

PANORAMA DA INTEROPERABILIDADE NO BRASIL



MINISTÉRIO DO PLANEJAMENTO ORÇAMENTO E GESTÃO
Secretaria de Logística e Tecnologia da Informação



**PANORAMA DA
INTEROPERABILIDADE
NO BRASIL**

Organizadoras:

Cláudia do Socorro Ferreira Mesquita
Nazaré Lopes Bretas







Brasília, DF
2010

Elaboração: MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO

Tiragem: 1000 exemplares

1ª edição: Ano 2010

Disponível também em: www.eping.e.gov.br

 Licença deste Documento	Sob as seguintes condições:
Para a utilização deste documento é necessário seguir as regras da licença Creative Commons pela mesma Licença 2.5 Brasil Você tem a liberdade de:	 Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).
 Compartilhar — Copiar, distribuir e transmitir a obra.	 Uso não comercial — Você não pode usar esta obra para fins comerciais.
 Remixar — Criar obras derivadas.	 Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.
Ficando claro que: <ul style="list-style-type: none">• Renúncia — Qualquer das condições acima pode ser renunciada se você obtiver permissão do titular dos direitos autorais.• Domínio Público — Onde a obra, ou qualquer de seus elementos, estiver em domínio público sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.• Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:<ul style="list-style-type: none">• Limitações e exceções aos direitos autorais ou quaisquer usos livres aplicáveis;• Os direitos morais do autor;• Direitos que outras pessoas possam ter sobre a obra ou sobre a utilização da obra, tais como direitos de imagem ou privacidade. <p>Aviso — 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 <i>link</i> para (http://creativecommons.org/licenses/by-nc-sa/2.5/br/deed.pt_BR).</p> <p>Observamos ainda que a responsabilidade pela autoria dos textos e imagens desta obra é exclusivamente do autor.</p>	

Brasil. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação.

Panorama da interoperabilidade no Brasil / Ministério do Planejamento, Orçamento e Gestão, Secretaria de Logística e Tecnologia da Informação. Org. Cláudia S. F. Mesquita e Nazaré L. Bretas. - Brasília : MP/SLTI, 2010.

251 p.: il. color.

ISBN 978-85-89199-07-0

1. Interoperabilidade - Serviço Público. 2. Informática – Arquitetura e-PING 3. Software Público. I. Título. II. Mesquita, Cláudia do Socorro Ferreira. III. Bretas, Nazaré Lopes.

CDU 316.776:35

Títulos para indexação:

Em Inglês: Overview of Interoperability in Brazil

Em Espanhol: Panorama de la Interoperabilidad en Brasil

Presidente da República
Luiz Inácio Lula da Silva

Ministro do Ministério do Planejamento Orçamento e Gestão

Paulo Bernardo Silva

Secretaria de Logística e Tecnologia da informação – SLTI

Loreni F. Foresti – Secretária Substituta

Chefe de Gabinete

Maria Lúcia de Carvalho Porto

**Departamento de Gestão Estratégica da
Informação – DGEI**

Clesito Cezar Arcoverde Fechine

Departamento de Governo Eletrônico – DGE

João Batista Ferri de Oliveira

**Departamento de Integração de Sistemas de
Informação - DSI**

Nazaré Lopes Bretas

**Departamento de Logística e Serviços Gerais –
DLSG**

Januário Flores

Departamento de Serviços de Rede – DSR

Antonio Carlos Alff

**Departamento Setorial de Tecnologia da
Informação – DSTI**

Fernando Antônio Braga de Siqueira Júnior

Colaboradores

Marcelo Martins Villar

Marcus Borges de Souza

Revisores Técnicos

Alex Pires Bacelar

Cláudia do Socorro Ferreira Mesquita

Corinto Meffe

Danielle Eulália Lelis dos Santos

Dayse Vianna

Fábio Gomes Barros

Fernando Almeida Barbalho

Flávio Soares Corrêa da Silva

Hime Aguiar e Oliveira Junior

Jose Ney de Oliveira Lima

Marcello Alexandre Kill

Marcos Antonio André da Rocha

Paulo Roberto da Silva Pinto

Raul Coelho Soares

Renan Mendes Gaya Lopes dos Santos

Sérgio Augusto Santos de Moraes

Xênia Soares Bezerra

Yuri Fontes de Oliveira

Sumário

Caminhos para interoperabilidade	13
A construção da e-PING situação atual e desafios	14
Desenvolvimento e implementação da arquitetura e-PING estratégias adotadas e possíveis implicações	22
Inovação e interoperabilidade	37
Padrões tecnológicos: o uso na prestação de serviços públicos e no relacionamento com o Governo Federal	50
Interação Estado/academia para a inovação em governo eletrônico no Brasil.....	64
Interoperabilidade semântica no LexML	74
Software público e interoperabilidade: uma oportunidade internacional para a produção compartilhada de conhecimento	80
Fatores críticos de segurança em <i>web services</i>	91
ICP-Brasil: sigilo e conhecimento	113
A integração de dados no âmbito do Macroprocesso de Planejamento, Orçamento e Finanças	117
Para além da e-PING: o desenvolvimento de uma plataforma de interoperabilidade de e-Serviços no Brasil.....	137
Experiências de interoperabilidade	159
Estruturação da ASI-PE por meio da orientação a serviços	160
Interoperabilidade do Infrasing-UFRN/MJ com os sistemas estruturantes do Governo Federal	176
e-STF processo eletrônico: Integração do Supremo com os demais órgãos do Poder Judiciário e da Administração Pública	194
SIMEC: uma mudança na cultura de gestão integrando informações setoriais estratégicas	201
AR – um modelo de interoperabilidade aplicado ao monitoramento do PAC	211
Sistema de gestão de convênios – SICONV interoperabilidade via <i>web services</i> no contexto do MDA	217
Sistema georreferenciado de gestão ambiental da Bahia – GEOBAHIA ferramenta de integração na gestão ambiental	227
Interoperabilidade no segmento de geotecnologias: semântica, metadados, serviços e formatos abertos	236
Projeto LexML Brasil	242

CAMINHOS PARA INTEROPERABILIDADE



ICP-Brasil: Sigilo e Conhecimento

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)¹ é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação do cidadão. Este artigo faz breve reflexão acerca de sigilo e conhecimento para abordar a definição de um dos padrões tecnológicos de segurança na Internet.

1. A idéia de criação de uma infraestrutura de chave pública para o Governo surgiu como ponto principal do grupo de trabalho de Segurança de Informação da Câmara Técnica de Serviços de Rede – gt3/CTSR, com vigência de julho a dezembro de 1999, sob gerência da SLTI/MP, com a participação dos órgãos: Ministério da Aeronáutica, Ministério do Planejamento Orçamento Gestão, Ministério do Exército, Ministério das Relações Exteriores, Ministério da Ciência e Tecnologia, Ministério da Fazenda/Serpro, Ministério das Comunicações/ Empresa de Correios e Telégrafos, Presidência da República/CEPESC.

“Ciencia y máquina fueron alejándose hacia un olimpo matemático, dejando solo y desamparado al hombre que les había dado existencia.”

(Ernesto Sabato)

Gostaria de afirmar, inicialmente, uma tese: discriminar ou evitar o compartilhamento de informações tem um caráter anti-intuitivo. De forma mais direta, quero dizer tão somente que nosso modo de ser se dispõe antes pela difusão e compartilhamento da informação e do conhecimento, que pelo seu *sigilo*. É, por conseguinte, natural nas organizações humanas, que desejemos a difusão do conhecimento. Tanto mais dinâmica ela é quanto mais o conhecimento se difunde. Podemos considerar, de certa forma, tal assertiva como bastante consensual. Ou seja, queremos vivamente que nossas organizações possuam mecanismos claros e bem definidos de difusão e compartilhamento da informação.

Não insistirei nesse ponto, até por seu aspecto consensualíssimo. Assim sendo, seria inconcebível, numa dada organização, que o setor X estivesse trabalhando no tema “A” e o setor Y trabalhando no mesmo tema “A” e tais segmentos da organização não compartilhassem nenhuma informação vital sobre o referido tema. Se os setores “X” e “Y” somente compartilhassem informações *periféricas*, já seria um desconforto na visão da avassaladora maioria de gestores e administradores. É consenso, creio, que uma organização hodierna faça o conhecimento fluir entre seus segmentos e setores. E cada vez mais usamos as ferramentas da infraestrutura da informação, tais como as redes computacionais, para este desiderato, e toda uma gama de sistemas e *softwares* para realizar tal objetivo.

Não considero, por outro lado, um problema predominantemente técnico ou de aparatos tecnológicos. Ainda que nestes casos sempre tendamos a observar *apenas* o “técnico” do problema e a descurarmos do lado *peopleware* do problema. Num livro clássico sobre o problema, pode-se ler:

A principal razão que nós tendemos a focar sobre o lado técnico antes que do lado humano do trabalho não é porque é mais crucial, mas porque é mais fácil de fazê-lo.¹

As “interações humanas são complicadas”, dizem os autores, e, mais ainda, nunca seus efeitos são *limpos* e *claros*, isto é, objetivamente definíveis. Entretanto, elas têm um gigantesco peso no mundo do trabalho e suas organizações.

O modo de ser do homem é o da comunicação e do compartilhar, do dividir, e, por fim, a informação — em regra geral, pode-se dizer que tendemos ontologicamente à comunicação. Por isso mesmo, a informação é *ponto de chegada* e não *ponto de partida*. Ponto de partida é, isto sim, a tendência do homem ao compartilhamento. Talvez seja possível aqui parafrasear a famosa sentença de Aristóteles, que diz: “todos os homens por natureza desejam conhecer”. Poder-se-ia asseverar, não em discordância, mas em complementação, que todos os homens, por natureza, desejam compartilhar, ou ainda: desejam, ao conhecer, compartilhar seus frutos.

1. Demarco e Lister (1999, p. 5).

O contrário do compartilhamento deve ser resultado de certo esforço — poder-se-ia dizer: de esforço significativo. Por isso, cheguei a falar anteriormente em *contraintuitividade*: é contraintuitivo no ser humano a “não comunicabilidade” em todos os seus aspectos, principalmente o do compartilhar. Mesmo que, por vezes, em uma comunidade de comunicação não estejamos tacitamente dispostos a dividir e compartilhar *soluções* de problemas. Por conseguinte, o segredo (*secrecy*) e o compartilhar podem ser definidos dentro do jogo “claro-escuro”, pois algo denominado *secreto* é uma “motivação autoconsciente e identificável para colocar alguém na escuridão (*dark*) sobre algo em particular”².

Afirmei, anteriormente, o caráter ontológico dessa comunicabilidade, ainda que a expressão, à primeira vista, possa confundir o leitor. Com isso, quero afirmar apenas que ferramentas e tecnologia ajudam, mas não determinam essa disposição. Aquelas são consequências destas — aquelas são o periférico, esta o essencial. As organizações, sejam complexas ou não, se utilizam de ferramentas, *softwares* e sistemas (mesmo toda uma *arquitetura*), e a rede em si, para aproximar e potencializar a disposição que temos de compartilhar. Todas as capacidades e potencialidades da “comunicação mediada por computadores”³ confirmam essa disposição e, na infraestrutura da informação, vimos o aparecimento de toda uma complexa rede de comunidades. Com efeito, boas plataformas tecnológicas (*wikis*, *CVSs*, *groupwares* etc.), boas metodologias, agudizam tal “tendência”, fazem-na mais fácil e simples e, por fim, radical.

Deve ser resultado de certo esforço desejar que um indivíduo, numa dada comunidade ou organização, *não divida*, por algum mecanismo, uma informação a que teve ou tem acesso. Aqui, talvez plataformas de *softwares* não sejam tão disponíveis em nossos dias, ainda que devêssemos considerar “sistemas de controle de acesso”, “sistemas de privilégio”, por exemplo, como algo que realizaria esses objetivos. Devem ser consideradas, realizando tal desiderato, *plataformas de identificação* robustas, isto é, plataformas que podem realizar uma forma de identificação inequívoca e forte. Poder-se-ia chamá-la também de “plataforma de identificação universal”⁴. Considerando-se, portanto, algo como exequível e desejável, ainda que alguns especialistas a contestem em defesa da falsa cobertura do anonimato. Diz ainda Jürgen Habermas, em recente trabalho⁵, que o mundo WWW surge de forma livre para apaziguar, com a comunicação internet, as fraquezas do caráter anônimo e assimétrico da comunicação de massa. Enquanto isso permite, segundo o mesmo autor, a reentrada de elementos interativos e deliberativos num intercâmbio não regulado entre interlocutores. Portanto, já em 1998 Habermas, em ensaio sobre *o curto século 20*, asseverara que, por fim, a “comunicação digital ultrapassa todas as outras mídias em riqueza e capacidade”⁶, e todo esse potencial explica exatamente por que os seres humanos, de forma mais rápida e massiva, podem fornecer e compartilhar múltiplas informações.

2. Sheppele (1988, p. 13).

3. Rheingold (1994, p. 5ss.).

4. Na visão de Bruce Schneier a “identificação universal é impossível”, (ver em “*Schneier-Ranum Face-Off: Should we ban anonymity on the Internet?*”); a meu ver a posição de Marcus Ranum é a correta ao asseverar que “*It's unfortunate that in the present environment anyone who wants to advocate Internet anonymity is largely serving a constituency of scammers, spammers and shells*”. Disponível em: <http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1380347,00.html>.

5. Habermas (2008, p. 161).

6. *Idem*, 1998, p. 71.

A plataforma que nos referimos anteriormente é, por isso mesmo, uma espécie de infraestrutura. Para uma plataforma de identidade ou identificação forte, podemos falar em “Infraestrutura de chaves públicas”⁷. Trata-se de um dos padrões tecnológicos que estabelecem os alicerces da segurança na internet, recebendo vigorosa implementação, técnica e institucional, em nosso país, no biênio (2006-2007) e com perspectiva crescente.

É, por conseguinte, um amplo conjunto de acordos e padronização internacionais, uma estrutura entre diferentes Autoridades Certificadoras e, enfim, métodos e protocolos para emitir, validar e revogar certificados digitais através de uma LCR (Lista de certificados revogados ou *Certificate Revocation List*). Um certificado digital nada mais é do que arquivos digitais que estabelecem um elo entre uma “entidade final”, seja uma empresa ou um indivíduo, e uma *autoridade* que tem o poder de certificação, também chamada de *trusted third part*. O “terceiro confiável” dessa relação verifica a identidade do sujeito e emite o certificado digital, segundo padrões tecnicamente concebidos e institucionalmente regulados. Tais certificados são de chave pública e asseguram que uma determinada chave pública pertence a um sujeito e que a AC possui sua própria chave privada correspondente.

REFERÊNCIAS

DEMARCO, T.; LISTER, T. **Peopleware**. Productive Projects and Teams. 2nd ed. New York: Dorset House Publishing, 1999, p. 5.

HABERMAS, J. **Ach, Europa**. Frankfurt am Main: Suhrkamp, 2008, p. 161.

_____. **Die Postnationale Konstellation**. Politische essays. Frankfurt am Main: Suhrkamp, 1998, p. 71.

MARTINI, R. **Ensaio sobre tecnologia, sociedade e segurança**. Rio de Janeiro: Brasport, 2008.

RHEINGOLD, H. **The Virtual Community**. Homesteading on the Electronic Frontier. New York: HarperPerennial, 1994, p. 5ss.

SCHNEIER, B.; RANUM, M. **Schneier-Ranum Face-Off**: Should we ban anonymity on the Internet? Disponível em: <http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1380347,00.html>.

SHEPPELE, K. L. **Legal Secrets**: equality and efficiency in the common law. Chicago: The University of Chicago Press, 1988, p. 13.

7. Consultar nossos estudos em trabalho recentemente publicado: *Tecnologia e Cidadania Digital*. Ensaio sobre tecnologia, sociedade e segurança. Rio de Janeiro: Brasport, 2008.