Ministério da Justiça

UnB

Centro de Apoio ao Desenvolvimento Tecnológico

latitude
Laboratório de tecnologias da tomada de decisão

Termo de Cooperação/Projeto:

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

Documento:

RT - Características e Questões de Pesquisa sobre Gestão de Identidades

Data de Emissão:

11/12/2014

Elaborado por:

Glaidson Verzeletti (IFSC/UNIVALI)
Michelle Wangham (UNIVALI)
Emerson Ribeiro de Mello (IFSC)
José Alberto Sousa Torres (MJ)

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
Alexandre Cardoso de Barros
Andréa Benoliel de Lima
Beatriz Merguiso Garrido
Celso Pereira Salgado
Delluiz Simões de Brito
Domingos Soares dos Santos
Duque Dantas
Elaine Fabiano Rocantins
Felipe Bragança Itaborahy
Fernando Saliba
Fernando Teodoro Filho
Guilherme Braz Carneiro
John Kennedy Ferrer Lima
José Alberto Sousa Torres
Joaquim de Oliveira Machado
Marcelo Martins Villar
Narumi Pereira Lima
Paulo Cesar Vieira dos Santos
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
Andréia Campos Santana
Andreia Guedes Oliveira
Cristiane Faiad de Moura
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Debora Nobre de Castro
Egmar Alves da Rocha
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Gilvan Fortalesa Ribeiro
João Luiz Xavier M. de Negreiros
Jonathas Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Julie Christine Tende Franco
José Elenilson Cruz
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Maria do Socorro Rocha
Pedro Augusto Oliveira de Paula
Renata Elisa Medeiros Jordão
Roberto Mariano de Oliveira Soares
Rosa Eliane Dias Rodrigues Silva
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Valério Aymoré Martins
Vitor Cardoso Borges Leal
Wladmir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
11/12/2014	1.0	Versão inicial

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5597 – 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, já que dá 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, os quais agregam 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 apresenta as características que serão identificadas e analisadas em uma pesquisa sobre estratégias nacionais de gestão de identidades eletrônicas que será realizada no escopo deste projeto e que envolverá diversos países.

2 ESTRATÉGIAS NACIONAIS DE GESTÃO DE IDENTIDADES

Para muitos países, o desenvolvimento de uma **Estratégia Nacional de Gestão de Identidades Eletrônicas (GId)** é fundamental para a realização de Programas de Governo Eletrônico (e-Gov) [OECD, 2011a]. Em portais nacionais, é importante que os governos possam regular, controlar e padronizar o acesso a seus serviços online. Como estratégia, muitos indicam a necessidade de oferecer serviços com processos de autenticação que exijam credenciais robustas de segurança. A adoção de um sistema de GId comum permite harmonizar a gestão de identidades em nível nacional. Isto implica reduzir ou limitar o número de identidades (p.ex identidade única) que cada cidadão precisa ter para interagir com os diversos serviços oferecidos pelo Governo.

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. O provimento de gestão de identidades é uma das características analisadas na pesquisa da ONU. O número de países que possuem estratégias nacionais cresceu de 52 (em 2012) para 69 países (2014), o que representa 36% do total de países analisados [United Nations, 2014].

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 eletrônicas. Segundo a OECED [2011a], os países se encontram em diversos estágios em relação ao desenvolvimento e implementação das estratégias nacionais de GId. A partir do desenvolvimento de políticas (definição de leis, planos, ações, etc), os governos conseguem implementar suas estratégias de gestão de identidades.

O governo brasileiro ainda não definiu a sua 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 GId para o governo brasileiro, é muito importante analisar as estratégias adotadas nos países que se destacam no provimento de e-Gov, porém sem esquecer das peculiaridades do país, tais como a sua dimensão territorial, o índice de

inclusão digital, o índice de desenvolvimento de e-Gov, o atual sistema de registro de identidade nacional e o elevado índice de fraudes eletrônicas.

Com o objetivo de analisar as estratégias nacionais de gestão de identidades (GId) de diferentes países, uma pesquisa bibliográfica e documental detalhada será realizada no escopo do Projeto RIC. De forma a sistematizar e padronizar a análise das estratégias, nacionais, algumas características foram identificadas e questões de pesquisa foram elaboradas. O mapa mental da Figura 1 ilustra as características que serão analisadas, sendo que estas estão organizadas em cinco categorias. Na Seção a seguir, cada categoria a ser analisada será descrita.

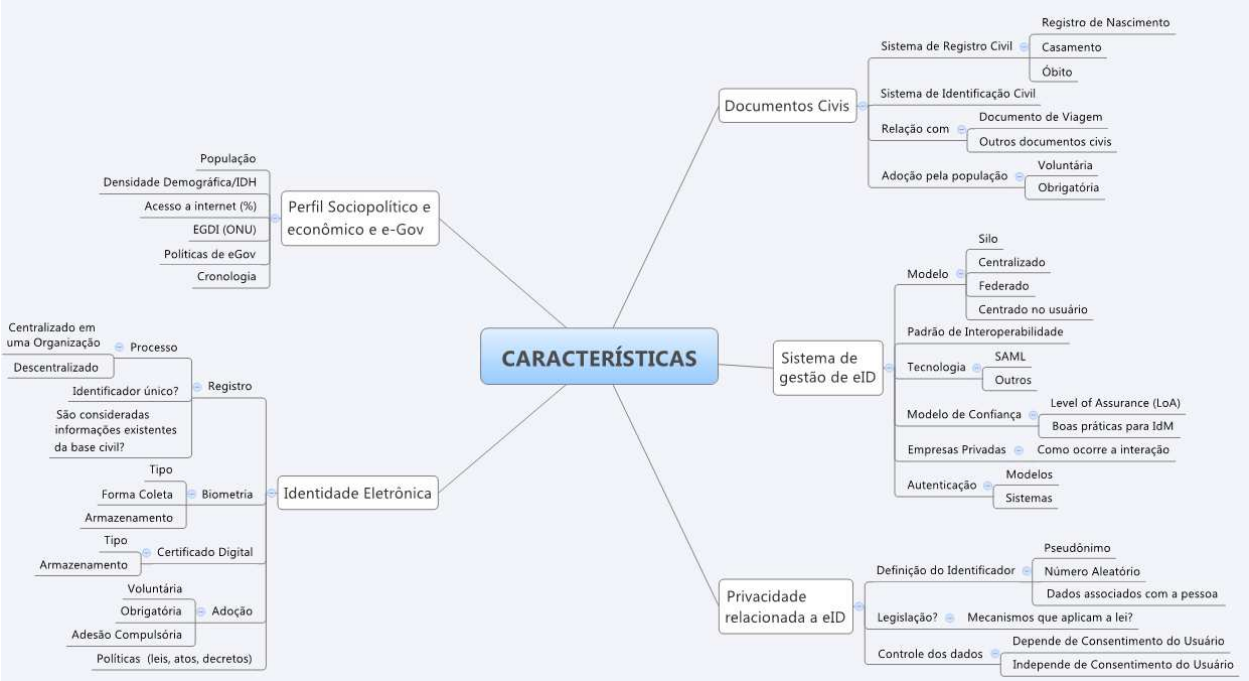

Figura 1 - Mapa conceitual com as características a serem analisadas

3 DESCRIÇÃO DAS QUESTÕES DE PESQUISA POR CATEGORIA

3.1 Perfil Sociopolítico e Econômico e o Governo Eletrônico

Devido a uma série de fatores, existem grandes disparidades entre regiões e países em relação ao desenvolvimento do governo eletrônico, como observado na pesquisa de 2014 da ONU. O nível de renda de um país é um indicador geral da sua capacidade econômica e de seu progresso, logo influencia diretamente no desenvolvimento de programas de e-Gov. Acesso às infraestruturas de Tecnologias de Informação e Comunicação (TICs) e o acesso à educação, incluindo a alfabetização digital, estão relacionados com o nível de renda de uma nação. A ausência desses fatores dificulta a implementação de iniciativas de e-Gov. No entanto, é claro que a renda nacional

não tem, por si só, como garantir o desenvolvimento de programas de e-Gov. Na pesquisa de 2014, apesar da renda nacional relativamente baixa, muitos países avançaram significativamente em seus programadas de e-Gov, assim como existem muitos países que estão atrasados, apesar de sua alta renda [United Nations, 2014].

De acordo com o relatório da ONU, além do nível de desenvolvimento social, político e econômico, outro fator que contribui para um alto nível de desenvolvimento de eGov é o investimento em infraestruturas avançadas de TICs (passado e presente) [United Nations, 2014]. O índice de desenvolvimento de e-Gov (EGDI - E-Government Development Index) de cada país avaliado pela ONU em seus relatórios é constituído de três dimensões, a saber: a provisão de serviços online, a infraestrutura de telecomunicações e o capital humano. No relatório da ONU de 2014, 25 países[1] (13%) possuem EGDI considerado muito alto, 62 países (32%) possuem EGDI muito alto, 74 países (38%) possuem um valor mediano e 32 países (17%) possuem um EGDI considerado baixo.

Na **Categoria 1** (**Perfil Sociopolítico e Econômico e o Governo Eletrônico**), as seguintes questões de pesquisa serão investigadas no estudo de cada país:

1.1. Qual o perfil sociopolítico e econômico do país? Indique a população, o território, a densidade demográfica, o índice de desenvolvimento humano, o sistema político e s organização política administrativa.

1.2. Quais os índices de acesso à Internet do país?

1.3. Qual a posição no *rank* da ONU de desenvolvimento de e-Gov nos anos de 2012 e 2014 (EGDI)? Qual a posição do país no *rank* que avalia o grau de participação dos cidadãos nas aplicações de e-Gov e no *rank* de serviços on-line oferecidos pelo governo?

1.4. Quais as principais políticas (leis, atos, decretos, etc.) de e-Gov do país?

1.5 Qual a cronologia do desenvolvimento de eGov e GId do país?

3.2 Modelo de Organização de Documentos Civis

O estudo dos modelos de organização dos documentos civis visa apresentar como as nações se organizam para conceder aos seus cidadãos a possibilidade de exercerem seus direitos civis de uma forma fácil, rápida e segura. No Brasil, os registros civis ou públicos são documentos feitos em cartórios de registro civil, dentre estes se destacam os registros de: nascimento, casamento e óbito. Estas certidões podem ser em papel ou eletrônicas (em alguns estados).

[1] Todos são países considerados de alta renda.

Um documento de identidade (*offline*) é um instrumento oficial que tem o fim de provar a identidade de uma pessoa física. Por exemplo, no Brasil, a identificação civil é atestada pelos seguintes documentos: carteira de identidade (RG); carteira de trabalho; carteira profissional; passaporte; carteira de identificação funcional; outro documento público que permita a identificação do cidadão. Em vários países, porém, existe grande resistência à criação de documentos de identidade *ad hoc* (criado especificamente para prova de identidade, p.ex o RG) [OECD, 2011a].

De acordo com a OECD [2011a], as estratégias nacionais de gestão de identidades eletrônicas, geralmente adotam uma abordagem semelhante a práticas e regulamentos dos sistemas de identidades em papel (*offline*). Por exemplo, na pesquisa da OECD, todos os países estudados que lançaram um cartão nacional de identidade eletrônica migraram este de seu cartão nacional em suporte de papel. A natureza voluntária ou obrigatória do cartão, geralmente também segue a mesma natureza do cartão em papel. Países que têm tradição em seus sistemas de registro da população nacional ou que usam identificadores nacionais estão tomando como base estes sistemas em suas estratégias de gestão de eID, por vezes, ajustando apenas as infraestruturas existentes para a utilização eletrônica [OECD, 2011a].

O objetivo desta categoria é apresentar os diversos modelos adotados pelos países pesquisados para o registro dos cidadãos e concessão de documentos de identificação civil *offline* e depois confrontar com a sua estratégia de gestão de identidades eletrônicas.

Na **Categoria 2** (**Modelo de Organização de Documentos Civis**), as seguintes questões de pesquisa serão investigadas no estudo de cada país:

2.1. Como é feito o registro de nascimento, casamento e óbito pela nação? Este registro é feito de forma centralizada por uma única entidade credenciada? O registro é feito exclusivamente por órgãos do governo ou há a participação de entidades privadas? Este documento pode ser eletrônico?

2.2. Em relação ao sistema de identificação civil, há um documento de identidade civil *adhoc offline*? Quem o emite e como é realizado o processo de criação do documento de identidade civil (centralizado ou distribuído)? Este documento é obrigatório? Qual a relação do documento de identidade com outros documentos civis?

2.3. Existe alguma relação entre o documento de viagem e o documento civil?

2.4. Nos sistema de identificação civil, é coletada algum tipo de biometria (p.ex impressões digitais)? Que tipo de dados biométricos são coletados? Como é feito o armazenamento destas informações (*smartcard*, banco de dados do governos e/ou em papel)?

3.3 Identidade eletrônica

A identidade de uma pessoa é composta por uma grande quantidade de informações pessoais que carateriza essa pessoa em diferentes contextos dos quais essa faz parte [Clauß e Köhntopp 2001]. A identidade é composta pela combinação de subconjuntos de identificadores (p.ex. número do CPF) e outras informações (p.ex. sexo), chamados de identidades parciais. Dependendo do contexto e da situação, uma pessoa pode ser representada por uma identidade parcial diferente. A identidade parcial de uma pessoa no contexto de uma universidade pode conter o número da matrícula como identificador e informações como seu nome, data de nascimento e as disciplinas que cursa. No contexto de uma empresa, a identidade pode estar associada com funções, privilégios, direitos e responsabilidades. Cabe salientar que uma mesma informação pessoal pode estar presente em diferentes identidades parciais.

Identidade eletrônica (eID) pode então ser definida como um conjunto de dados que representam uma entidade dentro de um determinado contexto [Wangham et al. 2010]. No ambiente digital, o número de identidades que uma pessoa pode ter é maior se comparado com o mundo real, já que a Internet permite a interação entre entidades que estão geograficamente distantes.

De acordo com a norma ITU-T Y.2720 [2009], uma identidade eletrônica pode consistir de:

- Identificador – conjunto de caracteres e símbolos ou qualquer outra forma de dados usados para identificar unicamente uma identidade;
- Credenciais – atesta a veracidade da identidade. Exemplo de credenciais incluem certificados digitais X.509 assinados por uma autoridade certificadora, senhas entre outras;
- Atributos – um conjunto de dados que descreve as características fundamentais de uma identidade. Como exemplo, o nome completo, o endereço domiciliar, a data de nascimento e papéis (roles).

De acordo com a OECD (2011b), a estratégia nacional de GId deve ter como objetivo reduzir ou limitar o número de credenciais digitais que os indivíduos têm de usar em serviços do setor público e privado. Em muitos países, os cidadãos utilizam uma identidade eletrônica nacional única para acesso aos sistemas de governo eletrônico. Os cidadãos que pretendem utilizar os serviços de e-Gov podem acessar uma ampla gama de serviços on-line através de credenciais únicas que permitem que o sistema reconheça o usuário, adeque os serviços às suas necessidades e permita o rastreamento fácil e rápido do estado de transações eletrônicas. Assim, os usuários não têm que memorizar muitas credenciais e nomes de usuário para acessar e-serviços. O uso de identidade única também é benéfica para o governo na medida em que permite que todas as agências, oferecendo diferentes serviços, disponham de informações confiáveis e

seguras sobre os usuários. Isso reduz os trâmites burocráticos, minimiza redundâncias e replicação dentro das agências e agiliza os resultados da prestação de serviços para os cidadãos [United Nations, 2014].

Para a OECD (2011b), um equilíbrio deve ser encontrado entre o estabelecimento de uma identidade eletrônica única para todas as interações digitais, que é sensível por razões de privacidade, e o uso entre múltiplas identidades que podem prejudicar a usabilidade.

Faz parte do escopo desta categoria pesquisar e identificar os critérios, leis e políticas adotadas pelas nações para criar as eID de seus cidadãos, bem como identificar se algum tipo de biometria ou certificado digital faz parte da eID do cidadão.

Na **Categoria 3** (**Identidade eletrônica**), as seguintes questões de pesquisa serão investigadas no estudo de cada país:

3.1. O cidadão pode ter mais de uma identidade eletrônica ou é permitido o uso de apenas uma única identidade eletrônica?

3.2. As políticas de e-Gov determinam que o cadastro seja feito de forma centralizada em uma única organização ou permite que o registro seja feito de forma descentralizada? Existe a participação de entidades privadas neste cadastro?

3.3. Quais informações são levadas em consideração para se criar a identidade eletrônica do cidadão? Existe alguma relação da eID com documentos de identidade civil?

3.4. Exite algum processo de coleta de dados biométricos dos cidadãos? Se sim, que tipo de dados biométricos são coletados e como é feita coleta? Como é feito o armazenamento destas informações (*smartcard*, banco de dados do governos e/ou em papel)?

3.5. A identidade eletrônica possui certificado digital? Se sim, é opcional ou obrigatório? O governo exige o uso de certificados digitais pelos seus cidadãos para o acesso de sistemas de e-Gov? Como é feita a gestão deste certificado digital pessoal?

3.6. O cidadão é obrigado a criar sua identidade eletrônica ou o governo permite a adesão voluntária?

3.4 Sistemas de Gestão de Identidade Eletrônica (SGId)

Um **sistema de gestão de identidades** (SGId) provê ferramentas para a gestão das identidades em um mundo digital. 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 mecanismos de autenticação, autorização, contabilização e auditoria [ITU, 2009]. Enquanto no mundo real uma pessoa escolhe quais informações revelar de si a outras pessoas, levando em

consideração o contexto e a sensibilidade da informação, no mundo digital essa tarefa é desempenhada pelo sistema de gestão de identidades.

Um sistema de gestão de identidades é caraterizado pelos seguintes elementos: **usuário** - aquele que deseja acessar um recurso; **identidade** - conjunto de atributos de um usuário; **provedor de identidade** (IdP) - responsável por gerenciar identidades de seus usuários e autenticá-los; **provedor de serviços** (SP) - oferece recursos aos usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso [Bhargav-Spantzel et al., 2007].

A disposição de cada um destes elementos de um SGId e a forma com que estes interagem entre si caraterizam os modelos de SGId, sendo estes classificados como: tradicional (isolado), centralizado, federado e centrado no usuário (Ver Figura 2).

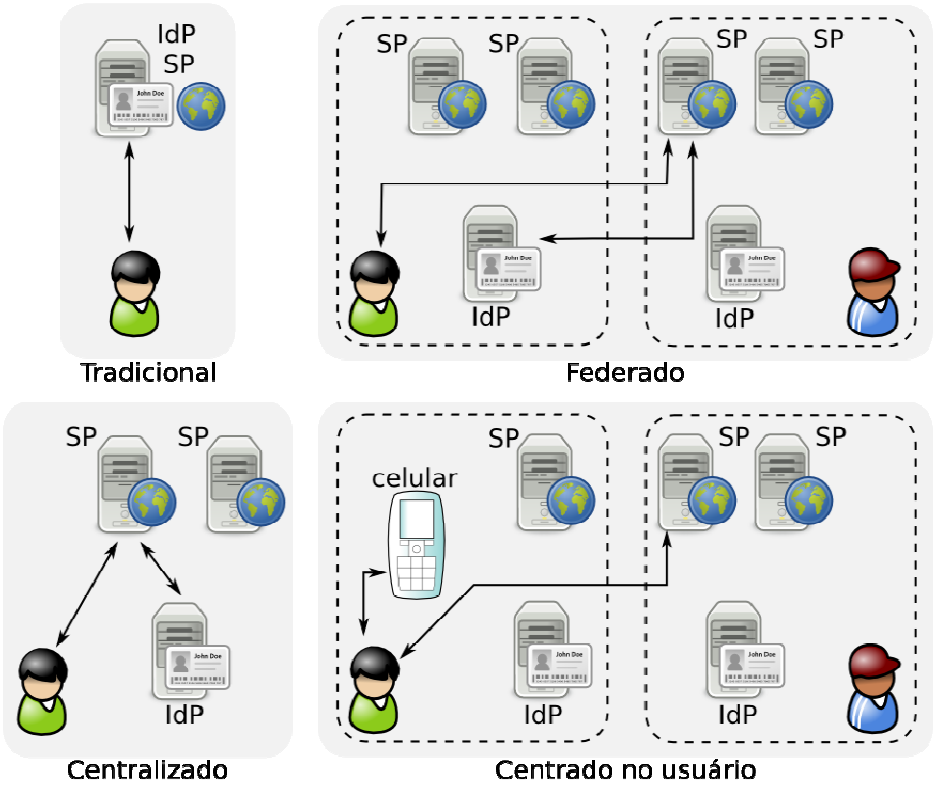

Figura 2- Modelos de gestão de identidades [Wangham et al., 2010]

No **modelo tradicional** (isolado em silos) provedores de identidades e de serviços são agrupados em uma única entidade e cabe a esta fazer a autenticação e controle de acesso de seus usuários sem depender de qualquer outra entidade. O usuário precisa então criar uma identidade diferente para cada provedor que desejar interagir e não existe o compartilhamento de identidades entre diferentes provedores.

O principal benefício deste modelo está na limitação do alcance de um ataque para o comprometimento de identidades de usuários. Por não compartilhar atributos dos usuários entre diferentes provedores, não é possível que um terceiro consiga, de maneira fácil, associar as diferentes identidades que um usuário possui em cada um dos silos onde atua.

Por outro lado, fazer com que o usuário gere uma identidade para cada provedor com quem queira interagir, resulta em problemas de usabilidade, pois este terá que gerenciar diferentes nomes de usuário e senha, bem como a proliferação de seus dados pessoais por diferentes serviços (problemas de privavidade). Para uma instituição que hospeda diversos provedores de serviços, tem-se então o desperdício de recursos, uma vez que haverá duplicação dos esforços para manutenção de diferentes contas de um mesmo usuário.

O **modelo centralizado** surge como uma solução para as dificuldades apresentadas pelo modelo tradicional. Só existe um provedor de identidades, o qual é responsável por autenticar os usuários, fornecer aos provedores de serviços informações sobre estes, sendo que todos os provedores de serviços devem confiar plenamente nas informações fornecidas por este provedor de identidades. O modelo centralizado fundamentalmente permite o compartilhamento de identidades dos usuários entre os provedores de serviços e permite o uso da autenticação única (*Single Sign-On - SSO*)

O **modelo de identidade federada** está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidades, estando estes dispostos em diferentes domínios administrativos. Um domínio administrativo pode representar uma empresa, uma universidade, entre outros, sendo composto por usuários, diversos provedores de serviços e um único provedor de identidades.

A gestão de identidades federadas é uma abordagem para otimizar a troca de informações relacionadas a identidade através de relações de confiança construídas nas federações [Camenisch e Pfitzmann, 2007]. Acordos de confiança estabelecidos entre provedores de identidades garantem que identidades emitidas em um domínio sejam reconhecidas por provedores de serviços de outros domínios e o conceito de passar pelo processo de autenticação uma única vez durante a sessão (*Single Sign-On*) pode ser garantido, mesmo diante de diferentes domínios. Desta forma, o modelo de identidades federadas consegue oferecer facilidades para os usuários, pois evita que estes tenham que lidar com diversas identidades e passar diversas vezes pelo processo de autenticação. Para os provedores de serviços, o benefício é que terão que gerenciar uma base menor de usuários e as informações terão uma probabilidade maior de estarem coesas e atualizadas.

A crítica sobre os modelos centralizado e federado se faz principalmente sobre o provedor de identidades, pois este possui total poder sobre os dados de seus usuários. Apesar de haver a distribuição das identidades por diversos provedores (no modelo federado), usuários não

conseguem garantir que suas informações não serão repassadas a terceiros sem o seu consentimento.

O **modelo centrado no usuário** objetiva dar ao usuário o total controle sobre suas identidades digitais, contudo as principais propostas e implementações deste modelo fazem uso de um dos modelos apresentados anteriormente, sendo o modelo de identidades federadas o mais usado. No modelo centrado no usuário, as identidades de um usuário são armazenadas em um dispositivo físico que fica em poder do próprio usuário, como por exemplo, um *smartcard* ou mesmo um telefone celular. Os usuários têm a liberdade de escolher os provedores de identidade que irão usar, independentemente dos provedores de serviços que desejam acessar e não precisam revelar informações pessoais aos provedores de serviços, como forma de garantir acesso ao recurso desejado.

No modelo centrado no usuário, os provedores de identidades continuam atuando como uma terceira parte confiável na interação entre usuários e provedores de serviços, contudo os provedores de identidades atuam de acordo com os interesses dos usuários e não de acordo com os interesses dos provedores de serviços.

De acordo com a OECD (2011a), os desafios relacionados a interoperabilidade, segurança e privacidade dos sistemas de gestão de identidades dependem da natureza centralizada ou descentralizada da política de registro de eID. Por exemplo, a política de registro influencia o nível de interoperabilidade que as políticas nacionais podem ter. Em um país com registro de eID descentralizada, a interoperabilidade é promovida no âmbito dos acordos da federação. As regras de operação comuns são descritas de forma independente das possíveis soluções tecnológicas. Em contraste, os países que adotam uma política de registo centralizada são mais propensos a adotar uma abordagem relativamente mais normativa (menos flexível) em relação a escolhas técnicas e regras. Políticas de registro centralizado levantam questões em relação à privacidade devido ao uso de um registro central, identificadores únicos e, em alguns casos, de *frameworks* que suportam cartões de identidade nacional. De acordo com a OECD (2011a), o registro descentralizado fornece a cada organização ou jurisdição um alto grau de autonomia em relação às medidas de proteção de privacidade.

Dentre as tecnologias de gestão de identidades, o padrão **SAML** (*Security Assertion Markup Language*) se destaca tanto na implementação do modelo de identidades federadas quanto no modelo centralizado. A transposição de informações sobre identidades de usuários de um domínio para o outro só é possível se houver uma linguagem padrão para expressar estes dados em ambos os domínios.

O padrão SAML consiste de um conjunto de especificações que define meios para expressar, em XML, informações sobre autenticação, autorização e atributos de um sujeito. A linguagem SAML é neutra a plataforma e tecnologias de segurança, visando garantir a

interoperabilidade entre os diferentes sistemas de autenticação e de autorização. SAML é o padrão recomendado pela arquitetura E-PING [BRASIL, 2014] e é o mais adotado por países que seguem o modelo de identidades federadas

Em sua primeira versão, SAML 1.0, o principal objetivo era permitir a transferência de autenticação e autorização entre aplicações web. A versão 1.1 foi lançada com o intuito de melhorar a interoperabilidade e garantir uma melhor integração com o XMLDSign, para assinaturas digitais em XML. Por fim, a versão 2.0 do SAML tem como foco principal o uso de identidades federadas, pseudônimos, mecanismos para garantir privacidade dos usuários, entre outros. SAML é hoje um padrão de fato usado em aplicações comerciais, como em Serviços Web, federações acadêmicas e em Estratégias Nacionais de GId.

O projeto STORK (*Secure idenTity acrOss boRders linKed*), uma iniciativa da comunidade europeia, objetiva permitir que cidadãos europeus façam uso do sistema de eID de seu país para acessar serviços de e-Gov de outros países. O *framework* proposto no projeto STORK faz uso do SAML 2.0 para implantar o modelo de identidades federadas e garantir a interoperabilidade de identidades eletrônicas.

O programa IDABC da comunidade europeia (http://ec.europa.eu/idabc/en), concluído em 2009, buscou apresentar uma solução legal, técnica e organizacional para a entrega de serviços de e-Gov interoperáveis para a administração pública, empresas e cidadãos. O SAML também é apresentado como solução para a interoperabilidade e para a privacidade dos usuários.

O governo dos Estados Unidos da América, através do sítio web www.idmanagement.gov, mantém um conjunto de recomendações, especificações e ferramentas nas áreas de identidade eletrônica, credenciais e controle de acesso que podem ser usadas por indivíduos ou organizações (empresas ou governo). O documento *Identity, Credential and Access Management* (ICAM) apresenta os requisitos para a construção e implementação de soluções interoperáveis, para serviços ofertados por empresas e para serviços de e-Gov. O documento também indica o SAML como solução para a interoperabilidade.

No documento ICAM, também existe uma preocupação sobre a classificação da qualidade das asserções emitidas pelos provedores de identidade (IdP) e isto é feito através dos níveis de garantia (*Levels of Assurance - LOA*) definidos pelo *National Institute of Standards and Technology* (NIST), sendo nível LOA 1 quando não se tem certeza sobre a asserção de autenticação emitida, uma vez que a identidade do usuário pode ter sido gerada através de auto cadastro; nível LOA 2 quando há alguma convicção sobre asserção identidade; nível LOA 3 quando há certeza sobre a asserção de identidade; e nível LOA 4 quando está completamente certo sobre a asserção de identidade, por exemplo, quando o usuário se autentica fazendo uso de nome de usuário e senha e um *smartcard*.

Em maio de 2014, a OASIS publicou a especificação *Electronic Identity Credential Trust Elevation Framework* que propõe métodos necessários para satisfazer os níveis de garantia (LOA) na avaliação da robustez sobre os mecanismos de autenticação e as identidades eletrônicas. O documento também está baseado nos níveis definidos pelo NIST, apresentando os vetores de risco associados a diferentes procedimentos de autenticação, bem como estratégias para mitigar tais riscos.

Na **Categoria 4** (**Sistemas de Gestão de eID**), as seguintes questões de pesquisa serão investigadas no estudo de cada país:

4.1 Existe um padrão de eID no país ou existe uma busca por um padrão de eID que seja interoperável e usado por diversos países?

4.2 Qual modelo de gestão de eID é adotado no país e quais os motivos para esta escolha?

4.3 Quais tecnologias de GId são utilizadas na Estratégia Nacional de GId?

4.4 Provedores de Identidade privados podem atuar em conjunto com o governo para autenticar usuários de serviços e-Gov? Provedores de serviços privados podem fazer uso do SGId usado na Estratégia Nacional de eID?

4.5 Quais padrões de interoperabilidade são utilizados na Estratégia Nacional?

4.6 Qual o modelo de gestão de confiança (*Trust Framework*) adotado na Estratégia Nacional de GId?

4.7 Existem mecanismos legais e/ou especificações técnicas sobre o uso de níveis de garantia (*LoA - Level of Assurance*) para os provedores de identidade?

4.8 Quais mecanismos/técnicas de autenticação são utilizados no(s) provedore(s) de identidade(s)?

3.5 Privacidade relacionada a Identidade Eletrônica (eID)

Privacidade da informação pode ser definida como o direito de uma pessoa determinar o grau de interação que suas informações pessoais devem ter perante o contexto no qual a identidade está inserida. Este contexto inclui o grau de comprometimento na divulgação destas informações a terceiros [Júnior et al., 2010]. 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 compartilhados com terceiros, como esse compartilhamento deve ser feito e o período de tempo que essas informações ficarão disponíveis nos sistemas.

De acordo com Hansen et al. (2008), determinar como aplicar os princípios e guias de privacidade em um sistema particular de gestão de identidades requer uma sólida compreensão

do ambiente em que o sistema opera e dos riscos e benefícios que o sistema tem que equilibrar. O projeto e concepção de um sistema de gestão de identidades que proteja a privacidade dos cidadãos requer ainda uma sólida formação em princípios fundamentais de privacidade.

O conjunto de princípios de privacidade mais aceito e empregado pelas nações é o FIPs (*Fair Information Practices*), elaborado 1970. Desde então, as políticas internacionais de privacidade da informação convergem em torno do FIPs como elemento central para privacidade dos cidadãos. Em 1980, a OECD emitiu um documento com diretrizes para proteção da privacidade e do fluxo de dados pessoais entre diferentes domínios administrativos (países), baseado no princípio FIPS, que foram amplamente adotados pelos países membro da OECD [Gelman, 2014]. Em 2013, este documento foi revisado e atualizado uma vez que os ambientes em que os princípios são agora implementados sofreram mudanças significativas, tais como: (1) grande volume de dados coletados, usados e armazenados; (2) aumento das ameaças contra a privacidade; (3) aumento na frequência e intensidade das interações envolvendo dados pessoais; e (4) a disponibilidade global de dados pessoais (OECD, 2013).

De acordo com a OECD (2013) e baseado no FIPS, os oito princípios básicos para proteção de dados pessoais são:

- **Limitação para coleta de dados**. Limites para coleta de dados pessoais devem existir. Dados pessoais devem ser coletados por meios legais e justos e, quando apropriado, com o conhecimento e consentimento da pessoa;
- **Qualidade do dado**. Dados pessoais devem ser relevantes para o propósito no qual estes foram coletados e são usados. Estes devem ser precisos, completos e devem estar atualizados;
- **Especificação da finalidade**. Dados pessoais devem ser usados para os propósitos especificados quando estes são coletados e o uso subsequente limitado ao cumprimento destes propósitos;
- **Limitação de uso**. O uso e revelação de dados pessoais deve ser limitado ao que foi especificado (princípio anterior). Estes dados não devem ser revelados sem o consentimento da pessoa ou de uma autoridade legal;
- **Salvaguardas de segurança**. Os dados pessoais devem ser protegidos por mecanismos e medidas de segurança contra acesso não autorizado, revelação, modificação e destruição de dados.
- **Abertura** (*openness*). A existência de sistemas que contêm dados pessoais deve ser de conhecimento público, juntamente com a descrição dos propósitos deste sistema e de como o sistema faz uso dos dados pessoais [Hansen et al, 2008];
- **Participação**. As pessoas devem ter o direito de: (1) saber do controlador de dados (ou de outro modo) se este tem ou não dados que lhe digam respeito; (2)

visualizar todas as informações coletadas relacionadas a elas; (3) corrigir ou remover dados que não estão atualizados, que não estão corretos, relevantes ou completos;

- **Responsabilização** (*accountability*). Um controlador de dados pessoais deve ser responsável pelo cumprimento de medidas para tornar efetivos os princípios acima referidos.

De acordo com Hansen et al (2008), no mundo digital, as duas preocupações centrais em relação à privacidade da informação são:

- **Observabilidade**: a possibilidade de que outras pessoas (observadores potenciais) possam obter informações pessoais. Os observadores podem ser os próprios participantes da comunicação, os provedores de serviços que facilitam a comunicação e "bisbilhoteiros" externos que fazem análise de tráfego (*eavesdropping*).
- **Habilidade de Ligação** (*Linkabilility)*: a possibilidade de ligação de dados com uma pessoa assim como a ligação de um conjunto de dados de uma pessoa para análise futura. Controlar a possibilidade de ligação envolve tanto a criação e a manutenção de contextos separados para que os observadores não possam acumular dados sensíveis, tanto ao ser cuidadoso quanto ao uso das identidades digitais.

Estes princípios de privacidade são o ponto de partida para qualquer projeto de sistema de gestão de identidades. Quando a interação da pessoa ocorre com um sistema nacional de gestão de identidades (SGId), a privacidade pode ser vista como a possibilidade de um cidadão determinar quais informações de sua identidade podem ser divulgadas para os provedores de serviços, optando por manter seu anonimato ou divulgando apenas os atributos pessoais que julgar adequados. Segundo Wangham et al. (2010), uma das formas de garantir o anonimato é fazer uso de pseudônimos, garantindo que as informações fornecidas, juntamente com a identidade digital, não possam ser utilizadas para descobrir dados de outras identidades. O uso de diferentes pseudônimos em diferentes contextos podem prevenir a ligação dos diferentes contextos a uma pessoa (*Linkabilility*) [Hansen et al, 2008]. O padrão SAML 2.0 provê suporte ao uso de pseudônimos, que são identificadores dinâmicos e não relacionados aos atributos de identidade do sujeito.

De acordo com Hansen et al (2008), projetistas de SGId devem resistir à centralização das informações de identidade ou ao uso de identidade (credencial) única para múltiplos fins, ou seja, optar pela diversidade e descentralização dos sistemas. Se for necessário ligar vários sistemas de gestão de identidade e bancos de dados (atributos de um cidadão), os projetistas devem implementar controles (salvaguardas) adequados para limitar os riscos associados de segurança

e de privacidade. Ainda segundo os autores, a quantidade, o tipo e a sensibilidade das informações coletadas e armazenadas em SGId devem ser consistentes e proporcionais aos objetivos do sistema. Por fim, a privacidade deve ser considerada desde as fases inicias do projeto de um SGId para que salvaguardas adequadas sejam projetadas e implementadas.

A principal ferramenta política dos cidadãos utilizada para garantir o direito à privacidade é a criação de leis específicas para este fim. Incorporar estas leis nas estratégias nacionais de gestão de identidades faz parte da políticas de alguns países como forma legal para proteger a privacidade [OECD. 2011a]. Em alguns países do mundo, como em muitos da Europa, um forte arcabouço jurídico com ferramentas que vão além dos FIPs, contribuem para proteção da privacidade da informação [Hansen et al, 2008].

Avaliações de impacto sobre a privacidade são também normalmente citadas pelos governos como uma ferramenta-chave no cumprimento destas obrigações legais aplicadas aos sistemas de gestão de identidade [OECD. 2011a]. Com a aplicação das avaliações de impacto é possível garantir que:

- Informações recolhidas sejam apenas utilizadas para a finalidade a que se destinam;
- As informações sejam oportunas e precisas;
- Informações sejam protegidas de acordo com as leis e regulamentos;
- O impacto dos sistemas de informação sobre a privacidade individual seja tratada na íntegra;
- Os usuários do sistema estejam cientes do propósito para o qual as informações pessoais foram coletadas.

De acordo com o relatório da [OECD, 2011a], quando a interoperabilidade é implementada, surgem novos desafios relacionados a segurança e privacidade, uma vez que o nível de proteção de privacidade dos indivíduos depende de acordos de confiança entre os vários participantes de uma federação. Este desafio é notado, pois cada país tem um alto grau de autonomia em relação às medidas de proteção de privacidade que estabelece para si próprios, uma vez que as políticas de registro são descentralizadas.

Garantir um alto nível de proteção de privacidade, consistente com o nível adequado de garantia (LoA), é fundamental para o desenvolvimento do mercado de serviços de eGov, em particular aqueles de médio e alto valor [OECD, 2011b].

De acordo com o "*Guidance for Goverment Policy Maker*" da OECD, a estratégia nacional de GId deve ter como objetivo reduzir ou limitar o número de identidades e suas credenciais digitais que os indivíduos tenham para uso em todos os serviços públicos e privados. Um equilíbrio deve ser encontrado entre o estabelecimento de uma identidade universal única para

todas as interações digitais (estratégia sensível por razões de privacidade) e o uso de múltiplas identidades que podem prejudicar a usabilidade.

A usabilidade das aplicações de eGov pode ser melhorada, por exemplo, promovendo a redução do número de identidades usadas para interações eletrônicas que aceitem nível de garantia baixo. Porém, segundo o documento, é importante o uso de abordagens na qual os usuários podem escolher quais identidades e níveis de garantia querem usar (modelo centrado no usuário) e o incentivo à adoção de credenciais que asseguram um elevado nível de segurança. A redução do número de identidade não deve ocorrer em detrimento da proteção da privacidade, mas deve primeiramente ser baseada em tecnologias que respeitem a privacidade [OECD, 2011b].

Na **Categoria 5** (**Privacidade relacionada a Identidade Eletrônica**), as seguintes questões de pesquisa serão investigadas no estudo de cada país:

5.1. O cidadão pode fazer uso de pseudônimos para acesso aos sistemas do governo? Quais são os dados que estão associados ao usuário? Como é formado o identificador (caso haja uma identidade nacional única)? De alguma forma o identificador pode identificar o cidadão?

5.2. O cidadão pode escolher qual identidade eletrônica ou provedor de identidade deseja usar?

5.3. Existe alguma forma de o cidadão poder controlar os dados pessoais que são encaminhados ao provedor de serviço (SP) - abordagem centrada no usuário? Existe alguma preocupação do SP ou do IdP em informar ao usuário qual informação pessoal está sendo enviada?

5.4. Existem leis específicas para proteção da privacidade?

5.5. Existem mecanismos nos SGId que aplicam a lei?

4 CONCLUSÃO

Através 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.

O presente relatório teve como propósito descrever quais características precisam ser analisadas para que se possa compreender as Estratégias Nacionais de Gestão de Identidades dos países que se destacam na prestação de serviços de e-Gov. Um estudo será realizado no escopo do Projeto RIC e este relatório apresentou as questões de pesquisa que nortearão este estudo que envolverá países de todos os continentes. Vinte e oito (28) questões foram descritas e organizadas em cinco categorias, a saber: (1) Perfil Sociopolítico e Econômico e o Governo Eletrônico; (2) Modelo de Organização de Documentos Civis; (3) Identidade eletrônica; (4) Sistemas de Gestão de eID; e, por fim, (5) Privacidade relacionada a Identidade Eletrônica. Após este estudo e análise das Estratégias Nacionais, a equipe do Projeto terá subsídios para indicar

(ou não) o uso do RIC como uma identidade eletrônica e para definir uma estratégia nacional de gestão de identidades para o Brasil.

As atividades envolvidas nesta 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, levaram a etapa do projeto a bom termo.

REFERÊNCIAS

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

[BRASIL, 2014] BRASIL (2014). ePING: Padroes de interoperabilidade de governo eletrônico. Comitê Executivo de Governo Eletrônico. Disponível em:

http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade

[Camenisch e Pfitzmann, 2007] Camenisch, J. e Pfitzmann, B. (2007). *Security, Privacy, and Trust in Modern Data Management*, Federated Identity Management, pag 213–238. Springer Verlag.

[Chadwick, 2009] Chadwick, D. (2009). Federated identity management. Foundations of Security Analysis and Design V, pag. 96–120.

[Clauß e Köhntopp, 2001] Clauß, S. e Köhntopp, M. (2001). Identity management and its support of multilateral security. Computer Networks, 37(2):205–219.

[Gelman 2014] Gelman, Robert (2014). Fair Information Practices: A Basic History. Version 2.12. http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

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

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

[Júnior et al. 2010] Júnior, A. M., Laureano, M., Santin, A.,and Maziero, C. (2010). Aspectos de segurança e privacidade em ambientes de Computação em Nuvem. In Mini-curso - SBSeg 2010 - Fortaleza - CE

[OASIS, 2005] OASIS (2005). Security Assertion Markup Language (SAML) 2.0 Technical Overview. OASIS.

[OECD, 2011a] OECD (2011a). National strategies and policies for digital identity management in OECD countries. OECD Digital Economy Papers, (177). OECD Publishing. http://dx.doi.org/10.1787/5kgdzvn5rfs2-en

[OECD, 2011b] OECD (2011b). Digital Identity Management: Enabling Innovation and Trust in the Internet Economy. OECD. http://www.oecd.org/sti/ieconomy/49338380.pdf

[OECD, 2013] OECD (2013). THE OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

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

[Wangham et al, 2010] Wangham, M. S., de Mello, E. R., da Silva Böger, D., Gueiros, M., and da Silva Fraga, J. (2010). *Livro de Minicursos do X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, Capítulo: Gerenciamento de Identidades Federadas, pag. 1–52.

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