Um Estudo Comparativo de Estratégias Nacionais de Gestão de Identidades para Governo Eletrônico

Glaidson Menegazzo Verzeletti[1,2], **Michelle Silva Wangham**[1], **Emerson Ribeiro de Mello**[2], **José Alberto Sousa Torres**[3]

[1]Universidade do Vale do Itajaí (UNIVALI) – SC – Brasil

[2]Instituto Federal de Santa Catarina – SC – Brasil

[3]Ministério da Justiça – DF – Brasil

{glaidson.verzeletti, mello}@ifsc.edu.br,

wangham@univali.br, alberto.torres@mj.gov.br

Resumo. *A adoção de programas de Governo Eletrônico (e-Gov) é uma importante ferramenta para promover a transparência dos gastos públicos e o acesso eficiente aos serviços. Para muitos países, é fundamental conceber sistemas de gestão de identidades que ofereçam a autenticação única e o acesso seguro dos cidadãos as aplicações de e-Gov. O presente trabalho descreve e analisa as estratégias nacionais de gestão de identidade dos dez primeiros países do ranking da ONU sobre e-Gov. Por fim, é apresentado um comparativo sobre estas estratégias, destacando as características e soluções comumente adotadas.*

Abstract. *The adoption of e-Gov programs is an important tool for promoting transparency of public expenditure and efficient access to services. To many countries, it is fundamental to conceive Identity Management systems (IdM) that offer single sing-on and also secure access to e-Gov applications by citizens. This paper describes and analyzes national IdM strategies of the top 10 countries on the The United Nations E-Government Survey. Finally, we describe a comparative analysis of these national strategies, highlighting the characteristics and solutions commonly adopted by these countries.*

1. Introdução

O desenvolvimento de programas de Governo Eletrônico (e-Gov) tem como princípio a utilização das tecnologias de informação e comunicação (TICs) para democratizar o acesso à informação, ampliar discussões, promover a transparência e responsabilização das ações e gastos públicos e dinamizar a prestação de serviços públicos, com foco na eficiência e efetividade das funções governamentais [Dawes and Pardo 2002]. Segundo [United Nations 2014], o governo eletrônico é uma importante ferramenta para revitalizar a administração pública tanto no nível nacional quanto local. Nos programas de e-Gov, as colaborações podem ser de cinco formas: entre organizações públicas (G2G), entre organizações públicas e o terceiro setor, entre organizações públicas e privadas (G2B), entre o governo e o cidadão (G2C) e entre governo e seus funcionários (G2E).

Um ponto chave para os programas nacionais de e-Gov é a criação de um sistema de identificação, de autenticação e de autorização de usuários. Esses sistemas são conhecidos como sistemas de gestão de identidades (*Identity Management Systems* – IdM)

[Baldoni 2012]. A gestão de identidades pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização, contabilização e auditoria [ITU 2009].

Possibilitar que as aplicações de e-Gov tenham suporte ao processo de autenticação única (*Single Sign-On* – SSO) de usuários é uma facilidade de interesse de muitos países. Porém, boa parte das instituições do governo ainda não formalizaram este processo e, por isto, duplicam o cadastro de pessoas já registradas. A privacidade dos cidadãos é um outro problema a ser tratado nas estratégias nacionais de IdM [Hansen et al. 2008]. Em um cenário ideal, os usuários devem exercer o direito de determinar como suas informações serão manipuladas, quais atributos poderão ser compartilhadas com terceiros, como esse compartilhamento deve ser feito e o período de tempo que essas informações ficarão disponíveis nos sistemas.

Os sistemas de gestão de identidades são complexos, com características poderosas, porém, com algumas vulnerabilidades que podem ser exploradas. Garantir a segurança sem comprometer a privacidade dos usuários e os requisitos não funcionais de usabilidade e de desempenho é um grande desafio no projeto destes sistemas e na concepção de uma estrategia nacional de IdM [Dhamija and Dusseault 2008].

Segundo a Organização para Cooperação e Desenvolvimento Econômico (*Organisation for Economic Cooperation and Development* – OECD), vários países já iniciaram alguma ação em relação à gestão de identidades. As ações de IdM de dezoito nações que fazem parte da OECD foram descritas e analisadas em um relatório [OECD 2011] que apresenta a visão, políticas e estratégias nacionais para gestão de identidades.

Este artigo temo como objetivo descrever e analisar as estratégias nacionais de gestão de identidades dos dez primeiros países do ranking da ONU de Governo Eletrônico [United Nations 2014]. A Seção 2 apresenta as principais características do países analisados e alguns conceitos sobre gestão de identidades e sobre ações de IdM. Uma descrição das estratégias de IdM dos dez países são apresentadas na Seção 3 e uma análise comparativa destas estratégias é descrita na Seção 4. Por fim, na Seção 5, são apresentadas as considerações finais.

2. Aspectos sobre Gestão de Identidade em Programas de e-Gov

A cada dois anos o Departamento de Assuntos Econômicos e Sociais da ONU conduz uma pesquisa sobre o desenvolvimento do e-GOV dos 193 Estados membros. O relatório gerado serve como ferramenta para identificar os pontos fortes e desafios dos programas nacionais e para orientar as políticas e estratégias de e-Gov. A publicação também destaca as novas tendências, questões e práticas inovadoras, bem como os desafios e oportunidades de desenvolvimento de e-Gov [United Nations 2014].

A Tabela 1 apresenta os dez primeiros países do rank da ONU de 2014, suas posições na pesquisa anterior, seus respectivos continentes, os seus índices de desenvolvimento de e-Gov (EGDI), as suas posições no rank que avalia o grau de participação dos cidadãos nas aplicações de e-Gov e no rank de serviços *on-line* que estes países oferecem.

Identidade pode ser definida como um conjunto de dados que representam uma entidade dentro de um determinado contexto. Alguns destes dados podem identificar

Tabela 1. Características dos Países Analisados

Rank (2012)	Rank (2014)	País	Região	EGDI (2014)	Rank e-Particip.	Serviços online
1	1	Coréia do Sul	Asia	0,9462	2	3
12	2	Austrália	Oceania	0,9103	7	7
10	3	Singapura	Asia	0,9076	10	2
6	4	França	Europa	0,8938	4	1
2	5	Holanda	Europa	0,8897	1	8
18	6	Japão	Asia	0,8874	5	4
5	7	EUA	Américas	0,8748	9	5
3	8	Reino Unido	Europa	0,8695	6	10
13	9	Nova Zelândia	Oceania	0,8644	20	14
9	10	Finlândia	Europa	0,8449	25	18

unicamente uma entidade (p.ex. número do CPF) e outros não (p.ex. data de nascimento) [Wangham et al. 2010].

Um sistema de gestão de identidades consiste na integração de tecnologias, políticas e processos de negócio, resultando em um sistema de autenticação de usuários aliado a um sistema de gestão de atributos. [Bhargav-Spantzel et al. 2007] classificam os sistemas de gestão de identidades (IdM) em quatro modelos: tradicional ou isolado, centralizado, federado e centrado no usuário.

No modelo tradicional, tarefas de autenticar usuários (*Identity Provider* – IdP) e prover serviço (*Service Provider* – SP) são realizadas por um mesmo servidor. No modelo centralizado, as tarefas de IdP são realizadas por um único servidor dentro de um domínio administrativo. O provimento de serviços é realizado por um ou mais SPs, os quais possuem relações de confiança com o IdP, garantindo assim que as identidades de usuários são válidas somente dentro deste domínio administrativo. Nos modelos federado e centrado no usuário, também existe uma separação dos papéis de autenticar e prover um serviço. Contudo, as relações de confiança entre IdPs e SPs ultrapassam os limites de domínios administrativos. Isto permite que usuários de uma determinada instituição possam acessar serviços oferecidos em domínios administrativos diferentes [Wangham et al. 2010].

A transposição de informações sobre identidades de usuários de um domínio para outro só é possível se houver uma linguagem padrão para expressar estes dados em ambos os domínios. Em 2005, a OASIS lançou um conjunto de especificações para a troca dinâmica de asserções de segurança baseada no XML. A *Security Assertion Markup Language* (SAML) [OASIS 2005] foi concebida para permitir a troca de informações de autenticação e autorização e garantir o conceito de autenticação única (SSO).

Para muitos países, o desenvolvimento de uma estratégia nacional de IdM é fundamental para a realização do e-Gov. Como estratégia, muitos indicam a necessidade de oferecer serviços com processos de autenticação que exijam credenciais de segurança robustas. A adoção de um sistema de IdM comum permite harmonizar a gestão de identidades em nível nacional. Isto implica em reduzir ou limitar o número de identidades que cada cidadão precisa ter para interagir com os diversos serviços oferecidos pelo governo.

Em suma, grande parte das estratégias dos países buscam reduzir o número de

contas que seus cidadãos precisarão gerenciar e até minimizar a quantidade de vezes que precisarão passar pelo processo de autenticação para ter acesso aos serviços. As soluções adotadas, ou que estão em estudo, geralmente partem da ideia de evoluir práticas e regulamentos usados na identificação tradicional, também chamada de *off-line*.

Segundo [OECD 2011], as políticas descrevem um conjunto de ferramentas que possibilita a implantação da estratégia. As políticas sobre registro dos cidadãos indicam como estabelecer e ligar as identidades eletrônicas com cada cidadão. O processo de registro pode ser centralizado, em países onde a administração pública local é menos autônoma; descentralizado ou federado, em países que dão mais autonomia para a administração local de cada região.

O relatório da [OECD 2011] indica que as políticas que possibilitam a adoção de identidades digitais podem ser voluntárias ou obrigatórias e a escolha entre uma destas está diretamente relacionada com a forma com que cada país opera seus meios de identificação *off-line*.

3. Estratégias Nacionais de Gestão de Identidades

Esta seção apresenta a situação sobre o desenvolvimento e implantação de estratégias nacionais para a gestão de identidade.

3.1. Coreia do Sul

A Coreia do Sul segue o modelo de gestão de identidade centralizada, sendo que todos os cidadãos coreanos possuem um Número de Registro de Residente (RRN) único. O RRN é composto por 13 dígitos e inclui informações como a data e local de nascimento. Desde sua implantação, o RRN tem sido amplamente utilizado em sistemas *on-line*, tanto para interações com o setor público quanto com o setor privado [OECD 2011].

Desde 1999, a estratégia de IdM coreana incentiva o uso de credenciais digitais baseadas em Infraestrutura de Chave Pública (ICP) e, desde 2005, promove o uso de um identificador digital seguro (*i-Personal Identification Number* – i-PIN), tendo como base o RRN. Este sistema de identificação pessoal foi desenvolvido para resolver problemas de segurança relacionados ao roubo de identidade e ao crescente aumento das violações de privacidade e crimes *on-line* [OECD 2011].

3.2. Austrália

O gerenciamento de identidade na Austrália é baseado em uma política de cadastramento descentralizada, sendo um dos principais pontos da estratégia nacional de segurança de identidade manter e tentar fortalecer as credenciais atualmente utilizadas. Documentos de prova de identidade, como passaporte ou carteira de motorista, são emitidos por departamentos específicos sem que haja a necessidade legal de interoperabilidade entre estes sistemas.

Na falta de um identificador único nacional, o documento de boas práticas em e-autenticação australiano permite às agências a utilização dos modelos em silo, centralizado e federado no provimento de autenticação para os seus serviços online.

Em 2007, foi criado o Serviço Nacional de Verificação de Documentos (*Document Verification Service* – DVS), com o intuito de ser usado por órgãos do governo e, potenci-

almente, pelo setor privado. Este serviço permite que agências do governo possam verificar se um documento apresentado pela pessoa foi realmente emitido pelo órgão de origem e se o mesmo foi cancelado ou roubado. Passaportes, vistos e carteiras de motorista são alguns exemplos de documentos que podem ser verificados pelo DVS [OECD 2011]. Em maio de 2014, o procurador geral anunciou o lançamento do DVS comercial, na conferência CeBIT[1] na Austrália. De forma rápida, segura e confiável este produto comercial está sendo expandido para o setor privado, o que permitirá às empresas proteger-se contra os crimes de identidade [Australian Government 2014].

3.3. Singapura

Singapura iniciou seu projeto de e-Gov na década de 80 com o objetivo de transformar o governo em um modelo mundial em termos de tecnologia da informação. No final dos anos 90, houve uma convergência das políticas de TIC o que permitiu abrir o caminho para a criação do plano de ação e-Gov I (2000-2003) e para o plano de ação II (2003-2006). O principal objetivo do primeiro plano era criar o maior número possível de serviços públicos *on-line*, enquanto a ênfase para o segundo foi melhorar a experiência dos usuários no uso dos serviços [Infocomm Development Authority of Singapore 2014].

Fatores como a alta renda per capita (US$ 47,210)[2], população pequena e a entrada dos dispositivos móveis no mercado, favoreceram o desenvolvimento e o acesso aos sistemas de governo, principalmente nas modalidades G2C e G2B. Desde de 2003, todos os residentes de Singapura com idade igual ou superior a quinze anos podem fazer uso de uma credencial única para realizar transações nos diferentes sistemas do governo, serviço este denominado *SingPass ID/password* [Infocomm Development Authority of Singapore 2014].

Desde 2009, empresas, sociedades, instituições de saúde, sindicatos, entre outros, que estão registradas em Singapura, passaram a utilizar uma identificação única (*Unique Entity Number - UEN*) para as interações com o governo. Dentre os benefícios trazidos pela UEN[3] para as entidades, estão a facilidade na apresentação de declarações fiscais, envio de contribuições de empregados e a aplicação de licenças de importação e exportação [Singapore Government 2008]. Atualmente, cidadãos e empresas podem acessar mais de 1.600 serviços *on-line* e mais de 300 serviços providos pelo governo da Singapura [IDA Singapore 2014].

3.4. França

Na França, todo provimento de serviços *on-line* para os cidadãos e empresas é feito a partir de um portal do governo[4], sendo que o processo de autenticação exige certificados digitais emitidos por provedores de serviços de certificação (CSPs) qualificados pelo governo e avaliados em função dos requisitos exigidos pelo "Framework Geral de Segurança" (*Référentiel Général de Sécurité - RGS*) [European Comission 2014b]. O RGS provê atualmente três níveis garantia de segurança (*Level of Assurance - LoA*): elementar[5], padrão

[1] http://www.cebit.com.au/conferences
[2] Singapore Police Force, 2013. Disponível em: http://www.spf.gov.sg/sms70999
[3] http://www.uen.gov.sg
[4] www.service-public.fr
[5] Nível Elementar: assinatura pode ser armazenada em um módulo de software.

e reforçado[6] [France Government 2013].

Em 2005, o governo da França iniciou o projeto (*Identité Nationale Electronique Sécurisée* – INES) com o intuito de criar um cartão de identidade eletrônico. O cartão eID contém informações pessoais, como por exemplo nome completo, data de nascimento e endereço, além de guardar informações que podem ser usadas em processos de autenticação mais robustos, como informações biométrica, certificado digital e assinatura eletrônica [European Comission 2014b].

O governo optou por não tornar obrigatório a adoção deste cartão para seus cidadãos, porém, de acordo com o plano de desenvolvimento para a economia digital de 2012, o governo Francês pretende fazer uso deste cartão para permitir aos seus cidadãos participar de processos de decisão pública [European Comission 2014b]. Desta forma, apesar de não ser obrigatório, o governo espera que a população busque pelo cartão, uma vez que o mesmo lhe dará direito a voz nos processos de decisão do governo.

3.5. Holanda

A estratégia holandesa de IdM está baseada no DigiD[7], um mecanismo nacional de identidade e autenticação digital para transações eletrônicas entre cidadãos e empresas com órgãos públicos [OECD 2011].Atualmente, o sistema oferece duas formas para realizar a autenticação: *DigiD Basic* – que faz uso somente de nome de usuário e senha; *DigiD Medium* – que além do nome de usuário e senha também exige uma verificação por meio de mensagens SMS.

O objetivo é que o DigiD se torne o sistema de autenticação utilizado na administração pública para prestar serviços eletrônicos aos cidadãos. Apesar da adoção não ser obrigatória, mais de 9,8 milhão de holandeses já ativaram a sua conta DigiD, que pode ser utilizada em mais de 600 organizações governamentais ou empresas privadas que executam serviços públicos [OECD 2011].

O governo está trabalhando em um programa chamado “eRecognition para empresa” com o objetivo de permitir que o DigiD seja usado também nas interações com empresas privadas (G2B). O eRecognition oferecerá diferentes mecanismos de autenticação, desde combinações de nome de usuário e senha até soluções baseadas em ICP [European Comission 2014c].

3.6. Japão

Atualmente todo cidadão japonês deve se cadastrar no sistema de Registro de Residente Básico, fornecendo aos governos municipais informações como: nome, data de nascimento, sexo e endereço físico. Em 2002, estas quatro informações começaram a alimentar o sistema JUKI-NET, criado para compartilhar dados entre os órgãos governamentais, nascendo assim o modelo centralizado de gestão de identidade no país. Este sistema tem como base os dados registrados em 3.200 municípios, oferecendo aos cidadãos a opção de obter o cartão de identificação (*My Number*)[8], o qual faz parte da estratégia nacional de oferecer uma identificação única a todo cidadão a partir de 2015 [Rebecca Bowe 2012].

[6]Nível Padrão e Reforçado: a chave de assinatura é armazenada em um dispositivo criptográfico de hardware, como um *smart card* ou uma chave USB.

[7]https://www.digid.nl

[8]Cartão com chip, que contém as informações de registro obrigatórias, foto e número de identificação.

Segundo projeto de lei aprovado em 2013 pela Câmara dos Deputados, a partir de 2016 todo cidadão japonês deverá possuir um cartão *My Number*. Este cartão será usado para compartilhar informações entre as agências que administram seguro social, impostos e programas de mitigação de desastres [Yumi Watanabe 2014]. Com o objetivo de expandir o uso para outras áreas, em 2018 o processo passará por uma avaliação.

3.7. Estados Unidos

Em 2003, os Estados Unidos decidiram adotar o modelo de identidades federadas, voltado para órgãos públicos ou entidades da iniciativa privada. A federação é baseada em quatro níveis de garantia e o cidadão, ao tentar acessar um serviço governamental, é direcionado para uma lista de provedores de identidade que possuem a garantia necessária para acesso àquele serviço específico. Em 2009, cerca de 27 agências americanas já proviam os seus serviços com base na federação [Seltsikas and van der Heijden 2010].

O conceito chave adotado pelo governo dos Estados Unidos é a participação voluntária de indivíduos e de organizações. Segundo o [OECD 2011], o governo não impõe o aceite de soluções específicas, p.e. uso de certificados digitais para autenticar pessoas ao realizarem transações *on-line* com o governo. As políticas específicas de segurança para a estratégia de IdM *on-line* ainda estão sendo escritas, entretanto, tem-se como diretrizes de segurança o uso de criptografia forte, padrões abertos, como por exemplo o SAML, e a adoção de sistemas de informações que possam ser auditáveis [OECD 2011].

3.8. Reino Unido

O portal *Website Government Gateway* permite aos cidadãos fazerem seu registro inicial, fornecendo informações pessoais, além de sua senha. Como resultado, o cidadão recebe um código de segurança (PIN) por meio de correspondência em sua residência. Este código é então usado pelo cidadão para usufruir de alguns dos serviços *on-line* oferecidos pelo governo. Alguns serviços, por serem considerados mais críticos, podem possuir mecanismos de autenticação mais rígidos, exigindo por exemplo, autenticação biométrica ou por meio de certificados digitais [European Comission 2014d].

O ano de 2012 marcou uma mudança radical no desenvolvimento do governo eletrônico do Reino Unido, já que foi o ano que iniciou o Programa de Garantia de Identidade (IDAP), capitaneado pelo Gabinete do Primeiro Ministro. Por meio deste programa, o governo pretende oferecer um meio mais seguro para os cidadãos provarem a sua identidade ao interagir com os serviços de governo eletrônico.

O modelo utiliza um "hub" que permite que diferentes provedores de identidade autentiquem os indivíduos para os provedores de serviço sem que seja necessário que o governo armazene de forma centralizada os dados pessoais dos usuários e sem que a privacidade seja afetada por trocas desnecessárias de dados ou por compartilhamento indevido dos dados do usuário sem o seu consentimento.

A primeira etapa do programa foi definir quais seriam os provedores de identidade. Para isso, o governo realizou um processo licitatório que terminou com a contratação de cinco empresas - Digidentity, Experian, Mydex, The Post Office e Verizon. É interessante ressaltar que, neste modelo, os próprios provedores de identidade efetuam os cadastros dos usuários, recebendo do governo por cada usuário cadastrado. A segunda etapa é marcada pela difusão da utilização do serviço dos provedores de identidade entre os órgãos governamentais [Government Digital Service 2014].

3.9. Nova Zelândia

Optou-se por uma estratégia de IdM visando acelerar o desenvolvimento e oferta de serviços *on-line* para seus cidadãos. Foi adotada uma política de registro descentralizada, sendo que cada governo local tem autonomia para indicar como registrar seus cidadãos, bem como para indicar quais mecanismos de autenticação podem ser usados nos serviços.

A chave de sucesso para a implantação da solução de IdM foi a adoção do *e-Government Interoperability Framework* (e-GIF), também conhecido como NZ e-GIF, lançado em 2002 [OECD 2011]. O e-GIF possui uma versão própria do SAML (NZ SAML), sendo que a primeira versão do *framework* teve como foco a autenticação e as versões subsequentes em atributos e autorização [Kãwanatanga 2008].

3.10. Finlândia

O "Sistema de Informação da População" é o responsável pelo cadastro nacional dos cidadãos finlandeses e dos cidadãos estrangeiros com residência permanente no país, o qual é mantido pelo Centro de Registro da População (CRP) e pelos cartórios locais. O CRP é a única autoridade certificadora na Finlândia capaz de realizar a emissão de certificados Pan-Europeus [European Comission 2014a], sendo o responsável pela emissão de identidades eletrônicas (eID) e dos certificados digitais para os cidadãos (FINeID[9]). Somente a partir destas credenciais, é possível acessar os serviços de e-Gov.

4. Comparação e Análise das Estratégias Nacionais

Segundo a [OECD 2011], os países encontram-se em diversos estágios em relação ao desenvolvimento e implementação das estratégias nacionais de IdM. A partir do **desenvolvimento de políticas** (definição de leis, planos, ações, etc), os governos conseguem **implementar suas estratégias de IdM**. Na Tabela 2, são apresentados os países de acordo com o estágio de desenvolvimento e implementação das suas estratégias.

Tabela 2. Status estimado para as Estratégias Nacionais de IdM [OECD 2011]

ESTÁGIO	DESENVOLVIMENTO	IMPLEMENTAÇÃO
Não iniciado	Japão	Japão, Estados Unidos
Estágio Inicial	Estados Unidos	Austrália, Nova Zelândia
Em Andamento		Coreia do Sul, Holanda
Estágio Final	Austrália	
Totalmente Desenvolvida	Coreia do Sul, Nova Zelândia	

Alguns países, como o Japão por exemplo, mostram sinais de evolução em relação ao estágio de desenvolvimento e implementação de suas estratégias, podendo ser classificado como "em andamento" e "estágio inicial", respectivamente. Porém, esta classificação só poderá ser realmente reavaliada entre 2015 e 2016, após as políticas do "*My Number*" serem de fato colocadas em prática. Por outro lado, a Coreia do Sul está com suas estratégias totalmente desenvolvidas e avança para o estágio final de implementação. Ainda de acordo com [OECD 2011], estes países procuram focar suas estratégias de Governo Eletrônico na administração pública, esperando que estas sejam adotadas pelo setor privado. Vale destacar que Singapura, França e Finlândia, foram países que não participaram da pesquisa da OECD e, por isto, o estágio de suas estratégias não estão indicados acima.

[9]Sistema de certificados do CRP, baseado em uma Infraestrutura de Chave Pública.

Tabela 3. Comparativo entre países

PAÍS	MODELO IdM	Id ÚNICO	SAML 2.0	Participação E. Privadas	Participação Cidadão
Coréia do Sul	Centralizado	Sim	Sim	Sim	Obrigatória
Austrália	Federado	Não	Sim	Sim	Voluntária
Singapura	Centralizado	Sim	-	Sim	Voluntária
França	Centralizado	Sim	-	Sim	Voluntária
Holanda	Centralizado	Sim	Sim	Sim	Voluntária
Japão	Centralizado	Sim	-	Não	Obrigatória
EUA	Federado	Não	Sim	Sim	Voluntária
Reino Unido	Federado	Sim	Sim	Não	Voluntária
Nova Zelândia	Federado e Centrado no usuário	Não	Sim	Não	Voluntária
Finlândia	Centralizado	Sim	-	Sim	Voluntária

A Tabela 3 resume e compara algumas características das estratégicas de gestão de identidade dos países analisados. Pode-se observar que a maioria dos países adota o SAML como padrão e, normalmente, é utilizado um identificador único para o acesso aos sistemas. A participação de entidades privadas e não-governamentais é geralmente incentivada, muito embora se observa nos países que não têm estratégias implementadas para este segmento, algumas iniciativas do governo em estender as políticas de G2B.

Embora não seja uma regra, nota-se a adoção de modelos de IdM centralizado ou federado, sendo que a participação do cidadão é normalmente voluntária. Além disso, o governo não impõe soluções específicas, como por exemplo, o uso de certificados digitais.

5. Conclusões

O governo brasileiro encontra-se na posição 54 do ranking da ONU [United Nations 2014] e ainda não definiu a estratégia nacional de gestão de identidades para e-Gov. Existe apenas uma definição de padrões de interoperabilidade de sistemas (arquitetura e-PING) [BRASIL 2014]. Dentre estas, destacam-se o uso do SAML como padrão para a troca de informação sobre autenticação e autorização entre domínios, da especificação WS-Security 1.1 para o fornecimento de segurança às mensagens trocadas e WS-Trust 1.4 para a gestão das relações de confianças (intermediação).

Para conceber uma estratégia nacional de IdM para o governo brasileiro, é muito importante analisar as estratégias adotadas nos países que se destacam na provimento de e-Gov, porém sem esquecer das peculiaridades do país, tais como a sua dimensão territorial, o índice de inclusão digital e o elevado índice de fraldes eletrônicas. Como trabalhos futuros, pretende-se aprofundar a análise considerando outros aspectos de gestão de identidades e aumentar o número de países analisados para os vinte melhores do rank da ONU.

Referências

Australian Government (2014). Identity security. http://goo.gl/9oy8EC.

Baldoni, R. (2012). Federated identity management systems in e–government: the case of italy. *Electronic Government, an International Journal*, 9(1):64–84.

Bhargav-Spantzel, A., Camenisch, J., Gross, T., and Sommer, D. (2007). User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527.

BRASIL (2014). e-ping padrões de interoperabilidade de governo eletrônico. Technical report, Comitê Executivo de Governo Eletrônico. http://goo.gl/PsV0UT.

Dawes, S. and Pardo, T. (2002). Building collaborative digital government systems. In *Advances in Digital Government*, volume 26, pages 259–273. Springer US.

Dhamija, R. and Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. *Security Privacy, IEEE*, 6(2):24–29.

European Comission (2014a). eGovernment in Finland. eGovernment Factsheets.

European Comission (2014b). eGovernment in France. eGovernment Factsheets.

European Comission (2014c). eGovernment in the Netherlands. eGovernment Factsheets.

European Comission (2014d). eGovernment in the U.K. eGovernment Factsheets.

France Government (2013). TSL and RGS. http://goo.gl/vgqjat.

Government Digital Service (2014). Identity Assurance: First delivery contracts signed. http://goo.gl/7El4Ys.

Hansen, M., Schwartz, A., and Cooper, A. (2008). Privacy and identity management. *Security Privacy, IEEE*, 6(2):38 –45.

IDA Singapore (2014). egov2015 masterplan (2011-2015) - visionstrategic thrusts. http://goo.gl/Yzqx8v.

Infocomm Development Authority of Singapore (2014). egov masterplans. http://goo.gl/Hrw8D2.

ITU, T. (2009). Series y: Global information infrastructure, internet protocol aspects and next-generation networks. *Rec. ITU-T Y*, 2720.

Kãwanatanga, T. K. O. N. T. (2008). *New Zealand E-government Interoperability Framework (NZ e-GIF)*. State Services Commission.

OASIS (2005). *Security Assertion Markup Language (SAML) 2.0 Technical Overview*.

OECD (2011). National strategies and policies for digital identity management in OECD countries. *OECD Digital Economy Papers*, (177).

Rebecca Bowe (2012). In japan, national ID proposal spurs privacy concerns. http://goo.gl/jTfLk6.

Seltsikas, P. and van der Heijden, H. (2010). A taxonomy of government approaches towards online identity management. In *43rd HICSS*, pages 1–8.

Singapore Government (2008). Unique entity number brings convenience to entities. http://goo.gl/mPCVSG.

United Nations (2014). e-Government Survey: E-Government for the Future We Want. Economy & Social Affairs.

Wangham, M. S., de Mello, E. R., da Silva Böger, D., Gueiros, M., and da Silva Fraga, J. (2010). *Minicursos X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, chapter Gerenciamento de Identidades Federadas, pages 1–52.

Yumi Watanabe (2014). ANALYSIS: Japanese law to establish new ID number system includes measures to address privacy concerns. http://goo.gl/TspeMG.