Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Estudos de Diretrizes em Interoperabilidade e Dados Abertos

Data de Emissão:

01/04/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Caio Rondon Botelo de Carvalho
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sandro Augusto Pavlik Haddad
Sgio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
28/02/2015	1.0	Versão inicial.
02/03/2015	2.0	Revisão de texto e forma.
02/03/2015	3.0	Revisão de conteúdo e forma.
10/03/2015	4.0	Atualização do modelo padrão de formatação.
01/04/2015	4.1	Revisão final do ajuste do modelo padrão de formatação.
01/04/2015	4.2	Ajuste gramatical e ortográfico e adequação textual.

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1 INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, uma vez que proporciona condições ao cidadão de requerer legalmente até 27 (vinte e sete) Cédulas de Identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis, ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura

tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

Resultante de um subconjunto das atividades previstas para inicialização da cooperação MJ/SE e FUB/CDT, o presente documento contempla o plano estratégico elaborado durante as oficinas técnicas e capacitação da equipe de desenvolvimento formada por pesquisadores da Universidade de Brasília e representantes dos órgãos: Ministério da Justiça, Ministério do Planejamento, Ministério do Desenvolvimento Social, Ministério do Desenvolvimento Agrário, Ministério da Previdência Social, Instituto Nacional de Tecnologia da Informação da Presidência da República, Polícia Federal, Instituto de Identificação do Distrito Federal, Dataprev e Serpro.

O presente relatório contempla uma análise do padrão de interoperabilidade e tratamento de dados abertos. Confrontando as diretrizes estabelecidas nos documentos com os objetivos e metodologias associadas ao Projeto RIC, foi possível elencar as especificações técnicas que deverão ser empregadas no durante a execução do mesmo. Assim, obtém-se um trabalho coeso e pronto para ser integrado ao ambiente de TIC do Governo Federal, seja na comunicação entre as diferentes áreas quanto a publicação de dados abertos.

2 PADRÃO DE INTEROPERABILIDADE DO GOVERNO FEDERAL – EPING

A arquitetura ePing define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia da Informação e Comunicação (TIC) na interoperabilidade de serviços de governo eletrônico, estabelecendo as condições de interação com as esferas de governo, demais poderes e sociedade.

São regidos pela ePing todos os novos sistemas de informação que vierem a ser desenvolvidos e implantados no governo federal e, de certa maneira, estabelecem interação governo federal – sociedade; sistemas de informação legados que sejam objeto de implementação e envolvam provimento de serviços de governo eletrônico e aquisição ou atualização de equipamento de TIC.

2.1 Políticas Gerais

Cada segmento previsto na ePing contém especificações técnicas que são baseadas em políticas gerais, as quais servem de orientação para os órgãos em soluções de interoperabilidade. Abaixo serão descritas algumas dessas especificações.

- Adoção Preferencial de Padrões Abertos: sempre que possível devem ser adotados padrões abertos em especificações técnicas. Padrões proprietários são aceitos quando há inexistência de padrão aberto. Nesta ocorrência, os padrões proprietários serão adotados até que um padrão esteja disponível, ou de forma transitória, mantendo as perspectivas de substituição.

- Uso de *Software* Público e/ou *Softwar*e Livre: em conformidade com diretrizes do Comitê Executivo de Governo Eletrônico e normas definidas no âmbito do SISP, deve-se priorizar o uso de *software* público e/ou livre.

- Transparência: a Lei de Acesso à Informação (LAI) reforça o uso da interoperabilidade na busca pela publicidade dos dados. Mais informações disponíveis minimizam o número de interações do cidadão com o governo.

- Segurança: deve-se considerar o nível de segurança requerido pelo serviço quanto a interoperabilidade na prestação dos serviços.

- Existência de Suporte de mercado: todas as especificações contidas na ePING contemplam soluções utilizadas pelo mercado, com o objetivo de reduzir custos e riscos na concepção e produção de serviços nos sistemas de informações governamentais.

- Alinhamento com a Internet: todos os sistemas de informação devem estar alinhados com as principais especificações usadas na Internet.

- Adoção de navegadores: todos os sistemas de informação do governo devem ser acessíveis, preferencialmente, por meio de tecnologia baseada em navegador. Outras

interfaces são permitidas em situações específicas, nas quais não haja alternativa disponível baseada em navegadores.

- Escalabilidade: as especificações técnicas devem ter a capacidade de atender alterações de demanda no sistema, como mudança em volume de dados, quantidade de transações ou quantidade de usuários.

2.2 Especificação Técnica: Componentes Eping Relacionados com o RIC

Para organizar melhor as definições dos padrões, a arquitetura ePing foi segmentada em cinco partes. Cada um dos segmentos foi subdividido em componentes para os quais foram estabelecidas as especificações técnicas que são classificadas de acordo com o grau de aderência às políticas gerais da arquitetura. Os quatro níveis são: Adotado (A), Recomendado (R), Em Transição (T) e Em Estudo (E).

No escopo deste relatório, serão analisados apenas os itens adotados ou recomendados pela arquitetura ePing que podem ser relacionados com as especificações do projeto de Registro de Identificação Civil (RIC).

2.2.1 Interconexão

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

Tabela 1: Aplicação

Componente	Especificação	Situação
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1 (RFC 2616, atualizada pelas RFCs 2817, 5785, 6266 e 6585).	A
Protocolos de transferência de arquivos	FTP (com reinicialização e recuperação) conforme RFC 959 (atualizada pela RFC 2228, RFC 2640, RFC 2773, RFC 3659 e RFC 5797) e HTTP conforme RFC 2616 (atualizada pelas RFCs 2817, 5785, 6266 e 6585) para transferência de arquivos. SFTP (*Secure File Transfer Protocol*) conforme RFC 913.	A
Diretório	LDAP v3 deverá ser utilizado	A

	para acesso geral ao diretório OpenLDAP, conforme RFC 4510.	
Serviços de Nomeação de Domínio	O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035.	A
Protocolos de Gerenciamento de rede	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 3.	R

Tabela 2: Rede/Transporte

Componente	Especificação	Situação
Transporte	TCP (RFC 793) UDP (RFC 768) quando necessário	A
Intercomunicação LAN/WAN	IPv6 conforme RFC 2460 (atualizada pela RFC 5095, RFC 5722 e RFC 5871).	A
Comutação por *Label*	Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço.	A
Qualidade de Serviço	Adoção de uma arquitetura para serviços diferenciados pelo uso do Diffserv (RFC 2475, atualizada pela RFC 3260).	A

Tabela 3: Enlace/Físico

Componente	Especificação	Situação
Rede local sem fio	IEEE 802.11g IEEE 802.11n Em conformidade com as determinações do *Wi-Fi Alliance* e com as normas da Anatel.	A R
Qualidade de Serviço	IEEE 802.1p	R
Virtual LAN	VLAN (IEEE 802.1q)	R
Resiliência Camada 2	*Spanning Tree Protocol* (802.1d, 802.1w, 802.1s)	R

2.2.2 Segurança

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

Tabela 4: Comunicação de dados

Componente	Especificação	Situação
Transferência de dados em redes inseguras	TLS – *Transport Layer Security*, RFC 52463 (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.	R
Algoritmos para troca de chaves de sessão, durante *handshake*	RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;	R
Algoritmos para definição de chave de cifração	RC4, IDEA, 3DES e AES	R
Certificação Digital	X.509 v3 – ICP-Brasil, SASL - *Simple Authentication and Security Layer*, RFC 4422	R
Hipertexto e transferência de arquivos	RFC 2818 (atualizada pela RFC 5785)	R
Transferência de arquivos	SSH FTP FTP com TLS, RFC 4217	R R
Segurança de redes IPv4	*IPSec Authentication Header* para autenticação de cabeçalho do IP. IKE – *Internet Key Exchange*, RFC 5282, deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento. ESP – *Encapsulating Security Payload,* requisito para VPN – *Virtual Private Network*.	A A A
Segurança de redes IPv4 para protocolos de aplicação	O S/MIME v3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.	A
Segurança de redes IPv6 na camada de rede	As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*) ou autenticação IP, e a segurança do encapsulamento IP, ESP	R

	(*Encrypted Security Payload*).	

Tabela 5: Criptografia

Componente	Especificação	Situação
Algoritmo de cifração	3DES ou AES	R
Algoritmos para assinatura/*hashing*	SHA-256 ou SHA-512 Obs..: os sistemas devem ter suporte para *hash* MD5 com RSA para garantir compatibilidade com implementações anteriores.	R
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	A
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (RFC 5480) ECIES 256 e ECIES 512 Obs.: ECDSA para assinaturas digitais e ECIES para cifração e transporte seguro de chaves criptográficas.	A
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3; FIPS 140-1 e FIPS 140-2.	R
Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	Devem ser aderentes aos padrões da ICP-Brasil	R

Tabela 6: Desenvolvimento de Sistemas

Componente	Especificação	Situação
Assinaturas XML	XMLsig - Sintaxe e Processamento de assinatura XML[1]	A
Cifração XML	XMLenc - Sintaxe e Processamento de Cifração XML[2]	R
Assinatura e Cifração XML	XMLdecrypt - Transformação de decifração para assinatura XML[3]	R
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XKMS 2.0 - XML – *Key Management Specification*[4]	R
Autenticação e autorização de acesso XML	SAML - *Security Assertion Markup Language*[5]	R
Intermediação ou Federação de Identidades	WS-Security 1.1 - arcabouço de padrões para garantir integridade e confidencialidade em	R

	mensagens SOAP.	
Navegadores	Somente utilizar *cookies* com concordância do usuário	A

[1]Conforme definido pelo W3C http://www.w3.org/TR/xmldsig-core/
[2]Conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/
[3]Conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt
[4]Conforme definido pelo W3C http://www.w3.org/TR/xkms2/
[5]Conforme definido pelo OASIS quando um ambiente ICP é utilizado http://www.oasisopen.org/committees/security/index.shtml

Tabela 7: Serviços de Rede

Componente	Especificação	Situação
Diretório	LDAPv3 extensão para TLS RFC 4510, RFC4511 e RFC 4513	R
DNSSEC		A
Carimbo do Tempo	RFC 3628 TSAs – *Policy Requirements for Time-Stamping Authorities*, *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (atualizada pela RFC 5816).	R

Tabela 8: Redes Sem Fio

Componente	Especificação	Situação
LAN sem fio 802.11	WPA2 (*Wi-Fi Protect Access*) com criptografia AES	R

Tabela 9: Resposta a Incidentes de Segurança da Informação

Componente	Especificação	Situação
Preservação de Registros	*Guidelines for Evidence Collecction and Archiving* RFC 3227.	R
Gerenciamento de incidentes em redes computacionais	*Expectations for Computer Security Incident Response*, RFC 2350.	A

2.2.3 Meios de Acesso

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

Tabela 10: Meios de Publicação

Componente	Especificação	Situação
Conjunto de caracteres	*Unicode Standard* v7.0; ISBN 978-1-936213-09-2; UTF-8 ISO/IEC 10646:2014	R
Formato de Intercâmbio de hipertexto	W3C XML v1 ou v1.1 W3C HTML 5	A A
Mobile	W3C *Mobile Web application Best Practice*s	R
Arquivos do tipo documento/publicação	Texto puro (.txt) *Open Document* (.odt) NBR ISO/IEC 26.300:2008. *Open Document* ODF 1.2 EPUB 3.0.1 *Portable Document Format* - PDF ISO 32000-1:2008 *Portable Document Format* - PDF/A NBR ISO 19005-1:2009	A A R R R R
Arquivos do tipo planilha	*Open Document* (.ods) NBR ISO/IEC 26.300:2008. *Open Document* ODF 1.2	A R
Arquivos do tipo apresentação	*Open Document* (.odp) NBR ISO/IEC 26.300:2008. *Open Document* ODF 1.2 HTML (.html ou .htm)	A R R
Arquivos do tipo “banco de dados” para estações de trabalho	Texto puro (.txt) Texto puro (.csv) XML (.xml) MySQL *Database* (.myd ou .myi) v4 ou superior Arquivo do Base (.odb) NBR ISO/IEC 26.300:2008.	A A R R R
Compactação de arquivos	ZIP (.zip) GNU ZIP (.gz) Pacote TAR (.tar)	R R R

2.2.4 Organização e Intercâmbio de Informações

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

Tabela 11:Tratamento e transferência de Dados

Componente	Especificação	Situação
Linguagem para intercâmbio de dados	XML (*Extensible Markup Language*) JSON (*Javascript Object Notation*)	A A
Transformação de dados	XSLT (*Extensible Stylesheet Language Transformation*)	A
Definição dos dados para intercâmbio	XML *Schema*	A

Tabela 12: Vocabulários e Ontologias

Componente	Especificação	Situação
Descrição dos recursos	RDF (*Resource Description Framework)*	R
Especificações de vocabulários para RDF	*Resource Description Framework* – RDF Schema Obs.: recomenda-se o uso do RDF *Schema* em situações em que o poder do processamento disponível for limitado ou onde não for necessária para descrever os dados toda a expressividade da linguagem OWL.	R
Sistemas de Organização do Conhecimento	SKOS (*Simple Knowlegde Organization System*)	R
Linguagem de definição de ontologias na web	OWL (*Web Ontology Language)*	R

2.2.5 Áreas de Integração para Governo Eletrônico

Estabelece a utilização ou construção de especificações técnicas para sustentar o intercâmbio de informações em áreas transversais da atuação governamental, cuja padronização seja relevante para a interoperabilidade de serviços de governo eletrônico.

Tabela 13: Web Services

Componente	Especificação	Situação
Infraestrutura de registro	UDDI v3.0.2 (*Universal Description Discovery and Integration*)	R
Linguagem de definição do serviço	WSDL 1.1 (*Web Service Description Language)*	A
Protocolo para acesso a Web Service	SOAP v1.2 HTTP/1.1 (RFC 2616)	A A

3 ANÁLISE DO PADRÃO DE DADOS ABERTOS DO GOVERNO FEDERAL – *DADOS.GOV.BR*

A criação de um padrão tem o objetivo de orientar as organizações governamentais brasileiras quanto às boas práticas de publicação de dados na Internet e o devido cumprimento dos critérios técnicos relacionados ao paradigma de dados abertos.

É neste contexto que a Secretaria de Logística e Tecnologia da Informação – SLTI vem desenvolvendo a Infraestrutura Nacional de Dados Abertos. A INDA é composta por um conjunto de padrões, tecnologias, procedimentos e mecanismos de controle necessários para atender as condições de disseminação e compartilhamento de informações no modelo de Dados Abertos. Para que a sua arquitetura seja implementada conjuntamente por todos os órgãos do governo, é imprescindível o alinhamento dos processos de publicação de dados na Internet, com metodologias e boas práticas comuns, que garantam a conformidade com esses padrões.

O Portal Brasileiro de Dados Abertos tem como principal objetivo ser o ponto central para a busca e o acesso a dados públicos governamentais no Brasil. O portal tem sua estrutura baseada na arquitetura da Web. Cada conjunto de dados deve estar logicamente referenciável na Web. Dessa forma, a INDA está fundamentada numa arquitetura distribuída, na qual tanto a infraestrutura física como a responsabilidade pela manutenção do portal são compartilhadas entre os órgãos que publicam dados.

3.1 Preparação e Validação dos Dados

Para que um conjunto de dados esteja apto a constituir a Infraestrutura Nacional de Dados Abertos, o responsável pelo repositório de dados daquele órgão deve garantir que o

conjunto de dados cumpra as seguintes condições gerais:

- os dados devem estar em seu formato mais bruto possível, ou seja, antes de qualquer cruzamento ou agregação;
- os dados devem estar em formato aberto, não proprietário, estável e de amplo uso;
- não deve existir nenhum instrumento jurídico que impeça sua reutilização e redistribuição;
- para dados estruturados ou em planilhas na sua fonte, deve-se preservar ao máximo a estrutura original;
- é recomendável a disponibilização dos dados em diversos formatos;
- cada conjunto de dados deve possuir um identificador único e persistente, seguindo uma padronização URL. Requisito imprescindível para que o conjunto de dados seja referenciável e eventualmente consumido por um aplicativo;
- é recomendável a utilização de considerações semânticas na definição URLs, de forma que seja possível deduzir o conteúdo de um conjunto de dados apenas lendo seu identificador;
- é recomendável que os nomes dos arquivos sigam as boas práticas de formação de um *slug*;
- cada conjunto de dados deve ter informações sobre seus dados e metadados. Deve ser possível recuperar o significado dos dados;
- para conjunto de dados muito grandes, recomenda-se a divisão em porções menores, permitindo uma fácil manipulação. Por exemplo, divisão temporal ou dimensão geográfica;
- é desejável que o repositório dos dados possibilite a composição de filtros dentro da URL, seguindo algum padrão de API.

3.2 Publicação de Dados Abertos

A publicação corresponde ao processo da disponibilização permanente do conjunto de dados por um órgão no portal *dados.gov.br*. Este processo deve incluir além da publicação dos dados, a publicação dos metadados, os quais são informações que possibilitam organizar, classificar e relacionar novos dados sobre o conjunto de dados.

3.2.1 Metadados

Metadados são dados sobre os dados. Pode-se afirmar que os metadados agregam mais valor ao conjunto de dados e melhoram a sua classificação e busca. São considerados metadados obrigatórios, a saber.

- Título: nome do conjunto de dados.
- Descrição: breve explicação sobre os dados.
- Catálogo origem: URL do órgão onde está publicado o conjunto de dados.
- Órgão responsável: nome e sigla do órgão responsável pela publicação do conjunto de dados.
- Categorias no Vocabulário Controlado de Governo Eletrônico (VCGE).
- Recursos: separa vários recursos em mais de um conjunto de dados, verificando se os mesmos divergem em vários metadados.

São considerados metadados desejáveis, a saber.

- Etiquetas: listas de palavras relacionadas ao conjunto de dados.
- Autoria: instituição responsável pela produção do recurso.
- Cobertura geográfica: localização a que se referem os dados.
- Cobertura temporal: período a que se referem os dados.
- Referências: relação com outros conjuntos de dados.

3.2.2 Inserção no Portal *dados.gov.br*

O portal *dados.gov.br* é uma ferramenta de catalogação, busca e acesso a dados abertos. Nele deverão ser catalogados todos os dados públicos do governo brasileiro, onde cada órgão será responsável pela catalogação e manutenção de seus registros de conjuntos de dados que publica.

Na atividade de manutenção toda URL que aponta para um recurso do conjunto de dados deve estar ativa e ser persistente. O órgão deve instituir uma norma a ser seguida pela área responsável pela publicação dos dados na Internet com o intuito de garantir a uniformização e disponibilidade do recurso publicado através da URL. A atividade de atualização dos metadados deve estar alinhada com o processo de publicação de dados do órgão com o intuito de garantir que a informação mais nova e correta estará disponível através do portal *dados.gov.br*.

4 CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da SE e da Universidade de Brasília, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas.

A interoperabilidade apresenta a capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações, permeados pelos parâmetros aqui expostos, de maneira eficaz e eficiente. Conjuntamente, o paradigma de dados abertos está fundamentado na constatação de que o dado quando compartilhado abertamente tem seu valor e seu uso potencializados. Com isso o governo pretende desenvolver um ecossistema de dados e informações que beneficia a sociedade e possibilita o envolvimento de todos seus setores, inclusive a iniciativa privada, o setor acadêmico e o próprio governo.

As atividades envolvidas nessa etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe da SE, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

REFERÊNCIAS

[1] Cartilha Técnica para Publicação de Dados Abertos no Brasil. Disponível em: <http://dados.gov.br/cartilha-publicacao-dados-abertos/>. Acesso em fevereiro de 2015.

[2] Padrões de Interoperabilidade de Governo Eletrônico. Disponível em: <http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em fevereiro de 2015.

[3] Acesso às RFCs disponível em <http://www.ietf.org/rfc.html>.

[4] Manual dos dados abertos: desenvolvedores. Disponível em: <http://www.w3c.br/pub/Materiais/PublicacoesW3C/manual_dados_abertos_desenvolvedores_web.pdf>. Acesso em fevereiro de 2015.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br