada em plataforma descentralizada e/ou distribuída	
2 – Segurança	Transferência de dados em redes inseguras pelos protocolos HTTP, LDAP, IMAP, POP3, Telnet	Tabela 4 – Especificações para Segurança (Comunicação de dados)
	Segurança de redes IPv4	
	Segurança de redes Ipv4 para protocolos de aplicação	
	Segurança de redes IPv6	
	Acesso a caixas postais	Tabela 5 – Especificações para Segurança (Correio Eletrônico)
	Conteúdo de e-mail	
	Transporte de e-mail	
	Assinatura	Tabela 6 – Especificações para Segurança (Criptografia)
	Algoritmo de cifração	
	Algoritmo para assinatura/hasing	
	Algoritmo para transporte de chave criptográfica de conteúdo/sessão	
	Algoritmos criptográficos baseados em curvas elípticas	
	Requisitos de segurança para módulos criptográficos	Tabela 7 – Especificações para Segurança (Desenvolvimento de Sistemas)
	Assinaturas e cifração XML	
	Principais gerenciamentos XML quando um ambiente PKI é utilizado	
	Autenticação e autorização de acesso XML	
	Intermediação ou Federação de Identidades	
	Navegadores	Tabela 8 – Especificações para Segurança (Serviços de Rede)
	Diretório	
	DNSSEC	
Transferência de arquivos de forma segura		

	Carimbo de tempo	
	LAN sem fio 802.11	Tabela 9 – Especificações para Segurança (Redes Sem Fio)
	Preservação de registros	Tabela 10 – Especificações para Segurança (Resposta a Incidentes de Segurança da Informação)
	Tratamento e resposta a incidentes em redes computacionais	
	Informática Forense	
4 – Meios de Acesso	Todos os componentes	Tabela 12 – Especificações para Meios de Acesso (Mobilidade)
	Transmissão	Tabela 13 – Especificações para Meios de Acesso (TV Digital)
	Codificação	
	Multiplexação	
	Receptores	
	Segurança	
	<i>Middleware</i>	
	Canal de Interatividade	
Guia de Operações		
5 – Áreas de Integração para Governo Eletrônico	Linguagem para Execução de Processos	Tabela 15 – Especificações para Áreas de Integração para Governo Eletrônico (Temas Transversais)
	Interoperabilidade entre sistemas de informação geográfica	
	Linguagem de definição do serviço	
	Infraestrutura de registro	Tabela 16 – Especificações para Áreas de Integração para Governo Eletrônico (<i>Web Services</i>)

3.2. Interoperabilidade Técnica e a Interconexão

Conforme descrito na Tabela 1, a interoperabilidade técnica para o segmento de Interconexão na e-PING é aqui considerada através de treze componentes, para os quais são definidas especificações para interconexão subdivididas em três grandes grupos: (i) Mensageria, (ii) Infraestrutura de Rede, e (iii) Serviços de Rede.

3.2.1. Especificações para Interconexão (Mensageria)

Os componentes especificados na e-PING para o segmento de Interconexão que tratam de Mensageria são apresentados na Tabela 2.

Tabela 2: Componentes do Segmento de Interconexão (Mensageria)

Componente	Especificação	Situação
Transporte de mensagem eletrônica	Produtos que suportem interfaces em conformidade com SMTP/MIME	A
Acesso à caixa postal	IMAP para acesso remoto à caixa postal	A
Mensageria em Tempo Real	Programas de correio eletrônico em conformidade com XMPP	R

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 e-PING 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 e-PING fomentar serviços governamentais prestados ao cidadão utilizando essa tecnologia, hoje amplamente suportada pelo mercado, e acessível à grande maioria da população.

3.2.2. Especificações para Interconexão (Infraestrutura de Rede)

Os componentes especificados na e-PING para o segmento de Interconexão que tratam de Infraestrutura de Rede são apresentados na Tabela 3.

Tabela 3: Componentes do Segmento de Interconexão (Infraestrutura de Rede)

Componente	Especificação	Situação
Transporte	TCP e UDP	A
Intercomunicação LAN/WAN	IPv4	A
Tráfego avançado	MPLS (pelo menos quatro classes de serviço)	A
Rede local sem fio	IEEE 802.11 g	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 diz respeito à estrutura de endereçamento utilizada: endereços de 32 bits no caso do IPv4, e de 128 bits no caso do IPv6. A e-PING preconiza o uso de TCP, UDP e IPv4, para os serviços de transporte e intercomunicação entre LANs (*Local Area Networks*) e WANs (*Wide Area Networks*), enquanto categoriza o IPv6 como em estudo.

No caso de redes de telecomunicação onde se necessita de alto desempenho, a e-PING 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 e-PING 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*.

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.

A utilização da tecnologia IEEE 802.11g deve 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. Vale ressaltar também que no final de 2009 o IEEE promulgou uma nova versão desse padrão chamado de IEEE 802.11n, que entre outros avanços, possibilita o aumento significativo da largura de banda utilizável através da tecnologia MIMO (*Multiple-Input, Multiple-Output*). A e-PING já sinalizou esse novo padrão para redes sem fio como objeto de estudo futuro.

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

3.2.3. Especificações para Interconexão (Serviços de Rede)

Os componentes especificados na e-PING para o segmento de Interconexão que tratam de Serviços de Rede são apresentados na Tabela 4.

Tabela 4: Componentes do Segmento de Interconexão (Serviços de Rede)

Componente	Especificação	Situação
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1	A
Protocolos de transferência de arquivos	FTP (com reinicialização e recuperação) e HTTP	R
Diretório	LDAP v3	A
Sincronismo de tempo	NTP v3.0 e SNTP v4.0	R
Protocolos de sinalização	SIP	A
Protocolos de gerenciamento de rede	SNMP v3	R
Protocolo de troca de informação estruturada em plataforma descentralizada e/ou distribuída	SOAP v1.2	A

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 e-PING para a transferência de hipertexto.

Para a transferência de arquivos, a e-PING 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 e-PING recomenda o 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 e-PING.

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 e-PING 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 e-PING recomenda a utilização da versão 3 desse protocolo.

O último serviço de rede mencionado na e-PING envolve a troca de informação estruturada em plataforma descentralizada e/ou distribuída. Nesse caso, a e-PING Adota (A) a versão 1.2 do protocolo SOAP (*Simple Object Access Protocol*), definindo-o como o protocolo de preferência na interoperabilidade entre sistemas através do uso de *Web Services*. Dada a importância do assunto, um espaço específico foi dedicado ao SOAP nesta Cartilha Técnica através da subseção 3.6.5.

3.3. Interoperabilidade Técnica e a Segurança

A e-PING 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 e-PING 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 apóiam 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.

A interoperabilidade técnica para o segmento de Segurança na e-PING é considerada através de vinte e seis componentes, para os quais são definidas especificações para segurança subdivididas em sete grandes grupos, apresentados nas Tabelas 5 a 11: (i) Comunicação de dados, (ii) Correio

Eletrônico, (iii) Criptografia, (iv) Desenvolvimento de Sistemas, (v) Serviços de Rede, (vi) Redes Sem Fio, e (vii) Resposta a Incidentes de Segurança da Informação.

3.3.1. Especificações para Segurança (Comunicação de dados)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Comunicação de Dados são apresentados na Tabela 5.

Tabela 5: Componentes do Segmento de Segurança (Comunicação de Dados)

Componente	Especificação	Situação
Transferência de dados em redes inseguras pelos protocolos HTTP, LDAP, IMAP, POP3, Telnet	TLS v1, HTTP sobre TLS, Certificado Digital X.509 v3 ICP-Brasil, SASL	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	Autenticação nativa AH, ou autenticação IP com ESP	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 e-PING 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 e-PING, é sua capacidade de emular o SSL v3, útil em situações que requeiram esse nível de compatibilidade.

Quanto aos certificados digitais, a e-PING 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 e-PING 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 e-PING 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 e-PING 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.

Um exemplo de estrita aderência às recomendações de e-PING quanto à segurança da comunicação de dados pela Internet é o do Portal de Compras do Governo Federal (<https://www.comprasnet.gov.br>). O Comprasnet é um sítio *web* instituído pelo Ministério do Planejamento, Orçamento e Gestão (MP) para disponibilizar à sociedade informações referentes às licitações e contratações promovidas pelo Governo Federal, bem como permitir a realização de processos eletrônicos de aquisição.

O MP, por meio da SLTI (Secretaria de Logística e Tecnologia da Informação) está implementando o projeto de certificação digital no âmbito do Comprasnet, com vista a promover maior segurança nos atos praticados pelos pregoeiros e ordenadores de despesas nas execuções dos pregões Eletrônico, Presencial, Cotação Eletrônica de Preços e outros serviços disponibilizados pelo Comprasnet. Nesse primeiro momento, estão sendo certificados os usuários do Comprasnet no eixo Brasília, Rio de Janeiro e São Paulo.

3.3.2. Especificações para Segurança (Correio Eletrônico)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Correio Eletrônico são apresentados na Tabela 6.

Tabela 6: Componentes do Segmento de Segurança (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	R
Assinatura	Padrão ICP-Brasil	A

A e-PING 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. Esse protocolo permite a criação de um canal seguro na Internet pela combinação dos protocolos HTTP e SSL/TLS, esse último descrito na seção 3.3.1.

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 e-PING 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 e-PING determina a utilização de certificados digitais no padrão X.509 v3, emitidos para esse fim por entidades pertencentes à rede certificadora ICP-Brasil.

3.3.3. Especificações para Segurança (Criptografia)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Criptografia são apresentados na Tabela 7.

Tabela 7: Componente do Segmento de Segurança (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

A confiabilidade de um procedimento de cifração depende da qualidade e robustez do algoritmo utilizado. Para a cifração de conteúdo de qualquer natureza, a e-PING 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 e-PING 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 e-PING determina a

utilização do algoritmo RSA (sigla construída a partir dos sobrenomes de seus inventores, Ronald Rivest, Adi Shamir e Leonard Adleman) 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 e-PING 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 e-PING 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).

3.3.4. Especificações para Segurança (Desenvolvimento de Sistemas)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Desenvolvimento de Sistemas são apresentados na Tabela 8.

Tabela 8: Componentes do Segmento de Segurança (Desenvolvimento de Sistemas)

Componente	Especificação	Situação
Assinaturas XML	XMLsig	A
Cifração XML	XMLenc	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 1.3	R
Navegadores	<i>Cookies</i> apenas com a concordância do usuário	A

A e-PING determina que os seguintes padrões de segurança sejam utilizados no desenvolvimento de sistemas, quando houver envolvimento de componentes XML 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 e-PING 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, 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.

3.3.5. Especificações para Segurança (Serviços de Rede)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Serviços de Rede são apresentados na Tabela 9.

Tabela 9: Componentes do Segmento de Segurança (Serviços de Rede)

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

A e-PING recomenda que a segurança de diretórios seja implementada com a extensão para TLS do LDAP v3. Para a transferência segura de arquivos, a e-PING 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 e-PING recomenda 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).

3.3.6. Especificações para Segurança (Redes Sem Fio)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Redes sem Fio são apresentados na Tabela 10.

Tabela 10: Componentes do Segmento de Segurança (Redes Sem Fio)

Componente	Especificação	Situação
LAN sem fio 802.11	WPA2	R

A e-PING 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.

3.3.7. Especificações para Segurança (Resposta a Incidentes de Segurança da Informação)

Os componentes especificados na e-PING para o segmento de Segurança que trata de Resposta a Incidentes de Segurança da Informação são apresentados na Tabela 11.

Tabela 11: Componentes do Segmento de Segurança (Resposta a Incidentes de Segurança da Informação)

Componente	Especificação	Situação
Preservação de registros	<i>Guidelines for Evidence Collection and Archiving</i>	R
Tratamento e resposta a incidentes em redes computacionais	<i>Expectations for Computer Security Incident Response</i> Norma Complementar N°. 05/09	R
Informática Forense	<i>Guide to Integrating Forensic Techniques into Incident Response</i>	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 e-PING 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 forense para a identificação, coleta, exame e análise de dados, mantendo a integridade da informação e a estrita cadeia de custódia desses dados.

3.4. Interoperabilidade Técnica e Meios de Acesso

Conforme descrito na Tabela 1, a interoperabilidade técnica para o segmento de Meios de Acesso na e-PING define especificações para componentes de interconexão, subdivididos em dois grandes grupos: (i) Mobilidade e (ii) TV Digital.

3.4.1. Especificações para Meios de Acesso (Mobilidade)

Os componentes especificados na e-PING para o segmento de Meios de Acesso que trata de Mobilidade são apresentados na tabela 12.

Tabela 12: Componentes do Segmento de Meios de Acesso (Mobilidade)

Componente	Especificação	Situação
Todos os componentes	Devem ser aderentes aos padrões <i>W3C – Mobile Best Practices</i>	R

A e-PING 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 e-PING recomenda a aderência às melhores práticas de implementação da web móvel definidas pelo Consórcio *World Wide Web* (W3C, 2008).

3.4.2. Especificações para Meios de Acesso (TV Digital)

Os componentes especificados na e-PING para o segmento de Meios de Acesso que trata de TV Digital são apresentados na tabela 13.

Tabela 13: Componentes do Segmento de Meios de Acesso (TV Digital)

Componente	Especificação	Situação
Transmissão	Norma ABNT NBR 15601 Parte 1 – Sistema de transmissão	R
Codificação	Norma ABNT NBR 15602 Parte 1 – Codificação de Vídeo Parte 2 – Codificação de Áudio Parte 3 – Sistema de multiplexação de sinais	R
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	R
Receptores	Norma ABNT NBR 15604 Parte 1 – Receptores	R
Segurança	Norma ABNT NBR 15605 Parte 1 – Tópicos de segurança	R

<i>Middleware</i>	<p>Norma ABNT NBR 15606</p> <p>Parte 1 – Codificação de dados</p> <p>Parte 2 – Ginga-NCL para receptores fixos e móveis; Linguagem de aplicação XML para codificação de aplicações</p> <p>Parte 3 – Especificação de transmissão de dados</p> <p>Parte 5 – Ginga-NCL para receptores portáteis; Linguagem de aplicação XML para codificação de aplicações.</p>	R
Canal de Interatividade	<p>Norma ABNT NBR 15607</p> <p>Parte 1 – Protocolos, interfaces físicas e interfaces de software</p>	R
Guia de Operações	<p>Norma ABNT NBR 15608</p> <p>Parte 1 – Sistema de Transmissão – Guia para implementação da ABNT NBR 15601</p> <p>Parte 2 – Codificação de vídeo, áudio e multiplexação – Guia para implementação da ABNT NBR 15602</p> <p>Parte 3 – Multiplexação e serviço de informação (SI); Guia de implementação da ABNT NBR 15603.</p>	R

O SBTVD (Sistema Brasileiro de Televisão Digital), ora em implantação e com cobertura nacional prevista para dezembro de 2014, 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 e-PING recomenda, 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.

Um recomendação da e-PING 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).

3.5. Interoperabilidade Técnica e as Áreas de Integração para Governo Eletrônico

A interoperabilidade técnica para o segmento de Áreas de Integração para Governo Eletrônico na e-PING é considerada através de três componentes apresentados na Tabela 14: (i) Linguagem para Execução de Processos, (ii) Interoperabilidade entre sistemas de informação geográfica, e (iii) Linguagem de definição do serviço. A Linguagem de definição de serviço será abordada em seção específica neste documento (seção 3.6) devido à grande importância do tema.

Tabela 14: Componentes do Segmento de Áreas de Integração para Governo Eletrônico

Componente	Especificação	Situação
Linguagem para Execução de Processos	BPEL4WS v1.1	R
Interoperabilidade entre sistemas de informação geográfica	WMS, WFS, WCS, CSW, WFS-T, WKT	A R
Linguagem de definição do serviço	WSDL 1.1	A

3.5.1. 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. 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, e utilizando-se XML (*Extensible Markup Language*). 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 XPD (XML Process Definition Language).

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.

3.6. 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 e-PING 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 e-PING.

3.6.1. 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)*).

O CORBA, cuja primeira versão foi divulgada em 1991, tem como objetivo especificar uma camada de *middleware* para facilitar a construção de sistemas distribuídos. Dessa forma, o padrão CORBA fornece um mecanismo de interoperabilidade entre clientes e servidores distribuídos em ambientes homogêneos e heterogêneos. Seus componentes principais são IDL (*Interface Definition Language*), linguagem declarativa de objetos e independente de linguagem de programação, e ORB (*Object Request Broker*), um conjunto de módulos de softwares que gerenciam a comunicação entre os objetos. Sua função é permitir que os objetos requisitem outros objetos locais ou remotos de forma transparente. Esse padrão ainda pode ser encontrado em sistemas legados, mas é importante lembrar que está caindo em desuso.

O padrão RMI define um mecanismo específico da linguagem Java para requisições entre cliente e servidor. Nesse sentido, é muito semelhante ao CORBA, mas é usado em arquiteturas Java e, por isso, não necessita da IDL. Devido à grande popularidade da linguagem Java, esse padrão pode ser facilmente encontrado em sistemas que fazem uso de comunicação distribuída, principalmente na área de telecomunicações.

O padrão DCOM define um mecanismo para requisitar objetos remotos a partir de *softwares* cliente, construídos em linguagens de programação distintas, mas apenas sob plataformas *Microsoft*. Essa característica de execução apenas em plataforma proprietária pode restringir o seu uso, embora tal padrão ainda possa ser encontrado em algumas aplicações legadas.

O *Servlets/JSP* é uma tecnologia que estende recursos de servidores através de programas escritos em Java e que são executados em servidor *Web*. Tais programas podem ser acionados por clientes que se comunicam através de protocolos da Internet, como o HTTP e HTTPS. Esse padrão tem sido amplamente utilizado devido à popularização da linguagem Java e das tecnologias para Internet.

Os padrões citados anteriormente 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) 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.

As primeiras publicações acerca da SOA surgiram em 1996 pelo Gartner Group. Entretanto, a difusão da SOA na comunidade de software iniciou-se com o advento dos *Web Services* em 2000, pois as melhores práticas da SOA ajudaram a tornar as iniciativas de *Web Services* em casos de sucesso (JOSUTTIS, 2007).

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).

3.6.2. 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.

Existem diversas definições acerca do termo “Serviço”. Josuttis (2007) define serviço como sendo uma representação da TI acerca de uma funcionalidade de negócio. Para o OASIS (*Organization for the Advancement of Structured Information Standards*), serviço é um mecanismo de acesso a uma ou mais capacidades tecnológicas, cuja utilização é provida através de interfaces bem definidas e em consonância com restrições e políticas de uso descritas na declaração do serviço (OASIS, 2006). Sob o ponto de vista técnico, serviço pode ser considerado como um componente reusável de TI que possui uma interface a qual divide o que é acessível externamente e o que está encapsulado e, por isso, restrito ao mundo exterior (implementação técnica) (NEWCOMER e LOMOW, 2005). Outra definição para serviço é que ele representa uma ou mais funcionalidades de negócio e que possui interfaces que permitem a publicação, descoberta e invocação por parceiros de negócio ou pela própria organização.

Assim, 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. Vale salientar também que a utilização do serviço é estabelecida por políticas de uso que definem os direitos do consumidor e também os deveres do provedor do serviço, na forma de um contrato eletrônico formal e bem elaborado.

3.6.3. Modelo de Referência SOA - OASIS

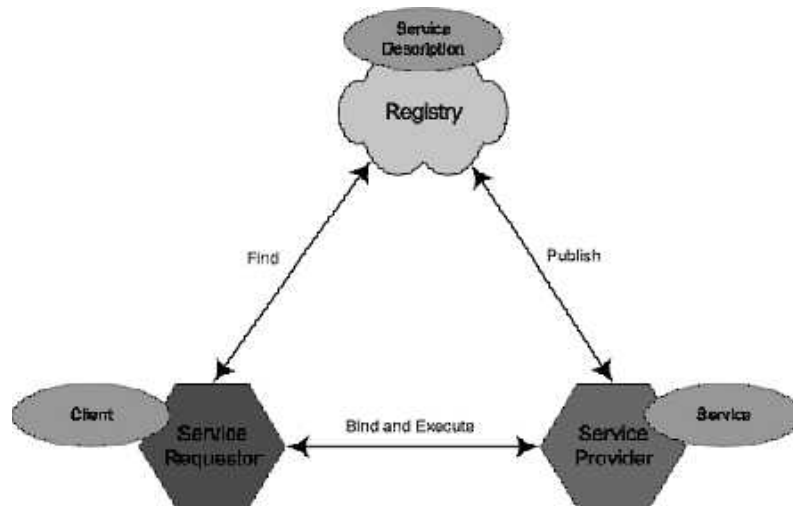
Um modelo de referência é um *framework* abstrato, constituído de conceitos, axiomas e relacionamentos entre as entidades que compõem determinado domínio de aplicação. Além disso, é independente de padrões específicos, tecnologias e implementações.

O Modelo de Referência para SOA do OASIS é um *framework* abstrato para a compreensão de entidades e seus relacionamentos no ambiente orientado a serviços, bem como para o desenvolvimento de padrões e especificações que suportem esse ambiente. Vale ressaltar que o

conceito de orientação de serviços é tratado no âmbito da arquitetura de software e, como modelo de referência, não está vinculado a tecnologias ou implementações específicas para SOA.

Assim, o Modelo de Referência para SOA do OASIS define a essência da arquitetura orientada a serviço e propõe um vocabulário comum e aceito pela comunidade de TI. Um exemplo simplificado dos principais componentes e relacionamentos que compõem esse modelo é descrito na Figura 3.

Figura 3: Modelo Conceitual da SOA (MCGOVERN, SIMS, *et al.*, 2006)



Os papéis representados no modelo são identificados e definidos como:

- *Provedor de Serviços*: organização que efetivamente provê o serviço, ou seja, aquele que dispõe de um ambiente tecnológico para colocar o serviço em funcionamento e acessível aos usuários finais.
- *Consumidor*: organização ou cidadão que utiliza um serviço disponibilizado por um provedor de serviço, ou seja, o usuário final do serviço. É importante salientar que o consumidor também pode ser um outro sistema ou serviço.
- *Registro*: localização central dos serviços fornecidos pelos provedores de serviço, contendo informações diversas acerca da descrição dos serviços tais como: características técnicas, objetivo, contatos da organização provedora, dentro outras. Vale ressaltar que, adicionalmente, o registro pode se tornar também um repositório, visto que arquivos diversos relacionados aos serviços podem ser fisicamente armazenados, por exemplo: especificações técnicas, regras de negócio, modelos de dados, entre outros documentos.

3.6.4. Opção por *Web Services*

Web Services são tipicamente APIs (*Application Programming Interfaces*) 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, e (ii) *Web Services* em conformidade com a arquitetura REST (*Representational State Transfer*).

A e-PING recomenda a utilização de *Web Services* que usam mensagens XML seguindo o padrão SOAP. 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.

Ao longo dos últimos anos, os fornecedores de tecnologia de TIC vêm trabalhando no sentido de definir um conjunto amplo de especificações, conjunto esse que, quando concluído, proverá uma infraestrutura completa para interoperabilidade de alta qualidade através de *Web Services*. Os nomes dessas especificações começam geralmente com o prefixo “WS-”, o que faz com que esse grupo de especificações seja referido como “WS*” (em português, costuma ser pronunciado como “WS-asterisco”; em inglês, como “*WS-splat*”). Os WS* constituem uma plataforma de interoperabilidade vasta e singular, entretanto sua investigação detalhada foge ao escopo deste documento.

Aqui convém uma reflexão de como o advento da linguagem XML foi um passo fundamental na simplificação do processo de integração entre aplicativos de TIC. O XML possibilitou aos desenvolvedores a separação clara entre o conteúdo e estrutura dos dados a serem publicados na *Web* e a forma como esses dados serão vistos. Uma linguagem como o HTML (*HyperText Markup Language*), com atributos de marcação predefinidos, viabiliza uma maneira de se descrever a informação apenas para uma classe específica de documentos. O XML, por outro lado, permite que quaisquer grupos de interessados em interoperabilidade definam suas próprias linguagens de *mark-up* para diferentes classes de documentos.

A possibilidade da definição de linguagens específicas para a troca de informações entre domínios de negócio (tecnicamente falando, implementações específicas do XML) facilita grandemente o compartilhamento de dados, não apenas entre seres humanos utilizando a Internet através de navegadores, mas também entre computadores comunicando-se através de protocolos padronizados. Hoje o XML já é de fato o padrão mundial para a troca de informações pela *Web*, e

por ser um formato público, não-proprietário e gratuito, pode ser livremente utilizado para o desenvolvimento de padrões de interoperabilidade em qualquer domínio de aplicação.

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.

A modularidade e flexibilidade dos *Web Services* fazem deles o mecanismo ideal para a implementação da interoperabilidade entre aplicativos. *Web Services* podem ser utilizados na montagem de soluções com um esforço mínimo de programação, podendo abranger funcionalidades que vão desde solicitações simples (como por exemplo, cotações de câmbio, previsão do tempo, programação de teatro ou cinema) até sistemas complexos que solicitam e processam informações de múltiplas naturezas e múltiplas fontes. Uma vez criados e publicados, outros aplicativos podem descobri-los e invocá-los através de mecanismos padronizados.

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.

3.6.5. 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.

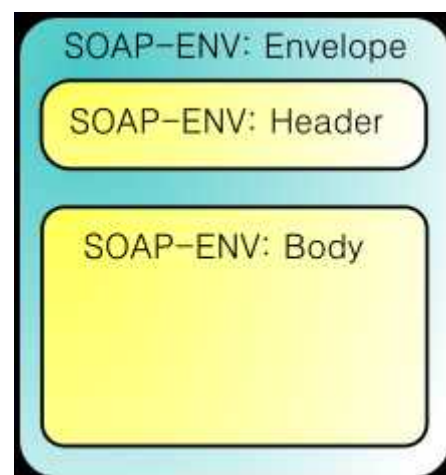


Figura 4: Estrutura do SOAP
(Fonte: Wikipedia)

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. SOAP foi submetido como Nota Técnica ao W3C (*World Wide Web Consortium*), órgão gestor e normatizador da *Web*, em 2000 por um

grupo formado pelas empresas IBM, *Microsoft*, *UserLand* e *DevelopMentor*. 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 5 e 6 apresentam, respectivamente, um exemplo de uma 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 5: 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 6: Exemplo de uma resposta SOAP (Fonte: W3Schools)

3.6.6. 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 15 ilustra como os verbos e métodos HTTP são usados na implementação de um *RESTful Web Service*:

Tabela 15: *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 <i>MIME type</i> 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

3.6.7. 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.

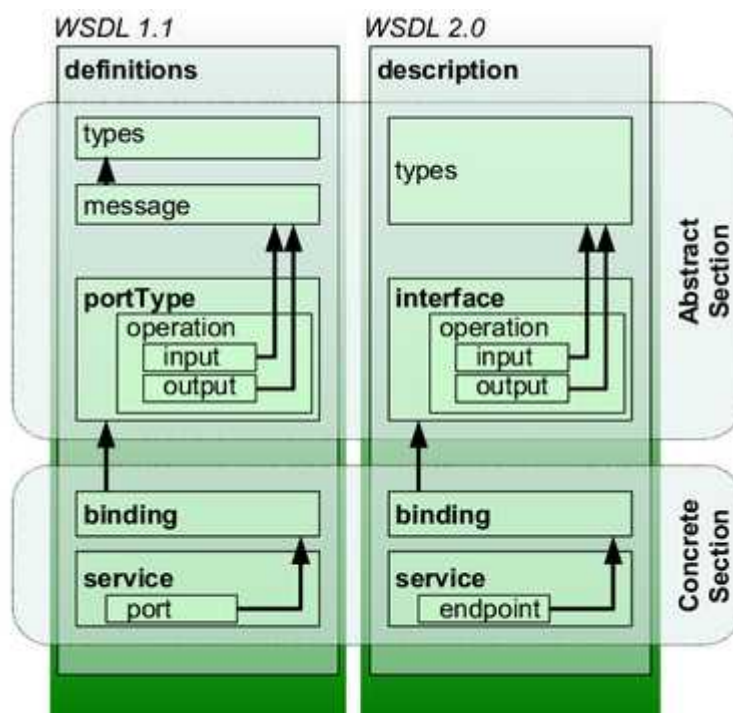


Figura 7: Conceitos definidos nas WSDL 1.0 e 2.0 (Fonte: Wikipedia)

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*.

A primeira versão do WSDL foi desenvolvida por um consórcio formado pelas empresas IBM, *Microsoft* e *Ariba*, e apresentada em setembro de 2000 como parte do ferramental SOAP e como linguagem para a descrição dos então emergentes *Web Services*. 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. A Figura 8 apresenta um exemplo da utilização do WSDL na descrição de um *Web Service* do governo brasileiro.

```

<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:tns="http://www.siorg.redegoverno.gov.br"
xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
targetNamespace="http://www.siorg.redegoverno.gov.br" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:types>
    <s:schema elementFormDefault="qualified" target Namespace="http://www.siorg.redegoverno.gov.br">
      <s:element name="ConsultaOrgao">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="pOrgao" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="ConsultaOrgaoResponse">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="ConsultaOrgaoResult" type="tns:DadosOrgao"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:complexType name="DadosOrgao">
        <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="co_erro" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="tx_mensagem_erro" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="co_orgao" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="Co_Orgao_Pai" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="co_tipo_orgao" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="co_nat_juridica" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="sg_classe" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="co_orgao_topo" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="co_orgao_antecessor" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="tx_estrutura_orgao" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="in_organizacao" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="no_orgao" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="no_orgao_reduzido" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="sg_orgao" type="s:string" />
        </s:sequence>
      </s:complexType>
      <s:complexType name="ParamSaida_Consulta">
        <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="pa_codigo" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="pa_nome" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="pa_cod_status" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="pa_desc_status" type="s:string" />
        </s:sequence>
      </s:complexType>
      <s:element name="DadosOrgao" type="tns:DadosOrgao" />
      <s:element name="ParamSaida_Consulta" type="tns:ParamSaida_Consulta" />
    </s:schema>
  </wsdl:types>
  <wsdl:message name="ConsultaOrgaoSoapIn">
    <wsdl:part name="parameters" element="tns:ConsultaOrgao" />
  </wsdl:message>
  <wsdl:message name="ConsultaOrgaoSoapOut">
    <wsdl:part name="parameters" element="tns:ConsultaOrgaoResponse" />
  </wsdl:message>
  <wsdl:message name="ConsultaOrgaoHttpGetIn">
    <wsdl:part name="pOrgao" type="s:string" />
  </wsdl:message>
  <wsdl:message name="ConsultaOrgaoHttpGetOut">
    <wsdl:part name="Body" element="tns:DadosOrgao" />
  </wsdl:message>
  <wsdl:message name="ConsultaOrgaoHttpPostIn">
    <wsdl:part name="pOrgao" type="s:string" />
  </wsdl:message>
  <wsdl:message name="ConsultaOrgaoHttpPostOut">
    <wsdl:part name="Body" element="tns:DadosOrgao" />
  </wsdl:message>
  <wsdl:portType name="WebServiceSiorgSoap">
    <wsdl:operation name="ConsultaOrgao">
      <wsdl:input message="tns:ConsultaOrgaoSoapIn" />
      <wsdl:output message="tns:ConsultaOrgaoSoapOut" />
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:portType name="WebServiceSiorgHttpGet">
    <wsdl:operation name="ConsultaOrgao">

```

```

    <wsdl:input message="tns:ConsultaOrgaoHttpGetIn" />
    <wsdl:output message="tns:ConsultaOrgaoHttpGetOut" />
  </wsdl:operation>
</wsdl:portType>
<wsdl:portType name="WebServiceSiorgHttpPost">
  <wsdl:operation name="ConsultaOrgao">
    <wsdl:input message="tns:ConsultaOrgaoHttpPostIn" />
    <wsdl:output message="tns:ConsultaOrgaoHttpPostOut" />
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="WebServiceSiorgSoap" type="tns:WebServiceSiorgSoap">
  <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
  <wsdl:operation name="ConsultaOrgao">
    <soap:operation soapAction="http://www.siorg.redegoverno.gov.br/ConsultaOrgao"
style="document"/>
    <wsdl:input>
      <soap:body use="literal" />
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal" />
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:binding name="WebServiceSiorgSoap12" type="tns:WebServiceSiorgSoap">
  <soap12:binding transport="http://schemas.xmlsoap.org/soap/http" />
  <wsdl:operation name="ConsultaOrgao">
    <soap12:operation soapAction="http://www.siorg.redegoverno.gov.br/ConsultaOrgao"
style="document" />
    <wsdl:input>
      <soap12:body use="literal" />
    </wsdl:input>
    <wsdl:output>
      <soap12:body use="literal" />
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:binding name="WebServiceSiorgHttpGet" type="tns:WebServiceSiorgHttpGet">
  <http:binding verb="GET" />
  <wsdl:operation name="ConsultaOrgao">
    <http:operation location="/ConsultaOrgao" />
    <wsdl:input>
      <http:urlEncoded />
    </wsdl:input>
    <wsdl:output>
      <mime:mimeXml part="Body" />
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:binding name="WebServiceSiorgHttpPost" type="tns:WebServiceSiorgHttpPost">
  <http:binding verb="POST" />
  <wsdl:operation name="ConsultaOrgao">
    <http:operation location="/ConsultaOrgao" />
    <wsdl:input>
      <mime:content type="application/x-www-form-urlencoded" />
    </wsdl:input>
    <wsdl:output>
      <mime:mimeXml part="Body" />
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:service name="WebServiceSiorg">
  <wsdl:port name="WebServiceSiorgSoap" binding="tns:WebServiceSiorgSoap">
    <soap:address location="http://www.siorg.redegoverno.gov.br/gestao/webservice/WSSiorg.asmx"/>
  </wsdl:port>
  <wsdl:port name="WebServiceSiorgSoap12" binding="tns:WebServiceSiorgSoap12">
    <soap12:address location="http://www.siorg.redegoverno.gov.br/gestao/webservice/WSSiorg.asmx"/>
  </wsdl:port>
  <wsdl:port name="WebServiceSiorgHttpGet" binding="tns:WebServiceSiorgHttpGet">
    <http:address location="http://www.siorg.redegoverno.gov.br/gestao/webservice/ WSSiorg.asmx"/>
  </wsdl:port>
  <wsdl:port name="WebServiceSiorgHttpPost" binding="tns:WebServiceSiorgHttpPost">
    <http:address location="http://www.siorg.redegoverno.gov.br/gestao/webservice/WSSiorg.asmx"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

Figura 8: Descrição de um *Web Service* com WSDL 2.0

3.6.8. Utilização de um *Web Service*

Em resumo, os passos envolvidos na criação e utilização de um *Web Service* são os seguintes:

1. O provedor do serviço cria o serviço e o registra em um repositório de registros (ver seção 5.1.4). Os repositórios de registros mais comuns hoje são os registros UDDI;
2. No caso de *Web Services* aderentes a e-PING, seu provedor deve documentá-lo de maneira clara e completa, segundo modelo específico (ver seção 5.1.1);
3. O solicitante do serviço (a pessoa, empresa, sistema ou entidade que deseja utilizar o serviço) pesquisa no repositório e encontra o *Web Service* desejado;
4. Encontrado o serviço, o solicitante obtém do mesmo repositório uma cópia do documento WSDL correspondente, que explica que protocolos devem ser utilizados, os parâmetros a serem fornecidos, as condições técnicas e legais subjacentes à utilização do serviço e o resultado que deve ser esperado;
5. De posse das informações negociais, legais e técnicas, o solicitante confecciona o programa cliente para interagir com o serviço;
6. O solicitante passa a interagir com o *Web Service* através do programa cliente confeccionado para esse propósito.

3.6.9. *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.

Embora o termo “ESB” tenha sido bastante popularizado nos últimos tempos, as dúvidas quanto às funcionalidades que se deve esperar de uma ferramenta como essa ainda são muito comuns entre os profissionais e gerentes de TI.

Assim, essa Cartilha Técnica apresenta na Tabela 16 uma descrição das principais funcionalidades encontradas em arquiteturas ESB de pequeno, médio e grande porte.

Tabela 16: Funcionalidades do ESB

Funcionalidade	Descrição	Observação
Invocação	Suporte a protocolos síncronos e assíncronos, além do recurso de mapeamento de serviços (<i>locating e binding</i>)	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 provêm 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 provêm 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.

Atualmente as ferramentas de ESB são fornecidas em três configurações básicas: (i) ESB corporativo, (ii) ESB leve (*light-weight*) e (iii) ESB *open-source*. O ESB corporativo, como o próprio nome sugere, é destinado a atender toda a organização e, geralmente, é fornecido pelas grandes empresas de TI. O ESB leve é muito utilizado pelos desenvolvedores de *software* para atender requisitos específicos de interoperabilidade nos projetos que executam. O ESB *open-source* é fornecido sob a égide de um licenciamento de *software* aberto o que garante o seu uso e alteração por parte da equipe especializada de TI.

Como se pode observar, a escolha de um ESB é um processo difícil e delicado, que exige conhecimento aprofundado do tema. Entretanto, como forma de auxiliar os profissionais de TI na escolha mais adequada de uma ferramenta como essa, fornecemos as seguintes recomendações básicas:

1. Quantidade de Serviços: investir em uma estrutura de ESB não faz sentido se a sua organização não dispor de pelo menos 25 serviços em produção. Se sua organização está apenas desenvolvendo uma prova de conceito com alguns poucos serviços a serem publicados, não é recomendado investir na compra ou implantação de uma estrutura de ESB complexa e definitiva.
2. Propósito: o investimento em uma infraestrutura de ESB deve representar não o uso da melhor tecnologia disponível (*technological appealing*), mas sim o uso de uma tecnologia necessária para a organização. Isso é facilmente percebido pelo retorno do investimento na forma de melhor serviço provido ao usuário final das aplicações.

-
3. Infraestrutura: o investimento em ESB envolve a capacidade de se manter uma infraestrutura de TI compatível, o que implica em dizer que o ambiente de produção se torna, naturalmente, mais complexo e, por isso, necessita de pessoal competente para mantê-lo, além de toda uma organização gerencial para direcionar as políticas e acordos de nível de serviços a serem praticados.

4. INTEROPERABILIDADE SEMÂNTICA

4.1. Interoperabilidade Semântica na e-PING

A interoperabilidade entre os sistemas de informação implica em sua habilidade de trocar e utilizar os dados de forma correta e eficiente. A prática da interoperabilidade semântica envolve o uso de técnicas de integração de informações, cujo foco não é somente a entrega da informação pela simples troca de mensagens. Ela abrange também o significado da informação, tanto no contexto do remetente (ou provedor), quanto do destinatário (ou consumidor) da mensagem.

O significado da informação está associado aos metadados e regras de negócio aplicadas aos dados que se deseja receber ou transmitir. Além disso, é importante considerar o uso da informação no contexto das aplicações que realizam transformações nos dados e retransmitem a informação logo em seguida (PAPAZOGLU e RIBBERS, 2006). Assim, segundo Papazoglou e Ribbers (2006), a interoperabilidade semântica levanta questões relacionadas não só à criação, formatação e representação da informação, mas também a como essa informação é interpretada e utilizada pelas diferentes entidades que cooperam entre si.

No contexto da e-PING, a interoperabilidade semântica está presente em quatro dos cinco segmentos da e-PING: (i) Interconexão, (ii) Meios de Acesso, (iii) Organização e Intercâmbio de Informações e (iv) Áreas de Integração para Governo Eletrônico.

O segmento de maior relevância para as questões de interoperabilidade semântica é o de Organização e Intercâmbio de Informações, que recomenda a adoção de padrões para a representação, formatação e interpretação de dados nas instituições do governo. Os demais segmentos relacionam-se com a interoperabilidade semântica, seja porque fornecem mecanismos para representar a informação trocada entre as partes, ou porque ditam regras para nomeação ou descrição de elementos que se deseja padronizar.

A Tabela 17 descreve os segmentos da e-PING associados à interoperabilidade semântica de modo a referenciar os componentes identificados como Adotados (A) e Recomendados (R) pelo governo brasileiro. Essa Tabela também inclui a referência às seções da e-PING onde os padrões citados podem ser facilmente localizados.

Tabela 17: Interoperabilidade Semântica na e-PING

Segmentos da e-PING	Componentes da e-PING	Referência na e-PING
1 – Interconexão	Endereços de caixa postal eletrônica	Tabela 1 – Especificações para Interconexão (Mensageria)
	Serviços de Nomeação de Domínio	Tabela 3 – Especificações para Interconexão (Serviços de Rede)
3 – Meios de Acesso	Conjunto de caracteres e alfabetos no padrão	Tabela 11 – Especificações para Meios de Acesso (Estações de Trabalho)
	Formato de intercâmbio de hipertexto	
	Arquivos do tipo documento	
	Arquivo 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	
	Especificação de padrões de animação	
	Arquivos do tipo áudio e vídeo	
	Compactação de arquivos de uso geral	
	Informações georreferenciadas	
	Todos os componentes	Tabela 12 – Especificações para Meios de Acesso (Mobilidade)
4 – Organização e Intercâmbio de Informações	Linguagem para intercâmbio de dados	Tabela 14 – Especificações para Organização e Intercâmbio de Informações (Mobilidade)
	Transformação de dados	
	Definição dos dados para intercâmbio	
	Descrição de recursos	
	Taxonomia para navegação	
5 – Áreas de Integração para Governo Eletrônico	Legislação, jurisprudência e proposições legislativas	Tabela 15 – Especificações para Áreas de Integração para Governo Eletrônico (Temas Transversais)

4.2. Interoperabilidade Semântica e a Interconexão

No segmento de Interconexão da e-PING, a interoperabilidade semântica é considerada através de dois componentes: (i) Endereços de caixa postal eletrônica e (ii) Serviços de Nomeação de Domínio. Esses componentes são ilustrados na Tabela 18.

Tabela 18: Especificações para o Segmento de Interconexão

Componentes	Especificação	Situação
Endereços de caixa postal eletrônica	Caixas Postais Individuais-Funcionais no Governo Federal	A
Serviços de Nomeação de Domínio (DNS)	Resolução CGI.br N.º 08, 28 de novembro de 2008	A

Embora o segmento de Interconexão seja geralmente associado à Interoperabilidade Técnica, seus dois componentes encontram-se no contexto da Interoperabilidade Semântica, pois ditam padrões para a nomeação de caixa postal eletrônica e serviços de nomeação de domínio.

No primeiro caso, a interoperabilidade semântica está associada à correta nomeação de endereço eletrônico de *e-mail* que deve descrever simultaneamente o detentor da caixa postal e o órgão de governo responsável pela gestão das mensagens. No segundo caso, a interoperabilidade semântica está presente na padronização dos serviços de nomeação de domínio no governo brasileiro. Em ambos os casos, a incorreta aplicação dos padrões pode resultar em extravio de mensagens para destinos desconhecidos, ou a identificação errônea de um serviço fornecido por um órgão ou entidade que pertence à estrutura governamental do país.

Os nomes das caixas postais de correio eletrônico devem seguir os padrões estabelecidos no documento “Caixas Postais Individuais-Funcionais no Governo Federal” (REDE DO GOVERNO, 2010). 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*).

Assim, as regras definidas para nomes das caixas postais de correio eletrônico no Governo Federal são as seguintes:

Regra Geral - a identificação da pessoa é formada por PRENOME.SOBRENOME

Exemplo: joaquim.xavier

Exceções - para evitar duplicidade, pode-se utilizar:

PRENOME.NOMES INTERMEDIÁRIOS.SOBRENOME

Os NOMES INTERMEDIÁRIOS podem ser abreviados ou concatenados com o PRENOME ou com o SOBRENOME através de um hífen.

Exemplos: joaquim.j.xavier@... joaquim.js.xavier@...
 joaquim-jose.xavier@... joaquim.silva-xavier@...
 joaquim-jose.s.xavier@... joaquim.j.silva-xavier@...
 joaquim-jose.da.silva-xavier@...

Restrições

- Não utilizar acentos.

- PRENOME: utilizar no máximo 16 caracteres alfabéticos, maiúsculos ou minúsculos.

-
- SOBRENOME: utilizar no máximo 40 caracteres alfabéticos, maiúsculos ou minúsculos. Quando constar sobrenome qualificador de geração (Júnior, Filho, Neto, etc...), recomenda-se o uso de sobrenome composto, por exemplo: joaquim.j.xavier-filho
 - Se utilizar hífen, não incluir espaços antes ou após o hífen.
 - Se fizer uso de iniciais, utilizar no máximo 3 caracteres alfabéticos, maiúsculos ou minúsculos, com ou sem hífen ou ponto.

- Regra de exibição – para efeitos de exibição do nome do servidor na lista de endereços de caixas postais do órgão de governo, deve-se utilizar o seguinte padrão (campos separados por espaço):
PRENOME NOMES INTERMEDIÁRIOS SOBRENOME – SIGLA DO ÓRGÃO

Exemplo: Joaquim José da Silva Xavier – MP

- Sigla do órgão: deve-se utilizar aquela definida pelo SIORG (Sistema de Informações Organizacionais)

Quanto aos serviços de nomeação de domínio, os padrões são dados pela Resolução N^o. 7, de 29 de julho de 2002 que estabelece as regras e diretrizes para os sítios da Administração Pública na Internet (PRESIDÊNCIA DA REPÚBLICA, 2002).

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).

4.3. Interoperabilidade Semântica e Meios de Acesso

No segmento de Meios de Acesso da e-PING, dois tipos de componentes podem ser associados à interoperabilidade semântica: (i) componentes que tratam do intercâmbio de informações entre as estações de trabalho e (ii) componentes que tratam do intercâmbio de informações em dispositivos móveis.

Assim como ocorre no segmento de Interconexão, os componentes do segmento de Meios de Acesso são normalmente associados à interoperabilidade técnica porque tratam basicamente de formato de arquivos. Entretanto, no contexto da e-PING o segmento de Meios de Acesso tem o objetivo de garantir a disponibilidade e acesso à informação governamental. Por isso, a inclusão desses componentes no contexto da interoperabilidade semântica tem por objetivo garantir o uso de padrões quando da representação e posterior distribuição da informação de governo. Assim, por exemplo, ao se representar uma informação de governo no formato de planilha eletrônica, deve-se optar pelo padrão aberto (*.ods*) em detrimento de outros padrões comercialmente utilizados. Com

isso, aumenta-se a capacidade de distribuição e de interpretação correta dessa informação por todos os órgãos da estrutura governamental do país.

A Tabela 19 arrola os componentes do segmento de Meios de Acesso que se relacionam com a interoperabilidade semântica. As subseções seguintes oferecem mais detalhamentos envolvendo esses elementos. Entretanto, devido à pouca utilização de dispositivos móveis no contexto das políticas públicas, os componentes que tratam o intercâmbio de informações nesses tipos de dispositivos não serão considerados em grande profundidade. Além disso, no contexto da e-PING, todos os padrões citados quanto à interoperabilidade móvel encontram-se em situação Recomendada (R), o que sugere a necessidade de maior maturidade no tema.

Tabela 19: Especificações para o Segmento de Meios de Acesso

Componentes	Especificação	Situação
Conjunto de caracteres e alfabetos	UNICODE, versão 4.0	R
Formato de intercâmbio de hipertexto	HTML, versão 4.01	A
	XHTML, versões 1.0 ou 1.1	R
	XML, versões 1.0 e ou 1.1	A
	SHTML	R
Arquivos do tipo documento	XML, versões 1.0 e ou 1.1	R
	<i>Open Document (.odt)</i>	A
	PDF versão aberta	R
	Texto puro (.txt)	A
Arquivos do tipo planilha	HTML, versão 4.01	R
	<i>Open Document (.ods)</i>	A
Arquivos do tipo apresentação	<i>Open Document (.odp)</i>	A
	HTML (.htm ou .html)	R
Arquivos do tipo “banco de dados” para estações de trabalho	XML, versões 1.0 e 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)	R
	TIFF (.tif)	R
	SVG (.svg)	R
	JPEG File Interchange Format (.jpeg, .jpg ou .jif)	R
Gráficos vetoriais	SVG (.svg)	R
	<i>Open Document (.odg)</i>	R
Especificação de padrões de animação	SVG (.svg)	R
Arquivos do tipo áudio e do tipo vídeo	MIDI (.mid)	R
	Audio Ogg Vorbis I (.ogg)	R
	Theora (.ogv)	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

4.3.1. Codificação dos Dados (*encoding*)

A interoperabilidade semântica nas estações de trabalho envolve, primeiramente, a definição do padrão para a representação e manipulação dos dados de acordo com a língua oficial do país. Neste caso, a e-PING 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.

4.3.2. Formato de Intercâmbio de hipertexto

Outro aspecto relacionado à interoperabilidade semântica nas estações de trabalho envolve a transferência de dados em formato de hipertexto. A e-PING adota como padrão o HTML (versão 4.01) e o XML (versões 1.0 e 1.1). Como padrões recomendados sugerem-se também o XHTML (*Extensible Hypertext Markup Language*) (versões 1.0 e 1.1) e o SHTML (*Server-side HTML*).

O XHTML é considerado por muitos o sucessor do HTML. Esse padrão utiliza-se do recurso de *tags* XML para a formatação de documentos de hipertexto. As diferenças de um arquivo XHTML para um arquivo HTML estão no fato de que as regras para a formação do arquivo XHTML são mais rígidas. Assim, um arquivo XHTML deve:

-
- Possuir todas as *tags* em letras minúsculas.
 - Conter os elementos devidamente aninhados.
 - Manter conformidade rígida com a versão adotada.
 - Prover o correto fechamento das *tags*, inclusive de *tags* vazias.

O padrão SHTML, por sua vez, é um arquivo HTML com a extensão *.shtml*, que possui em seu cabeçalho diretivas de comando para o servidor de aplicações incluir, em tempo de execução, informações adicionais na página. Assim, por exemplo, seria possível utilizar um arquivo SHTML para adicionar automaticamente a data da última atualização da página. Uma implicação do uso desse padrão é a necessidade de se consultar os administradores da infraestrutura para que estes configurem o servidor de aplicações de modo a possibilitar o uso das informações desejadas.

Como recomendações práticas para o uso adequado desses padrões (HTML, XML, XHTML e SHTML) sugerem-se o seguinte:

- Utilizar ferramentas para a verificação da conformidade com as versões sugeridas na e-PING.
- Consultar a e-MAG (Modelo de Acessibilidade de Governo Eletrônico), que define regras para acessibilidade no governo eletrônico.

4.3.3. Intercâmbio de arquivos

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 freqüente dificulta ou impede que a informação seja recebida e decifrada adequadamente.

Nesse contexto, para a troca de arquivos do tipo documento, a e-PING 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 – padrão ISO 19005-1:2005. Arquivos do tipo RTF (*Rich Text Format*) e PDF encontram-se em estado de transição e por isso, o seu uso deve ser restrito.

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

Visando o recebimento de arquivos gerados por sistemas de banco de dados em estações de trabalho, a e-PING 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*) e *Open Document (.odg)*. Na impossibilidade de uso desses padrões a e-PING recomenda o uso dos formatos TIFF (*.tif*), SVG (*.svg*) e JPEG (*.jpeg, .jpg ou .jif*). É importante notar que os formatos BMP (*.bmp*) e GIF (*.gif*) estão em estado de transição e, por isso, o seu uso deve ser evitado.

Para o tratamento de gráficos vetoriais nenhum padrão é definido como Adotado (A) na e-PING. Entretanto, há a recomendação pelo uso do formato SVG (*.svg*). A e-PING também referencia o formato SVG (*.svg*) como Recomendado (R) para a definição de arquivos de animação. Quanto à especificação de padrões de animação, a e-PING recomenda a utilização do formato SVG (*.svg*), e recomenda também que se evite o uso do formato GIF (*.gif*), por se encontrar em estado de transição.

No que tange ao uso de arquivos de áudio e vídeo, a e-PING ainda não define nenhum formato como Adotado (A). No entanto, recomenda o uso dos seguintes padrões: MIDI (*.mid*), Ogg Vorbis - formato aberto para *streaming* de áudio (*.oga*) e *Theora (.ogv)*. Os formatos que devem ser evitados, segundo a e-PING, são: *Audio-Video Interleaved (.avi)* com codificação divX ou Xvid, MPEG-4, *Audio Layer 3 (.mp3)* e WAVE (*.wav*).

Para o intercâmbio de informações georreferenciadas entre as estações de trabalho, 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*), TAR compactado ou não (*.tar, .tgz ou .tar.gz*), BZIP2 (*.bz2*) e TAR compactado com BZIP2 (*.tar.bz2*).

4.4. Interoperabilidade Semântica e a Organização e Intercâmbio de Informações

A visão de interoperabilidade semântica da e-PING associada ao segmento de Organização e Intercâmbio de Informações consiste na definição dos padrões para a criação, formação e transformação dos dados.

Para a criação da informação que será enviada a outro sistema ou unidade de processamento computacional, a e-PING 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.

A e-PING considera também a linguagem UML (*Unified Modeling Language*) como um padrão Adotado (A) para o intercâmbio de informações representadas na forma de modelos. De acordo com a e-PING, a UML pode ser utilizada para “a descrição de dados complexos visando melhor explicitação”.

Por fim, no contexto de classificação das informações por assunto de governo, a e-PING adota o VCGE (Vocabulário Controlado do Governo Eletrônico).

A Tabela 20 relaciona os componentes do segmento de Organização e Intercâmbio de Informações associados à interoperabilidade semântica e as subseções seguintes oferecem mais detalhes envolvendo cada um desses elementos.

Tabela 20: Especificações para o Segmento de Organização e Intercâmbio de Informações

Componentes	Especificação	Situação
Linguagem para intercâmbio de dados	XML	A
	JSON	R
Transformação de dados	XSL	A
Definição dos dados para intercâmbio	XML <i>Schema</i>	A
	UML	A
Descrição de recursos	RDF	R
Taxonomia para navegação	VCGE, versão 1.0	A

4.4.1. 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 recebida. 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 9 ilustra esse uso do XML, considerando duas camadas de uma arquitetura MVC (*Model-View-Controller*).

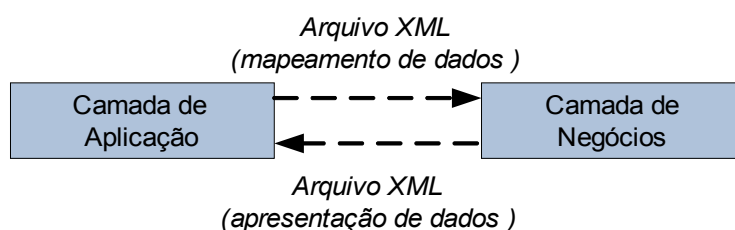


Figura 9: XML utilizado para transportar dados dentro de uma aplicação.

Quando o XML é utilizado para o transporte de informações entre aplicações, a e-PING 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 10 ilustra o processo de transporte de um arquivo XML, considerando o uso da tecnologia de *Web Services*.

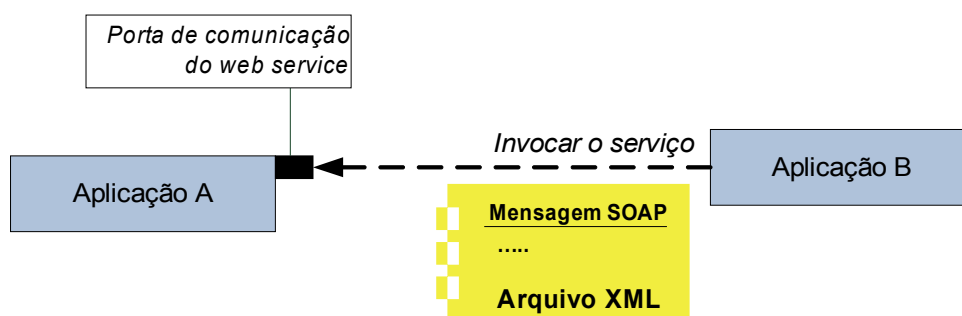


Figura 10: XML utilizado para transportar dados com a tecnologia de *Web Services*.

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 específicas para o tratamento de arquivos no formato XML (DOM,

SAX ou *Data Binding*). A Figura 11 ilustra o processo de utilização de XML como conversor de dados no contexto de uma aplicação.

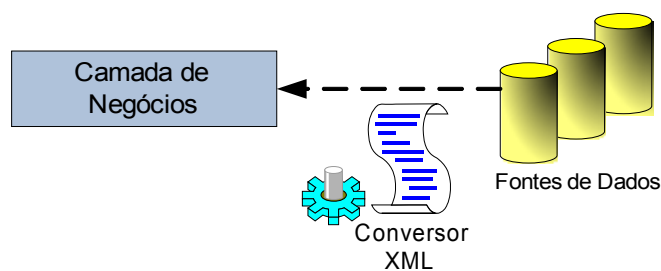


Figura 11: XML utilizado como conversor de dados no contexto de uma aplicação.

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 12 ilustra esse caso de utilização de XML.

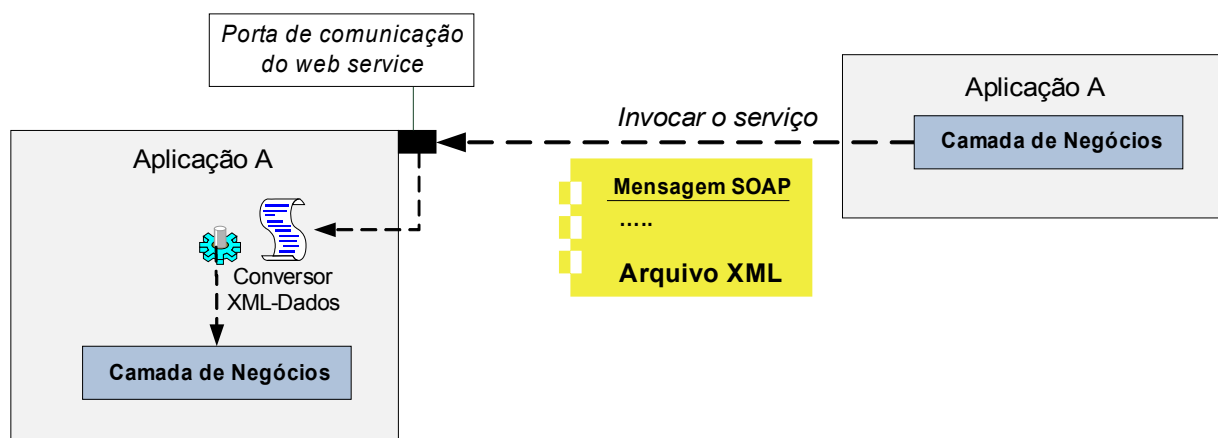


Figura 12: XML utilizado como conversor de dados no contexto de várias aplicações.

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 13 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.

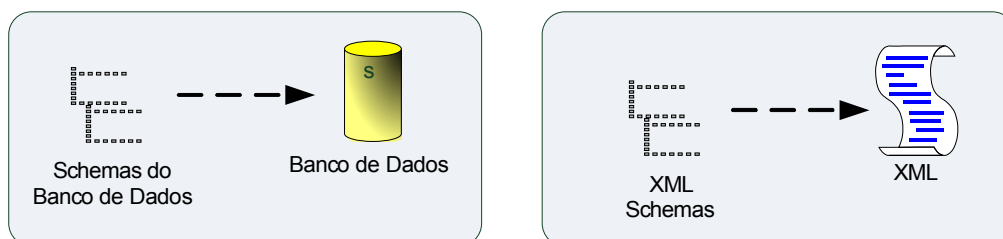


Figura 13: Comparação das tecnologias de Banco de Dados e XML (Modificado de Erl, 2004).

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 conseqüentemente 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 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 idéia 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.

4.4.2. 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 14 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 14: Exemplo de um arquivo JSON

4.4.3. 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 idéia 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. Entretanto, é importante entender que cada um deles 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 15 e 16 apresentam respectivamente um exemplo de documento XML e XSL. A Figura 17 ilustra o resultado final da transformação XSL sobre a informação contida no documento XML.

```

<?xml version="1.0" encoding="iso-8859-1"?>
<!-- Edited by XMLSpy@ -->
<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 15: Exemplo de um documento XML (Fonte: W3Schools)

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- Edited by XMLSpy@ -->
<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 16: 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 17: Resultado final da transformação XSL (Fonte: W3Schools)

4.4.4. 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.

Existem outras abordagens para validação de documentos XML no mercado, além do XML *Schema*. Na verdade, a primeira tecnologia para validação de documentos XML foi o DTD (*Document Type Definition*) também elaborado pelo W3C. No entanto, essa tecnologia tem sido gradativamente substituída pelo XML *Schema* e o seu uso não é aconselhado na atual versão da e-PING, o que implica em dizer que as atuais aplicações devem fazer uso do XML *Schemas*.

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 e-PING.

A Figura 18 apresenta um exemplo de um arquivo *XML Schema* enquanto que a Figura 19 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 18: 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 19: Referencia a um *XML Schema* a partir do XML (Fonte: W3Schools)

4.4.5. 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 21 descreve o conjunto de especificações ou recomendações que compõem toda a estrutura RDF:

Tabela 21: Estrutura do RDF (W3C, 2010)

Especificação	Descrição
RDF: <i>Concepts and Abstract Syntax</i>	Descreve os conceitos básicos do RDF e define uma sintaxe abstrata no qual o padrão é definido.
RDF <i>Semantics</i>	Define precisamente a semântica do RDF.
RDF <i>Primer</i>	Descreve uma linguagem para a representação de informações a respeito de recursos encontrados na <i>Web</i> . Descreve como o RDF pode ser utilizado e como se pode construir um vocabulário baseado neste padrão.
RDF <i>Vocabulary Description Language 1.0: RDF Schema</i>	Define uma linguagem de propósito geral para representar tipos diversos de informações na <i>Web</i> . Permite a definição de recursos da <i>Web</i> através de classes, propriedades e valores.
RDF/XML <i>Syntax Specification</i>	Define a sintaxe XML utilizada para descrever o RDF.
RDF <i>Test Cases</i>	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*. Tim Berners-Lee, fundador e diretor do W3C define a *Web Semântica* como “uma teia intrincada de informações que podem ser processadas direta e indiretamente por máquinas” (W3C, 2010). 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 20 ilustra e define os elementos básicos que compõem a especificação RDF.

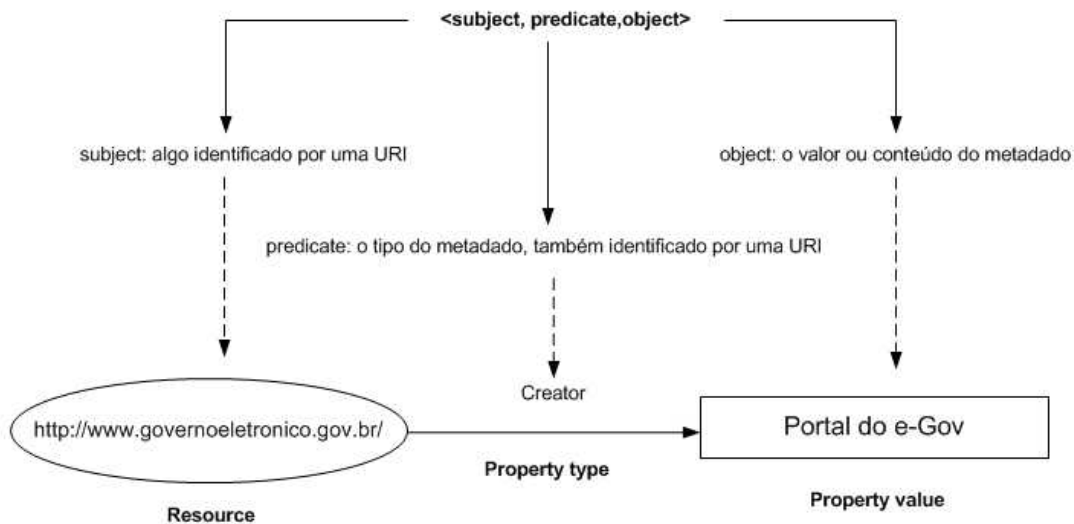


Figura 20: Elementos básicos do RDF

A Figura 21 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 21: Exemplo de um documento RDF (Fonte: W3Schools)

4.4.6. Taxonomia para navegação (VCGE)

As seções anteriores discutiram como as informações são formadas, validadas, transformadas e representadas de modo a atenderem requisitos básicos de interoperabilidade semântica. Nesta seção o foco é a descrição e classificação da informação, tópico também de interesse da interoperabilidade semântica.

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.

Existem diversos métodos de classificação que podem ser utilizados com o objetivo de agrupar informações semanticamente semelhantes, e um dos métodos mais comumente utilizados na área de TI é a taxonomia.

Taxonomia é uma forma de classificar informações através de uma estrutura hierárquica. Tipicamente, uma taxonomia organiza conceitos ou definições utilizando relacionamentos do tipo supertipo e subtipo, também conhecidos como de generalização e especialização, ou pai e filho.

O VCGE (Vocabulário Controlado do Governo Eletrônico) é uma taxonomia criada pelo governo brasileiro com o objetivo de organizar assuntos do governo. A primeira versão da taxonomia ficou conhecida como LAG (Lista de Assuntos do Governo), sendo substituída pela nova versão denominada VCGE que, além de associar os elementos taxonômicos com o e-PMG (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 diversos níveis, e o primeiro deles representa as áreas de atuação do governo no país. Os demais subníveis fornecem desmembramentos do nível imediatamente superior, de modo a prover uma visão mais detalhada e descritiva do primeiro nível. A Figura 22 ilustra a estrutura do VCGE e o desmembramento parcial de um nível em subníveis intermediários.



Figura 22: 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 e-PING 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.

Como o VCGE ainda é um padrão novo, os órgãos do governo encontram-se ainda em processo de adaptação para utilizá-lo em sua plenitude. Alguns sítios governamentais ainda fazem o uso da LAG, versão anterior para classificação de informações do governo, o que é perfeitamente aceitável considerando-se este momento de transição entre os dois padrões. Outros, no entanto, já estão utilizando esse novo padrão. A Figura 23 ilustra o exemplo de um sítio na Internet que faz uso do VCGE.



Figura 23: Exemplo de uso do VCGE

(Fonte: http://catalogo.governoeletronico.gov.br/pasta_servico/)

4.5. Interoperabilidade Semântica e as Áreas de Integração para Governo Eletrônico

A interoperabilidade semântica associada ao segmento de Áreas de Integração para Governo Eletrônico, conforme definido na e-PING, é considerada no componente que trata de Legislação, Jurisprudência e Proposições Legislativas (LexML). Na visão da e-PING, o LexML é considerado um padrão Recomendado (R), conforme descrito na Tabela 22.

Tabela 22: Especificações para o Segmento de Áreas de Integração para Governo Eletrônico (1)

Componentes	Especificação	Situação
Legislação, Jurisprudência e Proposições Legislativas	LexML	R

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 24 mostra o resultado da consulta ao documento, na página de referência do LexML.



[Página Anterior](#) | [Página Inicial](#) | [Pesquisa Avançada](#)

Localidade	Brasil
Autoridade	Federal
Título	Lei nº 8.666, de 21 de Junho de 1993
Data	21/06/1993
Ementa	Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
Nome Uniforme	urn:lex:br:federal:lei:1993-06-21;8666
Mais detalhes	Senado Federal (text/html)
Mais detalhes	Câmara dos Deputados (text/html)

Publicação Oficial

Publicação Original	1993-06-22	Diário Oficial da União. Seção 1. 22/06/1993. p. 8269
Republicação	1994-07-06	Diário Oficial da União. Seção 1. 06/07/1994. p. 10149
Retificação	2003-07-02	Diário Oficial da União. Seção 1. 02/07/2003. p. 1

Figura 24: Referência a documentos jurídicos no LexML (TICONTROLE, 2010).

Outra forma de se consultar o LexML é através da sua interface gráfica (Figura 25), disponível no endereço <http://www.lexml.gov.br/> .



Rede de Informação Legislativa e Jurídica

Tudo
 Legislação
 Jurisprudência
 Proposições Legislativas

[Pesquisa Avançada](#) | [Acervo](#) | [Sobre o LexML](#) ([English](#) , [Français](#) , [Español](#))

Figura 25: Interface de consulta do LexML (TICONTROLE, 2010).

5. INTEROPERABILIDADE ORGANIZACIONAL

5.1. Interoperabilidade Organizacional na e-PING

Outra dimensão da interoperabilidade é a organizacional, que consiste na habilidade de duas ou mais unidades fornecerem e consumirem serviços umas das outras de modo a compor uma cadeia de serviços colaborativos.

A interoperabilidade organizacional é muitas vezes caracterizada pela capacidade dinâmica das organizações realizarem operações (transações) através da composição de diversos serviços, sejam eles internos ou externos à instituição. Essa capacidade dinâmica de combinar serviços está associada à habilidade que uma instituição tem em integrar, construir e reconfigurar seus sistemas de informações, de modo a atender às mudanças constantes dos processos organizacionais (TEECE, PISANO e SHUEN, 1997). Assim, a interoperabilidade organizacional, no contexto do governo, reflete a capacidade das instituições públicas em realizar mudanças, inovar e atender aos desafios impostos por forças sociais, econômicas, políticas e organizacionais do país.

Nesse contexto, a e-PING descreve aspectos associados à interoperabilidade organizacional no segmento de Áreas de Integração para Governo Eletrônico, onde são referenciadas as seguintes recomendações: (i) a adoção gradual da Arquitetura Orientada a Serviços (SOA); (ii) a adoção do padrão XML e do desenvolvimento de XML *Schemas*; (iii) o uso da tecnologia de *Web Services*; e (iv) a utilização do Catálogo de Interoperabilidade do governo.

O tema “SOA” e os padrões baseados em XML foram devidamente tratados anteriormente nesse documento. Em relação à tecnologia de *Web Services*, a e-PING recomenda a documentação adequada de cada serviço provido pelos órgãos de governo de modo a incentivar a interoperabilidade organizacional em larga escala. Essa prática é também reforçada pela adoção, no governo, de um Catálogo de Interoperabilidade que permitirá a divulgação dos serviços governamentais, assim como o armazenamento de suas referidas documentações técnicas.

Além disso, a e-PING Recomenda (R), para a promoção da interoperabilidade organizacional, os padrões relacionados na Tabela 23. Esses padrões são descritos nas subseções seguintes.

Tabela 23: Especificações para o Segmento de Áreas de Integração para Governo Eletrônico (2)

Componentes	Especificação	Situação
PROCESSOS – Notação de Modelagem de Processos	BPMN 1.0	R
PROCESSOS – Linguagem para Execução de Processos	BPEL4WS V1.1	R
Infraestrutura de registro	UDDI v3.0.2	R

5.1.1. Catálogo de Interoperabilidade

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

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, 2011). 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 e-PING com essas duas iniciativas é a divulgação dos serviços de governo, assim como dos padrões das informações fornecidas e consumidas pelas instituições públicas. As Figuras 26 e 27 mostram, respectivamente, a funcionalidade de busca no CPD e no Catálogo de Serviços Interoperáveis.

The screenshot shows the header of the 'Catálogo de Interoperabilidade' website. The header includes the logo of the 'Ministério do Planejamento, Orçamento e Gestão' and the text 'Catálogo de Interoperabilidade'. There are navigation links for 'Login' and 'Mapa'. Below the header, there are links for 'Padrão De Dados', 'Mantenha-se Atualizado', 'Serviços', and 'Fale Conosco'. The main content area shows the breadcrumb 'você está aqui: página inicial → padrão de dados' and the title 'Consulta de Padrão de dados'. The search form includes fields for 'Nome Completo', 'Data início', and 'Data fim', along with 'Buscar' and 'Mostrar todos' buttons. At the bottom, there are dropdown menus for 'Nome Completo', 'Proprietário', and 'Data De Publicação'.

Figura 26: Busca no Catálogo Padrão de Dados.

Planejamento
Ministério do Planejamento, Orçamento e Gestão

Catálogo de Interoperabilidade

Login | Mapa

Padrão De Dados | Mantenha-se Atualizado | Serviços | Fale Conosco

você está aqui: página inicial → serviços

Consulta de Serviço

Nome:

Assunto:

Sistema:

Estruturante:

Órgão:

Buscar Mostrar todos

Nome	Órgão	Sistema	Assunto	Status
------	-------	---------	---------	--------

Figura 27: Busca no Catálogo de Serviços Interoperáveis.

5.1.2. Modelo de Documentação de Web Services

É essencial que os provedores de *Web Services* documentem cada serviço com precisão e clareza. Para tanto, a e-PING recomenda a utilização de um padrão específico cujo modelo pode ser encontrado no sítio do governo eletrônico <http://catalogo.governoeletronico.gov.br>, e ilustrado na Figura 28 (COORDENAÇÃO DA E-PING, 2010).

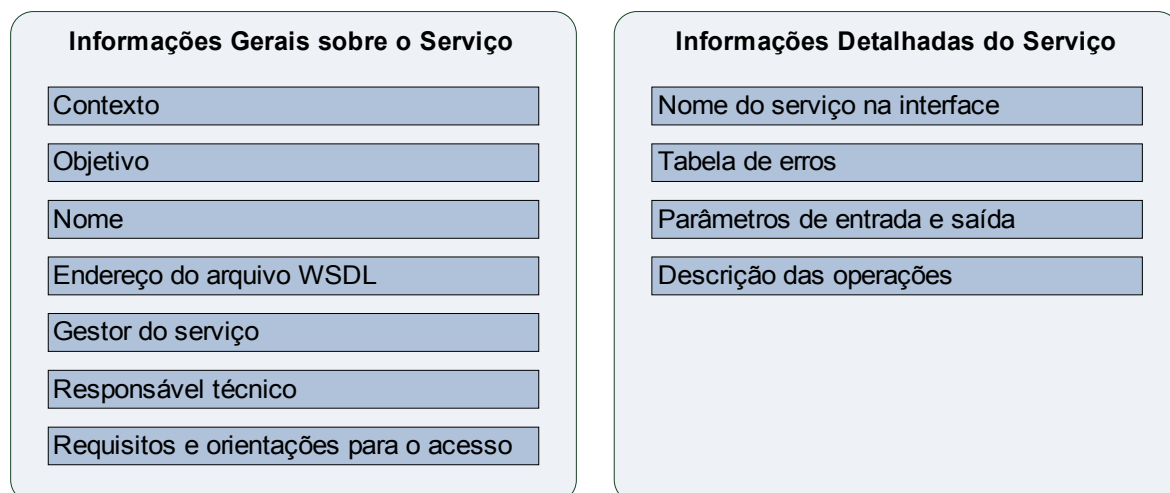


Figura 28: Padrão para a descrição dos *Web Services* de governo

As informações necessárias para a documentação dos *Web Services* do governo são organizadas hierarquicamente da seguinte forma:

Informações gerais sobre o serviço:

- **Contexto** – motivações e cenários que levaram ao desenvolvimento do serviço.
- **Objetivo** – descrição dos objetivos do serviço.
- **Nome** – nome do serviço na visão do negócio.
- **Endereço do arquivo WSDL** – URL desse arquivo, ponto de partida para o consumo ou invocação do serviço.
- **Gestor do serviço** – nome, e-mail e telefone do gestor responsável pelo serviço.
- **Responsável técnico** – nome, e-mail e telefone do responsável técnico.
- **Requisitos e orientações para o acesso** – informações sobre procedimentos que condicionam o uso do serviço, como termos de uso ou responsabilidade, cadastro ou criação de usuários, contato para obter autorização, uso de certificado digital, acesso ao ambiente de testes, entre outros.

Informações detalhadas do serviço:

- **Nome do serviço na interface** – nome do serviço conforme declarado no documento WSDL.
- **Tabela de Erros** – tabela com código e descrição de todos os erros que podem ser apresentados ao consumidor do serviço.
- **Considerações gerais sobre parâmetros de entrada e/ou saída** – devem ser informados os parâmetros de entrada e/ou saída comuns a todas as operações, bem como as particularidades sobre parâmetros que se repitam em várias operações e que mereçam esclarecimentos maiores.
- **Operações** – para cada operação, são necessárias as seguintes informações:
 - *Nome da operação na perspectiva de negócio* – identificar a operação apresentando uma breve descrição de sua natureza e propósito.
 - *Nome da operação na interface do serviço* – nome da operação conforme declarado no WSDL.

-
- **Parâmetro(s) de entrada** – apresentar em tabela a estrutura hierárquica dos parâmetros de entrada da operação, com as seguintes informações para cada parâmetro:
 - *nome* – elemento do XML Schema.
 - *tipo de dado* (*integer*, *string*, *date*, *float*, etc., especificado em <http://www.w3.org/TR/xmlschema-2/#built-in-datatypes>).
 - *ocorrência mínima* (0: opcional; 1: obrigatório).
 - *observações* – descrição do elemento, domínio válido, máscaras e outras.
 - **Parâmetro(s) de saída** – apresentar em tabela a estrutura hierárquica dos parâmetros de saída da operação, com as seguintes informações para cada parâmetro:
 - *nome* – elemento do XML Schema.
 - *tipo de dado* (*integer*, *string*, *date*, *float*, etc., especificado em <http://www.w3.org/TR/xmlschema-2/#built-in-datatypes>).
 - *ocorrência mínima* (0: opcional; 1: obrigatório).
 - *observações* – descrição do elemento, domínio válido, máscaras e outras.

5.1.3. 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.

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 29 ilustra os principais componentes da notação BPMN.

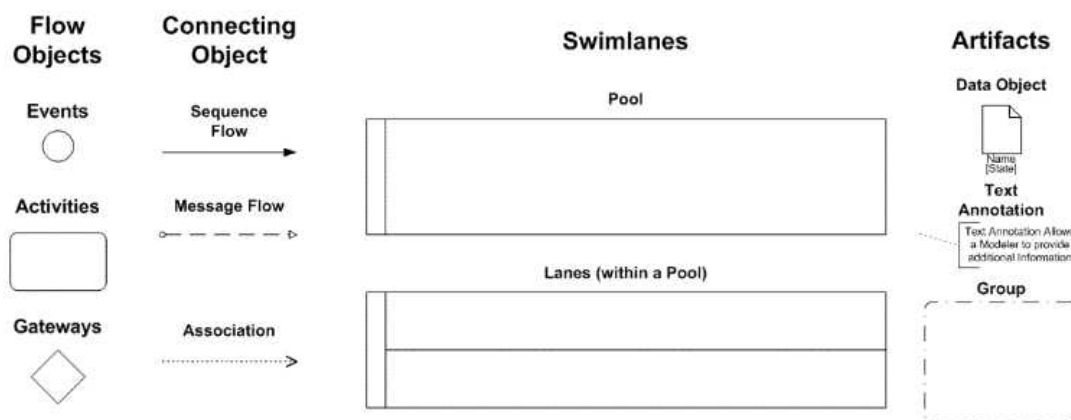


Figura 29: Principais componentes da notação BPMN (OMG, 2005).

Como se pode observar na Figura 29, 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 30 ilustra um processo de negócio do governo, mapeado em BPMN.

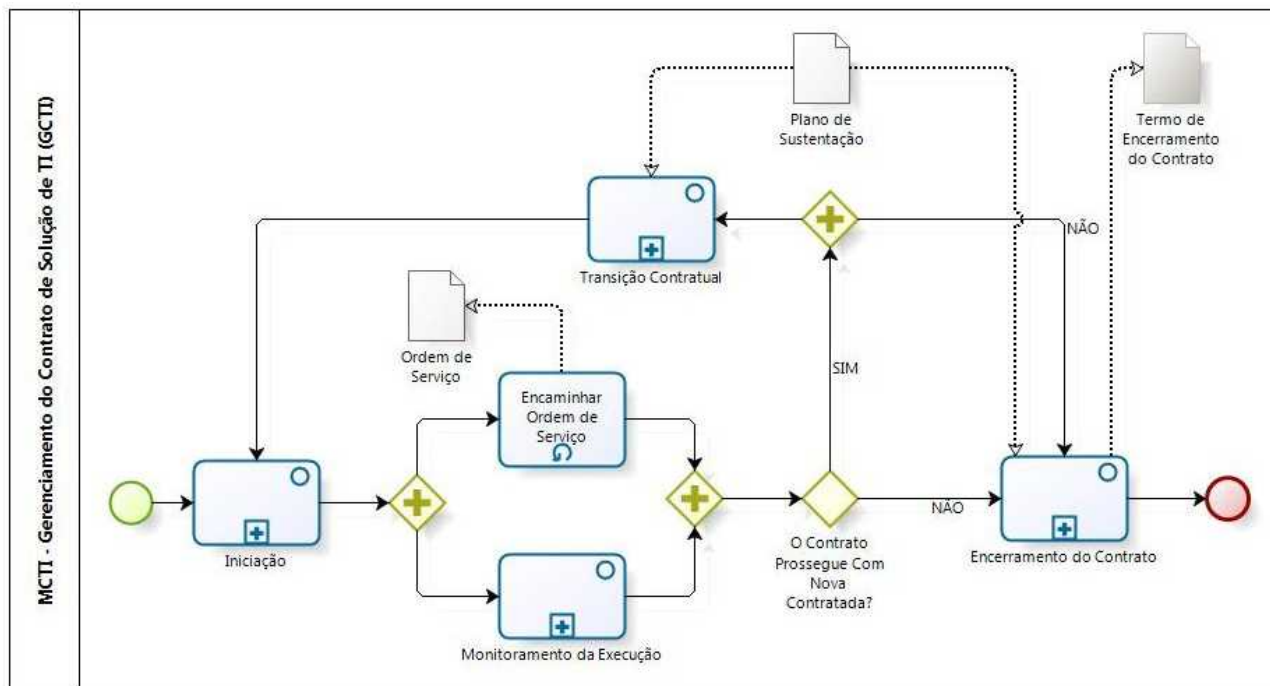


Figura 30: Exemplo de um processo de negócio mapeado em BPMN.

5.1.4. 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 idéia 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.

Um serviço de registro UDDI pode ser compreendido como um repositório de informações sobre os *Web Services* desenvolvidos. As informações sobre as organizações e os serviços por elas fornecidos são também armazenados nesse repositório em formato XML. O paradigma utilizado na organização desse repositório é o de um catálogo telefônico: assim como as organizações interessadas em disponibilizar serviços em um determinado mercado se fazem conhecer através de publicidade nas páginas amarelas, as organizações interessadas em disponibilizar serviços pela Internet publicam as informações necessárias em serviços públicos de registro UDDI.

Inicialmente o UDDI foi elaborado pela *Microsoft*, *IBM* e *Ariba*, e em 2002 foi incorporado à lista de especificações do OASIS. A especificação define dois tipos de serviços definidos no UDDI: (i) serviço de registro e (ii) serviço de repositório.

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.

Ainda seguindo o paradigma do catálogo telefônico, os dados em um registro UDDI podem ser divididos conceitualmente em três tipos diferentes de diretório: ***páginas brancas***, com informações de contatos para negócios; ***páginas amarelas***, categorizando negócios e serviços; e ***páginas verdes***, com informações técnicas sobre os serviços oferecidos.

Um exemplo típico da utilização de um registro UDDI é o da corretagem no mercado de ações, onde um aplicativo que informa valores das ações em tempo real pode localizar e utilizar um *Web Service* que oferece essas informações através de uma API *Web* de simples utilização. A Tabela 24 organiza a estrutura, funcionalidades e facilidades do UDDI:

Tabela 24: Estrutura e funcionalidades de um registro UDDI 2.0 (Modificado do XML.com)

Diretório	Operação	Informação e propósito
<p>Páginas brancas: Nome, endereço, telefone, fax, e-mail e outras informações de contato de uma determinada empresa.</p>	<p><i>Publish:</i> Como um provedor de um <i>Web Service</i> se registra, fornecendo as informações de contato necessárias.</p>	<p>Informação do negócio: Contida em um objeto do tipo <i>BusinessEntity</i>, que por sua vez contém informações sobre serviços categorias, contatos, URLs e muitas outras, necessárias à interação com um determinado negócio.</p>
<p>Páginas amarelas: Informações que categorizam o negócio das empresas</p>	<p><i>Find:</i> Como um aplicativo encontra um determinado <i>Web Service</i>.</p>	<p>Informação do serviço: Descreve um grupo de <i>Web Services</i>, contidos em um objeto do tipo <i>BusinessService</i>.</p>
<p>Páginas verdes: Informações técnicas sobre os <i>Web Services</i> disponibilizados por uma determinada empresa.</p>	<p><i>Bind:</i> Como um aplicativo se conecta a um determinado <i>Web Service</i> e com ele interage, após tê-lo encontrado.</p>	<p>Informação de enlace: Os detalhes técnicos necessários à interação com o <i>Web Service</i>, incluindo URLs, nomes de métodos, tipos de argumentos, etc. O objeto do tipo <i>BindingTemplate</i> representa esses dados.</p> <p>Detalhes do serviço: Metadados sobre as diversas especificações implementadas por um dado <i>Web Service</i>, são chamados de <i>tModels</i>.</p>

6. CONCLUSÃO

O ecossistema de interoperabilidade pode ser compreendido através de diferentes aspectos ou dimensões, quais sejam: interoperabilidade técnica, interoperabilidade semântica e interoperabilidade organizacional. Essa Cartilha Técnica discorreu sobre todas essas dimensões de interoperabilidade de modo a prover um guia prático para a melhor utilização da e-PING no âmbito do governo.

No que diz respeito à interoperabilidade técnica, este documento abordou componentes dos segmentos de interconexão, meios de acesso, segurança e áreas de integração para e-Gov. Foram fornecidas também informações envolvendo Arquitetura de Software, em particular SOA no contexto de utilização da tecnologia de *Web Services*.

Em relação à interoperabilidade semântica, os segmentos da e-PING que tiveram destaque foram os de interconexão, meios de acesso, organização e intercâmbio de informações e áreas de integração para e-Gov. Nesse contexto, as tecnologias baseadas no padrão XML foram exploradas de modo a reforçar as boas práticas quando da sua utilização no desenvolvimento de sistemas interoperáveis. Também mereceu destaque o padrão de classificação de informações governamental conhecido como VCGE.

Por fim, a interoperabilidade organizacional tratada nessa Cartilha Técnica reforçou a importância da modelagem de processos como um meio para garantir a interoperabilidade dentro das organizações públicas e também, além de suas fronteiras. No contexto da modelagem de processos, foi ressaltado o uso da notação BPMN explorando, inclusive, as diferenças entre os diversos níveis de granularidade de modelagem, além da transição do modelo de processos conceitual, concebido pelo analista de processos, para o modelo de processos para execução, concebido pelos analistas de sistemas e/ou desenvolvedores de softwares. Outro aspecto de grande importância para a interoperabilidade organizacional é o uso de registros/repositórios de serviços, o qual foi descrito através da explanação envolvendo o padrão UDDI e também da descrição da primeira iniciativa do governo brasileiro neste sentido, a qual leva o nome de Catálogo de Interoperabilidade.

Como se pode observar, uma gama enorme de temas foi tratada neste documento, não com o objetivo de esgotar os assuntos associados à interoperabilidade, mas com a meta de introduzi-los no contexto das políticas públicas do país, assim como de ressaltar a sua importância para a construção de sistemas públicos capazes de trocar informações uns com os outros, além de fornecer informações consistentes, relevantes e facilitadas à sociedade brasileira.

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: 19 Agosto 2010.
- 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: 3 dez. 2010.
- COORDENAÇÃO DA E-PING. Arquivos. Catálogo de Interoperabilidade, 2010. Disponível em: <http://catalogo.governoeletronico.gov.br/folder_arquivos>. Acesso em: 19 Agosto 2010.
- CROCKFORD, D. Network Working Group. RFC 4627, 2006. Disponível em: <<http://tools.ietf.org/html/rfc4627>>. Acesso em: Dezembro 2010.
- E-PING. e-PING: Programa de Governo Eletrônico Brasileiro. Governo Eletrônico, 2011. Disponível em: <<http://www.eping.e.gov.br>>. Acesso em: 7 Dezembro 2010.
- 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: 3 dez. 2010.
- ICP-BRASIL. Resolução Nº 58. Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil, 2008. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao_58.pdf>. Acesso em: 3 dez. 2010.
- ICP-BRASIL. Resolução Nº 65. Padrões e Algoritmos Criptográficos da ICP-Brasil, 2009. Disponível em: <<http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/resolucao65.pdf>>. Acesso em: 3 dez. 2010.
- IETF. RFC 3277: Guidelines for Evidence Collection and Archiving. Network Working Group, 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3227.txt>>. Acesso em: 3 dez. 2010.
- JOSUTTIS, N. M. SOA In Praticce. [S.l.]: O'Reilly, 2007.
- JSON.ORG. JSON, 2009. Disponível em: <<http://json.org/>>. Acesso em: Dezembro 2010.
- 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://www.itl.nist.gov/fipspubs/fip140-1.htm>,<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>>. Acesso em: 4 dez. 2010.

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: 3 dez. 2010.

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: 1 Dezembro 2010.

OMG. BPMN Graphical Elements. BPMN Core Elements, 2005. Disponível em: <http://www.bpmn.org/Samples/Elements/Core_BPMN_Elements.htm>. Acesso em: Dezembro 2010.

PAPAZOGLU, 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: 19 Agosto 2010.

PRESIDÊNCIA DA REPÚBLICA. Normas Complementares Nos. 4 a 7, 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_4_controle_acesso.pdf,http://dsic.planalto.gov.br/documentos/nc_5_controle_acesso.pdf,http://dsic.planalto.gov.br/documentos/nc_6_controle_acesso.pdf,http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf>. Acesso em: 3 dez. 2010.

REDE DO GOVERNO. Portal de Serviços e Informações do Governo. Caixas Postais Individuais-Funcionais no Governo Federal, 2010. ISSN S/N. Disponível em: <http://www.e.gov.br/correios/cp_individ.htm>. Acesso em: 19 Agosto 2010.

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: 19 Agosto 2010.

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: 19 Agosto 2010.

VIDIGAL, L. Sistemas Evolutivos e Gestão da Mudança da Administração Pública, 2011. Disponível em: <http://www.quidgest.pt/documentos/Apresentacoes/LV_Sistemas_Evolutivos_e_Gestão_da_Mudança_da_Administracao.pdf>. Acesso em: 2 jun. 2011.

W3C. Mobile Web Best Practices. W3C Recommendation, 2008. Disponível em: <W3C Recommendation>. Acesso em: 3 dez. 2010.

W3C. Semantic Web Standards. RDF, 2010. Disponível em: <<http://www.w3.org/RDF/>>. Acesso em: Dezembro 2010.

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

ÍNDICE REMISSIVO

<p>A</p> <p>Áreas de Integração para e-Gov... 40</p> <p>Arquitetura de software... 42</p> <p>Arquitetura de Software.....</p> <p style="padding-left: 20px;">EAI..... 58</p> <p style="padding-left: 20px;">ESB..... 58</p> <p>Arquitetura Orientada a Serviços... 42</p> <p>Arquivos de áudio e vídeo..... 70</p> <p>ASCII..... 67</p> <p>Audio-Video Interleaved..... 70</p> <p>B</p> <p>BMP..... 70</p> <p>BPEL..... 40</p> <p>broker..... 58</p> <p>BZIP2..... 70</p> <p>C</p> <p>Catálogo de Serviços Interoperáveis 93</p> <p>Compactação de arquivos..... 70</p> <p>CORBA..... 8, 43</p> <p>Correio Eletrônico..... 24</p> <p style="padding-left: 20px;">Caixas Postais Individuais- Funcionais..... 64</p> <p>D</p> <p>Data Biding.....</p> <p style="padding-left: 20px;">como utilizar..... 77</p> <p>Data Binding..... 76</p> <p>DCOM..... 8, 43</p> <p>Diretório..... 27</p> <p>divX..... 70</p> <p>DOM..... 75</p> <p style="padding-left: 20px;">como utilizar..... 77</p> <p>DSDL..... 83</p> <p>DTD..... 83</p> <p>E</p> <p>e-GIF..... 16</p> <p>e-PING.....</p> <p style="padding-left: 20px;">níveis de conformidade..... 19</p> <p style="padding-left: 20px;">sobre a e-PING..... 16</p> <p>EAI..... 59</p> <p>ebXML..... 98</p> <p>ESP..... 31</p> <p>Execução de Processos..... 40</p> <p style="padding-left: 20px;">BPELWS..... 40</p> <p style="padding-left: 20px;">BPML..... 40</p> <p style="padding-left: 20px;">engine BPEL..... 41</p> <p style="padding-left: 20px;">XPDL..... 40</p> <p>G</p> <p>GeoTIFF..... 70</p> <p>Gerenciamento de redes..... 28</p> <p>GIF..... 70</p> <p>GML..... 70</p> <p>H</p>	<p>HTML..... 68</p> <p>I</p> <p>IDL..... 43</p> <p>IKE..... 30</p> <p>Informação jurídica e legislativa... 89</p> <p>Informações georreferenciadas..... 70</p> <p>Infraestrutura de Rede..... 24</p> <p style="padding-left: 20px;">ATM..... 25</p> <p style="padding-left: 20px;">CoS..... 25</p> <p style="padding-left: 20px;">Frame-Relay..... 25</p> <p style="padding-left: 20px;">IEEE 802.11..... 26</p> <p style="padding-left: 20px;">IEEE 802.11g..... 26</p> <p style="padding-left: 20px;">IEEE 802.11n..... 26</p> <p style="padding-left: 20px;">IPv4..... 25</p> <p style="padding-left: 20px;">IPv6..... 25</p> <p style="padding-left: 20px;">MIMO..... 26</p> <p style="padding-left: 20px;">MPLS..... 25</p> <p style="padding-left: 20px;">SIPP..... 25</p> <p style="padding-left: 20px;">TCP/IP..... 25</p> <p style="padding-left: 20px;">UDP..... 25</p> <p style="padding-left: 20px;">WLAN..... 26</p> <p>Interoperabilidade.....</p> <p style="padding-left: 20px;">conceito..... 16</p> <p style="padding-left: 20px;">conformidade..... 19</p> <p style="padding-left: 20px;">dimensões..... 17</p> <p>Interoperabilidade Organizacional... 92</p> <p style="padding-left: 20px;">catálogo de interoperabilidade... 93</p> <p style="padding-left: 20px;">contextualização..... 92</p> <p style="padding-left: 20px;">documentação dos serviços de e- Gov..... 94</p> <p style="padding-left: 20px;">modelagem de processos..... 96</p> <p style="padding-left: 20px;">registro e repositório UDDI..... 98</p> <p>Interoperabilidade Semântica..... 62</p> <p style="padding-left: 20px;">classificação da informação..... 87</p> <p style="padding-left: 20px;">contextualização..... 62</p> <p style="padding-left: 20px;">criação de vocabulários..... 82</p> <p style="padding-left: 20px;">intercâmbio de arquivos..... 69</p> <p style="padding-left: 20px;">nas estações de trabalho..... 67</p> <p style="padding-left: 20px;">representação de dados..... 71</p> <p style="padding-left: 20px;">segmento de áreas de integração para e-Gov..... 89</p> <p style="padding-left: 20px;">segmento de interconexão..... 63</p> <p style="padding-left: 20px;">segmento de meios de acesso..... 65</p> <p style="padding-left: 20px;">segmento de organização e intecâmbio de informações... 70</p> <p style="padding-left: 20px;">segmentos da e-PING..... 59, 63</p> <p style="padding-left: 20px;">transferência de dados em hipertexto..... 68</p> <p style="padding-left: 20px;">transformação de dados..... 78</p> <p>Interoperabilidade Técnica.....</p> <p style="padding-left: 20px;">arquitetura de software..... 42</p> <p style="padding-left: 20px;">contextualização..... 21</p> <p style="padding-left: 20px;">segmento de áreas de integração para e-Gov..... 40</p> <p style="padding-left: 20px;">segmento de interconexão..... 23</p> <p style="padding-left: 20px;">segmento de segurança..... 28</p> <p style="padding-left: 20px;">segmentos da e-PING..... 22</p>	<p>IPv4..... 25</p> <p>J</p> <p>JPEG..... 70</p> <p>L</p> <p>LexML..... 89</p> <p>Linguagem de intercâmbio de dados 9, 77</p> <p>M</p> <p>Mensageria..... 23</p> <p style="padding-left: 20px;">IMAP..... 24</p> <p style="padding-left: 20px;">IMPP..... 24</p> <p style="padding-left: 20px;">POP3..... 24</p> <p style="padding-left: 20px;">SMS..... 24</p> <p style="padding-left: 20px;">SMTP..... 24</p> <p style="padding-left: 20px;">XMPP..... 24</p> <p>middleware..... 58</p> <p>MIDI..... 70</p> <p>Modelagem de Processos.....</p> <p style="padding-left: 20px;">BPMN..... 40, 96</p> <p style="padding-left: 40px;">elementos..... 97</p> <p style="padding-left: 20px;">modelagem analítica..... 97</p> <p style="padding-left: 20px;">modelagem descritiva..... 96</p> <p style="padding-left: 20px;">modelagem para execução..... 97</p> <p style="padding-left: 20px;">transição BPMN-BPEL..... 41</p> <p>Modelo de referência..... 45</p> <p style="padding-left: 20px;">SOA/OASIS..... 45</p> <p>MPEG-1..... 70</p> <p>MPEG-4..... 70</p> <p>MySQL Database..... 70</p> <p>N</p> <p>Nomeação de caixa postal eletrônica 64</p> <p>Nomeação de domínio..... 64</p> <p>O</p> <p>Ogg Vorbis..... 70</p> <p>Open Document..... 69, 70</p> <p>Open Office Base..... 70</p> <p>ORB..... 43</p> <p>P</p> <p>PDF..... 69</p> <p>PNG..... 70</p> <p>Protocolo de criptografia..... 29</p> <p>Proxy Authorization..... 30</p> <p>R</p> <p>RDF..... 84</p> <p>Redes locais sem fio..... 26</p> <p>Redes sem Fio..... 36, 37</p> <p>Registro UDDI..... 99</p> <p>RELAX..... 83</p> <p>RELAX NG..... 83</p> <p>Representação do conhecimento... 87</p> <p>RESTful..... 51</p>
---	--	--

RESTful Web API.....	52	registro de serviços.....	46	serviço de repositório.....	99
RMI.....	10, 43	serviços statefull.....	40	serviços de registro.....	99
RTF.....	69	serviços stateless.....	40	UML.....	71
S		WSDL.....	41	UNICODE.....	67
S/MIME.....	31	Serviços de conferências multimídia		V	
SAF.....	83	27	VCGE.....	11, 71
SAX.....	75	Serviços de Rede.....		W	
como utilizar.....	77	FTP.....	27	WAVE.....	70
Segurança.....		HTTP.....	27	Web Semântica.....	85
correio eletrônico.....	31	LDAP.....	27	Web Services.....	40, 47
criptografia.....	32	NTP.....	10, 27	criação e utilização.....	58
desenvolvimento de sistemas.....	34	SIP.....	27	documentação.....	94
incidentes de segurança.....	37	SMNP.....	10, 28	REST.....	47
serviços de rede.....	36	SNTP.....	27	RESTful Web Services.....	51
comunicação de dados.....	29	SOAP.....	10, 28	SOAP.....	47
3DES.....	30	Serviços de transporte e		vantagens.....	48
AES.....	30	intercomunicação.....	25	WS*.....	47
AH.....	31	Servlets/JSP.....	9, 43	WSDL.....	53
DHE_DSS.....	30	Sessão multicast.....	27	estrutura.....	54
DHE_RSA.....	30	Sessão multimídia.....	27	X	
Diffie-Hellman.....	30	ShapeFile.....	70	XHTML.....	11, 68
DSS.....	30	SHTML.....	68	XML.....	47, 70, 71
ICP.....	9, 30	Sincronização de relógios.....	27	APIs para processamento.....	75
ICP-Brasil.....	30	Sistema distribuído.....	42	boas práticas.....	71, 74, 76
IDEA.....	30	Sistemas de informação geográfica	40	formação.....	82
IPSec Authentication Header	30	SOAP.....	49	modelagem.....	74
PKI.....	29	estrutura.....	49	uso de atributos.....	74
RC4.....	30	SOX.....	83	validação.....	82
RSA.....	30	SVG.....	70	XML Schema.....	70
SASL.....	10, 30	T		XML Schemas.....	82
SHA-256.....	30	TAR.....	70	limitações.....	83
SHA-512.....	30	TIFF.....	70	XSL.....	78
SSL.....	29	Transferência de arquivos.....	27	XSL-FO.....	79
TLS.....	30	Transferência de hipertexto.....	27	XSLT.....	78
X.509 v3.....	30	U		Z	
Serviços.....	45	UDDI.....	11, 98	ZIP.....	70
consumidor de serviços.....	46	páginas brancas, amarelas e verdes			
políticas de uso.....	45	99		
provedor de serviços.....	46				