



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Alcimar Sanches Rangel

TRANSPARÊNCIA *versus* SEGURANÇA DA INFORMAÇÃO:
uma análise dos fatores de risco exposto na comunicação entre o
governo e a sociedade.

Brasília -DF

2015



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Alcimar Sanches Rangel

TRANSPARÊNCIA *versus* SEGURANÇA DA INFORMAÇÃO:
uma análise dos fatores de risco exposto na comunicação entre o
governo e a sociedade.

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade de Brasília como requisito parcial para obtenção do título de Mestre em Ciência da Informação.

Orientador: Prof. Dr. Jorge Henrique Cabral Fernandes

Brasília -DF

2015

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

R196t Rangel, Alcimar Sanches
TRANSPARÊNCIA versus SEGURANÇA DA INFORMAÇÃO: uma
análise dos fatores de risco expostos na comunicação
entre o governo e a sociedade. / Alcimar Sanches
Rangel; orientador Jorge Henrique Cabral Fernandes.
- Brasília, 2015.
143 p.

Dissertação (Mestrado - Mestrado em Ciência da
Informação) -- Universidade de Brasília, 2015.

1. Publicidade. 2. Transparência. 3. Privacidade.
4. Segurança da Informação. 5. Acesso à Informação. I.
Fernandes, Jorge Henrique Cabral, orient. II. Título.

FOLHA DE APROVAÇÃO

Título: "TRANSPARÊNCIA versus SEGURANÇA DA INFORMAÇÃO: uma análise dos fatores de risco expostos na comunicação entre o governo e a sociedade"


Autor (a): Alcimar Sanches Rangel

Área de concentração: Gestão da Informação

Linha de pesquisa: Comunicação e Mediação da Informação

Dissertação submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-graduação em Ciência da Informação da Faculdade em Ciência da Informação da Universidade de Brasília como requisito parcial para obtenção do título de **Mestre em Ciência da Informação**.


Brasília, 07 de agosto de 2015.



Prof. Dr. Jorge Henrique Cabral Fernandes
Presidente (UnB/PPGCINF)



Prof. Dr. Roberto Wagner da Silva Rodrigues
Membro Titular (MDS)



Profª. Drª. Dulce Maria Baptista
Membro Titular (UnB/PPGCINF)

Profª. Drª. Ivette Kafure Muñoz
Membro Suplente (UnB/PPGCINF)

RESUMO

Trata o presente trabalho de uma análise dos fatores de risco expostos na comunicação entre o governo e a sociedade, a partir da publicação dos dados de agentes públicos que atuam na segurança nacional e segurança pública federal. Tal análise está inserida na perspectiva interdisciplinar da ciência da informação, pois também aborda os campos de estudo da Computação e do Direito. Para tanto, desenvolveu-se uma pesquisa exploratória e qualitativa, por meio de investigação nos portais da *internet* que promovem a transparência pública, a fim de identificar os fatores de risco que impactam a privacidade dos agentes públicos investigados, e conseqüentemente os riscos gerados à segurança nacional e à segurança pública federal decorrentes da exploração dessa informação. A coleta de dados é realizada junto a fontes documentais em diversos portais dos Poderes Executivo, Legislativo e Judiciário por meio de uma amostragem qualitativa de indivíduos vinculados a órgãos que promovem a segurança nacional e segurança pública no âmbito da Administração Pública Federal. Busca-se analisar e compilar os dados coletados dos indivíduos pertencentes às amostragens, constatar, verificar e avaliar os riscos de segurança da informação dos dados coletados e, por fim, validar o processo de análise e discussões a respeito da investigação com as respostas do questionário enviado aos membros do Comitê Gestor da Segurança da Informação.

Palavras-chave: Publicidade, Transparência, Privacidade, Segurança da Informação, Acesso à Informação.

ABSTRACT

This study is an analysis of the risk factors set out in the communication between regarding government and society from the publication of data and information agents of the federal government working in national security and public security. It is inserted in the interdisciplinary perspective of information science, and also addresses the fields of study in Computing and Law. Therefore, it developed an exploratory and qualitative study through research in the internet portals that promote public transparency in order to identify the risk factors that impact the privacy of public officials investigated, as well as the risks posed to national security and public security. Data collection is performed by a documentary research in several internet portals of the executive, legislative and judiciary by means of a qualitative sampling of individuals in a population made up of agencies that promote national security and public safety within the Federal Public Administration. Seeks to analyze and discuss the data collected from individuals belonging to the sample, analyze and evaluate the information security risks of the data collected and ultimately validate the process of analysis and research discussions with the questionnaire responses sent to members of the Management Committee of Information Security.

Keywords: Publicity, Transparency, Privacy, Information Security, Classification, Access to Information.

DEDICATÓRIA

Dedico este Mestrado aos meus pais, **Alceo Rangel** (*in memoriam*) e **Carmen Gomes Sanches Rangel**, pela minha educação e todo apoio oferecido em todas as minhas decisões.

AGRADECIMENTOS

Às colaboradoras do PPGCINF,
Marta, Vivian e Jacqueline pela atenção, colaboração e solicitude.

Aos professores do PPGCINF, em especial, àqueles que tive a oportunidade de ser aluno e que contribuíram para a minha formação acadêmica:

André Porto Ancona Lopez, Cláudio Gottschalg Duque,
Fernando César Lima Leite, Renato Tarciso Barbosa de Sousa,
Rogério Henrique de Araújo Júnior, Sely Maria de Souza Costa,
Sofia Galvão Baptista e Suzana Pinheiro Machado Mueller.

Ao meu orientador, Jorge Henrique Cabral Fernandes, pela confiança,
dedicação, paciência e excelente orientação.

Aos membros da Banca Examinadora do Relatório Intermediário, Doutora Linda Soraya Issmael e Professora Doutora Lilian Maria Araújo de Rezende Alvares e, aos membros da Banca Examinadora de Defesa da Dissertação, Professor Doutor Wagner e Professora Doutora Dulce Maria Baptista pelas valiosas sugestões na melhoria deste trabalho.

Aos meus colegas do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República que me apoiaram e incentivaram em todo percurso desta dissertação.

A minha família, especialmente meus filhos João Pedro e Beatriz e meus irmãos e sobrinhos que, mesmo distante, me proporcionaram amor e carinho.

A minha namorada Ludmila por todo incentivo, apoio, carinho e compreensão neste momento tão importante de crescimento em minha vida.

“Os que se encantam com a prática sem a ciência são como os timoneiros que entram no navio sem timão nem bússola, nunca tendo certeza do seu destino”.

(Leonardo da Vinci)

LISTA DE ABREVIATURAS

ABIN -	Agência Brasileira de Inteligência
ABNT -	Associação Brasileira de Normas Técnicas
AGPENF -	Agente Penitenciário Federal
APF -	Administração Pública Federal
CDN -	Conselho de Defesa Nacional
CGSI -	Comitê Gestor da Segurança da Informação
CGU -	Controladoria-Geral da União
CI -	Ciência da Informação
CIA -	Conselho Internacional de Arquivos
CPF -	Cadastro de Pessoa Física
CRFB -	Constituição da República Federativa do Brasil
CTIR.Gov -	Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal
DHS -	<i>Department of Homeland Security</i>
DOU -	Diário Oficial da União
DPA -	<i>Data Protection Act</i>
DPF -	Delegado de Polícia Federal
DSIC -	Departamento de Segurança da Informação e Comunicações
EED -	Empresa Estratégica de Defesa
eMAG -	Modelo de Acessibilidade em Governo Eletrônico
ENCCLA -	Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro
EUA -	Estados Unidos da América
FFAA -	Forças Armadas
GRSIC -	Gestão de Riscos de Segurança da Informação e Comunicações
GSI-PR -	Gabinete de Segurança Institucional da Presidência da República
ICP-Brasil -	Infraestrutura de Chaves Públicas Brasileira

IEC -	<i>International Electrotechnical Commission</i>
ISO -	<i>International Organization for Standardization</i>
LAI -	Lei de Acesso à Informação
MP -	Ministério do Planejamento, Orçamento e Gestão
NIST -	<i>National Institute of Standards and Technology</i>
NBR -	Norma Brasileira
NVD -	<i>National Vulnerability Database</i>
ONU -	Organização das Nações Unidas
PDTI -	Plano Diretor de Tecnologia da Informação
PL -	Projeto de Lei
PPA -	Plano Plurianual
PRF -	Policia Rodoviária Federal
SGBD -	Sistema de Gerenciamento de Banco de Dados
SGSI -	Sistema de Gestão de Segurança da Informação
SI -	Segurança da Informação
SIC -	Segurança da Informação e Comunicações
SISBIN -	Sistema Brasileiro de Inteligência
SISP -	Sistema de Administração dos Recursos de Informação e Informática
SLTI -	Secretaria de Logística e Tecnologia da Informação
STF -	Superior Tribunal Federal
TCU -	Tribunal de Contas da União
TI -	Tecnologia da Informação
TIC-	Tecnologia da Informação e Comunicação
TSE -	Tribunal Superior Eleitoral
UF -	Unidade Federativa
UnB -	Universidade de Brasília
UNESCO -	Organização das Nações Unidas para a Educação, a Ciência e a Cultura

LISTA DE FIGURAS

Figura 1: Transparência ativa e passiva.....	34
Figura 2: Tela inicial do Portal da Transparência.....	35
Figura 3: Tela do Portal da Transparência referente ao servidor público.	36
Figura 4: Tela do Diário Oficial da União.....	37
Figura 5: Tela da pesquisa avançada no DOU.	39
Figura 6: Tela do Sistema IN Busca Total.	40
Figura 7: Exemplo de publicação de afastamento de servidor no DOU.	44
Figura 8: Linha do tempo de legislações sobre graus de sigilo	52
Figura 9: Modelo de Comunicação de Lasswell	55
Figura 10: Modelo comparativo do processo de GRSIC com o modelo da ABNT	70
Figura 11: Relacionamento entre os termos associados aos fatores de risco.	71
Figura 12: abordagem do processo de mapeamento e inventário de ativos de informação.	73
Figura 13: Tipos de ativos de informação	74
Figura 14: Modelo revisado baseado nos conceitos de Bain (1937) e Kaplan (2003).	75
Figura 15: Exemplo de publicação de dados pessoais no DOU	80
Figura 16: Fluxograma dos passos da coleta de dados dos indivíduos	92
Figura 17: Processo metodológico	94
Figura 18: Tela de consulta de Título por nome.....	99
Figura 19: Tela com o resultado da consulta de Título por nome	100
Figura 20: Matriz de risco - impacto <i>versus</i> probabilidade	105
Figura 21: Mapa sistêmico da relação Transparência e privacidade.	114

LISTA DE GRÁFICOS

Gráfico 1: Distribuição de incidentes de redes por categoria.....	57
Gráfico 2: Quantidade de dados coletados dos agentes de segurança nacional.	97
Gráfico 3: Quantidade de dados coletados dos agentes de segurança pública federal.....	97
Gráfico 4: Total de dados coletados dos indivíduos.....	98
Gráfico 5: Resultados das perguntas 1, 2 e 3 do questionário.....	109

LISTA DE QUADROS

Quadro 1: Identificação da origem do CPF por Unidades Federativas.	36
Quadro 2: Divisão do DOU por assuntos.	38
Quadro 3: Competências de classificação na APF e prazos de restrição de acesso.	54
Quadro 4: Exemplos de tipos de informação.....	60
Quadro 5: Normativos de SIC da APF.	62
Quadro 6: Família ISO/IEC 27000.....	63
Quadro 7: Exemplos de termos com diferentes conceitos nos normativos de SI.....	65
Quadro 8: Ameaças representadas por seres humanos.....	79
Quadro 9: Grupos de indivíduos que promovem a segurança nacional.	86
Quadro 10: Grupos de indivíduos que promovem a segurança pública federal.....	87
Quadro 11: Amostra de indivíduos que promovem a segurança nacional.	88
Quadro 12: Portais das Secretarias de Fazenda das UF por ordem de fragilidade.....	101
Quadro 13: Níveis de probabilidade.....	104
Quadro 14: Análise de impacto.....	105
Quadro 15: Resultado da análise e avaliação do risco.....	106
Quadro 16: Plano de tratamento de risco.....	107
Quadro 17: Informações publicadas dos membros do CGSI.	109
Quadro 18: Cargos públicos cujos dados dos ocupantes deveriam ser protegidos.	111
Quadro 19: Relação entre o modelo de comunicação de LASSWEEL com as LC n° 101/2000 e n° 131/2009.	112

LISTA DE TABELAS

Tabela 1: Nível de satisfação em relação ao funcionamento da democracia no país.	35
Tabela 2: Amostra de indivíduos que promovem a segurança pública federal, por UF.....	89
Tabela 3: Resultados da coleta de dados dos agentes de segurança nacional.	95
Tabela 4: Resultados da coleta de dados dos agentes de segurança pública.	96

SUMÁRIO

1	INTRODUÇÃO	18
1.1	Contextualização do Problema	19
1.2	Justificativa	20
1.3	Objetivos da Pesquisa	23
1.3.1	Objetivo Geral	23
1.3.2	Objetivos Específicos	23
2	REFERENCIAL TEÓRICO	25
2.1	Direitos e Garantias Fundamentais para o acesso à informação	26
2.1.1	Direito fundamental de acesso à informação	26
2.1.2	Princípio Legal da Publicidade	27
2.1.3	Transparência e opacidade informacional	29
2.1.4	Canais de Promoção da Transparência	33
2.1.4.1	Portal da Transparência do Governo Federal	34
2.1.4.2	Portal do DOU	37
2.1.4.3	Padrões mínimos para portais governamentais	40
2.1.5	O Direito à privacidade e a proteção de dados pessoais	42
2.2	Aspectos Relevantes da Gestão da Informação para a Segurança da Informação	46
2.2.1	Dado e Informação	46
2.2.2	Classificação da informação	50
2.2.3	Classificação da Informação quanto aos graus de sigilo	52
2.2.4	Comunicação da informação organizacional	54
2.3	Segurança da Informação	56
2.3.1	Conceitos gerais	56
2.3.2	Os normativos de segurança da informação	60
2.3.3	Sociedade do risco e a APF	66
2.3.4	Fatores de risco de SI	71
2.3.4.1	Ativos de Informação	72
2.3.4.2	Vulnerabilidades e ameaças	75

2.3.4.3 Impactos e probabilidades da quebra da SI	79
3 METODOLOGIA	84
3.1 Caracterização da pesquisa	84
3.2 Ambiente da pesquisa	85
3.3 População da pesquisa	86
3.4 Amostra da pesquisa	87
3.5 Coleta dos dados	90
3.5.1 Dados publicizados dos agentes públicos da APF	90
3.5.2 Questionário	93
4 ANÁLISE E DISCUSSÃO	94
4.1 Informações pessoais comunicadas por sistemas de promoção da transparência.....	95
4.2 Fatores de risco que impactam a privacidade	98
4.3 Análise e avaliação dos riscos que impactam o Estado e a sociedade	104
4.4 Análise dos resultados do questionário.....	108
4.5 Discussões finais.....	112
5 CONCLUSÕES E SUGESTÕES.....	116
5.1 Conclusões do estudo.....	116
5.2 Sugestões para trabalhos futuros	118
REFERÊNCIAS	120
ANEXO A – Lista dos Membros do CGSI/2015.....	136
APÊNDICE A – Lista das fontes de ameaças representadas por seres humanos	138
APÊNDICE B – Lista de vulnerabilidades	139
APÊNDICE C – Modelo de questionário	141

1 INTRODUÇÃO

À medida que os países democráticos tendem a ampliar a relação entre governo e cidadão por meio da publicidade e transparência de seus atos, observa-se uma explosão informacional em decorrência dessa comunicação, principalmente, com uso da Tecnologia da Informação (TI) associada à *internet*.

No Brasil, são inúmeras iniciativas que confirmam essa tendência, principalmente, aquelas impostas por leis e orientações normativas, como por exemplo, a Lei de Acesso à Informação (LAI)¹, que determina o uso da *internet* para a divulgação de informações produzidas e custodiadas pelos órgãos públicos, cujo interesse seja de caráter coletivo (BRASIL, 2011).

Atualmente é possível obter várias informações sobre gastos públicos, processos judiciais, eleitorais, trabalhistas; resultados de auditorias diretamente da *internet*. As publicações de tais informações são de responsabilidade de diversos órgãos, pertencentes a diferentes poderes e esferas governamentais. Tal fato, além de revelar a possibilidade de inconsistência dos dados, pode também caracterizar o indevido tratamento da informação, principalmente no que concerne à Segurança da Informação (SI).

Na ânsia do cumprimento do dever em prol da transparência, aspectos da SI podem ser desconsiderados. Nesse sentido, é preciso encontrar um equilíbrio entre o que é transparente e o que é seguro. Para auxiliar nessa harmonização, o uso da tecnologia pode oferecer excelentes soluções para a organização de grandes volumes de documentos dos órgãos públicos (ROBREDO, 2003).

Por outro lado, o uso da tecnologia interligada às redes pode oferecer riscos à informação e isto porque são inúmeras as ameaças do mundo virtual responsáveis por incidentes de segurança. De acordo com o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) estes incidentes são eventos adversos relacionados à segurança dos sistemas computacionais ou das redes de computadores (GSI-PR, 2009b, p. 3).

No entanto, independente da presença das possíveis ameaças que assombram o mundo cibernético, acredita-se que é de suma importância o desenvolvimento e ampliação de estudos voltados para a análise dos dados e informações divulgados pelo governo brasileiro na

¹ Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

internet, a fim de verificar se há indícios de divulgação de vulnerabilidades que afetam a SI do Estado ou da sociedade.

1.1 Contextualização do Problema

O arcabouço jurídico brasileiro tem apresentado diversos temas destacando a importância da transparência, tornando-a como um excelente mecanismo de controle das ações dos gestores públicos.

O governo brasileiro, por intermédio da Controladoria-Geral da União (CGU), vem ampliando cada vez mais a participação do cidadão no controle dos atos praticados pela Administração Pública Federal (APF), por meio do acesso às informações governamentais. Conseqüentemente, espera-se uma maior cobrança dos gestores públicos na prestação de contas a fim de evitar atos arbitrários e, principalmente, a corrupção.

A comunicação dos atos praticados pelo governo federal obedece ao princípio da publicidade consagrado no art. 37 da Constituição da República Federativa do Brasil (CRFB) e este princípio foi reforçado com a publicação da LAI.

A LAI além de reforçar o emprego do princípio da publicidade, tornou o sigilo uma exceção, considerando apenas os assuntos a seguir como informações que requeiram classificação em seu art. 23:

- I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
- II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
- III - pôr em risco a vida, a segurança ou a saúde da população;
- IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
- V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
- VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
- VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
- VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações. (BRASIL, 2011).

A restrição de acesso às informações não se limita apenas ao contido no art. 23 da LAI. Nesta lei também estão incluídas as informações relacionadas à “pessoa natural identificada ou identificável”, como também, outras hipóteses legais de sigilo e de segredo,

como os de justiça e industrial (BRASIL, 2011). Com isso, conclui-se que todas as informações ou dados que não estão incluídos nesse rol de restrições são de conhecimento público e de acesso irrestrito, e o resultado disso, é o fortalecimento da comunicação informacional entre o governo e a sociedade.

Por outro lado, aumenta a probabilidade de que algumas informações relacionadas à gestão de SI, sem o devido tratamento e a correta classificação, sejam expostas indevidamente, colocando em risco ou prejudicando os interesses do Estado e da sociedade.

Outro fator a ser observado diz respeito às divulgações de dados e informações efetuadas pelos órgãos do Poder Legislativo e do Poder Judiciário. Constitucionalmente, esses Poderes são independentes e com isso, parte-se da hipótese que um determinado dado ou informação pode ser considerado de acesso restrito para um Poder, enquanto para outro, de acesso livre.

Face ao exposto, para efetivar a gestão da SI, os órgãos públicos precisam unificar o tratamento da informação pública, observando os controles necessários de segurança, não apenas no aspecto tecnológico, mas considerando também e principalmente o ciclo de vida da informação.

1.2 Justificativa

Visando aumentar a participação do cidadão no cenário político brasileiro, a administração pública vem desenvolvendo ações alinhadas à transparência pública, no sentido de disponibilizar seus dados governamentais em formatos abertos. O acesso aos dados abertos permite que qualquer pessoa possa utilizá-los e redistribuí-los, sem qualquer tipo de restrição.

Entretanto, Soares (2014) observa que a atual facilidade de acesso aos dados governamentais, além de indicar informações sobre o funcionamento interno da APF, pode trazer diversas implicações para a SI. Os dados abertos expostos pelos órgãos governamentais já são suficientes para a identificação de vulnerabilidades, como por exemplo, a revelação da arquitetura tecnológica de uma determinada instituição, os seus sistemas de proteção contra intrusões e ataques cibernéticos, como também, as deficiências desses sistemas e aplicações.

Os órgãos governamentais, em conformidade com a Lei Complementar nº 131 de 4 de maio de 2009, disponibilizam informações sobre suas despesas decorrentes de compras de bens e contratações de serviços, sendo que, tais informações incluem a descrição do objeto do contrato, como por exemplo, marcas e modelos de equipamentos de segurança de TI (BRASIL, 2009).

Um órgão da APF, ao publicar no Diário Oficial da União (DOU) a sua intenção de aquisição de um determinado bem, equipamento ou sistemas de TI, não se preocupa com as implicações desta publicação para a SI. Entretanto, se realizado um acompanhamento do resultado desse processo, é possível levantar a descrição do bem adquirido, como por exemplo: valor, fornecedor, fabricante, modelo, quantidade. Esses dados e informações expostas pelos órgãos governamentais já são suficientes para qualquer pessoa mal-intencionada identificar as possíveis vulnerabilidades da tecnologia adquirida (SOARES, 2014, p. 19).

(...) as compras do exército são publicadas no DOU e disponibilizadas no portal de dados nacional de forma aberta e irrestrita. Uma análise dos insumos e valores associados às transações das forças armadas poderiam dar fortes indícios do tipo de operação em curso e, portanto, comprometê-las. Eis um exemplo de como a análise de dados abertos pode revelar mais do que inicialmente se pretendia comunicar (SOARES, 2014, p. 19).

Há várias iniciativas do governo federal em ações de pesquisa e desenvolvimento de produtos de tecnologia nacional, entretanto, o país ainda está fortemente dependente dos fabricantes estrangeiros, principalmente das indústrias norte-americanas.

Nos Estados Unidos da América (EUA), o órgão denominado *National Institute of Standards and Technology* (NIST) do *Department of Homeland Security* (DHS)² tem como missão promover a inovação e a competitividade industrial por meio do uso da metrologia, dos padrões e da tecnologia, com a finalidade de ampliar a segurança econômica do país e da melhoria da qualidade de vida.

O NIST possui um repositório de vulnerabilidades, *National Vulnerability Database* (NVD) que é destinado ao gerenciamento e medição do nível de segurança do governo americano. Atualmente, o NVD possui mais de sessenta mil vulnerabilidades registradas, bem como contém uma lista de milhares de empresas de TI cadastradas. Além disso, neste repositório de vulnerabilidades encontram-se informações de diversos equipamentos, inclusive daqueles adquiridos pelo governo brasileiro.

Outra forma de dar transparência pública aos atos da APF é a publicação dos resultados de auditoria realizada pelos órgãos de controle. O Tribunal de Contas da União (TCU), periodicamente, disponibiliza as deficiências encontradas nos órgãos auditados em sua página da *internet* e no DOU:

² O *United States Department of Homeland Security* (DHS) (em português: Departamento de Segurança Interna dos Estados Unidos, comumente denominado nos EUA apenas de "*Homeland Security*", é um departamento do governo dos Estados Unidos da América cuja responsabilidade é proteger o território dos EUA contra ataques terroristas e agir em caso de desastres naturais.

Observa-se também ligeira evolução no percentual de instituições que possuem processo de classificação das informações, que saltou de 11% para 17%. Entretanto, esse percentual ainda é baixo, sobretudo considerando o advento da Lei nº 12.527/2011, que regula o acesso a informações mantidas pelo Estado, haja vista que a ausência de classificação pode implicar em tratamento inadequado da informação, como a divulgação ostensiva de dados não públicos. (TCU, 2012b).

[...] Determinar, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso II, do Regimento Interno do TCU, à [...] que, em atenção aos arts. 27 a 29 da Lei 12.527/2011 e aos arts. 31 a 34 do Decreto 7.724/2012, no prazo de noventa dias a contar da ciência do decisor, elabore e publique formalmente processo para classificação e tratamento das informações no âmbito do Ministério, [...]

[...] Diante das evidências remetidas à equipe de auditoria, não foi possível identificar elementos que comprovem que as informações no âmbito do [...] têm sido efetivamente classificadas.

[...] inexistência de processos classificados após a vigência do Decreto 7.724/2012 (parágrafo 247) evidencia que, na prática, não tem ocorrido a devida classificação das informações corporativas do órgão [...] (TCU, 2014a).

No campo da SI, o termo “deficiência” está diretamente associado à fraqueza ou à fragilidade de algum ativo, definido pela ISO/IEC (2014) como vulnerabilidade. Impactos negativos poderão ser acarretados no negócio da organização, caso essas vulnerabilidades sejam exploradas por uma ou mais ameaças e como consequência a geração de riscos de SI (GSI-PR, 2013).

Expor fragilidades contraria todos os preceitos defendidos por renomados estrategistas (CLAUSEWITZ, 1996; SUN TZU, 1993), isto porque, as organizações, nos seus processos de negociação, devem administrar ou ocultar suas fraquezas (KOTLER, 1998).

No contexto da APF, a facilidade de acesso às informações governamentais pode servir para a base de construção do conhecimento de grupos maliciosos (NONAKA; TAKEUCHI, 1997). Na análise estratégica de Fernandes (2012, p. 2) sobre a constituição de um sistema de segurança e defesa cibernéticas nacionais, o autor demonstrou sensatez não expondo publicamente vulnerabilidades nível de detalhamento, pois tais informações podem ser suficientes para que haja ações adversas contra as infraestruturas críticas apresentadas:

“identificar as IEC”, “levantar e avaliar as vulnerabilidades das IECs e sua interdependência”, e “selecionar as causas e avaliar os riscos que possam afetar a segurança das IEC”; nota-se que o resultado do levantamento produz informações e conhecimento sensíveis. Sendo assim é essencial que sejam adotadas medidas de sigilo elevadas para a proteção dessas, uma vez que o vazamento de informações sobre riscos de uma das infraestruturas críticas pode produzir o efeito inverso do esperado, que seria a exposição de vulnerabilidades, especialmente se essas vulnerabilidades são de ordem

cibernética computacional, isso é, se são em controles de segurança computacional (FERNANDES, 2012, p. 25).

Além da exposição de fatores de risco que possam impactar a segurança da organização por ocasião do cumprimento do princípio da publicidade, também existem aqueles riscos referentes à pessoa, que no contexto desta pesquisa trata-se da divulgação das informações relativas aos agentes públicos da APF disponíveis na *internet*.

O citado art. 37 da CRFB traz o princípio da publicidade para todos os atos praticados pela APF, e neste rol de atos estão incluídas diversas informações divulgadas sobre os agentes públicos, tais como: remuneração, Cadastro de Pessoa Física (CPF), local de trabalho, função ou cargo, viagens efetuadas. Por outro lado, a própria CRFB, em seu art. 5º, além de garantir ao cidadão o direito individual, a proteção da intimidade e da vida privada, também, garante a igualdade entre todos, quer sejam servidores públicos, servidores da iniciativa privada ou autônomos.

A divulgação dos dados e informações sobre os servidores públicos pode ser um passo importante para o fortalecimento da transparência na APF. No entanto, uma vez executada de forma descontrolada e sem o devido tratamento da informação, pode expor vulnerabilidades que venham a comprometer não somente a intimidade e a vida privada da pessoa, bem como a segurança nacional e a segurança pública do Estado brasileiro.

Diante do exposto, cabe responder a seguinte pergunta: Quais os fatores de risco que são gerados em função da transparência na publicação de dados e informações dos agentes públicos da APF que atuam na segurança nacional e na segurança pública do Brasil?

1.3 Objetivos da Pesquisa

1.3.1 Objetivo Geral

Analisar os fatores de risco expostos na comunicação entre o governo e a sociedade, a partir da publicação dos dados e informações de agentes públicos que atuam na segurança nacional e na segurança pública federal.

1.3.2 Objetivos Específicos

- Identificar as informações comunicadas por sistemas de promoção da transparência pública, de natureza pessoal dos agentes públicos que atuam na segurança nacional e na segurança pública federal.

- Identificar os fatores de risco que impactam a privacidade dos agentes públicos que atuam na segurança nacional e segurança pública federal.
- Analisar os riscos que impactam o Estado e a sociedade no contexto da transparência.

2 REFERENCIAL TEÓRICO

Com a finalidade de fundamentar e nortear a proposta desta pesquisa foi inserido neste capítulo um referencial teórico baseado em literatura a fim de possibilitar um melhor entendimento sobre o tema proposto.

Sendo assim, foi realizada uma revisão dos principais conceitos sobre o princípio da publicidade e transparência pública na APF, privacidade, acesso à informação, gestão da informação, classificação da informação, modelos de comunicação, gestão da segurança da informação e fatores de risco.

Da mesma forma que Araujo (2010, p. 173) discutiu a respeito de “elementos necessários para integrar os campos da Biblioteconomia, Arquivologia e Museologia no âmbito da Ciência da Informação”, esta pesquisa também tenta aproximar os principais conceitos e autores da CI com os da SI, de forma a identificar os conceitos relacionados à esfera privada e com a esfera pública, neste contexto multidisciplinar.

Como resultados foram identificadas discrepâncias conceituais, e isso reforça a necessidade de ampliação de estudos e pesquisas sobre o tema SI no âmbito da CI, não se limitando apenas nas questões tecnológicas.

A citação das principais conclusões a que outros autores chegaram permite salientar a contribuição da pesquisa realizada, demonstrar contradições ou reafirmar comportamentos e atitudes. Tanto a confirmação, em dada comunidade, de resultados obtidos em outra sociedade quanto a enumeração das discrepâncias são de grande importância (LAKATOS, MARCONI, 2003, p. 255).

Para revisão da literatura, fez-se necessário buscar autores de diversos campos da ciência, principalmente da Ciência da Informação (CI), Direito e Computação, consequentemente, as referências selecionadas foram de diversas naturezas, como: leis, decretos, instruções e normas, artigos, teses e dissertações, dicionários, normativos técnicos, livros. Novamente, comprova-se que a SI pode ser também objeto de estudo na CI, pois esta:

(..) é uma ciência interdisciplinar derivada e relacionada com a matemática, a lógica, a linguística, a psicologia, a tecnologia do computador, a pesquisa operacional, as artes gráficas, as comunicações, a Biblioteconomia, a Administração e assuntos similares. (BORKO, 1968, p. 3).

2.1 Direitos e Garantias Fundamentais para o acesso à informação

2.1.1 Direito fundamental de acesso à informação

Para esta pesquisa, a expressão “acesso à informação” está relacionada ao efeito positivo do cumprimento da transparência pública. Para Jardim (2009), a noção de acesso à informação está presente nas diversas reflexões teóricas encontradas na Arquivologia, Biblioteconomia, Documentação e CI, como também, em outras áreas correlatas.

De acordo com a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), o acesso à informação é de suma importância para o desenvolvimento social do cidadão, tornando-o capaz de fazer melhores escolhas, bem como, compartilhar riquezas com os demais indivíduos da sociedade, que na visão marxista não se restringe apenas ao valor material das coisas, inclui-se principalmente a riqueza das relações humanas (UNESCO, 2014).

Sendo assim, exige-se cada vez mais dos profissionais da CI, pois estes são os elementos fundamentais para a garantia do livre acesso às informações essenciais para a sociedade atual e do futuro.

O passado demonstra que a falta de acesso às informações era a principal causa de retrocesso da humanidade. Toma-se como exemplo a Era Medieval, em que a sociedade era dividida em três classes sociais: o clero, a nobreza e a plebe. A primeira classe era formada pelos membros eclesiásticos da igreja católica que monopolizavam o conhecimento, deixando a plebe passível de manipulação pela falta de informação.

Nesse período, também chamado de Idade das Trevas, surgiram várias obras literárias e artísticas que ficavam inacessíveis à população, pois o acesso a tais obras era restrito aos membros do clero e a uma pequena parcela da nobreza. As bibliotecas daquela época encontravam-se instaladas no interior de protegidos mosteiros, como também em igrejas de difícil acesso. Isso impossibilitava a alfabetização das demais classes sociais, fomentando o avanço cultural apenas aos clérigos (MCGARY, 1999).

Além das restrições de acesso físico aos acervos bibliográficos, também existiam as restrições impostas pela religião, visto que a maioria das obras artísticas e literárias era classificada como de natureza profana:

O livro era entendido como um objeto sagrado, que deveria ser tocado apenas por iniciados, capazes de trabalhar com eles da maneira que entendiam ser a correta; por isso, na Idade Média a quase totalidade de leitores era formada por religiosos, já que “a leitura constituía

verdadeiramente o alimento espiritual dos monges (HAMESSE, 2002, p. 124).

Verifica-se que a restrição à informação no período da Idade Média era feita por dois tipos de controles de acessos. Um destinado a impedir o acesso físico à informação, como por exemplo, a dificuldade de entrar nos protegidos mosteiros, e o outro visava a implementação de níveis de permissão, nesse caso, somente aqueles eclesiásticos que tinham a necessidade de conhecer. Tal fato ainda é verificado nos dias atuais, pois há situações que o cidadão não obtém êxito no processo de aquisição de uma determinada informação de seu interesse junto aos órgãos e repartições públicas por motivos administrativos, tecnológicos e jurídicos.

Visando solucionar este problema, o art. 5º da CRFB assegura a todos brasileiros e residentes no Brasil, o acesso à informação (BRASIL, 1988). Consequentemente, esse direito fomentará a formação de novos membros da sociedade com condições necessárias para a construção de argumentos e discussões para o cumprimento de seu dever de cidadão como um gesto público (AUDARD, 2006).

Sendo assim, o acesso à informação não é somente um direito adquirido pelo cidadão, mas inclui todas as garantias que possibilitam o efetivo exercício desse direito que prevê, principalmente, os dispositivos materiais e culturais referentes ao atual ambiente virtual onde reside a informação. Não é possível garantir o acesso à informação, sem o fomento de políticas públicas de informação (JARDIM, 2009).

2.1.2 Princípio Legal da Publicidade

A origem da palavra “publicidade” vem do latim *publicus*, que significa público. Entretanto, ao longo do tempo, recebeu outras definições, tornando-se a mais comum na literatura atual, a seguinte: “conjunto de técnicas de ação coletiva no sentido de promover o lucro de uma atividade comercial conquistando, aumentando e mantendo clientes” (MALANGA, 1979, p. 12), ou seja, um meio de tornar um produto ou um serviço conhecido no mercado, visando despertar interesse dos consumidores pela coisa anunciada (SILVA Z., 1976).

Neste trabalho acadêmico, a palavra publicidade refere-se ao ato de divulgar ou de tornar público (RABAÇA; BARBOSA, 1998, p. 481), ou seja, a publicização dos atos praticados pela administração pública, como um princípio legal para a manutenção da democracia.

O art. 37 da atual Carta Magna estabelece, entre outros, a publicidade como princípio norteador da Administração Pública. Este princípio decorre da necessidade de dar transparência dos atos praticados pelo governo.

A publicidade, além de dar conhecimento aos interessados, fornece informações suficientes para que o povo, principal interessado, possa atuar no controle e na fiscalização desses atos, a fim de avaliar a atuação de seus governantes e dos agentes públicos. Para Vieira T. (2007, p. 47), a publicidade propicia conhecimento e controle de informações pelos interessados diretos e pelo povo em geral, bem como permite fiscalizar a atuação das condutas internas dos agentes públicos.

De acordo com Dellazzana (2009), à medida que ocorre a efetiva participação da sociedade no debate sobre os atos praticados pelo governo, estreita-se o relacionamento entre o princípio da publicidade e a democracia. Esta é uma prática da argumentação kantiniana que define a publicidade como uma esfera de justificação, a qual permite que os membros de uma determinada sociedade tomem decisões legítimas (OLIVEIRA, 2010).

A positivação do princípio da publicidade na CRFB resultou na publicação de diversas leis e atos administrativos sobre transparência pública, que para Pestana (2010, p. 225) é um marco da Administração Pública voltada para o interesse público, pois o Estado só é realmente considerado democrático, quando se percebe a participação do povo no processo de tomada de decisões (MARTINS JUNIOR, 2010, p.42) e para que isso aconteça, tornou-se imprescindível reduzir a desigualdade informacional na sociedade atual, por meio do amplo acesso às informações públicas (JARDIM, 1999, p. 75).

Existe uma relação direta entre o direito fundamental de acesso à informação com o princípio da publicidade. Por essa razão torna-se imprescindível a adoção de medidas voltadas a facilitar o acesso à informação para que haja a concretização do princípio da publicidade.

Indiscutivelmente, o uso de novas tecnologias associado à publicação de diversos atos administrativos vêm contribuindo para o cumprimento do princípio da publicidade (ROCHA, 1994, p. 246). Atualmente os órgãos públicos são dotados de poderosos bancos de dados que, além de possibilitar ao cidadão diversos tipos de consulta, emitem certidões e documentos, que no passado, requeriam custos e longo período de espera. O uso da *internet* para prestação de serviços públicos reduziu custos à administração pública, oferecendo considerável economia aos cofres públicos.

A disponibilização das edições dos diários oficiais dos diversos Poderes e esferas públicas em forma eletrônica na *internet* é um exemplo de medida voltada a facilitar o acesso à informação ao cidadão. No DOU eletrônico, por exemplo, são publicados diversos atos de

interesse do cidadão, que inclui desde nomeações e exonerações de agentes públicos, a publicação de atos normativos aprovados e sancionados pela União.

Notoriamente, os meios eletrônicos, em especial a *internet*, são as formas mais eficazes para publicação das informações públicas e o melhor caminho para a democratização do acesso às informações. No entanto, requer de cuidados especiais, visto o grande volume de dados e informações que estão armazenados em robustos bancos de dados dos governos.

No mesmo momento em que avançam as medidas para concretização do princípio da publicidade, verifica-se a necessidade de proteção da grande quantidade de informações disponível. Com isso, desenvolveu-se uma nova cultura de proteção para o desconhecido mundo virtual, e em consequência, foram produzidas inúmeras orientações normativas relativas a SI, especificamente para atender às exceções de sigilos impostas pela própria CRFB, concluindo-se que o princípio da publicidade não é absoluto.

As formas de aplicação do princípio da publicidade são de responsabilidade dos órgãos governamentais dos diferentes Poderes e esferas administrativas. Estes possuem liberdade para execução e regulamentação, em conformidade com as Leis vigentes, acima de tudo no que tange à publicação de dados pessoais. As consequências dessa liberdade são as diferentes formas de tratamento da informação e falta de padronização efetuada pelos órgãos de transparência pública. Sendo assim, o princípio da publicidade, na vertente pública, deve ser tratado de forma igualitária, a fim de evitar distorções e quebra de SI durante a divulgação de dados sensíveis e não públicos.

Por fim, o que mais importa para o cidadão é a prestação de contas do administrador de forma clara e transparente, de forma que todos entendam o que está publicado. Por conseguinte, criou-se o princípio da transparência a fim de fortalecer o princípio constitucional da publicidade.

2.1.3 Transparência e opacidade informacional

Para Resende (2006, p. 138), a transparência é definida como “abrangente disponibilidade de informação relevante e confiável” que tem como objetivo principal “garantir a todos cidadãos, individualmente, por meio de diversas formas em que costumam se organizar, acesso às informações que explicitam as ações a serem praticadas pelos governantes” (SILVA L., 2004, p. 10).

Entretanto, o controle da informação sempre foi o principal instrumento utilizado pelas classes dominadoras na história da humanidade. Aquele que detinha as informações dava um

passo à frente de seu oponente ou concorrente. Os governantes utilizavam-se de todos os artifícios para ocultarem informações dos seus governados. Essa é uma característica típica de regimes ditatoriais, uma vez que “a opacidade informacional beneficia e é favorecida pela reprodução e ampliação do controle do Estado”, mantendo a hegemonia da classe dominante, perante a classe dominada (JARDIM, 1999, p. 21).

Diante do exposto, remete-se o entendimento de opacidade informacional apenas para o significado de controle abusivo das informações. Porém, Rezende (2002) defende que aquilo que é comunicável possui valores, de ordem social, econômico ou jurídico, e a credibilidade das informações só será obtida por meio de medidas sociais que equilibram os efeitos de transparências e opacidades. Nesse contexto, a implementação da SI torna-se o melhor mecanismo para equilibrar o que é comunicável com a proteção do comunicável.

Para Jardim (1999, p. 24), tanto a transparência, quanto a opacidade informacional constituíam-se, naquela época, como temas “ainda não contemplados como objeto de pesquisa na Ciência da Informação”.

Entretanto, nos dias atuais, já existem estudos e pesquisas abordando tal discussão, principalmente, quanto ao acesso, ao uso e à disseminação da informação. Maroco (2011, p. 113) esclarece, que no Brasil, um país que tem como a publicidade um dos princípios constitucionais, é gerado um paradoxo entre os temas, limitação de acesso à informação *versus* transparência plena e ampla.

Os graus de opacidade e de transparência estão diretamente relacionados ao tipo de estratégia a ser definida em cada área de interesse, como por exemplo, na relação Estado e cidadão, a opacidade pode ser determinada pela restrição de acesso à informação ou até mesmo pelo emprego de controles de segurança da informação. Já a transparência, pode ser percebida no cumprimento às leis e normativos que garantem ao cidadão o acesso às informações públicas.

Tanto a transparência quanto a opacidade informacional estão presentes na relação do Estado com a sociedade. Esses fenômenos geram conflitos dentro da máquina administrativa, envolvendo o administrador público, o profissional da informação e o cidadão (JARDIM, 1999, pag. 73). A própria LAI exemplifica essa questão ao definir o amplo acesso às informações governamentais em prol da transparência, e também, ao definir as mínimas restrições de acesso.

Esse conflito também é gerado entre os diferentes normativos, há os que fomentam os princípios fundamentais da publicidade e da transparência. Por outro lado, há aqueles voltados à restrição de acesso. O GSI-PR (2014a, p. 8) corrobora com essa observação quando alerta

aos órgãos da APF que “a informação a ser disponibilizada por meio da transparência ativa e passiva deve ser objeto de prévia análise, a fim de que se identifiquem parcelas da informação com restrição de acesso”.

No início de 1964, ainda na vigência da Constituição de 1946, foi publicada a Lei nº 4.320/64, estabelecendo as diretrizes para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal. Essa Lei foi o marco na aplicação do princípio da transparência orçamentária (SOUZA, 2009, p. 9):

Art. 2º A Lei do Orçamento conterà a discriminação da receita e despesa de forma a evidenciar a política econômica financeira e o programa de trabalho do Governo, obedecidos os princípios de unidade universalidade e anualidade.

§ 1º Integrarão a Lei de Orçamento:

- I - Sumário geral da receita por fontes e da despesa por funções do Governo;
 - II - Quadro demonstrativo da Receita e Despesa segundo as Categorias Econômicas, na forma do Anexo nº. 1;
 - III - Quadro discriminativo da receita por fontes e respectiva legislação;
 - IV - Quadro das dotações por órgãos do Governo e da Administração.
- (BRASIL, 1964).

A CRFB, em seu art. 163, preconizava a necessidade de uma Lei Complementar para dispor sobre o tema “finanças públicas”. Fulcro dessa determinação foi a promulgação da Lei Complementar nº 101/2000 estabelecendo “normas de finanças públicas voltadas para a responsabilidade na gestão fiscal” (BRASIL, 2000b). Em 2009, os dispositivos dessa lei receberam acréscimos pela Lei Complementar nº 131, a qual dava incentivo à participação popular por meio de audiências públicas e à liberação ao pleno conhecimento e acompanhamento da sociedade em meios eletrônicos de informações sobre a execução orçamentária e financeira do país (BRASIL, 2009):

Art. 48. São instrumentos de transparência da gestão fiscal, aos quais será dada ampla divulgação, inclusive em meios eletrônicos de acesso público: os planos, orçamentos e leis de diretrizes orçamentárias; as prestações de contas e o respectivo parecer prévio; o Relatório Resumido da Execução Orçamentária e o Relatório de Gestão Fiscal; e as versões simplificadas desses documentos (BRASIL, 2000b).

No âmbito do Poder Executivo Federal, a divulgação de dados e informações foi disciplinada pela Portaria Interministerial nº 140 de 16 de março de 2006. Tal normativo foi elaborado em ato conjunto do Ministério do Planejamento, Orçamento e Gestão (MP) com a CGU e tem como destaque, o uso da rede mundial de computadores para o fortalecimento da transparência pública na comunicação entre governo e cidadão:

Art. 2º Os órgãos e entidades da Administração Pública Federal deverão manter em seus respectivos sítios eletrônicos na rede mundial de computadores página denominada “Transparência Pública”, tendo por conteúdo mínimo as informações previstas nesta Portaria. [...]

Art. 5º O acesso às páginas de Transparência Pública de cada órgão e entidade da Administração Pública Federal, deverá ser efetuado por meio de atalho em imagem gráfica, conhecida como banner, com identidade visual específica para a Transparência Pública, constante da página inicial de seu respectivo sítio, sempre em endereço estruturado como “www.domínio do órgão/transparencia”.

§ 1º As informações a que se refere esta Portaria também poderão ser obtidas na página do Portal da Transparência do Governo Federal, por meio dos endereços eletrônicos www.transparencia.gov.br, www.portaldatransparencia.gov.br ou www.portaltransparencia.gov.br (BRASIL, 2006).

A LAI estabelece procedimentos destinados a assegurar ao cidadão o acesso às informações públicas, tendo como uma das diretrizes estabelecidas o fomento ao desenvolvimento da cultura de transparência na administração pública. Para isso, torna-se imprescindível que os órgãos da administração pública criem locais de fácil acesso, obrigatoriamente em seus sítios oficiais na *internet*, a fim de promover a divulgação de suas informações, independente de solicitação, a chamada “transparência ativa”. No entanto, esses sítios deverão atender diversos critérios, inclusive de garantir a autenticidade e integridade das informações neles disponibilizados (BRASIL, 2011).

O Decreto nº 7.724 de 2012, que regulamentou a LAI no Poder Executivo Federal, além de trazer a obrigação do uso da *internet* para promoção da transparência ativa, determinou a criação de um serviço de informação ao cidadão, com o objetivo de atender e orientar o público quanto ao acesso à informação, informar sobre a tramitação de documentos nos órgãos da APF e receber e registrar pedidos de acesso à informação. O serviço de informação ao cidadão é uma forma de transparência passiva, que de acordo com a CGU, consiste na “disponibilização de informações públicas em atendimento a demandas específicas de uma pessoa física ou jurídica”.³

Em cumprimento ao disposto no art. 41 da LAI, coube a CGU, órgão que em 2004 teve a iniciativa de criar o “Portal da Transparência”, a responsabilidade de gerenciar o fomento da cultura e treinamento sobre o tema transparência pública para toda as esferas governamentais:

³ Transparência passiva - Disponível em: <http://www.acessoainformacao.gov.br/perguntas-frequentes-2/aspectos-gerais-da-lei#11> Acesso: 11 dez 2014.

O Poder Executivo Federal designará órgão da administração pública federal responsável: I - pela promoção de campanha de abrangência nacional de fomento à cultura da transparência na administração pública e conscientização do direito fundamental de acesso à informação; II - pelo treinamento de agentes públicos no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública; (BRASIL, 2011)

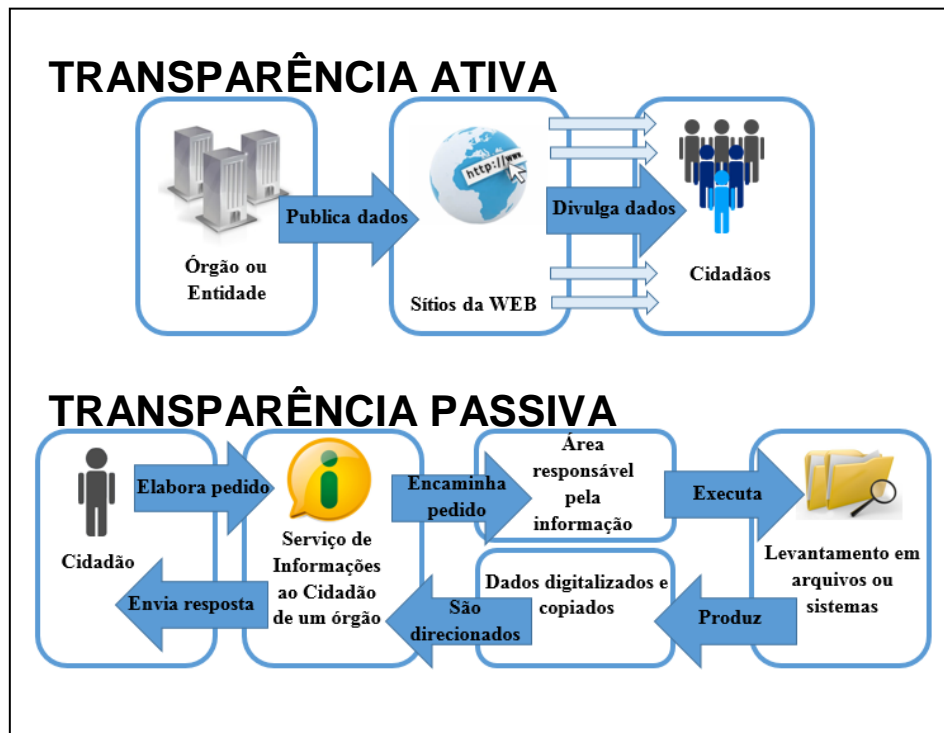
Art. 68. Compete à Controladoria-Geral da União, [...] II - promover campanha de abrangência nacional de fomento à cultura da transparência na administração pública e conscientização sobre o direito fundamental de acesso à informação; III - promover o treinamento dos agentes públicos e, no que couber, a capacitação das entidades privadas sem fins lucrativos, no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública (BRASIL, 2012a).

A transparência pública ativa não se resume apenas ao “Portal da Transparência”, existem outros canais e serviços em que os órgãos da APF se comunicam de forma ativa com o cidadão, como exemplos: as publicações do DOU, os resultados de julgamentos do TCU, os diversos portais dos órgãos na *internet*.

2.1.4 Canais de Promoção da Transparência

Os diversos modelos de comunicação estabelecem que a escolha do canal onde a informação será transmitida é de competência do emissor, cabendo a ele a definição dos critérios e requisitos básicos para que o receptor obtenha êxito no entendimento da mensagem. Com essa preocupação, a CGU determinou o uso da transparência ativa por meio da *internet* para as informações de caráter geral. Esta ação reduz o custo com a prestação de informações, bem como o acúmulo de pedidos de acesso sobre temas semelhantes. Diferente da transparência passiva, onde administração pública incorre em custos com pessoal e serviços e consegue atender somente a quem solicitou a informação. A obrigação do uso da *internet* para o cumprimento da transparência ativa é primordial para redução de custos e agilização dos processos. Porém, pelo fato de constituírem um grande volume de informações aberto ao mundo virtual, maiores controles de SI deverão ser adotados, principalmente nos aspectos da quebra da integridade e confidencialidade das informações. Uma vez publicadas as informações não íntegras e sensíveis, o dano pode ser irreversível. Diferentemente da transparência passiva, onde existe um processo de tramitação formalizada e a comunicação é feita diretamente ao solicitante. A Figura 1 apresenta o processo da transparência ativa e passiva.

Figura 1: Transparência ativa e passiva.



Fonte: Adaptado do Portal da Transparência (CGU), 2014.

2.1.4.1 Portal da Transparência do Governo Federal

Neste portal, disponível desde 2004, qualquer cidadão interessado pode acompanhar o emprego dos recursos públicos do governo federal. Nele poderão ser obtidas as informações sobre despesas, receitas, convênios, sanções, servidores, imóveis funcionais de propriedade da União.

Recentemente, a Universidade de Brasília (UnB) por meio de um acordo com a CGU realizou uma Pesquisa de Avaliação do Portal da Transparência do Governo Federal, onde foram coletadas diversas opiniões dos usuários visando obter subsídios para reestruturação do portal. Nessa pesquisa foram identificadas as seguintes informações sobre o Portal da Transparência: o perfil dos usuários, os conteúdos por eles acessados, a avaliação dos usuários e as sugestões de melhoria que poderiam ser adotadas pela CGU (UNB, 2014).

Dos itens avaliados, destaca-se que 71,5% dos respondentes avaliaram o Portal da Transparência como uma ferramenta eficaz para a divulgação de gastos do governo federal. Entretanto, 75% dos entrevistados estão insatisfeitos e muito insatisfeitos com o funcionamento da democracia no país, conforme demonstra a Tabela 1.

Tabela 1: Nível de satisfação em relação ao funcionamento da democracia no país.

Categorias	Frequência	Proporção (%)
Muito satisfeito	45	2,7
Satisfeito	300	18,2
Insatisfeito	675	40,9
Muito insatisfeito	563	34,1
Não respondeu	66	4,0
Total	1649	100

Fonte: Pesquisa de Avaliação do Portal da Transparência (UNB, 2014).

Quanto à facilidade de localizar as informações no Portal da Transparência, a citada pesquisa apontou que 70,4% consideram o portal de fácil a muito fácil navegação. O cidadão ao acessar o *site*, abrirá a página inicial (Figura 2) com todos os tipos de consultas possíveis, referentes às despesas, receitas, convênios, sanções, servidores, imóveis funcionais. Além dessas consultas, o portal possibilita baixar diversos arquivos, onde as informações são dispostas em formato aberto.

Figura 2: Tela inicial do Portal da Transparência.



Fonte: Portal da Transparência (CGU), 2014.

A pesquisa também apontou que quase 60% dos respondentes consideraram que o Portal da Transparência não possui a funcionalidade de associar e cruzar dados e informações. Nesse aspecto, é preciso uma melhor reflexão dos gestores do Portal, a fim de verificar se tal

cruzamento pode oferecer riscos a SI, pois, há outros *sites* que fomentam a transparência ativa. Isso significa que é preciso analisar se os controles de SI adotados no Portal da Transparência, também são adotados por outros portais. A Figura 3 exemplifica uma forma de controle de SI, ao qual não se divulga o CPF na íntegra.

Figura 3: Tela do Portal da Transparência referente ao servidor público.



Fonte: Adaptado do Portal da Transparência (CGU), 2014.

Outro fator que deve ser considerado sobre o número do CPF é que este comunica uma informação que pode ser de interesse para uma pessoa, empresa ou sistema. O nono dígito, que é informado no Portal da Transparência, indica qual o estado da federação que o CPF pertence e foi gerado, conforme apresentado no Quadro 1. Essa informação não afirma, mas sugere que o dono do CPF é natural do Estado indicado ou então reside ou residiu nele.

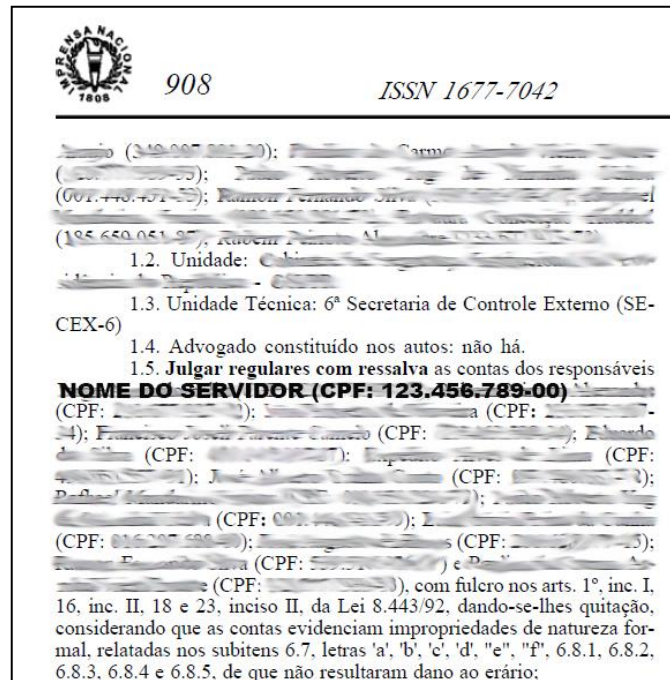
Quadro 1: Identificação da origem do CPF por Unidades Federativas.

Nono dígito do CPF (xxx.xxx.xx X -xx)	UNIDADES FEDERATIVAS
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso do Sul, Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia e Roraima
3	Ceará, Maranhão, Piauí
4	Alagoas, Paraíba, Pernambuco, Rio Grande do Norte
5	Bahia, Sergipe
6	Minas Gerais
7	Espírito Santo, Rio de Janeiro
8	São Paulo
9	Paraná, Santa Catarina

Fonte: O autor.

Como visto, a CGU empregou um tipo de controle de SI ao divulgar os CPF dos servidores da APF, porém, nenhuma ação foi implementada durante a divulgação do CPF do mesmo servidor no DOU, conforme exemplificado na Figura 4.

Figura 4: Tela do Diário Oficial da União



Fonte: Adaptado do DOU, 2014.

2.1.4.2 Portal do DOU

A história da Imprensa Nacional, instituição pública responsável pelo DOU, confunde-se com a história do Brasil, entretanto, esta pesquisa abordará os seus aspectos a partir da inserção do DOU em sua forma completa na *internet*.

Visando ampliar a democratização da informação ao cidadão brasileiro por meio do acesso aos atos publicados pelo governo federal, o art. 2º do Decreto nº 4.520 de 2002, que dispõe sobre a publicação do DOU preconiza que:

Art. 2º São obrigatoriamente publicados, na íntegra, no Diário Oficial da União:

I - as leis e demais atos resultantes do processo legislativo do Congresso Nacional;

II - os tratados, as convenções e outros atos internacionais aprovados pelo Congresso Nacional e os respectivos decretos de promulgação;

- III - as medidas provisórias, os decretos e outros atos normativos baixados pelo Presidente da República;
- IV - os atos dos Ministros de Estado, baixados para a execução de normas, com exceção dos de interesse interno;
- V - os pareceres do Advogado-Geral da União e respectivos despachos presidenciais, salvo aqueles cujos efeitos não tenham caráter geral;
- VI - dispositivos e ementas das ações diretas de inconstitucionalidade, das ações declaratórias de constitucionalidade e das arguições de descumprimento de preceito fundamental decorrente da Constituição;
- VII - julgamentos do Tribunal de Contas da União; e
- VIII - atos de caráter normativo do Poder Judiciário (BRASIL, 2002a).

Não cabe à Imprensa Nacional a verificação de quebra de SI, por ocasião da publicação do DOU. O conteúdo da publicação é de responsabilidade do órgão responsável pelo envio da matéria ou documento a ser divulgado. A Imprensa Nacional garante a autenticidade das publicações no DOU por meio da certificação digital emitida por autoridades certificadoras integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), garantindo os mesmos efeitos legais produzidos pela versão impressa (BRASIL, 2002a).

De acordo com a Portaria nº 268 de 2009 da Imprensa Nacional, o DOU é dividido em seções que no portal é identificado como jornal (IMPrensa NACIONAL, 2009). O Quadro 2 apresenta a divisão do DOU com seus referidos assuntos, que facilitam a busca no portal do DOU por ocasião de uma pesquisa avançada de algum termo específico (Figura 5).

Quadro 2: Divisão do DOU por assuntos.

Cadernos	Assuntos
Seção 1 ou DOU1	<ul style="list-style-type: none"> • Decisões relativas a Ação Direta de Inconstitucionalidade e Ação Declaratória de Constitucionalidade; • Leis, emendas à Constituição, decretos legislativos, resoluções e demais atos resultantes do processo legislativo; • Tratados, acordos, convenções e outros atos internacionais aprovados pelo Congresso Nacional e os respectivos decretos de promulgação; • Decretos, medidas provisórias e demais atos baixados pela Presidência da República; • Atos normativos do Poder Executivo, de interesse geral, excetuando-se os de caráter interno; • Pareceres do Advogado-Geral da União e respectivos despachos presidenciais, excetuando-se os de caráter interno; • Atos do Tribunal de Contas da União de interesse geral;

	<ul style="list-style-type: none"> • Atos normativos do Poder Judiciário e do Ministério Público da União, excetuando-se os de caráter interno; • Atas dos órgãos dos Poderes da União com publicidade exigida por legislação específica.
Seção 2 ou DOU2	<ul style="list-style-type: none"> • Atos relativos a pessoal dos servidores civis e militares da União, de suas autarquias e das fundações públicas, bem como dos servidores dos Poderes Legislativo e Judiciário e do Ministério Público da União, cuja publicação decorrer de disposição legal.
Seção 3 ou DOU3	<ul style="list-style-type: none"> • Extratos de instrumentos contratuais (acordos, ajustes, autorizações de compra, cartas-contrato, contratos, convênios, notas de empenho, ordens de execução de serviço, protocolos, termos aditivos e instrumentos congêneres), extratos de dispensa e inexigibilidade de licitação, distrato, registro de preços, rescisão, editais de citação, intimação, notificação e concursos públicos, comunicados, avisos de licitação, dispensa e inexigibilidade de licitação, registro de preços, anulação, revogação entre outros atos da administração pública decorrentes de disposição legal.
Diário da Justiça ou DJ	<ul style="list-style-type: none"> • Atos de caráter judicial dos órgãos do Poder Judiciário, dos Conselhos de Justiça, do Ministério Público da União, da Ordem dos Advogados do Brasil, do Serviço Notarial e de Registro e do Superior Tribunal de Justiça Desportiva.
Subseção Ineditoriais ou eDJF1	<ul style="list-style-type: none"> • Atos emanados das Seções Judiciárias da Justiça Federal nos Estados, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais e dos Tribunais de Justiça dos Estados (Comarcas), decorrentes de disposição legal ou decisão judicial, mediante pagamento da parte interessada.

Fonte: Adaptação da Portaria nº 268/2009 (IMPrensa NACIONAL, 2009).

Figura 5: Tela da pesquisa avançada no DOU.

BRASIL Acesso à informação Participe Serviços Legislação Canais

Ir para o conteúdo Ir para o menu Ir para a busca Ir para o rodapé

ACESSIBILIDADE ALTO CONTRASTE MAPA DO SITE

Imprensa Nacional

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Buscar no portal

INCom - Envio de Matérias | e-Diários - Assinatura Eletrônica | INBusca - Alerta de Publicação | Contato

TIPO DE PESQUISA PESQUISA AVANÇADA LEITURA DE JORNAIS EDIÇÕES EXTRAS SUPLEMENTOS

Informe o termo:

Selecione o Jornal: Todos DOU1 DOU2 DOU3 DJ eDJF1

Tipo de Pesquisa: Exata Fonética Data Inicial: Data Final: / Ano:

Verificação de autenticidade

Fonte: DOU (Imprensa Nacional), 2014.

O portal do DOU possui uma ferramenta que possibilita buscas seletivas na base de dados textuais chamada de IN Busca Total. Para acessar o sistema basta que o interessado efetue seu cadastro e configure sua busca preenchendo os itens de pesquisa desejados, conforme apresentado na Figura 6. Após esse processo, toda vez que for mencionado o termo pesquisado, o solicitante receberá em sua caixa de correio eletrônico os endereços dos referidos jornais publicados no *site*.

Figura 6: Tela do Sistema IN Busca Total.

Fonte: DOU (Imprensa Nacional), 2014.

2.1.4.3 Padrões mínimos para portais governamentais

Além do Portal da Transparência e do portal do DOU, os órgãos da APF também se comunicam com o cidadão por meio de seus respectivos portais na *internet*. Eles são padronizados por um modelo desenvolvido pelo MP denominado Modelo de Acessibilidade em Governo Eletrônico (eMAG). Este modelo estabelece um conjunto de recomendações a ser considerado para que o processo de acessibilidade dos sítios e portais do governo brasileiro seja conduzido de forma padronizada e de fácil implementação, além de considerar:

a necessidade de assegurar a todos interessados, independente de suas capacidades físico-motoras, perceptivas, culturais e sociais, o acesso à informação disponível, resguardados os aspectos de sigilo, restrições administrativas e legais, e em respeito a valores de igualdade, respeito e transparência (MP, 2007, p. 1).

A quebra da SI nos portais dos órgãos da APF tem um impacto significativo na confiabilidade e na imagem do órgão perante o cidadão. De acordo com o guia de administração de sítios elaborado pelo MP (2012a, p. 22), “os sítios oficiais devem garantir a

confidencialidade das informações de caráter pessoal armazenadas em suas bases de dados, sejam elas relativas aos usuários ou pessoas que compõem a Administração Pública”. Observa-se que não houve uma preocupação com a garantia da confidencialidade das informações de caráter organizacional, gerando riscos de SI que podem comprometer o funcionamento e a continuidade da organização.

A Instrução Normativa nº 4 da Secretaria de Logística e Tecnologia da Informação (SLTI) do MP, de 12 de novembro de 2010, determina que os órgãos da APF, integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP), que inclui todos os ministérios do Poder Executivo, deverão elaborar um Plano Diretor de Tecnologia da Informação (PDTI) como um “instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período” (MP, 2010).

O MP publicou um Guia de Elaboração de PDTI, que tem por finalidade disponibilizar informações para auxiliar os órgãos da APF no processo de elaboração, em fases, de seus respectivos PDTI (MP, 2012b, p. 10).

As fases que compõem o processo de elaboração do PDTI são: preparação, diagnóstico e planejamento. Na fase de diagnóstico, busca-se compreender a situação atual da TI na organização para identificar os problemas ou oportunidades, que se espera resolver. Nesta fase, são incluídas diversas informações como: pontos fortes e fracos, quantitativos e descrição da arquitetura de TI e soluções de *softwares* existentes, necessidades de recursos tecnológicos e humanos. Neste momento não são diagnosticados indícios de quebra de SI. Entretanto, na fase final do planejamento, há uma determinação de publicização do PDTI nos portais dos respectivos órgãos da APF. Isso significa que o funcionamento interno do órgão, bem como suas deficiências em diversos aspectos da TI estarão disponíveis na *internet*.

A EGTI propõe a publicação do resumo do PDTI no Diário Oficial da União. O resumo do PDTI pode conter informações sobre a aprovação interna do documento no órgão (com a data), a indicação do instrumento normativo que aprovou o PDTI, e do que designou o comitê de elaboração, a abrangência e o período de validade do PDTI. É importante que contenha a referência ao sítio onde pode ser encontrada a versão final/aprovada, na íntegra, do documento.

- Recomenda-se também a publicação do PDTI, em formato PDF ou HTML, no portal do SISP, para compartilhamento com os demais órgãos membros do SISP. O endereço para publicação é: <http://www.sisp.gov.br> → Comunidade SISP → Arquivos → PDTI – Elaboração e Monitoramento → PDTI dos órgãos (MP, 2012b, p. 70).

2.1.5 O Direito à privacidade e a proteção de dados pessoais

Desde o século XVI, o direito à privacidade vem sendo incluído com uma garantia fundamental do indivíduo nos ordenamentos jurídicos de diversos países. Por exemplo, a Constituição dos Estados Unidos da América de 1791 garante ao cidadão americano, além de outros, o direito à inviolabilidade da pessoa e de suas residências. A partir daí, aprofundou-se os estudos sobre esse tema, até que em 1890, Warren e Brandeis publicaram o famoso artigo *The Right to Privacy*, considerado o primeiro estudo jurídico sobre privacidade (GAMIZ, 2012, p. 12 e 21).

No fim do século XIX, a proteção da privacidade tornou-se uma nova preocupação no campo jurídico. Tal fato sucedeu-se após a invenção da máquina fotográfica instantânea que, conseqüentemente, despertou a atenção da imprensa sensacionalista, e com isso, o significado de privacidade ganhou um novo entendimento, não se resumindo apenas ao direito do indivíduo de estar só (WARREN; BRANDEIS, 1890; GAMIZ, 2012, p. 26).

Nessa mesma direção, a Organização das Nações Unidas (ONU) incluiu na Declaração Universal dos Direitos Humanos a seguinte recomendação para seus Estados-Membros: “Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques” (ONU, 1948). A CRFB também garantiu ao cidadão a inviolabilidade da vida privada, bem como o direito à intimidade, que para Gamiz (2012) tornou-se uma questão de difícil entendimento, pois, envolve aspectos que remetem a diversos âmbitos de proteção, como a honra, imagem, intimidade e vida privada.

Nos últimos anos, com a “evolução das novas tecnologias de informações” (CASTELLS, 1999, p. 43) e com o crescimento descontrolado da *internet*, a comunicação entre os indivíduos passou pela primeira vez a ser considerada de “muitos com muitos” em uma escala global, e com isso, criou-se uma nova abordagem sobre o tema privacidade, principalmente em relação aos dados das pessoas expostos em ambientes virtuais (CASTELLS, 2003, p. 8). Tais dados são vendidos e trocados por diversas empresas e escritórios virtuais, gerando uma violação do direito à privacidade daqueles que não consentiram no tráfego de suas informações na *internet*.

Recentemente, a Assembleia Geral da ONU aprovou, por consenso da maioria de seus Estados Membros, uma resolução proposta pelo Brasil e Alemanha que trata sobre: o direito à privacidade na era digital, com isso, a ONU reconhece que o direito humano à privacidade também inclui as informações pessoais disponibilizadas no mundo cibernético.

Reafirmando o direito humano à privacidade, segundo o qual ninguém será sujeito a interferências arbitrárias ou ilegais em sua privacidade, família, domicílio ou correspondência, e o direito à proteção da lei contra tais interferências, e reconhecendo que o exercício do direito à privacidade é importante para a realização do direito à liberdade de expressão e opinião sem interferência e do direito à liberdade de reunião e associação pacífica, e é um dos fundamentos de uma sociedade democrática (ONU, 2013).

A Lei nº 7.232 de 1984 dispõe sobre a política nacional de informática cujo objetivo é a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira. Um dos seus princípios é o “estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas” (BRASIL, 1984). Isto reforça o contido na CRFB que “todos são iguais perante a lei, sem distinção de qualquer natureza” (BRASIL, 1988).

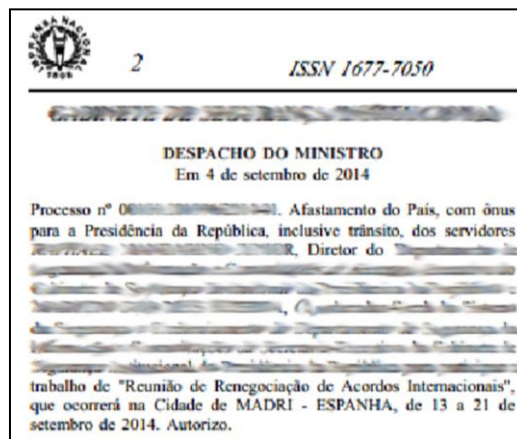
Entretanto, há uma discussão sobre a publicação das informações atinentes aos servidores públicos, como por exemplo, sua remuneração e seus dados cadastrais. A CGU afirma que a divulgação da remuneração dos servidores da APF não viola o direito de privacidade e que tal ação garante a transparência dos gastos públicos previsto na LAI. O Superior Tribunal Federal (STF) também interpreta dessa forma, visto que, quando se discute a legalidade da publicação de informações funcionais e remunerações dos servidores públicos não há interferência na vida privada e nem na intimidade. Entretanto, o próprio STF alerta sobre os riscos gerados tanto para o servidor público, como para sua família com tais divulgações, que somente serão atenuados com a proibição da divulgação do CPF, endereço residencial e carteira de identidade.

Não cabe falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo ‘nessa qualidade’ (§6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. (STF, 2011).

Fica assim evidenciado que há divergências entre a decisão tomada pelo STF (2011) com as publicações do governo sobre informações dos servidores públicos, pois, a publicação do CPF tornou-se uma prática usual em diversos portais do governo federal.

Destaca-se ainda, que existem outras formas de divulgação de informações de agentes públicos que também podem interferir na sua vida privada, como por exemplo, a divulgação de afastamento do país por motivo de serviço. Tal fato sugere que durante sua ausência, seu lar ficou desprovido da sua presença, conseqüentemente, tanto sua residência e sua família ficaram mais vulneráveis durante esse período. A Figura 7 apresenta a publicação de afastamento do país de um determinado servidor público.

Figura 7: Exemplo de publicação de afastamento de servidor no DOU.



Fonte: DOU (Imprensa Nacional), 2014.

São muitos os desafios para preservar a privacidade de uma pessoa diante do ambiente virtual que é a *internet*. A exposição de informações pessoais está além dos prejuízos que afetam a reputação e a dignidade da pessoa, há questões relativas à segurança que pode impactar o titular dos dados, a sua família e se tratando de um agente público, pode impactar a organização em que este trabalha.

Frente às ameaças virtuais, o Brasil disciplinou o uso da *internet* na Lei nº 12.965 de 2014, também conhecida como Marco Civil da *Internet* (BRASIL, 2014). Esta Lei objetiva o direito de acesso à *internet* a todos os cidadãos e o acesso à informação, fortalecendo o princípio da publicidade, por outro lado, inclui o direito da inviolabilidade da intimidade e da vida privada, fortalecendo assim o princípio da privacidade.

Para tal, torna-se imprescindível identificar se um determinado dado, ao ser divulgado, é pessoal ou não, e se essa divulgação pode afetar a privacidade ou vida do indivíduo. Diante desse problema, o Reino Unido publicou em 1998, uma orientação normativa conhecida como

*Data Protection Act (DPA)*⁴ que visa estabelecer passos, formulados em 8 (oito) perguntas descritas abaixo, que determinam se um dado é de carácter pessoal (DPA, 1998).

- **Pergunta 1:** Pode um indivíduo ser identificado a partir dos dados, ou, a partir dos dados e outras informações, ou é passível de entrar em posse de qualquer das partes?

SIM – Passar para a Pergunta 2.

NÃO – Os dados não são “dados pessoais”.

- **Pergunta 2:** O dado se refere à vida identificável do indivíduo, seja na vida pessoal ou familiar, nos negócios ou na profissão?

SIM – Os dados são “dados pessoais”.

NÃO – Os dados não são “dados pessoais”.

INCERTO – Ver as perguntas de 3 a 8.

- **Pergunta 3:** Está claro que o dado trata de um indivíduo em particular?

SIM – Os dados são “dados pessoais”.

NÃO – Passar para a Pergunta 4.

- **Pergunta 4:** Os dados são "ligados a" um indivíduo de modo que ele forneça informações particulares sobre esse indivíduo?

SIM – Os dados são “dados pessoais”.

NÃO – Passar para a Pergunta 5.

- **Pergunta 5:** Os dados são usados, ou estão para serem utilizados, para informar ou influenciar as ações ou decisões que afetam um indivíduo identificável?

SIM – Os dados são “dados pessoais”.

NÃO – Passar para a Pergunta 6.

- **Pergunta 6:** Os dados são "ligados a" um indivíduo de modo que ele forneça informações particulares sobre esse indivíduo?

SIM – Os dados são susceptíveis de serem dados pessoais.

NÃO – Passar para a Pergunta 7.

INCERTO – Passar para a Pergunta 7.

⁴ DPA (1998) – Data Protection Action – Lei que regula a obtenção, detenção, utilização e divulgação de dados pessoais no Reino Unido. Disponível em <http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf>. Acesso em: 12 de jun. 2015.

- **Pergunta 7:** Os dados focam ou se concentram no indivíduo como seu tema central, em vez de alguma outra pessoa, ou algum objeto, transação ou evento?

SIM – Os dados são susceptíveis de serem dados pessoais.

NÃO – Passar para a Pergunta 7.

INCERTO – Passar para a Pergunta 7.

- **Pergunta 8:** Os dados impactam ou têm o potencial de ter impacto sobre um indivíduo, quer seja na capacidade pessoal, familiar, comercial ou profissional?

SIM – Os dados são “dados pessoais”.

NÃO – Os dados são susceptíveis de serem dados pessoais.

Atualmente, o principal motivo que leva à erosão da privacidade é o forte interesse por informações pessoais. O Estado, no cumprimento do seu dever perante a sociedade, necessita de diversas informações dos cidadãos. Isso faz com que ele se torne um dos principais agressores do direito à privacidade. Entretanto, a erosão da privacidade está além da ingerência do Estado na vida da pessoa, pois na lista de agressores estão incluídas as empresas privadas, a sociedade e os próprios indivíduos titulares dos dados pessoais (VIDAL, 2010).

2.2 Aspectos Relevantes da Gestão da Informação para a Segurança da Informação

2.2.1 Dado e Informação

Segundo Robredo (2003), os dados constituem-se de uma série de observações ou fatos que podem ser representados em forma de números e palavras, porém, sem um significado próprio. Eles são considerados apenas como uma base para a construção de uma informação. São facilmente estruturados, obtidos por máquinas e transferíveis, tornando-se “observações sobre o estado do mundo” (DAVENPORT, 1998, p. 19).

Na comunicação telegráfica, os dados são representados por pontos e traços. Na computação, por 0 e 1. Na eletricidade, como ausência ou presença de sinal. Mas independente da área de ciência, o dado sempre será a matéria-prima da informação e com isso, precisam ser organizados e controlados de forma adequada, a fim de proporcionar valores às atividades organizacionais.

Com a evolução tecnológica e o uso da *internet*, a produção de dados cresceu de uma forma incontrolável. Bush (1945) descreve em seu artigo *As we may think* que o ser humano seria incapaz de processar e tratar com um grande volume de dados e para isso seria

necessário repensar em novas tecnologias e sistemas de armazenamento e processamento. Como resultado propôs o “Memex”.

Considere um dispositivo futuro para uso individual, que é uma espécie de biblioteca e arquivo mecanizado e privado. Ele precisa de um nome, e, para cunhar uma ao acaso, "Memex" assim será. Um Memex é um dispositivo no qual um indivíduo armazena todos os seus livros, registros e comunicações, e que é mecanizado de modo que possa ser consultado com extrema velocidade e flexibilidade. É um suplemento pessoal íntimo e alargada à sua memória.

Ele consiste de uma mesa, e enquanto ele pode, presumivelmente, ser operada a distância, é, sobretudo a peça de mobiliário em que ele trabalha. Na parte superior são oblíquos telas translúcidas, em que o material pode ser projetados para leitura conveniente. Há um teclado, e conjuntos de botões e alavancas. Caso contrário, ele se parece com uma mesa comum. (BUSH, 1945, tradução nossa).

Nos dias atuais, as pessoas e organizações possuem o conhecimento de como processar e armazenar grandes volumes de dados. Existem diversos Sistemas de Gerenciamento de Banco de Dados (SGBD), como também, diversos administradores desses bancos de dados. Entretanto, a maior dificuldade é de como usar tal volume de dados, principalmente no aspecto da segurança.

Pelo fato de ser considerado ainda como um elemento bruto para a formação de uma informação e posterior conhecimento, as organizações não se preocupam com a exposição de seus dados. Aparentemente um dado isolado pode não comunicar algo, mas associado com outro dado, já pode revelar indícios de uma estrutura informacional.

Silva C. (2014, p.23) defende que determinados arquivos, mesmo que seus respectivos identificadores não estejam acompanhados por um campo de dados, já podem ser considerados dado pessoal. Ele exemplifica o caso de uma listagem contendo apenas números de identidade pessoal, cuja identificação do arquivo é “HIV”.

(...) qualquer elemento que caracterize ao ser humano, por menor que seja, e respeitadas as diferentes gravidades, deve ser protegido. Pois o dado transformado em conhecimento transforma-se em Poder para quem o detém e pode significar constrangimentos e até subjugação para aquele que se torna um pouco mais desvelado (SILVA C., 2014, p. 23-24).

Assim sendo, a partir do momento que são agregados alguns valores a um determinado dado, este abandona sua forma puramente sintática e ingressa na forma semântica. É o início da transformação de um dado em informação.

Para a CI, a informação é muito mais do que um processo de transformação de dados com regras definidas que contém algum significado. Para Le Coadic (2004, p. 2), é um

“conhecimento inscrito (gravado) sob forma escrita (impressa ou digital), oral ou audiovisual em um suporte”. Já Capurro e Hjørland (2007) esclarecem que o uso do conceito de “informação”, no sentido de um conhecimento comunicado tem um papel fundamental dentro da sociedade contemporânea. O termo “informação” possui hoje, uma variedade de significados que não podem e não devem ser analisados de forma isolada. Torna-se importante analisar em que domínio a informação é o objeto de estudo. O conceito de informação somente pode ser analisado dentro de um contexto de uso bem definido (FLORIDI, 2002).

Belkin (1978) fez uma varredura em diversas definições sobre informação e as classificou por tipos de abordagem. No processo de conclusão dessa análise, o autor criou um conjunto de requerimentos para o conceito da informação. Tais requerimentos serviram como uma referência para fundamentar suas análises sobre cada uma das definições estudadas, entretanto, os resultados foram insatisfatórios. Por fim, ele esclarece que as melhores definições foram aquelas desenvolvidas para uma finalidade específica e que estas mesmo sendo desenvolvidas em outras áreas podem ser aplicadas com propriedade na CI, pois apresentam em suas estruturas, características intrínsecas dos requisitos da informação, e que todos os conceitos analisados em seu trabalho apresentam subsídios sólidos para auxiliar no desenvolvimento de um conceito único para a CI.

Capurro e Hjørland (2007) alertam em relação às diversas definições dadas ao termo “informação”, principalmente, aquelas que desprezam o significado semântico e pragmático. Os autores afirmam que os profissionais da CI devem continuar na busca de novos conceitos sobre informação, tanto dentro do campo da CI, como em relação a outros termos específicos, por exemplo, documentos e mídias. Muitas vezes as atenções são voltadas mais para o suporte tecnológico do que para a própria informação, “o que desprestigia o principal objetivo da informação, a significação, responsável pela aquisição do conhecimento” (SIQUEIRA, 2011, p. 26).

O significado sobre uma informação está relacionado aos processos socioculturais de um indivíduo ou grupos. Para Capurro e Hjørland (2007, p. 192), uma pedra pode representar um tipo de informação para o geólogo, como representar outro significado para o arqueólogo, e o mesmo acontece com os dados disponibilizados pelo governo federal na *internet*, a remuneração de um servidor público pode ser vista de uma forma pelo cidadão, como vista de outra forma por empresas de financiamento de créditos. O mesmo acontece com as informações sobre deficiências dos órgãos da APF em SI, tais informações podem ser

encaradas de diversas formas pelas empresas prestadoras de serviços ou pelos agentes maliciosos.

Buckland (1991) trata da ambiguidade que cerca a definição da palavra “informação”, classificando-a em ‘informação-como-processo’, ‘informação-como-conhecimento’ e ‘informação-como-coisa’. A ‘informação-como-processo’ tem como foco o ato de informar, nesse sentido, quando uma pessoa é informada, tudo aquilo que ela sabe é de alguma forma modificada. Já a ‘informação-como-conhecimento’ é algo que puramente pode ser assimilado e dessa forma, intangível, pois se baseia em coisas que não podem ser tocadas, sequer medidas, pois são opiniões, ou seja, a informação é algo subjetivo. Por fim, a ‘informação-como-coisa’ que é algo tangível, isto porque é uma coisa descrita ou ainda representada por alguma forma física.

Segundo Tognoli (2012) ‘a informação-como-coisa’ é o “objeto mais palpável da Ciência da Informação”, e conseqüentemente, da Arquivologia, tendo em vista que nesse campo de estudo, a informação é registrada em suportes (LE COADIC, 2004). Para Buckland (1991), qualquer coisa que denota um registro (artigos, livros, imagens) são documentos, sendo assim, possuem as características de serem armazenáveis e recuperáveis dentro de um sistema de informação, tornando-se um objeto potencialmente informativo. A *internet* pode ser considerada um grande registro de informações, potencialmente distribuída geograficamente, tornando-se uma poderosa ferramenta de interação social e de acesso às informações. Por outro lado, ainda ineficaz quanto à seleção e recuperação da informação, conseqüentemente, acarretando problemas na apreensão de conteúdos e geração de possíveis falhas e incertezas, que é conhecido como estado anômalo do conhecimento (BELKIN; ROBERTSON, 1976; BARRETO, 2002).

Qualquer coisa pode ser informação para alguém, desde que assim seja interpretada. Uma coisa será informativa dependendo da situação e das circunstâncias, entretanto, “somos incapazes de apontar com confiança uma coisa que não possa ser informação para alguém” critica Buckland (1991) ao referir-se à definição de informação como “dados processados e reunidos em formato significativo” (MEADOWS *et al.*, 1984, p. 105).

No entendimento de Cruz Mundet (2006), para que uma informação seja considerada um documento de arquivo, ela precisa ser, simultaneamente, interna, previsível e regulamentada, ou seja, ela dever ser: necessária para o exercício das atividades das pessoas, física ou jurídica; oriunda de um processo formalmente estabelecido; possuir regras que estabeleçam seu ciclo de vida: criação, uso, preservação.

A partir desse entendimento, torna-se claro que o conceito de ‘informação-como-coisa’ está diretamente associado a documentos de arquivos, e com isso, surge a necessidade de definição de regras claras e objetivas com a finalidade de promover, com a devida segurança, o amplo acesso às informações.

Uma das principais questões que movimenta a reflexão normativa em torno da informação, remete à possibilidade de estabelecer orientações normativas e critérios avaliativos que permitam afirmar a imputabilidade de agentes e atores sociais cuja intervenção na produção, acesso ou uso de informação, afeta a vida de terceiros, por vezes na extensão indefinida de coletivos em redes (GONZÁLEZ de GÓMEZ, 2009, p. 2).

2.2.2 Classificação da informação

A palavra se originou do latim “*Classis*”, de classe, visto que os povos da Roma Antiga eram divididos em classes de acordo com as condições sociais e políticas (VIEIRA; COELHO; BRAGA, 1873, p. 247). Para Bezerra *et al.* (2013, p. 3), o ato de classificar é “tão antigo quanto a humanidade, mas apenas recentemente adquiriu uma base teórica adequada - base esta que nos permite presumir que ela progrediu do status de arte para o de ciência” (DAHLBERG, 1979).

Classificar é a ação e efeito de ordenar e dispor os objetos e ideias que compartilham de características comuns (ALARCON; FACHIN; TRISTÃO, 2004). Lopes (1998) define que o ato de classificar consiste na "ordenação intelectual e física de acervos, baseada em uma proposta de hierarquização das informações referentes aos mesmos" e oferece a base para a gestão do conhecimento (GOPINATH; DAS, 1997).

Para Sousa (2003), “a classificação é uma função importante para a transparência e o compartilhamento de informações”, contribui consideravelmente nas atividades administrativas e técnicas das organizações, auxilia na tomada de decisão, fortalece a preservação da memória organizacional, e principalmente, contribui para o pleno exercício da cidadania.

Como visto, há várias considerações acerca do termo classificação, que para Eastwood (2004, p. 93) é um problema terminológico, pois o autor considera insatisfatório o uso da palavra “classificação” para definir processos de organização de documentos, sugerindo como mais adequado os termos arranjo ou ordenação.

O próprio *Dicionário Brasileiro de Terminologia Arquivística* possui 3 (três) definições para o termo classificação, sendo as duas primeiras relativas aos aspectos da organização e da recuperação dos documentos e estão diretamente relacionadas à CI, já a

terceira trata sobre o sigilo da informação e está relacionada à SI que é foco principal desta pesquisa.

- 1 Organização dos documentos de uma arquivo (1) ou coleção, de acordo com um plano de classificação, código de classificação ou quadro de arranjo.
- 2 Análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos.
- 3 Atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica. Também chamada classificação de segurança (ARQUIVO NACIONAL, 2005, p. 49).

Em 2013, a Associação Brasileira de Normas Técnicas (ABNT)⁵, publicou a Norma ABNT NBR 16167:2013 estabelecendo diretrizes básicas para a classificação, rotulação e tratamento das informações. De acordo com a ABNT (2013a, p. 1-2), classificação da informação é a “ação de definir o nível de sensibilidade da informação, a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização”. A sensibilidade, no contexto desta pesquisa, corresponde ao “grau de sigilo necessário para informação”, enquanto a criticidade é o impacto negativo que pode ocorrer por ocasião da divulgação indevida da informação.

Também há na CI um problema terminológico para o termo classificação da informação no contexto da SI nos normativos do governo federal. De acordo com a LAI e a Norma Complementar nº 20 da Instrução Normativa nº 1 do GSIPR, a classificação faz parte de um conjunto de ações para o tratamento da informação, dando a perceber que faz parte de uma das fases do ciclo de vida da informação:

V - tratamento da informação: conjunto de ações referentes à produção, recepção, **classificação**, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; (BRASIL, 2011, grifo nosso).

O tratamento da informação abrange as políticas, os processos, as práticas e os instrumentos utilizados pelos órgãos e entidades da APF para lidar com a informação ao longo de cada fase do ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, **classificação**, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (GSIPR, 2014a, p.4, grifo nosso).

Já a ABNT (2013a, p. 1) define tratamento da informação como um “conjunto de ações referentes ao estabelecimento de diretrizes de proteção da informação em função do seu nível de classificação, envolvendo todas as etapas do seu ciclo de vida”. Esta definição parece

⁵ A ABNT é o Foro Nacional de Normalização por reconhecimento da sociedade brasileira desde a sua fundação, em 28 de setembro de 1940, e confirmado pelo governo federal por meio de diversos instrumentos legais. É responsável pela publicação das Normas Brasileiras (NBR).

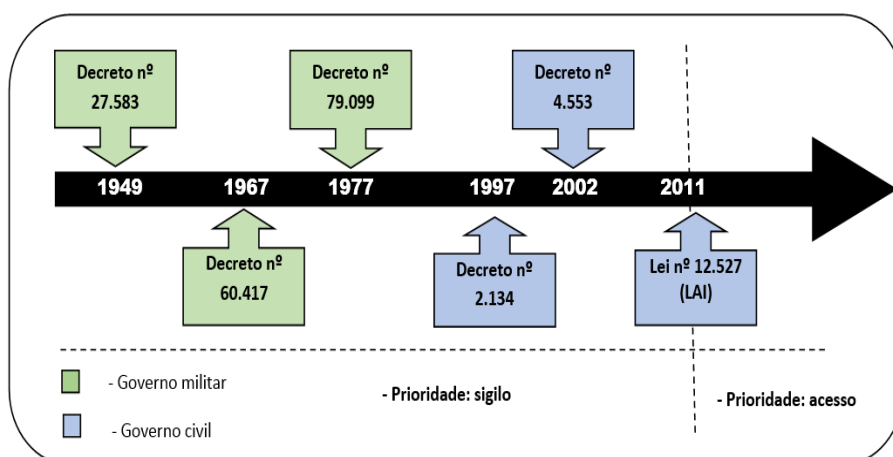
mais coerente, tendo em vista que ao classificar uma informação, será gerado um rótulo correspondente ao grau de sigilo indicado, e esta ação possibilita que sejam adotados todos os procedimentos necessários para o devido tratamento da informação durante o seu ciclo de vida. Classificar a informação é a principal ação de SI para a manutenção da confidencialidade (SIMIÃO, 2009, p. 58), como também, “é um dos primeiros passos para a implementação de uma política de segurança da informação”, pois, a classificação possibilita e orienta o gestor de SI na definição das formas de tratamentos e na seleção de mecanismos de SI adequados para proteção da informação (TCU, 2008).

2.2.3 Classificação da Informação quanto aos graus de sigilo

Grau de sigilo é a “gradação atribuída à classificação de um documento sigiloso, de acordo com a natureza de seu conteúdo e tendo em vista a conveniência de limitar sua divulgação às pessoas que têm necessidade de conhecê-lo” (ARQUIVO NACIONAL, 2001, p. 80).

Na história política do Brasil, as diretrizes para o estabelecimento para classificação da informação e as atribuições de graus de sigilo no governo brasileiro eram estabelecidas pelo Poder Executivo Federal por meio de decretos. O primeiro decreto foi o de nº 27.583 de 1949 que aprovou o Regulamento para a Salvaguarda das Informações que interessam à Segurança Nacional. Logo depois, foram publicados outros decretos revogando e alterando os diversos assuntos sobre tratamento da informação classificada (BRASIL, 1949). O último ordenamento jurídico sobre o tema em questão é a LAI. Como já mencionado, a publicação da LAI foi uma quebra de paradigma, em que é preconizado que o acesso à informação é a prioridade e o sigilo é a exceção. A Figura 8 apresenta a evolução das legislações sobre graus de sigilo em uma linha do tempo.

Figura 8: Linha do tempo de legislações sobre graus de sigilo



Fonte: O autor

Antes da LAI, os graus de sigilo atribuídos às informações sigilosas eram: ultrassecreto, secreto, confidencial e reservado (BRASIL, 2002b), porém no atual ordenamento jurídico, o grau de sigilo “confidencial” foi excluído. Esta mudança gerou vários impactos, principalmente aqueles referentes aos acordos internacionais já existentes entre o Brasil e outros países para troca de informações sigilosas, visto que aquilo que no Brasil era considerado como grau de sigilo “confidencial” teve de ser reclassificado para um maior ou menor grau de sigilo. No aspecto tecnológico, fez-se necessário atualizar diversos sistemas computacionais, principalmente aqueles de gestão de documentos eletrônicos. A retirada do sigilo “confidencial” também gerou um entendimento equivocado, quando muitos associaram a propriedade da confidencialidade com esse grau de sigilo.

Diferente dos decretos que a antecederam, a LAI não contextualiza e nem define os graus de sigilo. O conteúdo da informação deixou de ser requisito para a escolha do grau de sigilo. Na APF, o já revogado decreto nº 4.553 de 2002 em seu art. 5º definia que:

Art. 5º Os dados ou informações sigilosos serão classificados em ultrassecretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.

§ 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

§ 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

§ 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

§ 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos (BRASIL, 2002b).

Na LAI, o que diferencia as informações ultrassecretas, secretas e reservadas entre si é o prazo de restrição de acesso e suas respectivas autoridades competentes para classificar, conforme apresentado no Quadro 3.

Outro aspecto importante observado na LAI é a vedação da reclassificação da informação. Uma vez que a informação seja classificada como reservada ou secreta, ela não poderá ser reclassificada, com isso, não há como prorrogar o prazo de restrição de acesso dessas informações. Já as informações classificadas como ultrassecretas poderão ter a restrição de acesso prorrogado até 25 anos.

Quadro 3: Competências de classificação na APF e prazos de restrição de acesso.

AUTORIDADES CLASSIFICADORAS	RESERVADO (Até 5 anos)	SECRETO (Até 15 anos)	ULTRASSECRETO (Prorrogável até 25 anos)
Presidente da República	✓	✓	✓
Vice-Presidente da República	✓	✓	✓
Ministros de Estado e autoridades com as mesmas prerrogativas	✓	✓	✓
Comandantes da Marinha, do Exército e da Aeronáutica	✓	✓	✓
Chefes de Missões Diplomáticas e Consulares permanentes no exterior	✓	✓	✓
Titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista	✓	✓	✗
Autoridades que exerçam funções de direção, comando ou chefia, de hierarquia equivalente ou superior ao nível DAS 101.5	✓	✗	✗

Fonte: O autor.

2.2.4 Comunicação da informação organizacional

O ato de comunicar, oriundo do Latim “*communicare*” significa tornar comum. É um processo social e primário que possibilita a vida em sociedade. Para Chiavenato (2008, p.75), é impossível a sobrevivência das pessoas de forma isolada e autossuficiente e é por meio da comunicação que as pessoas se relacionam entre si e com o seu ambiente. Berlo (2003) entende que a comunicação é o fator determinístico no processo de influenciar pessoas, remetente ou destinatário, como também o ambiente em que estes residem. Para Brambilla et. al (2007), tanto a CI, como a Ciência da Comunicação possuem características semelhantes: são disciplinas ainda em fase de construção, estão relacionadas diretamente com a explosão informacional e, também, às tecnologias.

Assim como a comunicação é fundamental às atividades sociais, ela também é essencial para a troca de mensagens no ambiente organizacional, quer sejam no seu âmbito interno ou externo (KUNSCH, 1986). A comunicação organizacional determina o movimento da informação dentro de uma determinada organização, bem como a relação da organização com o seu ambiente externo (SHERMERHORN, 1991, p. 251).

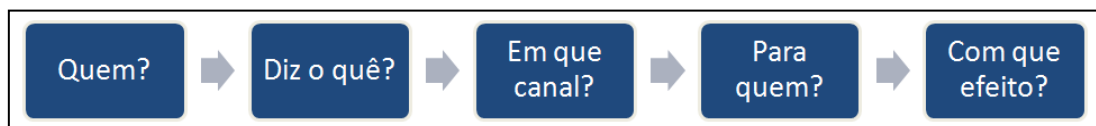
A direção dos movimentos de uma organização, bem como, a sua sobrevivência no mercado, é determinada pela comunicação (THAYER, 1976). É nesse pensamento que “o governo moderno orienta-se cada vez mais no sentido da comunicação” (BERLO, 2003).

Para Vieira R. (2004) a atual sociedade baseia-se na comunicação rápida e ampla da informação, considerando a comunicação organizacional mais significativa no contexto da inter-relação entre empresas, empregados e sociedade, porém, o sucesso da organização vai depender da capacidade de comunicação do meio em que ela se encontra e seus espaços internos e externos.

No contexto de uma organização pública, o ambiente ou espaço externo (KUNSCH, 1986; VIEIRA R., 2004) é representado pelos fornecedores, outras organizações, públicas ou privadas e, principalmente, a sociedade como cliente. Sendo que a interação com a sociedade, conjugada a comunicação e a tecnologia constituem fenômenos importantes para garantir o desenvolvimento da cidadania (PINHEIRO; LOUREIRO, 1995).

Já no atual contexto da administração pública brasileira, identificou-se o amplo uso da *internet* na comunicação dos órgãos, no papel de emissor, que mudou o comportamento do cidadão, no papel de receptor e destino da mensagem. Essa abordagem de comunicação se assemelha com o modelo linear de comunicação proposto por Lasswell (Figura 9).

Figura 9: Modelo de Comunicação de Lasswell



Fonte: McQuail e Windhall (1993)

Para Wolf (2003, p. 30), o processo de comunicação proposto por Lasswell é estritamente assimétrico, onde o emissor, ativamente, produz estímulos para a reação de uma determinada massa passiva de destinatários. Nesse caso, o objetivo principal da comunicação é a mudança de comportamento para quem se destina a mensagem. Isto independe da relação, quer seja social ou cultural, dos agentes, emissor e receptor.

As 5 (cinco) perguntas do modelo de Lasswell podem ser respondidas da seguinte forma no contexto dessa pesquisa:

- a) QUEM? – os órgãos da administração pública;
- b) DIZ O QUÊ? – gastos, gestão fiscal, atos administrativos, prestação de contas, despesas orçamentárias, recursos financeiros;
- c) EM QUE CANAL? – portais na *internet*;
- d) PARA QUEM? – cidadão e interessados; e
- e) COM QUE EFEITO? – incentivar a participação e o controle social, possibilitar denúncias, dar conhecimento, reduzir corrupção.

2.3 Segurança da Informação

2.3.1 Conceitos gerais

Os normativos da ABNT consideram que a SI é feita por ações que visam, principalmente, a preservação das propriedades de confidencialidade, de integridade e de disponibilidade das informações. O Governo Federal incorporou tais propriedades em seus normativos, porém, incluiu a preservação da autenticidade, que segundo Simião (2009, p. 61) é de suma importância no impacto dos processos de comunicações. Nesse sentido, para a APF surgiu uma nova denominação: gestão de Segurança da Informação e Comunicações (SIC).

Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações (GSI-PR, 2008a, p. 2).

Para Rangel (2010, p. 38) houve um incremento da gestão de SI para a gestão de SIC, “muito em função dos avanços das tecnologias da informação e comunicação (TIC) e da interdependência e interconexão dos sistemas e redes de informação”, conseqüentemente, aumentou-se a probabilidade da presença de ações adversas que inviabilizam a SIC, sendo que tais ações ou, até mesmo omissões, podem ser feitas de forma intencional ou acidental, e o resultado disso, de acordo com o GSI-PR (2008a, p.2) é definido como quebra de segurança. Isso significa que uma ou mais propriedades da SIC – disponibilidade, integridade, confidencialidade e autenticidade – foram comprometidas, e para evitar a quebra de segurança

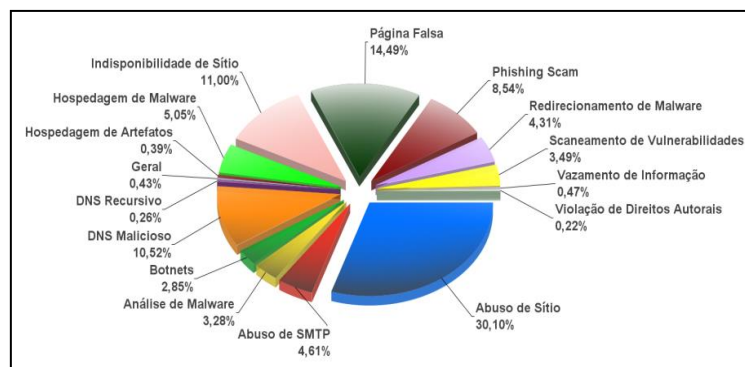
é preciso tratar a informação, assegurando essas propriedades em todo seu ciclo de vida (GSI-PR, 2014a, p. 3).

O GSI-PR (2008a, p.2) define disponibilidade como a “propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade”; já a LAI entende que disponibilidade é a “qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados” (BRASIL, 2011).

Para garantir a disponibilidade das informações, é preciso “uma série de ações ou de boas práticas”, como por exemplo, “o uso de backups; cópias de segurança; redundância de sistemas e eficácia no controle de acesso” (SIMIÃO, 2009, p. 54). Esta propriedade tornou-se o foco das atenções dos gestores de SI, pois, além dela contribuir com a transparência e o bom serviço prestado ao público (SIMIÃO, 2009, p. 55), a disponibilidade está diretamente relacionada com a observância da publicidade como preceito geral determinada pela LAI.

Também é preciso manter a integridade das informações disponibilizadas pelos órgãos da APF, ou seja, garantir que elas não sejam modificadas, nem destruídas de maneira não autorizada ou acidental (GSI-PR, 2008a, p. 2). As estatísticas apresentadas pelo Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da APF (CTIR Gov)⁶ referentes aos meses de janeiro a março de 2015 (Gráfico 1), apontam que o maior índice de incidentes de segurança relacionados aos *sites* do governo foram efetuados pela quebra da integridade das informações por meio da desfiguração das páginas oficiais da *internet* dos órgãos da APF.

Gráfico 1: Distribuição de incidentes de redes por categoria.



Fonte: CTIR Gov, 2015.

⁶ É o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - APF. Está subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC - do Gabinete de Segurança Institucional da Presidência da República - GSIPR.

Os controles de segurança necessários para a manutenção da integridade da informação não se limitam apenas aos controles lógicos das informações digitais. Também, é preciso manter a proteção dos documentos armazenados em suportes físicos. A Lei nº 8.159 de 1991, que dispõe sobre a política nacional de arquivos públicos e privados, determina que “é dever do Poder Público a gestão documental e o a proteção especial a documentos de arquivos”. Esta proteção refere-se principalmente aos aspectos da preservação dos documentos que futuramente servirão “como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação” (BRASIL, 1991). A LAI também menciona que “quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original” (BRASIL, 2011).

Como visto, a disponibilidade e a integridade das informações são propriedades que fortalecem o princípio da publicidade e da transparência pública, no entanto, é preciso saber se tais informações são autênticas. Segundo a LAI e o GSI-PR, o conceito de autenticidade está relacionado à qualidade ou à propriedade da informação que tenha sido produzida, expedida, recebida ou modificada por pessoas, organizações ou sistemas (BRASIL, 2011; GSI-PR, 2008a, p. 2). Entretanto, tais conceitos não mencionam se essas pessoas, organizações ou sistemas são realmente as que deveriam ser. As considerações do Conselho Internacional de Arquivos (CIA) são mais coerentes ao afirmar que “para mostrar que um documento de arquivo é autêntico apenas é necessário provar que é o que afirma ser” (CIA, 2005, p.42).

Outra propriedade da informação a ser considerada no contexto da SI é a confidencialidade. No atual cenário em que o sigilo tornou-se uma exceção no governo federal, os legisladores resolveram não citar a confidencialidade das informações na LAI. O fato da retirada do sigilo “confidencial” nas normas do governo, não justifica a sua omissão na LAI, houve um falso entendimento ao associar confidencialidade e sigilo, o que já previa Simião (2009, p. 58):

A confidencialidade, na maioria das vezes, é apresentada sob enfoque de sigilo, o que não deixa de estar correto, porém existe outro aspecto a considerar que é a ética de preservar ou guardar uma informação nem sempre classificada como sigilosa. Isto significa que nem sempre a informação tenha de receber um grau de sigilo para justificar a necessidade de medidas de proteção.

Os normativos do GSI-PR não desprezaram a importância dessa propriedade, considerando-a de suma importância para a segurança do Estado e da sociedade e com isso, definiu-se que confidencialidade é a “propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado” (GSI-PR, 2008a, p. 2).

Assim como as propriedades da disponibilidade, integridade e autenticidade possuem uma forte relação com o amplo acesso à informação, a propriedade da confidencialidade tem com as restrições de acesso. Contudo, para que seja realizado o adequado tratamento da informação é preciso considerar a presença de todas as propriedades nos diversos tipos de informação, quer sejam ostensivas, sigilosas e pessoais.

O Quadro 4 apresenta os diversos tipos de informações que precisam ser tratadas, inclusive as ostensivas, porém, não incluiu as informações ou conhecimentos que são veiculados nos materiais de acesso restrito.

Art. 45. São considerados materiais de acesso restrito qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tais como:

I - equipamentos, máquinas, modelos, moldes, maquetes, protótipos, artefatos, aparelhos, dispositivos, instrumentos, representações cartográficas, sistemas, suprimentos e manuais de instrução;

II - veículos terrestres, aquaviários e aéreos, suas partes, peças e componentes;

III - armamentos e seus acessórios, as munições e os aparelhos, equipamentos, suprimentos e insumos correlatos;

IV - aparelhos, equipamentos, suprimentos e programas relacionados a tecnologia da informação e comunicações, inclusive à inteligência de sinais e imagens;

V - recursos criptográficos; e

VI - explosivos, líquidos e gases. (BRASIL, 2012b).

O Poder Executivo Federal ao criar o termo “material de acesso restrito” por intermédio do Decreto nº 7.845 de 2012, estabeleceu uma nova regra que contraria os preceitos do amplo acesso às informações e do sigilo, como exceção estabelecida pela LAI. Entende-se que o sigilo das informações contidas no material de acesso restrito seja de caráter eterno. Além disso, não há um processo formal para classificar um material de acesso restrito, enquanto que durante o processo de classificação de sigilo, exigidos pela LAI, há diversas exigências.

Quadro 4: Exemplos de tipos de informação.

TIPO	DESCRIÇÃO
1. OSTENSIVA	Transparência Ativa
	Transparência Passiva
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 Reservada – Prazo máximo de restrição de acesso de 5 anos
	2.2 Secreta – Prazo máximo de restrição de acesso de 15 anos
	2.3 Ultrasecreta – Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 Sigilos Decorrentes de Direitos de Personalidade
	3.1.1 Sigilo Fiscal
	3.1.2 Sigilo Bancário
	3.1.3 Sigilo Comercial
	3.1.4 Sigilo Empresarial
	3.1.5 Sigilo Contábil
	3.2 Sigilos de Processos e Procedimentos
	3.2.1 Acesso a Documento Preparatório
	3.2.2 Sigilo do Procedimento Administrativo Disciplinar em Curso
	3.2.3 Sigilo do Inquérito Policial
	3.2.4 Segredo de Justiça no Processo Civil
	3.2.5 Segredo de Justiça no Processo Penal
	3.3 Informação de Natureza Patrimonial
	3.3.1 Segredo Industrial
	3.3.2 Direito Autoral e Propriedade Intelectual de Programa de Computador
3.3.3 Propriedade Industrial	
4. PESSOAL	4.1. Pessoal – Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.

Fonte: GSI-PR (2014a, p. 12).

2.3.2 Os normativos de segurança da informação

A recente notícia sobre o caso “*Edward Snowden*”⁷ traduz o quanto é importante a manutenção da SI, principalmente, daquelas relativas à soberania nacional e à defesa do Estado democrático. Entretanto, “não estamos ainda nem na adolescência, estamos na infância em relação a muitos desses temas. E as vulnerabilidades existem e’ são muitas”, afirmou o

⁷ Caso Snowden, "batizado" com este nome por causa do delator do esquema de monitoramento: Edward Snowden. O americano é um ex-consultor técnico da Agência Central de Inteligência (CIA) dos Estados Unidos (EUA). Na época, Snowden revelou os documentos secretos sobre o *modus operandi* da segurança norte-americana para os jornais *The Guardian* (Reino Unido) e *Washington Post* (EUA). Disponível em: <<http://www.abc.com.br/tecnologia/2013/08/web-vigiada-entenda-as-denuncias-de-edward-snowden>>

Ministro da Defesa, Celso Amorim, durante uma audiência pública no Senado Federal⁸. Essa notícia veio fortalecer ainda mais as ações que o governo federal vem desempenhando sobre o assunto de SI, ora tratado no âmbito do Conselho de Defesa Nacional (CDN), por intermédio do GSI-PR, que exerce as funções de Secretaria Executiva deste Conselho.

Dentro da estrutura do GSI-PR foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), pelo Decreto nº 5.772/2006, com a missão de planejar e coordenar as atividades de SIC na APF. As atividades de SI na APF não são executadas de forma isolada pelo GSI-PR, existe um Comitê Gestor da Segurança da Informação (CGSI), composto por 17 órgãos da APF e criado pelo Decreto nº 3.505/2000 com a finalidade de assessorar o GSI-PR sobre o tema, principalmente, para a formulação normas de SI (BRASIL, 2000a).

O atual arcabouço normativo de SIC da APF é composto por 1 (uma) instrução normativa e 21 (vinte e uma) normas complementares (NC), conforme apresentado no Quadro 5. Estes normativos têm o caráter mandatório, diferente das normas da ABNT, que constituem as boas práticas de SI.

9.8.2. em atenção à Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem II.8); (TCU, 2012a).

⁸ Palavras do Ministro da Defesa, Celso Amorim no dia 10/07/2013 durante a Comissão de Relações Exteriores do Senado, ao lado dos titulares das Relações Exteriores, Antonio Patriota, e do Gabinete de Segurança Institucional, José Elito Siqueira. Disponível em: < <http://veja.abril.com.br/noticia/brasil/redes-brasileiras-sao-vulneraveis-diz-celso-amorim>>

Quadro 5: Normativos de SIC da APF.

Instrução Normativa nº 1 de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.	
NC 01/2008	Atividade de Normatização.
NC 02/2008	Metodologia de Gestão de SIC.
NC 03/2009	Diretrizes para a Elaboração de Política de SIC.
NC 04/2013	Diretrizes para o processo de Gestão de Riscos de SIC - GRSIC. (Revisão 01)
NC 05/2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR.
NC 06/2009	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC.
NC 07/2014	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à SIC.
NC 08/2010	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais.
NC 09/2014	Estabelece orientações específicas para o uso de recursos criptográficos em SIC. (Revisão 02)
NC 10/2012	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC.
NC 11/2012	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à SIC.
NC 12/2012	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC.
NC 13/2012	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à SIC.
NC 14/2012	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC.
NC 15/2012	Estabelece diretrizes de SIC para o uso de redes sociais.
NC 16/2012	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de <i>Software</i> Seguro.
NC 17/2013	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de SIC.
NC 18/2013	Estabelece as Diretrizes para as Atividades de Ensino em SIC.
NC 19/2014	Estabelece Padrões Mínimos de SIC para os Sistemas Estruturantes da APF.
NC 20/2014	Estabelece as Diretrizes de SIC para Instituição do Processo de Tratamento da Informação. (Revisão 01)
NC 21/2014	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da APF.

Fonte: Adaptado do DSIC, 2014.

O TCU utiliza como referência as Normas da ABNT e do GSI-PR em suas auditorias, a fim de verificar o grau de conformidade e o nível de SI em que os órgãos da APF se encontram. A ISO/IEC (2014) conhecida como família ISO/IEC 27000 é uma norma internacional elaborada pelo *Technical Committee Information Technology da International Organization for Standardization (ISO)* e *International Electrotechnical Commission (IEC)* e descreve como as organizações devem implementar um sistema de gestão de SI (SGSI) trazendo em seu conteúdo uma visão geral e vocabulários sob o ponto de vista da TI. No Brasil, algumas normas da família 27000 foram traduzidas e adaptadas pela Comissão de Estudo de Segurança da Informação do Comitê Brasileiro de Computadores e Processamento de Dados da ABNT. O Quadro 6 apresenta todos normativos pertencentes à família ISO/IEC 27000.

Quadro 6: Família ISO/IEC 27000

ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos
ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação
ABNT NBR ISO/IEC 27003:2011 - Tecnologia da informação - Técnicas de segurança - Diretrizes para implantação de um sistema de gestão da segurança da informação
ABNT NBR ISO/IEC 27004:2010 - Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição
ABNT NBR ISO/IEC 27005:2011 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação
ABNT NBR ISO/IEC 27007:2012 - Diretrizes para auditoria de sistemas de gestão da segurança da informação
ABNT NBR ISO/IEC 27011:2009 - Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002
ABNT NBR ISO/IEC 27014:2013 - Tecnologia da Informação - Técnicas de Segurança - Governança de segurança da informação
ABNT NBR ISO/IEC 27031:2015 - Tecnologia da informação - Técnicas de segurança - Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação
ABNT NBR ISO/IEC 27037:2013 - Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital
ABNT NBR ISO/IEC 27038:2014 - Tecnologia da informação - Técnicas de segurança - Especificação para redação digital
ISO/IEC 27000:2014 - <i>Information technology - Security techniques - Information security management systems - Overview and vocabulary</i>
ISO/IEC 27006:2011 - <i>Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems</i>
ISO/IEC 27010:2012 - <i>Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications</i>
ISO/IEC 27013:2012 - <i>Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ISO/IEC 27018:2014 - <i>Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i>
ISO/IEC 27032:2012 - <i>Information technology - Security techniques - Guidelines for cybersecurity</i>

ISO/IEC 27033-4:2014 - <i>Information technology - Security techniques - Network security- Part 4: Securing communications between networks using security gateways</i>
ISO/IEC 27034-1:2011 - <i>Information technology - Security techniques - Application security- Part 1: Overview and concepts</i>
ISO/IEC 27035:2011 - <i>Information technology - Security techniques - Information security incident management</i>
ISO/IEC 27036-1:2014 - <i>Information technology - Security techniques - Information security for supplier relationships- Part 1: Overview and concepts</i>
ISO/IEC 27036-2:2014 - <i>Information technology - Security techniques - Information security for supplier relationships- Part 2: Requirements</i>
ISO/IEC TR 27008:2011 - <i>Information technology - Security techniques - Guidelines for auditors on information security controls</i>
ISO/IEC TR 27015:2012 - <i>Information technology - Security techniques - Information security management guidelines for financial services</i>
ISO/IEC TR 27016:2014 - <i>Information technology - Security techniques - Information security management - Organizational economics</i>
ISO/IEC TR 27019:2013 - <i>Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry</i>

Fonte: Catálogo da ABNT, 2014.

Algumas normas elaboradas pelo GSI-PR apresentadas no Quadro 5 receberam fortes influências dos normativos apresentados no Quadro 6, principalmente a Norma Complementar nº 2 da Instrução Normativa nº 1 do GSIPR que tem como objetivo definir a metodologia de GSIC utilizada pelos órgãos e entidades da APF:

2.1 A metodologia de gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo “**PDCA**” (*Plan-Do-Check-Act*), referenciado pela norma ABNT NBR ISO/IEC 27001:2006.

2.2 A escolha desta metodologia levou em consideração três critérios:

- a) Simplicidade do modelo;
- b) Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras;
- c) Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros (GSI-PR, 2008b, p. 2).

As normas ABNT NBR ISO/IEC 27001 e 27002, revisadas em 2013, buscam uma abordagem mais flexível e simplificada dos requisitos e códigos de prática para o SGSI, a fim de garantir uma gestão de risco de SI mais efetiva nas organizações (SÊMOLA, 2014, p. 70). Já os normativos do GSI-PR não possuem uma visão integrada dos controles de SI, como também, não possuem uma taxonomia própria que sirva para toda a APF. Nota-se que é preciso alinhar diversos conceitos, exemplificados no Quadro 7, e revisar algumas NC, principalmente aquelas publicadas antes da LAI e aquelas que tomaram como referência os normativos da ABNT já revisados.

Quadro 7: Exemplos de termos com diferentes conceitos nos normativos de SI

TERMO	CONCEITOS		
AGENTE RESPONSÁVEL	NC 10/IN01/GSIPR/2012	NC 05/IN01/GSIPR/2009	NC 09/IN01/GSIPR/2014
	Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação.	Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.	Servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da APF, direta ou indireta, possuidor de credencial de segurança;
ATIVOS DE INFORMAÇÃO	NC 04/IN01/GSIPR/2013	NC 10/IN01/GSIPR/2012	X-X-X
	Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.	Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.	X-X-X
TRATAMENTO DA INFORMAÇÃO	IN01/GSIPR/2008	NC 20/IN01/GSIPR/2014	LAI
	Recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.	Conjunto de ações referentes às fases do ciclo de vida da informação.	Conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Fonte: Adaptado do DSIC, 2014.

2.3.3 Sociedade do risco e a APF

De acordo com Gardner (2009, p. 15), os países modernos estão se tornando nações de preocupados, o citado autor designou o termo “sociedade do risco” para tais países, principalmente aqueles nos quais há um elevado grau de preocupação com riscos causados pela tecnologia moderna.

Para Beck (1998), o que diferenciou os riscos do mundo moderno em relação aos riscos do período medieval foi a globalização das ameaças. O progresso industrial trouxe a modernização e o desenvolvimento tecnológico, em contrapartida, surgiram novos riscos que até então não haviam sido experimentados pela sociedade. A democratização do risco iguala todos os indivíduos de uma sociedade. Não há mais fronteiras de ordem social, étnica, cultural que diferenciam os membros da sociedade do risco frente às novas ameaças globais. Nesse sentido, urge investir em novos processos e sistemas de segurança, a fim de acompanhar e tratar os novos riscos oriundos da evolução tecnológica.

De acordo com Fernandes (2010), a sociedade do risco busca garantir o controle e o domínio sobre o meio ambiente na busca de autonomia por meio da discussão e ações de segurança, a fim de controlar o risco que “erige-se na contemporaneidade como uma forma de comunicação”, que atualmente está tematizado pelas novas tecnologias (ATZ, 2011, p. 47) utilizadas cada vez mais pela administração pública na reformulação de sua comunicação organizacional com o público interno e externo (PRATES, 2012, p. 104).

Moreira e Queiroz (2007, p. 42) defendem que as novas tecnologias aumentaram a “capacidade de registrar, armazenar, analisar e transmitir grandes volumes de informações complexas de maneira segura, flexível, confiável, imediata e com independência geográfica”. Por outro lado, introduziu novos riscos que normalmente requerem apurados controles de segurança, gerando novas necessidades de recursos, material e pessoal, especializados.

A APF vem investindo com diversas ações a fim de reduzir os possíveis riscos provenientes do uso das novas tecnologias, particularmente aqueles referentes à SI. O MP (2010) determina que os órgãos integrantes do SISP realizem análise de risco na fase de planejamento da contratação de soluções de TI. Entretanto, tais medidas referem-se apenas às ações necessárias para evitar qualquer tipo de ocorrência que venha comprometer o processo de contratação, observa-se que não há clareza nas definições dos requisitos de SI do objeto contratado:

Art. 16. A Análise de Riscos será elaborada pela Equipe de Planejamento da Contratação contendo os seguintes itens: I - identificação dos principais riscos que possam comprometer o sucesso dos processos de contratação e de gestão contratual; II - identificação dos principais riscos que possam fazer com que a Solução de Tecnologia da Informação não alcance os resultados que atendam às necessidades da contratação; III - mensuração das probabilidades de ocorrência e dos danos potenciais relacionados a cada risco identificado; IV - definição das ações previstas a serem tomadas para reduzir ou eliminar as chances de ocorrência dos eventos relacionado a cada risco; V - definição das ações de contingência a serem tomadas caso os eventos correspondentes aos riscos se concretizem; e VI - definição dos responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência (MP, 2010).

Visando suprir essa necessidade, o GSI-PR incluiu em seus normativos itens que reforçam a necessidade de assegurar a SI e reduzir os possíveis riscos por ocasião da contratação:

5.1.10 O recurso criptográfico, baseado em algoritmo de Estado, deverá ser de desenvolvimento próprio ou por órgãos e entidades da APF, direta ou indireta, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos à APF, para tal finalidade.

5.1.11 Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.1.10 poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições: [...] (GSI-PR, 2014b, p. 4).

4.1.7 Os instrumentos contratuais celebrados entre a APF e prestadores de serviço, em decorrência das contratações de soluções de tecnologia da informação para projetos de implementação ou manutenção de sistemas estruturantes, deverão conter cláusulas que garantam a realização de auditorias nos aspectos de Segurança da Informação e Comunicações (GSI-PR, 2014c, p. 3).

Soares (2014, p.15) afirma que organizações públicas estão se coordenando em ações conjuntas que visam atingir os seus principais objetivos, porém, no âmbito da SI, essa afirmação é contraditória. Nota-se a falta de coordenação e comunicação entre os órgãos da APF. O MP (2010) determina que a gestão de SI não poderá ser objeto de contratação. Já a mencionada definição de Gestão de SIC dada pelo GSI-PR (2008a, p. 2) descreve diversas ações e métodos que normalmente são objetos de contratação, como por exemplo, aquisição de ferramentas e metodologias de gestão de riscos, mecanismos de controles, físico e lógico, para a segurança organizacional. Nesse sentido, o entendimento de gestão de SI para o MP (2010) corresponde apenas à vedação da contratação de recursos humanos para execução das atividades de gestor de SI, ou seja, obrigatoriamente, essa atividade deverá ser exercida exclusivamente por servidor público, o que já havia sido estabelecido pelos normativos do GSI-PR.

Art 5º – Não poderão ser objeto de contratação: I - mais de uma Solução de Tecnologia da Informação em um único contrato; e II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação. Parágrafo único. O suporte técnico aos processos de planejamento e avaliação da qualidade das Soluções de Tecnologia da Informação poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade. (MP, 2010)

5.3.7.2 Instituir o Gestor de Segurança da Informação e Comunicações do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso, com as seguintes responsabilidades: [...] (GSI-PR, 2009a, p. 4)

É importante ressaltar que apenas a limitação do exercício das atividades de gestor de SI aos servidores públicos não são suficientes a ponto de garantir a SI da organização, é preciso garantir que as ferramentas utilizadas para a identificação de vulnerabilidades e de riscos sejam desenvolvidas pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, e quando não possível, garantir que a ferramenta contratada seja desenvolvida por uma Empresa Estratégica de Defesa (EED), visto que normalmente, as ferramentas de análise de riscos encontradas no mercado são projetadas para armazenar informações que geram uma base de conhecimento. A coleta e o armazenamento de informações estratégicas de governo, além de aumentarem o poder de competitividade na iniciativa privada, também, podem representar um perigo para o Estado brasileiro, uma vez que sua indevida divulgação poderá servir de insumos para outras nações e grupos maliciosos.

IV - Empresa Estratégica de Defesa - EED - toda pessoa jurídica credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das seguintes condições:

- a) ter como finalidade, em seu objeto social, a realização ou condução de atividades de pesquisa, projeto, desenvolvimento, industrialização, prestação dos serviços referidos no art. 10, produção, reparo, conservação, revisão, conversão, modernização ou manutenção de PED no País, incluídas a venda e a revenda somente quando integradas às atividades industriais supracitadas;
- b) ter no País a sede, a sua administração e o estabelecimento industrial, equiparado a industrial ou prestador de serviço;
- c) dispor, no País, de comprovado conhecimento científico ou tecnológico próprio ou complementado por acordos de parceria com Instituição Científica e Tecnológica para realização de atividades conjuntas de pesquisa científica e tecnológica e desenvolvimento de tecnologia, produto ou processo, relacionado à atividade desenvolvida, observado o disposto no inciso X do caput;
- d) assegurar, em seus atos constitutivos ou nos atos de seu controlador direto ou indireto, que o conjunto de sócios ou acionistas e grupos de sócios ou acionistas estrangeiros não possam exercer em cada assembleia geral número de votos superior a 2/3 (dois terços) do total de votos que puderem ser exercidos pelos acionistas brasileiros presentes; e
- e) assegurar a continuidade produtiva no País (BRASIL, 2012c).

O recente levantamento de auditoria realizado pelo TCU com o objetivo de acompanhar a situação de governança de TI na APF utilizou como referência para elaboração das questões sobre Gestão Corporativa da SI, a norma técnica ABNT NBR ISO/IEC 27002:2005 e as NC apresentadas no Quadro 7. Os resultados desse levantamento foram publicados no acórdão nº 3.117/TCU-Plenário de 12 de novembro de 2014. Nos aspectos de SI foi apontada certa evolução em alguns itens auditados, entretanto, há um “distanciamento da situação ideal esperada, vez que a não adoção integral dessas práticas expõe as organizações a riscos diversos, como indisponibilidade dos serviços, perda de integridade, e riscos relativos à proteção das informações” (TCU, 2014c, p. 54).

Os números apurados revelam, em geral, que a alta administração das organizações públicas federais ainda não reconhece a importância da gestão de riscos para a consecução de seus objetivos, apesar dos altos valores geridos, em grande parte dos casos, e dos diversos riscos aos quais suas ações estão expostas, em geral. A principal consequência disso é a ineficácia das ações e o consequente desperdício de dinheiro público, com projetos inacabados ou inviáveis em decorrência de situações que constituíam riscos não considerados quando da tomada de decisão (TCU, 2014c, p. 14).

Para Sêmola (2014, p.113) “segurança é administrar riscos”, sendo assim, a gestão de riscos de SI torna-se um excelente instrumento para dimensionar a situação de segurança em que a organização se encontra, como também, “permite identificar e implementar as medidas necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação” (BEAL, 2005, p. 11). Verifica-se um baixo nível de adoção das práticas de gestão de riscos na APF. Uma gestão deficiente de SI pode causar diversos prejuízos para a instituição e, sobretudo, para a sociedade (TCU, 2014b, p. 39). No contexto desta pesquisa, um órgão que não adota as práticas de gestão de riscos em SI, tem uma alta probabilidade de expor informações indevidas em seus respectivos portais, tais informações poderão comprometer a propriedade da confidencialidade, bem como a privacidade das pessoas.

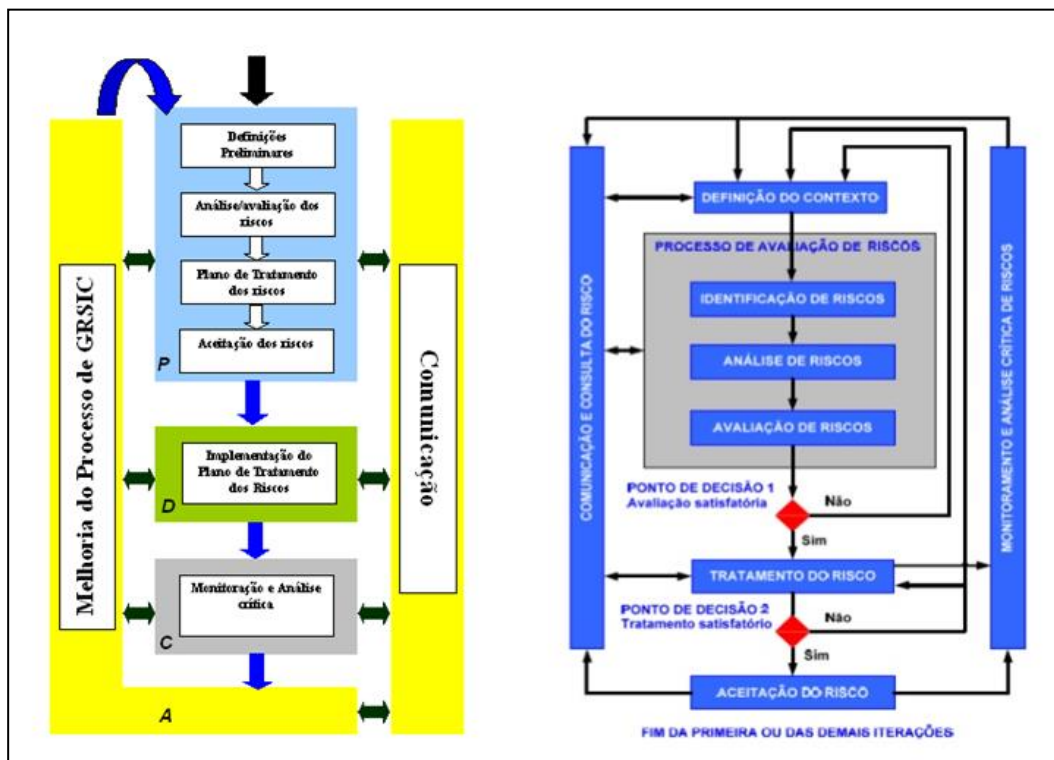
Visando estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) para os órgãos da APF, foi publicada a Norma Complementar nº 4 da Instrução Normativa nº 1 do GSIPR em 2008, que recebeu sua primeira revisão em 2013, resultante de uma recomendação do TCU (2012a) que verificou divergência da definição do termo “ativo de informação” em relação aos normativos da ABNT. Fulcros dessa anotação, o GSI-PR acrescentou na referida norma um item esclarecendo que GRSIC está “limitada ao escopo das ações de Segurança da Informação e Comunicações e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme definido” no GSI-PR (2013, p.2):

Recomendar, [...], ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) que: [...] reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1 (subitem 0). (TCU, 2012a).

Cabe ressaltar que tanto o modelo de processo de GRSIC apresentado pelo GSIP-PR (2013), como o conteúdo da referida norma não identificam os pontos de decisões necessários para avaliar a eficácia das ações adotadas até os pontos mais críticos do processo. Esse procedimento reduz os esforços e gastos desnecessários, evitando que possíveis falhas de avaliação e tratamento inadequado ou insuficiente sejam verificadas apenas no término de todo processo (ABNT, 2011, p. 11).

A Figura 10 apresenta uma comparação do modelo de GRSIC apresentado pelo GSI-PR (2013) com o modelo apresentado pela ABNT (2011, p. 9).

Figura 10: Modelo comparativo do processo de GRSIC com o modelo da ABNT



Fonte: adaptado do GSI-PR (2013) e ABNT (2011)

Por fim, considerando que o risco de SIC está “associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização” (GSI-PR, 2013b, p. 30), convém que a organização defina uma metodologia de gestão de riscos capaz de

identificar e analisar seus principais fatores de risco: ativos de informação, vulnerabilidades, ameaças, impactos e probabilidades.

2.3.4 Fatores de risco de SI

Para alcançar o sucesso na implementação do processo de gestão de riscos, independente da metodologia adotada, o gestor deverá compreender os principais conceitos básicos referentes aos fatores de risco que estão relacionados a SI.

Há vários entendimentos e interpretações sobre o processo de gestão de riscos de SI, mas nesta pesquisa decidiu-se que todo ativo de informação possui vulnerabilidades, e estas poderão ser exploradas por uma ou mais ameaças que produzirão riscos.

O nível do risco é fator determinante para verificar os danos ou custos que impactarão os ativos de informação. Para isso, torna-se imprescindível que as organizações estabeleçam um processo de análise e avaliação de riscos, a fim de determinar quais ações ou controles de segurança que atuarão no tratamento das vulnerabilidades de seus ativos de informação frente às ameaças identificadas e monitoradas.

Dependendo do tipo de ação ou controle tomado, os riscos serão modificados de acordo com os critérios estabelecidos pelo tomador de decisão da organização.

A Figura 11 apresenta o fluxo relacional entre os termos que compõem os fatores de risco de SI apresentados nesta pesquisa.

Figura 11: Relacionamento entre os termos associados aos fatores de risco.



Fonte: O autor.

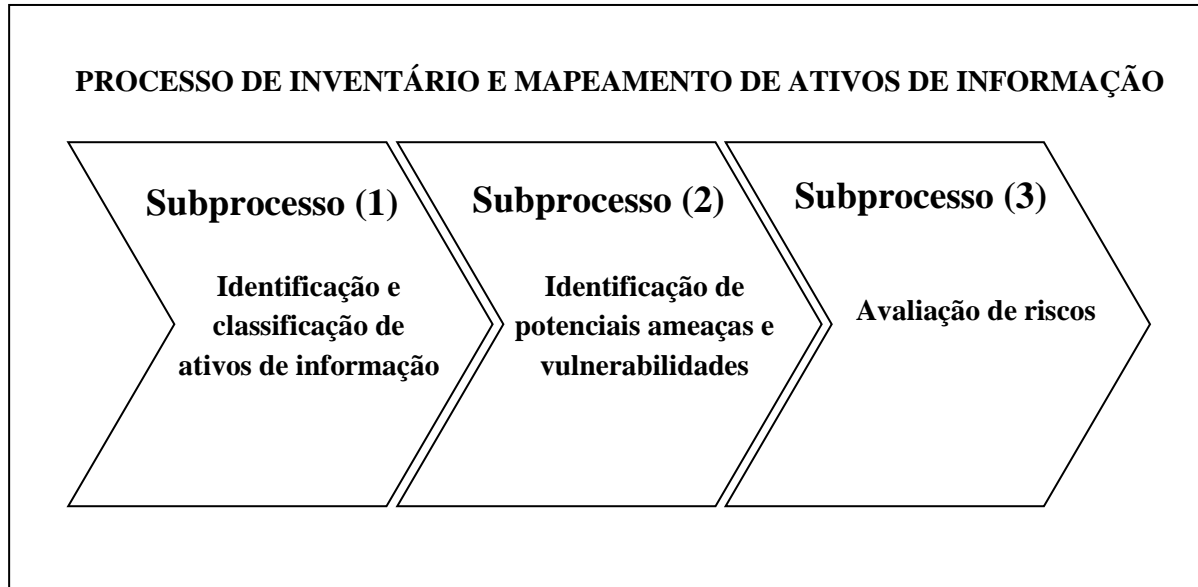
2.3.4.1 Ativos de Informação

O termo “ativo” é oriundo da área financeira, constitui-se de um valor para uma pessoa ou para uma organização, e por isso, necessita de uma adequada proteção (SÊMOLA, 2014, p. 44). O valor do ativo pode variar de acordo com o tempo de vida da informação, sendo assim, convém que a organização mantenha seus ativos identificados e inventariados de uma forma atualizada e consistente. O processo de identificação de ativos é de suma importância para a avaliação dos riscos, isto porque o tratamento do risco está diretamente relacionado com o valor do ativo. A ABNT (2011, p.41) tipifica os ativos em duas formas: ativos primários e ativos de suporte e infraestrutura. Os ativos primários são os processos e atividades relacionados ao negócio da organização, como também, a própria informação. Já os ativos de suporte e infraestrutura são os suportes de apoio dos ativos primários e são estes que possuem vulnerabilidades, como por exemplo, o *hardware*, o *software*, a infraestrutura de rede, os recursos humanos, as instalações físicas, a estrutura da organização. A exploração de uma vulnerabilidade dos ativos de suporte e de infraestrutura por ameaças poderá comprometer os ativos primários, especificamente a informação.

Nessa mesma direção, o GSI-PR (2012) estabeleceu diretrizes para o processo de inventário e mapeamento de ativos de informação no âmbito da APF, considerando que tais ativos são todos “os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso”.

A implementação de uma abordagem sistemática do processo de mapeamento e inventário dos ativos de informação, ilustrada na Figura 12, geram subsídios necessários para a implementação da gestão de riscos e da gestão de continuidade dos negócios nos aspectos de SI nas organizações.

Figura 12: abordagem do processo de mapeamento e inventário de ativos de informação.



Fonte: o autor

Como pode ser observado, todo processo de mapeamento e inventário de ativos de informação faz parte do processo de gestão de risco de SI. Os subprocessos 1 e 2 estão inseridos na fase da análise de risco, enquanto o subprocesso 3, como já denominado, integra a fase de avaliação de riscos (ABNT, 2011; GSI-PR, 2013).

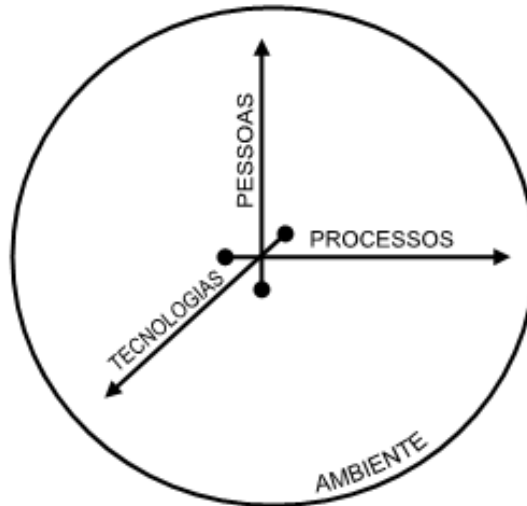
Observa-se que os órgãos da APF já possuem orientações suficientes para o controle de seus ativos de informação, entretanto, o TCU (2014a) registrou que 80% dos órgãos auditados ainda não dispõem de inventários de seus ativos de informação. Essa inobservância pode gerar um descontrole dos riscos a que os ativos, que possuem informações críticas para o negócio, estão submetidos, por outro lado, a proteção adequada dos ativos da informação possibilita garantir o sucesso do negócio da organização (SILVA R., 2010, p. 6).

Naturalmente, as atuais organizações vêm investindo cada vez mais em novas tecnologias, a fim de munir o seu pessoal com as melhores ferramentas e sistemas, especialmente, aqueles relacionados diretamente com o processo de negócio. Essa visão voltada aos processos, pessoas e tecnologia vem sendo o sucesso de muitas empresas no mercado atual, sendo assim, tornou-se o foco das atenções, principalmente, para a SI.

As empresas possuem características particulares e, com isso, terão soluções personalizadas capazes de levá-las também a um nível de SI personalizado (SÊMOLA, 2014,

p. 15), entretanto, ressalta-se a importância de aplicar, também, controles de SI no ambiente onde residem as tecnologias, processo e pessoas. Nesse sentido, os ativos de informação receberam uma nova forma de classificação: pessoas, processos, tecnologia e ambiente, conforme ilustrado na Figura 13.

Figura 13: Tipos de ativos de informação



Fonte: Adaptação da Figura 2.3 de Sêmola (2014, p. 16)

Bain (1937, p. 860) define tecnologia como um conjunto de instrumentos e maquinários que inclui os conhecimentos e as habilidades necessárias para a sua produção e uso. As tecnologias são sistemas que combinam técnicas e atividades realizadas por meio de artefatos dentro de um contexto organizacional. Isso significa que tecnologias não se definem apenas em artefatos e ferramentas, mas também em redes formadas pelas relações sociais que estruturam e permeiam a vida social. Isso demonstra a existência de um círculo entre o homem e a tecnologia, cada um modificando e afetando o outro (KAPLAN, 2003).

Atualmente, além dos aspectos relativos às habilidades e aos artefatos, surgiu a necessidade das organizações aumentarem a produtividade e qualidade dos seus serviços com redução de tempo e custos por meio da automação de seus processos.

Nesse sentido, a Figura 14 apresenta uma nova visão baseada nos conceitos de Bain (1937) e Kaplan (2003), onde o ambiente é representado pela organização que possui pessoas

com habilidades suficientes para usar qualquer tipo de artefato tecnológico, a fim de executarem seus processos de forma automatizada.

Figura 14: Modelo revisado baseado nos conceitos de Bain (1937) e Kaplan (2003).



Fonte: O autor.

Evidentemente, nos dias atuais, a maioria das informações organizacionais está armazenada em suportes de TI, ou então faz parte de processos automatizados, conseqüentemente, gera um falso entendimento em relacionar a SI à Computação. Cabe lembrar, que ainda existem arquivos e processos não automatizados, bem como a presença do recurso humano em todas as fases do ciclo de vida da informação. Sendo assim, os controles de SI devem envolver todos os ativos de informação, não somente na tecnologia, pois as ameaças existem e estão cada vez mais presentes no mundo contemporâneo, prontas para atacarem ou explorar as possíveis vulnerabilidades dos ativos de informação, principalmente, as fragilidades inerentes ao ser humano.

2.3.4.2 Vulnerabilidades e ameaças

Para o GSI-PR (2013, p. 3), vulnerabilidade é um “conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação”. E por se tratar de um fator interno, que independe do mundo externo à organização, todos os

esforços deverão ser direcionados a fim de reduzir ou eliminar as vulnerabilidades que são a raiz da alta exposição ao risco (WESTERMAN; HUNTER, 2008, p. 113).

O GSI-PR (2010, p. 77) considera que a vulnerabilidade possui baixa probabilidade de exploração caso haja um baixo nível de interesse ou potencialidade da fonte de ameaça ou, ainda, se houver controles eficazes de proteção, capazes de eliminar ou reduzir o impacto negativo do risco, haja vista que determinar o interesse ou medir a potência de uma ameaça é algo imprevisível, as organizações governamentais têm que focar suas ações de SI nas vulnerabilidades e não nas ameaças (SIMIÃO, 2009, p. 61).

O levantamento das vulnerabilidades não é algo tão simples. Dependendo do tipo de ativo de informação, deverá ser feito por pessoas especializadas ou até mesmo por meio de soluções de TI. As vulnerabilidades técnicas de sistemas ou aplicações computacionais normalmente necessitam de *softwares* especializados para seu levantamento, diferente de vulnerabilidades do ambiente, que requer o conhecimento técnico de especialistas das áreas onde estão resididos os ativos de informação.

A ABNT (2011, p. 57-58) fornece uma lista de vulnerabilidades conforme apresentado no Apêndice A. Essa lista não é exaustiva, visto que a todo o momento surgem novas vulnerabilidades, principalmente aquelas provenientes das novas tecnologias interligadas à *internet*.

Como já exposto, as vulnerabilidades estão associadas às fragilidades, deficiências ou fraquezas. Conhecer as vulnerabilidades do inimigo ou do concorrente é entender quais são os seus pontos fracos, ou seja, para onde a ameaça vai direcionar o seu ataque.

Normalmente, os ataques cibernéticos são realizados pelo levantamento de vulnerabilidades dos *sites* e equipamentos de proteção das redes computacionais, como roteadores e *firewalls*. Tais vulnerabilidades são passíveis de ocorrer em órgãos que estejam fragilizados nos aspectos de recursos humanos especializados e capacitados, de ausência de políticas de segurança da informação e gestão de riscos, ou processos de classificação. A divulgação dessas deficiências torna-se insumo importante para que os grupos maliciosos priorizem seus ataques:

A 5ª Secretaria de Controle Externo – Secex/5 realizou auditoria no Ministério das Relações Exteriores – MRE no período de 28/7 a 10/9/2010, com o objetivo de avaliar controles gerais de tecnologia da informação – TI e verificar se estão de acordo com a legislação pertinente e com as boas práticas de governança de TI. As ocorrências detectadas foram apresentadas pela equipe de auditoria nos seguintes termos (fls. 7/32): [...] 3.2 – Falhas no processo de software.[...] 3.4 – Inexistência de Comitê de Segurança da Informação e Comunicações [...] 3.5 – Inexistência de Gestor de Segurança

da Informação e Comunicações.[...] 3.7 – Inexistência de Política de Segurança da Informação e Comunicações (POSIC).[...]3.9 – Inexistência de processo de gestão de riscos de segurança da informação [...]3.22 – Inexistência de equipe de tratamento e resposta a incidentes em redes computacionais (ETIR). (TCU, 2011)

O Itamaraty admitiu nesta terça-feira um ataque de hackers ao sistema do Ministério das Relações Exteriores mas informou que a ação foi restrita aos e-mails dos funcionários. Segundo o Itamaraty, o acesso ao chamado IntraDocs, no qual ficam arquivados os telegramas e documentos sigilosos do serviço diplomático, e ao sistema de troca de informações entre o Ministério e os postos diplomáticos no exterior não foram atingidos. A informação sobre o ataque virtual foi noticiada pela coluna Radar.⁹

As vulnerabilidades apresentadas pelos ativos de informação não geram apenas impactos negativos aos negócios organizacionais. Quando se fala em APF, apenas uma publicação indevida de um determinado agente público pode impactar a sua privacidade e sua vida privada, incluindo seus familiares e, provavelmente, acarretará prejuízos de ordem financeira e de imagem para a organização.

Cabe lembrar que algumas atividades exercidas pelos agentes públicos na APF possuem riscos elevadíssimos inerentes às suas atividades, pois algumas interferem diretamente nas ações ilícitas que contrariam os interesses de grupos mal intencionados. Como exemplo de agentes públicos mais expostos, citem-se: auditores, corretores, militares, fiscais, agentes penitenciários, policiais federais e rodoviários federais.

A Lei n 9.883 de 1999 preconiza que as informações e documentos sobre atividades e assuntos de inteligência produzidos pela Agência Brasileira de Inteligência (ABIN) somente poderão ser fornecidos às autoridades que tenham competência legal para solicitá-las (BRASIL, 1999), neles incluem-se as informações sobre os servidores da ABIN, visto que poderão comprometer as “atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações” (BRASIL, 2011). Com esse fundamento, não são divulgadas informações sobre os agentes públicos da ABIN no DOU e Portal da Transparência.

Nota-se que o cumprimento dessa determinação foi, particularmente, aplicado em virtude dos interesses do Estado, e não em relação à integridade da pessoa dos seus agentes. Visto que as atividades de inteligência não são exclusivas à ABIN, pois todo órgão ou

⁹ Notícia publicada no dia 27 de maio de 2014 por Reinaldo Azevedo na VEJA.com.

Disponível em: <<http://veja.abril.com.br/blog/reinaldo/geral/itamaraty-admite-que-ciberataque-permitiu-acesso-a-e-mails-de-funcionarios/>>. Acesso em: 20 dez de 2014.

entidade da APF que produzir conhecimentos de interesse das atividades de inteligência, inclusive aqueles responsáveis pela segurança interna, integrarão o Sistema Brasileiro de Inteligência (SISBIN) (BRASIL, 1999). Com isso, torna-se notório o tratamento diferenciado da proteção das informações pessoais dos agentes públicos na APF.

Diferente das vulnerabilidades, as ameaças são “fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização” (GSI-PR, 2013, p. 2), entretanto, a ISO/IEC (2014) define apenas como uma causa potencial, considerando assim, que pode ser um fator interno ou externo, por outra palavra, a fonte de ameaça pode residir dentro ou fora da organização (ABNT, 2011, p. 17).

Como visto, as ações de SI são focadas nas vulnerabilidades e visam reduzir a probabilidade do êxito das ações das ameaças. Uma determinada organização, por exemplo, que invista em sistemas de controles de acesso físico e biométrico visando impedir a entrada de pessoas não autorizadas está aplicando uma ação de SI. Decerto, tais ações foram tomadas para bloquear o acesso de pessoas não credenciadas a esse local, ou seja, a entrada de possíveis ameaças.

Entretanto, isso não impede que haja um vazamento de informação efetuado por uma pessoa credenciada, mesmo que este não aja de forma intencional. Nesse caso, é preferível assumir que houve uma falha no processo de credenciamento ou então no processo de seleção e recrutamento da organização ao invés de considerar que houve um incidente gerado por uma ameaça interna.

O exemplo apresentado reforça que o tratamento das vulnerabilidades é uma ação de SI, já o tratamento das ameaças é uma atividade de inteligência (SIMIÃO, 2009, p. 70), porém, isso não significa que as ameaças serão desprezadas, a organização precisa compreendê-las e levá-las visando associá-las às suas vulnerabilidades a fim de aplicar os melhores controles de SI, considerando a relação custo-benefício. O monitoramento das ameaças é um tipo de ação ou controle de segurança.

A ABNT (2011, p. 53-54) disponibiliza uma tabela contendo exemplos de ameaças típicas que comprometem a SI. A referida tabela é apresentada de acordo com o tipo, descrição e origem das ameaças conforme apresentado no Apêndice B. As ameaças são classificadas como intencionais, acidentais e naturais, sendo que as ameaças intencionais e acidentais estão relacionadas com as ações de origem humana, já as naturais não há participação do fator humano para sua ocorrência.

Para fins deste estudo, é apresentado o Quadro 8 que descreve as fontes de ameaças representadas por seres humanos e suas motivações:

Quadro 8: Ameaças representadas por seres humanos

Origem das ameaças	Motivação
1. <i>Hacker, cracker</i>	a) Desafio
2. Criminoso digital	b) Ego
3. Crime organizado	c) Rebeldia
4. Espionagem comercial e empresarial	d) Status
5. Governos estrangeiros	e) Ganho monetário
6. Manifestantes	f) Destruição de informações
	g) Divulgação ilegal de informações
	h) Alteração não autorizada de dados
	i) Chantagem
	j) Vingança
	k) Vantagem competitiva
	l) Cobertura da mídia
	m) Questões políticas

Fonte: Adaptação da ABNT (2001, p. 55)

2.3.4.3 Impactos e probabilidades da quebra da SI

Depois de identificados os ativos, as ameaças, as vulnerabilidades e os controles de segurança já existentes durante a fase de identificação dos riscos, torna-se necessário estimá-los por meio de atribuição de valores e níveis definidos a fim de mensurar os impactos ou consequências causados por eventuais incidentes de segurança que venham afetar a confidencialidade, integridade e disponibilidade das informações.

Para a ABNT (2011, p.1), a consequência é o resultado que afeta os objetivos, podendo ser certo ou incerto, mas caso ocorra no âmbito da SI, os resultados serão sempre negativos. Um evento adverso pode gerar impactos em diferentes níveis para cada organização. As consequências de uma descarga elétrica originada por um raio pode ter um valor baixo para um órgão, entretanto, esta mesma ameaça pode causar impactos de alto nível a outro.

O impacto da quebra de SI da privacidade de um agente público acarretará consequências negativas tanto para a organização, como para a pessoa do agente. Para o órgão, as consequências refletirão em torno da imagem institucional, de perdas financeiras, de processos judiciais, já para o agente público, as consequências poderão ser irrecuperáveis, principalmente se afetar a sua integridade física e a sua intimidade.

Houve uma grande mudança de comportamento da atual sociedade diante da exposição de seus dados e informações no espaço virtual. No mundo real, quando algum documento era extraviado, roubado, furtado ou perdido, o seu titular imediatamente tomava as providências necessárias para lavrar um boletim de ocorrência, comunicar com os órgãos de proteção ao crédito, tudo a fim de evitar ou reduzir os possíveis impactos provenientes do uso indevido de suas informações.

Entretanto, atualmente, não existe essa preocupação no mundo virtual, muitos dados daqueles encontrados em documentos físicos estão disponíveis na *internet* sem que seu proprietário saiba, e às vezes estão expostos pela própria ação do indivíduo.

As atuais tecnologias de recursos gráficos e de impressão possibilitam a falsificação de documentos que dificultam a identificação de sua veracidade. Com um documento falso de boa impressão, associados com dados íntegros, qualquer um pode se passar por outra pessoa. A maioria das cédulas de identidade possui os seguintes campos essenciais: nome, número, filiação, data de expedição, naturalidade, nacionalidade. Estas informações são encontradas com facilidades na *internet*, inclusive, nos portais de governo, conforme ilustrado na Figura 15, que visualiza uma publicação de um julgado do Tribunal Regional Federal no DOU.

Figura 15: Exemplo de publicação de dados pessoais no DOU

O Exmo. Sr. Juiz exarou :
 Fls. 50/51
 (...)
 Ante o exposto, JULGO PROCEDENTE O PEDIDO, extinguindo o processo nos termos do art. 269, I, do Código de Processo Civil e condeno o réu à obrigação de conceder em favor da parte autora - [REDACTED] - o benefício de APOSENTADORIA POR INVALIDEZ, desde a data do requerimento administrativo, (DJB) em 20/03/2014, com data de início de pagamento (DIP) em 01/02/2015 (art. 80, par. Único, III, "g", da Resolução/Presi/Cojef nº 16/2010), pagando as diferenças devidas, que deverão sofrer a incidência, uma única vez, para fins de atualização monetária, remuneração do capital e compensação da mora, dos índices oficiais de remuneração básica e juros aplicados à caderneta de poupança, na forma do art. 1º F, da Lei 9.494/97, com alteração dada pela Lei 11.960/2009, devendo ser cessado qualquer benefício inacumulável e compensadas eventuais parcelas recebidas em decorrência de benefícios inacumuláveis concedidos e que foram gozados no mesmo período.
 Cópia desta sentença servirá como ofício requisitório ao INSS, para que proceda implantação do benefício em nome da parte autora, na forma acima exposta, devendo apresentar a este Juízo o comprovante da implantação.
 Parâmetros para a implantação do benefício, nos termos do art. 80, parágrafo único, III e IV, da Resolução/Presi/Cojef nº 16/2010:
 Nome completo: [REDACTED]
 Filiação: [REDACTED]
 Documento de identidade/Emissor/UF: [REDACTED]
 Cadastro pessoa física (CPF): [REDACTED]
 Data e local de nascimento: [REDACTED]
 Benefício concedido: APOSENTADORIA POR INVALIDEZ
 Renda mensal atual (RMA):
 Data de início do benefício (DIB): 20/03/2014
 Renda mensal inicial (RMI):
 Data de início do pagamento (DIP): 01/02/2015
 Número do benefício cessado:
 Outras informações:
 Sem honorários nem custas, por força do art. 55 da Lei 9.099/95.
 Com o trânsito em julgado, expeça-se RPV para as prestações vencidas até a DIP.
 Cumprida a sentença, arquivem-se os autos.
 Publique-se. Registre-se. Intime-se.

Fonte: DOU (Imprensa Nacional), 2014.

Enquanto o Projeto de Lei (PL) que dispõe sobre a proteção de dados pessoais e da privacidade não é aprovado, o cidadão fica exposto aos diversos riscos de SI. Os órgãos de governo responsáveis pelos portais e canais que promovem a transparência pública devem entender que tratar com dados pessoais é uma atividade de risco, pois pode causar danos e impactos de ordem patrimonial, moral e física ao cidadão, e consequentemente, responderão perante a Lei com obrigações de ressarcimento do dano gerado (BRASIL, 2015).

Existe uma similaridade entre os conceitos de dado pessoal e informação pessoal. O citado PL define que dado pessoal é “qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores” (BRASIL, 2015). A LAI define que informação pessoal é “aquela relacionada à pessoa natural identificada ou identificável” (BRASIL, 2011). Sendo assim, infere-se que tanto o CPF, quanto o endereço de um agente público, estão inseridos nos conceitos citados e a divulgação indevida desses, além de constituir como uma conduta ilícita (BRASIL, 2011), gera consequências negativas à vida privada do agente público (STF, 2011).

Para as organizações, “as consequências podem ser expressas em função dos critérios de impacto monetários, técnicos ou humanos, ou de outro critério relevante” (ABNT, 2011, p. 22). Sobre os aspectos da SI, os órgãos da APF podem utilizar os seguintes critérios para estimar os impactos decorrentes da quebra da confidencialidade, integridade, disponibilidade e autenticidade das informações:

- a) Violação das leis e normativos;
- b) Efeitos negativos sobre a imagem e reputação da organização;
- c) Violação de SI relacionada às informações pessoais;
- d) Perdas financeiras;
- e) Perigo ocasionado à segurança física de seus agentes públicos; e
- f) Crise governamental.

A ABNT (2011, p. 51) entende que o impacto está relacionado com o sucesso do incidente de segurança e ressalta a diferença entre o valor do ativo e o impacto do incidente. É preciso entender que na SI a preocupação está voltada especificamente para informação. O valor do ativo não pode ser mensurado em relação ao seu valor monetário e sim com a importância da informação que ele carrega. O impacto da perda de um *pen drive* pode ser superior que a perda de um *notebook*, entretanto, torna-se complexo aplicar os controles de SI

para cada ativo, visto que, surge um novo componente a ser considerado: o fator probabilístico.

Normalmente, o foco das atenções da maioria dos gestores de segurança da informação incide sobre os riscos que produzem danos de alto impacto para a organização. As metodologias e ferramentas de análise de riscos direcionam para essa visão, entretanto cabe salientar que incidentes frequentes, mesmo que possuam baixo impacto, podem ter efeitos cumulativos ou de longo prazo (ABNT, 2012, p. 9). Toma-se como exemplo, a divulgação de um tipo de dado ou informação cuja consequência ou impacto tenha baixo nível, mas quando, armazenado e associado a outros dados durante um período de tempo, forma uma grande base de dados capaz de gerar impactos de alto valor.

Como exemplificado acima, além da possibilidade de que o impacto da perda ou extravio de um *pen drive* seja maior de que a perda de um *notebook*, infere-se que a chance disso acontecer é bem maior. Esse fato não corresponde apenas ao tamanho e portabilidade do ativo e sim a frequência de ocorrência registrada sobre esse fato. Para a SI, a “chance de algo acontecer” é definida como probabilidade (ABNT, 2011, p. 3):

O vazamento de informações corporativas causado por perda ou roubo de pen drives tem se tornado cada vez mais freqüente nas estatísticas, de forma proporcional ao crescimento do uso desse tipo de memória portátil. Recentemente, nos Estados Unidos, nomes, endereços, números de identidade e registros médicos de 120 000 pacientes do hospital Wilcox Memorial, no Havaí, foram expostos por causa de um pen drive perdido. O mesmo aconteceu com 6 500 alunos da Universidade do Kentucky, que tiveram suas informações expostas após o extravio do pen drive de um professor. [...] ¹⁰

O impacto possui relação com os ativos e estes com as vulnerabilidades. Já a probabilidade está relacionada às ameaças. Sendo assim, é possível tratar alguns riscos reduzindo o fator exposição perante as ameaças. Para Ramos et. al (2008, p. 62), a probabilidade pode ser analisada por dois fatores: frequência e vulnerabilidade. A frequência representa as tentativas das ameaças na exploração das vulnerabilidades, enquanto as vulnerabilidades são as oportunidades cedidas para as ameaças atingirem seus objetivos.

A mensuração do nível de probabilidade depende de registros e históricos dos cenários de incidentes ocorridos no escopo onde é efetuada a gestão de risco. Torna-se imprescindível

¹⁰ Notícia publica no dia 26 de junho de 2008 pela Revista Exame.

Disponível em: <<http://exame.abril.com.br/revista-exame/edicoes/921/noticias/tao-pequeno-e-tao-perigoso-m0162637>>. Acesso em: 20 de janeiro de 2015.

conhecer o perfil das ameaças, suas motivações, suas competências. Subestimar uma ameaça é uma falha comum dos profissionais de segurança.

A ABNT (2012, 10) define três abordagens empregadas para estimar a probabilidade que podem ser utilizadas isoladamente ou em conjunto:

- a) A utilização de dados históricos para identificar eventos ou situações passadas;
- b) Previsões de probabilidade com uso de técnicas preditivas; e
- c) Opiniões de especialistas.

Nem sempre as organizações possuem dados confiáveis e registros históricos, como também não possuem profissionais habilitados em técnicas preditivas, e dessa forma ficam dependentes de fontes externas, pessoas e ferramentas, para execução das atividades de análise e avaliação de risco.

Em Knight (1921 *apud* Andrade 2011, p. 173) é fornecida uma taxonomia com três categorias para o termo probabilidade: *a priori*, estatística e estimativa. As duas primeiras auxiliam na análise quantitativa e a terceira na análise qualitativa. As probabilidades do tipo *a priori* e estatística requerem conhecimentos técnicos e habilidades específicas, pois tratam com números e dependem de dados registrados e confiáveis, sendo assim não são comumente utilizadas nas organizações públicas que preferem a do tipo estimativa.

Uma estimativa é um julgamento intuitivo que orienta o processo de tomada de decisão dos agentes; estes agem, de modo geral, com base em estimativas e não inferências, valendo-se de “julgamentos” ou “intuição”, e não de raciocínio lógico estrito (KNIGHT, 1921 *apud* ANDRADE, 2011, p. 174).

3 METODOLOGIA

3.1 Caracterização da pesquisa

Como já abordado na descrição da justificativa e dos objetivos deste estudo, o ato de verificar possibilidades ou hipóteses da quebra de SI durante a divulgação de dados e informações nos portais da *internet* do governo federal e torná-las explícitas, caracteriza esta pesquisa como exploratória (GIL, 2002, p.41), pois “busca-se descobrir se existe ou não um fenômeno” (MATIAS-PEREIRA, 2007, p. 48), a fim de elucidá-lo ou explicar aquilo que ainda não é aceito apesar de ser evidente (OLIVEIRA NETTO, 2006, p. 9). Quanto à natureza, esta pesquisa é classificada como aplicada, pois envolve verdades e busca produzir conhecimentos para aplicação prática sobre a SI (CERVO; BERVIAN, 1983).

Considerando a *internet* como um grande arquivo de documentos e informações de livre acesso, realiza-se um levantamento documental de fontes primárias disponíveis nas páginas oficiais da administração pública a fim de levantar dados que sustentam a realização desta pesquisa.

Para Lakatos e Marconi (2003, p. 159), “a soma do material coletado, aproveitável e adequado, variará de acordo com a habilidade do investigador, de sua experiência e capacidade em descobrir indícios ou subsídios importantes para seu trabalho”.

Para a realização deste estudo torna-se necessário descrever os *sites* de governo que promovem a transparência pública, determinando suas características, funcionalidades, bem como os tipos de dados e informações por eles divulgados, com isso, esta pesquisa também pode ser caracterizada como descritiva que “acaba servindo mais para proporcionar uma nova visão do problema”, aproximando-se das pesquisas exploratórias (GIL, 2002, 42).

Para a elaboração do referencial teórico, utilizou-se pesquisa bibliográfica a partir de consultas em livros, artigos, dissertações, teses de diversos pesquisadores, bem como pesquisa documental para o levantamento do arcabouço legal sobre o tema proposto, entre os quais: leis, decretos, instruções normativas e NC:

A pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores [...]. No caso da pesquisa documental, tem-se como fonte documentos no sentido amplo, ou seja, não só documentos impressos, mas sobretudo de outros tipos de documentos, tais como jornais, fotos, filmes, gravações, documentos legais (SEVERINO, 2007, p. 122-123).

A partir dos dados obtidos na *internet*, é possível construir informações e conhecimentos que permeiam os paradigmas da CI apresentados por Capurro e Hjørland

(2007), considerando que os dados e informações dos agentes públicos pesquisados estão inseridos no campo social, as informações do ambiente tecnológico da organização no campo físico, e por fim, o conhecimento gerado a partir dos dados e informações expostos pela organização, no campo cognitivo.

3.2 Ambiente da pesquisa

Para Meirelles (1998, p. 65) a “administração pública é todo o aparelhamento do Estado, preordenado à realização de seus serviços, visando à satisfação das necessidades coletivas”, no entanto, as atividades executadas no ambiente da administração pública de quaisquer Poderes da União, dos Estados, do Distrito Federal e dos Municípios devem ser reguladas em conformidade com a Constituição Federal, principalmente em obediência aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Os indivíduos investigados na presente pesquisa pertencem ao quadro dos órgãos da APF responsáveis pela segurança nacional e segurança pública, entretanto o fato de existirem dados e informações pessoais desses agentes em outras esferas administrativas, o ambiente pesquisado inclui outros portais da *internet* de órgãos pertencentes aos demais Poderes da União, dos Estados e do Distrito Federal.

As atividades de segurança nacional são aquelas destinadas a combater crimes que venham lesar ou expor o perigo de lesão: i) a integridade territorial e a soberania do Estado; ii) o regime representativo e democrático, a Federação e o Estado de Direito; e iii) a pessoa dos chefes dos Poderes da União (BRASIL, 1983). Nesse sentido, tais atividades são exclusivas às Forças Armadas (FFAA) e ao GSI-PR:

Art. 142. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem. (BRASIL, 1988)

Art. 6º. Ao Gabinete de Segurança Institucional da Presidência da República compete: [...] II - prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional; III - realizar o assessoramento pessoal em assuntos militares e de segurança; IV - coordenar as atividades de inteligência federal e de segurança da informação; V - zelar, assegurado o exercício do poder de polícia, pela segurança pessoal do Chefe de Estado, [...] (BRASIL, 2003).

Devido à importância do papel das autoridades responsáveis pela classificação em níveis de sigilo das informações listadas no art. 23 da LAI para a segurança do Estado e da

sociedade, consideraram-se nesta pesquisa tais autoridades como agentes públicos de segurança nacional.

Já as atividades de segurança pública federal são aquelas destinadas à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, e são exercidas no âmbito da APF pelo Departamento da Polícia Federal e pelo Departamento da Polícia Rodoviária Federal (BRASIL, 1988), ambos pertencentes à estrutura do Ministério da Justiça.

Em virtude da sua importância na articulação e integração do Sistema Penitenciário Federal com os órgãos componentes do Sistema Nacional de Segurança Pública, principalmente no planejamento de atividades de inteligência, considerou-se, também, o Departamento Penitenciário Nacional, também vinculado ao Ministério da Justiça, como um órgão de segurança pública.

3.3 População da pesquisa

A população desta pesquisa é formada por agentes públicos que atuam nas atividades relativas à segurança nacional e segurança pública federal. Estes agentes estão lotados em diversos órgãos da APF, distribuídos geograficamente por todo o território nacional.

No contexto da segurança nacional, a população é representada pelos militares das FFAA, pelos oficiais de inteligência da ABIN, pelos servidores da Secretaria de Segurança Presidencial, e também, pelas autoridades classificadoras estabelecidas pela LAI.

Já no contexto da segurança pública federal, a população é formada pelos delegados da Polícia Federal (DPF), pelos policiais rodoviários federais (PRF) e pelos agentes penitenciários federais (AGPENF). Para isso, definiu-se um conjunto de indivíduos que partilham, no mínimo, de uma característica comum (MARCONI; LAKATOS, 1996) apresentados nos Quadro 9 e 10, representando a população desses indivíduos a serem pesquisados.

Quadro 9: Grupos de indivíduos que promovem a segurança nacional.

SEGURANÇA NACIONAL	
ÓRGÃOS E AUTORIDADES	POPULAÇÃO
FFAA	Militares da Marinha do Brasil
	Militares do Exército Brasileiro
	Militares da Força Aérea Brasileira
GSI-PR	Servidores da Agência Brasileira de Inteligência
	Servidores da Secretaria de Segurança Presidencial
Autoridades da APF	Autoridades classificadoras em graus de sigilo

Fonte: O autor.

Quadro 10: Grupos de indivíduos que promovem a segurança pública federal.

SEGURANÇA PÚBLICA FEDERAL	
ÓRGÃOS	POPULAÇÃO
DEPARTAMENTO DE POLÍCIA FEDERAL	Delegados da Polícia Federal (DPF)
DEPARTAMENTO DE POLÍCIA RODOVIÁRIA FEDERAL	Policiais Rodoviários Federais (PRF)
DEPARTAMENTO PENITENCIÁRIO FEDERAL	Agentes Penitenciários Federais (AGPENF)

Fonte: O autor

3.4 Amostra da pesquisa

Para Cooper e Schindler (2003, p. 150), é por meio da amostragem que se tira conclusões ao extrair elementos de uma determinada população. Na pesquisa quantitativa, a amostra consiste em escolher subconjuntos da população que se pretende estudar a fim de obter resultados de forma generalizada, entretanto, por se tratar de uma pesquisa qualitativa, a maior preocupação neste estudo é o aprofundamento e a abrangência da compreensão dos riscos inerentes à divulgação de dados de uma específica classe de agentes públicos.

Assim, esta pesquisa é qualitativa, pois além de responder questões particulares as quais não se pode quantificar, necessita de definições claras e objetivas dos sujeitos que comporão a amostragem dos indivíduos investigados (MINAYO, 2001, p.21), haja vista que urge a necessidade de priorizar o critério de intencionalidade do pesquisador a fim de atender um fim específico (GIL, 2002, p. 145).

Sendo assim, com a finalidade de obter um “bom julgamento” das populações apresentadas no item anterior e considerando a intencionalidade do pesquisador, decidiu-se o uso da amostragem não probabilística do tipo intencional (SILVA; MENEZES, 2005, p. 32) para construção de dois planos de amostragem.

O primeiro plano de amostragem (Quadro 11) apresenta uma lista de autoridades que possuem um importante papel no atual cenário nacional e internacional, bem como são detentoras de informações imprescindíveis à segurança da sociedade ou do Estado.

Quadro 11: Amostra de indivíduos que promovem a segurança nacional.

POPULAÇÃO	AMOSTRA		
	Quantidade	Cargo	Competência
Militares da Marinha do Brasil	01 militar	Diretor do Centro Tecnológico da Marinha em São Paulo	Responsável pelo Programa Nuclear da Marinha do Brasil
Militares do Exército Brasileiro	01 militar	7º Subchefe do Estado-Maior do Exército	Responsável pelas Políticas e Estratégias do Exército Brasileiro
Militares da Força Aérea Brasileira	01 militar	Comandante da Defesa Aeroespacial Brasileira	Responsável pelo órgão central da defesa aeroespacial e do controle de engenhos espaciais, incumbido de liderar e de integrar todos os meios de monitoramento aeroespacial do País.
Servidores da Agência Brasileira de Inteligência (ABIN)	01 oficial de inteligência	Diretor-Geral da ABIN	Responsável pelo desenvolvimento e execução da atividade de Inteligência do Estado brasileiro
Servidores da Secretaria de Segurança Presidencial	01 servidor	Secretário de Segurança Presidencial	Responsável pela Segurança pessoal do Presidente da República e do Vice-Presidente da República e de seus familiares
Autoridades classificadoras em graus de sigilo	02 Ministros de Estado	Ministro da Defesa	Chefe superior das Forças Armadas
		Ministro Chefe do GSI-PR	Atua na prevenção da ocorrência e articulação do gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional

Fonte: O autor

Já o segundo plano de amostragem é composto por indivíduos que atuam na Segurança Pública e pertencentes aos cargos de DPF, de PRF e de AGPENF. Considerando que os indivíduos ocupantes dos cargos de DPF e PRF estão distribuídos em todas UF e o cargo de AGPENF em apenas cinco UF que possuem penitenciárias federais, optou-se investigar um indivíduo por UF, conforme distribuído na Tabela 2.

Tabela 2: Amostra de indivíduos que promovem a segurança pública federal, por UF.

UF	DPF	PRF	AGPENF	TOTAL
AC	1	-	-	1
AL	-	1	-	1
AM	1	-	-	1
AP	-	1	-	1
BA	1	-	-	1
CE	-	1	-	1
DF	-	-	1	1
ES	1	-	-	1
GO	-	1	-	1
MA	1	-	-	1
MG	-	1	-	1
MS	-	-	1	1
MT	1	-	-	1
PA	-	1	-	1
PB	1	-	-	1
PE	-	1	-	1
PI	1	-	-	1
PR	-	-	1	1
RJ	-	1	-	1
RN	-	-	1	1
RO	-	-	1	1
RR	1	-	-	1
RS	-	1	-	1
SC	1	-	-	1
SE	-	1	-	1
SP	1	-	-	1
TO	-	1	-	1
TOTAL				27

Fonte: O autor.

3.5 Coleta dos dados

Para Mill e Fidalgo (2007), o uso da *internet* como suporte técnico para coleta de dados para pesquisas científicas possui os seguintes benefícios:

- a) Alimentação automática do banco de dados;
- b) Coerência dos dados, por reduzir a margem de erros de digitação; e
- c) Organização automática das informações coletadas em banco de dados.

Outro fator importante a ser observado está relacionado à fonte de coleta de dados, visto que nesta pesquisa, o investigador limita-se apenas aos portais de governo, ora considerados fontes íntegras e autênticas de informações e, conseqüentemente, a análise de seus conteúdos representa uma excelente técnica de coleta de dados.

Para atingir os objetivos propostos nesta pesquisa, a coleta de dados foi executada em duas etapas. A primeira etapa realizada por meio do levantamento dos dados disponibilizados na *internet* relativos aos agentes públicos investigados. Já a segunda etapa, por meio de um questionário destinado aos representantes oficiais da área de SI na APF.

3.5.1 Dados publicizados dos agentes públicos da APF

Com a finalidade de verificar a existência de evidências que comprovem a possibilidade de quebra de privacidade dos indivíduos investigados, bem como os riscos gerados para o Estado com a divulgação dos dados pessoais de seus agentes públicos, realiza-se uma pesquisa documental em portais da *internet* da administração pública que promovem a transparência pública.

A coleta de dados dos indivíduos investigados foi realizada conforme os seguintes passos apresentados abaixo e ilustrado na Figura 16.

1º PASSO – Entrar no Portal da Transparência (<http://transparencia.gov.br/downloads/servidores.asp#getM>) e baixar os arquivos referentes aos servidores civis e militares.

Por meio desses arquivos é possível obter os seguintes dados:

- CPF incompleto, exemplo: (***.456.789-**)
 - Nome completo
 - Cargo
 - Órgão em exercício
 - UF do órgão em exercício – Este dado nem sempre é disponibilizado
 - Remuneração

2º PASSO – Entrar no Portal do DOU (www.portal.in.gov.br) na tentativa de obter os seguintes dados sobre o servidor investigado por meio de consultas pelo “Nome Completo”:

- CPF completo
- UF do órgão em exercício, caso não conste na busca anterior
- Períodos de afastamentos e viagens
- Data de nascimento
- Naturalidade
- Filiação
- Nome de filhos
- Resultados de julgamentos
- Outros dados relevantes

3º PASSO – Entrar no Portal do órgão em exercício do servidor investigado, indicado pelo campo “órgão em exercício”, a fim de obter dados não encontrados no passo anterior ou que sejam relevantes.

4º PASSO – Entrar no Portal da Secretaria de Fazenda referente ao Estado ou Distrito Federal indicado pelos campos “naturalidade” e “UF do órgão em exercício”, a fim de obter dados do servidor investigado por meio de consultas disponíveis ao cidadão, como por exemplo, emissão de certidões.

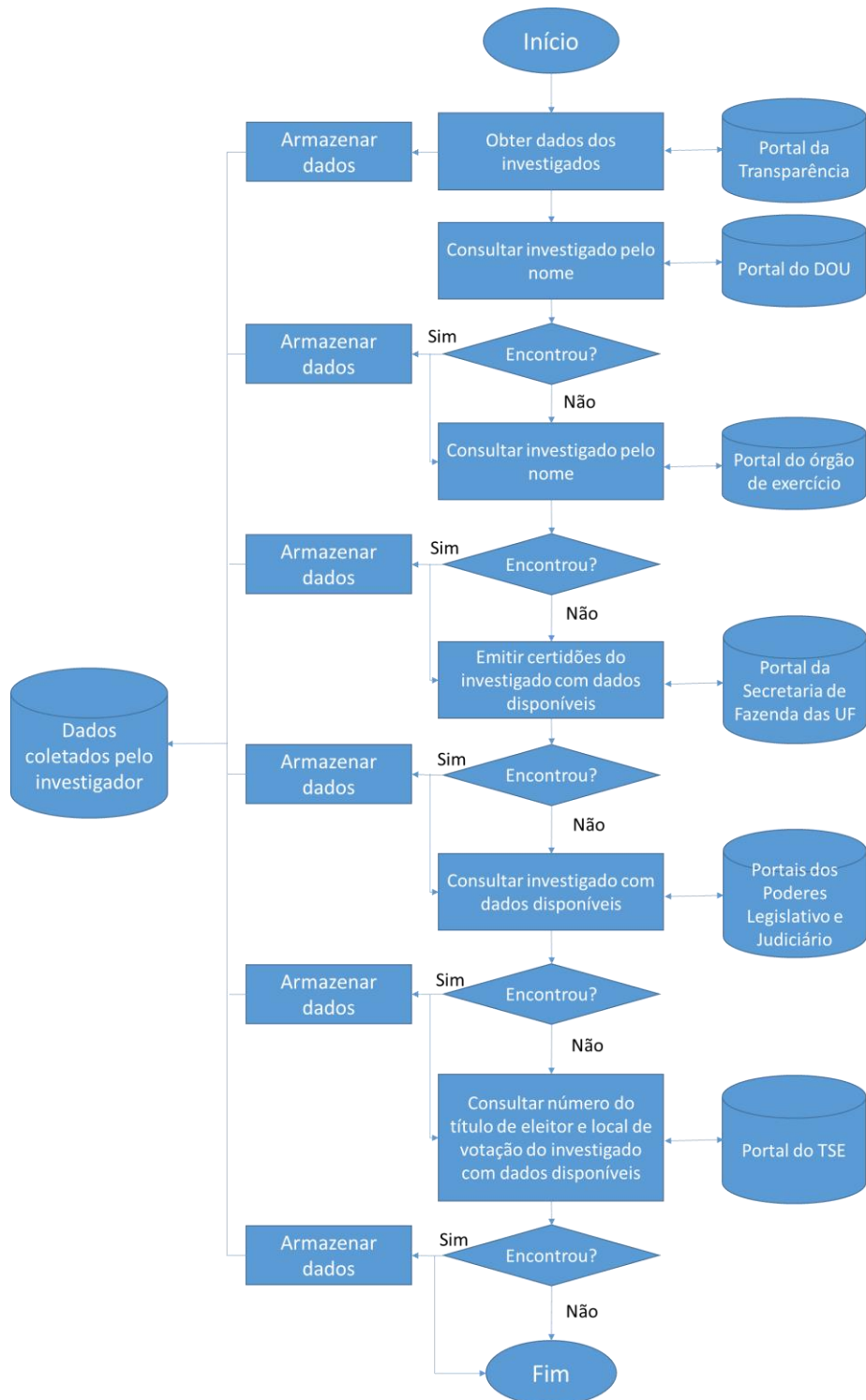
Caso não seja identificado o campo “naturalidade”, será investigado o portal da Secretaria de Fazenda referente ao Estado ou Distrito Federal indicado pelo nono campo do CPF conforme apresentado no Quadro 1.

5º PASSO – Entrar no Portal dos Poderes Legislativos e Judiciários da União e do Estado/Distrito, a fim de obter dados não encontrados nos passos anteriores ou que sejam relevantes.

6º PASSO – Caso seja identificado o campo “data de nascimento” e “nome da mãe”, entrar no Portal do Tribunal Superior Eleitoral (TSE) (<http://www.tse.jus.br/eleitor/servicos/titulo-e-local-de-votacao/consulta-por-nome>), a fim de se obter os seguintes dados:

- Número de inscrição eleitoral, zona e seção
- Local de votação
- Situação eleitoral

Figura 16: Fluxograma dos passos da coleta de dados dos indivíduos



Fonte: O autor

3.5.2 Questionário

Com objetivo de validar o processo de análise dos dados coletados por ocasião do desenvolvimento de um método de análise de impacto das informações dos agentes públicos da APF publicizadas em sistemas de promoção da transparência, foi realizado um questionário, conforme formulário apresentado no Apêndice B, por meio de um questionário (GOODE, HATT, 1960) entregue pessoalmente a cada representante titular ou suplente dos 17 (dezesete) órgãos pertencentes ao CGSI.

A atual composição do CGSI foi formalizada pela Portaria nº 7 de 17 de março de 2015 do Ministro de Estado Chefe do GSI-PR (Anexo A), publicada no DOU nº 52 de 18 de março de 2015.

Os representantes do CGSI possuem uma visão mais crítica e estratégica dos problemas relacionados a SI, visto que para indicação desses, o GSI-PR sugere que o perfil dos representantes indicados por cada Ministério seja de nível estratégico, como por exemplo, secretário ou equivalente.

Sendo assim, tornou-se de suma importância a participação dos representantes do CGSI nesta pesquisa, pois os seus membros além de possuírem perfil estratégico em seus órgãos, incluem 6 (seis) integrantes, cujos órgãos estão diretamente relacionados aos temas transparência, privacidade e SI, que são: a Advocacia-Geral da União, CGU, GSI-PR, Casa Civil, Ministério da Defesa e Ministério da Justiça.

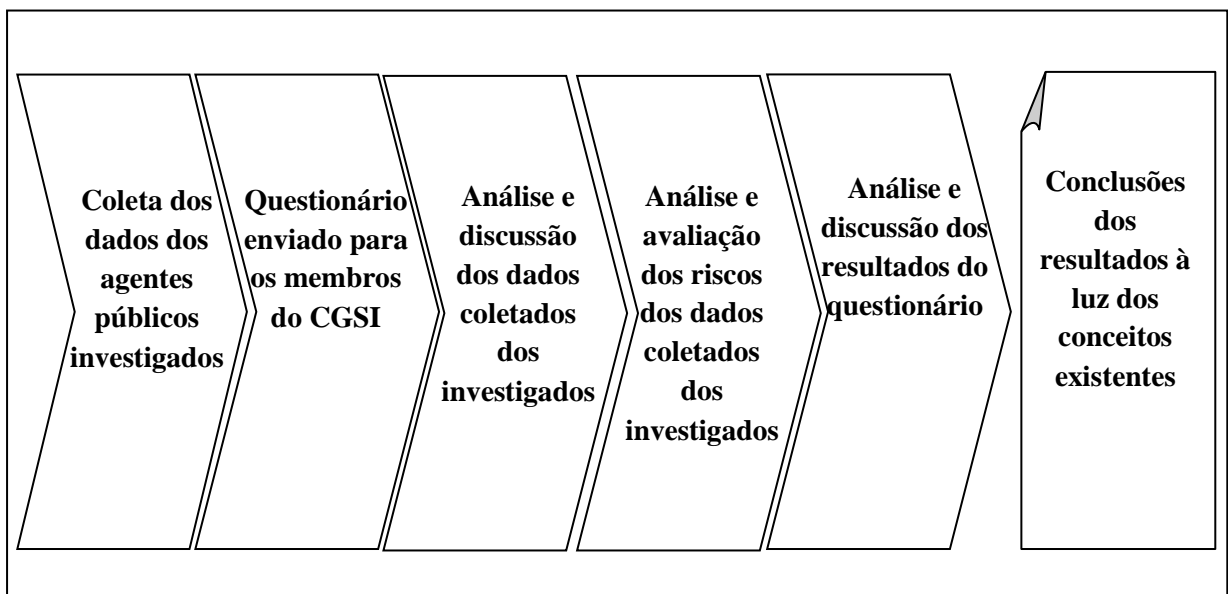
4 ANÁLISE E DISCUSSÃO

O presente capítulo trata da apresentação dos dados coletados referentes aos fatores de risco expostos a partir da publicação de informações de agentes públicos por meio de pesquisa documental e aplicação do método de investigação apresentado no item anterior e da apresentação dos resultados obtidos no questionário. Em seguida, realiza-se a análise e discussão dos resultados obtidos por meio da pesquisa documental e do questionário.

O processo de análise dos dados envolve diversos procedimentos: codificação das respostas, tabulação dos dados e cálculos estatísticos. Após, ou juntamente com a análise, pode ocorrer também a interpretação dos dados, que consiste, fundamentalmente, em estabelecer a ligação entre os resultados obtidos com outros já conhecidos, quer sejam derivados de teorias, quer sejam de estudos realizados anteriormente (GIL, 2002, p. 125).

A Figura 17 ilustra o processo de aplicação do método de investigação utilizado nesta pesquisa.

Figura 17: Processo metodológico



Fonte: O autor.

4.1 Informações pessoais comunicadas por sistemas de promoção da transparência

A Tabela 3 apresenta os resultados obtidos durante a coleta de dados dos 7 (sete) indivíduos constantes da amostragem de agentes públicos que atuam na segurança nacional na APF.

Tabela 3: Resultados da coleta de dados dos agentes de segurança nacional.

CODIGO DO INVESTIGADO	ORGAO	CARGO	NOME	UF DO ORGAO	CPF	IDENTIDADE	DATA DE NASCIMENTO	NATURALIDADE	NOME DO PAI	NOME DA MAE	NOME DO CONJUGUE	NOME DO FILHO	ENDEREÇO	PERIODO DE VIAGENS	TITULO DE ELEITOR	LOCAL DE VOTAÇÃO
I_01	MD	Ministro	Jaques Wagner	DF	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
I_02	GSI-PR	Ministro	Jose Elito Carvalho Siqueira	DF	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
I_03	GSI-PR	Secretário de Segurança Presidencial	Marcos Antonio Amaro dos Santos	DF	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
I_04	GSI-PR	Diretor-Geral da ABIN	Wilson Roberto Trezza	DF	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
I_05	ME	Diretor do Centro Tecnológico da Marinha em São Paulo	André Luis Ferreira Marques	SP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_06	EB	7º Subchefe do Estado-Maior	Fernando José Soares da Cunha Mattos	DF	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗
I_07	FAB	Comandante da Defesa Aeroespacial Brasileira	Antonio Carlos Egito Amaral	DF	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗

✓ ENCONTRADO ✗ – NÃO ENCONTRADO

Fonte: O autor.

Já a Tabela 4 apresenta os resultados obtidos da coleta de dados dos 27 (vinte e sete) indivíduos constante da amostragem dos agentes públicos da APF que atuam na segurança pública.

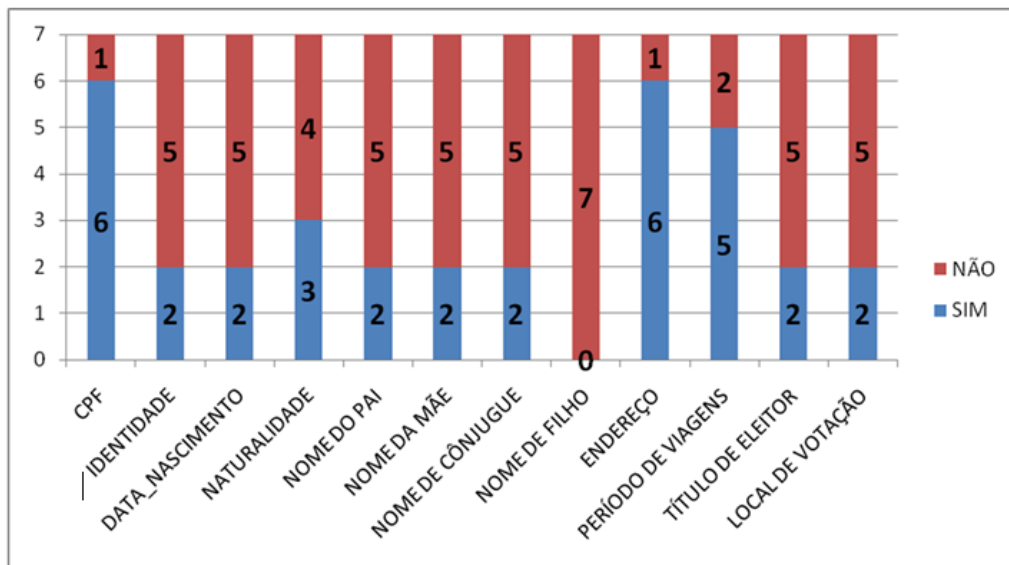
Tabela 4: Resultados da coleta de dados dos agentes de segurança pública federal.

CÓDIGO DO INVESTIGADO	UF	CARGO	CPF	IDENTIDADE	DATA DE NASCIMENTO	NATURALIDADE	NOME DO PAI	NOME DA MÃE	NOME DO CÔNJUGUE	NOME DO FILHO	ENDEREÇO	PERÍODO DE VIAGENS	TÍTULO DE ELEITOR	LOCAL DE VOTAÇÃO
I_08	AC	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_09	AL	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_10	AM	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_11	AP	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_12	BA	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_13	CE	PRF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_14	DF	AGPENF	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
I_15	ES	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_16	GO	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_17	MA	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_18	MG	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_19	MS	AGPENF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_20	MT	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_21	PA	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_22	PB	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_23	PE	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_24	PI	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_25	PR	AGPENF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_26	RJ	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_27	RN	AGPENF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_28	RO	AGPENF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_29	RR	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_30	RS	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
I_31	SC	DPF	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_32	SE	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_33	SP	DPF	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
I_34	TO	PRF	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗

Fonte: O autor.

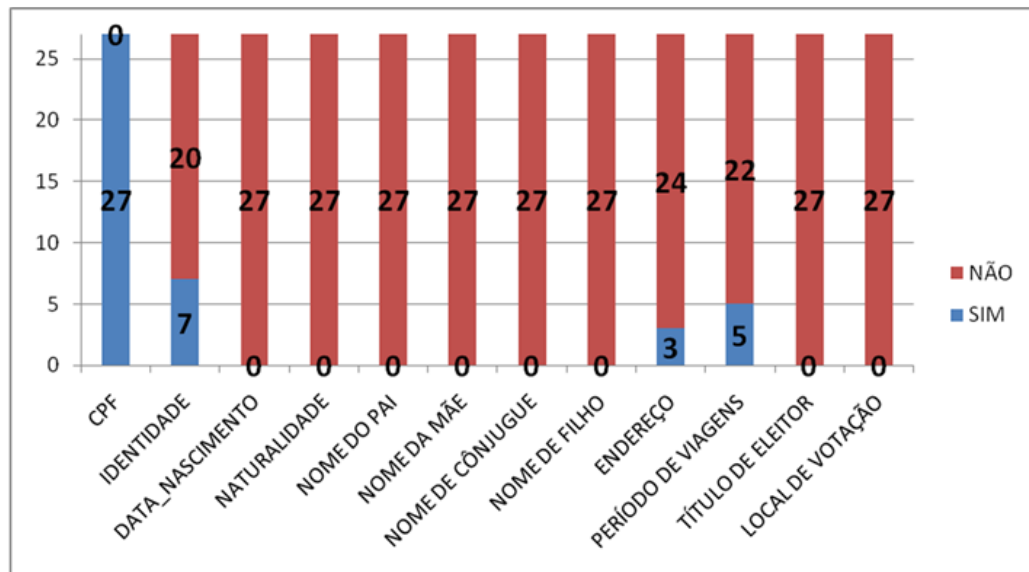
Os Gráficos 2 e 3 apresentam o percentual dos dados coletados dos investigados que atuam na segurança nacional e na segurança pública, respectivamente. Já o Gráfico 4 apresenta o total dos 34 indivíduos investigados.

Gráfico 2: Quantidade de dados coletados dos agentes de segurança nacional.



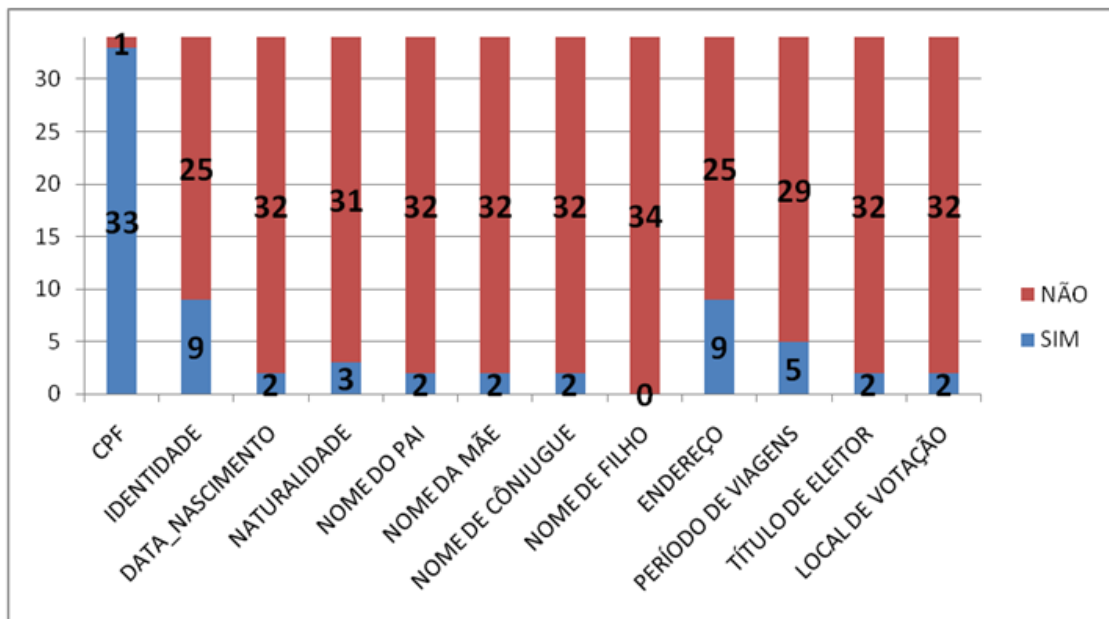
Fonte: O autor.

Gráfico 3: Quantidade de dados coletados dos agentes de segurança pública federal.



Fonte: O autor.

Gráfico 4: Total de dados coletados dos indivíduos.



Fonte: O autor.

4.2 Fatores de risco que impactam a privacidade

A finalidade desta seção é interpretar, descrever e discutir sistematicamente o significado dos dados coletados dos indivíduos investigados e apresentados no item anterior.

Os resultados demonstraram que 33 dos 34 investigados tiveram seus CPF divulgados nos portais da *internet* dos órgãos de governo (Gráfico 4). Isto vem em desencontro com o atual entendimento do STF (2011).

Neste contexto, ressalta-se que não obstante os esforços do governo federal em fortalecer as ações para a proteção de dados pessoais, não foi possível identificar no atual arcabouço jurídico, nem no já citado PL sobre proteção de dados pessoais e da privacidade (BRASIL, 2015), orientações claras e objetivas sobre a divulgação do CPF na *internet*.

Os resultados também apontaram que o indivíduo I_05 é o único indivíduo da Tabela 4 que não teve seu CPF divulgado, como também o único lotado no estado de SP, diferente dos demais que estão lotados no DF. Entretanto, essa observação torna-se irrelevante, visto que foi identificado o CPF do indivíduo I_33, também lotado no estado de SP (Tabela 5).

A Tabela 4 também apresenta uma grande quantidade de dados levantados atinentes aos indivíduos I_01 e I_02 em relação aos demais indivíduos. Possivelmente, os seguintes fatores cooperam para essa ocorrência:

- a) Cumprimento do art. 11 da Lei nº 12.813 de 16 de maio de 2013 que determina os órgãos divulgar, diariamente, por meio da *internet*, a agenda de compromisso das autoridades que ocupam cargo de ministro de Estado, de natureza especial, de presidente, vice-presidente e diretor de autarquias, fundações, empresas públicas ou sociedades de economia mista, como também, do Grupo-Direção e assessoramento, níveis 6 e 5 ou equivalente; e
- b) Publicação da biografia dos ministros de Estado nos portais institucionais.

A publicação de alguns dados na biografia dos Ministros, como por exemplo, filiação e data de nascimento, aparentemente não infere quebra de privacidade e nem quebra da SI, entretanto, foi por meio desses dados que o investigador desta pesquisa obteve informações eleitorais dos indivíduos I_01 e I_02, tais como: número do título de eleitor, zona, seção, local e endereço de votação, exemplificado nas Figuras 18 e 19.

Figura 18: Tela de consulta de Título por nome

The screenshot shows the website of the Tribunal Superior Eleitoral (TSE). The header includes the logo and name of the institution, along with navigation links like 'Mapa do site', 'Página inicial', 'Conteúdo principal', 'Ir para busca', and 'Portal JE'. There are also language options for 'English' and 'Acessibilidades'. The main navigation menu includes 'Institucional', 'Eleitor', 'Eleições', 'Jurisprudência', 'Legislação', 'Partidos', and 'Transparência'. The search bar contains the text 'Pesquisar...'. Below the search bar, there are links for 'Acompanhamento processual e Push', 'Diário da Justiça Eletrônico', 'Inteiro teor de decisões', 'Pesquisa de Jurisprudência', 'Petição eletrônica', and 'Sessões de julgamento'. The main content area is titled 'Eleitor' and contains a sidebar with links such as 'Disque-Eleitor', 'Eleitor no exterior', 'Estatísticas de eleitorado', 'Glossário Eleitoral', 'Mesário', 'Recadastramento biométrico', and 'Serviços'. The main form is titled 'Título e local de votação - consulta por nome' and includes the following fields: 'Nome do eleitor:' (text input), 'Data de nascimento:' (text input with format 'DD/MM/AAAA'), 'Nome da mãe:' (text input with a checkbox for 'não consta/em branco'), and 'Código:' (text input). Below the 'Código:' field is a CAPTCHA image with the letters 'YHPKO' and the instruction 'Por favor, repita os caracteres acima:'. At the bottom of the form is a 'Consultar' button. A small disclaimer at the bottom of the page states: 'Esta informação ajuda o Tribunal Superior Eleitoral a evitar a consulta por programas automáticos, que dificultam a utilização deste aplicativo pelos demais usuários.'

Fonte: TSE, 2015.

Figura 19: Tela com o resultado da consulta de Título por nome



Fonte: Adaptado do TSE, 2015.

Ainda não existe, também, uma decisão jurídica a nível nacional sobre a exposição de dados eleitorais do cidadão na *internet*. Essa questão foi discutida intensamente, no ano de 2013, por ocasião da formalização do acordo de cooperação técnica nº 07/2013¹¹ celebrado entre a Justiça Eleitoral e a *Serasa Experian* para repasse de informações cadastrais de 141 (cento e quarenta e um) milhões de brasileiros para a empresa. Entretanto, por iniciativa da Corregedora-Geral Eleitoral, o citado acordo foi cancelado pelo Procedimento Administrativo nº 29.542/2012-TSE¹² com o fundamento da confiança na Justiça Eleitoral e na inexpugnabilidade dos dados a ela confiados.

Naquela época, o representante da empresa *Serasa Experian* alegou, em nota jornalística, que “todas as informações obtidas por ela, através do convênio, são públicas e de natureza cadastral, podendo ser acessadas no site do TSE”¹³. Em resposta, na mesma nota, o Ministro do STF e também vice-presidente do TSE Marco Aurélio Mello declarou

¹¹ Publicado no D.O.U nº 140 de 23 de julho de 2013 seção 3. Disponível em: <<http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=3&pagina=148&data=23/07/2013>>. Acesso em: 28 de mai de 2015.

¹² Procedimento Administrativo n. 29.542/2012 do Tribunal Superior Eleitoral. Disponível em: <<http://www.justicaeleitoral.jus.br/arquivos/tse-acordo-cooperacao-serasa>>. Acesso em: 28 de mai de 2015.

¹³ Nota do Jornal Nacional publicada em 07/08/2013. Disponível em: <<http://g1.globo.com/jornal-nacional/noticia/2013/08/presidente-do-tse-quer-fim-de-acordo-que-permite-repasse-de-dados-de-eleitores-serasa.html>>

desconhecer essa permissão de consulta ao sítio do TSE, entretanto, os resultados aqui apresentados corroboram a declaração da empresa.

O Gráfico 2 demonstra que foi possível obter o endereço residencial de 6 indivíduos de um total de 7 agentes de segurança nacional investigados, ou seja, quase se aproximou da totalidade dos investigados. Já o Gráfico 3 apresenta uma relação bem inferior referente à detecção dos endereços dos agentes de segurança pública federal, cujo resultado foi de apenas 9 endereços encontrados em um total de 27 investigados. O fator determinístico para obtenção dos endereços residenciais de alguns investigados foi a fragilidade de controle de acesso lógico dos portais das Secretarias de Fazenda de algumas UF por ocasião da prestação de serviços de emissão de certidão negativa de débitos aos cidadãos. Isso explica os resultados do Gráfico 2, visto que a maioria dos seus investigados pertencem ao Distrito Federal e esta UF se encontra vulnerável conforme apresentado no Quadro 12.

Quadro 12: Portais das Secretarias de Fazenda das UF por ordem de fragilidade

ORDEM	UF	JUSITIFICATIVA
1	RS	<ul style="list-style-type: none"> • Apenas com o CPF, fornece o endereço dos indivíduos cadastrados na Secretaria de Fazenda da UF por ocasião da emissão de certidão negativa de débitos. • Associa o CPF solicitado com o nome do indivíduo, mesmo que este não tenha cadastro na Secretaria de Fazenda da UF.
2	AC/AP/DF/TO	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado, divulgando o endereço residencial dos indivíduos cadastrados na Secretaria de Fazenda da UF.
3	SC	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado associado ao nome do indivíduo, mesmo que este não tenha cadastro na Secretaria de Fazenda da UF, permitindo ainda, consultar o histórico das solicitações feitas pelo CPF.
4	MT	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado e associa o nome do indivíduo ao CPF cadastrado na Secretaria de Fazenda da UF.
5	AL/AM/BA/CE/ES/ GO/MA/MS/PA/PE/PR/RJ/ RN/RO/SE/SP	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado e não divulga outros dados.
6	PI	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado, gera um número de solicitação para análise do sistema e não divulga outros dados.
7	PB	<ul style="list-style-type: none"> • Fornece a certidão negativa de débito referente ao CPF solicitado, não divulga outros dados e solicita, também, o número da identidade e órgão expedidor como dados de entrada.
8	MG	<ul style="list-style-type: none"> • Requer instalação de <i>software</i> e cadastro para utilização de serviços de solicitação de certidões.
9	RR	<ul style="list-style-type: none"> • Fornece, apenas, a certidão negativa de débito somente para os cidadãos não cadastrados na Secretaria de Fazenda da UF. O solicitante fornece o CPF e nome e é gerada uma certidão com os dados fornecidos. • Para os indivíduos cadastrados na Secretaria de Fazenda da UF, informa que para a emissão da certidão, é necessário que o solicitante procure uma das agências da Secretaria de Fazenda.

Fonte: O autor.

Diante do atual cenário de insegurança pública e de instabilidade política no Brasil, divulgar endereços é facilitar o acesso de pessoas ou grupos mal intencionados à vida privada do cidadão, que conforme o exposto nessa pesquisa também poderá prejudicar a segurança nacional e a segurança pública.

A tabela 4 apresenta 3 (três) indivíduos que tiveram seus endereços revelados, como também os períodos que estes estiveram ausentes por motivos de viagens. Presume-se que nesses períodos, tanto os familiares, quanto as suas residências ficaram vulneráveis pela ausência desses servidores.

A revelação do endereço, além de oferecer riscos à privacidade e à vida privada do agente público, também pode oferecer riscos à segurança nacional. Como visto, um dos investigados é um dos seguranças da presidência da república. Sendo assim, este servidor à luz da LAI, deverá ter seus dados protegidos, pois estes podem servir como elementos necessários para que um grupo mal intencionado aja contra a vida da presidente da república, como por exemplo, sequestro de familiares seguido de chantagem.

A Tabela 4 apresenta, também, os dados coletados do indivíduo I_04 que atua na ABIN. O CPF e o número da identidade desse indivíduo foram levantados por meio da publicação de um acordo de cooperação técnica firmada entre o TCU e a ABIN.

Para formalização desse acordo, fez-se necessário a assinatura e identificação das autoridades dos órgãos partícipes, em cumprimento ao princípio da publicidade. Entretanto, conforme já apresentado nesta pesquisa, é extenso o arcabouço jurídico que protege as informações que possam comprometer as atividades de inteligência. Nesse caso, inicialmente, foi observado o cumprimento do art. 9º da Lei 9.883/1999, que publicou apenas o extrato do referido acordo de cooperação técnica no DOU¹⁴, entretanto o acordo foi publicado na íntegra no portal do TCU¹⁵. Com isso, de posse CPF do indivíduo I_04, obteve-se o seu endereço residencial no portal da Secretaria de Fazenda do DF, que de acordo com o Quadro 12, encontra-se vulnerável.

Já a divulgação dos endereços levantados e apresentados na Tabela 5, além de comprometer a vida privada dos indivíduos investigados, pode afetar a segurança pública e, conseqüentemente, toda a sociedade. Como por exemplo, a divulgação do endereço residencial de um determinado agente penitenciário federal poderá afetar drasticamente o

¹⁴ Extrato de Cooperação Técnica publicada no DOU nº 217 de 7 de novembro de 2013, seção 3. Disponível em: < <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=3&pagina=212&data=07/11/2013>>. Acesso em: 31 de mai 2015.

¹⁵ Acordo de Cooperação Técnica (Processo TCU nº 028.845/2010-1). Disponível em: < <http://portal3.tcu.gov.br/portal/pls/portal/docs/2607099.PDF>>. Acesso em: 31 de mai 2015.

sistema prisional brasileiro. De posse dessa informação, elementos do crime organizado podem utilizá-la para chantagear um agente a fim de facilitar fugas de presidiários. Uma forma simples de efetuar uma chantagem seria por meio de sequestro de um de seus familiares.

O indivíduo I_14 é um agente penitenciário federal. Em particular, este agente está respondendo por um inquérito do Ministério Público Federal (MPF),¹⁶ pelo crime de tortura de presos. Observou-se que durante a formulação dos autos do inquérito, o Poder Judiciário ocultou os dados do citado agente, considerando-os como sigilosos. No entanto, não houve a devida proteção dos dados do referido agente penitenciário pelo Poder Executivo federal e distrital.

Evidencia-se a falta de coordenação e controle dos dados pessoais que são custodiados pelo governo, em especial os dados sensíveis de pessoas físicas que, pelo desempenho de suas atividades, são considerados de extrema importância para a segurança da sociedade.

Por fim, é importante ressaltar que, de acordo com o Boletim Estatístico do Pessoal do MP (2015), o DF concentra aproximadamente 180.000 (cento e oitenta mil) servidores públicos federais. Somando-se este número com os quantitativos das UF do AC, AP, RS e TO, totalizam-se aproximadamente 271.000 (duzentos e setenta e um mil) servidores. Isso significa que 23% de um total aproximado de 1.200.000 (um milhão e duzentos mil) de servidores podem estar com seus endereços residenciais divulgados nos respectivos portais da Secretaria de Fazenda das UF onde seus órgãos estão localizados.

¹⁶ Inquérito Civil Público nº 1.16.000.006065/2010-23 do Ministério Público Federal. Disponível em: http://www.prdf.mpf.mp.br/imprensa/arquivos_noticias/aia-tortura-papuda3-tarjada.pdf. Acesso em: 31 de maio de 2015.

4.3 Análise e avaliação dos riscos que impactam o Estado e a sociedade

Neste capítulo, realizou-se a análise e avaliação dos riscos nos portais das Secretarias de Fazenda das UF responsáveis pela promoção da transparência aos cidadãos.

Considerou-se como ativo de informação, o conjunto de agentes públicos investigados, bem como os referidos portais das Secretarias de Fazendas das UF.

Por se tratarem de ativos de informação do tipo pessoa, há de se considerar que ainda não existe uma metodologia adequada para valorar o nível de impacto gerado para o agente público como cidadão na sua vida privada, pois constitucionalmente, todos são iguais. Sendo assim, o teor dessa análise remete apenas aos fatores de risco gerados para o Estado e para a sociedade em decorrência da quebra de privacidade dos agentes públicos.

Considerou-se como vulnerabilidade, conforme apresentado no Apêndice B, a inexistência de mecanismos de autenticação e identificação para autenticação de usuários nos portais consultados o que, conseqüentemente, possibilitou a coleta do endereço residencial do investigado.

Utilizou-se o Quadro 12, apresentado anteriormente, para construção dos níveis de probabilidade, conforme demonstra o Quadro 13.

Quadro 13: Níveis de probabilidade

PROBABILIDADE	POSIÇÕES	UF
ALTA	1 / 2 / 3	RS/AC/AP/DF/TO/SC
MÉDIA	4 / 5 / 6	MT/AL/AM/BA/CE/ES/GO/MA/MS/PA/PE/PR/RJ/RN/RO/SE/SP/PI
BAIXA	7 / 8 / 9	PB/ MG/ RR

Fonte: O autor.

O impacto aqui analisado está diretamente relacionado ao cargo e função exercida pelo agente público. Mas considerando que todos os investigados atuam na Segurança Nacional e Segurança Pública, o nível de impacto analisado será “Alto”, conforme apresenta o Quadro 14.

Quadro 14: Análise de impacto

IMPACTO	CARGOS/FUNÇÕES
ALTO	Atividades relacionadas à Segurança Nacional, Segurança Pública, Inteligência Federal.
MÉDIO	Atividades relacionadas à Gestão Orçamentária, Econômica e Financeira.
BAIXO	Atividades Administrativas, Técnicas, Assistencial, de Apoio Gerencial.

Fonte: O autor.

Para qualificar o nível de risco, foi gerada uma matriz de risco da relação impacto *versus* probabilidade (Figura 20), cujo resultado será:

- a) **Alto** – Devem ser tratados imediatamente;
- b) **Médio** – Devem ser tratados em médio prazo ou monitorados constantemente; e
- c) **Baixo** – riscos que poderão ser aceitos ou tratados em longo prazo.

Figura 20: Matriz de risco - impacto *versus* probabilidade

		PROBABILIDADE		
		BAIXA	MÉDIA	ALTA
IMPACTO	ALTO	MÉDIO	MÉDIO	ALTO
	MÉDIO	BAIXO	MÉDIO	MÉDIO
	BAIXO	BAIXO	BAIXO	MÉDIO

Fonte: O autor.

O Quadro 15 apresenta o resultado final da análise dos fatores de risco dos indivíduos investigados nesta pesquisa.

Quadro 15: Resultado da análise e avaliação do risco.

CÓDIGO DO INVESTIGADO	UF	IMPACTO	PROBABILIDADE	RISCO	DESCRIÇÃO
I_01	DF	ALTO	ALTA	ALTO	Devem ser tratados imediatamente
I_02	DF	ALTO	ALTA	ALTO	
I_03	DF	ALTO	ALTA	ALTO	
I_04	DF	ALTO	ALTA	ALTO	
I_05	SP	ALTO	MÉDIA	MÉDIO	Devem ser tratados em médio prazo ou monitorados constantemente
I_06	DF	ALTO	ALTA	ALTO	Devem ser tratados imediatamente
I_07	DF	ALTO	ALTA	ALTO	
I_08	AC	ALTO	ALTA	ALTO	
I_09	AL	ALTO	MÉDIA	MÉDIO	Devem ser tratados em médio prazo ou monitorados constantemente
I_10	AM	ALTO	MÉDIA	MÉDIO	
I_11	AP	ALTO	ALTA	ALTO	Devem ser tratados imediatamente
I_12	BA	ALTO	MÉDIA	MÉDIO	Devem ser tratados em médio prazo ou monitorados constantemente
I_13	CE	ALTO	MÉDIA	MÉDIO	
I_14	DF	ALTO	MÉDIA	MÉDIO	
I_15	ES	ALTO	MÉDIA	MÉDIO	
I_16	GO	ALTO	MÉDIA	MÉDIO	
I_17	MA	ALTO	MÉDIA	MÉDIO	
I_18	MG	ALTO	BAIXA	MÉDIO	
I_19	MS	ALTO	MÉDIA	MÉDIO	
I_20	MT	ALTO	MÉDIA	MÉDIO	
I_21	PA	ALTO	MÉDIA	MÉDIO	
I_22	PB	ALTO	BAIXA	MÉDIO	
I_23	PE	ALTO	MÉDIA	MÉDIO	
I_24	PI	ALTO	MÉDIA	MÉDIO	
I_25	PR	ALTO	MÉDIA	MÉDIO	
I_26	RJ	ALTO	MÉDIA	MÉDIO	
I_27	RN	ALTO	MÉDIA	MÉDIO	
I_28	RO	ALTO	MÉDIA	MÉDIO	
I_29	RR	ALTO	BAIXA	MÉDIO	
I_30	RS	ALTO	ALTA	ALTO	Devem ser tratados imediatamente
I_31	SC	ALTO	ALTA	ALTO	
I_32	SE	ALTO	MÉDIA	MÉDIO	Devem ser tratados em médio prazo ou monitorados constantemente
I_33	SP	ALTO	MÉDIA	MÉDIO	
I_34	TO	ALTO	ALTA	ALTO	Devem ser tratados imediatamente

Fonte: O autor.

Por fim, o Quadro 16 apresenta o resultado do processo de avaliação de riscos.

Quadro 16: Plano de tratamento de risco.

Prioridade	Ativos de Informação	Vulnerabilidades	Ameaças	Riscos	Ação de Segurança da Informação
1	Portal das Secretarias de Fazenda do: AC/AP/DF/RS/TO	- Inexistência de mecanismos de autenticação e identificação de usuários. - Serviços desnecessários que permanecem habilitados.	<ul style="list-style-type: none"> ● Criminoso digital ● Crime organizado ● Espionagem Política, comercial e empresarial ● Governos estrangeiros ● Manifestantes ● Terrorismo 	<ul style="list-style-type: none"> ● Suborno por informação ● Spoofing (fazer-se passar por outro) ● Vazamento de informações ● Uso ilegal de informações ● Chantagem ● Sequestro ● Roubo e Fraude ● Venda de informações pessoais ● Acesso não autorizado ao sistema ● Vandalismos ● Destruição de equipamentos ● Agressão física ● Ataque terrorista ● Atentado contra a vida 	<p>a) GSIPR (Órgão responsável pela Segurança da Informação):</p> <ul style="list-style-type: none"> - Notificar o governo da UF responsável pelo portal <p>b) Órgão de controle da jurisdição do portal:</p> <ul style="list-style-type: none"> - Auditar o Portal. <p>c) Responsável pelo portal:</p> <ul style="list-style-type: none"> - instalar mecanismos de controle de acesso, como autenticação, autorização e identificação de usuários. - remover serviços desnecessários, como cadastro de CPF não vinculados ao órgão.
2	Portal da Secretaria de Fazenda de SC	- Serviços desnecessários que permanecem habilitados.		<ul style="list-style-type: none"> ● Uso ilegal de informações 	<p>a) Responsável pelo portal:</p> <ul style="list-style-type: none"> - remover serviços desnecessários, como cadastro de CPF não vinculados ao órgão.
3	Portal das Secretarias de Fazenda do: AL/AM/BA/CE/ES/GO/MA/MG/MS/MT/PA/PB/PE/PI/PR/RJ/RN/RO/RR/SE/SP	- desconhecidas		<ul style="list-style-type: none"> - não identificado 	<p>a) Responsável pelo portal:</p> <ul style="list-style-type: none"> - Manter o monitoramento do Portal

Fonte: O autor.

4.4 Análise dos resultados do questionário

Esta seção apresenta as análises e discussões dos resultados obtidos do questionário enviados aos membros do CGSI. As análises foram realizadas com base nas respostas dos informantes que serviram para validar as discussões e o posicionamento do investigador desta pesquisa.

É importante ressaltar que o questionário foi enviado para um pequeno grupo de respondentes. Entretanto, todos os indivíduos participantes têm um vínculo significativo com o problema investigado, e com isso, pressupõe-se que as respostas coletadas desses indivíduos são mais relevantes para a validação desta pesquisa qualitativa. Além disso, nota-se que existe uma relação de comunidade entre o pesquisador e os indivíduos do CGSI que vivenciam a realidade do tema investigado (MINAYO, 2001, p.65).

Dos 17 (dezesete) órgãos componentes do CGSI, apenas 1 (um) deixou de responder o questionário enviado, por motivo de troca dos representantes titular e suplente e a não substituição desses pela autoridade responsável do órgão.

O questionário conforme apresentado no anexo foi constituído por 8 (oito) perguntas, sendo 5 (cinco) do tipo dicotômica, com respostas de “sim” ou “não” e 3 (três) perguntas encadeadas da pergunta anterior, caso esta seja respondido “sim”.

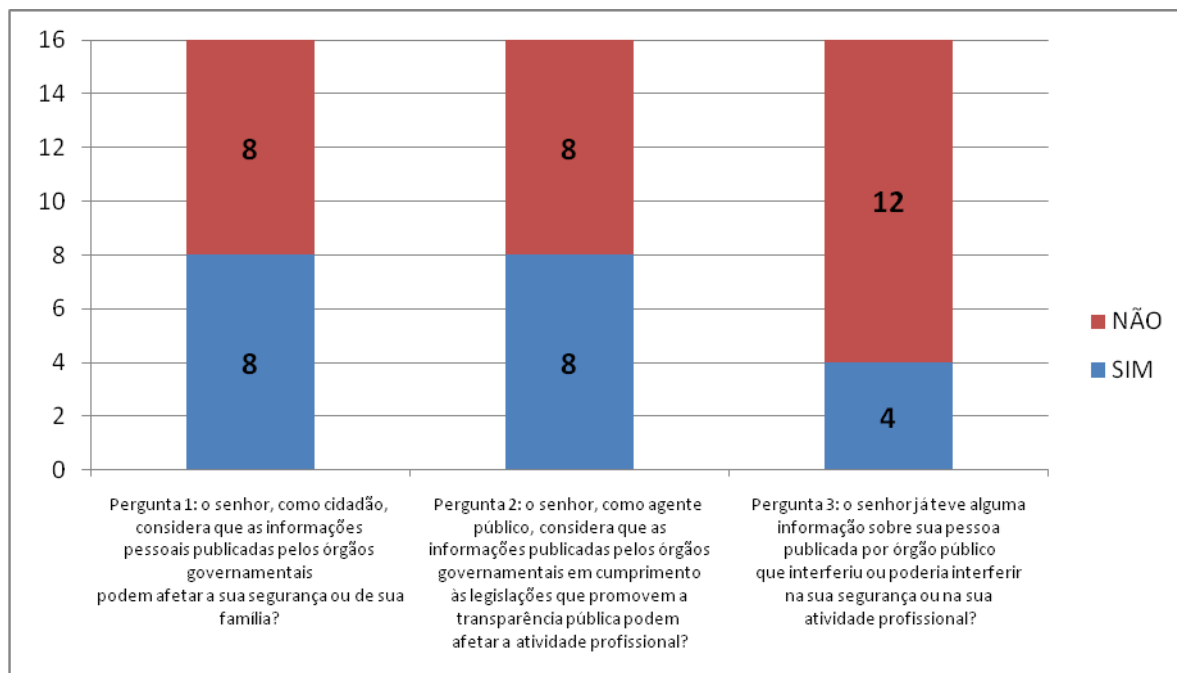
Quando perguntado se o informante, na condição de cidadão, considera que as suas informações pessoais publicadas pelos órgãos de governo podem afetar a sua segurança ou de sua família (pergunta 1), 8 (oito) dos 16 (dezesesseis) responderam que “sim”.

Quando perguntado aos informantes, que dessa vez na situação de agente público, se as mesmas informações publicadas podem afetar suas atividades profissionais, também 8 (oito) dos 16 (dezesesseis) responderam que “sim”.

No entanto, quando perguntado aos informantes se eles já tiveram alguma informação publicada por órgão público que tenha interferido ou que poderia interferir na sua segurança ou na sua atividade profissional (pergunta 3), apenas 4 (quatro) responderam que “sim”.

Os resultados das 3 (três) primeiras perguntas são apresentados no Gráfico 5.

Gráfico 5: Resultados das perguntas 1, 2 e 3 do questionário.



Fonte: O autor.

Os resultados referentes às perguntas 1 e 2 (Gráfico 5) demonstraram que há uma divisão de opiniões dos representantes do CGSI. Essas respostas indicam que apesar dos informantes possuírem maior consciência e cultura de segurança, existem aqueles que desconhecem os riscos afetos à divulgação de dados pessoais.

Em continuação à pergunta 3, foi perguntado aos 4 (quatro) informantes que já tiveram informações pessoais divulgadas, “quais informações que poderiam interferir ou interferiram em sua segurança pessoal ou profissional?”. O resultado da pergunta 4 é apresentado no Quadro 17.

Quadro 17: Informações publicadas dos membros do CGSI.

Dados e informações	Quantidade de informantes
CPF	3
Carteira de identidade	2
Remuneração	3
Viagens	3
Ocupação de imóvel funcional	1
Órgão de lotação	1
Participação em Grupos de Trabalho para tratar de assuntos sensíveis	1

Fonte: O autor.

Nenhum dos investigados relatou que seus endereços foram disponibilizados, entretanto, houve 3 (três) indivíduos que demonstraram preocupações relacionadas à divulgação de períodos de viagens. Inclusive, um dos investigados comentou sobre o perigo da divulgação do período de afastamento do agente público no DOU, pois de acordo com esse respondente, essa informação é “um presente para um ladrão visitar a sua residência”. Observa-se que este depoimento vai ao encontro às discussões já apresentadas, principalmente, a relação entre endereço divulgado com informações sobre viagens.

Ademais, um dos informantes alertou que o valor da remuneração pode ser insumo de grande importância para empresas de financiamento e empréstimos. Associada a essa resposta observa-se que esta pesquisa incluiu em sua amostragem, indivíduos que atuam em áreas que despertam interesses de grandes organizações nacionais e internacionais, inclusive no setor nuclear. Sendo assim, informações sobre remuneração desses indivíduos, também podem ser insumo para a prática de crimes de subornos ou de corrupção ativa, que consiste em “oferecer ou prometer vantagem indevida a funcionário público, para determiná-lo a praticar, omitir ou retardar ato de ofício” (BRASIL, 1940).

Quando perguntado se os membros do CGSI visualizavam algum tipo de norma ou orientação que possa fortalecer a SI dos agentes públicos (pergunta 5), 7 (sete) dos informantes responderam que “sim”. Sendo que 5 (cinco) desses relataram a necessidade de uma Lei ou normativo que venha distinguir dados pessoais de dados funcionais.

Segundo um dos informantes: “não há motivos para que os órgãos publiquem o CPF no DOU, uma vez que todos servidores públicos podem ser identificados pelo número do SIAPE¹⁷ ou por outros identificadores funcionais”. Nota-se que uma vez adotada essa sugestão, o investigado desta pesquisa teria dificuldades nas coletas de endereços em portais vulneráveis que exigiam apenas o CPF como dado de entrada.

Por fim, foi perguntado se os membros do CGSI visualizavam outros cargos públicos, cujos dados poderiam ser protegidos por Lei, nos mesmos moldes que as informações dos agentes da ABIN são protegidas (pergunta 7). Como resultado, 7 (sete) dos informantes responderam que “sim” e quando questionado quais seriam tais cargos (pergunta 8), foram obtidas várias respostas que foram agrupadas por atividades, conforme apresentado no Quadro 18.

¹⁷ O Sistema Integrado de Administração de Recursos Humanos (Siape) é um sistema de abrangência nacional criado com a missão de integrar todas as plataformas de gestão da folha de pessoal dos servidores públicos.

Quadro 18: Cargos públicos cujos dados dos ocupantes deveriam ser protegidos.

Cargos públicos	Quantidade de informantes
Atividades policiais	6
Militares	1
Atividades de auditorias e fiscalizações	4
Pesquisadores	1
Todos os cargos	3

Fonte: O autor.

Em relação aos cargos apontados pelos respondentes, 4 (quatro) indivíduos responderam que cargos relacionados às atividades de auditoria e fiscalização, que não foi objeto de investigação nesta pesquisa, deveriam ter seus dados protegidos por força de Lei. Nesse caso, um dos respondentes deu exemplo de um recente caso que ganhou notícia no país referente ao assassinato de 3 (três) auditores-fiscais do trabalho em decorrência de suas atividades funcionais.

Seis informantes relataram que os ocupantes de cargos relacionados às atividades policiais devem ter seus dados protegidos. Essa informação reforça a necessidade de proteção dos dados dos agentes públicos federais que atuam na segurança pública e foram objetos de investigação nesta pesquisa.

Apenas um dos respondentes considerou que os dados dos pesquisadores deveriam ser protegidos em virtude do conhecimento gerado e armazenado por esses agentes que despertam interesses internacionais.

Por fim, três dos respondentes consideraram que todos os agentes públicos deveriam ter seus dados pessoais resguardados por Lei, entretanto, não houve declarações que justificassem essa consideração.

4.5 Discussões finais

Demonstrou-se nesta pesquisa que o governo brasileiro vem ampliando a participação da sociedade no debate sobre os atos praticados na esfera pública por meio da publicidade e da transparência.

Porém, os resultados aqui obtidos vão ao encontro da pesquisa de Soares (2014), especificamente em relação à atual facilidade de acesso aos dados governamentais. Observou-se que por meio da publicidade de dados e informações de agentes públicos foi possível identificar implicações nos aspectos de SI.

O uso indevido dos dados coletados dos agentes públicos que atuam na segurança nacional e segurança pública federal já são suficientes para pôr em risco o Estado e a sociedade. Sendo assim, tais informações requerem ações de classificações em grau de sigilo ou restrições de acesso.

No contexto da comunicação organizacional nos aspectos relativos à transparência pública, foi possível identificar uma relação entre o modelo de comunicação de Lasswell apresentado por Mcquail e Windhall (1993) e as Leis Complementares que estabelecem normas de finanças públicas voltadas para a responsabilidade na gestão fiscal (BRASIL, 2000b, 2009), conforme demonstrado no Quadro 19:

Quadro 19: Relação entre o modelo de comunicação de LASSWELL com as LC nº 101/2000 e nº 131/2009.

Quem?	Diz o quê?	Em que canal?	Para quem?	Com que efeito?
ÓRGÃOS DA APF	<u>Gestão fiscal:</u> - planos - orçamentos - diretrizes orçamentárias - prestações de contas - Relatórios <u>Despesas:</u> - número do processo - bem fornecido - serviço prestado - procedimento licitatório realizado <u>Receitas:</u> - lançamento e recebimento das unidades gestoras - recursos extraordinários.	<i>Internet</i>	Sociedade (pessoa física ou jurídica)	- Incentivar a participação popular e realização de audiências públicas, durante os processos de elaboração e discussão dos planos, lei de diretrizes orçamentárias e orçamentos. - Dar conhecimento e acompanhamento à sociedade, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira. - Oferecer denúncia ao TCU e ao órgão Ministério Público da União o descumprimento das prescrições estabelecidas pela Lei.

Quanto aos resultados obtidos durante a fase de coleta de dados, observou-se que alguns dados estão associados a assuntos que podem prejudicar ou causar risco: à segurança da população, aos planos das FFAA, às instalações de interesse estratégico nacional, à segurança de altas autoridades nacionais e às atividades de inteligência (BRASIL, 2011). Sendo assim, em cumprimento do contido na LAI, deveriam ser classificados em graus de sigilo ou terem seu acesso restrito.

Constataram-se diversos aspectos divergentes sobre os assuntos relativos a dados e informações pessoais. A LAI define que informação pessoal é “aquela relacionada à pessoa natural identificada ou identificável” (BRASIL, 2011). Já o PL que dispõe sobre tratamento de dados pessoais define dado pessoal como aquele “relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos” (BRASIL, 2015). Independente da definição dada, quer seja para dado ou informação, sabe-se que a divulgação desses dados ou informações pode constituir uma conduta ilícita. Isto porque as informações pessoais devem ter seu acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos a contar da sua data de produção (BRASIL, 2011).

Há que se observar, também, que foi possível levantar diversos dados dos agentes públicos investigados que, de acordo com as definições apresentadas, são considerados dados ou informações pessoais, como por exemplo, o CPF (BRASIL, 2011, 2015; DPA, 1989).

Em sentido oposto, o ato de divulgar o CPF de agentes públicos constitui-se como meta da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), coordenada pela Secretaria Nacional de Justiça, do Ministério da Justiça:

Recomenda aos entes de todos os poderes e de todas as esferas de governo que incluam em seus procedimentos de nomeação e publicação nos Diários Oficiais o número do CPF das pessoas nomeadas ou exoneradas de cargos públicos e funções de confiança, respeitadas as exceções previstas em lei, visando à elaboração de lista de pessoas expostas politicamente, bem como viabilizar a implementação de rotinas de controle (BRASIL, 2012d).

Novamente, evidenciam-se pensamentos e políticas contraditórias no âmbito governamental, especificamente no tratamento de dados e informações pessoais dos agentes públicos. A título de exemplo, o Brasil (2012d) é favorável à transparência do CPF do agente público, já o STF (2011) proíbe a divulgação do CPF com a finalidade de atenuar os impactos decorrentes da divulgação de outras informações do servidor público.

Observou-se também que a promoção da transparência pública pode levar o governo a fazer distinção entre as pessoas físicas de caráter público e as de caráter privado. Sendo que

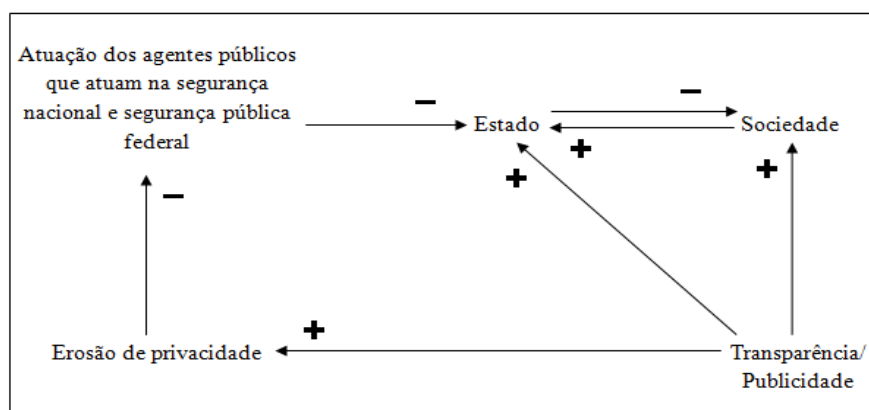
isso contraria o art. 5º da CRFB, haja vista que todos são iguais perante a lei e que não pode haver distinção quanto à natureza do indivíduo (BRASIL, 1988).

Por outro lado, nota-se que a Lei que dispõe sobre a Política Nacional de Informática está alinhada com a Carta Magna, pois ela determina que é dever do Estado estabelecer “mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas” (BRASIL, 1984).

Os resultados também apontaram que é possível coletar dados pessoais, por meio da metodologia apresentada, de diversos agentes públicos de qualquer nível, área, cargo ou função, quer sejam da área operacional quer sejam da área estratégica, tal qual explica Beck (1998) ao afirmar que não há mais fronteiras que diferenciam os membros da atual sociedade do risco.

Salienta-se ainda que, baseado na fundamentação teórica e nos resultados desta pesquisa, foi possível identificar as relações existentes entre os principais elementos apresentados neste estudo. Sabe-se que os princípios da transparência e da publicidade aumentam a participação da sociedade na tomada de decisões dos atos praticados pelo governo (DELLAZZANA, 2009; OLIVEIRA, 2010) que conseqüentemente consolida o país como um Estado democrático. No entanto, por ocasião do cumprimento de tais princípios, caso não sejam tomadas as devidas cautelas e precauções de SI, aumenta-se a probabilidade de erosão de privacidade. Isso provavelmente prejudicará a atuação dos agentes públicos que atuam na segurança nacional e na segurança pública federal, fazendo com que não haja qualidade dos serviços prestados pelo Estado à sociedade. Visando prover uma melhor compreensão dessa abordagem, a Figura 21 ilustra o mapa sistêmico do processo descrito por meio da extração de elementos da realidade do processo apresentado e suas interligações.

Figura 21: Mapa sistêmico da relação Transparência e privacidade.



Fonte: O autor.

Por fim, notou-se que muito se tem discutido sobre os aspectos relativos à erosão de privacidade nos aspectos que impactam a vida privada do indivíduo. Sobre esse viés, foram identificados diversos estudos. No entanto, não foi possível identificar pesquisas que associam os impactos gerados ao Estado e à sociedade em decorrência da quebra da privacidade.

5 CONCLUSÕES E SUGESTÕES

Neste capítulo são apresentadas as conclusões da pesquisa, que se coadunam com os resultados e discussões da coleta de dados apresentados no capítulo anterior e em seguida são apresentadas algumas recomendações consideradas fundamentais para a elaboração de estudos futuros neste tema.

5.1 Conclusões do estudo

Esta pesquisa demonstrou por meio de uma análise dos dados publicados na *internet* referentes aos agentes públicos da APF que atuam na segurança nacional e na segurança pública que há evidências que comprovam a quebra da segurança da informação, o que compromete a privacidade de tais agentes e a segurança do Estado e da sociedade. Neste sentido, ao optar pela realização de uma pesquisa documental, este estudo obteve dados concretos acerca dos riscos que os indivíduos investigados e, também, o Estado estão expostos, frente às diversas ameaças do mundo real e virtual.

Dessa forma, os resultados respondem as questões levantadas no percurso do estudo, evidenciando o cumprimento de seus objetivos específicos de (1) identificar as informações comunicadas por sistemas de promoção da transparência pública, de natureza pessoal dos agentes públicos que atuam na segurança nacional e segurança pública federal, (2) identificar os fatores de risco que impactam a privacidade dos agentes públicos que atuam na segurança nacional e segurança pública federal e (3) analisar os riscos que impactam o Estado e a sociedade no contexto da transparência.

Para tal, foi realizada uma revisão de literatura que apresentou os aspectos relevantes da gestão da informação para a segurança da informação, assim como os direitos e garantias fundamentais que permeiam o acesso à informação para o cidadão, e por fim, os principais conceitos na área de segurança da informação.

A partir dos dados levantados durante a investigação, foi possível identificar respostas que reforçam alguns argumentos descritos no decorrer do estudo. Conforme apresentado na introdução, comprovou-se a necessidade de unificação das formas de tratamento da informação pública. Os resultados apontaram que os órgãos dos diferentes Poderes e esferas divulgam informações pessoais dos agentes públicos de forma diferenciada, com isso, aspectos de segurança ora são cumpridos por um, ora não são por outros.

O método apresentado para coleta de dados pessoais dos agentes públicos revelou a facilidade de obtenção de dados pessoais por qualquer pessoa sem o apoio de ferramentas automatizadas. Embora não tenha sido o cerne desta pesquisa, observou-se que alguns dados não encontrados referentes aos agentes públicos estavam disponíveis na *internet* em portais não governamentais, o que demonstra ser o problema bem maior do que aqui apresentado.

Os resultados da coleta de dados também apontaram que não existe uma política pública que estabelece regras claras e objetivas sobre a publicação de dados pessoais nos portais de transparência das UF. Nesse sentido, urge a necessidade de uma Lei específica que estabeleça um sistema único de transparência para todo o Estado brasileiro e um órgão central com as atribuições de supervisionar tal sistema.

Atualmente, existe no âmbito da APF um sistema de controle interno e de correição, supervisionado pela CGU, com a finalidade de prestar orientações técnicas por meio de normativos, entretanto, esse sistema não atende as necessidades apresentadas no estudo, visto que, o sistema existente destina-se apenas às unidades de ouvidoria do Poder Executivo Federal.

Ademais, pode-se concluir que a APF ainda se encontra em fase de consolidação frente às profundas exigências emanadas dos princípios da publicidade e transparência, bem como às imposições feitas pela LAI. Logo, por meio das análises e discussões aqui realizadas, é possível identificar os principais pontos vulneráveis e que merecem especiais atenções para o fortalecimento da SI, a fim de evitar ou mitigar impactos negativos para o agente público e para o Estado e sociedade.

Observa-se também, que os resultados obtidos no questionário vieram ao encontro de vários aspectos apontados pelo pesquisador neste estudo. Com isso, conclui-se que há um consenso significativo voltado à proteção dos dados pessoais dos agentes investigados, mesmo que a natureza destes seja de caráter público.

Quanto ao método utilizado para a coleta de dados dos indivíduos, apesar de sua simplicidade, ele demonstrou que é possível sistematizar, com o uso de recursos especializados e automáticos, a produção de conhecimento afetos às atividades de inteligência e contra-inteligência. Sendo assim, torna-se importante trazer o debate sobre os temas transparência e privacidade para o campo da CI.

A pesquisa também apresenta a importância da inserção do método de análise e avaliação de riscos como ferramenta para apoiar as questões relativas às ações governamentais voltadas à aplicação dos princípios legais da publicidade e transparência, visto a abrangência e as exigências imprimidas pela LAI aos órgãos da administração pública.

Por fim, é possível concluir que o presente estudo apresenta resultados preocupantes que demonstram a fragilidade do Estado brasileiro com a publicação de dados pessoais dos seus agentes públicos. Por outro lado, esses resultados podem servir de alerta às autoridades e órgãos de controle e de transparência pública sobre uma visão ainda não pesquisada. Atualmente, as discussões sobre os impactos das publicações de dados pessoais são direcionadas apenas à quebra da privacidade, diferente do que apresentado nesta pesquisa que, além deste impacto, acrescentou os riscos decorrentes dessas divulgações à segurança do Estado e da Sociedade.

5.2 Sugestões para trabalhos futuros

Observou-se nesta pesquisa a necessidade de novos estudos que aprofundassem o tema por meio de pesquisas exploratórias e quantitativas, com o intuito de analisar a atual situação dos portais que promovem a transparência pública com critérios de avaliações mais elaborados visando medir o nível de maturidade desses canais nos aspectos relacionados à SI.

Outras pesquisas podem ser direcionadas focando, também, outros setores cuja publicação dos dados de seus agentes possam impactar drasticamente o Estado, como por exemplo, os setores financeiro, de infraestrutura, de pesquisa e desenvolvimento.

Pesquisas futuras também podem ser direcionadas abrangendo outros debates e aspectos da segurança da informação, que não somente aqueles relativos ao tratamento de dados pessoais, como também aqueles referentes aos bens materiais que são adquiridos e divulgados na *internet*, ou então, aqueles referentes à publicação de vulnerabilidades e fragilidades dos órgãos governamentais na *internet* pelos órgãos de controles.

Salienta-se também, investigar a possibilidade da construção de bases de conhecimentos por meio de coleta de dados abertos e disponibilizados pela administração pública por órgãos não governamentais. Nesses termos, inclui-se a possibilidade de efetivação do processo de inteligência competitiva nas empresas privadas, como também, a construção de banco de dados contendo informações sensíveis de interesses para as ameaças.

Recomenda-se, por fim, a continuidade desta pesquisa no âmbito da CI, em razão da necessidade de elaboração de uma proposta de política nacional de transparência pública para o Estado brasileiro, considerando-se que pesquisas precisam ser feitas dentro da temática da

SI abrangendo múltiplas tendências de análise, para construção ou adaptação de um novo modelo de comunicação entre a administração pública e o público externo na aplicação do princípio da publicidade e transparência pública.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 16167**: Diretrizes para classificação, rotulação e tratamento da informação. Rio de Janeiro, 2013a.

_____. **NBR ISO/IEC 27002**. Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. 2013b.

_____. **NBR ISO/IEC 27005**. Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de segurança da Informação. 2011.

_____. **NBR ISO/IEC 31010**. Gestão de Riscos – Técnicas para o processo de avaliação de riscos. 2012.

ALARCON, Orestes Estevam; FACHIN, Gleisy Regina Bóries; TRISTÃO, Ana Maria Delazari. **Sistema de classificação facetada e tesauros: instrumentos para organização do conhecimento**. Ci. Inf., Brasília, v. 33, n. 2, p. 161-171, maio/ago. 2004.

ANDRADE, Rogério P. de. **A construção do conceito de incerteza: uma comparação das contribuições de Knight, Keynes, Shackle e Davidson**. Nova Economia. Belo Horizonte, 21 (2) , p. 171-195, maio/agosto. 2011.

ARAUJO, C. A. A. **Ciência da Informação como campo integrador para as áreas de Biblioteconomia, Arquivologia e Museologia**. Informação & informação, v. 15,n.1, p. 173-189, 2010.

ARQUIVO NACIONAL (Brasil). Conselho Nacional de Arquivos. **Classificação, temporalidade e destinação de documentos de arquivo; relativos às atividades-meio da administração pública/Arquivo Nacional**. Rio de Janeiro: Arquivo Nacional, 2001. Disponível em: < http://www.conarq.arquivonacional.gov.br/media/publicacoes/cdigo_de_classificacao.pdf>. Acesso: em 04 dez 2014.

_____. **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. Disponível em: < http://www.conarq.arquivonacional.gov.br/Media/publicacoes/dicionrio_de_terminologia_arquivstica.pdf>. Acesso: em 04 dez 2014.

ATZ, Ana Paula. **A dimensão da informação no contexto dos novos Direitos (ambiental e consumidor) a partir da observação do risco das novas tecnologias**. Dissertação (mestrado). Universidade do Vale do Rio dos Sinos – Unisinos. Programa de Pós-Graduação em Direito, São Leopoldo, RS, 2011.

Disponível em: <<http://biblioteca.asav.org.br/vinculos/tede/AnaPaulaAtz.pdf>>. Acesso: em 12 out 2014.

AUDARD, Catherine. **Processos e limites da Democracia deliberativa: Habermas, Arendt e Hawl. In: Cidadania e democracia deliberativa.** Porto Alegre. EDIPUCRS, 2006.

BAIN, Read. *Technology and state government.* *American Sociological Review*, 1937.

BARRETO, A. A. **A condição da informação.** Perspectiva, São Paulo, v. 16, n.3, 2002.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2005.

BECK, Ulrich. **A sociedade do risco.** Barcelona: Paidós, 1998.

BELKIN, N. J. **Information concepts for information science.** *Journal of Documentation*, London, v. 34, n.1, p. 55-85, Mar. 1978.

BELKIN, N. J; ROBERTSON, S.E. **Information science and the phenomenon of information.** *Journal of the American Society for Information Science*, Jasis, 1976.

BERLO, David. **O processo de comunicação: introdução à teoria e à prática.** São Paulo: Martins Fontes, 2003.

BEZERRA, Midinai Gomes; NASCIMENTO, Bruna Laís Campos do; NORONHA, Walkene Wytiza Freire e Medeiros; SOUSA, Maria Gersomara de Carvalho; LIMA, Vanusia Edna Leite de. **Trajetória histórica da classificação: mudança do status de arte para ciência.** XXV Congresso Brasileiro de Biblioteconomia, Documentação e Ciência da Informação – Florianópolis, SC, 2013.

BORKO, H. *Information Science: What is it?* *American Documentation*, v.19, n.1, p.3-5, Jan. 1968. (Tradução Livre)

BRAMBILLA, Sônia Domingues santos; LAIPELT, Rita do Carmo Ferreira; CAREGNATO, Sônia Elisa; STUMP, Ida Regina C. **Interfaces entre os campos da Comunicação e da Informação.** VII ENANCIB – Encontro Nacional de Pesquisa em Ciência da Informação, São Paulo. 2007.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF. 1988.

Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 23 dez. 2014.

_____. Decreto nº 27.583, de 14 de dezembro de 1949. **Aprova o Regulamento para a Salvaguardas das Informações que interessam à Segurança Nacional.** Rio de Janeiro, DF. 1949.

Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/D27583.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto nº 3.505, de 13 de junho de 2000. **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.** Brasília, DF. 2000a.

Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto nº 4.520, de 16 de dezembro de 2002. **Dispõe sobre a publicação do Diário Oficial da União e do Diário da Justiça pela Imprensa Nacional da Casa Civil da Presidência da República, e dá outras providências.** Brasília, DF. 2002a.

Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4520.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto nº 4.553, de 27 de dezembro de 2002. **Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.** Brasília, DF. 2002b.

Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4553.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto nº 7.724, de 16 de maio de 2012. **Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.** Brasília, DF. 2012a.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7724.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto nº 7.845, de 14 de novembro de 2012. **Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.** Brasília, DF. 2012b.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>. Acesso em: 23 de dez. 2014.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Brasília, DF. 1940.

Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 4.320, de 17 de março de 1964. **Estatui Normas Gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal.** Brasília, DF. 1964.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4320.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 7.170, de 14 de dezembro de 1983. **Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências.** Brasília, DF. 1983.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/17232.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 7.232, de 29 de outubro de 1984. **Dispõe sobre a Política Nacional de Informática, e dá outras providências.** Brasília, DF. 1984.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/17232.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 8.159, de 8 de janeiro de 1991. **Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.** Brasília, DF. 1991.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.** Brasília, DF. 1999.

Disponível em: <http://www.planalto.gov.br/CCiVil_03/Leis/L9883.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 10.683, de 28 de maio de 2003. **Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.** Brasília, DF. 2003.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 12.527, de 18 de novembro de 2011. **Regula o acesso a informações.** Brasília, DF. 2011.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 12.598, de 21 de março de 2012. **Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa; dispõe sobre regras de incentivo à área estratégica de defesa; altera a Lei no 12.249, de 11 de junho de 2010; e dá outras providências.** Brasília, DF. 2012c.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12598.htm>. Acesso em: 23 de dez. 2014.

_____. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília, DF. 2014.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 23 de dez. 2014.

_____. Lei Complementar nº 101, de 4 de maio de 2000. **Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências.** Brasília, DF. 2000b.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm>. Acesso em: 23 de dez. 2014.

_____. Lei Complementar nº 131, de 27 de maio de 2009. **Acrescenta dispositivos à Lei Complementar nº 101, de 4 de maio de 2000, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências, a fim de determinar a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios.** Brasília, DF. 2009.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp131.htm>. Acesso em: 23 de dez. 2014.

_____. Portaria Interministerial nº 140, de 16 de março de 2006. **Disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores- internet, e dá outras providências.** Controladoria-Geral da União e Ministério do Planejamento, Orçamento e Gestão. Brasília, DF. 2006.

Disponível em: <http://www.comprasnet.gov.br/legislacao/portarias/p140_06.htm>. Acesso em: 23 de dez. 2014.

_____. Projeto de Lei. **Dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências.** 2015.

Disponível em: <<http://www.acessoainformacao.gov.br/menu-de-apoio/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf>>. Acesso em: 20 de jan. 2015.

_____. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Enccla : Estratégia nacional de combate à corrupção e à lavagem de dinheiro : 10 anos de organização do estado brasileiro contra o crime organizado** / Secretaria Nacional de Justiça, Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI). – Ed. comemorativa – Brasília: Ministério da Justiça, 2012d.

Disponível em: <<http://www.justica.gov.br/sua-protecao/cooperacao-internacional/arquivos/enccla-10-anos.pdf>>. Acesso em: 08 jun. 2014.

BUCKLAND, M. K. *Information as thing. Journal of American Society for Information Science.* n. 42,v.5, p. 351-360, 1991.

BUSH, Vannevar. *As We May Think.* The Atlantic Monthly, Julho, 1945.

Disponível em: <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/?single_page=true> Acesso em : 08 jun. 2012.

CAPURRO, Rafael; HJØRLAND Birger. **O conceito de informação. Perspectivas em Ciência da Informação**, v. 12, n. 1, p. 148-207, jan./abr. 2007.

CASTELLS, Manuel. **A sociedade em rede**. Tradução: Roneide Venancio Majer. Atualização para 6ª edição: Jussara Simões. São Paulo: Paz e Terra, 1999.

_____. **A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Tradução: Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed. 2003.

CERVO Amado I.; BERVIAN, Pedro A. **Metodologia científica: para uso dos estudantes universitários**. 3ª ed. São Paulo: McGraw-Hill do Brasil, 1983.

CHIAVENATO, Idalberto. **Recursos Humanos: O Capital humano das organizações**. 8ed. 4 impressão. São Paulo. Atlas, 2008.

CIA, Conselho Internacional de Arquivos. **Documentos de Arquivo Electrónicos: Manual para Arquivistas (ICA Estudo nº 16)**. Publicado inicialmente em inglês como "*Electronic Records: a Workbook for Archivists*" pelo Comité de Arquivos Correntes em Ambiente Electrónico (2000-2004) do Conselho Internacional de Arquivos, 2005. Disponível em: <<http://www.ica.org/download.php?id=1616>>. Acesso em: 23 de dez. 2014.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: Martins Fontes, 1996.

COOPER, D. R.; SCHINDLER, P. S. **Métodos de pesquisa em administração**, 7ª ed. Porto Alegre: Bookman, 2003.

CRUZ MUNDET, José Ramón. **A gestão de documentos nas organizações**. Madrid: Ed. Pirâmide, 2006.

DAHLBERG, Ingetraut. **Teoria da Classificação, ontem e hoje**. Tradução Henry B. Cox. In: Conferência Brasileira de Classificação Bibliográfica, 1972, v.1. p. 352-370. Rio de Janeiro. Anais Brasília: IBICT/ABDF, 1979.

Disponível em: <http://www.conexaorio.com/bit/dahlbergteoria/index_teoriam.htm>. Acesso em: 02 de dez. 2014.

DAVENPORT, Thomas H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação**. Tradução Bernadette Siqueira Abrão. São Paulo: Futura, 1998.

DELLAZZANA, Angela Lovato. **Publicidade e democracia: regulamentação versus censura**. Centro Universitário Franciscano – UNIFRA, Santa Maria, 2009.

DPA. *DATA PROTECTION ACT. Personal data. United Kingdom of Great Britain and Northern Ireland*, 1998.

Disponível em: < http://legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf>. Acesso em: 12 jun. 2015.

EASTWOOD, T. *Jenkinson's writings on some enduring archival themes. American Archivist* . n. 67 , spring/summer, p.31-44, 2004.

FERNANDES, Jorge Henrique Cabral. **Segurança da Informação: nova disciplina na Ciência da Informação?** XI ENANCIB – Encontro Nacional de Pesquisa em Ciência da Informação - Inovação e inclusão social: questões contemporâneas da informação. Rio de Janeiro. 2010.

Disponível em: < <http://enancib.ibict.br/index.php/xi/enancibXI/paper/viewFile/527/210>>. Acesso em: 20 dez 2014.

_____. **Segurança e Defesa Cibernéticas para Reduzir Vulnerabilidades nas Infraestruturas Críticas Nacionais**. 2012.

FLORIDI, L. *Information ethics: an environmental approach to the digital divide. Philosophy in the Contemporary World*, v. 9, n. 1, 2002.

GAMIZ, Mario Sergio de Freitas. **Privacidade e intimidade: doutrina e jurisprudência**. Curitiba: Juruá, 2012.

GARDNER, Daniel. **Risco: a ciência e a política do medo**. Tradução: Léa Viveiros de Castro e Eduardo Sussekind. Rio de Janeiro: Odisséia, 2009.

GASPARI, Elio. **A ditadura envergonhada**. São Paulo: Companhia das Letras, 2002.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GONZÁLEZ de GÓMEZ, María Nélide. **Desafios contemporâneos da ciência da informação: as questões éticas da informação**. ENANCIB, João Pessoa, 2009.

GOODE, W. J.; HATT, P. K. Métodos em Pesquisa Social. 4a ed. São Paulo: Comp. Ed. Nacional, p. 35-67,1960.

GOPINATH, M. A.; DAS, P. *Classification and representation of knowledge*. Library Science with a Slant to Documentation and Information Studies, v. 34, n. 2, p. 85-90, 1997.

GSI-PR. Gabinete de Segurança Institucional da Presidência da República. **Guia de referência para a segurança das infraestruturas críticas da informação**. Brasília: GSIPR/SE/DSIC, 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 20 de dez. 2014.

_____. Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13 de Junho de 2008 (IN01/GSI-PR). **Gestão de Segurança da Informação e Comunicações na Administração Pública Federal**. 2008a.

Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidisic.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 2 da Instrução Normativa nº 01 GSI-PR (NC02/IN01/DSIC/GSIPR), de 13 de outubro de 2008. **Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC**. 2008b.

Disponível em: <http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 3 da Instrução Normativa nº 01 GSI-PR (NC03/IN01/DSIC/GSIPR), de 30 de junho de 2009. **Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal**. 2009a.

Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 4 da Instrução Normativa nº 01 GSI-PR (NC04/IN01/DSIC/GSIPR rev.1), de 15 de fevereiro de 2013.

Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC. 2013. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 5 da Instrução Normativa nº 01 GSI-PR (NC05/IN01/DSIC/GSIPR), de 14 de agosto de 2009. **Criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**. 2009b.

Disponível em: <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 9 da Instrução Normativa nº 01 GSI-PR (NC09/IN01/DSIC/GSIPR rev. 2), de 15 de julho de 2014. **Orientações Específicas para Uso de Recursos Criptográficos em Segurança da Informação e Comunicações**. 2014b.

Disponível em: <http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 10 da Instrução Normativa nº 01 GSI-PR (NC10/IN01/DSIC/GSIPR), de 30 de janeiro de 2012. **Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal**. 2012. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 19 da Instrução Normativa nº 01 GSI-PR (NC19/IN01/DSIC/GSIPR), de 15 de julho de 2014. **Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.** 2014c.

Disponível em: http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS ESTRUTURANTES.pdf>. Acesso em: 20 de dez. 2014.

_____. Norma Complementar nº 20 da Instrução Normativa nº 01 GSI-PR (NC20/IN01/DSIC/GSIPR rev. 1), de 15 de dezembro de 2014. **Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal.** 2014a.

Disponível em: http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf>. Acesso em: 20 de dez. 2014.

HAMESSE, J. **O modelo escolástico da leitura.** In: CAVALLO, G.; CHARTIER, R. (Org.). *História da leitura no mundo ocidental: I.* São Paulo: Ática, p. 123-46, 2002.

IMPrensa NACIONAL. Portaria nº 268 de 5 de outubro de 2009. **Dispõe sobre normas para publicação de matérias nos Jornais Oficiais.** Imprensa Nacional, Casa Civil da Presidência da República. Brasília: outubro, 2009.

ISO/IEC. *International Organization for Standardization e International Electrotechnical Commission. ISO/IEC 27000: Information technology - Security techniques – Information Security management systems - Overview and vocabulary.* 2014.

JARDIM, José Maria. **Transparência e opacidade do estado no Brasil: usos e desusos da informação governamental.** Niterói: EdUFF, 1999.

JARDIM, José Maria. **O acesso à informação arquivística no Brasil: problemas de acessibilidade e disseminação.** Niterói: EdUFF, 2009.

Disponível em: http://www.conarq.arquivonacional.gov.br/Media/publicacoes/mesa/o_ace_sso_informao_arquivstica_no_brasil.pdf>. Acesso em: 11 de jan. 2015.

KAPLAN. David M. *Ricoeur's Critical Theory. Reviewed by Philosophy in Review.* 2003.

KOTLER, P. **Administração e marketing: análise, planejamento, implementação e controle.** 5 ed São Paulo: Atlas, 1998.

KUNSCH, Margarida Maria Krohling. **Planejamento de relações públicas na comunicação interna.** São Paulo: Summus Editorial, 1986.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica - 5. ed. -** São Paulo: Atlas, 2003.

LE COADIC, Y. F. **Princípios científicos que direcionam a ciência e a tecnologia da informação digital**. Transinformação, Campinas, 2004.

LOPES, Luís Carlos. **Os arquivos, a gestão da informação e a reforma do estado**. Arquivo & História, Rio de Janeiro, n.4, p.37-49, out., 1998.

MALANGA, Eugênio. **Publicidade: uma introdução**. Atlas, São Paulo, 1979.

MAROCO, Cássio. **O princípio da publicidade administrativa no estado constitucional de direito**. Dissertação (mestrado em direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2011.

MARTINS JÚNIOR, Wallace Paiva. **Transparência administrativa: publicidade, motivação e participação popular**. 2. ed. São Paulo: Saraiva, 2010.

MATIAS-PEREIRA, José. **Manual de metodologia de pesquisa científica**. São Paulo: Atlas, 2007.

MCGARRY, Kevin. **O Contexto Dinâmico da Informação: uma análise introdutória**. Tradução de Helena Vilar de Lemos. Brasília, DF: Briquet de Lemos, 1999.

McQUAIL, Denis; WINDAHL, Sven. *Communication model. London*. Longman. 1993.

MEADOWS, A. J. et al. *Dictionary of computing and new information technology*. London: Kegan Paul, 1984.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 23.ed. São Paulo: Malheiros, 1998.

MILL, Daniel; FIDALGO, Fernando. **A Internet como suporte técnico para coleta de para pesquisas científicas**. Vertentes (São João Del Rei), v. 29, p. 38-50, 2007.

Disponível em: <http://intranet.ufsj.edu.br/rep_sysweb/File/vertentes/Vertentes_29/mill_e_fidalgo.pdf>. Acesso em: 11 de jan. 2015.

MINAYO, Maria Cecília de Souza (org). **Pesquisa social: teoria, método e criatividade**. Petrópolis/RJ: Vozes, 2001

MOREIRA, Daniel Augusto; QUEIROZ, Ana Carolina S. **Novas tecnologias e confiança nas organizações: um estudo de caso no contexto hospitalar**. Revista de Negócios, Blumenau, v. 12, n. 1, p. 42 - 55, janeiro/março, 2007.

MP. Ministério do Planejamento, Orçamento e Gestão. Portaria nº 3 de 7 de maio de 2007. **Institucionaliza o Modelo de Acessibilidade em Governo Eletrônico – eMAG no âmbito do Sistema de Administração dos Recursos de Informação e Informática - SISP**, Secretaria de Logística e Tecnologia da Informação. Brasília: 2007.

Disponível em: <<http://www.governoeletronico.gov.br/o-gov.br/legislacao/portaria-no-03-de-07-de-maio-de-2007>>. Acesso em: 24 de dez. 2014.

_____. Instrução Normativa nº 4 de 12 de novembro de 2010. **Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática - SISP do Poder Executivo Federal**. Secretaria de Logística e Tecnologia da Informação. Brasília: 2010. Disponível em: < <http://www.governoeletronico.gov.br/sisp-conteudo/nucleo-de-contratacoes-de-ti/modelo-de-contratacoes-normativos-e-documentos-de-referencia/instrucao-normativa-mp-slti-no04>>. Acesso em: 24 de dez. 2014.

_____. **Padrões Web em Governo Eletrônico - Guia de administração de sítios**, versão 1.4. Secretaria de Gestão Pública. Brasília: julho, 2012a.

Disponível em: < <http://www.governoeletronico.gov.br/acoes-e-projetos/padroes-brasil-e-gov/guia-de-administracao/index/?searchterm=guia%20de%20administra%C3%A7%C3%A3o>>. Acesso em: 24 de dez. 2014.

_____. **Guia de Elaboração do PDTI do SISP**, versão 1.0. Secretaria de Logística e Tecnologia da Informação. Brasília. 2012b.

Disponível em: < <http://www.governoeletronico.gov.br/biblioteca/arquivos/guia-de-elaboracao-de-pdti-do-sisp-versao-1.0/view?searchterm=guia%20de%20elabora%C3%A7%C3%A3o>>. Acesso em: 24 de dez. 2014.

_____. **Boletim Estatístico de Pessoal e Informações Organizacionais**, Vol. 19 nº 225 parte I e II. Secretaria de Gestão Pública. Brasília: janeiro, 2015.

Disponível em: <<http://www.planejamento.gov.br/ministerio.asp?index=6&ler=t10204>>. Acesso em: 24 de mai. 2015.

NONAKA, Ikujiro e TAKEUCHI, Hirotaka. **Criação do Conhecimento na Empresa: como as empresas geram a dinâmica da inovação**. Rio de Janeiro: Campus, 1997.

OLIVEIRA, Gracione Batista de. **Publicidade, discurso e procedimento deliberativo: uma análise da teoria democrática de Jürgen, Habermas**. Dissertação (mestrado) – Universidade Federal da Bahia, Faculdade de Filosofia e Ciências Humanas, Salvador, 2010.

OLIVEIRA NETTO, Alvim Antônio de. **Metodologia da Pesquisa Científica: Guia Prático para Apresentação de trabalhos Acadêmicos**. 2º ed. Florianópolis: Visual Books, 2006.

ONU. Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas em 10 de dezembro de 1948.

Disponível em: <<http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>>. Acesso em: 23 de dez. 2014.

_____. **O direito à privacidade na era digital**. Aprovada pela resolução A/RES/68/167 da Assembleia Geral das Nações Unidas em 18 de dezembro de 2013.

Disponível em: < http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=/english/&Lang=S>. Acesso em: 26 de fev. 2015.

PESTANA, Márcio. **Direito administrativo brasileiro**. 2. ed. Rio de Janeiro: Elsevier, 2010.

PINHEIRO, Lena Vânia R., LOUREIRO, José Mauro M. **Traçados e limites da Ciência da Informação**. Ciência da Informação, Brasília, MCT/CNPq/IBICT, v. 24, n. 1, jan./abril, p. 42-53, 1995.

PRATES, Naudé Pedro. **Transparência na administração pública e as novas tecnologias como ferramenta na efetivação dos direitos sociais**. Dissertação (mestrado). Universidade do Vale do Rio dos Sinos – Unisinos. Programa de Pós-Graduação em Direito, São Leopoldo, RS, 2012. Disponível em: < <http://biblioteca.asav.org.br/vinculos/000000/0000006B.pdf>>. Acesso: em 12 out 2014.

RABAÇA, Carlos Alberto e BARBOSA, Gustavo. **Dicionário da comunicação**. São Paulo: Ática, 1998.

RAMOS, Anderson. **Security Officer – 1: guia oficial para formação de gestores em segurança da informação**. Módulo Security Solutions, 2ª ed. - Porto Alegre, RS: Zouk, 2008.

RANGEL, Alcimar Sanches. **Estudo da Metodologia de Análise de Riscos EBIOS para Aplicação na Administração Pública Federal: Potencial Alinhamento à Legislação Brasileira**. Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a obtenção do título de Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações. Brasília: 2010.

RESENDE, Tomáz de Aquino. **Roteiro do terceiro setor. Associações e Fundações: o que são, como instituir, administrar e prestar contas**. 3 ed. Belo Horizonte: Prax, 2006.

REZENDE, Pedro Antonio Dourado. **Transparência, Opacidade e Equilíbrio**. Coluna: Segurança, Bits & Cia do Jornal do Commercio, publicado em 14/02/02, 2002.

Disponível em: <<http://www.cic.unb.br/~rezende/trabs/jcsbc1.htm>>. Acesso em: 22 de nov.2014.

ROBREDO, J. **Da Ciência da informação revisitada aos sistemas humanos de informação**. Brasília: Thesaurus, 2003.

ROCHA, Cármen Lúcia Antunes. **Princípios Constitucionais da Administração Pública**. Belo Horizonte: Del Rey, 1994.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2ª ed. Rio de Janeiro: Elsevier, 2014.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. Edição Revista e atualizada – São Paulo: Cortez, 2007.

SHERMERHORN JR, John R. **Fundamentos do comportamento organizacional**. 3. ed. Rio Grande do Sul: Bookman, 1991.

SILVA, Edna Lúcia da e MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. – Florianópolis: UFSC, 2005.

SILVA C., Carlos Bruno Ferreira da. **Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil**. Belo Horizonte: Arraes Editores, 2014.

SILVA R., Rozelito Felix da. **Proposta de adaptação do modelo balanced scorecard – BSC para a gestão de segurança da informação em órgãos da administração pública**. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM - 427/2010, Departamento de Engenharia Elétrica, Universidade de Brasília, DF, 2010.

SILVA Z., Zander Campos da. **Dicionário de Marketing e Propaganda**. Rio de Janeiro: Pallas, 1976.

SILVA L. Lino Martins da. **Contabilidade governamental: um enfoque administrativo**. 7. ed. São Paulo: Atlas, 2004.

SIMIÃO, Reinaldo Silva. **Segurança da Informação e Comunicações: conceito aplicável em organizações governamentais**. Brasília: UnB, 2009.

Disponível em: <<http://dsic.planalto.gov.br/cegsic/83-monografias-da-1o-turma-do-cegsic>>. Acesso em: 23 de dez. 2014.

SIQUEIRA, Jéssica Camara. **Relações entre Ciência da Informação e Ciências da Comunicação**. Salvador, v.5, n.2, p. 20-30, ago, 2011.

Disponível em: <<http://www.portalseer.ufba.br/index.php/revistaici/article/view/4492/3905>>. Acesso em: 22 de dez. 2014.

SOARES, Rafael Henrique Santos. **Métodos para análise da comunicação e mediação da informação em organizações públicas por meio de redes sociais**. Dissertação (Mestrado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2014.

SOUSA, Renato. T. B. **Os princípios arquivísticos e o conceito de classificação**. In: RODRIGUES, Georgete Medleg; LOPES, Ilza Leite. (Org.). Organização e representação do conhecimento na perspectiva da Ciência da Informação. Brasília: Thesaurus, 2003.

SOUZA, Simone Rita Zibetti de. **Controle Jurisdicional do Orçamento e da Destinação dos Tributos**. Dissertação (mestrado em direito) – Faculdades Integradas do Brasil – UniBrasil, Curitiba, 2009.

STF. Superior Tribunal Federal. **Suspensão de Segurança n.º 3.902-4/SP**. Relator Ministro Min. Ayres Britto, Tribunal Pleno, julgado em 09/06/2011 – Brasília: 2011.

Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=6281985>>. Acesso em: 22 de dez. 2014.

SUN TZU. **A arte da guerra**. - 14a ed. - Rio de Janeiro: Record, 1993.

TCU. Tribunal de Contas da União. **Segurança da informação no TCU: política corporativa comentada** – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

_____. Acórdão nº 758 de 30 de março de 2011. **Relatório de auditoria. Avaliação de controles gerais de tecnologia da informação. Constatação de irregularidades, precariedades e oportunidades de melhoria. Determinações, recomendações e alertas para o Ministério das Relações Exteriores**. Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2011.

_____. Acórdão nº 1.233 de 23 de maio de 2012. **Trata-se de relatório consolidado das ações do TMS 6/2010, cujo objeto foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI**. Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012a.

_____. Acórdão nº 2.585 de 26 de setembro de 2012. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Relator Ministro Walton Alencar Rodrigues – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012b.

_____. Acórdão nº 1.221 de 14 de maio de 2014. **Monitoramento de diversos acórdãos prolatados em fiscalização de TI, com objetivo de avaliar a gestão e uso em diversos órgãos à luz da legislação vigente e das boas práticas de governança. Grande quantidade de determinações e recomendações feitas aos diversos órgãos. Realização de audiência de responsáveis que não apresentaram justificativas para o não cumprimento das deliberações. Reiteração de determinações. Recomendações. Novo monitoramento.** Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2014a.

_____. Acórdão nº 3.051 de 5 de novembro de 2014. **Fiscalização de orientação centralizada (FOC). Governança de TI. Recomendações. Arquivamento.** Relator Ministro Weder de Oliveira. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2014b.

_____. Acórdão nº 3.117 de 12 de novembro de 2014. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal.** Relator Ministro Augusto Sherman Cavalcanti. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2014c.

THAYER, Lee. **Comunicação: fundamentos e sistemas, na organização, na administração, nas relações interpessoais.** São Paulo: Altas, 1976.

TOGNOLI, Natália. **A informação no contexto arquivístico: uma discussão a partir dos conceitos de informação-como-coisa e informação orgânica.** Informação Arquivística, Rio de Janeiro, 2012.

UNB. Universidade de Brasília. **Relatório de Pesquisa de Avaliação do Portal da Transparência do Governo Federal.** Brasília: agosto de 2014.

Disponível em: <http://www.portaltransparencia.gov.br/sobre/Boletim/Especial_Pesquisa-de-Avaliacao2014.pdf>. Acesso em: 24 de dez. 2014.

UNESCO. Relatório Global [livro eletrônico]: **Abrindo novos caminhos para o empoderamento: TIC no acesso à informação e ao conhecimento para as pessoas com deficiência;** tradução: DB Comunicação. -- São Paulo: Comitê Gestor da Internet no Brasil, 2014.

Disponível em: <<http://cetic.br/publicacao/relatorio-global-unesco-abrindo-novos-caminhos-para-o-empoderamento-tic-no-acesso-a-informacao-e-ao-conhecimento-para-as-pessoas-com-deficiencia/>>. Acesso: 22 de dez. 2014.

VIDAL, Gabriel Rigoldi. **Privacidade e internet.** Universidade Estadual Paulista – Faculdade de Ciências Humanas e Sociais, 2010.

Disponível em: <http://www.direitorp.usp.br/arquivos/noticias/sites_eventos/3_semana_juridica_2010/papers/Gabriel%20Rigoldi%20Vidal.pdf>. Acesso: 22 de dez. 2014.

VIEIRA, Domingos; COELHO, Adolfo; BRAGA, Teófilo. **Grande dicionário português ou tesouro da língua portuguesa**. Editores: Ernesto Chardron e Bartholomeu H. De Moraes. Segundo Volume, Porto, 1873.

Disponível em: <http://books.google.com.br/books?id=_q9CAQAAMAAJ&pg=PA247&lpg=PA247&dq=calare+classis+classificar&source=bl&ots=QJLcPPqlxQ&sig=EfFqRC5bm0hBCKf5GP_aPOmu2TI&hl=pt-BR&sa=X&ei=tkl-VLqwJ8WWNuG2gZgB&ved=0CCUQ6AEwAQ#v=onepage&q=calare%20classis%20classificar&f=false>. Acesso: 02 de dez. 2014.

VIEIRA R., Roberto Fonseca. **Comunicação Organizacional: gestão de relações públicas**. Rio de Janeiro: Mauad, 2004.

VIEIRA T., Tatiana Malta. **O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007.

Disponível em: <http://www.fd.unb.br/index.php?option=com_zoo&task=item&item_id=66&Itemid=1469&lang=br>. Acesso em: 09 de mar. 2015.

WARREN, Samuel; BRANDEIS, Louis. *The right to privacy*. In *Havard Law Review*. Vol. IV, 1890.

Disponível em: <<http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>>. Acesso: 20 de nov. 2014.

WESTERMAN, George; HUNTER Richard. **O Risco de TI. Convertendo ameaças aos negócios em vantagem competitiva**. 1ª ed. São Paulo. M. Books do Brasil Editora, 2008.

WOLF, Mauro. **Teorias da Comunicação**. Editorial Presença, Lisboa. 2003.

ANEXO A – Lista dos Membros do CGSI/2015

**CONSELHO DE DEFESA NACIONAL
SECRETARIA EXECUTIVA**

PORTARIA Nº 7 DE 17 DE MARÇO DE 2015

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições e tendo em vista o disposto no art. 6º e no art. 7º do Decreto nº 3.505, de 13 de junho de 2000, com nova redação dada pelo Decreto nº 8.097, de 4 de setembro de 2013, resolve:

Art. 1º Designar membros para compor o Comitê Gestor de Segurança da Informação:

Órgão	Representantes
Ministério da Justiça.	Marcelo Nogueira Lino (Titular)
	Eduardo Spano Junqueira de Paiva (Suplente)
Ministério da Defesa.	Edgar Wilson Gonçalves de Souza (Titular)
	Luciano Aguiar Brandão (Suplente)
Ministério de Relações Exteriores.	Nestor José Forster Junior (Titular)
	João Eduardo Gonçalves da Silva (Suplente)
Ministério da Fazenda.	Fernando Nascimento Barbosa (Titular)
	Sérgio Fuchs (Suplente)
	Marcio Nahas Ribeiro (Suplente)
	Vilson da Silva Santos Junior (Suplente)
	Marcos Allemand Lopes (Suplente)
Ministério da Previdência Social.	Rogério Gabriel Nogalha De Lima (Suplente)
	Marcelo Henrique de Ávila (Titular)
	Elisete Berchiol da Silva Iwai (Suplente)
	José Maria Freire de Menezes Filho (Suplente)
	Sueli Aparecida Carvalho Romero (Suplente)
	Humberto Degrazia Campedelli (Suplente)
	Joel Jurandir Ferreira Correa (Suplente)
Ministério da Saúde.	Neusa Peixoto Campos (Suplente)
	Giliate Cardoso Coelho Neto (Titular)
Ministério do Desenvolvimento, Indústria e Comércio Exterior.	Rodrigo Franco de Souza (Suplente)
	Thiago da Conceição Freire (Titular)
Ministério Planejamento, Orçamento e Gestão.	Natália Lorenzetti (Suplente)
	Fernando Antônio Braga de Siqueira Júnior (Titular)
	José Ney de Oliveira Lima (Suplente)
	Gilson Fernando Botta (Suplente)

Ministério das Comunicações.	James Marlon Azevedo Gorgen (Titular)
	Luis Felipe Salin Monteiro (Suplente)
Ministério de Ciência, Tecnologia e Inovação.	Vírgilio Augusto Fernandes Almeida (Titular)
	José Henrique de Lima Correia Dieguez Barreiro (Suplente)
Casa Civil da Presidência da República	Renato da Silveira Martini (Titular)
	Eduardo Magalhães de Lacerda Filho (Suplente)
	Daniel André Silva Ribeiro (Suplente)
Gabinete de Segurança Institucional da Presidência da República.	Marconi dos Reis Bezerra (Coordenador)
	Antônio Magno Figueiredo de Oliveira (Titular)
	David Bernardes de Assis (Suplente)
	Josita Arcanjo Ramos Ferreira (Suplente)
	Otávio Carlos Cunha da Silva (Suplente)
	Rodrigo Colli (Suplente)
	Antônio Augusto Muniz de Carvalho (Suplente)
Secretaria de Comunicação Social da Presidência da República.	Mauricio Bichara Hortêncio de Medeiros (Titular)
	Carlos Márcio Chaves (Suplente)
Ministério de Minas e Energia.	Hiram Costa Botelho (Titular)
	Hisao Fujimoto (Suplente)
Controladoria-Geral da União.	Gilson Libório de Oliveira Mendes (Titular)
	Henrique Aparecido da Rocha (Suplente)
Advocacia-Geral da União.	Rosângela Silveira de Oliveira (Titular)
	Eduardo Alexandre Lang (Suplente)
Secretaria-Geral da Presidência da República.	Cláudio Crossetti Dutra (Titular)
	José Sérgio Lima Caldana (Suplente)
	Carlos Henrique Ribeiro dos Santos (Suplente)
	Fraide Barreto Sales (Suplente)

Art. 2º Esta Portaria entra em vigor da data de sua publicação.

Art. 3º Fica revogada as Portarias Nº 13 - CDN, de 7 de março de 2014, 21 - CDN, de 4 de julho de 2014, 36 - CDN, de 15 de setembro de 2014, 37 - CDN, de 30 de setembro de 2014, 39 - CDN, de 6 de outubro de 2014 e 42 - CDN, de 31 de outubro de 2014.

JOSÉ ELITO CARVALHO SIQUEIRA

APÊNDICE A – Lista das fontes de ameaças representadas por seres humanos

Origem das ameaças	Motivação	Possíveis consequências
<i>Hacker, cracker</i>	<ul style="list-style-type: none"> • Desafio • Ego • Rebeldia • Status • Dinheiro 	<ul style="list-style-type: none"> • <i>Hacking</i> • Engenharia social • Invasão de sistemas, infiltrações e entradas não autorizadas • Acesso não autorizado ao sistema
Criminoso digital	<ul style="list-style-type: none"> • Destruição de informações • Divulgação ilegal de informações • Ganho monetário • Alteração não autorizada de dados 	<ul style="list-style-type: none"> • Crime digital (por exemplo, perseguição no mundo digital) • Ato fraudulento (por exemplo, reutilização indevida de credenciais e dados transmitidos, fazer-se passar por uma outra pessoa, interceptação) • Suborno por informação • <i>Spoofing</i> (fazer-se passar por outro) • Invasão de sistemas
Terrorista	<ul style="list-style-type: none"> • Chantagem • Destruição • Explosão • Vingança • Ganho político • Cobertura da mídia 	<ul style="list-style-type: none"> • Bomba/terrorismo • Guerra de informação • Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço) • Invasão de sistema • Alteração do sistema
Espionagem industrial (serviços de inteligência, empresas, governos estrangeiros, outros grupos de interesse ligados ao governo)	<ul style="list-style-type: none"> • Vantagem competitiva • Espionagem econômica 	<ul style="list-style-type: none"> • Garantir a vantagem de um posicionamento defensivo • Garantir uma vantagem política • Exploração econômica • Furto de informação • Violação da privacidade das pessoas • Engenharia social • Invasão de sistema • Acesso não autorizado ao sistema (acesso a informação restrita, de propriedade exclusiva e/ou relativa à tecnologia)
Pessoal interno (funcionários mal treinados, insatisfeitos, mal intencionados, negligentes, desonestos ou dispensados)	<ul style="list-style-type: none"> • Curiosidade • Ego • Obtenção de informações úteis para serviços de inteligência • Ganho monetário • Vingança • Erros e omissões não intencionados (por exemplo, erro na entrada de dados, erro de programação) 	<ul style="list-style-type: none"> • Agressão a funcionário • Chantagem • Vasculhar informação de propriedade exclusiva • Uso improprio de recurso computacional • Fraude e furto • Suborno por informação • Entrada de dados falsificados ou corrompidos • Interceptação • Código malicioso (por exemplo, vírus, bomba lógica, Cavalo de Tróia) • Venda de informações pessoais • Defeitos (bugs) no sistema • Invasão de sistemas • Sabotagem de sistemas • Acesso não autorizado ao sistema

Fonte: ABNT (2011, p. 55)

APÊNDICE B – Lista de vulnerabilidades

Tipos	Exemplos de vulnerabilidade
<i>Hardware</i>	Manutenção insuficiente/instalação defeituosa de mídia de armazenamento
	Falta de rotina de substituição periódica
	Sensibilidade à umidade, poeira, sujeira
	Sensibilidade à radiação eletromagnética
	Inexistência de um controle eficiente de mudança de configuração
	Sensibilidade a variações de voltagem
	Sensibilidade a variações e de temperatura
	Armazenamento não protegido
	Falta de cuidado durante o descarte
	Realização de cópias não controladas
<i>Software</i>	Procedimentos de teste de <i>software</i> insuficientes ou inexistentes
	Falhas conhecidas no <i>software</i>
	Não execução do <i>logout</i> ao se deixar uma estação de trabalho desassistida
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção de dados
	Atribuição errônea de direitos de acesso
	<i>Software</i> amplamente distribuído
	Utilizar programas aplicativos com um conjunto errado de dados (referentes a um outro período)
	Interface de usuário complicada
	Documentação inexistente
	Configuração de parâmetros incorreta
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuários
	Tabela de senhas desprotegidas
	Gerenciamento de senhas mal feito
	Serviços desnecessários que permanecem habilitados
	<i>Software</i> novo ou imaturo
Especificações confusas ou incompletas para os desenvolvedores	
Inexistência de um controle eficaz de <i>software</i>	
Inexistência de cópia de segurança (<i>back-up</i>)	
Inexistência de relatórios de gerenciamento	
<i>Rede</i>	Inexistência de evidências que comprovem o envio ou recebimento de mensagens
	Linhas de comunicação desprotegidas
	Trafego sensível desprotegido
	Junções de cabeamento mal feitas
	Ponto único de falha
	Não identificação e não autenticação do emissor e do receptor
	Arquitetura insegura da rede
	Transferência de senhas em claro
	Gerenciamento de rede inadequado (quanto á flexibilidade de roteamento)
Conexões de redes públicas desprotegidas	

Recursos Humanos	Ausência de recursos humanos
	Procedimentos de recrutamento inadequados
	Treinamento insuficiente em segurança
	Uso incorreto de <i>software</i> e <i>hardware</i>
	Falta de conscientização em segurança
	Inexistência de mecanismos de monitoramento
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
Organização	Inexistência de um procedimento formal para o registro e a remoção de usuários
	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Inexistência de auditorias periódicas (supervisão)
	Inexistência de procedimentos para a identificação, análise e avaliação de riscos
	Inexistência de relatos de falha nos arquivos (<i>logs</i>) de auditoria das atividades de administradores e operadores
	Acordo de nível de serviço inexistente
	Inexistência de procedimentos de controle de mudanças
	Inexistência de um procedimento formal para o controle da documentação do SGSI
	Inexistência de um processo formal para a autorização das informações disponíveis publicamente
	Atribuição inadequada das responsabilidades pela segurança da informação
	Inexistência de um plano de continuidade
	Inexistência de política de uso de correspondência eletrônica (<i>email</i>)
	Inexistência de procedimentos para a instalação de <i>software</i> em sistemas operacionais
	Ausência de registros nos arquivos de auditoria (<i>logs</i>) de administradores e operadores
	Inexistência de procedimentos para a manipulação de informações classificadas
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
	Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação
	Inexistência de uma política formal sobre o uso de computadores móveis
Inexistência de análises críticas periódicas por parte da direção	
Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	

APÊNDICE C – Modelo de questionário

PESQUISA: Transparência *versus* Segurança da Informação: uma análise dos fatores de risco expostos na comunicação entre o governo e a sociedade.

Prezado Participante,

Este questionário é parte de uma pesquisa de mestrado em desenvolvimento no Programa de Pós-graduação em Ciência da Informação da Universidade de Brasília que tem como objetivo validar o processo de análise de riscos inerentes à divulgação de dados pessoais de agentes públicos federais que atuam na segurança nacional e segurança pública.

A escolha de Vossa Senhoria como participante deste questionário se deu ao fato pela importância estratégica de sua pessoa na tomada de decisões relativas ao tema Segurança da Informação na APF. Outro aspecto relevante é que o senhor é membro do Comitê Gestor da Segurança da Informação, nomeado pela Portaria nº 7 de 17 de março de 2015 do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, na condição de Secretário Executivo do Conselho de Defesa Nacional.

Entre as principais diretrizes estabelecidas na Lei de Acesso à Informação (LAI), destacam-se a observância da publicidade como preceito geral e do sigilo como exceção; como também, a divulgação de informações de interesse público, independentemente de solicitações, como por exemplo, dados e informações de agentes públicos. Nesse sentido, solicito a vossa senhoria o preenchimento do formulário anexo.

Desde já agradeço sua colaboração,

ALCIMAR SANCHES RANGEL
Mestrando em Ciência da Informação (UnB)

JORGE HENRIQUE CABRAL FERNANDES
Professor Doutor - Faculdade de Ciência da Informação (UnB) - Orientador.

5) O senhor como representante do CGSI, visualiza algum tipo de norma ou orientação que venha fortalecer a segurança da informações dos agentes públicos?

SIM

NÃO

6) Se sim, qual tipo de norma ou orientação?

7) Assim como existe uma Lei que protege as informações dos agentes da Agência Brasileira de Inteligência, o senhor visualiza outros cargos, cujos dados dos ocupantes também poderiam ser protegidos por Lei?

SIM

NÃO

8) Se sim, quais cargos?
