FUNDAÇÃO JOÃO PINHEIRO

Escola de Governo Professor Paulo Neves de Carvalho

Mestrado em Administração Pública – Gestão da Informação

REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO ELETRÔNICO FEDERAL: ESTUDO COMPARADO BRASIL E CANADÁ

Kamila Araújo Rola Fontes Moreira

Belo Horizonte

2009

Kamila Araújo Rola Fontes Moreira

REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO ELETRÔNICO FEDERAL: ESTUDO COMPARADO BRASIL E CANADÁ

Dissertação apresentada ao curso de Pós-Graduação do Mestrado em Administração Pública, da Escola de Governo Paulo Neves de Carvalho, da Fundação João Pinheiro, como requisito parcial à obtenção do título de Mestre em Administração Pública.

Área de Concentração: Gestão da Informação

Orientadora: Profa. Dra. Sulamita Crespo Carrilho Machado

Belo Horizonte

2009

FICHA CATALOGRÁFICA

M838r Moreira, Kamila Araújo Rola Fontes
Regulamentação da política de segurança da informação do Governo Eletrônico Federal: estudo comparado Brasil e Canadá / Kamila Araújo Rola Fontes Moreira. - Belo Horizonte, 2009.
163 f.: il.

Orientadora: Prof. Dra. Sulamita Crespo Carrilho Machado

Dissertação (Mestrado) – Fundação João Pinheiro – Escola de Governo Paulo Neves de Carvalho. Programa de Pós-Graduação em Administração Pública.

1. Governo Eletrônico. 2. Segurança da Informação. 3. Regulamentação. I. Machado, Sulamita Crespo Carrilho. II. Fundação João Pinheiro. Escola de Governo Paulo Neves de Carvalho. Programa de Pós-Graduação em Administração Pública. III. Título.

CDU: 681.324

Aos meus pais,
fontes de luz.

AGRADECIMENTOS

Ao bom Deus, pela vida,

À minha avó Cynira, pela ajuda incondicional e aos avôs, *in memoriam,* Maria, José e Nestor pelas asas,

À minha família, tios e primos, pela compreensão e incentivo,

À minha orientadora, Sulamita Crespo, pelas orientações, apoio e integridade,

Ao professor Ricardo Carneiro, pelas idéias e pelas ajudas na pesquisa,

Aos professores, Simone Dufloth, Ronaldo Oleto, Elisa Rocha e Bruno Lazzarotti, pelas orientações do projeto de pesquisa,

Aos professores, Ricardo Gomes, Marconi Braga e Wagner Araújo, e aos funcionários da Secretaria de Fazenda de Minas Gerais, Leopoldo Souza e Margarida Rodrigues, pelos auxílios com o tema de pesquisa,

Ao professor Carlos Resende, pelas elucidações a respeito do Canadá,

À Larisse Santos, por me indicar o Mestrado da Fundação João Pinheiro,

Às minhas amigas, Vivianne, Larissa, Renata, Fernanda, Ana Luiza e Natália, pelo incentivo e pelo carinho,

Às queridas parceiras do Mestrado, Conceição, Célia e Raíssa, pelo aprendizado,

Aos colegas de Mestrado, Taís, Fabiana, Cláudio, Jamir e Reinaldo, pelas ótimas trocas de idéias,

Às secretarias, Juliana e Rosália, pelas disponibilidades,

Às bibliotecárias, Elisa, Judite e Jana, pelas orientações de pesquisas bibliográficas,

À Ângela Campelo e Isabel, por me ensinarem a respirar e a meditar,

Ao Cláudio Moretzsohn, Marília Campolina e Beth, por me ajudarem a mudar paradigmas,

Ao Tiago Rodolphi, pelo incentivo e ajuda em todas as horas,

E aos meus pais, Letícia e Nestor, pelo apoio incondicional.

RESUMO

A presente dissertação tem por propósito pesquisar a respeito da regulamentação do Governo Eletrônico Federal referente à política de segurança da informação, fazendo-se um estudo comparativo entre os Governos Eletrônicos do Brasil e do Canadá. A dissertação dedica-se aos antecedentes do governo eletrônico, como a revolução tecnológica, a sociedade do conhecimento e a rede de computadores; e especificamente ao governo eletrônico e segurança da informação. A partir desse embasamento teórico, seguem-se para as considerações da atividade de regulamentação e das características dos Estados Brasil e Canadá. E Finalmente, compara-se a regulamentação sobre a segurança da informação dos Governos Eletrônicos de Brasil e Canadá, suas semelhanças e diferenças.

Palavras-chave: Governo Eletrônico. Segurança da Informação. Regulamentação.

ABSTRACT

The present thesis has a main objective of research the electronic government regulation concerned with information about security policy, conducting a comparative study between Electronic Governments of Brazil and Canada. The thesis concentrates in antecedents of the electronic government such as technological revolution, knowledgeable society and computer network, specifically with respect of electronic government and security information. Based in this theoretical approach, the study takes into consideration the regulation activities and characteristics of Brazil and Canada. Finally, there is a comparison of regulation about information security of the Electronic Governments of Brazil and Canada, with their similarities and differences.

Key words: *Electronic Government. Information Security. Regulation*.

LISTA DE ABREVIATURAS

ABIN – Agência Brasileira de Inteligência

ABNT – Associação Brasileira de Normas Técnicas

AC – Autoridade Certificadora

ARPA – *Advanced Research Projects Agency*

ARPANET – *Advanced Research Projects Agency Network*

ART. – Artigo

AS/NZS – *Standards Austrália/Standards New Zealand*

BITNET – *Because It's Time Network*

B2G– *Business-to-Government* (Negócios para Governo)

BMS - Belgo Mineira Sistemas

BNDES – Banco Nacional par o Desenvolvimento Econômico e Social

BSI – *British Standards Institution*

CDN – Conselho de Defesa Nacional

CD-R – *Compact Disc - Recordable*

CD-ROM – *Compact Disc - Read Only Memory*

CD-RW – *Compact Disc - Rewritable*

CEGE – Comitê Executivo do Governo Eletrônico

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT/CC - Centro de Coordenação do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

C2G– *Consumer-to-Government* (Cidadão para Governo)

CGI.br – Comitê Gestor da Internet no Brasil

CH/GSI – Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República

CGSI – Comitê Gestor de Segurança da Informação

CLAD – *Centro Latinoamericano de Administración para el Desarrollo*

CMVP – *Cryptographic Module Validation Program*

CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico

CONARQ – Conselho Nacional de Arquivos

CPSA – *Cyber Protection Supply Arrangement*

CRA – *Canadian Revenue Agency*

CSE – *Communications Security Establishment*

CSEC – *Communications Security Establishment Canada*

CSNET – *Computer Science Network*

CSIS – *Canadian Security Intelligence Service*

DFAIT – *Foreign Affairs and International Trade Canada*

DND – *Department of National Defence*

DSP – *Depository Services Program*

DTV – Televisão Digital

DVD – *Digital Video Disk ou Digital Versatil Disk*

EAD – Ensino à Distância

e-CAC – Centro Virtual de Atendimento ao Contribuinte

e-Gov – Governo Eletrônico

EGTI – Estratégia Geral de Tecnologia da Informação

e-MAG – Modelo de Acessibilidade de Governo Eletrônico

EMAX – *Government of Canada telephone directories, and the Email Address Exchange Service*

ENIAC – *Electronica Numeral Integrator and Computer*

e-PING – Padrões de Interoperabilidade de Governo Eletrônico

ERM – *Enterprise Risk Management*

FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo

Fermilab – Fermi National Accelerator Laboratory

FIPS – *Federal Information Processing Standard*

G2B – *Government-to-Business* (Governo para Negócios)

G2C – *Government-to-Consumer* (Governo para Cidadão)

G2G – *Government-to-Government* (Governo para Governo)

GEDS – *Government Electronic Directory Services*

GOL – *Government On Line*

GOV – Governo

GOV.br. – Governo Eletrônico Brasileiro

GRC – Governança, Riscos e Compliance

GSI – Gabinete de Segurança Institucional

GTTI – Grupo de Trabalho Interministerial em Tecnologia da Informação

IBGE – Instituto Brasileiro de Geografia e Estatística

IBM – *International Business Machines*

Icann – *Internet Corporation for Assigned Names and Numbers*

ICP-Brasil – Infra-Estrutura de Chaves Públicas Brasileira

IDS – *Intrusion Detection System*

IEC – *International Electrotechnical Commission*

INFOSEG – Sistema Nacional de Integração de Informações em Justiça e Segurança Pública

IGA – *Intergovernmental Affairs*

IP – *Internet Protocol* (Protocolo de Interconexão)

IRPF – Imposto de Renda de Pessoa Física

IRPJ – Imposto de Renda de Pessoa Jurídica

ISMS – *Information Security Management System*

ISO – *International Organization for Standardization*

ITH – *Internetworking Technology Handbook*

ITI – Instituto Nacional de Tecnologia da Informação

ITIL – *Infrastructure Technology Information Library*

ITSB – *Information Technology Services Branch*

ITSS – *Information Technology Security Strategy*

ITU – *Word Telecommunication Indicators*

LSI – *Large Scale Integration*

MC – Ministério das Comunicações

MCT – Ministério da Ciência e Tecnologia

MEC – Ministério da Educação e Cultura

MILINET – *Military Network*

MPOG – Ministério do Planejamento, Orçamento e Gestão

NIC.br – Núcleo de Informação e Coordenação do Ponto BR (Brasil)

NIST – *National Institute of Standards and Technology*

NSF – *National Science Foundation*

NSFNET – *National Science Foundation Network*

OEA – Organização dos Estados Americanos

ONU – Organização das Nações Unidas

OPC – *Office of the Privacy Commissioner of Canada*

PCO – *Privy Council Office*

PDCA – *plan, do, check, act*

PL – Projeto de Lei

PMO – *Prime Minister's Office*

PNAD – Pesquisa Nacional por Amostra de Domicílios

PRODABEL – Empresa de Informática e Informação do Município de Belo Horizonte

PRODEMGE – Empresa de Tecnologia de Informação do Estado de Minas Gerais

PSI - Política de Segurança da Informação

RCMP – *Royal Canadian Mounted Police*

SBIN – Sistema Brasileiro de Inteligência

Seed – Secretaria de Educação a Distância

SERPRO – Serviço Federal de Processamento de Dados

SIAPE – Sistema Integrado de Administração de Recursos Humanos

SIDOF – Sistema de Geração e Tramitação de Documentos Oficiais

SIORG – Sistema de Informações Organizacionais do Governo Federal

SIP – *Inter American Press Association* (Sociedade Interamericana de Imprensa)

SIRC – *Security Intelligence Review Committee*

SISP – Sistema de Administração dos Recursos de Informação e Informática

SLTI – Secretaria de Logística e Tecnologia da Informação

S/N – sem número

SNI – Serviço Nacional de Informações

SOCINFO – Programa Sociedade de Informação

STATCAN – *Statistic Canadá*

TBS – *Treasury Board Secretariat*

TCP – *Transmission Control Protocol* (Protocolo de Controle de Transmissão)

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

TICs – Tecnologias da Informação e Comunicação

TRADIC – *Transistor Digital Computer*

TV – Televisão

UFSCAR – Universidade Federal de São Carlos

VLSI – *Very Large Scale Integration*

WSIS – *World Summit on the Information Society*

WWW – *World-Wide Web*

UNCTAD – Conferência da Organização das Nações Unidas sobre Comércio e Desenvolvimento

USB – *Universal Serial Bus*

SUMÁRIO

REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO ELETRÔNICO FEDERAL: ESTUDO COMPARADO BRASIL E CANADÁ

INTRODUÇÃO

Os Estados Democráticos de Direito requerem uma administração centrada nas necessidades de seu povo e de sua época. Nem sempre essas necessidades são atendidas pela elite governista – que efetivamente governa e representa o povo. Como governar e administrar o Estado dependem de entendimentos políticos, sociais, econômicos etc., o aparato estatal deve preocupar com a gestão de suas informações.

A gestão da informação é importante, pois facilita a administração do Estado, o processo decisório e a defesa nacional contra intromissões não-autorizadas ou indevidas no Estado. Segundo Thomas Wilson (1989), a gestão da informação é entendida como a gestão eficaz de todos os recursos de informação relevantes para a organização, tanto de recursos gerados internamente como os produzidos externamente, utilizando-se, sempre que necessário, a tecnologia de informação.

A gestão da informação nos Estados provoca ajustes em seu *modus operandi*, não apenas na busca da informação, mas, principalmente, no uso que se faz dela por meio de seu gerenciamento. Como o *modus operandi* do Estado evolui constantemente foi criado recentemente o governo eletrônico (e-Gov) para auxiliar no gerenciamento das informações ao permitir a prestação de serviços, informações, consultas, atendimentos e participação popular por meio de tecnologias, sem a necessidade do cidadão se deslocar até um órgão da Administração Pública. Dentre as tecnologias citam-se o telefone fixo, o celular, a Internet, e a TV digital.

As tecnologias incentivam o Estado a adequar e aperfeiçoar sua gestão da informação, pois são novas formas de obter, utilizar, armazenar e processar informações. As informações precisam ser protegidas e devidamente processadas, armazenadas, usadas e publicadas para garantir a segurança das mesmas ao manter sua confidencialidade, sua disponibilidade e sua integridade.

O elevado volume de informações e de tecnologias disponíveis na sociedade do conhecimento impõe ao e-Gov Federal brasileiro uma regulamentação mais expressiva a respeito da política de segurança da informação, pois, a todo o momento, a Administração

Pública precisa tomar decisões acertadas, de acordo com as informações disponíveis em seus sistemas de informação. Há que garantir a legitimidade dessas informações e a segurança das mesmas, pois são imprescindíveis para as decisões acertadas dos governantes e proteção dos direitos e deveres dos cidadãos.

A consideração desses aspectos suscita a definição da problemática da presente pesquisa, que pode ser compreendida a partir dos seguintes questionamentos: O que já foi, como foi e por que foi regulamentado sobre a política de segurança da informação dos Governos Eletrônicos Federais do Brasil e do Canadá? Quais são as semelhanças e diferenças dessa política nesses países sob o prisma da Teoria do Conhecimento, do Governo Eletrônico, da Gestão da Informação e do Direito?

O objetivo geral é um estudo comparativo entre os Governos Eletrônicos Federais do Brasil e Canadá, do que já foi, como foi e por que foi regulamentado sobre a política de segurança da informação. Os objetivos específicos da pesquisa são identificar toda a regulamentação, descrever as semelhanças e diferenças na regulamentação e interpretá-las, baseada na literatura da Teoria do Conhecimento, do Governo Eletrônico, da Gestão da Informação e do Direito.

O estudo comparativo é justificado por ser o Canadá referência mundial em questões de políticas de e-Gov. Além disso, a implantação do e-Gov é recente, com precária legislação e escassas bibliografias a respeito. É um tema de vanguarda, havendo necessidade de pesquisar mais a respeito, pois há uma crescente informatização da Administração Pública, que utiliza cada vez mais informações e serviços em meios eletrônicos. Outro fator é a importância da política de segurança da informação para a Administração Pública, que se utiliza de informações para tomar suas decisões e possui um banco de dados altamente valioso para seus cidadãos, que deve ser protegido e garantido a confidencialidade, a integridade, a disponibilidade, a legalidade e a legitimidade de seu conteúdo.

No procedimento metodológico foi realizada primeiramente a revisão literária e a análise descritiva do que foi, como foi e por que foi regulamentado sobre a política de segurança da informação nos Governos Eletrônicos Federais do Brasil e Canadá. Posteriormente foi feita uma análise comparativa a respeito das semelhanças e diferenças da regulamentação sobre a política de segurança da informação dos Governos Eletrônicos Federais do Brasil e Canadá. Finalmente, a partir da descrição e da comparação acima foram interpretadas essas semelhanças e diferenças de ambos os governos eletrônicos, pautando-se na literatura da Teoria do Conhecimento, do Governo Eletrônico, da Gestão da Informação e do Direito.

A pesquisa teve como universo de abrangência as normas constitucionais e infra-constitucionais do Brasil e Canadá relacionadas à política de segurança da informação do Governo Eletrônico (Constituição Federal; Normas Internacionais; Leis; Decretos; Decretos Legislativos; Portarias; Instruções Normativas; Norma de Execução Conjunta; Resoluções).

Na coleta de dados, foram utilizadas primordialmente as técnicas da pesquisa bibliográfica, a qual abarcou uma busca de informações relacionadas ao assunto em livros, brochuras, artigos publicados em conferências sobre o tema, relatórios, artigos de periódicos, informações disponibilizadas na Internet, e legislação. Foi feita revisão bibliográfica de alguns conceitos centrais para a dissertação, como: governo eletrônico, sociedade do conhecimento, segurança da informação, regulamentação. E pesquisa nos sites de Brasil e Canadá referentes à segurança da informação, como:

a) Brasil[1]: Governo Eletrônico; Ministério do Planejamento, Orçamento e Gestão; Comitê Gestor da Segurança da Informação; Departamento de Segurança da Informação e Comunicações; Comitê Gestor da Internet no Brasil; dentre outros.

b) Canadá[2]: Governo Eletrônico; *Canadian ePolicy Resource Centre*; *Treasury Board of Canada Secretariat*; *Departments and Agencies*; *Science Direct*; *Department of Justice Canada*; *Communications Security Establishment Canada*; *Government Electronic Directory Services*; Parlamento Canadense, dentre outros.

A presente dissertação foi dividida em seis capítulos e conclusão. No primeiro capítulo disserta-se sobre os antecedentes do e-Gov; no segundo, especificamente sobre o e-Gov; no terceiro, segurança da informação; no quarto, regulamentação e características do Brasil e Canadá; no quinto, descrição da regulamentação da segurança da informação no Brasil e no Canadá; no sexto, interpretação das semelhanças e diferenças da regulamentação da segurança da informação no Brasil e no Canadá.

[1] Disponível respectivamente em: <http://www.governoeletronico.e.gov.br>; <http://www.planejamento.gov.br/tecnologia_informacao/conteudo/principais_atv/seguranca_info.htm>; <http://www.planalto.gov.br/gsi/cgsi/index.htm>; <http://gsisic.serpro.gov.br/cgsi/>; <http://governanca.cgi.br/seguranca>;

[2] Disponível respectivamente em: <http://canada.gc.ca>; <http://www.ceprc.ca/cgol_ e.html>; <http://www.tbs-sct.gc.ca/pgol-pged/index-eng.asp>;<http://canada.gc.ca/depts/major/depind-eng.html>; <http://www.sciencedirect.com>; <http://laws.justice.gc.ca>; <http://www.cse-cst.gc.ca>; <http://sage-geds.tpsgc-pwgsc.gc.ca>; <http://www.parl.gc.ca>.

CAPÍTULO 1 – ANTECEDENTES DO GOVERNO ELETRÔNICO

Os antecedentes que levaram ao surgimento do Governo Eletrônico serão elucidados, a seguir, para embasar o propósito da dissertação de fazer um estudo comparativo da regulamentação sobre a política de segurança da informação entre os Governos Eletrônicos Federais do Brasil e Canadá.

1.1. Estado Democrático de Direito

O Estado apresentado como Estado Democrático de Direito surgiu na Grécia Antiga e passou por várias transformações, principalmente com o advento do Estado Moderno na segunda metade do século XV. Transformações significativas ocorreram com a revolução industrial (1750-1950) e a revolução pós-industrial (1950-atual). Esta última conhecida por revolução tecnológica, que transformou a sociedade industrial em sociedade do conhecimento.

Em cada período, os Estados mantiveram documentos arquivados em diferentes contextos. Segundo Robert-Henri Bautier[3] (1963, citado por MUNDET, 1994; TALLAFIGO, 1994) a evolução dos arquivos é dividida em quatro períodos: arquivos de palácio, que correspondem à Antigüidade; arquivos de cartórios, compreendendo os séculos XII a XVI; arquivos como arsenal de autoridade, que se estende do século XVI ao século XIX; e, arquivos como laboratório da história, início do século XIX a meados do século XX.

A partir do século XX, os arquivos abriram-se à administração, aos cidadãos e aos pesquisadores de diferentes áreas e, à frente desses, foi necessária a presença de profissionais preparados a responder às expectativas e necessidades dos usuários que buscam informações para a elaboração de seu trabalho (CALDERON *et al*, 2004) e de seu interesse.

A partir da revolução tecnológica, em 1950, houve um grande avanço das tecnologias de informação e comunicação (TIC), que possibilitaram ao Estado rever, alterar, aperfeiçoar e/ou modificar seu *modus operandi* no campo institucional.

[3] BAUTIER, Robert-Henri. *La phase cruciale de l'histoire des archives: la constitution des dépôts d'archives et la naissance de l'archivistique (XVIe - début du XIXe s.).* ***Archivum,*** t. XVIII. Paris: Gallimard, 1968, p.139-149.

Por ser Estado de Direito, toda ação institucional deve se pautar no princípio da legalidade. Conforme Jacques Chevallier[4] (1990, citado por MACHADO, 2007), o princípio da legalidade traduz-se em três significados:

> a) ninguém pode ser obrigado a fazer ou deixar de fazer algo senão em virtude de lei;
> b) todas as autoridades incumbidas de aplicar o direito e os próprios órgãos que o elaboram estão sujeitos à lei; e
> c) contra os atos das autoridades que, independentemente ou contra disposição legal contendam com interesses alheios, existe recurso que protege os direitos individuais. (MACHADO, 2007, p. 05)

Mediante essa análise, pode-se concluir que o princípio da legalidade e o fundamento do Estado de Direito é fundamental, pois assegura aos indivíduos garantias normativas frente à atuação estatal. Além disso, garante a separação das funções do poder estatal, determinando as regras das atividades administrativas, de modo que todo ato administrativo deve ser expressamente previsto na hipótese normativa. E consoante Sulamita Crespo Machado (2007:06) "o Direito sempre precede o ato da Administração Pública".

O governo eletrônico se desenvolveu, primordialmente, por meio de Estados de Direito, que têm como função pública, de acordo com Celso Antônio Bandeira de Mello (2003, p. 27), "a atividade exercida no cumprimento do dever de alcançar o interesse público, mediante o uso dos poderes instrumentalmente necessários conferidos pela ordem jurídica". Ressalte-se que várias evoluções tecnológicas ocorreram em períodos de Guerras e de Ditaduras, nos quais haviam Estados de Direito, mas não Democráticos.

O computador foi criado durante a Segunda Guerra Mundial, e inserido no Brasil na década de 1960, antes e durante o período de ditadura militar (1964-1985). Nessas épocas, as atividades estatais se deram por meio de instrumentos autorizados pelo Estado de Direito, tendo como subjacente a inspiração de realizar o interesse público.

Nesse contexto, foi desenvolvido o governo eletrônico para atender melhor às funções do Estado na sociedade atual, conhecida como a sociedade do conhecimento.

1.2. Sociedade do Conhecimento

A sociedade atual possui várias denominações: sociedade em rede, sociedade cibernética, sociedade da informação, sociedade do conhecimento, sociedade tecnológica etc.

---

[4] CHEVALLIER, Jacques. *La dimensión symbolique du principe de legalité*. In: ***Revue du Droit Public***, 1990, n. 6, p. 1651-1677.

Para fins dessa dissertação, será utilizada a denominação sociedade do conhecimento pelo entendimento que será exposto, pautando-se nos autores Manuel Castells (2003) e Pierre Lévy (1999).

Na visão de Manuel Castells (2003), o modo de desenvolvimento das sociedades é definido pelo elemento fundamental à promoção da produtividade no processo produtivo:

> No modo agrário de desenvolvimento, a fonte de incremento do excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em particular a terra) no processo produtivo, bem como na dotação natural desses recursos.
> No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivos e de circulação.
> No novo modo informacional de desenvolvimento, a *fonte* (grifo nosso) de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos.
> O industrialismo é voltado para o crescimento da economia, isto é, para maximização da produção; o informacionalismo visa o desenvolvimento tecnológico, ou seja, a acumulação de conhecimento e maiores níveis de complexidade do processamento da informação (CASTELLS, 2003, p. 53).

Conhecimento e informação são elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processamento da informação. Contudo, o que é específico ao modo de desenvolvimento informacional é a influência de conhecimentos sobre os próprios conhecimentos como principal *fonte* de produtividade (CASTELLS, 2003).

De acordo com Pierre Lévy (1999) uma técnica é produzida dentro de uma cultura, e uma sociedade encontra-se condicionada por suas *técnicas*, e não determinada por ela. Para o autor, não há uma causa identificável para o estado de fato social, mas um conjunto infinitamente complexo e parcialmente indeterminado de processos de interação de *técnicas* que se auto-sustentam ou se inibem. A *técnica* condiciona por gerar possibilidades, mas nem todas são aproveitadas – as *técnicas* não são boas, ruins ou neutras, dependem apenas do contexto que se inserem. Assim a *técnica* não determina o tipo de sociedade, pois nem sempre é utilizada em todas as culturas da mesma forma.

A partir do entendimento dos autores, foi formulada uma nova compreensão para interpretar a sociedade atual. Manuel Castells (2003) disserta sobre a Sociedade em Rede e Pierre Lévy (1999) sobre Cibercultura. Ambos possuem entendimentos semelhantes a respeito dos acontecimentos atuais na sociedade, porém com nomenclaturas diferentes e com significados conexos.

Em vista disso, cria-se uma nova interpretação, correlacionando os termos empregados pelos autores. Para fins dessa interpretação, o modo de desenvolvimento informacional ocorre

na sociedade do conhecimento e a sua *fonte* de produtividade é vista como a *técnica* de produtividade que condiciona a sociedade:

a) Se no novo modo informacional de desenvolvimento, a *fonte* de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos, conclui-se que a *técnica* da produtividade que condiciona sociedade do conhecimento é a tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos.
b) Se o que é específico ao modo de desenvolvimento informacional é a influência de conhecimentos sobre os próprios conhecimentos como principal *fonte* de produtividade, conclui-se que a sociedade do conhecimento é condicionada especificamente pela *técnica* de produtividade de influência de conhecimento sobre conhecimento.

Na sociedade do conhecimento a técnica de produtividade é a tecnologia associada à influência de conhecimento sobre conhecimento, ou seja, a transmissão e criação de conhecimentos entre os membros da sociedade por meio de inovações tecnológicas. Esse fato liga-se ao conceito de capital humano, e interpretando os autores Manuel Castells (2003) e Pierre Lévy (1999), conceitua-se capital humano.

Capital humano é entendido como a capacidade do membro da sociedade processar, transformar dados e/ou informações em conhecimento e transmiti-lo. O material utilizado (dado e/ou informação) é processado e transformado em produto (conhecimento) que pode ser processado e compartilhado por outros membros. Estes, por sua vez, podem transformar esse produto em novos produtos e compartilhá-los com os demais membros e assim por diante. Essa técnica de influência de conhecimento sobre conhecimento associada à tecnologia gera possibilidades, que poderão ser aproveitadas ou não, ocasionando o estado de fato da sociedade do conhecimento.

Isso se deve à possibilidade atual de um indivíduo ter acesso num só dia a um número de informações que um sujeito teria em toda sua vida na Idade Média (LUCCI, 2003). Por isso é necessário saber como compartilhar e usufruir esses produtos, para aumentar o conhecimento e não restringi-lo apenas em benefício próprio. Contudo, ao indivíduo é dado o direito de usar o conhecimento em benefício próprio, o compartilhamento é uma opção. É necessário haver liberdade de pensamento e de expressão para que tal ocorra, como direito e como elemento de cultura pessoal e organizacional. Há também o papel das instituições, na produção, preservação e comunicação dos produtos, na democratização do conhecimento.

Esses produtos ocasionam modificações na sociedade, e oferecem novas oportunidades e descobertas em desenvolvimento tecnológico. As modificações refletem as ações do Estado, que precisam se adequar e se aperfeiçoar às novas técnicas. No entanto, essas modificações são dinâmicas e o Estado não consegue se adequar e aperfeiçoar rapidamente às novas técnicas. Uma dessas modificações foi o nascimento do governo eletrônico nos Estados Democráticos de Direito e Estados Autoritários, sendo um fator estratégico para a construção de um novo modelo de gestão pública da informação, embasado em capital humano e tecnologia.

1.3. Tecnologia

Harvey Brooks[5] (1971, citado por CASTELLS, 2003, p. 67) entende a tecnologia como "o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível".

Na sociedade do conhecimento a tecnologia prevalecente é a tecnologia de informação e comunicação (TIC). Esta é entendida como a solução ou conjunto de soluções sistematizadas baseadas no uso de métodos, recursos de informática, de comunicação e de multimídia que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, e a subsidiar processos que convertem dados e informação (BEAL, 2005).

Dentre as tecnologias de informação e comunicação (TICs), incluim-se o conjunto convergente de tecnologias em microeletrônica (transistor), computação (*software e hardware*), telecomunicações/ radiodifusão, e optoeletrônica, além da engenharia genética e seu crescente conjunto de desenvolvimentos e aplicações.

1.4. A Revolução Tecnológica

O que caracteriza a atual revolução tecnológica é a aplicação de conhecimentos para geração de novos conhecimentos em um ciclo de realimentação cumulativo desse processo produtivo (CASTELLS, 2003), que alia tecnologia ao capital humano.

A revolução tecnológica se consolidou durante a Segunda Guerra Mundial e no período seguinte em que se deram as principais descobertas tecnológicas em eletrônica: o

[5] Harvey Brooks. *Technology and the ecological crisis.* Palestra proferida em Amherst, 9 de maio de 1971.

primeiro computador programável e o transistor – fonte da microeletrônica. Ressalte-se, entretanto, que algumas técnicas em microeletrônica eram observadas anos antes da década de 1940, como a invenção do telefone por Alexander Graham Bell, em 1876; da lâmpada elétrica por Thomas Alva Edison, em 1879; do rádio por Guglielmo Marconi, em 1898; e da válvula a vácuo por Lee De Forest, em 1906 (CASTELLS, 2003).

1.4.1. Computador

O computador nasceu com a Segunda Guerra Mundial, nos Estados Unidos. A Marinha em conjunto com a Universidade de Harvard e a IBM (*International Business Machines*) desenvolveram em 1944 o Mark I, um gigante eletromagnético que ocupava 120 m³ (SOFTWARELivre.Org., 2003).

Posteriormente, houve avanços tecnológicos utilizados para a fabricação de computadores, subdivididas por gerações. A primeira geração foi marcada em 1946 com a criação do ENIAC (*Electronica Numeral Integrator and Computer*), pelo físico John Mauchly e pelo engenheiro eletricista John P. Eckert, da Universidade da Pensilvânia, Estados Unidos. Foi o primeiro computador a usar eletrônica digital (SPACEBlog, 2007).

A segunda geração surgiu com o desenvolvimento de transistores (semicondutor ou *chip*) em 1947, inventado pelos físicos Bardeen, Brattain e Shockley (ganhadores do Prêmio Nobel pela descoberta). Possibilitou a codificação da lógica e da comunicação com e entre as máquinas, sendo o primeiro computador transistorizado o TRADIC (*Transistor Digital Computer*), do *Bell Telephone Laboratories*, em Murray Hill, Nova Jersey, Estados Unidos (CASTELLS, 2003). A terceira geração ocorreu em 1957 com a introdução dos circuitos integrados por Jack Kilby, engenheiro da *Texas Instruments* (que o patenteou) em parceria com Bob Noyce[6]. O avanço da microeletrônica ocorreu em 1971 quando o engenheiro da Intel, Ted Hoff, Vale do Silício, Estados Unidos, inventou o microprocessador, que é o computador em um único *chip* (CASTELLS, 2003).

A quarta geração (1981-1990) adveio com os *chips*, técnica dos circuitos LSI (*Large Scale Integration*) e VLSI (*Very Large Scale Integration*). Desenvolveu-se também o processamento distribuído, o disco ótico e o microcomputador, que passou a ser utilizado para

[6] Essa iniciativa acionou uma explosão tecnológica: em apenas três anos, entre 1959 e 1962, os preços dos semicondutores caíram 85%, e nos dez anos seguintes a produção aumentou vinte vezes, sendo que 50% dela foi destinada a usos militares. A título de comparação histórica, levou setenta anos (1780-1850) para que o preço do tecido de algodão caísse 85% na Inglaterra durante a Revolução Industrial (CASTELLS, 2003, p. 77).

processamento de texto, cálculos auxiliados etc. A quinta geração (1991-até hoje) utiliza sistemas especialistas, sistemas multimídia (combinação de textos, gráficos, imagens e sons), banco de dados distribuídos e redes neurais. Características: simplificação e miniaturização do computador, melhor desempenho e maior capacidade de armazenamento (SPACEBlog, 2007).

1.4.2. A Construção de uma Rede de Computadores

Em 1962, iniciou-se a construção de uma rede de computadores que pudessem trocar informações no *Advanced Research Projects Agency* (Agência de Projetos e Pesquisa Avançada), ARPA, do Departamento de Defesa dos Estados Unidos, para impedir a tomada ou destruição do sistema norte-americano de comunicação pela União Soviética, em caso de guerra nuclear – período da chamada Guerra Fria.

Com o lançamento do primeiro satélite artificial, Sputnik, em fins da década de 1950, pela União Soviética, a ARPA empreendeu inúmeras iniciativas ousadas. Uma destas, desenvolvida por Paul Baran na *Rand Corporation* em 1960-1964, foi criar um sistema de comunicação invulnerável a ataques nucleares. Com base na tecnologia de comunicação da troca de pacotes, o sistema tornava a rede independente de centros de comando e controle, para que a mensagem procurasse suas próprias rotas ao longo da rede, sendo remontada para voltar a ter sentido coerente em qualquer ponto da rede (CASTELLS, 2003).

Para realizar o primeiro experimento com a rede, foram escolhidas quatro universidades (Universidade da Califórnia em Los Angeles, *Stanford Research Institute*, Universidade da Califórnia em Santa Bárbara e Universidade de Utah) que seriam conectadas em janeiro de 1970 na rede computacional ARPANET (ARPA *Network*), além da comunidade militar norte-americana (MANDEL *et al*, 1997).

A rede de computadores foi conseqüência de uma difusão singular estratégica militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural. O resultado foi uma arquitetura de rede que não pudesse ser controlada a partir de nenhum centro e é composta por milhares de redes de computadores autônomos com inúmeras maneiras de conexão (CASTELLS, 2003). Essa tecnologia digital permitiu o empacotamento de todos os tipos de mensagens, inclusive de som, imagens e dados, nessa rede capaz de comunicar seus nós sem usar centros de controles.

1.4.3. A Internet

O sucesso da ARPANET se propagou rapidamente a outras comunidades, que não possuíam contratos com o Departamento de Defesa dos Estados Unidos, mas desejavam participar da nova era das comunicações (MANDEL *et al*, 1997).

A certa altura, tornou-se difícil separar a pesquisa voltada para fins militares das comunicações científicas e das conversas pessoais. Assim, permitiu-se o acesso à rede de cientistas de todas as disciplinas e, em 1983, houve a divisão entre ARPANET, dedicada a fins científicos, e a MILINET (*Military Network*), orientada às aplicações militares. A *National Science Foundation* (NSF) também se envolveu na década de 1980 na criação de outra rede científica, a CSNET (*Computer Science Network*), e – em colaboração com a IBM – de mais uma rede para acadêmicos não-científicos, a BITNET (*Because It's Time Network*). Contudo, todas as redes usavam a ARPANET como espinha dorsal do sistema de comunicação (CASTELLS, 2003).

Posteriormente, com a proliferação das redes, o modelo e protocolos TCP/IP[7] emergiram como o padrão predominante da área, tornando mais fácil a interligação de redes independentes, resultando na chamada rede Internet (MANDEL *et al*, 1997), ainda sustentada pelo Departamento de Defesa norte-americano e operada pela NSF.

Nos anos intermediários da década de 1980, a rede ARPANET começou a mostrar sinais de fadiga. Dado o enorme interesse de toda a comunidade acadêmica na conexão à rede, a NSF criou a rede acadêmica NSFNET (*National Science Foundation Network*), que viria a absorver a ARPANET, desativada em 1990 (MANDEL *et al*, 1997).

Com as pressões comerciais, o crescimento de redes de empresas privadas e de redes cooperativas sem fins lucrativos, a NSF logo percebeu que a rede construída excederia rapidamente o seu interesse e o seu potencial de financiamento, e que, vencida a fase de introdução da rede Internet, esta poderia caminhar com seus próprios pés. Assim, em 1994,

---

[7] *Transmission Control Protocol* - Protocolo de Controle de Transmissão/ *Internet Protocol* - Protocolo de Interconexão. TCP/IP é um conjunto de protocolos de comunicação entre computadores que os identifica na rede. Pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. Dentro de uma rede TCP/IP, cada computador recebe um endereço IP único que o identifica na rede. Um endereço IP é composto de uma seqüência de 32 bits, divididos em 4 grupos de 8 bits cada. Cada grupo de 8 bits recebe o nome de octeto. O endereço IP é dividido em duas partes. É composto de dois protocolos. O IP cuida do endereçamento eletrônico - identifica a rede à qual o computador está conectado. O TCP cuida da transmissão dos dados e correção de erros - identifica o *host* (hospedeiro da página eletrônica – *observação nossa*). O segredo do TCP/IP é dividir a grande rede em pequenas redes independentes, interligadas por roteadores. Como (apesar de interligadas) cada rede é independente da outra, caso uma das redes pare, apenas aquele segmento fica fora do ar, sem afetar a rede como um todo (MORIMOTO, 2006).

ela anunciou que se retiraria em 1995 do financiamento da rede NSFNET. A rede Internet estava aberta para a exploração comercial e para o uso com fins lucrativos. Esta transição veio a ser conhecida como a "privatização" da Internet (MANDEL *et al*, 1997).

Para Mandel *et al* (1997), o principal responsável pela chegada da Internet no Brasil foi o professor Oscar Sala da Universidade de São Paulo. Este professor trouxe a rede BITNET para o Brasil, em fins de 1988, conectando a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) ao *Fermilab*[8] nos Estados Unidos, através de uma linha dedicada de velocidade 4.800 bps, alugada da Embratel.

1.4.4. A Privatização da Internet e suas conseqüências

Uma vez privatizada, a Internet não contava com nenhuma autoridade supervisora. Diversas instituições e mecanismos improvisados, criados durante todo o desenvolvimento da Internet, assumiram alguma responsabilidade informal pela coordenação das configurações técnicas e pela corretagem de contratos de atribuição de endereços da Internet (CASTELLS, 2003).

Atualmente, a função de coordenação internacional da Internet se dá por meio de acordos multilaterais de atribuição de endereços de domínios no mundo inteiro. Não existe alguma autoridade muito clara e indiscutível sobre a Internet, tanto nos Estados Unidos quanto no resto do mundo. Por falta de uma autoridade sobre a Internet, a entidade que a tem coordenado e registrado domínios é a Icann - *Internet Corporation for Assigned Names and Numbers*. Esta pertence ao Departamento de Comércio norte-americano e tem como característica interagir com participantes múltiplos: governos, iniciativa privada e terceiro setor. A coordenação e o registro de domínios se dão por meio de um consenso tácito, pela prática pioneira e reiterada da Icann, enquanto não houver uma autoridade clara sobre isso.

Assim, de acordo com Manuel Castells (2003), a ARPANET tornou-se a base de uma rede de comunicação horizontal global composta de milhares de redes de computadores. Essa rede foi apropriada por indivíduos e grupos do mundo inteiro e com todos os tipos de objetivos, bem diferentes das preocupações de uma extinta Guerra Fria, sem ter uma determinada autoridade comandando e coordenado a rede Internet.

---

[8] *Fermilab* (*Fermi National Accelerator Laboratory*) é um laboratório especializado em física de partículas de alta energia dos Estados Unidos.

1.5. A Rede Cibernética

A Internet criou uma interatividade entre os membros da sociedade do conhecimento, que resultou na participação ativa de transação de informações. É um espaço virtual que não substitui o real, mas multiplica as oportunidades para atualizá-lo (LÉVY, 1999).

Esse espaço é conhecido por muitos como ciberespaço. Pierre Lévy (1999, p.92) define-o como "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores". Essa definição inclui o conjunto de sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais[9] ou destinadas à digitalização.

Para Pierre Lévy (1999, p. 93) esse novo meio de comunicação "tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação (*sic*)". E continua "a perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do início do próximo século" (LÉVY, 1999, p. 93).

Nesse sentido, o ciberespaço é visto também como uma nova técnica de produtividade da sociedade do conhecimento.

1.6. A nova técnica

Toda a revolução tecnológica aliada à rede de computadores, mais especificamente à Internet (ou ciberespaço), foi gerada pela técnica de produtividade de tecnologia aliada à ação do capital humano (influência do conhecimento sobre conhecimento). Formaram-se novos produtos (computador, transistores, *chips* etc) que ocasionaram modificações na sociedade, e refletiram nas ações do Estado, como se deu com o advento do governo eletrônico, embasado em capital humano e tecnologia.

Manuel Castells (2003) observa que o que deve ser guardado para o entendimento da relação entre tecnologia e a sociedade do conhecimento é que o papel do Estado, seja interrompendo, seja promovendo, seja liderando a inovação tecnológica, é um fator decisivo no progresso geral, à medida que expressa e organiza as forças sociais dominantes em um espaço e uma época determinada.

A seguir, trata-se a respeito do governo eletrônico na sociedade do conhecimento.

[9] A codificação digital (zero e um) permite a utilização da informação virtual e condiciona o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo na Internet.

CAPÍTULO 2 – GOVERNO ELETRÔNICO

Por se tratar de um tema de estudo acadêmico relativamente recente, ainda há carência de pesquisas e bibliografias a respeito do assunto. E, em razão de se constituir em assunto de caráter multidisciplinar, o conceito de governo eletrônico pode apresentar diversas definições, conforme a perspectiva de estudo assumida. Para os fins desta dissertação, enfatizam-se os aspectos tecnológico, administrativo, social, político e jurídico.

2.1. Governo Eletrônico: e-Gov

O termo governo eletrônico (e-Gov) e suas especificidades decorreram de avanços tecnológicos, circunstâncias sociais, movimentos globais e locais, que aliam tecnologia e influência de conhecimento sobre conhecimento (CHAHIN *et al*, 2004).

Em relação aos avanços tecnológicos, houve a criação do microcomputador durante a Segunda Guerra Mundial, e dos transistores e da rede de computadores no período da Guerra Fria. No tocante às circunstâncias sociais e políticas, é certo que a Segunda Guerra Mundial, a Guerra Fria e a Globalização possibilitaram os avanços tecnológicos na pesquisa acirrada pelo controle e pela geração de informações. Um desses avanços tecnológicos foi a criação da rede de computadores pelo Departamento de Defesa do Estado Unidos para obter e transmitir informações em qualquer lugar, sem uma base central a fim de proteger suas informações contra as investidas da União Soviética, na época da Guerra Fria.

Quanto aos movimentos globais menciona-se a conexão de vários indivíduos em todo o mundo pela Internet, com a formação de grupos de pesquisa, discussão e entretenimento. E movimentos locais, como no Vale do Silício, nos Estados Unidos, onde pesquisadores desenvolveram os transistores, a rede de computadores, local propício para desenvolver tecnologias, haja vista a liberdade de pesquisa e as matérias-primas disponíveis na década de 1960 e posterior.

Houve também movimentos localizados em 1980, quando as concessionárias de telecomunicações, em especial as da Europa, impuseram outro protocolo de comunicação X.25[10] como padrão internacional. O mundo aproximou-se bastante de se dividir em redes

[10] X.25 é um conjunto de protocolos padronizado pela ITU (*International Telecommunication Union*) para comunicações de longa distância, que define como as conexões entre os dispositivos de usuários e dispositivos de rede são estabelecidas e mantidas (ITH, 2009).

não-comunicáveis, o X.25 e o TCP/IP, contudo, prevaleceu a capacidade de TCP/IP de adaptar-se à diversidade.

Mais especificamente, e abstraindo-se desse conjunto de fatores, o fato que marcou o surgimento do e-Gov como movimento mundial foi o lançamento do Mosaic – primeiro *browser*[11] que permitiu uma navegação fácil pela *World Wide Web*[12], em agosto de 1993. Foi criado por um grupo de estudantes de pós-graduação da Universidade de Illinois, nos Estados Unidos, que posteriormente lançou o *Netscape*[13] (CHAHIN *et al*, 2004).

Além disso, o movimento mundial do e-Gov se formalizou em janeiro de 1999, quando Al Gore, o então Vice-Presidente da República norte-americano, abriu o Primeiro Fórum sobre Reinvenção do Governo em Washington, com a presença de representantes de 45 países (CHAHIN *et al*, 2004).

Em meio a essas circunstâncias, abriram-se novas perspectivas para as atividades do aparato estatal tais como: tornar mais eficientes serviços já existentes, incorporar novos serviços, reduzir custos de operação dos serviços, tornar mais transparentes as ações e gastos públicos, possibilitar a participação dos cidadãos na fiscalização do Governo e propiciar o uso de meios eletrônicos pelos cidadãos para receber informações e serviços públicos.

Essas perspectivas foram e são aprimoradas e aperfeiçoadas pelo e-Gov e, com isso, afirmam a democracia e a garantia de direitos humanos, como o direito à informação, à educação, à saúde, ao trabalho etc. Como exemplos dessa afirmação, apontam-se os casos brasileiros:

1) Direito à informação: aprimorado nas páginas eletrônicas do e-Gov, nas quais o cidadão ao conectá-las, tem acesso a algumas informações em qualquer tempo e em qualquer lugar, antes não divulgadas ou divulgadas por outros meios eletrônicos limitados ao tempo e espaço (jornal, telefone, televisão).
2) Direito à educação: ampliado com o Ensino à Distância (EAD), criado pela Secretaria de Educação a Distância (Seed), do Ministério da Educação. Alia-se inovação tecnológica aos métodos didático-pedagógicos nos processos de ensino e aprendizagem, gerando novos conceitos e práticas nas escolas públicas brasileiras.
3) Direito à saúde: estendido no Portal Saúde do Ministério da Saúde, onde reúne informações sobre políticas e ações do Ministério para promover a saúde dos

[11] *Browser* - Palavra em inglês utilizada para designar os programas de navegação na Internet. Em português o termo que se deve empregar é Navegador. Dentre o mais conhecidos navegadores: Netscape, Internet Explorer, Mozilla Firefox (UFSCAR, 2009).
[12] WWW ou "*World Wide Web*" (Grande Teia Mundial), ou "Web". A Web é um sistema de informações na Internet que utiliza uma interface designada Hipertexto, usando recursos multimídia. *Ibidem*.
[13] *Browser* ou navegador de Internet.

diversos segmentos da população brasileira, e serviços do Sistema Único de Saúde (acesso integral, universal e gratuito).

4) Direito ao trabalho: no site do Ministério do Trabalho é possível encontrar serviços e informações de interesse dos cidadãos, sobre emprego, abono salarial, carteira de trabalho, leis trabalhistas etc.

Em correspondência a essas perspectivas, o acesso aos meios eletrônicos pelos cidadãos brasileiros é crescente[14], notadamente a Internet e o telefone fixo (mesmo com a crescente aquisição de telefones móveis). Os que possuem esses meios fazem movimentar o aparato estatal com algumas intervenções e cobranças dantes não realizadas, como criticar serviços pela Internet, pelo telefone, assistir às sessões plenárias dos Parlamentos, fiscalizar contas públicas pela Internet. São atitudes que, em tempos mais remotos, só eram possíveis a uma pequena parcela da população mais privilegiada em questões financeiras, sociais, políticas e/ou culturais. Ainda permanecem essas questões, entretanto, uma parcela que antes não tinha esse acesso ao Governo, foi inserida por meio desses meios eletrônicos.

Assim, o e-Gov pode ser usado como instrumento de controle social, e também como garantidor de direitos dos cidadãos na sociedade do conhecimento, requerendo a transparência dos atos administrativos e reivindicando pelos seus direitos à privacidade, liberdade, meio-ambiente, saúde, trabalho, educação, etc.

2.2. Conceito

Durante algum tempo, confundiu-se o termo governo eletrônico com a ampliação da prestação de serviços públicos utilizando os meios eletrônicos de informação e comunicação. Dentre esses meios, citam-se a Internet, os telefones celulares e fixos, os *pagers*[15] e a TV digital[16] (CHAIN *et al*, 2004).

Há vários entendimentos a respeito do que seja o e-Gov. Em sentido mais amplo, Ali Chain *et al* (2004, p. 58), entendem que o "e-Gov é mais que um governo informatizado. Trata-se de um governo aberto e ágil para melhor atender à sociedade (*sic*)".

---

[14] Ver item 2.8. Estudos sobre uso da Internet. p. 34.

[15] Aparelho pequeno de telecomunicação usado para receber e, em alguns casos, transmitir, sinais de alerta e pequenas mensagens.

[16] A TV digital brasileira foi oficialmente inaugurada em 2 de dezembro de 2007 na grande São Paulo. É uma nova tecnologia de transmissão de sinais de televisão, que proporcionará gratuitamente ao telespectador melhor qualidade de imagens e sons e uma série de novos benefícios, tais como ver televisão quando em deslocamento e interagir com os programas (DTV, 2009).

Em sentido mais estrito, Ferrer e Santos (2004, p. 05), conceituam o e-Gov como "o conjunto de serviços e o acesso a informações que o governo oferece aos diferentes agentes da sociedade civil por meios eletrônicos".

Outros autores, como Lenk e Traunmüllerv (2001), adicionam quatro perspectivas acerca de Governo Eletrônico, quais sejam:

> 1. A Perspectiva do Cidadão - visa oferecer serviços de utilidade pública ao cidadão contribuinte;
> 2. A Perspectiva de Processos - visa repensar o *modus-operandi* dos processos produtivos ora existentes no Governo, em suas várias esferas, tais como, por exemplo, os processos de licitação para compras (*e-procurement*);
> 3. A Perspectiva da Cooperação - visa integrar os vários órgãos governamentais, e estes com outras organizações privadas e não-governamentais, de modo que o processo decisório possa ser agilizado, sem perda de qualidade, assim como se evitando fragmentação, redundâncias etc. hoje existentes nas relações entre esses vários atores;
> 4. A Perspectiva da Gestão do Conhecimento - visa permitir ao Governo, em suas várias esferas, criar, gerenciar e disponibilizar em repositórios adequados, o conhecimento tanto gerado quanto acumulado por seus vários órgãos (LENK e TRAUNMÜLLERV, 2001, p. 63-74).

Já a Carta Iberoamerica de governo eletrônico[17], considera as expressões governo eletrônico e administração eletrônica como sinônimas, se analisadas como o uso das TICs[18] nos órgãos da Administração para melhorar a informação e os serviços oferecidos aos cidadãos, nortear a eficiência e a eficácia da gestão pública, e aumentar substancialmente a transparência do setor público e a participação dos cidadãos. Tudo sem prejuízo das denominações estabelecidas nas legislações nacionais (CLAD, 2007). Ou seja, não importa a denominação do e-Gov em cada país, mas o que é feito em torno do seu objeto.

Nesse sentido, conceitua-se e-Gov como uma forma de governar que incrementa as atividades do Poder Público, através de meios eletrônicos de informação e comunicação ao prestar serviços, informações e produtos aos cidadãos, em qualquer lugar e a qualquer momento, de modo a integrar todos os *stakeholders*[19] envolvidos com a esfera pública; além de repensar o *modus operandi* dos processos produtivos do Governo; integrar os vários órgãos governamentais, e estes com organizações privadas e não-governamentais para cooperação mútua; e criar, gerenciar e disponibilizar com liberdade, transparência e responsabilidade os conhecimentos tanto gerados quanto acumulados por seus órgãos.

---

[17] *A los efectos de la presente Carta Iberoamericana se entienden las expresiones de "Gobierno Electrónico" y de "Administración Electrónica" como sinónimas, ambas consideradas como el uso de las TIC en los órganos de La Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiência de la gestión pública e incrementar sustantivamente La transparencia del sector público y la participación de los ciudadanos. Todo ello, sin perjuicio de las denominaciones establecidas en las legislaciones nacionales* (CLAD, 2007).

[18] Tecnologias de informação e comunicação.

[19] *Stakeholders* são os indivíduos e/ou organizações que têm interesse em determinado assunto (CHAIN *et al*, 2004) e influenciam o cenário político, social, econômico, financeiro, cultural etc.

2.3. Governança Eletrônica

Recentemente o termo e-Gov vêm sendo aliado ao termo governança eletrônica, como uma forma de justificar que as ações do e-Gov não se limitam a simplesmente oferecer serviços e informações aos cidadãos. Ao conceito de governança eletrônica adicionaria essas ações à capacidade de articulação do Estado com os diversos agentes sociais (*stakeholders*) na consecução de interesses públicos.

Conforme Marcelo Barroso Campos (2004), o atual conceito de "governança", em inglês *governance*, relaciona-se com o modelo de exercício do poder, representa a capacidade de governar ou administrar o Estado, objetivando eficácia na implementação de políticas públicas. Envolve também o sistema de intermediação de interesses por meio da participação dos diversos agentes sociais no processo de elaboração, implementação e avaliação de políticas públicas.

Governança eletrônica contempla, entre outras atividades, todo o suporte digital para a elaboração de políticas públicas, para a tomada de decisões, para as *public choices*[20], para o *workgroup*[21], entre os vários gestores públicos de diferentes escalões e também a gestão dos recursos públicos, financeiros, humanos, informacionais e de conhecimento, patrimoniais e outros (CHAIN *et al,* 2004). Isso possibilitou a transformação no modo como o Estado recebe, armazena, e transmite a informação, e toma suas decisões.

2.4. Instrumento de transformação

Conforme o documento do Ministério do Planejamento, Orçamento e Gestão, "Oficinas de Planejamento Estratégico" – Relatório Consolidado do Comitê Executivo do Governo Eletrônico (MPOG, 2004), o e-Gov deve ser tratado como instrumento de transformação profunda da sociedade, pois há múltiplos papéis que o Governo pode desempenhar no processo de sua implantação. Dentre os papéis possíveis do e-Gov, têm-se:

1) Promotor da cidadania e do desenvolvimento: orientar suas ações pelas demandas dos cidadãos enquanto indivíduos e promover o acesso e a consolidação dos direitos da cidadania (acesso aos serviços públicos; à informação; ao usufruto do

[20] *Public choice* é um programa de pesquisas criado a partir dos anos 1960 pelo economista James M. Buchanan. Diferentemente da ortodoxia que associa o estudo econômico a problemas de alocação de recursos, esse programa é centrado na coordenação de atividades ou trocas que ocorrem nos mercados e no processo político. Em decorrência, a escolha de mecanismos decisórios (instituições) é trazida para o topo das preocupações analíticas do economista (MONTEIRO, 2007).

[21] Grupo de indivíduos que trabalham em conjunto para um objetivo comum.

tempo – economia de tempo e deslocamentos; a ser ouvido pelo governo; ao controle social dos agentes públicos; e à participação política).

2) Instrumento de mudança das organizações públicas: não se deve apenas reproduzir lógicas tradicionais de funcionamento, nem somente colocar serviços disponíveis na Internet, mas promover o acesso efetivo aos serviços públicos.
3) Promover a disseminação da TIC: contribuir para o desenvolvimento do país. Cabe à política do e-Gov eliminar a dependência de fornecedores de bens, serviços e licenças de *software*; estimular e promover o desenvolvimento de *software* e de novas tecnologias computacionais por entidades de pesquisa e empresas nacionais; e fomentar a adoção de instrumentos de e-Gov pelos outros níveis de governo.
4) Disseminar práticas de Gestão do Conhecimento. Definição de Gestão do Conhecimento - conjunto de processos sistematizados que governam a criação, a captação, o armazenamento, o tratamento, a disseminação e a utilização de conhecimentos para atingir os objetivos institucionais. Torna-se instrumento estratégico para o desenvolvimento do país, ao se criar um novo perfil da função pública com: ética, produção compartilhada e colaborativa da informação e do conhecimento, e distinção clara entre o interesse público e o interesse individual.

De acordo com esses papéis que o e-Gov pode desempenhar ou já desempenha, torna-se possível a implementação de uma via de mão-dupla nas relações Estado-cidadãos por meio de novas TICs. Com isso, ter-se-ão nos cidadãos e nas suas organizações os parceiros mais importantes para definição do conteúdo de suas ações. Constitui-se em uma nova capacidade de articulação do processo decisório, de gestão das suas políticas estratégicas e de inclusão de um novo produtor de conhecimento geralmente esquecido: a sociedade e suas organizações.

2.5. Forma de governar

Didaticamente, as formas de governar do e-Gov são divididas em G2C (Governo relacionado com cidadão), G2B (Governo relacionado com fornecedores) e G2G (Governo relacionado com Governo). O G2G pode ser subdividido em relações horizontais (dentro de órgãos e agências de um nível de federação e entre eles) e verticais (entre órgãos e agências de diferentes instâncias da federação – União, estados, regiões, municípios).

No sentido inverso, da sociedade relacionada com o Governo – B2G (fornecedores relacionados com Governo) e C2G (cidadãos relacionados com Governo) – alcança uma

dimensão que não tem paralelo no mundo empresarial. Representa a participação da sociedade na formulação de políticas públicas e no exercício do controle social.

2.6. Transparência e *Accountability*

Desde os primórdios a transparência, que advém do princípio da publicidade, era questionada como forma de controlar os atos dos governantes em benefício dos cidadãos (que poderiam ser classes, grupos, ou população como um todo). Com o surgimento do e-Gov, este se apresentou como mais uma possibilidade de tornar transparentes os atos dos governantes e efetivar o controle social.

O controle social deve possibilitar ao cidadão informações que confiram transparência à gestão da coisa pública. Conforme Ticoll & Tapscott (2004, p. 75) "o acesso à informação de boa qualidade é um pré-requisito para o exercício da cidadania e condição essencial para que os problemas socioeconômicos sejam debatidos e resolvidos no convívio democrático". Para os autores, a transparência administrativa significa o acesso crescente à informação pelos *stakeholders* sobre toda e qualquer faceta das decisões administrativas, a fim de assegurarem a eficiência e efetividade dentro de preceitos da democracia.

Uma denominação bastante utilizada para esse fenômeno é a *accountability.* É um termo traduzido do inglês como imputabilidade, responsividade, responsabilidade na prestação de contas de recursos públicos. Desta forma, o mecanismo de controle social deve-se pautar na *accountability*, ou seja, uma nova denominação para situações que vem se perpetuando nos Governos, que é a obrigação de atos governamentais responsáveis.

Para Ali Chain *et al* (2004, p. 50), *accountability* é "a obrigação que tem aquele que administra os recursos públicos de prestação de contas de sua gestão e da possibilidade de ser responsabilizado pelo que fez". É a obrigação que os agentes do Estado têm em responder por suas decisões, ações e omissões, isto é, prestar contas dos resultados conseguidos em função da posição que ocupam.

Consoante Marcelo Barroso Campos (2004):

> A *accountability*, como atributo do princípio da publicidade insculpido no art. 37, *caput*, da Constituição de 1988, envolve a questão da legitimidade e é instrumento básico necessário para se concretizar o controle social, pois a participação dos atores sociais na gestão da *res* pública denota que nem tudo o que é público é somente estatal. Há espaço público não-estatal que deve ser preenchido pelos atores sociais em harmonia com o Poder instituído e com a iniciativa privada, para a integração dos interesses envolvidos (CAMPOS, 2004, p. 29).

Isso possibilita a participação dos agentes sociais (*stakeholders*) no processo de elaboração, implementação e avaliação das políticas públicas a fim de efetivar o controle social. Não se trata de promover o discurso vazio de "transparência", mas de promover a apropriação dos recursos de relacionamento entre governo e sociedade por meio de novas TICs. Se o discurso de responsabilidade é antigo, sua forma de expressão tornou-se mais abrangente com as novas possibilidades oriundas de TICs.

Cabe ressaltar que qualquer atuação pública se dá por meio do princípio da responsabilidade, que informa toda ação humana; do contrato social, em respeito ao pacto público, para garantia da liberdade e da igualdade entre os indivíduos; da separação dos poderes, em atenção à necessidade de limitar o poder; e, do constitucionalismo, para proteção dos direitos fundamentais.

Ainda há baixo nível de *accountability* na União, nos estados da Federação e nos municípios, porém, algumas práticas eletrônicas no Brasil demonstram a sua ocorrência. Nos portais eletrônicos da União, de estados e municípios nascem novas formas de comunicação com a sociedade e a autoridade máxima do Poder Executivo. É o caso do "Fale com o governador" ou "Fale com o prefeito". Outras ocorrências são os incentivos ao cidadão a exercer sua cidadania, a divulgação do orçamento participativo, a criação e a divulgação de locais de acesso público à Internet e a adoção de políticas que assegurem o acesso à Internet aos portadores de necessidade especial (CHAIN *et al*, 2004).

Pela possibilidade de controle social sobre o Governo ser ampliada pelo e-Gov, há que se ressaltar que a transparência e a *accountability* (responsabilidade) devem nortear a política de segurança da informação. A classificação dos ativos da informação (ver Capítulo 3, p. 41) deve ser bem elaborada para se evitar que informações sigilosas tornem-se públicas, ou que informações que deveriam ser públicas tornem-se sigilosas e, com isso, impedir o controle social e a responsabilização do agente público.

2.7. Aplicação do Governo Eletrônico

Os Governos dos Estados Democráticos de Direito, como Brasil[22], Canadá[23], Estados Unidos[24], Reino Unido[25], México[26], Cingapura[27], Coréia do Sul[28], Austrália[29], dentre outros,

[22] e-Gov Brasil: <http://www.governoeletronico.gov.br>.
[23] e-Gov Canadá: <www.canada.gc.ca>.
[24] e-Gov EUA: <http://www.firstgov.gov>.
[25] e-Gov Reino Unido: <http://www.ukonline.gov.uk>.
[26] e-Gov México: <http://www.e-mexico.gob.mx> (possui convênio com Canadá para aprimorar seu e-Gov).

vêm se amoldando ao e-Gov e ao mecanismo de *accountability* (responsabilidade), notadamente com criação do primeiro computador em 1944. Esses Governos atualizaram e implantaram sistemas de gestão informacionais por meio do computador, pois este, diferentemente de outras tecnologias anteriores, abarca um número maior de opções de armazenamento, distribuição, uso, cálculo, logística e distribuição de dados e informações.

Outro fator de amoldamento foi a criação da rede de computadores em 1967 e da Internet na década de 1980, sendo impulsionado seu uso em 1995, com sua liberação comercial para toda a sociedade civil e não mais apenas para os militares e pesquisadores de universidades.

Apesar dessas adaptações feitas nos Estados Democráticos de Direito e também nos Estados Autoritários, há o problema da ineficiência, da falta de recursos e dos altos custos, resultante da estagnação da hierarquia e da formalidade burocráticas. Esse fato resultou no redimensionamento da relação cidadão-Estado, com a cooperação entre as organizações estatais e a parceria com o setor privado (MACHADO, 2007).

De acordo com Sulamita Crespo Machado (2007), a década de 1980 mostra-se como a década da nova Administração Pública, da sua modernização, seguida pela década de 1990, a década das reformas. Objetivava-se mudar a forma de governar e administrar. No México houve a disposição eletrônica de informações. Na Coréia do Sul, o sistema eletrônico de requerimentos. No Japão, a redução do número de funcionários civis. Na Austrália e Canadá, identificação de falhas por usuários. No Brasil, debates sobre a modernização, a consideração dos preceitos da administração privada, do modelo gerencial e da responsabilidade por resultados, baseados nos países anglo-saxônicos. Na França e Noruega, observa-se a satisfação dos cidadãos, por meio de um diálogo democrático, numa relação transparente e responsável. Na Alemanha, a satisfação das necessidades e expectativas dos cidadãos integram a noção de gerenciamento eficiente. Há busca pela eficiência interna (meios) e externa (beneficiados).

Com isso, os Governos citados acima começaram a disponibilizar informações e serviços aos cidadãos pela Internet, além de inovar sua atuação com a democracia participativa (consultas públicas virtuais), e a transparência das contas públicas na Internet. Essas possibilidades de atuação já existiam antes do computador e da Internet. Entretanto,

---

[27] e-Gov Cingapura: <http://www.e-citizen.gov.sg> e <http://www.gov.sg/>.
[28] e-Gov República da Coréia: <http://www.egov.go.kr> ou <http://info.egov.go.kr/pa/html/eng_main.htm>.
[29] e-Gov Austrália: <http://autralia.gov.au>.

com estes, ela foi ampliada, e, para se adequar e se inserir no campo da tecnologia virtual, o Estado regulamentou ou desregulamentou alguns aspectos de seu *modus operandi*.

Dentre os serviços públicos prestados pelo e-Gov, citam-se os serviços nos quais o Brasil é líder mundial: eleições eletrônicas, Sistema Brasileiro de Pagamentos, e Receita Federal, com declarações de imposto de renda de pessoas física e jurídica (IRPF e IRPJ) entregues pela Internet. Outros serviços públicos e informações prestadas pelo e-Gov brasileiro são: informações sobre programas do governo federal; divulgação de editais de compras governamentais; prestação de informações sobre aposentadorias e benefícios da Previdência Social; emissão de certidão de pagamentos de impostos; e acesso aos indicadores econômicos e sociais e aos dados dos censos (GOV.br, 2007).

Apesar de haver alguma regulamentação das ações governamentais no e-Gov, o processo de divulgação de informações e apresentação de serviços na Internet apresenta-se desordenado, mesmo entre os países desenvolvidos. Isso tem feito com que a busca por uma gestão mais transparente se processe de modo desorganizado e não obedeça a um plano prévio. Algumas formas mais exitosas de organização estão presentes em alguns países como Canadá, Austrália, Irlanda, Nova Zelândia, Noruega, Suécia e Reino Unido (BNDES, 2000).

2.8. Estudos sobre uso da Internet

O acesso à Internet e a posse de telefone móvel celular para uso pessoal foi investigado em 2005, na Pesquisa Nacional por Amostra de Domicílios (PNAD). Esta pesquisa foi resultado de um convênio entre o Instituto Brasileiro de Geografia e Estatística (IBGE) e o Comitê Gestor da Internet no Brasil (CGI.br). O objetivo era ampliar o conhecimento sobre a utilização das TICs no País, para criar indicadores nacionais e comparar aos indicadores internacionais de estatísticas sobre a sociedade da informação (do conhecimento). Para tal, foram considerados em seu planejamento os indicadores-chave das TICs aprovados na Cúpula Mundial da Sociedade da Informação - *World Summit on the Information Society* – WSIS (IBGE, 2007).

Em março de 2007 foram divulgados os resultados: 32,1 milhões de brasileiros, cerca de 21,9% da população acima dos 10 anos de idade, utilizaram a Internet no país; e 36,7% tinham telefone móvel celular para uso pessoal (IBGE, 2007)[30]. Em contraponto, 71% da população adulta canadense acessavam a Internet, em 2003 (STATCAN, 2009)[31].

[30] IBGE. Disponível em: <http://www.ibge.gov.br/home/estatistica/ populacao/acessoainternet/comentarios.pdf>.
[31] STATCAN. Disponível em: <http://www41.statcan.gc.ca/2008/2256/ceb2256_000-eng.htm>.

O número divulgado coloca o Brasil como o primeiro país da América Latina e o quinto no mundo no uso da Internet. Se for considerado, no entanto, o número de internautas em relação à população do país, a situação relativa do país é bem diferente. Nesta avaliação, o Brasil ocupa a 62ª posição mundial e a quarta na América Latina, sendo ultrapassado pela Costa Rica, Guiana Francesa e Uruguai (ITU, 2003)[32].

Em novembro de 2003, a ITU (*Word Telecommunication Indicators*) elaborou estudo estabelecendo o Índice de Acesso Digital. Com base em dados de 2002, o levantamento classificou 186 países. Em relação ao Índice de Acesso Digital o Brasil ocupa a 65ª posição mundial e a 15ª posição nas Américas, enquanto o Canadá ocupa a primeira posição mundial. As classificações brasileiras nas categorias de infra-estrutura, preço de acesso, nível educacional, qualidade e utilização foram, respectivamente, 64º, 74º, 49º, 53º e 67º lugares (ITU, 2003).

Todavia, em alguns segmentos específicos, as aplicações de e-Gov brasileiras são líderes mundiais. A experiência da urna eletrônica, por exemplo, vem despertando o interesse de diversos países, como os Estados Unidos e Canadá. A entrega de declaração de imposto de renda via Internet é uma das mais avançadas, sendo que em 2007, 98% dos contribuintes brasileiros prestam contas ao fisco federal por meio da Internet (GOV.br, 2007)[33]. Em contrapartida, no Canadá, apenas 43% dos contribuintes utilizam esse instrumento (STATCAN, 2009).

Em vista disso, o ministro do Planejamento, Paulo Bernardo, apresentou as iniciativas de e-Gov brasileiras e a infra-estrutura de tecnologia do país na abertura do *Gtec Week* 2007, em Ottawa, Canadá. Dentre as iniciativas exitosas apresentadas tem-se: a declaração eletrônica do Imposto de Renda; o Sistema Nacional de Integração de Informações em Justiça e Segurança Pública (Infoseg); nota fiscal eletrônica; certificação digital; voto eletrônico; pregão eletrônico; Padrões e-Gov: e-PING – Padrões de Interoperabilidade de Governo Eletrônico e e-MAG – Modelo de Acessibilidade de Governo Eletrônico (GOV.br., 2007).

2.9. Governo Eletrônico: Canadá

O país que mais se destaca em termos de e-Gov é o Canadá, pois suas bases tecnológicas, estruturais e políticas foram construídas com o apoio e a contribuição de sua

[32] ITU. Disponível em: <http://www.itu.int/net/home/index.aspx>.
[33] GOV.br. Disponível em: <https://www.governoeletronico.gov.br/noticias-e-eventos/noticias/paulo-bernardo-abre-forum-no-canada-que-homenageia-e-gov-brasileiro/?searchterm=gtec>.

população. A maioria dos serviços públicos do Canadá são realizados pela Internet, evitando o deslocamento e o tempo que seriam necessários para se obter os mesmos serviços em órgãos da Administração Pública.

Desde 1999, o chamado *Government On-Line* (GOL) objetivou ser reconhecido como o e-Gov mais conectado aos cidadãos. Foi construído escutando opiniões dos cidadãos e respondendo com a entrega de serviços em formatos que ultrapassam as fronteiras organizacionais tradicionais entre departamentos ou governos (AGNER, 2007).

Para Thomas Riley (2007), um dos fatores do sucesso do e-Gov no Canadá é a entrega de serviços centrados no cidadão e não baseados na estrutura de departamentos existentes. Não trabalha com pressuposições, mas com a ajuda de pesquisas, consciente do processo de evolução do e-Gov, com investimentos em:

1. Políticas, padrões, legislação e critérios de privacidade;
2. Desenvolvimento de métricas de avaliação e programas de comunicação;
3. Desenvolvimento de equipes aptas a trabalhar com os novos serviços e interfaces;
4. Desenvolvimento de infra-estrutura tecnológica e redes padronizadas.

O Governo do Canadá evitou erros cometidos em diversos países por meio da liderança efetiva, do trabalho cooperativo, de prioridades bem-definidas, da identificação das necessidades do público e de investimentos em pessoal capacitado a atingir metas. Os erros têm sido reconhecidos e as mudanças realizadas (RILEY, 2007).

O Canadá ficou em primeiro lugar nas pesquisas anuais da *Accenture*[34] realizadas em 2000, 2001 e 2003, sendo conhecido desde 1999 como o Governo mais conectado aos seus cidadãos. A visão oficial do *Government On-Line* (GOL) canadense é que seus cidadãos tenham acesso a todas as informações e serviços do Governo *on line* no tempo e lugar de sua escolha (CHAHIN *et al*, 2004).

Nessas pesquisas o Brasil teve decréscimo do Índice de Desenvolvimento do e-Gov entre os anos de 2001 e 2002. No estudo, o País caiu do 9º para o 21º lugar no *ranking* mundial. Um dos motivos apontados para o fraco desempenho foram as eleições realizadas em 2002, que retiraram o foco dos investimentos governamentais das iniciativas de menor apelo eleitoral, como é o caso dos programas de e-Gov (AGNER, 2007).

[34]Empresa norte-americana de consultoria que elaborou um esquema sobre e-Gov no mundo em sua pesquisa anual. Acesse: <http://www.accenture.com/Countries/Brazil/default.htm>.

Em 2006, mais de 99% das famílias canadenses tinham serviços de telefonia fixa ou móvel; 68% das famílias tinham acesso à Internet em casa, a grande maioria, com alta velocidade de serviço em banda larga (STATCAN, 2009). Os canadenses são grandes usuários da Internet no que tange aos serviços governamentais. Três quartos dos canadenses estão *on-line* e, entre estes, mais da metade são usuários do e-Gov (RILEY, 2007).

A página oficial do e-Gov canadense é <http://www.canada.gc.ca>. É uma página bilíngüe, com as duas línguas oficiais: inglês e francês, onde se encontram todas as páginas dos órgãos governamentais. Toda a regulamentação canadense é encontrada no site *Department of Justice* (Ministério da Justiça) <http://canada.justice.gc.ca/eng/index.html>. Outras regulamentações podem ser encontradas nos órgãos da Administração Pública e nos sites do Senado e da Câmara dos Comuns.

Não foi encontrada regulamentação específica sobre o e-Gov do Canadá, como ocorreu no Brasil, pois naquele país o direito é baseado nos usos e costumes (*common law*), legislando apenas temas específicos, como Lei de Segurança da Informação, Lei de Privacidade, Lei Antiterror, Lei das Telecomunicações, Consolidação da Constituição de 1982 etc. No Brasil, o direito é baseado na tradição romano-germânico, no qual prevalece o direito regulamentado em normas escritas, e não pelos usos e costumes. Por isso, no Brasil serão encontradas mais normas escritas sobre o e-Gov e também por se ter maior facilidade em pesquisar normas no país de origem da dissertação.

2.10. Governo Eletrônico: Brasil

Devido à difusão de novos sistemas informacionais na Administração Pública, o Governo Federal, em 1995, criou o Comitê Gestor da Rede Internet no Brasil, pela Portaria Interministerial nº 147, 1995 (BRASIL, 1995), em Nota Conjunta pelo Ministério das Comunicações (MC) e pelo Ministério da Ciência e Tecnologia (MCT), para coordenar e incentivar a implantação daquela rede no país[35].

No ano de 1996, apesar de ainda não haver uma política específica, as atividades do e-Gov ocorriam de maneira esparsa e não integrada, decorrentes do emprego convencional dos recursos de TIC (MORAES, 2006).

[35] A Portaria Interministerial Conjunta CIVIL/MC/MCT nº 739, 2003 (BRASIL, 2003*f2*), dá nova redação aos arts. 2º e 3º da Portaria Interministerial MC/MCT nº 147, 1995 – apenas medidas administrativas. Ver APÊNDICE A, p. 144.

Em 1998, o MCT, juntamente com o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), discutiram a respeito de um programa sobre a nova Sociedade da Informação – ou do conhecimento (SOCIEDADE, 2004). Após um período de definições e articulações políticas, o programa foi instituído pelo Decreto n° 3.294, 1999 (BRASIL, 1999*k1*).

Ao criar o Programa Sociedade de Informação (Socinfo), o Governo Federal teve como objetivo integrar, coordenar e fomentar ações para a utilização de TICs. Pretendeu-se, também, viabilizar a economia do país para que o mesmo tivesse condições de competir no mercado global e, ao mesmo tempo, contribuir na inclusão social de todos os brasileiros na nova sociedade da informação (MCT, 2002).

Em 2000, foi lançado o Livro Verde pelo MCT, conjugando esforços de vários colaboradores a respeito das TICs. É um programa que está estruturado em sete linhas de ação, a saber: mercado, trabalho e oportunidades; universalização de serviços para a cidadania; educação na sociedade da informação; conteúdos e identidade cultural; Governo ao alcance de todos; incentivo à pesquisa e desenvolvimento, tecnologias-chave e aplicações; infra-estrutura avançada e novos serviços (LIVRO, 2000).

Ainda no ano 2000, o Governo Federal lançou as bases para a constituição do e-Gov em consonância com a recente sociedade de informação, atualmente conhecida como sociedade do conhecimento.

Com base na atuação coordenadora e mobilizadora, empreendida pela Presidência da República, com apoio técnico e gerencial da Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão (MPOG), o Governo criou o Grupo de Trabalho Interministerial em Tecnologia da Informação (GTTI). Este Grupo tem como finalidade examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação (GOVERNO, 2005), através do Decreto Presidencial s/nº de 03 de abril de 2000 (BRASIL, 2000*j4*).

As ações deste Grupo, formalizado pela Portaria da Casa Civil n° 23, 2000 (BRASIL, 2000*j7*), coadunaram-se com as metas do Programa Sociedade da Informação, coordenado pelo MCT. Por orientação do Governo Federal, o trabalho do GTTI concentrou esforços em três das sete linhas de ação do Programa Sociedade da Informação: universalização de serviços, governo ao alcance de todos e infra-estrutura avançada.

Em outubro de 2000, o Governo criou o Comitê Executivo do Governo Eletrônico (CEGE) no âmbito do Conselho do Governo pelo Decreto s/nº de 18 de outubro de 2000 (BRASIL, 2000*j2*), com o objetivo de formular políticas, estabelecer diretrizes, coordenar e

articular as ações de implantação do Governo Eletrônico, voltado para a prestação de serviços e informações ao cidadão, sendo apresentada a "Política de Governo Eletrônico", baseada na transparência democrática.

Para entender melhor o que seria uma "Política de Governo Eletrônico", busca-se a definição de e-Gov idealizada pelo grupo de estudo de Iniciação do Governo Eletrônico, o *Gartner Group*[36]. Este grupo define o e-Gov como sendo "a contínua otimização da prestação de serviços do Governo, da participação do cidadão e da administração pública pela transformação das relações internas e externas através da tecnologia, da Internet e dos novos meios de comunicação" (EINSENBERG; CEPIK, 2002, p. 104).

A página oficial do e-Gov brasileiro é <http://www.governoeletronico.gov.br/>. No portal do e-Gov <http://www.e.gov.br/> é onde se encontram todas as páginas dos órgãos governamentais. A maior parte da regulamentação brasileira é encontrada no site da Presidência da República <http://www.presidencia.gov.br/legislacao/>. Outras regulamentações podem ser encontradas nos órgãos da Administração Pública e nos sites do Senado e da Câmara dos Deputados.

Anteriormente à implantação da política de e-Gov, o Governo Federal criou o Decreto n° 3.505, 2000 (BRASIL, 2000*j3*), por meio do qual foi instituída a política nacional de segurança das informações. Com este ato normativo, o governo brasileiro atentou para a necessidade de proteção de assuntos que mereçam tratamento especial, adotando medidas para prevenir o risco de vulnerabilidade[37] dos sistemas de gestão da informação.

Em 2006 foram criadas cartilhas sobre a segurança da informação e a Internet pelo CERT.br[38] – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. A Cartilha de Segurança para Internet[39] contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

---

[36] *Gartner Group*, empresa norte americana especializada em consultoria para utilização da tecnologia da informação, elaborou em 2003 para o governo federal dos Estados Unidos um plano de ação para e-Gov.

[37] As "vulnerabilidades determinam o grau de exposição de um ativo da informação, ambiente ou sistema a determinada ameaça" (BEAL, 2005, p. 18).

[38] O CERT.br é o grupo de resposta a incidentes de segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. O CERT.br é responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O NIC.br – Núcleo de Informação e Coordenação do Ponto BR (Brasil) – é uma entidade civil, sem fins lucrativos, que desde dezembro de 2005 implementa as decisões e projetos do Comitê Gestor da Internet no Brasil (CERT.br, 2009).

[39] A Cartilha pode ser encontrada em: <http://cartilha.cert.br/>.

CAPÍTULO 3 – GOVERNO ELETRÔNICO E SEGURANÇA DA INFORMAÇÃO

De acordo com o princípio da legalidade, só é permitido ao Estado de Direito fazer o que a lei determina. Cabe, portanto, ao Estado legislar seu modo de ação, para delimitar seus atributos, seja governamental, seja administrativamente no campo da tecnologia virtual.

Nesse sentido, um dos pontos relevantes para o Estado diz respeito à política de segurança da informação (PSI) na Internet. Para assegurá-la e proteger o ambiente tecnológico, o Estado deve atuar de acordo com as normas precedentes a esse respeito, além de legislar as novas modalidades de atuação.

A obediência a requisitos de segurança da informação é imprescindível num relacionamento eletrônico que envolva informações individualizadas e transações financeiras, como a nova geração de serviços oferecida pelos sites governamentais. O Governo deve investir nessa área, pois o conhecimento técnico envolvido exige especialização. De acordo com Ali Chain *et al* (2004, p. 71), "sem a instalação de procedimentos de segurança, é melhor não oferecer o relacionamento eletrônico, não expor as informações à quebra de privacidade nem a infra-estrutura de informática a visitantes indesejados e aos diversos tipos de invasão".

Esse raciocínio deve ser observado pelos Governos na implantação e continuação do e-Gov, pois se não houver uma adequada política de segurança de informação (PSI), todo o seu aparato estatal correrá risco de ser alterado ou destruído. Deve-se, portanto, resguardar seus ativos de informação, pois são essenciais para o funcionamento da máquina pública e de qualquer organização que necessite dessa proteção.

3.1. Gestão da Informação

A gestão das informações nos Governos provoca ajustes em seus *modus operandi*, não apenas na busca da informação, mas principalmente no uso que se faz dela por meio de seu gerenciamento. Alguns autores como McGee e Prusak (1994), Adriana Beal (2004), Chun Wei Choo (2003), e Thomas Davenport (1998) apresentam modelos genéricos para o processo de gerenciamento da informação.

Para McGee e Prusak (1994) um modelo de gerenciamento da informação deve ser genérico porque a informação recebe diferentes ênfases na organização e ainda porque dentro do modelo, as diferentes tarefas podem assumir diferentes níveis de importância e valor entre

as organizações. O modelo identifica as necessidades e requisitos de informação até a análise e uso da informação.

Adriana Beal (2004) apresenta um modelo de gerenciamento da informação com sete etapas que correspondem ao ciclo de vida da informação: identificação das necessidades e dos requisitos da informação (repetido periodicamente); obtenção das informações (internas e externas); tratamento da informação (acessível, organizada); distribuição da informação (a quem necessita); uso da informação (nos resultados pretendidos); armazenamento da informação (conservação para uso e reuso); descarte da informação (vida útil). Ressalte-se que o gerenciamento da informação não necessariamente envolve todas as etapas e as seqüências citadas.

Chun Wei Choo (2003) apresenta um modelo de uso da informação onde os ciclos de busca e uso da informação estão inseridos em três dimensões: no meio profissional/social, nas necessidades cognitivas e das reações emocionais. O modelo tenta identificar e relacionar os principais elementos que podem influenciar o comportamento daquele que busca e usa a informação. Apresenta ainda, uma estrutura onde o conceito de processo de uso da informação é dividido em três estágios: necessidade, busca e uso da informação.

De acordo com Thomas Davenport (1998) o gerenciamento da informação pode ser considerado como um conjunto estruturado de atividades que envolvem a forma como as organizações obtêm, distribuem e usam a informação e o conhecimento. O modelo proposto é composto de quatro passos: determinação das exigências, obtenção, distribuição e utilização da informação.

Os quatro modelos de gerenciamento da informação apresentados possuem processos, tarefas ou atividades relacionados, com o objetivo de fornecer as informações para os responsáveis pela gestão da informação no momento certo da tomada de decisões. Nesse sentido, ao se aplicar a gestão da informação nos Estados, adequações e aperfeiçoamentos de seu *modus operandi* são necessários, notadamente no gerenciamento dos ativos da informação com o surgimento de novas tecnologias e sua conseqüente PSI.

3.2. Ativo de Informação

Como qualquer outro ativo valioso para as organizações, as informações precisam ser gerenciadas e protegidas contra ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada.

O ativo de informação pode ser entendido como qualquer dado ou informação a que esteja associado um valor para a organização. Em sentido amplo, ativo da informação abrange as informações relevantes mantidas na mente de tomadores de decisão, em base de dados, arquivos de computador, documentos e planos registrados em papel etc. Além disso, abarca os componentes do patrimônio de TIC da organização: *hardware* e *software*, mídias de armazenamento e mecanismos de comunicação necessários para a execução de sistemas e processos de informação e comunicação (BEAL, 2005).

Não há uma padronização quanto à classificação da informação nas organizações. Contudo, do ponto de vista de seu conteúdo, ela pode ser dividido em três categorias:

> *Informações pessoais:* dados individuais de funcionários, clientes e outras pessoas, incluindo idade, endereço, número de telefone, peso, salário, histórico de compras ou de desempenho e preferências.
> *Informação de segurança nacional:* aquela que precisa ser protegida para garantir a segurança da sociedade e do Estado.
> *Informação de negócio:* utilizada pelas organizações para desempenhar sua missão. Ex.: informações financeiras, técnicas de marketing, planos e métodos de produção (BEAL, 2005, p. 59).

Essas classificações da informação são independentes e mutáveis, sendo que sua proteção é relevante para dar prosseguimento ao objeto da organização. Outras classificações podem ser enquadradas, dependendo do objeto da organização. Algumas informações, por natureza, têm requisitos de confidencialidade e devem ter seu sigilo preservado. Um exemplo está previsto no Decreto nº 4.553, 2002 (BRASIL, 2002*g2*), que classifica os documentos sigilosos em quatro categorias: ultra-secretos; secretos, confidenciais e reservados[40].

O gerenciamento e a proteção da informação normalmente envolvem investimentos de alto valor. Formas de armazenar, impedir o acesso indevido e recuperar informações em caso de falhas requerem investimentos. Se estes não são adequados para os diversos tipos de informação, de sistemas e processamentos de informação, pode acarretar enormes desperdícios de dinheiro, recursos e capacidade de processamento (BEAL, 2005). Gastam-se com tecnologias, mas não se preocupam com sua utilização e proteção.

A expressão *segurança da informação* é utilizada para indicar a proteção desses ativos de informação contra as ameaças a que estão expostas: tanto as informações mantidas em componentes de TICs, quanto às armazenadas na mente humana, num pedaço de papel ou em microfichas ou microfilmes.

[40] Ver Capítulo 5, item 5.3. Privacidade, p.86.

3.3. Segurança da Informação

Segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra: acessos não autorizados, alterações indevidas, indisponibilidade, repúdio e ilegalidade.

Consoante Adriana Beal (2005), a segurança da informação visa preservar ativos de informação, levando em conta três objetivos fundamentais:

> **Confidencialidade**: garantia de que o acesso à informação é restrito aos seus usuários legítimos.
> **Integridade**: garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados de informações. O objetivo de *autenticidade* da informação é englobado pelo de integridade, quando se assume que este visa a garantir não só que as informações permaneçam completas e precisas, mas também que a informação capturada do ambiente externo tenha sua fidedignidade verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo.
> **Disponibilidade**: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna (BEAL, 2005, p. 01).

Podem-se acrescentar mais dois objetivos fundamentais que são a legalidade e o uso legítimo. A legalidade é a garantia de que a informação foi produzida em conformidade com a lei. O uso legítimo é a garantia de que os recursos de informação são usados por pessoas autorizadas, o que também é determinado em lei, quando se trata de Administração Pública.

3.4. Segurança da Comunicação

Há também a necessidade de se estabelecer alguns objetivos adicionais relativos à segurança da comunicação[41], pois pode haver problemas na origem de uma comunicação ou no recebimento de uma informação transmitida.

Nesse aspecto, a segurança da comunicação pretende preservar a:

> *Integridade do conteúdo:* garantia de que a mensagem enviada pelo emissor é recebida de forma completa e exata pelo receptor.
> *Irretratabilidade da comunicação:* garantia de que o emissor ou o receptor não tenha como alegar que uma comunicação bem-sucedida não ocorreu.
> *Autenticidade do emissor e do receptor:* garantia de que quem se apresenta como remetente ou destinatário da informação é realmente quem diz ser.
> *Confidencialidade do conteúdo:* garantia de que o conteúdo da mensagem somente é acessível ao(s) seu(s) destinatário(s).

[41] Comunicação: processo de transmissão de informação que se efetiva quando um emissor (remetente) envia uma mensagem (contendo uma ou mais informações) a um receptor, utilizando um canal (conexão que viabiliza a transmissão) e um conjunto de protocolos (regras e convenções utilizadas no processo de comunicação, comuns a emissor e receptor).

> *Capacidade de recuperação do conteúdo pelo receptor:* garantia de que o conteúdo transmitido pode ser recuperado em sua forma original pelo destinatário (BEAL, 2005, p. 02-03).

Há que se observar que nem todas essas pretensões se aplicam a todo tipo de informação e transmissão de dados, e nem a todas as etapas do ciclo de vida da informação.

3.5. Etapas do ciclo de vida da informação

Conforme os estudos de Adriana Beal (2005, p. 05-07) balizados nos consagrados autores McGee e Prusak (1994), Chun Wei Choo (2003) e Thomas Davenport (1998), entre outros, as etapas do ciclo de vida da informação são as seguintes:

a) *Identificação das necessidades e dos registros:* desenvolver serviços e produtos informacionais orientados para cada grupo e necessidade interna e externa.
b) *Obtenção:* atividades de criação, recepção, captura de informação, provenientes de fonte externa ou interna, em qualquer mídia[42] ou formato.
c) *Tratamento:* por processos de organização, formatação, estruturação, classificação, análise, apresentação e reprodução. Propósito: tornar a informação mais acessível, organizada e fácil de localizar pelos usuários.
d) *Distribuição:* quanto melhor a comunicação da organização mais eficiente é a distribuição interna da informação, pois facilita as decisões e melhora o desempenho.
e) *Uso:* conhecimento e atuação nos ambientes interno e externo da organização.
f) *Armazenamento:* assegura a conservação dos dados e informações, permitindo o uso e reuso dentro da organização.
g) *Descarte:* uma informação obsoleta ou sem utilidade para a organização deve ser descartada, obedecendo normas legais, políticas operacionais e exigências internas. Isso melhora o processo de gestão da informação, pois economiza recursos de armazenamento, aumenta a rapidez e a eficiência na localização da informação etc.

3.6. Vulnerabilidades

As vulnerabilidades determinam o grau de exposição de um ativo da informação, ambiente ou sistema a determinada ameaça. Há vulnerabilidade em relação à ameaça de erro humano, como a falta de treinamento dos usuários; aos eventos da natureza, como uma ameaça de inundação a uma instalação de um *data center*[43] no subsolo de um prédio (BEAL, 2005); e aos sistemas lógicos, como venda de aparelhos de TIC desatualizados, sem apagar as

[42] A mídia é o suporte da mensagem: o impresso, o rádio, a televisão, o cinema ou a Internet. Multimídia é quando se emprega diversos suportes de comunicação. O termo multimídia é corretamente empregado quando há interconexão, integração de várias mídias: lançamento de filme e de videogame simultaneamente, exibição de série de televisão, camisetas, brinquedos etc. Mas para designar a confluência de mídias separadas em direção à mesma rede digital integrada, deve-se usar de preferência a palavra unimídia (LÉVY, 1999).
[43] Centro de dados é um repositório centralizado, físico ou virtual, para a armazenagem, gestão e divulgação de dados e de informação organizada em torno de um determinado corpo de conhecimentos.

senhas. Esse último fator pode trazer muitos transtornos futuros, como acesso indevido por terceiros, uso indevido de informações pelos mesmos, e desvio de ativos de informações etc.

Outra forma de vulnerabilidade refere-se aos equipamentos. Um erro de operação pode acarretar a entrada incorreta de dados no sistema e trazer conseqüências negativas. Se o erro é corrigido antes de entrar no sistema, suas conseqüências são o retrabalho, a perda de eficiência e os atrasos operacionais. Se o erro não for corrigido, cresce o impacto resultante, sendo traduzido em tomada de decisões incorretas, perturbação das funções do negócio, redução do lucro, perda de clientes, perda da boa imagem etc. (BEAL, 2005).

3.7. Gestão de Riscos

Os ativos de informação estão sujeitos a todo tipo de ameaça e vulnerabilidade, como entrada de *hackers*[44] nos sistemas de informação da organização, incêndios e inundações nos ambientes que são armazenados os ativos de informação.

A organização ao implantar uma política de segurança da informação (PSI) torna mais fundamentada e confiável sua tomada de decisão sobre como e quanto gastar com a proteção de seus ativos da informação. Esse procedimento é designado como gestão de risco.

Como explicita Adriana Beal, gestão de risco é o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (BEAL, 2005).

Para Francesco de Cicco (2003), a gestão de riscos é uma disciplina em constante evolução. Várias tentativas de padronização desta disciplina são realizadas pelos *stakeholders* e pelos diversos públicos e setores que a adotam, pois há necessidade de um entendimento comum para se administrar riscos (públicos, privados, individuais, coletivos, difusos).

A gestão de riscos tem como finalidade a busca do equilíbrio apropriado entre o reconhecimento de oportunidades de ganhos e a redução de perdas. As vantagens de se preservar os ativos da informação por meio da gestão de risco apresentam-se na redução dos riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros. Em vista disso, recomenda-se elaborar uma PSI na organização, fundamental para o estabelecimento de um sistema de gestão de segurança da informação eficaz.

---

[44] *Hacker*: "termo para referenciar indivíduos que buscam obter acesso não autorizado a sistemas computacionais com o propósito de acessar informações, corromper dados ou utilizar os recursos disponíveis para realizar atividades ilegítimas numa rede" (BEAL, 2005, p. 09).

3.8. Política de Segurança da Informação (PSI)

A PSI é um conjunto de diretrizes e princípios adotados pela organização a fim de proteger seus ativos de informação. Formaliza-se em documento que contém todos os aspectos relevantes para a proteção, o controle e o monitoramento dos ativos de informação. Esse documento[45] deve ser observado por todos integrantes e colaboradores da organização, sendo aplicado a todos os sistemas de informação e processos corporativos (BEAL, 2005).

Consoante Adriana Beal (2005, p. 43). "a elaboração de uma PSI representa um passo fundamental no estabelecimento de um sistema de gestão de segurança da informação eficaz". E por meio dela a direção da organização demonstra seu comprometimento com a proteção da informação, e cria a base para a colaboração de todos os integrantes com os processos de identificação e tratamento dos riscos.

Independente da forma adotada pela organização a respeito da PSI, a versão final do documento deve estar coerente com as diretrizes organizacionais (missão, visão, valores, objetivos), com a estratégia corporativa e com as diretrizes de segurança em geral existentes na organização (CICCO, 2003).

Nesse sentido, a PSI deve ter uma abrangência ampla, ser flexível e manter seu foco nas questões de princípio, sem entrar em detalhes técnicos e de implementação. Deve também explicar a importância da informação e dos recursos computacionais e a necessidade de protegê-los contra as ameaças provenientes dos ambientes externo, interno, e das vulnerabilidades associadas aos ativos de informação. Essa explicação visa prevenir as conseqüências negativas que poderiam advir da destruição, da alteração indevida, da divulgação não autorizada de informações (BEAL, 2005), e das mudanças suscetíveis a todo ambiente organizacional.

Para evitar as conseqüências negativas, a PSI deve ser divulgada em todos os níveis hierárquicos da organização, evitando-se a alegação de desconhecimento das regras existentes como justificativa para sua violação. Deve também estar disponível para consulta pelos seus destinatários a qualquer tempo, para que dúvidas e esquecimentos possam ser corrigidos e o nível de proteção seja mantido ao longo do tempo (BEAL, 2005).

Além disso, a implantação da PSI depende de uma boa estratégia de divulgação e treinamento entre os usuários, clientes e fornecedores; e de uma forma eficiente de sua análise de desempenho. Convém que a PSI seja analisada criticamente a intervalos planejados ou

[45] Uma norma cujo cumprimento não é (ou não pode ser) exigido pode ser até mesmo pior do que a ausência de normatização, pois pode beneficiar os culpados pelo mau uso da informação.

quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia (ISO, 2009).

As possíveis barreiras quanto à implementação da PSI são as seguintes: falta de consciência dos usuários, clientes e fornecedores em relação à PSI; orçamento reduzido da organização para a PSI; reduzido número de recursos humanos especializado em PSI; e ausência de ferramentas adequadas para o bom funcionamento da PSI (CICCO, 2003).

Cabe ressaltar que a criação de uma PSI apenas por constar, sem sua efetiva implantação, pode gerar prejuízos à organização, tanto financeiro (perda de capital investido) quanto pessoal (perda de confiança dos usuários, clientes e fornecedores da organização). Seria melhor cumprir os requisitos mínimos de norma sobre gestão de segurança da informação e preparar-se para arcar com os possíveis resultados advindos da falha de segurança da informação (CHAIN *et al*, 2004).

3.9. Gestão de Segurança da Informação

Uma PSI torna-se mais eficiente com a devida gestão de segurança da informação. Para isso, a gestão da segurança da informação pode estabelecer uma estrutura formal de segurança baseada no ciclo de PDCA, a fim de administrar as constantes mudanças organizacionais.

O PDCA (*plan, do, check, act*) é um método utilizado em processos de gestão da qualidade que se aplica aos mais diversos tipos e níveis de gestão. É útil para fornecer uma visão global das etapas que devem compor a gestão da segurança da informação:

> P= *Plan*, de planejar: estabelecer objetivos, metas e meios de alcançá-los.
> D= *Do*, de executar.
> C= *Check*, de verificar, avaliar (comparação do executado com o planejado).
> A= *Act*, de agir corretivamente (caso sejam detectados desvios ou falhas a serem corrigidos) (BEAL, 2005, p. 37).

Conforme Adriana Beal (2005, p. 52), esse "método auxilia na administração das constantes mudanças organizacionais, pois estas são inevitáveis". Por exemplo, modifica-se o número de funcionários e usuários de sistemas; substituem-se estratégias de negócio; implementam-se novas tecnologias, etc. Isso afeta o valor da informação e o grau de exposição dos ativos da informação às ameaças existentes.

Caso o sistema de gestão de segurança da informação não acompanhe essas alterações, as medidas de segurança da informação implantadas podem rapidamente perder a eficácia, colocando em risco a integridade, a disponibilidade e a confidencialidade de informações

essenciais para a organização. Seguem-se as medidas de segurança da informação: humana, ambiente físico, ambiente lógico, e s*oftware* de código aberto.

3.9.1. Segurança Humana

Os indivíduos que têm acesso ao sistema de gerenciamento da informação de qualquer organização podem, casualmente ou não, falir com o sistema de segurança de informação da organização. Qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de um único indivíduo que decida abusar de seus privilégios de acesso a dados ou instalações de processamento da informação.

De acordo com Adriana Beal (2005, p. 71) "a melhor política de segurança em relação a qualquer pessoa com acesso aos recursos de informação corporativos continua sendo descrita pela conhecida expressão *trust, but verify* (confie, mas verifique)". E afirma que estudos demonstram que grande parte dos incidentes de segurança é provocada por integrantes da própria organização, sejam eles acidentais (decorrentes da ignorância, erro, negligência ou distração) ou intencionais (por motivo de fraude, vingança, descontentamento etc.), e não apenas provocados pelos *hackers*[46].

Para evitar tais acontecimentos na gestão de segurança da informação em TIC, necessita-se da permanente colaboração dos funcionários da organização, tanto na prevenção, quanto na reação a eventuais problemas de segurança (relatando falhas nos controles e incidentes observados). Ademais, os procedimentos de segurança dos usuários de sistemas de informação devem estar associados a regras claras, de obediência obrigatória, e sujeita a punições em caso de seu descumprimento, tornado público para evitar que seu desconhecimento diminua a eficácia dos controles existentes (BEAL, 2005).

A gestão da segurança da informação deve preocupar-se também com prevenção de atividades ilegítimas, como fraudes, vazamento de informações etc. Deve refletir-se em controles destinados a evitar que membros da alta direção ou da gerência média adquiram privilégios excessivos na manipulação de informações ou na realização de atividades críticas nos sistemas corporativos, efetivando-se em processos seguros de demissão. Acordos ou contratos de confidencialidade são úteis para alertar empregados e prestadores de serviços

[46] Os *hackers* não são necessariamente criminosos que provocam prejuízos, apossam-se de dados confidenciais e fazem uso deles. Mesmo involuntariamente, são responsáveis pela descoberta de falhas nos *softwares*, redes coorporativas e grandes corporações e sítios governamentais. Podem auxiliar nos testes de vulnerabilidade contra os novos e velhos elementos disponíveis na rede para detectar alguma falha que possa ser utilizada de forma inapropriada ou causar algum prejuízo à organização ou serem os causadores disso (VIOLA JUNIOR, 2005).

sobre os requisitos existentes com relação a informação de caráter sigiloso (ISO, 2009). Deve haver também uma documentação das responsabilidades de segurança de contratos de trabalho de funcionários e prestadores de serviço (BEAL, 2005).

Os contratos de prestação de serviço (terceirização) devem contemplar os requisitos legais e organizacionais de segurança a serem atendidos pelos fornecedores ou parceiros e explicitar os procedimentos usados para garantir que os envolvidos estejam cientes de suas responsabilidades de segurança. A confiança atribuída a indivíduos de fora da organização deve ser baseada em verificações de antecedentes, na obtenção de referências e em verificações rotineiras das atividades desempenhadas (BEAL, 2005).

Outra questão a ser pensada é a prevenção contra ataques de engenharia social. Esta ocorre quando *hackers* ou indivíduos mal-intencionados valem-se da ingenuidade de usuários para obter informações confidenciais como senhas, tipos de equipamentos utilizados ou outros dados que podem comprometer a segurança da organização (TURBAN *et al*, 2007).

Relatórios da CERT/CC[47] indicam que *hackers* ou indivíduos mal-intencionados utilizam-se de ferramentas automatizadas para enviar mensagens instantâneas e/ou correio eletrônico (*e-mail*) aos computadores de usuários desavisados. Essas mensagens normalmente oferecem *downloads*[48] de *softwares* de interesse do usuário, como música, proteção antivírus, ou pornografia. Quando o usuário baixa (*download*) um arquivo e executa o *software* em seu computador, em vez de ter apenas o conteúdo indicado, é instalado em seu sistema o "verdadeiro" conteúdo do *software (url malicioso*[49]*)*, que será utilizado conforme a programação do desenvolver (CERT, 2002).

---

[47] CERT/CC - Centro de Coordenação CERT faz parte do Instituto de Engenharia de *Software* da Universidade Carnegie Mellon, em Pittsburgh, Pensilvânia, Estados Unidos. CERT é um centro provedor de informações sobre incidentes para a comunidade da Internet. Estuda as vulnerabilidades de segurança na Internet, pesquisa mudanças nos sistemas de redes ao longo do tempo, e desenvolve informação e treinamento para ajudar no melhoramento da segurança. No Brasil, há convênio com esta instituição, sendo chamado CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

[48] Arquivo (documentos, textos, figuras, programas etc.) recebido virtualmente pelo usuário ao acessar conteúdos de páginas eletrônicas ou e-mail e instala em seu computador.

[49] Os *softwares* maliciosos podem ser: vírus (seqüência de código inserida em outro código executável; quando o programa é executado num computador, o código do vírus também o é); bombas lógicas (códigos que permanecem inativos por um período de tempo até serem parados); cavalos de tróia ou *trojan horses* (código malicioso embutido em um aplicativo aparentemente inofensivo, como um jogo, que realiza atividades ilegítimas, como apagar arquivos, reformatar discos etc., ou código embutido em sistemas com capacidade de afetá-los de maneira imprevista e indesejada); *worms* (programas que podem rodar de forma independente, transmitir-se de máquina em máquina usando conexões de rede e provocar dano, como impedir os computadores contaminados de funcionar corretamente) (TURBAN *et al*, 2007); *spams* (programas que enviam mensagens a um número indeterminado de usuários, se acessados, o *software* malicioso recolhe informações dos usuários) a caixa de entrada de e-mail fica com vários e-mails sem que possa identificar onde ou como aquele remetente conseguiu o endereço eletrônico. Os spams vêm como anúncios dos mais diversos produtos, correntes, avisos de bancos, de Tribunais, de Receita Federal, dentre outros (SERPRO, 2006*b*).

De acordo com o Comitê Gestor da Internet no Brasil (CGI.br), as instituições bancárias, privadas e oficiais, são o foco principal dos desenvolvedores de arquivos maliciosos. O Banco do Brasil e órgãos oficiais como o Tribunal Superior Eleitoral, e a Receita Federal, seguindo uma tendência mundial, descartam qualquer tipo de envio de e-mail aos usuários. A Secretaria da Receita Federal criou o Centro Virtual de Atendimento ao Contribuinte (e-CAC) para que o cidadão ou a empresa possa conversar com a Receita por meio de uma caixa postal segura, mediante a tecnologia da certificação digital, sem envio de *e-mail* (SERPRO, 2006*b*).

As conseqüências dos ataques de engenharia social são para o usuário e/ou para sua organização como: o controle remoto dos computadores pelo *hacker*, a exposição de dados confidenciais, a instalação de outro *software* malicioso no computador, a alteração ou a destruição de arquivos (CERT, 2002).

Dentre as recomendações do CERT no combate à engenharia social nunca se deve baixar (*download*), instalar ou executar um programa, a menos que seja de autoria de uma pessoa ou empresa confiável (CERT, 2002). Toda essa cautela pode ser desconfigurada se a pessoa ou a empresa confiável também estiverem infectados por um *software* malicioso e contaminar usuários sem intenção de fazê-lo. Por isso, uma gestão de segurança da informação deve ser sempre reavaliada e discutida com os membros da organização, a fim de atualizá-los sobre os riscos de suas ações no campo virtual.

3.9.2. Segurança do Ambiente Físico

A organização em sua gestão da informação deve ter como base um meio seguro para produzir, armazenar, modificar, recuperar e destruir informações. O ambiente físico pode ser por meio de papéis, fitas magnéticas, *hardwares* etc. E, por ser a principal forma de manifestação e transmissão da informação, o ambiente físico precisa ser resguardado.

Dentre as diversas formas de se resguardar o ambiente físico, podem-se citar: segurança em escritórios, salas e instalações de processamento; áreas de segurança e de expedição e carga; proteção de documentos em papel; proteção de mídias de computador; arquivo de documentos eletrônicos; proteção e comunicações não baseadas em computador; proteção de *hardware;* cabeamento; instalação, proteção e manutenção de equipamentos; remoção, descarte e transporte de equipamentos; políticas de mesa limpa e tela limpa; trabalho remoto (BEAL, 2005).

Em relação à proteção do ambiente físico digital, podem-se utilizar padrões abertos e metadados, assim como estratégias de migração periódica, pois facilitam a recuperação e a utilização da informação digital. Além disso, reduzem os riscos da obsolescência tecnológica ao evitar a indisponibilidade de informações contidas em documentos criados num ambiente tecnológico não mais disponível (BEAL, 2005).

Para efeitos de esclarecimentos, os padrões abertos são definidos por meio de consenso entre os fabricantes e instituições padronizadoras internacionais. Isso aumenta a confiabilidade, a compatibilidade, a facilidade de manutenção e a economicidade das soluções de gestão eletrônica de documentos. Eles reduzem os problemas de interoperabilidade e de recuperação de informações causadas pelo uso de "soluções proprietárias" e evitam a dependência em relação a determinados fornecedores.

Os metadados são "dados a respeito de dados". Eles permitem resguardar elementos considerados essenciais para a preservação de documentos eletrônicos em longo prazo, tais como data, autor, produtor, versão, fonte etc. Facilitam os processos de gestão, recuperação e reprodução de informações nesses documentos.

Já a migração periódica dos acervos digitais para tecnologias atualizadas contribui para a garantia de disponibilidade das informações, protegendo-as de mudanças nos métodos de gravação, armazenamento e recuperação. O processo de migração periódica visa evitar que futuros dispositivos de mídias só leiam as mídias futuras, ou seja, ele permite a recuperação e a leitura de documentos eletrônicos antigos em mídias eletrônicas ou digitais mais modernas. Como exemplo, as mídias magnéticas foram transferidas e recuperadas em mídias mais modernas e estáveis: CD-ROM[50] e DVD[51]. Atualmente, o CD-ROM está obsoleto em relação às novas mídias pen-drives[52].

As estratégias de *backup* são necessárias para um plano de continuidade dos serviços da organização baseados em TIC. *Backups* são cópias-reserva de segurança dos dados e de *softwares* essenciais à organização, que devem ser de fácil acesso e de acesso remoto à

[50] CD-ROM: *Compact Disc – Read Only Memory*. São discos ópticos gerados através de um processo de masterização a partir de um original. É gravado por um processo de estampagem e pode ser apenas lido. O CD-R: *Compact Disc – Recordable* ou *Writable*, são discos ópticos com o mesmo padrão de leitura do CD-ROM. Diferente do CD-ROM podem ser gravados em casa. Permite gravação livre em qualquer área, mas não é regravável, contudo o CD-RW: *Compact Disc – Rewritable*, é regravável (KOCH, 1998, p. 60). Masterizar é a arte de ouvir cuidadosamente uma mixagem completa com objetivo de apurar e corrigir deficiências sonoras e problemas.

[51] DVD: *Digital Video Disk ou Digital Versatil Disk*. São discos ópticos que podem ser gravados por meio de feixes de laser, com capacidade de armazenamento maior que o CD-ROM (KOCH, 1998, p. 62).

[52] Memória USB (*Universal Serial Bus*) *Flash Drive*. É um dispositivo de armazenamento constituído por uma memória flash tendo uma fisionomia semelhante à de um isqueiro ou chaveiro e uma ligação USB tipo A, que permite sua conexão a uma porta USB de um computador. Sua capacidade de armazenamento atual é superior ao DVD, e, em condições ideais, pode armazenar informação durante 10 anos.

organização. O acesso remoto pode ser em uma localidade remota que permita tratar eficazmente de falhas menores, de problemas em mídias ou servidores, e de desastres que destruam ativos armazenados na instalação principal. Além dos *backups* armazenados à distância, sempre que possível devem ser mantidos recursos e instalações alternativas que permitam a recuperação desses dados e *softwares* em caso de desastre (BEAL, 2005).

3.9.3. Segurança do Ambiente Lógico

O ambiente lógico é composto por todo o ativo de informações das organizações.

De acordo com a política de segurança da ICP-Brasil (2008) a informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação.

Os dados, as informações e os sistemas de informação das entidades e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo (confidencialidade) e disponibilidade desses bens. As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado (ICP-Brasil, 2008).

Os dados, as informações, e os *software*s quando apagados no disco rígido de um computador podem ser restaurados, a menos que o usuário utilize também um programa especial para apagar com segurança o arquivo. Outra preocupação deve se dar quando os *hardwares* são doados, vendidos ou jogados no lixo, pois se não apagarem as informações contidas nos mesmos, qualquer indivíduo que tenha acesso a esses equipamentos poderá gerar algum risco para a organização.

No que tange à proteção de informação em redes, os mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*[53]) devem ser utilizados para proteger as transações entre redes externas e a rede interna da organização. O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias, e solicitar nova autenticação após certo tempo de inatividade da sessão (ICP-Brasil, 2008).

[53] O *firewall* "consiste numa barreira de proteção entre um computador ou uma rede interna e seu ambiente externo. O tráfego de informações entre esse computador ou rede e o mundo exterior é examinado e bloqueado quando uma informação não atende a critérios predefinidos de segurança" (TURBAN *et al*, 2007, p. 72).

Um dispositivo complementar ao *firewall* na proteção contra invasões é o IDS (*Intrusion Detection System*). Enquanto o *firewall* limita o acesso entre redes para prevenir uma invasão, o IDS inspeciona toda a atividade de rede de dentro para fora e vice-versa, identifica e avalia padrões suspeitos que podem indicar ataque à rede (interno ou externo) e emite um alarme quando existe a suspeita de uma invasão (BEAL, 2005).

Para se proteger das redes conectadas à Internet é essencial ter um bom sistema antivírus e antispam. Os *softwares* antivírus e antispam ajudam a impedir ataques de código malicioso vasculhando arquivos periodicamente em busca de mudanças não esperadas em tamanho de arquivos, seqüências de código similares às armazenadas numa base de dados de vírus conhecidos, anexos de *e-mail* suspeitos e outros sinais de alertas de riscos.

O correio eletrônico (*e-mail*), se não usado cautelosamente, pode disseminar vírus e transferir informações proprietárias para terceiros não autorizados. Controles sugeridos pela ISO 17799 sobre políticas formais de utilização do *e-mail* são responsabilizar funcionários pelo conteúdo de mensagens e orientá-los sobre quando não se deve usar *e-mail*; uso de técnicas de criptografia para proteger a confidencialidade e a integridade de mensagens sensíveis; controles adicionais para a investigação de mensagens que não puderem ser autenticadas; e proteção de anexos de correio eletrônico (ISO, 2009).

O problema do uso de correio eletrônico é que a maioria dos usuários pensa que as mensagens trocadas são isentas de interferências. Contudo, não é uma carta fechada, assemelha-se mais a um cartão postal, ou seja, pode ser lido por outros, interceptado, modificado e até destruído. Senhas são outro domínio sobre o qual usuários acreditam ter poder, e não se preocupam em manter secreto o código pessoal. *Hacker* só precisa de 30 segundos para vasculhar um computador e enviar mensagens para outras pessoas passando-se pelo usuário, e/ou pedir e conseguir acesso em seu nome e à sua revelia (COSTABILE, 2004).

Outra forma de se proteger os ativos de informação são os mecanismos de criptografia[54]. São amplamente adotados em ambientes computacionais para oferecer garantia de autenticação, privacidade e integridade de dados e comunicações, e sem essa tecnologia não teria sido possível popularizar o comércio eletrônico (TURBAN *et al*, 2007).

Segundo Adriana Beal (2005):

> A criptografia simétrica, ou tradicional, utiliza uma única chave que serve tanto para cifrar como decifrar a informação. Como duas ou mais partes compartilham a mesma chave para codificar e decodificar, qualquer descuido na preservação da chave criptográfica pode levar ao comprometimento da segurança do processo. A

[54] "Criptografia (*kriptós*=escondido, oculto; *grápho*=grafia) é a arte ou ciência de escrever em cifra ou em código, com o propósito de restringir ao destinatário da mensagem (detentor da chave ou senha desencriptação ou decifragem) a capacidade de descodificá-la e compreendê-la" (BEAL, 2005, p. 100).

> criptografia assimétrica, ou de chave pública, trabalha com duas chaves diferentes, matematicamente relacionadas, para codificação e decodificação da mensagem. A chave pública está disponível a todos que queiram criptografar informações e enviá-las ao dono da chave privada, ou verificar uma assinatura digital criada com aquela chave privada. A Chave privada, de uso exclusivo do proprietário para assinar ou decodificar mensagens a ele destinadas, deve ser mantida em segredo para garantir a confiabilidade desse processo (BEAL, 2005, p. 100).

Já a estereografia (*stereós*=sólido, fixo; *grápho*=grafia) é uma técnica que possibilita a "ocultação de uma informação dentro de outra, usando o princípio da camuflagem. No caso da estereografia digital, informações podem ser escondidas em arquivos de imagem, som, texto, código binário, etc." (BEAL, 2005, p. 104).

Com a evolução da tecnologia, surgiram a certificação digital e a assinatura digital. A certificação digital baseia-se no ideal de que as transações eletrônicas devem atender a uma série de requisitos para serem executadas de forma ampla e confiável (SERPRO, 2004):

1) disponibilidade (utilização ininterrupta do documento ou informação);
2) integridade (não-alteração do documento original);
3) confidencialidade (proteção da informação do conhecimento ou ação indevida de terceiros);
4) autenticidade (garantia da autoria, origem e destino); e
5) irretratabilidade (uma vez efetuada, a transação não pode ser negada).

Assegurados esses requisitos, o usuário ao receber um documento com certificado digital tem a garantia da identidade da pessoa que assinou digitalmente e terá certeza se o documento foi adulterado ou não (SERPRO, 2004).

A tecnologia de certificação digital utiliza a criptografia. Trata-se de um processo de cifragem e decifragem iniciado pelo uso de mecanismo de chaves. Quando um usuário adquire um certificado digital, automaticamente gera duas chaves correspondentes, protegidas por senhas, uma secreta e uma pública. A secreta é a identificação pessoal do usuário e só deve ser do conhecimento do titular. A pública pode ser obtida pelo público em geral. Um texto cifrado pela chave privada de um usuário só pode ser decifrado pela chave pública do mesmo e vice-versa. Utilizando esse sistema é possível fazer a assinatura digital de um documento de qualquer procedência: .doc, .jpg, .pdf e .bmp (SERPRO, 2004).

Já a assinatura digital é o sistema de criptografia de chave pública aplicado a um documento específico, que vai garantir a integridade e a autoria de quem o assinou. O certificado digital é a vinculação de uma chave pública a uma pessoa física ou jurídica ao meio virtual. Um certificado tem período de validade, nome e assinatura digital da entidade

que o forneceu (Autoridade Certificadora), nome do usuário e a chave pública do usuário (SERPRO, 2004).

A assinatura digital é interpretada pelo *Information Technology Security Strategy* (ITSS), grupo de trabalho sobre matérias legais do Governo do Canadá, da seguinte forma:

> No mundo eletrônico, o original de um documento eletrônico é indistinguível de uma cópia, não existe assinatura escrita de próprio punho e ele não está sobre o papel. O potencial para fraudes é grande, devido à facilidade de interceptação e alteração dos documentos eletrônicos, e à velocidade de processamento de múltiplas transações. Sempre que as partes tratem entre si com muita freqüência, ou onde não existam conseqüências legais, uma assinatura pode não ser necessária. Todavia, existindo um alto potencial para disputa, uma assinatura tradicional ou uma assinatura digital são requeridas (DSP, 2007, p. 01).

Como demonstrado, o uso da assinatura digital e da certificação digital é abalizado tanto no Brasil como no Canadá, na busca pelo aperfeiçoamento da PSI.

3.9.4. Segurança do Software de Código Aberto

Em muitas organizações, notadamente as estatais, há políticas de inserção de *software* de código aberto ou livre em detrimento de *software* de código fechado ou proprietário. O uso do código aberto pode ser visto como uma fonte de soluções, programas e serviços para a otimização de recursos e investimentos em tecnologia da informação. O *software* de código aberto é um sistema operacional[55] que possui um código-fonte disponível para ser utilizado, desenvolvido, copiado, distribuído, estudado, aperfeiçoado e modificado por qualquer indivíduo, sem despender muitos recursos. O responsável por uma alteração no código-fonte pode optar por manter essa alteração para si ou devolvê-la para a comunidade de usuários e desenvolvedores, para que seja eventualmente incorporada em versões futuras do *software*. Um exemplo desse *software* é o Linux (MOREIRA, 2006).

Em contrapartida, o *software* de código fechado é um sistema operacional que precisa ser comprado, sujeito a licenças e multas. Não é "permitido" modificar, copiar e aperfeiçoar sua estrutura, ou seja, vem sob a forma de um "pacote fechado e inviolável". Isto se torna inconveniente quando ocorre alguma falha no sistema, pois se fica condicionado à manutenção, à atualização e à cobrança do serviço pelo proprietário do *software* de código fechado. Um exemplo desse *software* é a *Microsoft Windows* (MOREIRA, 2006).

[55] "Os sistemas operacionais são programas que gerenciam os recursos dos computadores (memória, entrada e saída etc.) e organizam a mediação entre *hardware* e *software* aplicativo. O *software* aplicativo não se encontra, portanto, em contato direto com o *hardware*" (LÉVY, 1999, p. 42).

Enquanto o *software* de código fechado é desenvolvido por um grupo ou indivíduo que atua de forma isolada até que o produto esteja pronto para ser vendido no mercado; o *software* de código aberto é desenvolvido por uma rede de programadores "voluntários" que trabalha paralelamente no desenvolvimento e revisão do código, submetendo alterações para um coordenador do projeto. Este analisa as modificações propostas e incorpora as consideradas mais adequadas, possibilitando liberação mais freqüente de novas versões para os usuários. No caso do *software* proprietário é comum que o fornecedor se responsabilize por manter o usuário/organização informado do lançamento de atualizações recomendadas, enquanto no *software* livre passa a ser responsabilidade da organização usuária acompanhar a evolução do código (BEAL, 2005).

Em vista disso, a opção pelo *software* livre não pode ser motivada apenas por aspectos econômicos, mas pelas possibilidades que abre no campo da produção e circulação de conhecimento. Além disso, esse sistema operacional possibilita o acesso a novas tecnologias, podendo-se estimular o desenvolvimento de *softwares* nacionais, garantindo ao cidadão o direito de acessar os serviços públicos sem obrigá-lo a usar plataformas específicas, como o navegador *Windows Explore* (MOREIRA, 2006).

Para que isto ocorra, deve-se acabar com a negligência da maioria das páginas eletrônicas do Governo Federal que somente funcionam adequadamente com navegadores *Microsoft* para o sistema operacional *Windows*, sendo tecnologias de *softwares* proprietários que envolvem a compra dos mesmos a preços elevados. "Isto bate de frente com uma política pública baseada em estratégias de uso de *software* livre em telecentros, escolas públicas e no serviço público em geral" (AFONSO, 2002, p. 181).

Carlos Afonso (2002, p. 182) ainda afirma que "*software* aberto não é *software* a custo zero". Como qualquer outro *software*, pode requerer especialistas para configuração, instalação, adaptação, desenvolvimento e treinamento, traduzindo-se em serviços pagos. A vantagem é que acaba com o custo de atualização do código e com o custo de licenças de uso.

A organização que decidir criar e implementar um *software* livre deve se pautar nos futuros riscos, pois pode não conseguir atrair um conjunto suficiente de desenvolvedores tecnicamente competentes e organizados para manter o produto ao longo do tempo. Ou podem surgir diferentes correntes de desenvolvimento, que levem a versões inconsistentes do *software*. Em virtude disso, o uso do *software* livre deve ser entendido como uma opção tecnológica da organização, e mais especificamente do Governo, utilizada quando possível e quando viável economicamente.

3.10. Controles de Acesso

Os controles de acesso impedem acessos não autorizados aos ativos de informação.

Para que não haja esses acessos não autorizados, deve haver o controle de acessos físico e lógico. O adequado controle desses acessos possibilita o alcance dos três principais objetivos de segurança da informação: confidencialidade, integridade e disponibilidade da informação.

Os controles de acesso colaboram para o alcance dos seguintes objetivos de segurança da informação numa organização pautada pela PSI:

> *Objetivo de confidencialidade*: o controle de acesso evita o acesso de pessoas não autorizadas a informações confidenciais, salvaguardando segredos de negócio e protegendo a privacidade de dados pessoais.
> *Objetivo da integridade:* o controle de acesso evita que pessoas não autorizadas tenham acesso à informação para criá-la, destruí-la ou alterá-la indevidamente.
> *Objetivo da disponibilidade*: o controle de acesso permite identificar os usuários legítimos da informação para que lhes possa ser liberado o acesso quando solicitado (BEAL, 2005, p. 111-112).

Em relação ao objetivo da confidencialidade a Constituição Federal traz explicitamente a proteção do mesmo em seu artigo 5 , X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 2009*a1*). Nesse sentido, a confidencialidade é um direito garantido constitucionalmente, sendo mais um motivo para se enquadrar nos objetivos de uma política de segurança da informação.

3.11. Avaliação do Desempenho de Gestão da Segurança

A avaliação do desempenho de Gestão da Segurança da organização é necessária em uma organização que pretende aplicar uma séria política de segurança da informação. Notadamente o Governo, que deve pautar questões de segurança da informação, respeitando o princípio de Publicidade, e em decorrência, o princípio da transparência e a *Accountability* (responsabilidade), como já explicitado no Capítulo 2 – Governo Eletrônico, p. 31.

Avaliar o desempenho de como o Governo ou qualquer outra organização conduz sua gestão de segurança da informação possibilita esclarecer os objetivos estratégicos da segurança e manter o foco nos processos, sinais e variáveis críticas para o desempenho da segurança e controle de riscos.

A medição do desempenho de segurança da informação deve existir por quatro razões:

> *Caracterizar a gestão da segurança* (proporcionar um entendimento dela e estabelecer referências para futuras comparações).
> *Avaliar a gestão da segurança* (determinar a situação em relação àquilo que foi planejado, permitindo saber se os projetos e processos estão ou não atingindo os objetivos propostos, para que se possa, quando necessário, adotar medidas para melhorar os resultados).
> *Prever e preparar ações* (compreender as relações entre os fatores determinantes do resultado e identificar tendências que ajudem a planejar os próximos passos).
> *Aprimorar as operações* (identificar obstáculos, causas-raiz, ineficiências e oportunidades de aperfeiçoamento das ações) (BEAL, 2005, p. 163-164).

Essa avaliação de desempenho pode abalizar as ações do Governo e da organização no tocante à forma como trata da segurança da informação.

Em relação ao Governo, duas questões devem ser feitas: como garantir a segurança da informação para todos os dados e informações, mesmo que não sejam de sigilo de grau mais elevado; e como garantir que os dados e as informações, respeitando-se os princípios de Publicidade e Transparência, sejam resguardados das ações de improbidade (servidor) e inescrupulosidade (cidadão)?

São questões que ainda não têm respostas categóricas e precisas. São mais observações que questionamentos, e visam mostrar que adequadas avaliações de desempenho poderão auxiliar no amadurecimento dessas observações e na efetiva política de segurança da informação. Para que isso ocorra, as avaliações devem ser feitas periodicamente, pois a cada momento surgem novas TICs e formas de armazenar, processar, distribuir e alterar dados e informações. Conseqüentemente, a segurança da informação deverá ser repensada para estar atualizada com as novas TICs.

3.12. Inclusão Digital

Outro fator preocupante quanto à PSI está relacionado à inclusão digital, que se apresenta em processo crescente, ao inserir a cada ano milhares de indivíduos na Internet. Isso reforça a necessidade de manter campanhas educativas permanentes voltadas para o uso consciente da Internet, como no uso de senhas e de *e-mails*.

A conscientização é relevante, pois são indivíduos acessando conteúdos e que nunca tiveram nenhum treinamento para desconfiar daquilo que acessam. Portanto, o trabalho de conscientização deve ser constante e ilimitado, tanto por parte de governos, instituições privadas e não-governamentais, e os próprios usuários já atentos para essas questões.

CAPÍTULO 4 – REGULAMENTAÇÃO E CARACTERÍSCAS DOS ESTADOS BRASIL E CANADÁ

Antes de explicitar as normas brasileiras e canadenses a respeito da PSI do e-Gov Federal, conceitua-se regulamentação e faz-se uma breve caracterização dos países Brasil e Canadá, para melhor entendimento de suas culturas. A comparação desses dois países se deve ao fato do Canadá ser referência mundial em questões de e-Gov, sendo esse estudo uma forma de colaborar com as iniciativas de e-Gov brasileiro, ao demonstrar as semelhanças e diferenças de ambos.

4.1. Regulamentação

Regulamentação, em sentido amplo, é o ato de criar normas para o ordenamento jurídico, significa tornar uma conduta média, previsível, através do estabelecimento de limites para o comportamento, é ditar regras.

A regulamentação, em sentido estrito, são as normas imperativas (princípios e condutas gerais) realizadas pelo Poder Legislativo (leis ordinárias, complementares etc.) e excepcionalmente pelo Poder Executivo (leis delegadas, regulamentos, medidas provisórias).

Diferentemente da regulamentação, a regulação é o ato de controlar determinadas atividades, é fazer observar regras necessárias ao funcionamento de uma organização. Regular significar esclarecer e facilitar a aplicação das regras por meio de disposições. São normas dispositivas as estipuladas pelas Agências Reguladoras[56] referentes às questões econômicas, profissionais, técnicas e científicas que foram regulamentadas pelo poder legiferante do Estado (HEINEN, 2004).

Regulação ou ato de regular, ligado às Agências Reguladoras, possui um significado eminentemente ligado à técnica e à economia. Já a regulamentação é ato do poder legiferante do Estado, possui um critério eminentemente político e jurídico, além do técnico, econômico e social. Há que se observar que o ato de regular não pode extrapolar as matérias específicas pertinentes à Agência Reguladora, bem como contrariar a lei e os princípios constitucionais. Deve ser um instrumento de integração de normas, a fim de dar maior especificidade às regras

[56] As "Agências Reguladoras são entes administrativos conceituados como sendo autarquias de regime especial, em face de certas peculiaridades que possuem, entre elas, o poder de regular matérias atinentes a sua especialidade e capacidade específica" (MELLO, 2003).

que possuem valores mais genéricos, trabalhando no campo da sua execução (HEINEN, 2004). Mesmo porque a regulação é decorrente da concessão de poder legiferante aos órgãos burocráticos, logo, delegação do poder legislativo ao executivo, além de que são normas de escala hierárquica inferior às legisladas por regulamentação.

Há também o conceito de regulamento. No Brasil, os regulamentos são chamados de decreto. Decreto é "ato do Chefe Executivo para regulamentar as leis, ou seja, para expedir normas administrativas necessárias a que a lei possa ser executada" (CARVALHO FILHO, 2006, p. 118). A diferença entre a lei e o regulamento reside no fato de que a lei inova originariamente o ordenamento jurídico, enquanto o regulamento não o altera, mas fixa, tão-somente, as regras orgânicas e processuais destinadas a pôr em execução os princípios institucionais estabelecidos por lei, ou para desenvolver os preceitos constantes da lei, expressos ou implícitos, dentro da órbita por ela circunscrita, isto é, as diretrizes, em pormenor, por ela determinadas (MENDES; FORSTER JR., 2002). Conforme Celso Antônio Bandeira de Mello (2003, p. 311) o "regulamento é ato estritamente subordinado, dependente da lei".

No Canadá há leis e regulamentos. Estes têm o mesmo sentido do brasileiro, contudo é emanado do Gabinete do Primeiro-Ministro. As leis são chamadas de estatutos e os decretos de regulamentos.

Nesta dissertação o termo regulamentação é utilizado em sentido amplo como o ato de ditar regras, realizado pelo poder legiferante do Estado. Abarca toda legislação do Brasil e do Canadá referente à política de segurança da informação. É um tema atual, que passou a ser observado e normatizado com cautela pelos Estados ao implantarem seu e-Gov.

A PSI do e-Gov deve ser compatível com as características técnicas e operacionais das TICs e conduzir a uma nova conformação de institutos jurídicos no *modus operandi* da Administração Pública Federal. A regulamentação da PSI será tratada como um processo de institucionalização que modifica a forma de atuação da Administração Pública Federal em questões de segurança da informação de e-Gov.

Em relação à regulamentação da Internet, o relatório divulgado pela UNCTAD (Conferência da ONU sobre Comércio e Desenvolvimento) em 2006 elucida que qualquer tentativa de regulamentação da Internet deve respeitar as noções legais e políticas vigentes na sociedade fora da rede. Deve ser próxima das noções existentes e aceitas da teoria legal e política em uso. A UNCTAD sugere que algum grau de regulamentação é necessário, ao dizer que os governos não podem mais deixar a Internet como está. A sociedade está indo para a Internet e com ela também vai a necessidade de organizá-la e governá-la (GLYCERIO, 2006).

Algumas regulamentações estão presentes no ordenamento jurídico e outras poderão ser criadas para se adequar aos objetos, valores e/ou conteúdos das relações jurídicas. Visa-se ilustrar não somente a regulamentação específica sobre PSI do e-Gov, como também demonstrar a regulamentação existente relacionada direta e indiretamente ao tema.

Antes, porém, serão caracterizados os países objeto do estudo comparado: Brasil e Canadá, para esclarecer suas culturas e a forma como governam, julgam e legislam.

4.2. Características dos Estados: Brasil e Canadá

4.2.1. Geografia, População e Colonização

Brasil

O Brasil é o quinto maior país do mundo e se caracteriza pela diversidade geográfica e grandes variações climáticas. É dividido territorialmente em 26 Estados, um Distrito Federal e 5.563 municípios. Sua população aproxima-se a 189.6 milhões de habitantes. De acordo com o IBGE de 2008 as cidades mais populosas são São Paulo, Rio de Janeiro e Salvador; e cerca de 0,3% dos brasileiros são indígenas, sendo a tribos mais populosas: Ticuna, Guarani, Caiagangue. O Brasil foi colonizado por portugueses sendo sua língua oficial o Português, com características da língua Tupi-Guarani e dos idiomas africanos (PORTAL, 2009).

Canadá

O Canadá é o segundo maior país do mundo e se caracteriza pela diversidade geográfica e grandes variações climáticas. É dividido territorialmente em 10 províncias e 3 territórios, e distritos. Sua população aproxima-se a 33.1 milhões (janeiro de 2008), sendo 79% urbana. De acordo com o Censo de 2006, 34,7% da população vivem nas três maiores cidades: Toronto, Montreal e Vancouver; e cerca de 3,8% dos canadenses pertencem a um ou mais dos três grupos indígenas reconhecidos pela Constituição de 1982 (CANADA, 1982): Índios Norte-Americanos, Métis e Inuit – esquimós (CONSULADO, 2008*a*).

O Canadá foi colonizado por ingleses e franceses e, por isso, possui duas línguas oficiais: o inglês, língua materna de 57,2% dos canadenses e, o francês, a língua de 21,8% da população. Entretanto, 19,7% dos canadenses têm outra língua materna além do inglês ou do francês, como: italiano, chinês, alemão, português, polonês, espanhol, árabe, holandês, ucraniano, holandês, grego, entre outras (CONSULADO, 2008*a*).

4.2.2. Estrutura do Governo

Brasil

Possui o Presidente da República como o chefe de Estado e do Poder Executivo Federal, auxiliado pelos Ministros de Estado; o Congresso Nacional, composto pelo Senado e Câmara dos Deputados; o Superior Tribunal Federal, Tribunal Superior de Justiça, Tribunal Superior do Trabalho, Tribunal Superior Eleitoral e o Superior Tribunal Militar (PORTAL, 2009).

Canadá

Possui o Soberano, que é a Sua Majestade, a Rainha Elizabeth II (chefe de Estado), representada pelo Governador Geral, Michaëlle Jean; o Primeiro-Ministro, Stephen Harper (chefe do Poder Executivo), Gabinete de Ministros e Ministérios; o Parlamento, composto pelo Senado e Câmara dos Comuns; o Supremo Tribunal do Canadá, Tribunal Federal do Canadá, e Tribunal Eleitoral (*GOVERNMENT*, 2009).

4.2.3. O sistema político

Brasil

O Brasil é uma república federativa presidencialista democrática representativa. Simultaneamente às eleições presidenciais, vota-se para o Congresso Nacional, sede do Poder Legislativo, dividido em duas casas parlamentares: a Câmara dos Deputados, que têm mandato de quatro anos, e o Senado Federal, cujos membros possuem mandatos de oito anos e elegem-se em um terço e dois terços, alternadamente, a cada quatro anos. Adota-se o sistema majoritário para a eleição dos senadores e, o proporcional, para os deputados. Os Estados mais populosos têm direito a eleger uma quantidade maior de deputados federais, entretanto, as regras dão um peso relativo muito maior aos Estados menos populosos. Além disto, o número de deputados é limitado a, no mínimo, oito e, no máximo, setenta para cada Estado, num total de 513 deputados. Há três senadores representando cada unidade da Federação (atualmente 27), independentemente da população (PORTAL, 2009).

Os poderes são divididos em Poder Executivo, Poder Legislativo e Poder Judiciário, totalmente independentes e com igual peso político. Como atribuição típica, o Poder Legislativo elabora leis; o Poder Executivo administra, ou seja, realiza os fins do Estado,

adotando concretamente as políticas para este fim; e o Poder Judiciário soluciona conflitos entre cidadãos, entidades e o Estado (PORTAL, 2009).

O Presidente da República é auxiliado pelos Ministros de Estado. Na estrutura da Presidência, os órgãos estão classificados, legalmente, como essenciais; de assessoramento imediato ao Presidente; consultivos e integrantes. A Casa Civil, reconhecida como essencial, atua na coordenação e na integração das ações do Governo. Os órgãos de assessoramento imediato são o Conselho de Governo, a Advocacia-Geral da União e a Secretaria de Imprensa e Divulgação. Os Conselhos da República e de Defesa Nacional são órgãos de consulta. Vinculada ao Presidente da República, a Comissão de Ética Pública é integrante e tem como competência a revisão das normas sobre conduta ética na Administração Pública Federal, elaboração e proposta da instituição do Código de Conduta das Autoridades (PORTAL, 2009).

Canadá

O Canadá é uma monarquia constitucional federal parlamentar democrática. O sistema parlamentarista canadense tem suas origens na Grã-Bretanha, conservando as tradições herdadas pelo Parlamento Britânico. O Parlamento Canadense é instância máxima de Governo, composto pela Rainha (representada pelo Governador Geral), Senado e Câmara dos Comuns (CONSULADO, 2008*b*; GONÇALVES, 2008).

Elizabeth II, Rainha da Inglaterra, é também Rainha do Canadá e soberana de vários reinos – *Commomwealth of Nations*: Reino Unido, Canadá, Austrália (VANCOUVER, 2009). A Rainha é a Chefe de Estado e os Poderes Executivo e Legislativo são exercidos em seu nome: as leis são sancionadas por ela, sob orientação e consentimento do Senado e da Câmara dos Comuns, e publicadas em seu nome. A justiça também é realizada em seu nome. Efetivamente, "as funções da Coroa são exercidas pelo Governador-Geral, nomeado pela Rainha por indicação do Primeiro-Ministro" (GONÇALVES, 2008, p. 363).

O Senado[57], também chamado de Câmara Alta segue os moldes da Câmara dos Lordes da Inglaterra. Seus 104 membros não são eleitos, mas nomeados entre sujeitos notáveis (professores, jornalistas, cientistas, ex-políticos, juristas etc.) por um mandato vitalício (VANCOUVER, 2009).

[57] O professor visitante da Fundação João Pinheiro e *Senior Analiyst International Department – Bank of Canada*, Carlos de Resende, informou que o Senado vota leis que tenham sido originadas nesta Casa. No entanto, a prática é que o Senado não tem poder algum, o voto é apenas um protocolo, e os senadores são aparentemente figurativos, sendo a Câmara quem decide tudo.

A Câmara dos Comuns contém 295 membros, cada um vindo das 295 zonas eleitorais, renovada pelo menos a cada 5 anos. O partido que ganha o maior número de assentos geralmente forma o governo. O líder do partido majoritário é nomeado Primeiro-Ministro pelo Governador Geral, tornando-se o Primeiro-Ministro. Este escolhe os Ministros para formar o Gabinete sob sua direção (VANCOUVER, 2009).

O "Gabinete é o fórum para criar um consenso entre os Ministros. Seu número varia a cada novo governo. Não é entendido como o conjunto dos ministros, mas como um corpo menor ao qual pertencem ministros mais influentes" (GONÇALVES, 2008, p. 366). A governabilidade só é possível se o Gabinete tiver o apoio do Parlamento. Quando o Primeiro-Ministro perde apoio ou renuncia ao mandato, dissolve-se o Gabinete e Governador Geral deve encontrar um sucessor que tenha a confiança da Câmara dos Comuns (PCO, 2009).

Embora o sistema parlamentarista tenha em seu fundamento a supremacia do Parlamento, efetivamente o poder centra-se no Gabinete, e, em particular, no Primeiro-Ministro. Há concentração de poderes deste, que pela disciplina partidária (que leva os membros de um partido a votarem conforme determina a liderança), acaba controlando o Parlamento, tornando-se um verdadeiro "monarca eleito" (GONÇALVES, 2008, p. 366).

O Primeiro-Ministro e os Ministros do Gabinete são membros do Parlamento, mais freqüentemente da Câmara dos Comuns, de modo que os Poderes Executivo e Legislativo não se encontram claramente separados. Essa fusão de poderes envolve as atribuições do Gabinete de iniciar a maior parte do processo legislativo. Por ter apoio da maioria, presume-se que as leis e políticas propostas pelo Governo serão aprovadas pelo Parlamento, garantindo-se a estabilidade institucional (GONÇALVES, 2008).

O Gabinete é assessorado por quarto órgãos de coordenação central: o *Prime Minister's Office* (PMO), o *Privy Council Office* (PCO), o *Treasury Board* e o *Department of Finance.* Enquanto os dois últimos têm seus próprios ministros, o PCO e o PMO reportam-se diretamente ao Primeiro-Ministro e têm papel importante na Administração Pública e na política canadense (GONÇALVES, 2008). O *Privy Council Office* (PCO) é o núcleo do serviço público de apoio ao Primeiro-Ministro e seu Gabinete. Estrutura a tomada de decisão, articula e ajuda a implementar a agenda política do Governo e a dar respostas aos problemas enfrentados pelo país, procurando manter os mais altos padrões profissionais e éticos no Serviço Público Federal (PCO, 2009).

4.2.4. O sistema jurídico

Brasil

O direito brasileiro tem origem na tradição romano-germânica e se caracteriza pelo primado da lei, com atribuição de valor secundário às demais fontes de direito[58]. A tradição latina ou continental (*civil law* – direito civil) acentuou-se após a Revolução Francesa, quando a lei passou a ser considerada a única expressão autêntica da Nação, da vontade geral (REALE, 2001).

Ao lado dessa tradição, que preconiza o elemento legislativo, há a tradição dos povos anglo-saxões (*common law* – direito comum), nos quais o direito se revela mais pelos usos e costumes[59] e pela jurisprudência[60] do que pelo trabalho abstrato e genérico dos parlamentos (REALE, 2001). É essa tradição que prevalece no Canadá, apesar de haver influências do direito civil na parte colonizada pelos franceses, na província de Quebéc.

A legislação brasileira advém do primado do processo legislativo, mas acolhe outras fontes de direito quando, diante do caso concreto, a lei não for satisfatória para proporcionar um julgamento justo. Conforme o artigo 4º, da Lei de Introdução ao Código Civil: "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito" (BRASIL, 1942). A analogia não é uma regra não escrita, e sim um método correspondente a uma técnica de integração do sistema de normas. Os princípios gerais de direito são normas escritas, postulados científicos, tipificados ou não. Os costumes são as normas não-escritas, mas podem vir a sê-lo, caso passem pelo crivo jurisprudencial.

O Poder Judiciário, cuja instância máxima é o Supremo Tribunal Federal é composto de onze ministros indicados pelo presidente sob aprovação do Senado, dentre indivíduos de renomado saber jurídico. A composição dos ministros do Supremo Tribunal Federal não é completamente renovada a cada mandato presidencial: o presidente somente indica um novo

---

[58] "Fontes de direito são os processos ou meios em virtude dos quais as regras jurídicas se positivam com legítima força obrigatória, isto é, com vigência e eficácia no contexto de uma estrutura normativa. São quatro as fontes de direito: o processo legislativo, expressão do Poder Legislativo; a jurisdição, do Poder Judiciário; os usos e costumes, do poder social; e a fonte negocial, do poder negocial ou da autonomia da vontade" (REALE, 2001, p. 140-141).

[59] "Usos e costumes baseiam-se na crença e na tradição, sob a qual está o argumento de que algo deve ser feito, e deve sê-lo porque sempre o foi. A autoridade repousa nesta força conferida ao tempo e ao uso contínuo como reveladores de normas" (FERRAZ JÚNIOR, 1994, p. 240).

[60] "A jurisprudência se processa em virtude de uma sucessão harmônica de decisões dos tribunais. Os juízes ao aplicarem o direito no caso concreto, para dirimir conflitos, deve realizar um trabalho prévio de interpretação das normas, que nem sempre são suscetíveis de uma única apreensão intelectual. Exige um esforço de superamento de entendimentos contrastantes, para aplicar as normas em consonância com as exigências da sociedade em um determinado momento e lugar. É a razão pela qual o direito jurisprudencial não se forma em uma ou três sentenças, mas exige uma série de julgados que guardem, entre si, uma linha essencial de continuidade e coerência quanto à substância das questões objeto de julgamento" (REALE, 2001, p. 167-168).

ministro quando um deles se aposenta ou vem a falecer (PORTAL, 2009). O cargo de juiz é ocupado por meio de concurso público, sem eleições, diferentemente do que ocorre com os chefes do Poder Executivo e membros dos Parlamentos.

Os tribunais se organizam em diversos ramos separados por competências, havendo um para a justiça comum e outros para justiça militar, trabalhista (relações entre empregados e empregadores) e eleitoral (organização e fiscalização de eleições). Assuntos de justiça comum que envolvem interesses da União devem ser julgados em tribunais federais. Os estados possuem seus tribunais para a justiça comum, organizados em uma primeira instância de julgamento por um juiz e uma segunda instância de julgamento colegiado (em grupo) por um tribunal (PORTAL, 2009).

Canadá

O Canadá possui um sistema jurídico rico tanto em tradição anglo-saxônica quanto romano-germânica, possuindo dois tipos de jurisprudência, o direito comum e o direito civil. O direito comum, de origem colonizadora anglo-saxônica, é empregado na maioria das províncias do país, enquanto que o direito civil é utilizado na província de Quebéc, de origem colonizadora francesa (CONSULADO, 2008*c*). No Canadá, suas leis são codificadas por influência do direito civil. Há uma mistura de fontes de direito, devido a sua colonização ter sido feita tanto por franceses, de origem romano-germânica, como pelos ingleses, de origem anglo-saxônica.

As leis estatutárias não compõem todas as leis do Canadá. Há muitas leis verbais que são baseadas nas tradições do direito comum. Isto é especialmente verdadeiro na área civil, que versa sobre assuntos particulares entre os indivíduos – propriedade, responsabilidades familiares e transações comerciais (CONSULADO, 2008*c*).

As leis civis, em 9 entre 10 províncias, baseiam-se na lei comum. O direito comum é um sistema baseado em precedente legal. Sempre que um juiz toma uma decisão, esta decisão torna-se um precedente, uma regra que orientará outros juízes quando estiverem considerando casos semelhantes no futuro. Muitas das leis canadenses são originadas desses precedentes e práticas comuns que se desenvolveram ao longo dos anos (CONSULADO, 2008*c*).

Em Quebéc, entretanto, o direito civil baseia-se em um código escrito – o Código Civil – que contém princípios gerais e regras para diferentes tipos de casos. Diferentemente da lei comum, o juiz primeiro se orienta pelo código e depois considera os precedentes de decisões anteriores (CONSULADO, 2008*c*).

As leis canadenses são interpretadas e aplicadas pelas côrtes, que são presididas por juízes, cuja independência é garantida, como ocorre no Brasil. Cada província estabelece sua própria côrte, que trata de questões provenientes tanto da lei federal quanto provincial. Além disso, o Parlamento federal estabeleceu uma côrte geral de apelação para o Canadá e várias côrtes de jurisdição especializada (CONSULADO, 2008*c*).

4.2.5. O processo legislativo

Brasil

O processo legislativo abrange a elaboração das leis propriamente ditas (lei ordinária, lei complementar, lei delegada), e também a das emendas constitucionais, das medidas provisórias, dos decretos legislativos e das resoluções, sendo desdobrado nas seguintes etapas: a) iniciativa; b) discussão; c) deliberação ou votação; d) sanção ou veto; e) promulgação; f) publicação (MENDES; FORSTER JR., 2002).

A iniciativa é a proposta de edição de direito novo. A discussão e a votação dos projetos de lei de iniciativa do Presidente da República, do Supremo Tribunal Federal, dos Tribunais Superiores e da iniciativa popular terão início na Câmara dos Deputados. Há também iniciativas originárias da Câmara dos Deputados e do Senado. O projeto de lei aprovado por uma casa será revisto pela outra em um só turno de discussão e votação. No caso de proposição normativa submetida a regime de urgência (medida provisória), se ambas as Casas não se manifestarem cada qual, sucessivamente, em até quarenta e cinco dias, o projeto deve ser incluído na ordem do dia, ficando suspensas as deliberações sobre outra matéria, até que seja votada a proposição do Presidente (MENDES; FORSTER JR., 2002).

A votação da matéria legislativa constitui ato coletivo das Casas do Congresso. Realiza-se, normalmente, após a instrução do Projeto nas comissões e dos debates no Plenário. Essa decisão toma-se por maioria de votos: maioria simples (maioria dos membros presentes) para aprovação dos projetos de lei ordinária; e maioria absoluta dos membros das Casas para aprovação dos projetos de lei complementar (MENDES; FORSTER JR., 2002).

A sanção é o ato pelo qual o Chefe do Executivo manifesta a sua aquiescência ao projeto de lei aprovado pelo Poder Legislativo. A sanção pode ser expressa ou tácita. Será expressa quando o Presidente da República manifestar a sua concordância, no prazo de 15 dias úteis, contados daquele em que o recebeu, excluído esse. A sanção tácita ocorre quando decorrido o prazo de quinze dias úteis sem manifestação expressa do Chefe do Poder Executivo, considera-se sancionada tacitamente a lei (MENDES; FORSTER JR., 2002).

O veto é o ato pelo qual o Chefe do Poder Executivo nega sanção ao Projeto – ou a parte dele –, obstando à sua conversão em lei. O Projeto volta ao Congresso, se o veto for mantido por este, o projeto, ou parte dele, há de ser considerado rejeitado, podendo a matéria dele constante ser objeto de nova proposição. Contudo, o Congresso Nacional poderá, em sessão conjunta, rejeitar, em escrutínio secreto, o veto, pela manifestação da maioria absoluta de Deputados e de Senadores. Se o veto não for mantido, será o projeto enviado, para promulgação, ao Presidente da República. Se a lei não for promulgada dentro de quarenta e oito horas pelo Presidente da República, o Presidente do Senado o promulgará (MENDES; FORSTER JR., 2002).

A promulgação atesta a existência da lei, produzindo dois efeitos básicos: reconhece os fatos e atos geradores da lei; e indica que a lei é válida. A promulgação compete ao Presidente da República. A publicação constitui a forma pela qual se dá ciência da promulgação da lei aos seus destinatários. É condição de vigência e eficácia da lei (MENDES; FORSTER JR., 2002). Nos níveis estadual e municipal da federação ocorre processo semelhante.

Canadá

Dentro dos limites impostos pela Constituição, as leis podem ser criadas ou alteradas por meio de estatutos aprovados pelo Parlamento ou por uma legislatura provincial ou territorial. As leis estatutárias automaticamente assumem o lugar de quaisquer precedentes verbais conflitantes, ou lei comum, que versem sobre o mesmo assunto (CONSULADO, 2008*c*).

Qualquer membro do Parlamento ou legislatura provincial pode propor uma nova lei, mas a maioria delas é primeiro formulada pelo Governo em vigor. Uma lei proposta deve ser apresentada para a consideração de todos os membros do Parlamento, que a estudam e a debatem. A proposta torna-se uma lei estatutária se for aprovada pela maioria (CONSULADO, 2008*c*).

Para um projeto de lei federal tornar-se lei deve ser iniciado ou no Senado ou na Câmara dos Comuns. Em cada Casa Legislativa, o projeto passa por três leituras e em seguida recebe autorização real (DSP, 2007).

São dois tipos de projetos de lei, os públicos e os privados. Os projetos de lei públicos são propostas de leis que afetam o público em geral. A maioria dos projetos públicos é introduzida pelos Ministros. Os projetos de lei privados são de âmbito limitado, se referem a

um indivíduo ou grupo de indivíduos somente. Eles conferem um direito sobre uma pessoa ou grupo, ou isenta de uma responsabilidade (DSP, 2007).

A proposta legislativa é apresentada ao Gabinete dos Ministros para uma comissão adequada que fará recomendações para o Gabinete. Se os Ministros aprovarem, o Ministro responsável por aquela matéria encaminhará o projeto para a Seção Legislativa do Departamento de Justiça elaborar a lei. Esta deve ser realizada em duas línguas oficiais, francês e inglês, e aprovada pelo Ministro responsável. Depois este submete o projeto para a aprovação do Gabinete dos Ministros. Se aprovado seguirá para o Parlamento (DSP, 2007).

A primeira leitura do projeto é feita ou Senado ou na Câmara dos Comuns de forma impressa. Na segunda leitura, na mesma Casa, é feito debate e votação dos membros sobre o princípio do projeto de lei. Remete para a avaliação do projeto de lei em uma comissão especial ou para Comissão Geral. Na comissão parlamentar competente será analisada cláusula por cláusula, podendo convocar peritos que forneçam informações para melhorar o texto do projeto. O relatório da comissão é remetido à Casa, indicando as propostas de alteração. A Casa vota a favor ou contra essas propostas. Na terceira leitura, há debate e votação do projeto alterado. Uma vez lido em uma das Casas, remete-se para a outra Casa fazer suas considerações (DSP, 2007).

Posteriormente o projeto é apresentado ao Governador Geral para dar seu parecer. O parecer pode ser favorável e é dado em nome da Rainha, ou ser retido ou favorável com reservas. Quando é dada a autorização real, torna-se lei o projeto de lei (DSP, 2007).

Importa igualmente notar que atualmente só o Governo Federal é bicameral (Senado e Câmara dos Comuns). As províncias são todas unicamerais. O legislativo provincial geralmente é chamado de Assembléia Legislativa (em Quebéc - *Assemblée Nationale*).

As mudanças podem ser feitas para o projeto até a terceira leitura em cada Casa. Após a terceira leitura, tanto na Câmara dos Comuns e no Senado, o projeto deve receber aprovação da Coroa (*Royal Assent*), a fim de se tornar lei. Ela recebe um número de capítulo e é publicado no volume anual de estatutos. Salvo disposição em contrário do ato da Coroa, este tem imediata força de lei. Quando não entram em vigor no momento da *Royal Assent* são proclamados em uma data posterior.

4.2.6. Relações bilaterais

Canadá e Brasil possuem vastos territórios, com algumas regiões escassamente habitadas, riquezas naturais e diversidade cultural, incluindo as populações indígenas. O

Brasil representa mais da metade da América do Sul em termos de superfície, população e economia. É um importante participante nas questões mundiais relativas à liberação do comércio, segurança internacional e reforma das Nações Unidas (CONSULADO, 2009).

Canadá abriu seu primeiro escritório comercial no Brasil em 1866, e a Embaixada em 1944. Nos anos seguintes à Segunda Guerra Mundial, o Brasil foi o centro da política externa canadense na América do Sul. No Brasil, o Canadá é representado pela Embaixada do Canadá em Brasília e pelos Consulados Gerais em São Paulo e Rio de Janeiro. Há também um escritório comercial em Belo Horizonte e uma Agência Canadense de Desenvolvimento Internacional em Recife. No Canadá o Brasil é representado por uma Embaixada em Otawa, e por consulados em Halifax, Montreal, Toronto, e Vancouver (CONSULADO, 2009).

As relações do Canadá com o Brasil estão crescendo, o que é confirmado pelo nível elevado de visitas oficiais, pela expansão do comércio e de investimentos e por um maior interesse mútuo em aprender mais sobre o outro, tanto sob a ótica das políticas públicas como sob a perspectiva individual (CONSULADO, 2009).

Os dois países mantêm regularmente consultas bilaterais formais para questões políticas e de segurança internacional. A cooperação em diversas áreas, tais como direitos humanos, governança, federalismo, diversidade cultural, meio ambiente, trabalho, assuntos indígenas, esportes, saúde e educação contribuem igualmente para fortalecer as relações (CONSULADO, 2009).

Canadá e Brasil assinaram uma série de acordos, tratados e memorandos de entendimento com o passar dos anos. Uma das mais recentes iniciativas entre os dois países é o estabelecimento de um Acordo-Quadro de Cooperação em Ciência, Tecnologia e Inovação, assinado em novembro de 2008. O Acordo Canadá-Brasil Ciência e Tecnologia dará oportunidades de cooperação bilateral em áreas de interesse comum. O acordo vai estimular e acelerar as atividades de investigação e desenvolvimento comercial do setor, favorecendo a indústria e a colaboração entre universidades e indústrias (CONSULADO, 2009).

Do ponto de vista multilateral, o Canadá e o Brasil trabalham cada vez mais juntos na Organização dos Estados Americanos (OEA) e na Organização das Nações Unidas (ONU), entre outras organizações. Áreas de interesse comum incluem a pesca predatória, a promoção da diversidade cultural, o envolvimento em operações de manutenção da paz e avanços no respeito pelos direitos humanos no mundo (CONSULADO, 2009).

Após breve caracterização e comparação do Brasil e do Canadá em termos culturais, estruturais e proximidades realizadas entre ambos, seguem suas regulamentações referentes à PSI.

CAPÍTULO 5 - REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)– BRASIL E CANADÁ

Após serem apresentados o conceito de regulamentação e as caracteríscas dos Estados Brasil e Canadá, será descrito o que foi, como foi e por que foi regulamentado sobre a PSI dos Governos Eletrônicos do Brasil e Canadá.

Foram pesquisadas as regulamentações específicas e correlacionadas ao tema PSI dos países Brasil e Canadá. Pelo fato de se ter compilado grande parte da regulamentação e esta ser ampla para descrevê-la neste texto, foram criados APÊNDICES[61] com essa informação, separando-se as normas por hierarquia, lapso temporal, ementa, artigos e tradução (quando do Canadá) relacionados à PSI.

Para que o texto seja mais claro e objetivo as regulamentações foram descritas por meio de temáticas referentes à PSI.

5.1. Segurança da Informação

Brasil

1) A primeira norma específica sobre a PSI no Brasil foi o Decreto n° 3.505, 2000 (BRASIL, 2000*j3*)[62], criado pelo Poder Executivo (Presidente da República), tendo em vista o disposto na Lei n° 8.159, 1991 (BRASIL, 1991*m2*)[63], e no Decreto n° 2.910, 1998 (BRASIL, 1998), que tratam respectivamente sobre a política nacional de arquivos públicos e privados; e estabelece normas para a salvaguarda de documentos, materiais. Entretanto o Decreto n° 2.910, 1998 (BRASIL, 1998) foi revogado pelo Decreto n° 4.553, 2002 (BRASIL, 2002*g2*)[64], que consolidou a legislação regulamentar referente a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.

O motivo da criação da norma sobre PSI na Administração Federal foi para adequá-la às novas tecnologias e formas de obtenção, armazenamento, processamento, distribuição, uso

[61] APÊNDICE A – Normas Relacionadas à Segurança da Informação: Brasil, 129.
APÊNDICE B – Normas Relacionadas à Segurança a Informação: Canadá, 149.
APÊNDICE C – Normas Técnicas Internacionais, 162.
[62] APÊNDICE A, p. 141.
[63] APÊNDICE A, p. 135.
[64] Ver item 5.3. Privacidade, p. 84; e APÊNDICE A, p. 139.

e descarte das informações. Tem como intuito ser referência de aplicação da PSI nos órgãos da Administração Pública. Os pressupostos da referida norma visam assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações; o uso soberano de mecanismos de segurança da informação; a criação, desenvolvimento e manutenção de mentalidade de segurança da informação; a capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e a conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

São objetivos da PSI, dentre outros, dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis (BRASIL, 2000*j3*).

O Decreto n° 3.505, 2000 (BRASIL, 2000*j3*) institui também o Comitê Gestor da Segurança da Informação (CGSI), para assessorar, juntamente com a Agência Brasileira de Inteligência – ABIN, a Secretaria-Executiva do Conselho de Defesa Nacional[65] na consecução das diretrizes da PSI nos órgãos e nas entidades da Administração Pública Federal a fim de tornar mais seguro e ágil o processo de decisão dos governantes. O Conselho de Defesa Nacional (CDN) – órgão de consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do Estado Democrático – foi criado pelo Poder Legislativo (Congresso Nacional) pela Lei nº 8.183, 1991 (BRASIL, 1991*m1*)[66], para dispor sobre a organização e o funcionamento do CDN, após ser extinto o Serviço Nacional de Informações (SNI) em 1990.

2) O Decreto n° 4.376, 2002 (BRASIL, 2002*g3*)[67], regulamenta a organização e o funcionamento do Sistema Brasileiro de Inteligência (SBIN), instituído pela Lei n° 9.883, 1999 (BRASIL, 1999*k2*)[68] que também criou a ABIN. O SBIN foi criado pelo Poder Legislativo, por meio do processo legislativo para integrar as ações de planejamento e

[65] O Conselho de Defesa Nacional CDN, órgão de consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do Estado, é presidido pelo Presidente da República e dele participam, como membros natos: o Vice-Presidente da República; o Presidente da Câmara dos Deputados; o Presidente do Senado Federal; o Ministro da Justiça; os Ministros Militares; o Ministro das Relações Exteriores; o Ministro de Estado Chefe da Secretaria de Planejamento, Orçamento e Coordenação da Presidência da República (BRASIL, 2000*j3*).
[66] APÊNDICE A, p. 135.
[67] APÊNDICE A, p. 139.
[68] APÊNDICE A, p. 134.

execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. O motivo de sua concepção foi o de preservar a soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária.

O SBIN é responsável pelo processo de obtenção e análise de dados e informações e pela produção e difusão de conhecimentos necessários ao processo decisório do Poder Executivo, em especial no tocante à segurança da sociedade e do Estado, e salvaguarda de assuntos sigilosos de interesse nacional. Cabe à ABIN (órgão da Presidência da República), na posição de órgão central do SBIN, planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País (BRASIL, 1999*k2*).

O SBNI e a ABIN foram criados recentemente na década de 1990, após o período de redemocratização brasileira, em 1985. Anteriormente, o responsável pela inteligência e segurança era o SNI – Serviço Nacional de Inteligência, criado pela ditadura militar em 1964. Tinha como razão a necessidade do Poder Executivo dispor de informações seguras, oportunas e convenientemente avaliadas que sirvam de base às múltiplas decisões a tomar. Entre 1985 e 1990, o SNI continuou em funcionamento. No governo de Fernando Affonso Collor de Mello (1990-1992), entre seus primeiros atos, o SNI foi extinto em 15 de março de 1990, num contexto de reestruturação da Administração Pública Federal. Na segunda metade da década de 1990, no governo Fernando Henrique Cardoso (1995-1998) ressurgiu a discussão sobre a importância do Estado brasileiro possuir um serviço de inteligência, e criou em 1997 um grupo de trabalho para elaborar um Projeto de Lei a ser submetido no Congresso (GONÇALVES, 2008).

Vários modelos e serviços de inteligência pelo mundo foram analisados. Dentre eles, o modelo canadense, *Canadian Security Intelligence Service* (CSIS) pareceu o mais interessante à realidade brasileira: uma única organização civil, sem poder de polícia, com atribuições de inteligência interna, externa e contra-inteligência, voltada sobretudo para a segurança doméstica, mas sem caráter repressivo-autoritário, e conduzindo suas atividades na estrita observância do ordenamento jurídico-constitucional em defesa do Estado Democrático e da sociedade (GONÇALVES, 2008).

O Projeto de Lei n° 3.651 (BRASIL, 1997*i1*) foi remetido ao Congresso Nacional em 19 de setembro de 1997, dispondo sobre a instituição do SBNI e a criação da ABIN –

estruturada conforme a CSIS[69]. A ABIN deveria estar sob controle externo, como ocorre no Canadá, nos Estados Unidos e outras democracias. Entretano, no Projeto proposto pelo Executivo o controle externo da atividade de inteligência no Brasil caberia ao Congresso Nacional. Depois de discutido no Congresso, o projeto entrou em vigor pela Lei n° 9.883, 1999 (BRASIL, 1999*k2*).

3) A Lei nº 11.754, 2008 (BRASIL, 2008*b4*)[70] é uma norma que trata indiretamente do tema PSI, dispondo sobre a função do Gabinete de Segurança Institucional da Presidência da República (GSI). Foi criada pelo Poder Legislativo por meio do processo legislativo. Tem como fim, dentre outros, definir as atribuições do GSI, que é assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, coordenar as atividades de inteligência federal e de segurança da informação.

A Portaria Nr 11 - CH/GSI, 2003 (BRASIL, 2003*f1*)[71], criada pelo Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI), institui, no âmbito do Comitê Gestor de Segurança da Informação[72] (CGSI), o Grupo de Trabalho do Programa de Proteção ao Conhecimento e Segurança da Informação. Tem como finalidade desenvolver e propor um programa de proteção ao conhecimento e segurança da informação para aplicação nos diversos órgãos da Administração Pública Federal, para haver uniformidade e efetiva aplicação da PSI nesses órgãos.

A Instrução Normativa nº 4, 2008 (BRASIL, 2008*b2*), foi criada pela Secretaria de Logística e Tecnologia, vinculada ao Ministério do Planejamento, Orçamento e Gestão, do Poder Executivo. Tem como intuito adequar e formalizar o processo de contratação de serviços de TI pela Administração Pública Federal direta, autárquica e fundacional, pois não havia nos órgãos do Governo Federal critérios para assegurar a segurança das informações do

[69] O CSIS e a ABIN tiveram em sua criação grande influência das reações da sociedade civil e das autoridades governamentais às condutas arbitrárias dos serviços que os antecederam (o SNI e o *Security Service* – anos 1960 e 1970). Tanto no Brasil quanto no Canadá, os serviços de informações estiveram intensamente envolvidos com segurança doméstica e combate à subversão e inimigos internos. No caso canadense, houve luta contra o separatismo da Província de Québec (colonizada por franceses), e no Brasil, a luta armada contra o regime militar. Os dois países sofreram com o terrorismo doméstico nos anos 1960 e 1970 e vivenciaram reações dos serviços de segurança interna contra os chamados "grupos subversivos". As condutas desses serviços foram profundamente criticadas pela comunidade de informações nos dois países e clamores por reformas, contribuindo para o preconceito com relação à atividade de inteligência (GONÇALVES, 2008).

[70] APÊNDICE A, p. 133.

[71] APÊNDICE A, p. 144.

[72] O CGI tem 320 redes ligadas ao Poder Executivo, entre elas, Receita Federal, Serpro, Banco Central. Em agosto de 2008, o Tribunal de Contas da União determinou ao Governo Federal a unificação da sua PSI, quando 48% dos órgãos federais não possuíam políticas de segurança estruturadas e 64% não adotavam qualquer medida restrita de acesso às informações. Em dados contabilizados em agosto de 2008, o Centro de Incidência de Redes, do Poder Executivo, subordinado ao Gabinete Institucional da Presidência da República, registrou 2.100 tentativas de invasão/dia no Governo Federal (SERPRO, 2008).

governo, a transferência do conhecimento para o governo e a continuidade dos serviços em caso de uma eventual interrupção no contrato. Em vista disso, a norma determina que a gestão de processos de TI, assim como as atividades de coordenação na área de segurança de sistemas não podem ser terceirizadas, deverão seguir porcessos de contratação conforme estipulada em seu conteúdo, a fim de evitar o acesso e transferência de informações por terceiros não autorizados para tanto.

4) A Medida Provisória nº 2.200-2, 2001 (BRASIL, 2001*h4*)[73], institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. Foi criada pelo Poder Executivo, como uma forma de ingerência no âmbito do Poder Legislativo, ao legislar uma medida provisória sobre matéria importante que não demandava urgência e relevância. Foi uma forma de pressionar o Poder Legislativo a legislar sobre a matéria. A norma tem como intuito garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Criou o Comitê Gestor da ICP-Brasil para, dentre outras prerrogativas, promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança. Transformou o Instituto Nacional de Tecnologia da Informação (ITI) em uma autarquia federal, subordinada ao Ministério da Ciência e Tecnologia, dando-lhe atribuição de Autoridade Certificadora Raiz da ICP-Brasil[74].

O Decreto nº 6.605, 2008 (BRASIL, 2008*b1*)[75], regulamenta o Comitê Gestor da ICP-Brasil e o Decreto n° 3.996, 2001 (BRASIL, 2001*h2*)[76], dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal - subordinados à ICP-Brasil. Ambos foram criados pelo Poder Executivo tendo como referência a Medida Provisória nº 2.200-2, 2001 (BRASIL, 2001*h4*), para torná-la aplicável e efetiva, enquanto não é transformada em lei pelo Poder Legislativo.

[73] APÊNDICE A, p. 136.
[74] A Autoridade Certificadora Raiz (AC) da ICP-Brasil é a primeira autoridade da cadeia de certificação. É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu. A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor (ITI, 2009).
[75] APÊNDICE A, p. 137.
[76] APÊNDICE A, p. 140.

Canadá

1) A lei canadense específica sobre segurança da informação é a *Security of Information Act*, 1985 (CANADA, 1985*q*)[77]. Foi criada pelo Poder Legislativo (Parlamento), por meio do processo legislativo. No Canadá há modificações nas legislações, contudo, não são expressas como ocorre nas leis brasileiras. Apesar de ser uma lei de 1985, foi reformulada em 24 de dezembro de 2001, para se adequar ao *Government Security Policy - Operational Standard for the Security of Information Act*. Esta reforma tem por finalidade reforçar a política de segurança da informação, com foco no cidadão, nos valores, nos resultados e nos gastos responsáveis. A tendência em focar nesses fatores se deve pelo movimento mundial de privilegiar os verdadeiros soberanos, que são os cidadãos, realçar os valores humanos e cobrar dos governantes resultados e a forma de seus gastos com o erário público. A norma também condena o indivíduo que receber qualquer código secreto oficial, palavra, senha, esboço, plano, modelo, artigo, nota, documento ou informação, estará infringindo a Lei, salvo se provar que o recebimento do código era contrário ao seu desejo. É uma medida de salvaguarda das informações estatais e de punição aos infratores.

2) A *Canadian Security Intelligence Service Act*, 1985 (CANADA, 1985*m*)[78] é uma norma criada pelo Parlamento após três anos de discussão, para estabelecer o Serviço de Inteligência – *Canadian Security Intelligence Service* (CSIS) –, extinguir o *Security Service*[79], e definir as ameaças à segurança do Canadá como espionagem ou sabotagem. Conforme a norma, as informações obtidas no desempenho das atribuições e funções do CSIS não devem ser divulgadas, protegendo a privacidade e assuntos sigilosos de interesse nacional. O CSIS é um serviço civil, subordinado ao Ministro de Segurança Pública, voltado à segurança interna, mas com mandato para realizar inteligência externa em defesa dos interesses canadenses. Seus servidores não têm poder de polícia, tendo como função reunir, analisar e manter informações e produzir inteligência no que concerne a atividades que representem ou possam vir a representar ameaça à segurança do Canadá. A função precípua do CSIS é assessorar o processo decisório governamental, trabalha também com produção de informações sobre ameaças a sistemas críticos de informação e à infra-estrutura. A lei cria também o órgão

[77] APÊNDICE B, p. 153.
[78] APÊNDICE B, p. 154.
[79] Na década de 1970 foi criado o *Security Service*, vinculado à *Royal Canadian Mounted Police* (RCMP), mudando a estrutura organizacional para separar as atividades de inteligência e as de investigação criminal relacionadas à segurança nacional. Até 1984, a atividade de inteligência ficou a cargo do *Security Service*, voltado à segurança interna e à contra-espionagem. Em suas atividades, envolveu-se em escândalos, sendo acusado de arbitrariedades e de invasão da privacidade de cidadãos canadenses. Suas atividades intrusivas geraram questionamentos na sociedade contra os poderes dos serviços secretos (GONÇALVES, 2008).

independente de controle externo para o CSIS, o *Security Intelligence Review Commitee* (SIRC), que deveria se reportar ao Parlamento (GONÇALVES, 2008). O emprego dos serviços de inteligência a proteção de sistemas de informações e de infra-estrutura é tema que tem estimulado muitos estudos e é objeto de preocupação cada vez maior das autoridades canadenses.

3) *National Defence Act*, 1985 (CANADA, 1985o)[80], é uma norma criada pelo Parlamento sobre a defesa nacional. Tem como justificativa legislar sobre a defesa nacional e defender os interesses canadenses e sua soberania. Estabelece o *Communications Security Establishment Canada* (CSEC), a fim de (a) adquirir e usar informação de infra-estrutura global, de acordo com prioridades de inteligência do Governo do Canadá; (b) aconselhar, orientar e ajudar a garantir serviços para a proteção de informação eletrônica e de informação de infra-estruturas de grande importância para o Governo do Canadá; e (c) prestar assistência técnica e operacional para a aplicação da lei federal e agências de segurança no desempenho das suas funções legais. É uma norma sobre defesa nacional e conseqüente defesa das informações do Estado, salvaguardando a segurança das informações. O CSEC foi criado em 1996 para fiscalizar o CSE (*Communications Security Establishment*) criado em 1975. A equipe de Segurança de TI do CSEC dispõe de orientação de vanguarda e aconselhamento estratégico sobre a segurança de TI do Governo do Canadá. Trabalhando em parceria com os ministérios, as agências e as empresas privadas, o CSEC define novos produtos de TI, serviços e prestações de serviços estratégicos referentes às necessidades operacionais e prioridades para o Governo do Canadá a fim de garantir a segurança dos sistemas de informação. O CSEC criou o acordo *Cyber Protection Supply Arrangement* (CPSA), em 2008, com o objetivo de apoiar o Governo do Canadá na realização de uma política de segurança coerente e dar respostas adequadas aos atuais riscos e ameaças de segurança de informações (CSEC, 2008).

4) O CSEC e o *National Institute of Standards and Technology* (NIST) criaram em conjunto o *Cryptographic Module Validation Program* (CMVP) em 17 de julho de 1995. O CMVP é uma norma de validação de criptografia originada em acordo conjunto pelo Canadá com o CSEC e pelos Estados Unidos com a NIST, agência federal dos Estados Unidos do *Commerce Department's Technology Administration*.

O motivo da criação do CMVP é para validar modelos de criptografia comercial para *Federal Information Processing Standard* (FIPS) 140-2 e outras normas, como a criptografia

[80] APÊNDICE B, p. 156.

baseada em algoritmos. O CMVP é gerido conjuntamente pelo NIST e CSEC. Os produtos validados conforme a FIPS 140-2 são aceitos pelas agências federais dos países para a proteção das informações sensíveis (Estados Unidos) ou informações protegidas (Canadá). O objetivo do CMVP é o de promover a utilização de modelos criptográficos válidos e fornecer às agências federais de segurança uma métrica para usar na aquisição de equipamentos que contenham modelos criptográficos válidos (CSEC, 2008).

O *Secure Electronic Signature Regulations* (CANADA, 2005*f*)[81] criado pelo Governador Geral do Conselho, sob recomendação do *President of Treasury Board*, regulamenta a segurança das assinaturas eletrônicas, em conformidade com a subseção 48 (1) da *Personal Information Protection and Electronic Documents Act* (CANADA, 2000)[82] e parágrafo e 31,4 (a) da *Canada Evidence Act* (CANADA, 1985*l*)[83]. Define a autoridade certificadora como uma entidade que emite certificados de assinatura digital, sendo a autoridade certificadora a Secretaria do *Treasury Board of Canadá*, vinculada ao Governo.

A *Personal Information Protection and Electronic Documents Act* (CANADA, 2000), foi criada em 2000 pelo Parlamento canadense para inserir medidas de proteção a informação pessoal no setor privado, criar uma alternativa eletrônica para fazer negócios com o Governo Federal, e esclarecer a forma como os tribunais irão avaliar a confiabilidade dos registros eletrônicos utilizados como provas. O objetivo declarado do Governo é em razão de tornar o Canadá líder mundial no comércio eletrônico.

5.2. Acesso à Informação

Brasil

1) O acesso à informação é assunto resguardado pela Constituição Federal (BRASIL, 2009*a1*)[84], criada em 1988 pela Assembléia Nacional Constituinte, dissolvida após sua conclusão. O intuito de uma Constituição é conter os princípios que deverão ser seguidos pelas legislações infraconstitucionais e prescrever os ideais da nação. A Constituição de 1988,

[81] APÊNDICE B, p. 157.
[82] APÊNDICE B, p. 152.
[83] APÊNDICE B, p. 152.
[84] Preâmbulo da Constituição da República Federativa do Brasil: "Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL" (BRASIL, 2009). APÊNDICE A, p. 130.

conhecida como “Constituição Cidadã”, foi criada para restabelecer a democracia no país após o período de ditadura militar (1964-1985), primando, dentre outros, pelo princípio da Publicidade (artigo 37), que rege o direito de acesso à informação e limita as práticas sigilosas dos agentes públicos.

O sistema constitucional brasileiro foi criado no período imperial e sucessivamente reconstruído ao longo da República. A primeira Constituição foi a Constituição de 1824, por D. Pedro I após a dissolução da Assembléia Constituinte de 1823. Com o fim do Império e início da República foi criada a Constituição de 1891 pelo Congresso Constituinte. Com a Revolução de 1930, em 1933, foi eleita a Assembléia Constituinte para redigir a Constituição da República Nova de 1934. Em 1937 é implantada a ditadura do Estado Novo e criada a Constituição de 1937. Finalizada a ditadura do Estado Novo foi promulgada a Constituição de 1946 pela Assembléia Constituinte, consagrando as liberdades expressas na Constituição de 1934, que haviam sido retiradas em 1937. A Constituição de 1946 também foi substituída pela Constituição de 1967 e, posteriormente, pela Constituição de 1969, época da ditadura militar. Iniciada a redemocratização brasileira em 1985, a atual Constituição foi promulgada em 1988.

A Constituição de 1988 (BRASIL, 2009*a1*) legisla sobre o acesso à informação em vários artigos para assegurá-lo aos cidadãos brasileiros, o que nem sempre foi resguardado em Constituições anteriores. Em seu artigo 5º, XIV, assegura a todos o acesso à informação e deixa resguardado o sigilo da fonte, quando necessário ao exercício profissional. Neste artigo, há defesa ao direito de acesso à informação, mas ao mesmo tempo o sigilo das informações relacionadas à intimidade ou à vida privada de alguém, e deixa resguardado o sigilo profissional. No mesmo artigo 5º, XXXIII, dispõe que todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Este artigo é regulamentado pela Lei nº 11.111, 2005 (BRASIL, 2005*d4*)[85], criada pelo Congresso Nacional, para regular o direito à informação e ao acesso aos registros públicos.

Outro instituto previsto na Constituição é o *habeas data* (BRASIL, 2009*a1*, art. 5°, LXXII), destinado ao direito de conhecer o conteúdo de informações a respeito do impetrante sob a guarda do Estado. A Lei nº 9.507, 1997 (BRASIL, 1997*i3*)[86], criada pelo Congresso Nacional, regulamenta o direito de acesso a informações e disciplina o rito processual do *habeas data*, para dar efetividade ao artigo 5°, LXXII, da Constituição (BRASIL, 2009*a1*).

[85] APÊNDICE A, p. 133.
[86] APÊNDICE A, p. 134.

O *habeas data* foi inovação da Constituição Federal de 1988, fruto de uma experiência constitucional anterior em que o governo arquivava, a seu critério e sigilosamente, dados referentes a convicção filosófica, política, religiosa e de conduta pessoal dos indivíduos. É um instituto baseado no *habeas data* originado nos Estados Unidos em 1974. A partir do *habeas data* começaram os pedidos de informações junto ao SNI e aos órgãos que o sucederam relativas aos arquivos do período militar. A ABIN chegou a criar um setor encarregado de responder a esses pedidos, informando ao solicitante se há registros nos arquivos do serviço de inteligência sobre o indivíduo que solicitava essas informações. O *habeas data* não se confunde com a garantia à informação, previsto pelo mesmo artigo 5°, XXXIII da Constituição (BRASIL, 2009*a1*), pois a informação protegida pelo *habeas data* é sempre relativa à pessoa do impetrante, com a particularidade de constar de banco ou registro de dados pela Administração Pública, sendo uma via judicial. Contudo, o direito à informação exercido na via administrativa é mais amplo e pode se referir a temas variados (GONÇALVES, 2008).

O artigo 37, § 3º da Constituição (BRASIL, 2009*a1*) também dispõe sobre o direito à informação e ao acesso aos registros públicos. Representa a disponibilidade das informações constantes nos órgãos públicos, como o faz o artigo 5º, XXXIV da Constituição (BRASIL, 2009*a1*) que dá o direito de petição e de obtenção de certidões em repartições públicas, assegurados a todos, independentemente do pagamento de taxas. Cultuou o princípio da Publicidade dos atos da Administração Pública e limitou bastante quaisquer práticas sigilosas por parte dos agentes públicos.

2) A Lei Complementar nº 75, 1993 (BRASIL, 1993)[87], foi criada pelo Congresso Nacional para estabelecer a organização, as atribuições e o estatuto do Ministério Público da União. Dentre as atribuições que prescreve para o Ministério Público da União, dispõe que este poderá requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta; e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública.

3) O Decreto nº 5.482, 2005 (BRASIL, 2005*d2*)[88], criado pelo Poder Executivo em razão da tendência mundial dos Governos Eletrônicos em tornar públicos seus dados e informações na Internet, em páginas de governo. A norma dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet. Foi criado o Portal da Transparência do Poder

[87] APÊNDICE A, p. 132.
[88] APÊNDICE A, p. 138.

Executivo Federal (sítio eletrônico) para veicular dados e informações detalhados sobre a execução orçamentária e financeira da União, no intuito de tornar a Administração Pública Federal mais transparente, apesar de algumas informações só poderem ser entendidas por técnicos da área. Mas não deixa de ser um avanço do Governo pela manifestação do princípio da Publicidade e da transparência.

Canadá

1) O acesso à informação é assunto também resguardado pela Constituição do Canadá (CANADA, 1982)[89]. A Constituição do Canadá[90] é um conjunto de leis constitucionais, conhecida como *Consolidation of Constitution Acts*, 1867 *to* 1982. A Consolidação contém o texto da *Constitution Act, 1867* (anteriormente conhecido como *British North America Act, 1867),* juntamente com as alterações feitas a ela desde a sua promulgação, e o texto da *Constitution Act, 1982,* alterada desde a sua promulgação. A *Constitution Act, 1982* teve como intuito findar o controle do Reino Unido sobre as emendas da Constituição, e seus poderes restantes no Canadá. Contém ainda a *Canadian Charter of Rights and Freedoms* (Carta Canadense dos Direitos e Liberdades) que estabelece os direitos básicos das pessoas que estão em território canadense (CONSULADO, 2008*c*), dentre eles o direito de acesso à informação.

A Constituição do Canadá (CANADA, 1982) legisla sobre o acesso à informação na parte emendada pela *Constitution Act, 1982 – Canadian Charter of Rights and Freedoms,* criada pelo Parlamento canadense, sem influências do Parlamento do Reino Unido para

---

[89] Preâmbulo da *Consolidation of the Constitution Acts*, 1867 to 1982: *"An Act for the Union of Canada, Nova Scotia, and New Brunswick, and the Government thereof; and for Purposes connected therewith (29th March 1867). Whereas the Provinces of Canada, Nova Scotia, and New Brunswick have expressed their Desire to be federally united into One Dominion under the Crown of the United Kingdom of Great Britain and Ireland, with a Constitution similar in Principle to that of the United Kingdom:And whereas such a Union would conduce to the Welfare of the Provinces and promote the Interests of the British Empire:And whereas on the Establishment of the Union by Authority of Parliament it is expedient, not only that the Constitution of the Legislative Authority in the Dominion be provided for, but also that the Nature of the Executive Government therein be declared:And whereas it is expedient that Provision be made for the eventual Admission into the Union of other Parts of British North America:1. This Act may be cited as the Constitution Act, 1867"* (CANADA, 1982). APÊNDICE B, p. 150.

[90] Para efeitos de entendimento da Constituição do Canadá (CANADA, 1982), conceitua-se Constituição e como ela é aplicada no Canadá e em outros países anglo-saxões. De acordo com o *Intergovernmental Affairs* vinculado ao *Privy Council Office* (PCO) do Canadá, uma Constituição é o conjunto de regras que definem os princípios políticos, as instituições, os poderes e as responsabilidades dos cidadãos, podendo incluir uma carta de direitos humanos. É considerada a lei suprema, fundamental de um Estado, contendo princípios que deverão ser seguidos pelas legislações infraconstitucionais. Na maioria dos Estados, a Constituição é escrita, ou seja, suas regras são codificadas, ou em um único texto (como a Constituição dos Estados Unidos) ou em uma série de leis constitucionais (como a Constituição canadense). No Reino Unido a Constituição é um conjunto de regras não codificado (costumes), com base em estatutos, jurisprudência e convenções (IGA, 2007). A Constituição do Canadá também possui normas não-escritas que consistem principalmente em usos e costumes. Basicamente, toda a parte escrita da Constituição do Canadá está escrita na *Constitution Act, 1982* (CANADA, 1982).

aprová-la. Em seu artigo 18. (1) prescreve que as leis e registros do Parlamento devem ser impressos e publicados em inglês e francês, sendo ambas as versões lingüísticas oficiais, como ocorre em todas as páginas eletrônicas do e-Gov do Canadá em que o acesso às informações do Governo é possibilitado nestas duas versões. No artigo 20.(1) dispõe que qualquer cidadão no Canadá tem o direito de se comunicar e receber os serviços disponíveis em qualquer órgão de uma instituição governamental, em inglês ou francês. Caso quaisquer dos direitos sejam violados ou negados, o artigo 24. (1) permite ao cidadão recorrer ao tribunal de jurisdição competente para a obtenção da solução (CANADA, 1982).

2) A *Access to Information Act*, 1985 (CANADA, 1985*k*)[91], foi criada pelo Parlamento canadense, em razão de legislar especificamente sobre o direito dos cidadãos canadenses e dos residentes permanentes, bem como dos indivíduos e das corporações presentes no Canadá, de solicitar o acesso às informações e registros federais controlados pelos órgãos públicos.

Em 2009 a *Access to Information Act*, 1985 (CANADA, 1985*k*) foi regulamentada pela *Access to Information Regulations*, 2009 (CANADA, 2009*a*)[92], por meio do *President of the Treasury Board*, atualizando a forma de solicitar o acesso às informações presentes nos órgãos públicos, e prescrevendo o pagamento da taxa necessária para o pedido de acesso aos registros. Registre-se que o chefe da instituição governamental pode se recusar a divulgar qualquer registro solicitado desde que contenha informações relativas às técnicas investigativas ou planos para investigações legais específicas; divulgação de informações que possam interferir em direitos contratuais ou de outras negociações de um terceiro; e informações de segurança nacional.

A *Treasury Board Secretariat* (TBS) é a responsável pela administração e aplicação da *Access to Information Act* (CANADA, 1985*k*) *e da Privacy Act* (CANADA, 1985*p*)[93] no âmbito governamental, cabendo-lhe a elaboração de políticas gerais de comunicações e compartilhamento de informação entre os órgãos do governo federal. A TBS desenvolve políticas para a proteção governamental, com o auxílio da *Royal Canadian Mounted Police* (RCMP) e do *Communications Security Establishment* (CSE), inclusive diretrizes para desclassificação de documentos nos termos da *Security of Information Act*, 1985 (CANADA, 1985*q*). É importante destacar que em razão dos episódios de terrorismo em 11 de setembro nos Estados Unidos, a *Access to Information Act*, 1985 (CANADA, 1985*k*), e as leis *Privacy*

[91] APÊNDICE B, p. 154.
[92] APÊNDICE B, p. 159.
[93] APÊNDICE B, p. 155.

Act, 1985 (CANADA, 1985*p*) e *Personal Information Protection and Electronic Documents*, 2000 (CANADA, 2000) foram emendadas para alterar procedimentos e limites à desclassificação de documentos, e ao acesso às informações consideradas relevantes para a segurança nacional.

A *Royal Canadian Mounted Police* (RCMP) é uma agência governamental com poder de polícia, com atribuições voltadas à atividade de inteligência criminal, de segurança nacional e de levantamento de dados e produção de conhecimento para auxiliar nas operações de combate às ameaças ao Canadá e na aplicação da lei. Em 1988, foi criado o *Royal Canadian Mounted Police External Review Committee Security and Confidentiality Regulations*, 1988 (CANADA, 1988)[94] pelo Ministro de Defesa Nacional para regulamentar quais informações os membros da RCMP poderiam acessar no exercício das suas funções. O regulamento tinha como propósito evitar o exacerbado de acesso a informações privilegiadas que os membros da RCMP tinham em razão da sua função. Conforme o artigo 2. qualquer membro da Comissão no desempenho das suas funções, deve cumprir os requisitos de segurança e de confidencialidade para ter acesso e uso da informação, guardando sigilo da mesma. Convém destacar que, em conseqüência dos atentados terroristas de 11 de setembro de 2001 nos Estados Unidos, as atividades da RCMP na área de segurança nacional foram expandidas, para prevenir, detectar e neutralizar a atividade terrorista por meio de mecanismos de integração e orientação de inteligência e segurança da informação (GONÇALVES, 2008).

3) O Governo canadense e a maior parte dos governos provinciais e municipais são obrigados sob a *Privacy Act*, 1985 (CANADA, 1985*p*)[95], a fornecer ao público o acesso às informações pessoais de controle do Governo. A legislação estabelece o procedimento para a solicitação dessas informações e fornece diretrizes para a forma, o período e que tipo de informações podem ser disponíveis. Os registros obtidos sob essa lei são considerados documentos públicos, garantindo a manutenção do sigilo (SIP, 2002). A *Privacy Act*, 1985 (CANADA, 1985*p*), foi criada em 1985 pelo Parlamento em razão de legislar sobre o recolhimento, a utilização, a divulgação, a conservação e a eliminação de informações pessoais. Muitos especialistas advogam por sua revisão, argumentando que a lei encontra-se defasada diante da realidade de comunicação e processamento de dados.

Importante assinalar que em 1985, a Internet estava iniciando, as comunicações em rede de computadores eram bastante restritas a círculos militares e universidades, telefone

[94] APÊNDICE B, p. 158.
[95] APÊNDICE B, p. 155.

celular era artigo de luxo, e o terrorismo cibernético (virtual) era quase exclusividade da ficção científica. A realidade de segurança doméstica também era outra. Os argumentos de uma reforma na lei defendem maior transparência e responsabilidade na Administração Pública na reunião, utilização, difusão e proteção de informações pessoais (GONÇALVES, 2008).

No Canadá há o Comissário para Proteção à Vida Privada (*Office of the Privacy Commissioner of Canada* - OPC) com o propósito de garantir o respeito no tratamento das informações pessoais por órgãos da Administração Pública Federal garantido pela *Privacy Act*, 1985 (CANADA, 1985*p*) e pelo setor privado, garantido pela *Personal Information Protection and Electronic Documents Act*, 2000 (CANADA, 2000). O OPC tem por missão precípua proteger e promover o direito à privacidade no Canadá, sendo um dos órgãos mais importante da Administração Pública canadense em termos de proteção a direitos e garantias individuais (GONÇALVES, 2008).

5.3. Privacidade

Brasil

1) Na Constituição Federal de 1988 (BRASIL, 2009*a1*) o artigo 5°, X prescreve que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (...)". A motivação desse artigo é preservar e proteger o direito à privacidade, com o sigilo das informações relacionadas à intimidade ou à vida privada de alguém. No mesmo sentido o artigo 5, XII também prescreve que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial. A razão dessa norma é proteger e preservar o direito à privacidade das comunicações, com o sigilo dos dados e das comunicações privadas, podendo incluir o sigilo dos dados via Internet. Esse inciso XII é regulamentado pela Lei nº 9.296, 1996[96] (BRASIL, 1996).

2) A principal norma referente a arquivos públicos no Brasil é a Lei nº 8.159, 1991 (BRASIL, 1991*m2*)[97], formulada pelo Poder Legislativo. Tem como intuito dispor sobre a Política Nacional de Arquivos Públicos e Privados, considerando arquivo, o conjunto de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e

[96] Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa (BRASIL, 1996). APÊNDICE A, p.135.
[97] APÊNDICE A, p. 135.

entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

Essa determinação legal provocou reações de historiadores e pesquisadores, que passaram a exigir acesso a arquivos de Estado referentes ao século XIX e a primeira metade do século XX. Setores da Administração nos três Poderes que dispunham de arquivos criaram comissões para avaliá-los e determinar sua abertura. O primeiro regulamento da Lei nº 8.159, 1991 (BRASIL, 1991*m2*) foi o Decreto n° 2.134, 1997 (BRASIL, 1997*i2*), do Poder Executivo, que dispunha sobre a categoria dos documentos públicos sigilosos e o acesso a eles. Texto mais complexo e detalhado sobre a salvaguarda de assuntos sigilosos foi o Decreto n° 2.910, 1998 (BRASIL, 1998), do Poder Executivo, referente a normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa. Foi importante no sentido de estabelecer conceitos relacionados a sigilo de documentos, materiais, áreas, comunicações, bem como normas para a gestão de documentos sigilosos, segurança das comunicações e dos sistemas de informação, com ênfase à criptografia, e salvaguarda de áreas e material sigilosos (GONÇALVES, 2008). Esses dois decretos – Decreto n° 2.134, 1997 (BRASIL, 1997*i2*) e Decreto n° 2.910, 1998 (BRASIL, 1998) – foram revogados pelo Decreto nº 4.553, 2002 (BRASIL, 2002*g2*), do Poder Executivo.

O atual decreto que regulamenta a Lei nº 8.159, 1991 (BRASIL, 1991*m2*) é o Decreto n° 4.073, 2002 (BRASIL, 2002*g4*)[98] formulado pelo Poder Executivo, dando ao Conselho Nacional de Arquivos – CONARQ a atribuição de definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo.

O Decreto nº 4.553, 2002 (BRASIL, 2002*g2*)[99] foi criado pelo Poder Executivo no intuito de atualizar o Decreto n° 2.910, 1998 (BRASIL, 1998 - *revogado*) 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. Dentre as atualizações importantes, considera sigilosos dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. Outro aspecto importante diz respeito à classificação dos dados ou

[98] APÊNDICE A, p. 140.
[99] APÊNDICE A, p. 139.

informações sigilosos em ultra-secretos[100], secretos[101], confidenciais[102] e reservados[103] em razão do seu teor ou dos elementos intrínsecos. Essa classificação é relevante para a Administração Pública na medida em que separa as informações em graus de sigilo, pois facilita o manuseio das mesmas pelos técnicos administrativos, pelos dirigentes e pelos governantes. São classificações que devem ser respeitadas para garantir a lisura dos atos administrativos frente aos administrados. Senão tornar-se-ia uma norma inócua, que não atenderia à sua razão de ser. O Decreto ainda dispõe sobre gestão de dados ou informações sigilosos, acessos estes, inclusive com especificações sobre credencial de segurança. Trata também dos sistemas de informação das áreas e instalações sigilosas e do material sigiloso. Neste há preocupação específica com a espionagem industrial e a produção, manutenção e transporte de bens sensíveis.

O Decreto n° 5.301, 2004 (BRASIL, 2004*e1*)[104] introduziu reformas no Decreto n° 4.553, 2002 (BRASIL, 2002*g2*) sobre salvaguarda de assuntos, locais e materiais sigilosos, isto é, disposições que não foram previstas adequadamente e que necessitavam serem reforçadas, sendo realizada pelo Poder Executivo. Outra ação deste Poder foi reformar o Decreto n° 4.553, 2002 (BRASIL, 2002*g2*) na parte em que tratava sobre documentos públicos pela Medida Provisória n° 228, 2004 (BRASIL, 2004*e2*)[105], que foi convertida no Congresso Nacional em Lei n° 11.111, 2005 (BRASIL, 2005*d4*)[106], ambas regulamentando o final do artigo 5°, XXXIII da Constituição (BRASIL, 2009*a1*). Não há muita diferença de conteúdo entre essas duas normas, mas a forma como é redigida a Medida Provisória n° 228, 2004 (BRASIL, 2004*e2*) foi modificada pela Lei n° 11.111, 2005 (BRASIL, 2005*d4*) para adequar o texto ao seu objeto e minimizar interpretações legislativas diversas do seu conteúdo.

A Lei n° 11.111, 2005 (BRASIL, 2005*d4*) ao tratar do acesso a documentos públicos que contenham informações sigilosas imprescindíveis à segurança do Estado e da sociedade, determinou ao Poder Executivo a criação da Comissão de Averiguação e Análise de Informações Sigilosas, no âmbito da Casa Civil da Presidência da República, com a finalidade

---

[100] Os ultra-secretos referem-se à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País (BRASIL, 2002*g2*, Art. 5º § 1º).
[101] Os secretos referem-se a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência (BRASIL, 2002*g2*, Art. 5º § 2º).
[102] Os confidenciais referem-se a conhecimento restrito das partes (BRASIL, 2002*g2*, Art. 5º § 3º).
[103] Os reservados são aqueles cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos (BRASIL, 2002*g2*, Art. 5º § 4º).
[104] APÊNDICE A, p. 138.
[105] APÊNDICE A, p. 136.
[106] APÊNDICE A, p. 133.

de decidir sobre a aplicação da ressalva ao acesso de documentos, em conformidade com o disposto nos parágrafos do artigo 6° desta Lei.

Observa-se que, apesar de ser o GSI o órgão encarregado da segurança institucional e da inteligência, a Comissão foi criada na esfera da Casa Civil da Presidência da República, atribuindo-lhe a competência de conduzir o processo de "abertura dos arquivos". Essa questão talvez se deva à influência do então Ministro-Chefe da Casa Civil, José Dirceu, e de seu grupo, uma vez que a Casa Civil no início do Governo do Presidente Luís Inácio Lula da Silva começou a se imiscuir na área de inteligência. Muito pouco foi feito em relação à abertura dos arquivos, em especial os referentes ao período da ditadura militar (1964-1985) desde a edição da Medida Provisória 228, 2004 (BRASIL, 2004*e2*), e da própria Lei n° 11.111, 2005 (BRASIL, 2005*d4*). Outra observação refere-se ao Decreto n° 5.584, 2005 (BRASIL, 2005*d1*)[107] que transfere o acervo do SNI, do Conselho de Segurança Nacional de Investigações, sob custódia da ABIN, para o Arquivo Nacional. O Decreto prevê que recolhidos ao Arquivo Nacional, os documentos referidos deverão ser disponibilizados para acesso público, resguardadas a manutenção de sigilo e a restrição ao acesso de documentos que se refiram à intimidade da vida privada de pessoas ou cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do Decreto n° 4.553, de 2002 (BRASIL, 2002*g2*). O problema dessa ressalva se deve pela dificuldade recorrente em acessar esses arquivos (GONÇALVES, 2008). Permite-se o acesso, mas na prática esse acesso é impedido por circunstâncias alheias. Apesar da pesquisa incessante sobre esse tema, não foi encontrada explicação mais pormenorizada sobre a dificuldade dos acessos aos arquivos recolhidos no Arquivo Nacional.

3) Outras normas infraconstitucionais legislam sobre a proteção do sigilo, da privacidade, da segurança, do acesso e da retificação de informações existentes em bases de dados públicas ou privadas, além do sigilo das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública e/ou privada. Essas normas podem ser encontradas detalhadamente no APÊNCIE A – Normas Relacionadas à Segurança da Informação: Brasil (p. 131 e 135) como: a Lei nº 7.232, 1984 (BRASIL, 1984), sobre a Política Nacional de Informática; Código de Conduta da Alta Administração, 2000 (BRASIL, 2000*j1*); o Código de Ética do Servidor Público, Decreto nº 1.171, 1994 (BRASIL, 1994*l1*), o Código de Processo Civil, Lei n° 5.869, 1973 (BRASIL, 1973); e o Código Tributário Nacional, Lei nº 5.172, 1966 (BRASIL, 1966).

[107] APÊNDICE A, p. 138.

Canadá

1) No Canadá, duas leis protegem a privacidade: a *Privacy Act*, 1985 (CANADA, 1985*p*)[108], relativa ao tratamento das informações pessoais por órgãos da Administração Pública Federal, e a *Personal Information Protection and Electronic Documents Act*, 2000 (CANADA, 2000)[109], que trata da proteção às informações pessoais no setor privado. Esta última estabelece dez princípios que as organizações devem respeitar no que concerne à coleta, uso, divulgação e armazenamento de dados pessoais (DSP, 2007). Foram criadas pelo Parlamento canadense para garantir o acesso a informações pessoais, sendo que as informações pessoais públicas foram garantidas em 1985, época de Guerra Fria, contexto de indignação por parte da sociedade canadense sobre o exacerbado poder dos serviços de inteligência e a invasão indevida da privacidade de seus cidadãos. Em 2000 foi criada a lei para proteger o acesso às informações no setor privado, contexto de Globalização com exacerbado poder do setor privado sobre informações pessoais, notadamente com o uso das novas TCIs, como a Internet, para divulgar e acessar informações pessoais. Em meio ao uso exacerbado desses poderes, o Estado foi obrigado a legislar sobre o assunto.

A *Privacy Act*, 1985 (CANADA, 1985*p*), teve por objetivo expandir as leis do Canadá que protegem a privacidade das pessoas no que diz respeito às informações pessoais sobre si próprias guardadas em instituição governamental e que forneçam às mesmas o direito de acesso a essas informações. Na presente Lei, informações pessoais são as informações que identificam um indivíduo, gravada em qualquer suporte, como raça, nacionalidade ou origem étnica. De acordo com o artigo 4., nenhuma informação pessoal é recolhida por uma instituição governamental, salvo se relacionada diretamente a um programa ou atividade operacional da instituição. No artigo 5. (2), uma instituição governamental deve informar qualquer indivíduo que a instituição recolhe informações pessoais sobre ele e a finalidade dessa ação. No artigo 6. (2), a instituição do governo tomará todas as medidas razoáveis para assegurar que as informações pessoais utilizadas para uma finalidade administrativa serão precisas, atualizadas e completas.

A *Personal Information Protection and Electronic Documents Act*, 2000, (CANADA, 2000) apóia e promove o comércio eletrônico ao legislar sobre a proteção das informações pessoais que são recolhidas, utilizadas ou divulgadas no setor privado, prevendo a utilização de meios eletrônicos para transmitir ou gravar informações ou transações. O propósito desta lei é estabelecer, em uma era na qual a tecnologia facilita a circulação e a troca de informação,

[108] APÊNDICE B, p. 155.
[109] APÊNDICE B, p. 152.

regras para administrar o armazenamento, o uso e a revelação de informação pessoal até os limites do direito à privacidade de indivíduos em relação à informação pessoal e à necessidade de organizações privadas para armazenar, usar ou descobrir informação pessoal para propósitos que uma pessoa mediana consideraria apropriada nessas circunstâncias.

2) Alguns regulamentos e ordens foram criados pelo *President of the Treasury Board*, para regulamentar e atualizar a *Privacy Act*, 1985 (CANADA, 1985*p*). O *Privacy Regulations*, 2009 (CANADA, 2009*d*)[110], foi expedido para que o cidadão tenha melhor acesso às informações pessoais sob o controle de uma instituição governamental. No artigo 4. (1), as informações pessoais solicitadas devem ser mantidas pela instituição por, pelo menos, dois anos após a última vez que as informações pessoais foram usadas, a menos que o cidadão consinta na sua disposição. A *Privacy Act Extension Order* n° 1, 2009 (CANADA, 2009*b*)[111] e, posteriormente, a *Privacy Act Extension Order*, n° 2, 2009 (CANADA, 2009*c*)[112] tiveram como motivação ampliar o direito de acesso a informações pessoais da subsecção 12 (1) da *Privacy Act*, 1985 (CANADA, 1985*p*) a todas as pessoas presentes no Canadá, para quem esse direito não tenha sido prorrogado anteriormente, como reclusos, estrangeiros, imigrantes, extraditados.

5.4. Administração Pública e Transparência

Brasil

1) Na Constituição (BRASIL, 2009*a1*) em seu artigo 23, prescreve dever do Estado proteger os documentos e obras, a fim de proteger a integridade, a autenticidade e a disponibilidade das informações do Estado. Também o artigo 216 prescreve que cabem à Administração Pública a gestão da documentação governamental e as providências para franquear sua consulta. É a proteção à integridade, à autenticidade, à disponibilidade e ao sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

Em seu artigo 37, há a vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. A razão desse artigo é prescrever quais princípios nortearão o agente público, como tornar público o acesso de informações, melhorar a gestão das informações, respeitar as normas, tornar mais eficiente o

[110] APÊNDICE B, p. 159.
[111] APÊNDICE B, p. 159.
[112] APÊNDICE B, p. 159.

órgão ou entidade. Esse artigo é corroborado pelo artigo 93, da Constituição (BRASIL, 2009*a1*) que dispõe sobre o princípio da publicidade dos atos públicos, e também o direito à privacidade quando o sigilo das informações relacionadas à intimidade ou à vida privada de alguém não prejudique o interesse público à informação. São normas que prescrevem a publicidade dos atos públicos e ainda protegem o direito à privacidade quando não prejudique a sociedade.

No artigo 37, § 6º, da Constituição (BRASIL, 2009*a1*) como no artigo 43, do Código Civil (BRASIL, 2002*g1*), este criado pelo Congresso Nacional para atualizar o direito civil, que era normatizado em 1916, as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa. Essas normas estabelecem a responsabilidade objetiva decorrente da má gestão das funções e das informações pelos órgãos e entidades da Administração Pública e das pessoas de direito privado prestadoras de serviços públicos, para responsabilizar aqueles que em sua posição devem zelar pela lisura de suas ações e omissões.

2) Em 1994 o Poder Executivo criou o Decreto nº 1.048, 1994 (BRASIL, 1994*l2*)[113], para implantar o Sistema de Administração dos Recursos de Informação e Informática, na Administração Pública Federal. Foi motivado pela expansão do uso de computadores e pelo início da Internet, e com isso teria que adequar o aparato estatal aos novos recursos de TI. Essa lei permitiu difusão de novos sistemas informacionais na Administração Pública, notadamente em 1995, com sua liberação comercial da Internet para toda a sociedade civil, e não mais apenas para os agentes públicos, militares e pesquisadores de universidades.

Apesar dos avanços tecnológicos, do ponto de vista jurídico e institucional, até 1995, não havia qualquer dispositivo normativo formal regulamentado a Internet no país. Nesse mesmo ano "começaram a surgir os instrumentos institucionais para conferir maior formalização normativa como se deu com a criação do Comitê Gestor da Rede Internet no Brasil" (LEMOS, 2005, p. 109), pela Portaria Interministerial n° 147, 1995 (BRASIL, 1995)[114], em Nota Conjunta pelo Ministério das Comunicações (MC) e pelo Ministério da Ciência e Tecnologia (MCT), para coordenar e incentivar a implantação daquela rede no país. Esta Portaria foi modificada pela Portaria Interministerial Conjunta CIVIL/MC/MCT nº 739, 2003 (BRASIL, 2003*f2*), de procedência da Casa Civil da Presidência da República. Não houve a criação de um decreto pelo Presidente da República, apenas decisão do Ministro

[113] APÊNDICE A, p. 142.
[114] APÊNDICE A, p. 144.

Chefe da Casa Civil em alterar a redação da Portaria anterior, ao aumentar o número de membros do Comitê Gestor e seus mandatos de dois para três anos.

A partir de 1995, o Governo, por meio do Poder Executivo, criou normas[115] para inserir o País na sociedade do conhecimento e implantar o e-Gov. Em outubro de 2000, o Governo criou o Comitê Executivo do Governo Eletrônico (CEGE) no âmbito do Conselho do Governo pelo Decreto s/nº de 18 de outubro de 2000 (BRASIL, 2000*j2*)[116], a fim de formular políticas, estabelecer diretrizes, coordenar e articular as ações de implantação do e-Gov, voltado para a prestação de serviços e informações ao cidadão por meio de TI. Ao criar o CEGE, surgiu a necessidade de se criar um grupo responsável para planejar e deliberar sobre a execução, a operação e a evolução das etapas do projeto de integração das diversas redes de comunicação de dados do Governo Federal. Para isso, o Chefe do Executivo editou o Decreto s/n°, de 04 de dezembro de 2001 (BRASIL, 2001*h1*)[117], e criou, no âmbito do Comitê Executivo do Governo Eletrônico (CEGE), o Subcomitê da Rede Brasil.gov , incumbido dessas prerrogativas.

3) Em 2006, o Presidente da República, pelo Decreto nº 5.687, 2006 (BRASIL, 2006*c1*)[118], promulgou a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003. Esta Convenção entrou em vigor internacionalmente em 14 de dezembro de 2005, e foi aprovada pelo Congresso Nacional por meio do Decreto Legislativo nº 348, 2005 (BRASIL, 2005*d3*)[119]. A finalidade da Convenção e do Governo ao ter assinado-a é promover e fortalecer as medidas para prevenir e combater a corrupção com cooperação internacional para haver integridade das contas e a devida gestão dos assuntos e dos bens públicos. São afinal, medidas para aumentar a transparência da Administração Pública, inclusive no relativo à organização, funcionamento e processos de adoção de decisões.

Outras normas foram criadas nesse escopo, como o Decreto nº 6.029, 2007 (BRASIL, 2007)[120], editado pelo Poder Executivo para instituir o Sistema de Gestão da Ética do Poder Executivo Federal. O Decreto tem como prerrogativa, dentre outras, de contribuir para a implementação de políticas públicas tendo a transparência e o acesso à informação como instrumentos fundamentais. Já a Lei Complementar nº 131, 2009 (BRASIL, 2009*a2*)[121], mais

[115] Ver item 2.10. Governo Eletrônico: Brasil, p. 37.
[116] APÊNDICE A, p. 140.
[117] APÊNDICE A, p. 140.
[118] APÊNDICE A, p. 138.
[119] APÊNDICE A, p. 142.
[120] APÊNDICE, A, p. 137.
[121] APÊNDICE A, p. 132.

recente e criada pelo Poder Legislativo por maioria absoluta, determina a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios por meio do e-Gov. Esta norma tem como intuito acrescentar essa deliberação aos dispositivos da Lei Complementar n° 101, 2000 (BRASIL, 2000*j5*)[122], que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal. O motivo dessa determinação é tornar mais responsável a gestão fiscal, tendo ação planejada e transparente, ao prevenir riscos e corrigir desvios capazes de afetar o equilíbrio das contas públicas, com disponibilização dessas informações em tempo real.

Canadá

1) No Canadá, as normas sobre o dever do Estado proteger os documentos e obras, gerir documentos e franquear consultas estão previstas nas leis citadas anteriormente *Privacy Act*, 1985 (CANADA, 1985*p*)[123], e *Access to Information Act*, 1985 (CANADA, 1985*k*)[124], e atualmente foi criada a *Public Servants Disclosure Protection Act*, 2005 (CANADA, 2005*e*)[125], a fim de estabelecer procedimentos para revelação dos erros de servidores no setor público, inclusive a proteção de servidores que revelam os erros.

2) Com relação aos avanços tecnológicos, o Canadá tomou medidas para implantar sistemas de gestão e prestação de serviços em instrumentos de TI. A implantação do e-Gov foi iniciada em 1999 e tornou-se referência mundial em questões de prestação de serviços e informações governamentais. O *Government Electronic Directory Services* (GEDS) criou em 2008 um diretório com informações de servidores públicos federais de todas as regiões do Canadá. O *Information Technology Services Branch* (ITSB) iniciou este projeto para integrar dois diretórios: o *Government of Canada telephone directories, and the Email Address Exchange Service* (EMAX) (GEDS, 2009). Ressalte-se que não foram encontradas normas específicas sobre o e-Gov no Canadá, apesar de ter sido feito um levantamento minucioso e pragmático no site oficial responsável pela publicação das normas, *o Department of Justice Canada*.

3) A Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas em 31 de outubro de 2003 foi assinada pelo Canadá em 21 de maio de 2004, sendo ratificada pelo Governo do Canadá através do *Minister of Foreign Affairs* em

[122] APÊNDICE A, p. 132.
[123] APÊNDICE B, p. 155.
[124] APÊNDICE B, p. 154.
[125] APÊNDICE B, p. 153.

2 de outubro de 2007. A Convenção representa um consenso internacional sobre o que os Estados devem fazer nas áreas de prevenção da corrupção, a criminalização, o combate à lavagem de dinheiro, recuperação de ativos e cooperação internacional na investigação e repressão. O Governo canadense tem como motivação conciliar a transparência essencial e desejável e as investigações com o grau de confidencialidade e de equidade necessárias contra alegações de má administração, prevaricação e corrupção pessoal, para promover a *accountability* e a transparência.

O Ministério dos Assuntos Exteriores e do Comércio Internacional – *Foreign Affairs and International Trade Canada* (DFAIT), em um artigo sobre a Reforma do Sistema de Segurança e Estado de Direito, elucida que o desenvolvimento de um sistema de segurança eficaz e responsável e um sistema de justiça imparcial e acessível são condições essenciais para promover a boa governança e o Estado de Direito, na defesa dos direitos humanos, na atenuação da violência, e na prevenção de impunidade. Para isso, apregoam a reforma do sistema de segurança baseada nos princípios de *accountability* (responsabilidade), transparência, igualdade, proteção civil, regras democráticas e o respeito aos direitos humanos. Isto envolve investimentos de longo prazo que devem perpetuar desde o início, por tempo indeterminado. No Canadá, essa reforma possui uma abordagem coerente e abrangente, pois reconhece a interdependência de forças armadas, polícia, justiça, gestão das fronteiras, alfândegas e setores, bem como a necessidade de reforçar a supervisão civil e parlamentares de todo o sistema de segurança (DFAIT, 2008).

5.5. Ilicitudes

Brasil

1) O Código Penal Brasileiro – Decreto-Lei n° 2.840, 1940 (BRASIL, 1940)[126] foi alterado recentemente pela Lei n° 9.983, 2000 (BRASIL, 2000*j6*), para adequar os ilícitos às novas práticas de TIC na Administração Pública, principalmente em relação aos aspectos de segurança da informação. A Lei, criada pelo Congresso Nacional demonstra a preocupação do legislador com a prevenção de inserção ou alteração de dados e informações em bancos de dados da Administração Pública por funcionários com acesso autorizado. O Código Penal, 1940 (BRASIL, 1940), nos artigos 184, 297, 305, 313-A, 313-B, 314, também dispõe sobre a proteção da integridade, autenticidade e disponibilidade dos documentos públicos e

[126] APÊNDICE A, p. 132.

informações constantes nos órgãos e entidades públicos, e prescreve criminalização para tanto.

Nas regulamentações: Consolidação das Leis do Trabalho, Decreto-Lei n.º 5.452, 1943 (BRASIL, 1943)[127], artigo 482; Código de Processo Penal, Decreto-Lei nº 3.689, 1941 (BRASIL, 1941)[128], artigos 20 e 207; Código Penal (BRASIL, 1940) artigos 153 e 325 – há proteção de informações sigilosas acessadas no exercício de cargo, função ou emprego público, constantes nos sistemas ou bancos de dados da Administração Pública. São normas criadas pelo Poder Legislativo, com exceção da primeira que foi pelo Poder Executivo, preceituam penalidades para o desrespeito de normas correlacionadas à segurança da informação.

No Brasil não há legislação específica sobre os crimes praticados na área de informática. O debate sobre o assunto ocorre desde sua implantação e liberação para o uso privado em 1995. Muitos projetos de leis foram criados, dentre eles, um tem se destacado na sociedade pelo intenso debate que realiza com a mesma: é Projeto de Lei (PL) do Senador Eduardo Azeredo[129], de 2006 (BRASIL, 2006*c2*)[130]. Trata-se de um projeto de lei substitutivo que aglutina três projetos de lei: o PL da Câmara dos Deputados nº 89, de 2003, e os PL do Senado nº 137, de 2000, e nº 76, de 2000 – todos referentes a crimes na área de informática. O substitutivo tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares. Estabelece 13 crimes civis e pune com multa e prisão por delitos como roubo de senha (estelionato eletrônico), difusão de vírus, acesso não autorizado a dados, ataques a redes de computadores, armazenamento de conteúdo pedófilo, divulgação não autorizada de informações pessoais, e clonagem de cartões e celulares (FUSCO, 2008). O Projeto encontra-se em discussão no Congresso Nacional, não tendo sido aprovado até o presente momento.

Outro projeto de lei relacionada à área de informática é o Projeto de Lei nº 21, de 2004 (BRASIL, 2004*e3*)[131] do Senado, que proíbe o envio de mensagens não solicitadas (*spam*); estabelece multa; cria nova modalidade do crime de falsidade ideológica a conduta de impedir a identificação do remetente ou o bloqueio automático de mensagens eletrônicas, ou de inserir

[127] APÊNDICE A, p. 131.
[128] APÊNDICE A, p. 131.
[129] Eduardo Azeredo, engenheiro, é senador da República pelo PSDB-MG. Foi prefeito de Belo Horizonte e governador de Minas Gerais, além de analista de sistemas da IBM, presidente do Serpro, da Prodemge, da Prodabel e da BMS - Belgo Mineira Sistemas.
[130] APÊNDICE A, p. 148.
[131] APÊNDICE A, p. 148.

declaração falsa ou diversa da que deveria constar, com o fim de impossibilitar a identificação da origem ou o rastreamento da mensagem. São tipificações não encontradas na legislação brasileira, contudo essas condutas têm sido julgadas pelos Tribunais.

2) Outra questão de ilicitude relacionada à PSI se refere ao terrorismo. A Constituição (BRASIL, 2009*a1*, artigos 4º e 5°, XLIII) preceitua que a República Federativa do Brasil rege-se nas suas relações internacionais com repúdio ao terrorismo, e que a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia o terrorismo. A Lei Complementar 105, 2001, (BRASIL, 2001*h3*, artigo 1°, § 4°, I)[132] criada pelo Congresso Nacional, legisla sobre o sigilo das operações de instituições financeiras, e permite a quebra de sigilo para apuração de terrorismo. Essas normas se devem ao fato do combate ao terrorismo ser uma questão de defesa e segurança nacional e mundial, principalmente com o surgimento de novas TIC que permitem o ataque terrorista remoto, em qualquer parte do mundo. Isso não deixa de ser uma preocupação com a segurança das informações, pois informações privilegiadas podem desencadear problemas inimagináveis.

3) A ilicitude na Internet também tem ocorrido contra crianças e adolescentes, sendo demanda de defesa do Estado aos direitos humanos. Sobre essas demandas, a Lei nº 11.829, 2008 (BRASIL, 2008*b3*)[133], alterou o Estatuto da Criança e do Adolescente – Lei n° 8.069, 1990 (BRASIL, 1990) para tipificar condutas, aprimorar o combate à produção, venda e distribuição de pornografia infantil, e criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet.

Canadá

1) O *Criminal Code*, 1985 (CANADA, 1985*n*)[134], em seus artigos 140. (1) e 184. (1), dispõem sobre a prevenção de inserção ou alteração de dados e informações em bancos de dados da Administração Pública por seus funcionários, e condena a interceptação de comunicação privada. O *Criminal Code* também prescreve sobre a proteção da integridade, autenticidade e disponibilidade dos documentos públicos e informações constantes nos órgãos e entidades públicos, e prescreve criminalização para tanto.

2) Em virtude dos atentados terrorista de 11 de setembro de 2001 nos Estados Unidos, o *Criminal Code*, 1985 (CANADA, 1985*n*) foi modificado no Parlamento, passando a prever crimes terroristas nos artigos 83.02 a 83.04; cometido em benefício de um grupo terrorista;

[132] APÊNDICE A, p. 132.
[133] APÊNDICE A, p. 132.
[134] APÊNDICE B, p. 150.

uma conspiração ou uma tentativa de cometer o ato terrorista. Foi criada também uma lei específica sobre o terrorismo, a *Anti-terrorism Act*, 2001 (CANADA, 2001*i*)[135], pelo Parlamento, tipificando praticamente todas as ações referentes ao terrorismo, além de expandir as atividades da RCMP na área de segurança nacional. Compete à RCMP investigar e aplicar a Lei, tendo como foco prevenir, detectar e neutralizar a atividade terrorista no Canadá e no estrangeiro.

Outra norma que legisla sobre o terrorismo é a *Public Safety Act*, 2002 (CANADA, 2002*g*)[136], criada pelo Parlamento em 2002. Esta Lei alterou 18 leis federais para reforçar a capacidade do Governo em proteger os canadenses, prevenir ataques terroristas e responder rapidamente às ameaças, como exigência às transportadoras aéreas de aviação ou os que operam sistemas de reserva de fornecerem informações básicas sobre determinadas pessoas ou de vôos quando são necessárias para fins de segurança. A Lei capacita o Ministro da Defesa Nacional a autorizar o *Communications Security Establishment* (CSE) a interceptar as comunicações privadas entre o Canadá e outros países com o objetivo de obter informações relacionadas a assuntos internacionais, de defesa ou de segurança (SIP, 2002).

Há ainda o Projeto de Lei LS-400E, Bill C-16 *Charities Registration (Security Information) Act* (CANADA, 2001*j*)[137], de 2001 formulado pela Câmara dos Comuns. Tem por objetivo concentrar esforços internacionais para negar apoio a todos envolvidos no terrorismo, a fim de proteger a integridade do sistema de registro de caridade da Lei de Imposto de Renda, 1985 (*Income Tax Act*, 1985*r*), e manter a confiança dos contribuintes canadenses para as instituições de caridade, ao garantir que são registradas apenas organizações que operam exclusivamente com fins de filantrópicos. O Projeto de Lei decorre do compromisso que o Canadá teve com o G-8[138]: investigar as organizações caridosas utilizadas por terroristas para acobertar atividades, e tomar medidas para prevenir o financiamento de organizações terroristas indiretamente através de organizações que têm, ou reivindicam beneficência. Ele também responde ao relatório de 1999 da Comissão Especial do Senado sobre a Segurança e Inteligência, o qual observou que os grupos terroristas com filiações em atividades de angariação de fundos, muitas vezes utilizavam a beneficência ou organizações filantrópicas como frentes para cometer suas ilicitudes.

---

[135] APÊNDICE B, p. 152.
[136] APÊNDICE B, p. 152.
[137] APÊNDICE B, p. 161.
[138] A sigla G-8 corresponde ao grupo dos 8 países mais ricos e influentes do mundo, fazem parte os Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia. Antes chamada de G-7, a sigla alterou-se com a inserção da Rússia, que ingressou no grupo em 1998.

3) No Canadá há projetos de lei para o combate de ilicitudes na Internet contra crianças e adolescentes. São três Projetos de Lei C-15, C-15A e C-15B propostos pela Câmara dos Comuns em 2002 (CANADA, 2002*h*)[139]. Estes projetos dispõem sobre alteração no *Criminal Code*, 1985 (CANADA, 1985*n*) e em outras leis. Adicionam infrações e outras medidas que proporcionam uma proteção adicional para as crianças da exploração sexual, incluindo a exploração sexual que envolva o uso da Internet. Na Cláusula 11, conceitua pornografia infantil como uma fotografia, cinema, vídeo ou outra representação visual, ou não foi feito por meio eletrônico ou mecânico. E prescreve que toda pessoa que importa, distribui, vende ou possuir, para efeitos de distribuição ou qualquer venda de pornografia infantil é culpado de crime infantil.

5.6. Normas e Padrões Internacionais da Segurança da Informação

Após descrever as normas do Brasil e Canadá, passa-se para a descrição das normas e padrões internacionais de segurança da informação[140].

As normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços.

Houve várias tentativas de padronização sobre segurança da informação. Uma delas foi desenvolvida pelo governo do Reino Unido, no final da década de 1980, para registrar as melhores práticas na área de gestão de serviços de tecnologia da informação sob a denominação de ITIL - *Infrastructure Technology Information Library* (REINO UNIDO, 1980). Embora não represente exatamente um padrão de segurança da informação, o ITIL contempla as áreas de gestão de incidentes, problemas, configuração, implantação de suporte de *software*. Colaborou para a padronização e a melhoria da qualidade do serviço ofertado pela área de tecnologia de informação, e para o estabelecimento de processos voltados para o alcance dos objetivos de segurança da informação (BEAL, 2005).

Contudo, as tentativas de padronização sobre segurança da informação iniciaram-se com a norma australiana e neozelandesa AS/NZS 4360 (AUSTRÁLIA, 2004), publicada em 1995 e revisada em 1999 e em 2004. Foi elaborada pela *Standards Australia e Standards New Zealand* através do Comitê de Gestão de Riscos da Austrália. Seguiram-se outras normas como a de Gestão de Riscos do Canadá, em 1997; do Reino Unido, em 2000; e do Japão, em 2001 (CICCO, 2003).

---

[139] APÊNDICE B, p. 161.
[140] Ver APÊNDICE C, p. 163.

A norma AS/NZS 4360, foi a primeira norma internacional sobre Sistemas de Gestão de Riscos Empresariais. Trata-se de uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza. Propõe um processo estruturado para o gerenciamento dos mais diversos tipos de riscos, como: os relacionados à segurança, ao meio ambiente e às políticas públicas (CICCO, 2003).

Outros padrões são os da "família" BS 7799 (REINO UNIDO, 1995) que tratam da gestão da segurança da informação. O objetivo inicial desses padrões foi estabelecer um sistema de gestão para segurança da informação que oferecesse subsídios para o desenvolvimento de normas e práticas relacionadas ao assunto. Ou seja, ao garantir que as informações internas são gerenciadas de forma segura, comprova aos usuários e clientes que a organização dispõe de controles adequados para a proteção das informações (SERPRO, 2006*a*).

A parte 1 do padrão BS 7799 corresponde ao Código de Práticas para a Gestão da Segurança da Informação. Foi publicada em 1995 pelo *British Standards Institution* (BSI), no Reino Unido, e seus pontos essenciais para o adequado tratamento dos riscos de segurança da informação são (BEAL, 2005):

- *Do ponto de vista legal*: proteção de dados e da privacidade de informações pessoais, salvaguarda de registros organizacionais e dos direitos de propriedade intelectual.
- *Do ponto de vista das melhores práticas*: formalização da política de segurança da informação, definição das responsabilidades na segurança, educação e treinamento em segurança, relatório dos incidentes e gestão da continuidade.

A parte 2 do padrão BS 7799 define o Sistema de Gestão de Segurança da Informação (ISMS, de *Information Security Management System*). Especifica uma série de processos voltados para garantir a avaliação e o tratamento dos riscos. A certificação envolve uma auditoria do ISMS para verificar se a organização dispõe de processos adequados para gerenciar riscos, manter o sistema atualizado e garantir o desenvolvimento da segurança da informação (BEAL, 2005). Essas normas consistem no tratamento da informação como um patrimônio, que deve ser protegido como qualquer outro ativo, de acordo com a classificação prévia de seu grau de confidencialidade, integridade, disponibilidade e privacidade. Para isso é necessário implementar o sistema de gerenciamento de segurança da informação, documentar o sistema, aprimorar a documentação operacional existente, e realizar o ciclo PDCA (*Plan, Do, Check e Act*) (SERPRO, 2006*a*).

O padrão BS 7799[141] tornou-se um padrão internacional em 2000, com sua adoção pela *International Organization for Standardization* (ISO)[142] sob o nome ISO/IEC 17799. Posteriormente, a nomenclatura ISO 17799 foi modificada pela própria ISO (ISO, 2009) com a finalidade de estruturar os padrões de segurança da informação para as séries 'ISO 27000'. Em 2005, a parte 1 foi denominada de ISO 27002 (SWITZERLAND, 2005), e, em 2006, a parte 2 de ISO 27001:2006 (SWITZERLAND, 2006).

Uma norma mais abrangente é o ISO/IEC *Guide 73* (SWITZERLAND, 2002), *Risk Management: Vocabulary - Guidelines for use in standards*, publicada em 2002 pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commission* (IEC)[143], ambas com sede em Genebra, na Suíça (CICCO, 2003).

O *ISO Guide 73*, define 29 termos da Gestão de Riscos, os quais foram agrupados nas seguintes categorias: a) termos básicos; b) termos relacionados a pessoas ou organizações afetadas por riscos; c) termos relacionados à avaliação de riscos; d) termos relacionados ao tratamento e controle de riscos (CICCO, 2003). Essas definições são genéricas e amplas, a fim de permitir aos usuários uma idéia do que é a Gestão de Riscos, ou, ao menos, usar uma linguagem mais universal.

A partir de outubro de 2009 será publicada uma norma universal sobre Gestão de Riscos, chamada ISO 31000: *Principles and Guidelines for Risk Management*. É a nova série de orientações da *International Organization for Standardization* (ISO), que tem por finalidade harmonizar padrões, regulamentações e *frameworks*[144] publicados anteriormente e que de alguma forma estão relacionados com a Gestão de Riscos (BASTOS[145], 2009).

---

[141] Itens de controle abrangidos pelo padrão BS 7799: Política de segurança de informação; Organização da segurança; Classificação e controle dos recursos de TI; Segurança do quadro de pessoal; Segurança física e ambiental; Gerência de redes e computadores; Controle de acesso; Desenvolvimento e manutenção do sistema; Planejamento da continuidade do serviço; Conformidade com a política de segurança (SERPRO, 2006*a*).

[142] A ISO é uma rede que reúne entidades padronizadas em 148 países. A instituição conta com um escritório central em Genebra, Suíca, e dispõe de uma única entidade representante em cada país – como o BSI no Reino Unido e a ABNT no Brasil (BEAL, 2005).

[143] A IEC é uma organização que prepara e publica normas internacionais para todos os equipamentos elétricos, eletrônicos e tecnologias relacionadas (IEC, 2009).

[144] *Framework* é uma abstração que une códigos comuns entre vários projetos de *softwares* provendo uma funcionalidade genérica. O desenvolvedor de *software* decomporá um conjunto de códigos de *softwares* com problemas semelhantes para criar um *framework*. O *framework* seria a união desses conjuntos de problemas semelhantes em um novo *software*, a fim de obter o resultado desejado para uma determinada aplicação. Poderá ser reutilizado posteriormente por outros desenvolvedores, na construção de outras aplicações, especificando apenas suas particularidades. Reduz trabalho futuro por ser um *software* quase completo, com código aberto, que possibilita ser alterado (SAUVÉ, 2009).

[145] Alberto Bastos é sócio-fundador da Módulo – empresa brasileira especializada em tecnologia para Governança, Riscos e Compliance (GRC) - e Coordenador no Brasil da Comissão Especial da Associação Brasileira de Normas Técnicas (ABNT) sobre as Normas de Gestão de Riscos, da qual a autora da dissertação é participante desde junho de 2009.

A causa dessa norma decorre da falta de consenso em relação às terminologias e aos conceitos utilizados para a Gestão de Riscos. Isso faz com que as organizações enfrentem dificuldades em integrar diferentes funções e atividades relativas ao assunto, sendo tratado de forma isolada (ilhas).

O desafio da norma será estabelecer uma linguagem comum, e padronizar as melhores práticas e abordagens para que as organizações possam implementar a Gestão de Riscos em seus processos. Essa norma poderá ser aplicada em organizações de qualquer tipo, tamanho ou área de atuação, pois objetiva reduzir as incertezas relacionadas às suas atividades – operacionais, processos ou projetos (BASTOS, 2009).

Por se tratar de uma proposta de convergência alinhada com a visão integrada da ERM (*Enterprise Risk Management*)[146], a nova norma não concorre com outras orientações já existentes como a ISO/IEC 27005:2008 (SWITZERLAND, 2008) – norma técnica específica de gestão de riscos em segurança da informação. Visa fornecer orientações e alinhar outros conjuntos de regras específicos (BASTOS, 2009).

O texto original da ISO 31000 foi baseado na norma AS/NZS 4360, e encontra-se atualmente em estágio de revisões. Estas estão sendo feitas por um comitê especial composto por delegações de 35 países, dentre eles Brasil e Canadá, que se uniram para criar um grupo de trabalho (multidisciplinar) denominado ISO *Technical Management Board on Risk Management* (BASTOS, 2009).

[146] Empresa que trabalha com métodos e processos utilizados pelas organizações para gerenciar riscos e oportunidades relacionadas.

CAPÍTULO 6 – SEMELHANÇAS E DIFERENÇAS NA REGULAMENTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo visa-se interpretar as semelhanças e diferenças na regulamentação da política de segurança da informação dos Governos Eletrônicos Federais do Brasil e do Canadá, apresentada no Capítulo 5, por temáticas. A interpretação baseia-se na literatura da Teoria do Conhecimento, do Governo Eletrônico, da Gestão da Informação e do Direito.

6.1. Segurança da Informação

A segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra: acessos não autorizados, alterações indevidas, indisponibilidade, repúdio e ilegalidade. Tem como objetivos fundamentais a confidencialidade, a integridade (autenticidade) e a disponibilidade, podendo acrescentar a legalidade e o uso legítimo. Esses fundamentos foram encontrados nas regulamentações do Brasil e Canadá.

1) No Brasil há o Decreto n° 3.505, 2000 (BRASIL, 2000*j3*), que estipula a PSI na Administração Federal, enquanto no Canadá há a *Security of Information Act*, 1985 (CANADA, 1985*q*), que trata sobre a segurança da informação, reformulada em 2001. São normas recentes que reforçam a PSI com foco no cidadão, nos valores, nos resultados e nos gastos responsáveis.

Interessante observar que o serviço de inteligência do Canadá, *Canadian Security Intelligence Service* (CSIS) serviu como modelo para a estruturação da ABIN, na década de 1990, com esta reproduzindo não só as características estruturais daquele, mas também aspectos doutrinários sobre a atividade exercida (GONÇALVES, 2008). A ABIN foi criada pela Lei n° 9.883, de 1999 (BRASIL, 1999*k2*) e o CSIS pela *Canadian Security Intelligence Service Act*, de 1985 (CANADA, 1985*m*), 14 anos de diferença.

O CSIS trabalha também com produção de informações sobre ameaças a sistemas críticos de informação e à infra-estrutura. Nesse contexto, destacam-se as “atividades de governos estrangeiros, empresas privadas ou mesmo indivíduos (como *hackers*) que têm interesse em ataques cibernéticos contra órgãos públicos, empresas, sistemas de comunicação e banco de dados” (GONÇALVES, 2008, p. 420). No Brasil o responsável por esse trabalho é o Comitê Gestor da Segurança da Informação (CGSI), juntamente com a ABIN, e a Secretaria-Executiva do Conselho de Defesa Nacional, pautando-se nas diretrizes da PSI.

A ABIN e o CSIS são órgãos civis, sem poder de polícia, voltados à inteligência doméstica – nem o Brasil e o Canadá possuem serviços de inteligência externa. Os dois sistemas contam com uma comunidade de inteligência atuante, com destaque para os órgãos vinculados às autoridades policiais, locais e federais – o DPF (Departamento de Polícia Federal) e a RCMP (Real Polícia Montada) – a inteligência militar e a fiscal, com entes centrais de coordenação das atividades de segurança que não são o serviço de inteligência – a Casa Civil brasileira e o PCO canadense. Tanto no Brasil quanto no Canadá, o "Diretor do serviço de inteligência não tem acesso direto ao Chefe de Governo, estando subordinado ao ministro da pasta de segurança que reúne outros órgãos – o GSI no Brasil e o Ministério de Segurança Pública, no Canadá" (GONÇALVES, 2008, p. 607).

A lei que criou o CSIS, também instituiu um órgão externo de controle, o *Security Intelligence Review Committee* (SIRC), independente e composto por não-parlamentares, com a função de revisar as atividades do serviço secreto prestando contas diretamente ao Parlamento. Apesar de estruturar seu serviço de inteligência nos moldes do Canadá, os brasileiros decidiram por um sistema de controle externo feito diretamente pelo Poder Legislativo (GONÇALVES, 2008), por meio do Tribunal de Contas da União.

Ressalte-se que a ABIN e o CSIC foram criados para substituírem órgãos anteriores que exacerbaram seus poderes nos dois países. Com isso, os atuais órgãos e governos devem se precaver para evitar que a recorrente utilização da noção de segurança nacional e interesse público sejam utilizadas como princípios de justificação de práticas políticas repressivas e autoritárias. Isso é "incompatível com uma concepção democrática de governo e de resolução de conflitos nas sociedades contemporâneas" (CEPIK, 2001, p. 138). Deve ser tratada com cautela, visando a transparência dos atos administrativos, garantindo-se o sigilo quando indispensável para a segurança da sociedade.

2) O SBIN é responsável, no Brasil, pelo processo de obtenção e análise de dados e informações e pela produção e difusão de conhecimentos necessários ao processo decisório do Poder Executivo, em especial no tocante à segurança da sociedade e do Estado, e salvaguarda de assuntos sigilosos de interesse nacional. No Canadá o acordo *Cyber Protection Supply Arrangement* (CPSA) do *Communications Security Establishment Canada* (CSEC) tem por objetivo apoiar o Governo do Canadá na realização de uma política de segurança coerente e dar respostas adequadas aos atuais riscos e ameaças de segurança de informações.

3) No Brasil o Gabinete de Segurança Institucional (GSI) da Presidência da República é o órgão que assiste direta e imediatamente o Presidente da República no desempenho de suas atribuições, relacionadas às atividades de inteligência federal e de segurança da

informação, sendo a ABIN subordinada ao mesmo. No Canadá o *Privy Council Office* (PCO) é o responsável por assistir o Primeiro-Ministro nessas questões pela secretaria especial *Security and Intelligence Secretariat*. Observa-se uma preocupação e atuação dos e-Gov brasileiros e canadenses em questões de segurança da informação para auxiliar as tomadas de decisões dos governantes de seus respectivos países. A diferença entre os países é que enquanto no Brasil os órgãos são de caráter consultivo do Chefe de Governo, no Canadá são órgãos de caráter deliberativo do Chefe de Governo, demonstrando a diferença de culturas e as possibilidades de organização dos Estados Democráticos de Direito em questões de segurança, defesa e soberania.

Conforme Adriana Beal (2005), o sistema de gestão de segurança da informação deve acompanhar as alterações ocorridas no cenário interno e externo da Administração Pública, para não perder a eficácia e não colocar em risco a integridade, a disponibilidade e a confidencialidade de informações essenciais para a organização, notadamente no campo das decisões de Governo que refletem em toda sociedade.

No Brasil, o Grupo de Trabalho do Programa de Proteção ao Conhecimento e Segurança da Informação foi criado pelo CGSI para desenvolver e propor um programa de proteção ao conhecimento e segurança da informação para aplicação nos diversos órgãos da Administração Pública Federal. No Canadá a equipe de Segurança de TI do CSEC foi criada para dar orientação de vanguarda e aconselhamento estratégico sobre a segurança de TI e sistemas de informação do Governo do Canadá, em parceria com os ministérios, as agências e as empresas privadas.

4) No Brasil o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, foi criado para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, pela Medida Provisória nº 2.200-2 (BRASIL, 2001*h4*). O Instituto Nacional de Tecnologia da Informação (ITI) é a Autoridade Certificadora Raiz da ICP-Brasil.

No Canadá o *Secure Electronic Signature Regulamentos*, 2005 (CANADA, 2005) regulamenta a segurança das assinaturas eletrônicas. A Secretaria do *Treasury Board of Canada* é a Autoridade Certificadora do Governo do Canadá.

O CSEC do Canadá e o *National Institute of Standards and Technology* (NIST) dos Estados Unidos criaram em conjunto o *Cryptographic Module Validation Program* (CMVP) para promover a utilização de modelos criptográficos válidos e fornecer às agências federais de segurança uma métrica para usar na aquisição de equipamentos que contenham modelos criptográficos válidos. A diferença está no fato de que o Canadá é vizinho dos Estados Unidos

e estes são parceiros em várias atividades, o que não ocorre com essa intensidade com o Brasil. No Brasil a utilização da criptografia está disposta no Decreto n° 3.996, 2001 (BRASIL, 2001*h2*), que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

Observa-se tanto no Brasil quanto no Canadá a preocupação com o ambiente lógico do Estado, que compõe todo ativo de informações. De acordo com a ICP-Brasil (2008) a informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade.

6.2. Acesso à Informação

1) Tanto o Brasil quanto o Canadá asseguram a todos o direito de acesso à informação, mas ao mesmo tempo resguardam o sigilo das informações relacionadas à intimidade ou à vida privada de alguém, e garantem o sigilo profissional.

Os dois países legislam a respeito do acesso à informação, que é um dos requisitos do princípio da publicidade. Isso possibilita acessar as informações privadas e públicas (com seus requisitos) e controlar os atos dos governantes. Conforme Ticoll & Tapscott (2004, p. 75) “o acesso à informação de boa qualidade é um pré-requisito para o exercício da cidadania”. O e-Gov apresenta-se como mais uma possibilidade de tornar transparentes os atos dos governantes e efetivar o controle social. Possibilita também o acesso a algumas informações de uma maneira mais rápida e ágil, podendo ser acessadas em casa, no trabalho ou em qualquer lugar que possua meios de conectar-se ao e-Gov.

2) No Brasil o Ministério Público tem acesso incondicional às informações da Administração direta e indireta e zela pela proteção a direitos e garantias. No Canadá, a *Royal Canadian Mounted Police* (RCMP) tem acesso limitado às informações da Administração direta e indireta, e cabe ao Comissário para Proteção à Vida Privada (OPC) proteger e promover o direito à privacidade no Canadá.

Assim como o instituto do *habeas data* no Brasil, o *Privacy Act,* 1985 (CANADA, 1985*p*) garante a qualquer pessoa o acesso a informações pessoais suas de posse do governo, inclusive para corrigi-las. Entretanto, esse acesso não é pleno, uma vez que há limitações a informações recebidas de governos ou instituições estrangeiras, bem como ao fornecimento de dados que possam ameaçar a segurança nacional ou as relações exteriores do Canadá, e ainda, informação utilizada em investigação criminal.

No sistema canadense existem os “arquivos inconsultáveis” (“*exempt banks")* – bancos de dados que estão fora da liberdade de acesso prevista no *Privacy Act,* 1985

(CANADA, 1985*p*). São arquivos relacionados à segurança nacional e à segurança pública, e as informações pessoais neles contidas não podem ser consultadas nem por ordem judicial. Os *exempt banks* estão previstos em decreto e compreendem: os Registros de Inteligência Criminal (*Criminal Operations Intelligence Records*), controlados pela RCMP (*Royal Canadian Mounted Police*); os Registros de Investigações do CSIC (*Canadian Security Intelligence Service Investigational Records*); e os Registros de Investigações de Segurança Nacional (*National Security Investigations Records*), também sob a guarda da RCMP. O fato do cidadão comum não ter acesso aos *exempt banks* não significa que o OPC não o tenha. O Comissário para a Vida Privada pode acessar esses registros, examiná-los e verificar eventuais irregularidades. Nesse sentido, produz relatório que é encaminhado ao Ministro da Segurança Pública com recomendações (GONÇALVES, 2008).

3) A legislação trata dos que tem direito à informação e dos órgãos que podem acessar essas informações. Por se tratar de PSI, o acesso à informação deve ser observado em relação àqueles que manipulam diretamente essas informações. Em questões de e-Gov, a PSI deve prever o controle de acesso, para restringir os indivíduos não autorizados de usarem recursos de informação, ao forçar a identificação do usuário. O controle de acesso pode ser pelo exame das características físicas do usuário (biométricos), por cartões de identificação, por voz e assinatura, e por senhas. Há também necessidade de prever a proteção, modificação e destruição dos dados e informações contra exposição acidental ou voluntária a pessoas não autorizadas (TURBAN *et al*., 2007). Sem esses cuidados, nada adiantaria legislar sobre o acesso a informações no e-Gov.

6.3. Privacidade

1) Em geral, a privacidade é o direito de ficar em paz e estar livre de invasões pessoais injustificáveis e indesejáveis. A privacidade de informações é o direito de determinar quando e até que ponto as informações sobre um indivíduo podem ser coletadas e/ou comunicadas a outros indivíduos (TURBAN *et al*., 2007).

Tanto no Brasil quanto no Canadá há defesa da privacidade de informações relacionadas à intimidade, à vida privada de alguém, e privilegiadas em razão da função que ocupa, como também o direito à privacidade das comunicações, com o sigilo dos dados e das comunicações privadas, podendo incluir o sigilo dos dados via Internet.

Questão atrelada à privacidade é a PSI. Foi verificada que a privacidade é protegida nos ordenamentos jurídicos do Brasil e Canadá por meio do sigilo, guardando algumas

similitudes e diferenças em seus aspectos normativos e operacionais. Ambos são países democráticos e primam pelo princípio da Publicidade e da Dignidade da Pessoa Humana na PSI.

Do princípio da Publicidade decorre a transparência administrativa, pois não pode haver em um Estado Democrático de Direito ocultamento aos atos administrativos dos assuntos que a todos interessam, e muito menos em relação aos sujeitos individuais afetados por alguma medida. O sigilo só se admite na esfera pública quando imprescindível à segurança da sociedade e do Estado (MELLO, 2003).

Do princípio da Dignidade da Pessoa Humana decorre a garantia do sigilo das informações privadas. Conforme a Declaração Universal dos Direitos do Homem "ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou reputação" (ONU, 1948). Contudo, quando há investigações relacionadas a problemas com segurança da informação e preservação da sociedade e do Estado, há exigência de quebra de sigilo das informações privadas.

Surge então a dicotomia dos Estados Democráticos: preservar a privacidade ou o interesse público? Neste caso, a intromissão na vida privada deve ser uma excepcionalidade precedida de fundamento de interesse público. As informações privadas deverão ser divulgadas com autorização ou por motivação pública, amparada pelo ordenamento jurídico.

2) No Brasil a Lei nº 8.159, 1991 (BRASIL, 1991), dispõe sobre a Política Nacional de Arquivos Públicos e Privados e o Decreto n° 4.073, 2002 (BRASIL, 2002*g4*) regulamenta sobre a gestão documental e à proteção especial aos documentos de arquivo. No Canadá a *Personal Information Protection and Electronic Documents Act*, 2000, (CANADA, 2000), estabelece dez princípios que as organizações no que concerne à coleta, uso, divulgação e armazenamento de dados pessoais, e sobre a proteção dos mesmos. Esses procedimentos estão correlacionados à teoria de Gestão da Informação, apregoadas pelos autores Thomas Wilson (1989), Chun Wei Choo (2003), Adriana Beal (2004), McGee e Prusak (1994) e Thomas Davenport (1998). A proteção à privacidade é observada pelos modelos genéricos de gerenciamento da informação, pois a gestão das informações nos Estados provoca ajustes em seus *modus operandi*, principalmente no uso que se faz delas. E o direito à privacidade é um direito garantido pelo Brasil e Canadá, excetuando-se quando o interesse público prevalecer, conforme um dos objetivos fundamentais da PSI: confidencialidade das informações.

6.4. Administração Pública e Transparência

1) À Administração Pública brasileira é previsto constitucionalmente seu dever de proteger os documentos e obras, a fim de proteger a integridade, a autenticidade e a disponibilidade das informações do Estado, além de realizar a gestão da documentação governamental e as providências para franquear sua consulta. No Canadá, essa proteção e gestão estão previstas nas leis *Privacy Act*, 1985 (CANADA, 1985*p*), e *Access to Information Act*, 1985 (CANADA, 1985*k*). Essas normas, tanto no Brasil quanto no Canadá, contêm preceitos de PSI, pois a proteção à integridade, à confidencialidade, à disponibilidade e ao sigilo das informações são objetivos fundamentais da PSI, sendo mais um motivo para esta ser devidamente implantada na Administração Pública por meio do e-Gov.

No Brasil, o Subcomitê da Rede Brasil.gov é o responsável pelo projeto de integração das diversas redes de comunicação de dados do Governo Federal. No Canadá, o *Government Electronic Directory Services* (GEDS) administra as informações de servidores públicos federais, e o *Communications Security Establishment* (CSE) é o responsável pelos serviços de inteligência estrangeira de apoio à defesa e à política externa, e de proteção das informações e das comunicações eletrônicas. Conforme Marco Cepick (2001, p. 138) os governantes tendem "a justificar institucionalmente e a delimitar as funções dos serviços de inteligência em termos de sua necessidade para a segurança nacional. Entretanto, a noção de segurança nacional é problemática, pois tanto seu significado quanto as conseqüências práticas de seu uso não são auto-evidentes". Assim, a regulamentação é mais política do que propriamente técnica.

Em virtude disso, a gestão da informação na Administração Pública é necessária para tornar eficaz a gestão de todos os recursos de informação relevantes, tanto de recursos gerados internamente como os produzidos externamente, delimitados pela PSI de cada Estado. Pode-se utilizar a tecnologia de informação para tornar a gestão da informação mais eficaz, como é feito pelo e-Gov. O e-Gov, em sua essência, gerencia informações por meio de novas tecnologias, e por ser relevante esse procedimento, as informações presentes no aparato estatal precisam ser protegidas e devidamente processadas, armazenadas, usadas e publicadas para garantir a segurança das mesmas ao manter sua confidencialidade, sua disponibilidade, sua integridade e a privacidade dos indivíduos.

A Constituição (BRASIL, 2009*a1*) brasileira também prevê os princípios que regem a Administração Pública: legalidade, impessoalidade, moralidade, publicidade e eficiência. Há defesa ao direito à privacidade quando o sigilo das informações relacionadas à intimidade ou à vida privada de alguém não prejudique o interesse público à informação. O texto

constitucional dispõe ainda sobre a responsabilidade objetiva das pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos decorrente da má gestão das funções e das informações. Essa regulamentação não vem explícita na Consolidação das Leis Constitucionais, 1867-1982 do Canadá (CANADA, 1982). Entretanto, a *Public Servants Disclosure Protection Act*, 2005 (CANADA, 2005*e*), estabelece um procedimento para a revelação de erros de servidores no setor público, inclusive a proteção de servidores que revelam os erros. A garantia da preservação dos princípios administrativos e da privacidade está prevista na punição dos agentes públicos, ou não, quando agem indevidamente. Se não houver punição aos infratores, não adianta implantar a PSI na Administração Pública.

2) Em 1994 houve a difusão de novos sistemas informacionais na Administração Pública em geral, notadamente em 1995 com o uso da Internet. Com isso, o Brasil e o Canadá tomaram medidas para criar o e-Gov. A implantação do e-Gov ocorreu em 1999 no Canadá e em 2000 no Brasil.

Com relação aos avanços tecnológicos, o Canadá tomou medidas para implantar sistemas de gestão e prestação de serviços em instrumentos de TI. A implantação do e-Gov foi iniciada em 1999 e tornou-se referência mundial em questões de prestação de serviços e informações governamentais. No Canadá não foram encontradas regulamentações sobre o e-Gov, mas no Brasil sim. Ronaldo Lemos (2005) faz uma observação sobre a norma que instituiu o Comitê Gestor da Internet no Brasil. Para ele, o Comitê, produto da Portaria Interministerial nº 147, 1995 (BRASIL, 1995), em Nota Conjunta do MC e MCT, nasceu com características híbridas: sem personalidade jurídica própria, nem de direito público ou privado, sem respaldo em qualquer legislação, sem qualquer competência normativa e criado por portarias interministeriais sem competência para tanto. Ainda critica as decisões judiciais que citam as resoluções normativas do Comitê, dando a estas, força de lei. Dessa forma, o Comitê, eivado de problemas institucionais, tornou-se fonte normativa no país (LEMOS, 2005)

3) O Brasil e o Canadá ratificaram a Convenção das Nações Unidas contra a Corrupção, em 2006 e 2007, respectivamente. Notam-se similitudes em suas pretensões, pois ambos os países buscam prevenir e combater a corrupção, tornar seus atos mais transparentes e promover a *accountability*. São medidas imprescindíveis para a implantação da PSI, pois não se admite uma PSI não pautada nos preceitos de segurança humana. Se houver práticas de corrupção, não transparência e não responsabilização dos agentes públicos implica na não observância da segurança humana, e conseqüentemente da PSI. A segurança humana é a parte

mais fraca da PSI, pois “um só indivíduo” pode destruir toda infra-estrutura da base de dados de sua organização.

Para David Luban (1996, p. 154), a transparência dos atos, normas e políticas governamentais é uma “condição necessária para a manutenção da confiança popular que sustenta as instituições democráticas e legitima as pretensões dos governantes de obtenção da colaboração e obediência dos governados”. Isso se aplica à PSI no Brasil e Canadá, pois se percebe a busca de ambos no exercício da transparência administrativa, notadamente por meio do e-Gov que é mais uma possibilidade de tornar efetivo o princípio da responsabilidade, e em decorrência a transparência e a *accountability* dos governantes.

6.5. Ilicitudes

Brasil

1) No Brasil e no Canadá prescrevem como crimes a inserção ou alteração de dados e informações em bancos de dados da Administração Pública por funcionários com acesso autorizado. Também protegem a integridade, a autenticidade, a confidencialidade e a disponibilidade dos documentos públicos e informações constantes nos órgãos e entidades públicos, objetivos fundamentais da PSI.

Essas regulamentações demonstram a necessidade de uma gestão da segurança da informação baseada na segurança humana. Conforme Adriana Beal (2005) a melhor política de segurança em relação a qualquer indivíduo com acesso aos recursos de informação corporativos é confiar desconfiando, pois grande parte dos incidentes de segurança é provocada por integrantes da própria organização, sejam eles acidentais ou intencionais. Necessita-se da permanente colaboração dos funcionários da organização, tanto na prevenção, quanto na reação a eventuais problemas de segurança, principalmente no âmbito da Administração Pública que lida com informações de relevância para a sociedade.

De acordo com Alexandre Atheniense (2007) as ferramentas que permitem regular o uso seguro das informações estão se aperfeiçoando com o uso das identidades biométricas e certificação digital, de modo a deixar indícios inequívocos sobre o acesso e o compartilhamento de materiais considerados ilícitos. Isso é uma prática de PSI voltada para a segurança humana, que demanda vigília e revisão permanente.

Por isso, a PSI deve ser pautada em regras claras e preventivas, com constantes atualizações dos funcionários da organização a fim de atualizá-los sobre os riscos de suas

ações e de minimizar os efeitos nocivos da engenharia social, especialmente em relação às ações do e-Gov, que expande a forma de publicidade dos atos da Administração Pública.

Foram encontrados dois projetos de lei no Senado brasileiro – PL substitutivo do Senador Eduardo Azeredo, de 2006 (BRASIL, 2006*c2*) e PL nº 21, de 2004 (BRASIL, 2004*e3*) – que podem facilitar a implantação da PSI no Governo e nas organizações privadas e não governamentais. Tipificam condutas não legisladas importantes para a segurança lógica, humana e física, como difusão de vírus, roubo de senhas, e acesso não autorizado a dados. No Canadá não foram encontrados projetos de leis semelhantes, após pesquisa detalhada e minuciosa no Parlamento canadense.

A regulamentação brasileira sobre segurança da informação e sua punição no Código Penal, 1940 (BRASIL, 1940) é muito discutida e criticada como insuficiente. Apesar disso e da suposta subjetividade de julgamentos pelos juízes, o ordenamento jurídico brasileiro prescreve em seu o art. 4º, da Lei de Introdução ao Código Civil que: "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito" (BRASIL, 1942)[147]. Entretanto, a interpretação jurídica é técnica e será subjetiva somente quando o profissional for mal preparado ou anti-ético. Há métodos para enquadramento de situações não previstas em lei, por isso não há necessidade de uma norma para cada evento no mundo, o que também tornaria inviável o controle social dado o volume de normas a conhecer e operar, a obsolescência das normas e a necessidade de criar outras tantas em decorrência de novos fatos. No Canadá, ao contrário, é o caso concreto que prevalece devido ao seu ordenamento jurídico baseado no direito comum, ou seja, o juiz que decidirá sobre a conduta do indivíduo em desagrado às condutas médias da população, independente de lei anterior abstrata como ocorre no Brasil.

Um exemplo sobre PSI que tem ocorrido nas organizações do Brasil, inclusive em órgaos da Administração Pública direta e indireta, é o monitoramento do conteúdo de *e-mails* pessoais dos funcionários. Conforme Patrícia Peck Pinheiro (2008) a organização deve avisar previamente sobre a monitoração, com avisos no próprio ambiente de trabalho. Adverte que nos últimos dois anos o número de organizações que estão adotando normas de PSI vem aumentando, mas que a maioria ainda não possui essas regras claramente. Se as normas não são explícitas, a organização não tem a possibilidade de processar juridicamente o funcionário. Se o indivíduo for demitido e descobrir-se que o motivo foi devido a uma conversa por *e-mail*, sem aviso de monitoramento da organização, o indivíduo poderá entrar

[147] APÊNDICE A, p. 142.

com um pedido de indenização. Os juízes têm entendido que quem tem a responsabilidade das ferramentas de trabalho é a organização e ela é responsável por seu mau uso (PINHEIRO, 2008).

2) Outra questão de ilicitude relacionada à PSI se refere ao terrorismo, legislado no Brasil e no Canadá. Após os atentados terroristas de 11 de setembro de 2001 nos Estados Unidos, ocorreram muitas modificações na legislação canadense.

No Canadá a regulamentação sobre terrorismo é mais esparsa por vários motivos. Dentre os motivos podem-se citar o ataque terrorista de 23 de junho de 1985, quando o Boeing 747 da *Air India* que fazia o vôo 182 de Montreal a Déli explodiu matando 329 indivíduos, dos quais 289 cidadãos canadenses (GONÇALVES, 2008); e o ataque terrorista de 11 de Setembro de 2001 nos Estados Unidos, país vizinho e principal aliado, que resultou em mortes de cidadãos canadenses e afetou as empresas canadenses (DFAIT, 2003). Frente a isso, o Canadá considera a prevenção ao terrorismo uma das componentes chaves de sua estratégia de segurança nacional, por isso criou a *Anti-Terrorism Act*, em 15 de outubro de 2001 (CANADA, 2001*i*), um mês após o ataque de 11 de setembro, a fim de fornecer novas ferramentas de investigação para a aplicação da lei e agências de segurança nacional.

O *Criminal Code*, 1985 (CANADA, 1985*n*), foi modificado, passando a conceituar ataque terrorista e prever os delitos desse fim. A *Public Safety Act*, 2002 (CANADA, 2002*g*), alterou 18 leis federais para reforçar a capacidade do Governo para proteger canadenses e prevenir ataques terroristas. O projeto de lei LS-400E, Bill C-16 que visa modificar a *Charities Registration (Security Information) Act* (CANADA, 2001*j*), tem por objetivo concentrar esforços internacionais para negar apoio a todos envolvidos no terrorismo. Sua finalidade é proteger a integridade do sistema de registro de caridade da Lei de Imposto de Renda, 1985 (*Income Tax Act*, 1985*r*) contra ameaça de entidades terroristas que se passam por entidades caridosas.

A Receita Federal do Canadá (*Canadian Revenue Agency - CRA*) também possui seu segmento de inteligência. Um dos focos de suas atividades de segurança nacional diz respeito ao controle das organizações beneficentes do país, verificando possíveis vínculos de algumas delas com financiamento do terrorismo (GONÇALVES, 2008). A *Anti-Terrorism Act*, 2001 (CANADA, 2001*i*) prevê que uma entidade beneficente pode perder seu *status* se o Ministro da Fazenda (*Minister of National Revenue*) ou o da Segurança Pública entender que há motivos razoáveis para crer que a organização tem alguma relação com o financiamento de grupos ou atividades terroristas, sendo emitido um documento (certificado) sobre isso.

O Brasil em resposta às demandas internacionais de combate ao terrorismo, e mesmo não tendo sido identificada ameaça terrorista no território brasileiro, criou o Departamento de Contra-terrorismo, com funções de planejar a execução de atividades de prevenção às ações terroristas no território nacional, bem como obter informações e produzir conhecimentos sobre tais organizações terroristas (GONÇALVES, 2008).

Em termos de segurança, Canadá e Brasil não têm inimigos declarados entre Estados. Ambos encontram-se nas regiões mais pacíficas do planeta, são membros de organizações internacionais e regionais, defendem posições semelhantes em foros globais e em regimes internacionais (GONÇALVES, 2008).

O Canadá tem-se mostrado referência importante na área de segurança da informação e inteligência pelo seu aparato eficiente, exatamente pelo perfil de sua população, território e governo, e por sua proximidade e relações estreitas com os Estados Unidos e Europa. O país possui importante sistema de segurança de informações que tem servido de paradigma para outros países como o Brasil (GONÇALVES, 2008).

Numa análise mais minuciosa de Brasil e Canadá leva à constatação que os dois países possuem posições convergentes em termos de política externa e de segurança da informação. Há aproximação entre os sistemas de inteligência dos dois países nos últimos anos, com o Brasil reestruturando seu serviço secreto baseado no modelo canadense. Em termos de ameaças, destacam-se as preocupações com o terrorismo e o crime organizado. Também possuem diversidade étnica e cultural significativa em suas próprias populações e dificuldades de convencer a opinião pública de que o país é alvo de ameaças externas. Essa heterogeneidade associada à significativa inserção de distintos grupos de imigrantes e seus descendentes nas estruturas sociais e na composição dos quadros do Estado constitui aspecto interessante em termos de segurança, sobretudo para a inteligência da informação. Em maior ou menor escala, é possível encontrar pessoas das mais diferentes etnias no serviço público, inclusive nos órgãos de inteligência canadense e brasileiro (GONÇALVES, 2008).

A cultura canadense e, sobretudo, a brasileira não vêem em defesa e inteligência temas prioritários de debate pela sociedade. O debate sobre os riscos de atentados terroristas no Canadá ainda é incipiente, e no Brasil é praticamente desconsiderado.

3) Nos dois países não há regulamentações específicas sobre os crimes praticados na área de informática, sendo julgados e decididos sobre a punição em Tribunais. Em relação aos crimes de pedofilia praticados pela Internet, os dois países já possuem projetos de lei sobre o tema e resguardam os direitos das crianças e adolescentes.

Nota-se a preocupação de ambos países com questões de direito humano, do cidadão exercer seus direitos e ser respeitado, notadamente as crianças. Com isso criminalizam a pedofilia e a pornografia infantil tão presentes na rede Internet. Essas condutas também podem abarcar outras atividades ilegítimas, como estereografia de fotos pornográficas contendo cavalos de tróia, *spams*, vírus etc. O indivíduo que acessar essas fotos displicentemente ou intencionalmente num órgão da Administração Pública poderá corromper todo o sistema de informações daquele órgão ou também de outros órgãos se executar o arquivo malicioso. Informações sigilosas e ultra-secretas poderão ser utilizadas por *hackers*, que por sua vez poderão utilizá-las de forma indevida e criminosa.

6.6. Normas e Padrões Internacionais da Segurança da Informação

O Brasil como o Canadá são signatários das normas e padrões internacionais nas questões relacionadas à segurança da informação. Dentre as normas e padrões podem-se citar a Gestão de Riscos do Canadá, em 1997; a "família" BS 7799, posteriormente modificada pela ISO com a finalidade de estruturar os padrões de segurança da informação para as séries 'ISO 27000'; e a ISO/IEC *Guide 73, Risk Management: Vocabulary - Guidelines for use in standards*, publicada em 2002. Uma nova norma universal será publicada a partir de outubro de 2009 sobre Gestão de Riscos, chamada ISO 31000: *Principles and Guidelines for Risk Management*.

No Brasil, essas normas são publicadas pela ABNT, Associação Brasileira de Normas Técnicas, criada em 1940, como uma organização sem fins lucrativos que se dedica à normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro. No Brasil as normas das séries 'ISO 27000' citadas acima recebem a denominação NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão da Segurança da Informação e NBR ISO/IEC 27001:2006 Sistemas de Gestão de Segurança da Informação (ISO, 2009).

No Canadá essas normas são publicadas pelo *Standards Council of Canada* (SCC), empresa criada pelo Parlamento, em 1970, para incentivar e promover a normalização voluntária no Canadá. O SCC não desenvolve normas em si, mas coordena a entrada e o uso de normas internacionais no Canadá. Diferentemente do Brasil, mantêm a mesma nomenclatura das normas do ISO (ISO, 2009).

Em relação à norma universal sobre Gestão de Riscos, chamada ISO 31000, que será publicada a partir de outubro de 2009, a versão brasileira está sendo desenvolvida e deverá ser

lançada quase que simultaneamente à versão original pela ABNT, e a versão canadense será lançada pelo SCC.

No Brasil, em 2001, o Serpro[148] adotou a metodologia prevista nas normas internacionais BS 7799 e ISO 17799-1 de que todo e qualquer sistema, antes de entrar em produção, teria de necessariamente passar por uma análise de riscos. Em março de 2006, o Serpro foi a primeira empresa pública brasileira e da América do Sul a conquistar a certificação *British Standart* 7799 (BS7799), e a sexta no rol de empresas nacionais, dando reconhecimento internacional da qualidade dos serviços de segurança do Serpro (SERPRO, 2006*a*). O modelo de certificação e auditoria usado é equivalente aos das normas ISO 9001 e ISO 14000. No Canadá, a *Standards Store* que possui esse certificado, respaldada pela SCC.

Pode-se notar que tanto Brasil quanto Canadá seguem as normas técnicas internacionais e fazem suas adaptações de acordo com os órgãos responsáveis por estudá-las e publicá-las. Essas normas são baseadas em questões de segurança da informação, pautando-se nas seguranças físicas, humanas, lógicas e de *software* de código aberto. São normas relevantes que possibilitam a uniformização da gestão da informação e sua aplicação e replicação em diferentes organizações interessadas em assegurar suas informações. São amplamente aplicadas na segurança da informação do e-Gov tanto do Brasil quanto do Canadá, preocupados com a eficiência e efetividade de suas ações frente à sociedade.

[148] Serpro - Serviço Federal de Processamento de Dados. Empresa pública líder em soluções de Tecnologia da Informação e Comunicações (TICs) para realização das Políticas Públicas. Visa prover e integrar soluções em TICs para o êxito da gestão das finanças públicas e da governança do Estado, em benefício da sociedade.

CONCLUSÃO

1) A sociedade do conhecimento desenvolveu possibilidades administrativas inimagináveis que facilitam o acesso a informações sem precisar estar no local e horário pré-condicionados. As novas TICs possibilitaram a criação do e-Gov, que modificou o *modus operandi* estatal ao ampliar a cidadania, a transparência e a participação dos cidadãos na Administração Pública, mesmo que para uma parcela da sociedade. Entretanto, essas ações beneficiam a todos em geral (*free riders)*, pois ganhos democráticos atingem toda a população.

2) A gestão da informação é importante para identificar as etapas da vida da informação e para classificar os ativos da informação. A gestão permite a concepção de novos conhecimentos, que poderiam se perder numa organização – pública ou privada. Sem a gestão, não há que se falar em PSI, pois não se terá conhecimentos para fazê-la. Antes de implementar uma PSI, os responsáveis devem ter conhecimentos sobre o que pretendem proteger, como, quando e quanto isso custa. Após, passariam a implementar a PSI, que deverá ser avaliada, reavaliada, aperfeiçoada e modificada quando necessário ou estipulado. Se essas questões não forem pensadas, de nada adiantaria uma PSI, seria apenas perda de tempo, recursos financeiros e humanos.

]3) A PSI deve ser pensada sobre vários aspectos, tendo em vista a segurança humana, a segurança do ambiente físico, a segurança do ambiente lógico, e a segurança do *software* de código aberto. A Administração Pública ao implantar uma PSI em seu e-Gov pautada nesses aspectos torna mais fundamentada e confiável sua tomada de decisão em questões de políticas públicas, ao reduzir o número de informações falsas e desnecessárias, e disponibilizar a informação certa, na hora certa.

4) A regulamentação da segurança da informação no Brasil e Canadá é ampla, com o respeito aos princípios de Legalidade, Publicidade, e Dignidade da Pessoa Humana. Legislam sobre privacidade, sigilo profissional, classificação das informações de Estado, o seu acesso, e sua criminalização pela manipulação indevida da informação. Apesar de serem países com muitas similitudes, possuem suas singularidades, com algumas diferenças em seus aspectos normativos e operacionais. Ambos são países colonizados, com variedades naturais e multiculturais; sistemas jurídicos advindos de tradições diferentes; e instituídos como Estados Democráticos de Direito. Essas características norteiam a PSI com respeito à transparência administrativa e à garantia do sigilo das informações de segurança nacional. São países respeitados, possuem políticas de e-Gov modernas, servem de exemplo para outros países em questões de PSI, e trilham caminhos semelhantes no aprimoramento da mesma.

BIBLIOGRAFIA

ABNT. **Associação Brasileira de Normas Técnicas**. Disponível em: <http://www.abnt.org.br>. Acesso em: 30 ago. 2009.

AFONSO, Carlos A. Internet no Brasil – alguns dos desafios a enfrentar. **Revista de Informática Pública**, Belo Horizonte, v. 4 (2), pp. 169-184, 2002.

AGNER, Luiz Carlos. **O movimento dos e-governos do Brasil e do Canadá em direção a uma cultura de interfaces centradas no cidadão**. Este trabalho baseia-se parcialmente na tese de doutorado: Arquitetura de informação e governo eletrônico: diálogo cidadãos-Estado na *World Wide Web* – estudo de caso e avaliação ergonômica de usabilidade de interfaces humano-computador. 2007. 358f. Tese de Doutorado – Departamento de Artes e Design, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

ATHENIENSE, Alexandre. O monitoramento eletrônico e as relações trabalhistas. **Revista Fonte** – Tecnologia da Informação na Gestão Pública. Julho/Dezembro de 2007. Ano 4 – Número 07. 2007.

AUSTRÁLIA. **AS/NZS 4360**. Publicada em 1995 e revisada em 1999 e em 2004. Norma australiana e neozelandesa para padronização da segurança da informação. Disponível em: <http://www.softexpert.com.br/norma-asnzs.php>. Acesso em: 30 ago. 2009.

BASTOS, Alberto. ISO 31000: a nova era da gestão de riscos começa em outubro. **Baguete Diário**. Artigo escrito em 17 de fevereiro de 2009. Disponível em: <http://www.baguete.com.br/artigosDetalhes.php?id=786>. Acesso em: 11 mai. 2009.

BEAL, Adriana. **A Gestão Estratégica da Informação:** Como Transformar a Informação e a Tecnologia da Informação em Fatores de Crescimento e de Alto Desempenho nas Organizações. São Paulo: Atlas, 2004.

_____. **Segurança da Informação**: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas, 2005.

BNDES. **E-Governo: O que ensina a experiência internacional.** Secretaria Para Assuntos Fiscais – SF. Boletim "Informe-se" nº 17, agosto, 2000. Disponível em <http://www.bndes.gov.br/conhecimento/informeSF/inf_17.pdf> Acesso em 28/05/2008.

BRASIL. **Câmara dos Deputados**. Projeto de Lei nº 4.036, de 2008. Brasília, 2008. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=410666>. Acesso em: 30 ago. 2009.

BRASIL. **Câmara dos Deputados**. Projeto de Lei n° 3.651, de 19 de setembro de 1997. Brasília, 1997*i1*. Disponível em: <http://www.camara.gov.br/sileg>. Acesso em: 30 ago. 2009.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 2009*a1*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Código Civil**: Lei n◦ 10.406, de 10 de janeiro de 2002. Brasília, 2002*g1*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Código de Conduta da Alta Administração**, 2000. Brasília, 2000*j1*. Disponível em: <http://www.presidencia.gov.br/estrutura_presidencia/cepub/legislacao/etica3/>. Acesso em: 30 ago. 2009.

BRASIL. **Código de Ética do Servidor Público**, Decreto nº 1.171, de 22 de junho de 1994. Brasília, 1994*l1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d1171.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Código de Processo Civil**, Lei n° 5.869, de 11 de janeiro de 1973. Brasília, 1973. Disponível em: <http://www.planalto.gov.br/CCIVIL/Leis/L5869.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Código de Processo Penal**, Decreto-Lei nº 3.689, de 3 de outubro de 1941. Brasília, 1941. Disponível em: <http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Código Penal:** Decreto-lei n◦ 2.840, de 7 de dezembro de 1940. Brasília, 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 30 ago. 2009.

BRASIL. **Código Tributário Nacional**, Lei nº 5.172, de 25 de outubro de 1966. Brasília, 1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L5172Compilado.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Consolidação das Leis do Trabalho**, Decreto-Lei n.º 5.452, de 1º de maio de 1943. Brasília, 1943. Disponível em: <http://www.planalto.gov.br/ccivil/Decreto-Lei/Del5452.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 6.605, de 14 de Outubro de 2008**. Brasília, 2008*b1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6605.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 6.029, de 1º de fevereiro de 2007**. Brasília, 2007. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Decreto/D6029.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 5.687, de 31 de janeiro de 2006***c1*. Brasília, 2006*c1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 5.584, de 18 de novembro de 2005**. Brasília, 2005*d1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5584.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 5.482, de 30 de junho de 2005**. Brasília, 2005*d2*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5482.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 5.301 de 9 de dezembro de 2004**. Brasília, 2004*e1*. Disponível em: <http://www.planalto.gov.br/CCIVIL/_Ato2004-2006/2004/Decreto/D5301.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n◦ 4.553, de 27 de dezembro de 2002**. Brasília, 2002*g2*. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553Compilado.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n◦ 4.376, de 13 de setembro de 2002**. Brasília, 2002*g3*. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4376a.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n◦ 4.073, de 3 de janeiro de 2002**. Brasília, 2002*g4*. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4073.htm>. 30 ago. 2009.

BRASIL. **Decreto s/n°, de 04 de dezembro de 2001**. Brasília, 2001*h1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/DNN/2001/Dnn9402.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n° 3.996, de 31 de outubro de 2001**. Brasília, 2001*h2*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto s/nº de 18 de outubro de 2000**. Brasília, 2000*j2*. Disponível em: <https://www.governoeletronico.gov.br/o-gov.br/legislacao/decreto-de-18-de-outubro-de-2000>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n◦ 3.505, de 13 de junho de 2000**. Brasília, 2000*j3*. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto Presidencial s/nº de 03 de abril de 2000**. Brasília, 2000*j4*. Disponível em:<https://www.governoeletronico.gov.br/.../E15_90Decreto_3_de_abril_de_2000.pdf>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto n° 3.294, de 15 de dezembro de 1999**. Brasília, 1999*k1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3294.htm >. Acesso em: 30 ago. 2009.

BRASIL. **Decreto no 2.910, de 29 de dezembro de 1998 (Revogado)**. Brasília, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D2910.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 2.134, de 24 de janeiro de 1997 (Revogado)**. Brasília, 1997*i2*. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/D2134.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto nº 1.048, de 21 de janeiro de 1994**. Brasília, 1994*l2*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D1048.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Decreto Legislativo nº 348, de 18 de maio de 2005**. Brasília, 2005*d3*. DOU. Diário Oficial da União, 19 Maio 2005 (núm. 348).

BRASIL. **Instrução Normativa nº 4, de 19 de maio de 2008**. SLT – MPOG. Brasília, 2008*b2*. Disponível em: <http://biblioteca.idbrasil.gov.br/publicacoes/decretos-editais-portarias-e-pregoes/instrucao-normativa-no-4>. Acesso em: 30 ago. 2009.

BRASIL. **Lei Complementar nº 131, de 27 de maio de 2009**. Brasília, 2009*a2*. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp131.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei Complementar 105, de 10 de janeiro de 2001**. Brasília, 2001*h3*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei Complementar nº 101, de 4 de maio de 2000**. Brasília, 2000*j5*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/lcp101.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei Complementar nº 75, de 20 de maio de 1993**. Brasília, 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp75.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei de Introdução ao Código Civil Brasileiro.** Decreto-lei nº 4.657, de 4 de setembro de 1942. Brasília, 1942. Disponível em: <http://www.planalto.gov.br/Ccivil_03/ Decreto-Lei/Del4657.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Brasília, 2008*b3*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 11.754, de 23 de julho de 2008**. Brasília, 2008*b4*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11754.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 11.111, de 05 de maio de 2005**. Brasília, 2005*d4*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei n◦ 9.983, de 14 de julho de 2000**. Brasília, 2000*j6*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei n◦ 9.883, de 7 de dezembro de 1999**. Brasília, 1999*k2*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Brasília, 1997*i3*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Brasília, 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 8.183, de 11 de abril de 1991**. Brasília, 1991*m1*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8183.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei n◦ 8.159, de 8 de janeiro de 1991**. Brasília, 1991*m2*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8159.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei n° 8.069, de 13 de julho de 1990**. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Lei nº 7.232, de 29 de outubro de 1984**. Brasília, 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Medida Provisória n◦ 228, de 9 de dezembro de 2004**. Brasília, 2004*e2*. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/Mpv/228.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Medida Provisória n◦ 2.200-2, de 24 de agosto de 2001**. Brasília, 2001*h4*. Disponível em: <https://www.planalto.gov.br/ccivil_03/MPV/2200-2.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Portaria Nr 11 - CH/GSI, de 27 de junho de 2003**. Brasília, 2003*f1*. Disponível em: <http://dsic.planalto.gov.br/documentos/portaria_n11.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Portaria Interministerial Conjunta CIVIL/MC/MCT nº 739, de 02 abril de 2003**. Brasília, 2003*f2*. Disponível em: <http://www.cgi.br/regulamentacao/port739.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Portaria da Casa Civil n° 23 de 12 de maio de 2000**. Brasília, 2000*j7*. Disponível em: <http://www.planalto.gov.br/ccivil_03/dnn/2000/.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Portaria Interministerial Conjunta CIVIL/MC/MCT nº 147, de 31 de maio de 1995**. Brasília, 1995. Disponível em: <http://www.cgi.br/regulamentacao/port147.htm>. Acesso em: 30 ago. 2009.

BRASIL. **Senado Federal**. Projeto de Lei do Senador Eduardo Azeredo, 2006. Brasília, 2006*c2*. Disponível em: <http://www.senado.gov.br/sf/senadores/senadores_institucional.asp?leg=a&codparl =3400>. Acesso em: 30 ago. 2009.

BRASIL. **Senado Federal**. Projeto de Lei nº 21 de 2004. Brasília, 2004*e3*. Disponível em: <http://www.senado.gov.br/sf/atividade/materia/detalhes.asp?p_cod_mate=66397>. Acesso em: 30 ago. 2009.

CALDERON, Wilmara Rodrigues *et all*. O processo de gestão documental e da informação arquivística no ambiente universitário. **Revista Ciência da Informação**, Vol. 33, N° 3. 2004.

CAMPOS, Marcelo Barroso Lima Brito de. **Regime Próprio de Previdência Social dos Servidores Públicos**. Belo Horizonte: Líder, 2004.

CANADA. ***Access to Information Regulations,* 2009.** Ottawa, 2009*a*. Disponível em: <http://laws.justice.gc.ca/en/A-1/SOR-83-507/index.html>. Acesso em: 30 ago. 2009.

CANADA. ***Privacy Act Extension Order* n° 1, 2009.** Ottawa, 2009*b*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cr/SOR-83-553>. Acesso em: 30 ago. 2009.

CANADA. ***Privacy Act Extension Order,* n° 2, 2009.** Ottawa, 2009*c*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cr/SOR-89-206>. Acesso em: 30 ago. 2009.

CANADA. ***Privacy Regulations,* 2009.** Ottawa, 2009*d*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cr/SOR-83-508>. Acesso em: 30 ago. 2009.

CANADA. ***Public Servants Disclosure Protection Act,* 2005.** Ottawa, 2005*e*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cs/P-31.9>. Acesso em: 30 ago. 2009.

CANADA. ***Secure Electronic Signature Regulations,* 2005**. Ottawa, 2005*f*. Disponível em: <http://canadagazette.gc.ca/archives/p2/2005/2005-02-23/html/sor-dors30-eng.html>. Acesso em: 30 ago. 2009.

CANADA. ***Public Safety Act,* 2002. Ottawa, 2002**. Ottawa, 2002*g*. Disponível em: <http://laws.justice.gc.ca/en/P-31.5/>. Acesso em: 30 ago. 2009.

CANADA. **Projetos de Lei C-15, C-15A e C-15B de setembro de 2002**. Ottawa, 2002*h*. Disponível em: <http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?Parl=37&Ses=1&ls=C15A>. Acesso em: 30 ago. 2009.

CANADA. ***Anti-terrorism Act,* 2001.** Ottawa, 2001*i*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cs/A-11.7>. Acesso em: 30 ago. 2009.

CANADA. **Projeto de Lei. LS-400E, *Bill* C-16 *Charities Registration (Security Information) Act,* em março de 2001.** Ottawa, 2001*j*. Disponível em: <http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/LS/371/c16-e.htm>. Acesso em: 30 ago. 2009.

CANADA. ***Personal Information Protection and Electronic Documents Act,* 2000**. Ottawa, 2000. Disponível em: < http://laws.justice.gc.ca/en/P-8.6/>. Acesso em: 30 ago. 2009.

CANADA. ***Royal Canadian Mounted Police External Review Committee Security and Confidentiality Regulations,* 1988**. Ottawa, 1988. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cr/SOR-88-397>. Acesso em: 30 ago. 2009.

CANADA. ***Access to Information Act,* 1985**. Ottawa, 1985*k*. Disponível em: <http://laws.justice.gc.ca/en/A-1/index.html>. Acesso em: 30 ago. 2009.

CANADA. ***Canada Evidence Act,* 1985**. Ottawa, 1985*l*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cs/C-23>. Acesso em: 30 ago. 2009.

CANADA. ***Canadian Security Intelligence Service Act,* 1985**. Ottawa, 1985*m*. Disponível em: <http://laws.justice.gc.ca/en/showtdm/cs/C-23>. Acesso em: 30 ago. 2009.

CANADA. ***Criminal Code,* 1985**. Ottawa, 1985*n*. Disponível em: <http://laws.justice.gc.ca/en/C-46/>. Acesso em: 30 ago. 2009.

CANADA. ***National Defence Act,* 1985**. Ottawa, 1985*o*. Disponível em: <http://laws.justice.gc.ca/en/N-5/index.html>. Acesso em: 30 ago. 2009.

CANADA. ***Privacy Act,* 1985**. Ottawa, 1985*p*. Disponível em: <http://laws.justice.gc.ca/en/P-21/index.html>. Acesso em: 30 ago. 2009.

CANADA. ***Security of Information Act,* 1985**. Ottawa, 1985*q*. Disponível em: <http://laws.justice.gc.ca/en/O-5/>. Acesso em: 30 ago. 2009.

CANADA. ***Income Tax Act,* 1985**. Ottawa, 1985*r*. Disponível em: <http://laws.justice.gc.ca/en/>. Acesso em: 30 ago. 2009.

CANADA. ***Consolidation of Constitution Acts,* 1867 *to* 1982**. Ottawa, 1982. Disponível em: <http://laws.justice.gc.ca/en/Const/index.html>. Acesso em: 30 ago. 2009.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 16.ed. Rio de Janeiro: Lumen Juris, 2006

CASTELLS, Manuel. **A Sociedade em Rede**. Vol.1 . 7.ed. Revista e Ampliada. Tradução: Roneide Venancio Majer. Colaboração de Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 2003.

CEPIK. Marco Aurélio Chaves. **Serviços de Inteligência**: Agilidade e Transparência como Dilemas de Institucionalização. 2001. 310 f. Tese de Doutorado em Ciência Política - Instituto Universitário de Pesquisas do Rio de Janeiro, IUPERJ-Tec, Rio de Janeiro, Brasil. 2001.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Home.** Disponível em: < http://www.cert.br/>. Acesso em: 30 jun. 2009.

CERT Incident Note. ***Social Engineering Attacks via IRC and Instant Messaging***. *March 19*, 2002. Disponível em: <http://www.cert.org/incident_notes/IN-2002-03.html>. Acesso em: 28 mai. 2009.

CHAHIN, Ali *et al*. **e-Gov.br**: a próxima revolução brasileira. São Paulo: Prentice Hall, 2004.

CHOO, Chun Wei. **A organização do conhecimento.** Como as organizações usam a informação para criar significado, construir e tomar decisões. São Paulo: Senac, 2003.

CICCO, Francesco. **A Gestão de Riscos no Século XXI.** QSP - Centro de Qualidade, Segurança e Produtividade. Edição 01/2003. Disponível em: <http://www.qsp.org.br/risk_ management.shtml>. Acessado em: 06 mai. 2009.

CLAD. **Carta Iberoamericana de Gobierno Electrónico**. Aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado. Pucón, Chile, 31 de mayo y 1° de junio de 2007. Concepto de Gobierno Electrónico. 2007.

CONSULADO. Geral do Canadá. Governo do Canadá. Canadá – Brasil. Relações Bilaterais. **Relações Canadá-Brasil**. São Paulo. Atualizado em abril de 2009. Disponível em: <http://www.canadainternational.gc.ca/brazil-bresil/bilateral_relations_bilaterales/index.aspx ?lang=por&menu_id=46&menu=L>. Acesso em 10 jun 2009.

CONSULADO. Geral do Canadá. Governo do Canadá. Descubra o Canadá. Sobre o Canadá. **Canadá**. São Paulo. Atualizado em março de 2008*a*. Disponível em: <http://www.canadainternational.gc.ca/brazil-bresil/about_a-propos/overview-apercu.aspx?lang=por>. Acesso em 10 jun 2009.

CONSULADO. Geral do Canadá. Governo do Canadá. Descubra o Canadá. Sobre o Canadá. **O Governo**. São Paulo. Atualizado em dezembro de 2008*b*. Disponível em: <http://www.canadainternational.gc.ca/brazil-bresil/about_a-propos/organization-organisation.aspx?lang=por>. Acesso em 10 jun 2009.

CONSULADO. Geral do Canadá. Governo do Canadá. Descubra o Canadá. Sobre o Canadá. **O Sistema Jurídico**. São Paulo. Atualizado em dezembro de 2008*c*. Disponível em: <http://www.canadainternational.gc.ca/brazil-bresil/about_a-propos/law-loi.aspx?lang=por>. Acesso em 10 jun 2009.

COSTABILE, Henrique. Presidente do Serviço Federal de Processamento de Dados (Serpro). Segurança em casa e na rede. **Correio Braziliense**, Opinião, 07 de junho de 2004.

CSEC. *Communications Security Establishment Canada*. ***IT Security Program.*** Modificado em dezembro de 2008. Disponível em: <http://www.cse-cst.gc.ca/its-sti/index-eng.html>. Acesso em: 15 mar. 2009.

DAVENPORT, Thomas H. **Ecologia da informação:** porque só a tecnologia não basta para o sucesso na era da informação. 6. ed. São Paulo: Futura, 1998.

DFAIT. *Department of Foreign Affairs and International Trade Canada*. (Ministério de Relações Exteriores e Comércio Internacional do Canadá). *Foreign Policy. Policy Agenda. Rule of Law and Accountability.* ***Security System Reform and Rule of Law***. Atualizado em novembro de 2008. Disponível em: <http://www.dfait-maeci.gc.ca/glynberry/reform-reforme.aspx?lang=eng>. Acesso em: 10 jun. 2009.

DFAIT. *Department of Foreign Affairs and International Trade Canada*. ***Backgrounder. Canada's Actions Against Terrorism Since September 11***. Atualizado em fevereiro de 2003. Disponível em: <http://www.dfait-maeci.gc.ca/anti-terrorism/canadaactions-en.asp>. Acesso em: 10 jun. 2009.

DSP. *Depository Services Program.* ***How a Government Bill becomes Law*** *– Canada*. Atualizado em fevereiro de 2007. Disponível em: <http://dsp-psd.pwgsc.gc.ca/Reference/queens-e.html>. Acesso em: 12 jun. 2009.

DTV. **O que é TV Digital?** Site Oficial da TV Digital Brasileira. Disponível em: <http://www.dtv.org.br/materias.asp?id=83&menuid=3>. Acesso em: 01 abr. 2009.

EINSENBERG, José e CEPIK, Marco. (Org.). **Internet e Política**: Teoria e Prática da Democracia Eletrônica. Organizadores. Belo Horizonte: UFMG, 2002.

FERRAZ JÚNIOR, Tércio Sampaio. **Introdução ao Estudo do Direito**: técnica, decisão, dominação. 2.ed. São Paulo: Atlas, 1994.

FERRER, Florência; Santos, Paula (Org.). **e-Government: o governo eletrônico no Brasil.** São Paulo: Saraiva, 2004.

FUSCO. Camila. O big brother vem aí? **Portal Exame**. Revista Ed. Abril. 24 jul. 2008. Disponível em: <portalexame.abril.com....cnologia/m0164541.html>. Acesso em: 10 jun 2009.

GEDS. ***Government Electronic Directory Services.*** Modificado em fevereiro de 2009. Disponível em: <http://sage-geds.tpsgc-pwgsc.gc.ca/cgi-bin/direct500/eng/TE?FN=index.htm>. Acesso em: 15 mar. 2009.

GLYCERIO, Carolina. ONU adverte contra excesso de regulamentação da internet. **BBC Brasil**. 16 nov. 2006. Disponível em: <http://www.bbc.co.uk/portuguese/reporterbbc/story/2006/11/061116_unctadregulamentacaocg.shtml>. Acesso em: 10 mai. 2009.

GONÇALVES, Joanisval Brito. ***Sed quis custodiet ipso custodes***? O controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá. 2008. 837 f. Tese de Doutorado em Relações Internacionais - Universidade de Brasília, Brasília, 2008.

GOV.br. Governo Eletrônico Brasileiro. **Paulo Bernardo abre Fórum no Canadá que homenageia e-Gov Brasileiro**. Notícias e Eventos. Notícias. Publicado em 11 de outubro de 2007. Disponível em: <https://www.governoeletronico.gov.br/noticias-e-eventos/noticias/paulo-bernardo-abre-forum-no-canada-que-homenageia-e-gov-brasileiro/?searchterm=gtec>. Acesso em: 16 jun. 2009.

GOVERNMENT of Canada. ***Structure of the Government of Canada***. Atualizado em 30 junho de 2009. Disponível em: <http://www.canada.gc.ca/aboutgov-ausujetgouv/structure-eng.html>. Acesso em: 02 jul. 2009.

GOVERNO Eletrônico. **Histórico.** Disponível em <www.governoeletronico.e.gov.br/governoeletronico/index.html>. Acesso em: 10 nov. 2007.

HEINEN, Juliano. **Agências reguladoras e o seu "poder" de regular(mentar).** *Jus navegandi.* Janeiro de 2004. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=4821>. Acesso em: 30 jun. 2008.

IBGE. Análise dos resultados. **Acesso à Internet e posse de telefone móvel celular para uso pessoal 2005**. Março de 2007. Disponível em: <http://www.ibge.gov.br/home/estatistica/populacao/acessoainternet/comentarios.pdf>. Acesso em: 10 jun. 2009.

ICP-Brasil. **Política de Segurança da ICP-Brasil** - DOC-ICP-02 – V 3.0. Infra-Estrutura de Chaves Públicas Brasileira. 01 de dezembro de 2008.

IEC. ***International Electrotechnical Commission***. Disponível em: <http://www.iec.ch/>. Acesso em 19 mai. 2009.

IGA. *Intergovernmental Affairs. Privy Council Office. About Canada*. ***The Canadian Constitution***. Atualizado em agosto de 2007. Disponível em: <http://www.pco-bcp.gc.ca/aia/index.asp?lang=eng&page=canada&sub=constitution&doc=constitution-eng.htm>. Acesso em: 10 jun. 2009.

ISO. ***The ISO 17799 Community Portal***. Disponível em: <http://www.17799.com>. Acesso em: 30 ago. 2009.

ITH. *Internetworking Technology Handbook.* X.25 Overview. **Cisco Systems.** San Jose, Estados Unidos, 2009. Disponível em: <http://www.cisco.com/en/US/docs/internetworking/technology/handbook/X25.html>. Acesso em: 30 jun. 2009.

ITI. Instituto Nacional de Tecnologia da Informação. **Estrutura da ICP-Brasil**. Disponível em: < http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp>. Acesso em: 30 jun. 2009.

ITU. *Word Telecommunication Indicators.* ***International Telecommunication Union Regional Profile***. November 2003. Disponível em: <http://www.itu.int/net/home/index.aspx>. Acesso em: 24 jun. 2009.

KOCH, Walter W. **Gerenciamento Eletrônico de Documentos**: Conceitos, Tecnologias e Considerações Gerais. São Paulo: CENADEM, 1998.

LEMOS, Ronaldo. **Direito, Tecnologia e Cultura**. Rio de Janeiro: FDV, 2005.

LENK, K. ; Traunmuller, R. *Broadening the Concept of Electronic Government, In:* PRINS, J. E. J. (Ed.). **Designing E-Government**. [S. l.] : *Kluwer Law International*, 2001.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999. 264p.

LIVRO Verde. **Apresentação**. Brasília: MCT, 2000. Disponível em <http:/www.socinfo.org.br/livro verde/index.htm>. Acesso em: 01 abr. 2008.

LUBAN, David. *The Publicity Principle.* In. Robert E. Goodin, ed., ***The Theory of Institutional Design***, *Cambridge University Press*, 1996, pp. 154-198.

LUCCI, Elian. Alabi. **A era pós-industrial**: a sociedade do conhecimento e a educação para o pensar. Editora Saraiva, 2003. Disponível em: <http://www.hottopos.com/vidlib7/e2.htm>. Acesso em: 09 jun. 2008.

McGEE, James; PRUSAK, Laurence. **Gerenciamento estratégico da informação:** aumente a competividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. 12 ed. Rio de Janeiro: Campos, 1994.

MACHADO, Sulamita Crespo Carrilho. **Administração Pública e Direitos Humanos: considerações por uma revisão conceitual a propósito da experiência**. Texto para discussão nº 42. Escola de Governo da Fundação João Pinheiro (EG/FJP): Belo Horizonte, out/2007. Disponível em: <http://www.eg.fjp.mg.gov.br/publicacoes/ material/textos/427. pdf>. Acesso em: 05 jun. 2009.

MANDEL, Arnaldo; SIMON, Imre; e LYRA, Jorge L. de. Informação: Computação e Comunicação. 16 de Julho de 1997. Documento encomendado pela Academia Brasileira de Ciências. **IME - Instituto de Matemática e Estatística.** Departamento da Ciência da Computação. Universidade de São Paulo. São Paulo, SP, Brasil. Disponível em: <http://www.ime.usp.br/~is/abc/abc/abc.html>. Acesso em: 20 abr. 2007.

MCT. Ministério da Ciência e Tecnologia. Legislação. **Decreto.** Disponível em <http:/www.mct.gov.br/legis/decreto>. Acesso em: 25 nov. 2002.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 16.ed. São Paulo: Malheiros, 2003.

MENDES, Gilmar Ferreira e FORSTER JR., Nestor José. **Manual de redação da Presidência da República**. 2. ed. rev. e atual. – Brasília: Presidência da República, 2002.

MONTEIRO, Jorge Vianna. Escolhas públicas no Brasil. **Revista de Administração. Pública**, vol.41. Rio de Janeiro, 2007.

MORAES, André Figueiredo. **O impacto econômico, a desburocratização e a transparência nas compras governamentais com a implantação do *egovernment***. 2006. Dissertação de Mestrado em Administração e Desenvolvimento Empresarial, Universidade Estácio de Sá, Rio de Janeiro, Rio de Janeiro, 2006.

MOREIRA, Kamila Araújo Rôla Fontes. **Publicização e efetivação das consultas públicas do governo eletrônico**. Assembléia Legislativa do Estado de Minas Gerais. Escola do Legislativo. Banco do Conhecimento. Belo Horizonte, 2006. Disponível em: <http://www.almg.gov.br/index.asp?grupo=escola_legislativo&diretorio=bancoconhecimento &arquivo=banco_conhecimento>. Acesso em: 30 jun. 2009.

MORIMOTO, Carlos E. **Redes e TCP/IP**. Tutorias. 13 out. 2006. Disponível em: < http:// www.guiadohardware.net/tutoriais/tcp-ip/>. Acesso em: 30 mai. 2008.

MPOG. Ministério do Planejamento, Orçamento e Gestão. Oficinas de Planejamento Estratégico. **Relatório consolidado do Comitê Executivo do Governo Eletrônico, 2004**. Brasília, 2004. Disponível em: < http://www. acessobrasil. org. br http://www. acessobrasil. org. br.> Acesso em: 15 ago. 2008.

MUNDET, José Ramón Cruz. **Manual de *archivística*** . 3. ed. Madrid : *Fundación Germán Sánches Ruipérez,* 1994.

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

PINHEIRO, Patrícia Peck. Comunicadores instantâneos e e-mail pessoal não estão livres da vigilância. **UOL Tecnologias**. 07 abr. 2008. Disponível em: <http://tecnologia.uol.com.br/ dicas/ultnot/2008/04/07/ult2665u275.jhtm>. Acesso em: 10 jun. 2009.

PCO. *Privy Council Office. Information Resources.* ***The Swearing-In of Privy Councillors***. Atualizado em junho de 2009. Disponível em: <http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information>. Acesso em: 10 jun. 2009.

PORTAL do Governo Brasileiro. República Federativa do Brasil. **O País**. Disponível em: <http://www.brasil.gov.br/pais/>. Acesso em: 10 jun. 2009.

REALE, Miguel. **Lições Preliminares de Direito**. 25. ed. São Paulo: Saraiva, 2001.

REINO UNIDO. **BS 7799**. Trata da gestão da segurança da informação. Londres, 1995. Disponível em: <http://www.thewindow.to/bs7799/>. Acesso em: 30 ago. 2009.

REINO UNIDO. **ITIL**. *Infrastructure Technology Information Library*. Registra as melhores práticas na área de gestão de serviços de tecnologia da informação. Londres, 1980. Disponível em: < http://www.itil-officialsite.com/home/home.asp>. Acesso em: 30 ago. 2009.

RILEY, Thomas. ***Successful eGovernment in Canada***. Disponível em: <www.egovmonitor.com/node/709>. Acesso em: 15 out. 2007.

SAUVÉ, Jacques. **O que é um *Framework*?** DSC – Departamento de Sistemas e Computação, do Centro de Engenharia Elétrica e Informática – CEEI, da Universidade

Federal de Campina Grande. Disponível em: <http://www.dsc.ufcg.edu.br/~jacques/cursos/map/html/frame/oque.htm>. Acesso em: 10 abr. 2009.

SERPRO. **Crimes em TI: Governo Federal sofre 2.100 tentativas de invasão/dia**. Convergência Digital, Ana Paula Lobo, 22 de setembro de 2008. Disponível em: <http://www.serpro.gov.br/serpronamidia/2008/setembro/crimes-em-ti-governo-federal-sofre-2-100-tentativas-de-invasao-dia/?searchterm=segurança da informação>. Acesso em: 10 abr. 2009.

SERPRO. **Segurança do Serpro tem reconhecimento internacional**. Coordenação de Comunicação Empresarial do Serpro, Luciana Azevêdo, 13 de março de 2006*a*. Disponível em: <http://www.serpro.gov.br/noticias-antigas/noticias-2006/20060313_01/?searchterm=segurança da informação>. Acesso em: 10 abr. 2009.

SERPRO. Invasão de Privacidade. **Revista Tema**. Ano XXX - Edição 187 Setembro/Outubro 2006*b*. Disponível em: <http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_187/materias/invasao-de-privacidade/?searchterm=segurançada informação>. Acesso em: 10 abr. 2009.

SERPRO. **Desvendando a certificação digital**. 07 de julho de 2004. Disponível em: <http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040707_01/?searchterm=segurançadainformação>. Acesso em: 10 abr. 2009.

SIP. Sociedade Interamericana de Imprensa – *Inter American Press Association*. Canadá. Relatórios País-por-País. Reunião de Meio de Ano da SIP. **Casa de Campo República Dominicana**. 18 de março de 2002. Disponível em: <http://www.sipiapa.org/portugues/pulications/li-canada-port.cfm>. Acesso em: 10 jun. 2009.

SOCIEDADE da Informação. Sobre a Socinfo. **Histórico.** Brasília, 2004. Disponível em: <http://www.socinfo.org.br/sobre/historico.htm>. Acesso em: 31 out. 2008.

SOFTEXPERT Excellence Suite. **AS/NZS 4360**. Disponível em: <http://www.softexpert.com.br/norma-asnzs.php>. Acesso em: 11 mai. 2009.

SOFTWARELivre.Org. **O Senado e o *Software Livre*.** Editoria: Governos. 05/Sep/2003. Disponível em: <http://www.softwarelivre.org/news/1259>. Acesso em: 19 mar. 2009.

SPACEBlog. Tecnologia e Informática. **O surgimento do computador**. Quinta 31 maio 2007. Disponível em: <http://netica.spaceblog.com.br/24872/O-surgimento-do-computador/>. Acesso em: 19 mar. 2009.

STATCAN. *Statistic Canada*. ***Information and communications technology***. *Discover CYB. CYB Overview* 2008. Atualizado em janeiro de 2009. Disponível em: <http://www41.statcan.gc.ca/2008/2256/ceb2256_000-eng.htm>. Acesso em: 10 jun. 2009.

SWITZERLAND. **ISO/IEC 27005:2008**, norma técnica específica de gestão de riscos em segurança da informação. Geneva, 2008. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107>. Acesso em: 10 jun. 2009.

SWITZERLAND. **ISO 27001:2006**, parte 2 do padrão BS 7799. Geneva, 2006. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber= 42103>. Acesso em: 10 jun. 2009.

SWITZERLAND. **ISO 27002:2005**, parte 1 do padrão BS 7799. Geneva, 2005. Disponível em: < http://www.iso.org/iso/catalogue_detail?csnumber=50297>. Acesso em: 10 jun. 2009.

SWITZERLAND. **ISO/IEC *Guide 73***, *Risk Management: Vocabulary - Guidelines for use in standards*. Geneva, 2002. Disponível em: <http://www.iso.org/iso/catalogue_detail.htm?csnumber=34998>. Acesso em: 10 jun. 2009.

TALLAFIGO, Manuel Romero. ***Archivística y archivos*** : *soportes, edificio y organización.* Carmona : SeC, 1994.

TICOLL, David e TAPSCOTT, Don. **A empresa transparente**. São Paulo, Makron Books: 2004.

TURBAN, Efraim *et al*. **Introdução a Sistemas de Informação**. Tradução Daniel Vieira. Rio de Janeiro: Elsevier, 2007.

UFSCAR. **Universidade Federal de São Carlos**. (F.A.Q.) Ajuda Rápida SOS Informática. Suporte ao Usuário. Disponível em: < http://www.ufscar.br/~suporte/faq00.php >. Acesso em: 31 mar. 2009.

VANCOUVER *English Centre*. **Governo do Canadá**. Disponível em: <http://www.vec.ca/portuguese/2/canada_governo.cfm>. Acesso em 10 jun 2009.

VIOLA JUNIOR, Waldyr. *Hacker*, nos dias de hoje. Serpro. **Revista Tema**. Ano XXIX - Edição 179 maio/junho 2005.

WILSON, Thomas Daniel. (1989) - *Towards an information management curriculum*. ***Journal of Information Science***. vol. 15, nº 4/5, p. 203 - 209.

Verba volant, scripta manent
(As palavras voam e as escritas permanecem)

APÊNDICE A – Normas Relacionadas à Segurança da Informação: Brasil

Constituição Federal de 1988

Constituição Federal	Ementa	Origem	Artigos	Aspecto da Segurança Informação
Constituição da República Federativa do Brasil de 1988	Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fratema, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.	Poder Constituinte	Art. 5 X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;	Direito à privacidade. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
			Art. 5 XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;	Direito à privacidade das comunicações. Sigilo dos dados telemáticos e das comunicações privadas.
			Art. 5 XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;	Resguardo do sigilo profissional em caso de ofício que exige a ampla confidência no interesse de quem confidencia, como advogados, padres, médicos, psicólogos, etc. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém
			Art. 5 XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; Art. 37. § 3º - A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;	Direito à informação e ao acesso aos registros públicos. Disponibilidade das informações constantes nos órgãos públicos.
			Art. 5 XXXIV - são a todos assegurados, independentemente do pagamento de taxas: a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal;	Direito de petição e de obtenção de certidões em repartições públicas. Disponibilidade das informações constantes nos órgãos públicos
			Art. 23. É competência comum da União, dos Estados, do Distrito Federal e dos Municípios: III - proteger os documentos, as obras e outros bens de valor histórico, artístico e cultural, os monumentos, as paisagens naturais notáveis e os sítios arqueológicos; IV - impedir a evasão, a destruição e a descaracterização de obras de arte e de outros bens de valor histórico, artístico ou cultural;	Dever do Estado de proteger os documentos e obras. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
			Art. 37.*caput* - A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:	Vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
			Art. 37. § 6º - As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa. Código Civil, Art. 43. As pessoas jurídicas de direito público interno são civilmente responsáveis por atos dos seus agentes que nessa qualidade causem danos a terceiros, ressalvado direito regressivo contra os causadores do dano, se houver, por parte destes, culpa ou dolo.	Responsabilidade objetiva do Estado e das pessoas de direito privado prestadoras de serviços públicos pelos danos causados a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa, decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
			Art. 37. § 7º A lei disporá sobre os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o acesso a informações privilegiadas.	Necessidade de regulamentação do acesso a informações privilegiadas.
			Art. 93. Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios: IX todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;	Princípio da publicidade dos atos públicos. Direito à privacidade quando o sigilo das informações relacionadas à intimidade ou à vida privada de alguém sigilo não prejudique o interesse público à informação.
			Art. 181. O atendimento de requisição de documento ou informação de natureza comercial, feita por autoridade administrativa ou judiciária estrangeira, a pessoa física ou jurídica residente ou domiciliada no País dependerá de autorização do Poder competente.	Autorização do Poder competente para obter informações de natureza comercial.
			Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem: § 2º - Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.	Obrigação da Administração Pública de promover a gestão documental. Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Códigos

Códigos	Origem	Artigos	Aspecto da Segurança Informação
Código de Conduta da Alta Administração, Aprovado em 22 de agosto de 2000	Poder Executivo	Art. 5o As alterações relevantes no patrimônio da autoridade pública deverão ser imediatamente comunicadas à Comissão de Ética Pública - CEP, especialmente quando se tratar de: § 4o A fim de preservar o caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública, as comunicações e consultas, após serem conferidas e respondidas, serão acondicionadas em envelope lacrado, que somente poderá ser aberto por determinação da Comissão.	Caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública. Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).
Código de Conduta da Alta Administração, Aprovado em 22 de agosto de 2000	Poder Executivo	Art. 14. Após deixar o cargo, a autoridade pública não poderá: II - prestar consultoria a pessoa física ou jurídica, inclusive sindicato ou associação de classe, valendo-se de informações não divulgadas publicamente a respeito de programas ou políticas do órgão ou da entidade da Administração Pública Federal a que esteve vinculado ou com que tenha tido relacionamento direto e relevante nos seis meses anteriores ao término do exercício de função pública	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Código de Propriedade Industrial Lei nº 9.279, de 14 de maio de 1996.	Poder Legislativo	Art. 75. O pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso e não estará sujeito às publicações previstas nesta Lei.	Sigilo das patentes de interesse da defesa nacional.
Código de Ética do Servidor Público Decreto nº 1.171, de 22 de junho de 1994	Poder Executivo	Seção I, VII - Salvo os casos de segurança nacional, investigações policiais ou interesse superior do Estado e da Administração Pública, a serem preservados em processo previamente declarado sigiloso, nos termos da lei, a publicidade de qualquer ato administrativo constitui requisito de eficácia e moralidade, ensejando sua omissão comprometimento ético contra o bem comum, imputável a quem a negar. X - Deixar o servidor público qualquer pessoa à espera de solução que compete ao setor em que exerça suas funções, permitindo a formação de longas filas, ou qualquer outra espécie de atraso na prestação do serviço, não caracteriza apenas atitude contra a ética ou ato de desumanidade, mas principalmente grave dano moral aos usuários dos serviços públicos.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Código de Ética do Servidor Público Decreto nº 1.171, de 22 de junho de 1994	Poder Executivo	Seção I, IX - Da mesma forma, causar dano a qualquer bem pertencente ao patrimônio público, deteriorando-o, por descuido ou má vontade, não constitui apenas uma ofensa ao equipamento e às instalações ou ao Estado, mas a todos os homens de boa vontade que dedicaram sua inteligência, seu tempo, suas esperanças e seus esforços para construí-los. Seção III, XV - E vedado ao servidor público; h) alterar ou deturpar o teor de documentos que deva encaminhar para providências; l) retirar da repartição pública, sem estar legalmente autorizado, qualquer documento, livro ou bem pertencente ao patrimônio público;	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações. Proteção da integridade das informações públicas. Proteção da disponibilidade das informações públicas.
Código de Defesa do Consumidor Lei nº 8.078, de 11 de setembro de 1990.	Poder Legislativo	Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.
Código de Processo Civil Lei no 5.869, de 11 de janeiro de 1973.	Poder Legislativo	Art. 347. A parte não é obrigada a depor de fatos: II - a cujo respeito, por estado ou profissão, deva guardar sigilo. c/c Art. 363. A parte e o terceiro se escusam de exibir, em juízo, o documento ou a coisa: IV - se a exibição acarretar a divulgação de fatos, a cujo respeito, por estado ou profissão, devam guardar segredo;	Direito da parte de guardar sigilo profissional. Proteção da privacidade de seus clientes.
Código de Processo Civil Lei no 5.869, de 11 de janeiro de 1973.	Poder Legislativo	Art. 406. A testemunha não é obrigada a depor de fatos: II - a cujo respeito, por estado ou profissão, deva guardar sigilo. c/c Art. 414. Antes de depor, a testemunha será qualificada, declarando o nome por inteiro, a profissão, a residência e o estado civil, bem como se tem relações de parentesco com a parte, ou interesse no objeto do processo. § 2o A testemunha pode requerer ao juiz que a escuse de depor, alegando os motivos de que trata o art. 406; ouvidas as partes, o juiz decidirá de plano.	Direito da testemunha de guardar sigilo profissional. Proteção da privacidade de seus clientes.
Código Tributário Nacional Lei nº 5.172, de 25 de outubro de 1966.	Poder Legislativo	Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades. § 1o Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes: I – requisição de autoridade judiciária no interesse da justiça; II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa. § 2o O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo. § 3o Não é vedada a divulgação de informações relativas a: I – representações fiscais para fins penais; II – inscrições na Dívida Ativa da Fazenda Pública; III – parcelamento ou moratória. (art 198, §§ 1°, 2° e 3° - Incluídos pela Lcp nº 104, de 10.1.2001)	Proteção do sigilo fiscal.
Consolidação das Leis do Trabalho – CLT Decreto-Lei n.º 5.452, de 1º de maio de 1943	Poder Executivo	Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador: g) violação de segredo da empresa;	Rescisão de contrato de trabalho de empregado que viola segredo da empresa. Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
Código de Processo Penal. Decreto-lei nº 3.689, de 3 de outubro de 1941.	Poder Executivo	Art.20. A autoridade assegurará no inquérito o sigilo necessário à elucidação do fato ou exigido pelo interesse da sociedade.	Proteção de informações sigilosas.
Código de Processo Penal. Decreto-lei nº 3.689, de 3 de outubro de 1941.	Poder Executivo	Art. 207. São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho.	Proteção do sigilo profissional.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Códigos	Origem	Artigos	Aspecto da Segurança Informação
Código Penal. Decreto-lei no 2.848, de 7 de dezembro de 1940.	Poder Executivo	Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: § 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 9.983, de 2000).	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
Código Penal. Decreto-lei no 2.848, de 7 de dezembro de 1940.	Poder Executivo	Art. 184. Violar direitos de autor e os que lhe são conexos: § 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 10.695, de 1º.7.2003)	Proteção da autenticidade.
Código Penal. Decreto-lei no 2.848, de 7 de dezembro de 1940.	Poder Executivo	Art. 297 - Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro: Pena - reclusão, de dois a seis anos, e multa. § 1º - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aumenta-se a pena de sexta parte.. § 3o Nas mesmas penas incorre quem insere ou faz inserir: (Incluído pela Lei nº 9.983, de 2000) I - na folha de pagamento ou em documento de informações que seja destinado a fazer prova perante a previdência social, pessoa que não possua a qualidade de segurado obrigatório; II - na Carteira de Trabalho e Previdência Social do empregado ou em documento que deva produzir efeito perante a previdência social, declaração falsa ou diversa da que deveria ter sido escrita; III - em documento contábil ou em qualquer outro documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado. § 4o Nas mesmas penas incorre quem omite, nos documentos mencionados no § 3o, nome do segurado e seus dados pessoais, a remuneração, a vigência do contrato de trabalho ou de prestação de serviços. (§3°, I, II,II; § 4° - incluídos pela Lei nº 9.983, de 2000)	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal. Decreto-lei no 2.848, de 7 de dezembro de 1940.	Poder Executivo	Art. 305 - Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor: Pena - reclusão, de dois a seis anos, e multa, se o documento é público, e reclusão, de um a cinco anos, e multa, se o documento é particular. Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000). Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (Incluído pela Lei nº 9.983, de 2000). Art. 314 - Extraviar livro oficial ou qualquer documento, de que tem a guarda em razão do cargo; sonegá-lo ou inutilizá-lo, total ou parcialmente: Pena - reclusão, de um a quatro anos, se o fato não constitui crime mais grave.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal. Decreto-lei no 2.848, de 7 de dezembro de 1940.	Poder Executivo	Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1o Nas mesmas penas deste artigo incorre quem: I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II - se utiliza, indevidamente, do acesso restrito. § 2o Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa. (§ 1°, I, II; § 2° - incluídos pela Lei nº 9.983, de 2000).	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Leis

Leis	Ementa	Origem	Artigos Segurança Informação
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.	Poder Legislativo	Determina a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios.
Lei Complementar 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências	Poder Legislativo	Art. 1o As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. § 4o A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes: I – de terrorismo;
Lei Complementar nº 101, de 4 de maio de 2000.	Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal	Poder Legislativo	Art. 1o Esta Lei Complementar estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal, com amparo no Capítulo II do Título VI da Constituição.
Lei Complementar nº 75, de 20 de maio de 1993	Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União.	Poder Legislativo	Art. 8º Para o exercício de suas atribuições, o Ministério Público da União poderá, nos procedimentos de sua competência: II - requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta; VIII - ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública; § 1º O membro do Ministério Público será civil e criminalmente responsável pelo uso indevido das informações e documentos que requisitar; a ação penal, na hipótese, poderá ser proposta também pelo ofendido, subsidiariamente, na forma da lei processual penal. § 2º Nenhuma autoridade poderá opor ao Ministério Público, sob qualquer pretexto, a exceção de sigilo, sem prejuízo da subsistência do caráter sigiloso da informação, do registro, do dado ou do documento que lhe seja fornecido.
Lei nº 11.900, de 08/01/2009	Altera dispositivos do Decreto-Lei nº 3.689, de 03/10/1941 - Código de Processo Penal, para prever a possibilidade de realização de interrogatório e outros atos processuais por sistema de videoconferência.	Poder Legislativo	Art. 1º Os arts. 185 e 222 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, passam a vigorar com as seguintes alterações: Art. 2º O Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, passa a vigorar acrescido do seguinte art. 222-A:
Lei nº 11.829, de 25/11/2008	Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.	Poder Legislativo	Art. 1º Os arts. 240 e 241 da Lei no 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação: Art. 2º A Lei nº 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:
Lei nº 11.776, de 17 de Setembro de 2008	Dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN, cria as Carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência e Agente Técnico de Inteligência e dá outras providências; e revoga dispositivos das Leis nºs 9.651, 1998, 11.233, 2005, e 11.292, 2006, e as Leis nºs 10.862, 2004, e 11.362, 2006.	Poder Legislativo	Art. 8º São atribuições do cargo de Oficial de Inteligência: d) atividades de pesquisa e desenvolvimento científico ou tecnológico direcionadas à obtenção e à análise de dados e à segurança da informação>>; Art. 11. São atribuições do cargo de Oficial Técnico de Inteligência: d) atividades de pesquisa e desenvolvimento científico ou tecnológico, direcionadas à obtenção e análise de dados e à segurança da informação;

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Leis	Ementa	Origem	Artigos Segurança Informação
Lei nº 11.767, de 07 de agosto de 2008	Altera o art. 7º da Lei nº 8.906, de 04/07/1994, para dispor sobre o direito à inviolabilidade do local e instrumentos de trabalho do advogado, bem como de sua correspondência.	Poder Legislativo	Art. 1º O art. 7o da Lei no 8.906, de 4 de julho de 1994, passa a vigorar com a seguinte redação: II – a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia; § 6o Presentes indícios de autoria e materialidade da prática de crime por parte de advogado, a autoridade judiciária competente poderá decretar a quebra da inviolabilidade de que trata o inciso II do caput deste artigo, em decisão motivada, expedindo mandado de busca e apreensão, específico e pormenorizado, a ser cumprido na presença de representante da OAB, sendo, em qualquer hipótese, vedada a utilização dos documentos, das mídias e dos objetos pertencentes a clientes do advogado averiguado, bem como dos demais instrumentos de trabalho que contenham informações sobre clientes.
Lei nº 11.754, de 23 de Julho de 2008	Acresce, altera e revoga dispositivos da Lei nº 10.683, de 28 de maio de 2003, cria a Secretaria de Assuntos Estratégicos da Presidência da República, cria cargos em comissão; revoga dispositivos das Leis nºs 10.869, de 13 de maio de 2004, e 11.204, de 5 de dezembro de 2005; e dá outras providências.	Poder Legislativo	Art. 1º A Lei nº 10.683, de 28 de maio de 2003, passa a vigorar com as seguintes alterações: "Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação (...)".
Lei nº 11.484, de 31/05/2007	Dispõe sobre os incentivos às indústrias de equipamentos para TV Digital e de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual das topografias de circuitos integrados; altera a Lei nº 8.666, de 21/06/1993.	Poder Legislativo	Art. 1º Fica instituído o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores – PADIS, nos termos e condições estabelecidos por esta Lei.
Lei nº 11.419, de 19/12/2006	Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11/01/1973 – Código de Processo Civil	Poder Legislativo	Art. 1 O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.
Lei nº 11.344, de 08 de Setembro de 2006	Dispõe sobre a reestruturação das carreiras de Especialista do Banco Central do Brasil; e dá outras providências.	Poder Legislativo	Art. 1º A Lei nº 9.650, de 27 de maio de 1998, passa a vigorar com a seguinte redação: "Art. 3º São atribuições dos titulares do cargo de Analista do Banco Central do Brasil: XI - desenvolvimento de atividades na área de tecnologia e segurança da informação>> voltadas ao desenvolvimento, à prospecção, à avaliação e à internalização de novas tecnologias e metodologias; "Art. 5º São atribuições dos titulares do cargo de Técnico do Banco Central do Brasil: III - execução de atividades de suporte e apoio técnico necessárias ao cumprimento das competências do Banco Central do Brasil que, por envolverem sigilo e segurança do Sistema Financeiro, não possam ser terceirizadas, em particular as pertinentes às áreas de: a)tecnologia e segurança da informação voltadas ao desenvolvimento, à prospecção, à avaliação e à internalização de novas tecnologias e metodologias;
Lei nº 11.341, de 07/08/2006	Altera o parágrafo único do art. 541 do Código de Processo Civil - Lei no 5.869, de 11/01/1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial.	Poder Legislativo	Art. 1° O parágrafo único do art. 541 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, passa a vigorar com a seguinte redação: "Art. 541. ..... Parágrafo único. Quando o recurso fundar-se em dissídio jurisprudencial, o recorrente fará a prova da divergência mediante certidão, cópia autenticada ou pela citação do repositório de jurisprudência, oficial ou credenciado, inclusive em mídia eletrônica, em que tiver sido publicada a decisão divergente, ou ainda pela reprodução de julgado disponível na Internet, com indicação da respectiva fonte, mencionando, em qualquer caso, as circunstâncias que identifiquem ou assemelhem os casos confrontados." (NR)
Lei nº 11.280, de 16/02/2006	Altera os arts. 112, 114, 154, 219, 253, 305, 322, 338, 489 e 555 da Lei nº 5.869, de 11/01/1973 - Código de Processo Civil, relativos à incompetência relativa, meios eletrônicos, prescrição, distribuição por dependência, exceção de incompetência, revelia, carta precatória e rogatória, ação rescisória e vista dos autos; e revoga o art. 194 da Lei nº 10.406, de 10/01/2002 - Código Civil.	Poder Legislativo	Art. 1° Os arts. 112 e 114 da Lei no 5.869, de 11 de janeiro de 1973, Código de Processo Civil, passam a vigorar com a seguinte redação: "Art. 112. .Parágrafo único. A nulidade da cláusula de eleição de foro, em contrato de adesão, pode ser declarada de ofício pelo juiz, que declinará de competência para o juízo de domicílio do réu." (NR) "Art. 114. Prorrogar-se-á a competência se dela o juiz não declinar na forma do parágrafo único do art. 112 desta Lei ou o réu não opuser exceção declinatória nos casos e prazos legais." (NR)
Lei nº 11.111, de 05/05/2005	Regulamenta a parte final do disposto no inciso XXXIII do caput do art. 5º da Constituição Federal (direito à informação e ao acesso aos registros públicos).	Poder Legislativo	Art. 2° O acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral será ressalvado exclusivamente nas hipóteses em que o sigilo seja ou permaneça imprescindível à segurança da sociedade e do Estado, nos termos do disposto na parte final do inciso XXXIII do caput do art. 5o da Constituição Federal. Art. 3º Os documentos públicos que contenham informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado poderão ser classificados no mais alto grau de sigilo, conforme regulamento.
Lei nº 10.973, de 02 de dezembro de 2004.	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.	Poder Legislativo	Art. 1° Esta Lei estabelece medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação e ao alcance da autonomia tecnológica e ao desenvolvimento industrial do País, nos termos dos arts. 218 e 219 da Constituição.
Lei nº 10.869, de 13 de Maio de 2004	Altera a Lei nº 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.	Poder Legislativo	Art. 1º A Lei nº 10.683, de 28 de maio de 2003, passa a vigorar com as seguintes alterações: "Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação (...)".
Lei nº 10.862, de 20 de Abril de 2004	Dispõe sobre a criação do Plano Especial de Cargos da Agência Brasileira de Inteligência - ABIN e dá outras providências.	Poder Legislativo	Art. 29. São atribuições do Cargo de Analista de Informações: I - planejar, executar, coordenar, supervisionar e controlar: d)as atividades de pesquisa e desenvolvimento científico ou tecnológico, direcionadas à obtenção e análise de dados e à segurança da informação;
Lei nº 10.740, de 01/10/2003	Altera a Lei nº 9.504, de 30/09/1997, e a Lei nº 10.408, de 10/01/2002, para implantar o registro digital do voto.	Poder Legislativo	Art. 1o Os arts. 59 e 66 da Lei no 9.504, de 30 de setembro de 1997, com as alterações introduzidas pela Lei no 10.408, de 10 de janeiro de 2002, passam a vigorar com a seguinte redação: "Art. 59 ---§ 4o A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor. § 5o Caberá à Justiça Eleitoral definir a chave de segurança e a identificação da urna eletrônica de que trata o § 4o. § 6o Ao final da eleição, a urna eletrônica procederá à assinatura digital do arquivo de votos, com aplicação do registro de horário e do arquivo do boletim de urna, de maneira a impedir a substituição de votos e a alteração dos registros dos termos de início e término da votação.
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.	Poder Legislativo	Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação, (...).
Lei no 10.408, de 10 de janeiro de 2002.	Altera a Lei nº 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, para ampliar a segurança e a fiscalização do voto eletrônico.	Poder Legislativo	Art. 59 § 4o A urna eletrônica disporá de mecanismo que permita a impressão do voto, sua conferência visual e depósito automático, sem contato manual, em local previamente lacrado, após conferência pelo eleitor.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Leis	Ementa	Origem	Artigos Segurança Informação
Lei nº 10.176, de 11 de Janeiro de 2001	Altera a Lei nº 8.248, de 23 de outubro de 1991, a Lei nº 8.387, de 30 de dezembro de 1991, e o Decreto-Lei nº 288, de 28 de fevereiro de 1967, dispondo sobre a capacitação e competitividade do setor de tecnologia da informação.	Poder Legislativo	Art. 2º O art. 11 da Lei n° 8.248, de 23 de outubro de 1991, passa a vigorar com a seguinte redação: "Art. 11. Para fazer jus aos benefícios previstos no art. 4° desta Lei, as empresas de desenvolvimento ou produção de bens e serviços de informática e automação deverão investir, anualmente, em atividades de pesquisa e de desenvolvimento em tecnologia da informação a serem realizadas no País, no mínimo cinco por cento de seu faturamento bruto no mercado interno, decorrente da comercialização de bens e serviços de informática, deduzidos os tributos correspondentes a tais comercializações, bem como o valor das aquisições de produtos incentivados na forma desta Lei, conforme projeto elaborado pelas próprias empresas, a partir da apresentação da proposta de projeto de que trata o § 1° C do art. 4°. § 2º Os recursos de que trata o inciso III do § 1º destinam-se, exclusivamente, à promoção de projetos estratégicos de pesquisa e desenvolvimento em tecnologia da informação, inclusive em segurança da informação.
Lei nº 9755, de 16 de dezembro de 1998	Dispõe sobre a criação de "homepage" na "Internet", pelo Tribunal de Contas da União, para divulgação dos dados e informações que especifica, e dá outras providências.	Poder Legislativo	Art. 1o O Tribunal de Contas da União criará homepage na rede de computadores Internet, com o título "contas públicas", para divulgação dos seguintes dados e informações:
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.	Poder Executivo	Art. 1o Fica instituído o Sistema Brasileiro de Inteligência, que integra as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. § 1o O Sistema Brasileiro de Inteligência tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária. § 2o Para os efeitos de aplicação desta Lei, entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. § 3o Entende-se como contra-inteligência a atividade que objetiva neutralizar a inteligência adversa. Art. 2o Os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República. § 1o O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
Lei nº 9.609, de 19 de fevereiro de 1998.	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.	Poder Legislativo	Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.
Lei nº 9.605, de 12 de fevereiro de 1998	Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências.	Poder Legislativo	Art. 62. Destruir, inutilizar ou deteriorar: I - bem especialmente protegido por lei, ato administrativo ou decisão judicial; II - arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, ato administrativo ou decisão judicial: Pena - reclusão, de um a três anos, e multa. Parágrafo único. Se o crime for culposo, a pena é de seis meses a um ano de detenção, sem prejuízo da multa.
Lei nº 9.507, de 12 de novembro de 1997.	Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.	Poder Legislativo	Art. 1º (VETADO) Parágrafo único. Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações. Art. 7° Conceder-se-á habeas data: I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.
Lei nº 9.504, de 30 de setembro de 1997	Estabelece normas para as eleições.	Poder Legislativo	Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.
Lei nº 9.472, de 16 de julho de 1997	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.	Poder Legislativo	Art. 1° Compete à União, por intermédio do órgão regulador e nos termos das políticas estabelecidas pelos Poderes Executivo e Legislativo, organizar a exploração dos serviços de telecomunicações. Parágrafo único. A organização inclui, entre outros aspectos, o disciplinamento e a fiscalização da execução, comercialização e uso dos serviços e da implantação e funcionamento de redes de telecomunicações, bem como da utilização dos recursos de órbita e espectro de radiofreqüências. Art. 2° O Poder Público tem o dever de: I - garantir, a toda a população, o acesso às telecomunicações, a tarifas e preços razoáveis, em condições adequadas; II - estimular a expansão do uso de redes e serviços de telecomunicações pelos serviços de interesse público em benefício da população brasileira; III - adotar medidas que promovam a competição e a diversidade dos serviços, incrementem sua oferta e propiciem padrões de qualidade compatíveis com a exigência dos usuários; IV - fortalecer o papel regulador do Estado; V - criar oportunidades de investimento e estimular o desenvolvimento tecnológico e industrial, em ambiente competitivo; VI - criar condições para que o desenvolvimento do setor seja harmônico com as metas de desenvolvimento social do País. Art. 21. As sessões do Conselho Diretor serão registradas em atas, que ficarão arquivadas na Biblioteca, disponíveis para conhecimento geral. § 1º Quando a publicidade puder colocar em risco a segurança do País, ou violar segredo protegido ou a intimidade de alguém, os registros correspondentes serão mantidos em sigilo. Art. 39. Ressalvados os documentos e os autos cuja divulgação possa violar a segurança do País, segredo protegido ou a intimidade de alguém, todos os demais permanecerão abertos à consulta do público, sem formalidades, na Biblioteca. Art. 69. As modalidades de serviço serão definidas pela Agência em função de sua finalidade, âmbito de prestação, forma, meio de transmissão, tecnologia empregada ou de outros atributos. Parágrafo único. Forma de telecomunicação é o modo específico de transmitir informação, decorrente de características particulares de transdução, de transmissão, de apresentação da informação ou de combinação destas, considerando-se formas de telecomunicação, entre outras, a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens. Art. 74. A concessão, permissão ou autorização de serviço de telecomunicações não isenta a prestadora do atendimento às normas de engenharia e às leis municipais, estaduais ou do Distrito Federal relativas à construção civil e à instalação de cabos e equipamentos em logradouros públicos.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Leis	Ementa	Origem	Artigos Segurança Informação
Lei nº 9.296, de 24 de julho de 1996.	Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.	Poder Legislativo	Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.
Lei nº 8.443, de 16 de julho de 1992.	Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências.	Poder Legislativo	Art. 86. São obrigações do servidor que exerce funções específicas de controle externo no Tribunal de Contas da União: IV - guardar sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.
Lei nº 8.248, de 23 de outubro de 1991.	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.	Poder Legislativo	Art. 3o Os órgãos e entidades da Administração Pública Federal, direta ou indireta, as fundações instituídas e mantidas pelo Poder Público e as demais organizações sob o controle direto ou indireto da União darão preferência, nas aquisições de bens e serviços de informática e automação, observada a seguinte ordem, a: I - bens e serviços com tecnologia desenvolvida no País; II - bens e serviços produzidos de acordo com processo produtivo básico, na forma a ser definida pelo Poder Executivo.(Redação dada pela Lei nº 10.176, de 11.1.2001)
Lei nº 8183, de 11 de abril de 1991	Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional e dá outras providências.	Poder Legislativo	Art. 1° O Conselho de Defesa Nacional (CDN), órgão de Consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do estado democrático, tem sua organização e funcionamento disciplinados nesta lei.
Lei nº 8.159, de 08 de janeiro de 1991.	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.	Poder Legislativo	Art. 1º É dever do Poder Público a gestão documental e a de proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. Art. 2º Consideram-se arquivos, para os fins desta lei, os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos. Art. 3º Considera-se gestão de documentos o conjunto de procedimentos e operações técnicas à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. Art. 4º Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.
Lei nº 8.137, de 27 de dezembro de 1990.	Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências.	Poder Legislativo	Art. 3° Constitui crime funcional contra a ordem tributária, além dos previstos no Decreto-Lei n° 2.848, de 7 de dezembro de 1940 - Código Penal (Título XI, Capítulo I): I - extraviar livro oficial, processo fiscal ou qualquer documento, de que tenha a guarda em razão da função; sonegá-lo, ou inutilizá-lo, total ou parcialmente, acarretando pagamento indevido ou inexato de tributo ou contribuição social
Lei nº 8.112, de 11 de dezembro de 1990	Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.	Poder Legislativo	Art. 116. São deveres do servidor: VIII - guardar sigilo sobre assunto da repartição; Art. 132. A demissão será aplicada nos seguintes casos: IX - revelação de segredo do qual se apropriou em razão do cargo;
Lei nº 8.027, de 12 de abril de 1990.	Dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências.	Poder Legislativo	Art. 5º São faltas administrativas, puníveis com a pena de demissão, a bem do serviço público: I - valer-se, ou permitir dolosamente que terceiros tirem proveito de informação, prestígio ou influência, obtidos em função do cargo, para lograr, direta ou indiretamente, proveito pessoal ou de outrem, em detrimento da dignidade da função pública; V - exercer quaisquer atividades incompatíveis com o cargo ou a função pública, ou, ainda, com horário de trabalho;
Lei no 7.492, de 16 de junho de 1986.	Define os crimes contra o sistema financeiro nacional, e dá outras providências.	Poder Legislativo	Art. 18. Violar sigilo de operação ou de serviço prestado por instituição financeira ou integrante do sistema de distribuição de títulos mobiliários de que tenha conhecimento, em razão de ofício: Pena - Reclusão, de 1 (um) a 4 (quatro) anos, e multa.
Lei nº 7.232, de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática, e dá outras providências.	Poder Legislativo	Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios: VIII - 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; IX - estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas;
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	Poder Legislativo	Art. 13 - Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos. Pena: reclusão, de 3 a 15 anos. Parágrafo único - Incorre na mesma pena quem: I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa; II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional; III - oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública; IV - obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Medidas Provisórias

Medidas Provisórias	Ementa	Origem	Artigos Segurança Informação
Medida Provisória nº 437, de 29 de Julho de 2008	Altera as Leis n°s 7.853, de 24 de outubro de 1989, 9.650, de 27 de maio 1998, 9.984, de 17 de julho de 2000, e 10.683, de 28 de maio de 2003, dispõe sobre a transformação da Secretaria Especial de Aqüicultura e Pesca da Presidência da República em Ministério da Pesca e Aqüicultura, cria cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, Funções Comissionadas do Banco Central – FCBC.	Poder Executivo	Art. 1º A Lei nº 10.683, de 28 de maio de 2003, passa a vigorar com as seguintes alterações: "Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação (...)".
Medida Provisória nº 434, de 04 de Junho de 2008	Dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN, cria as Carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência e Agente Técnico de Inteligência, e dá outras providências.	Poder Executivo	Art. 8º São atribuições do cargo de Oficial de Inteligência: d) atividades de pesquisa e desenvolvimento científico ou tecnológico direcionadas à obtenção e à análise de dados e à segurança da informação>>; Art. 11. São atribuições do cargo de Oficial Técnico de Inteligência: d) atividades de pesquisa e desenvolvimento científico ou tecnológico, direcionadas à obtenção e análise de dados e à <<segurança da informação;
Medida Provisória nº 377, de 18 de Junho de 2007	Acresce e altera dispositivos da Lei nº 10.683, de 28 de maio de 2003, acresce dispositivos à Lei nº 11.356, de 19 de outubro de 2006, cria a Secretaria de Planejamento de Longo Prazo da Presidência da República, cria cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS e Funções Gratificadas, e dá outras providências.	Poder Executivo	Art. 1º A Lei nº 10.683, de 28 de maio de 2003, passa a vigorar com as seguintes alterações: "Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação, (...)".
Medida Provisória nº 295, de 29 de Maio de 2006	Dispõe sobre a reestruturação das carreiras de Especialista do Banco Central do Brasil, de Magistério de Ensino Superior e de Magistério de 1º e 2º Graus e da remuneração dessas carreiras.	Poder Executivo	Art. 1º A Lei nº 9.650, de 27 de maio de 1998, passa a vigorar com a seguinte redação: "Art. 3º São atribuições dos titulares do cargo de Analista do Banco Central do Brasil: XI - desenvolvimento de atividades na área de tecnologia e segurança da informação voltadas ao desenvolvimento, à prospecção, à avaliação e à internalização de novas tecnologias e metodologias;" "Art. 5º São atribuições dos titulares do cargo de Técnico do Banco Central do Brasil: III - execução de atividades de suporte e apoio técnico necessárias ao cumprimento das competências do Banco Central do Brasil que, por envolverem sigilo e segurança do Sistema Financeiro, não possam ser terceirizadas, em particular as pertinentes às áreas de: a)tecnologia e segurança da informação voltadas ao desenvolvimento, à prospecção, à avaliação e à internalização de novas tecnologias e metodologias;"
Medida Provisória nº 228, de 9 de dezembro de 2004.	Regulamenta a parte final do disposto no inciso XXXIII do art. 5ª da Constituição e dá outras providências.	Poder Executivo	Art. 2o Exclusivamente nas hipóteses em que o sigilo dos documentos públicos de interesse particular, ou de interesse coletivo ou geral, seja ou permaneça imprescindível à segurança da sociedade e do Estado, o seu acesso será ressalvado, nos termos do disposto na parte final do inciso XXXIII do art. 5o da Constituição.
Medida Provisória nº 158, de 23 de Dezembro de 2003	Dispõe sobre a criação do Plano Especial de Cargos da Agência Brasileira de Inteligência - ABIN, e dá outras providências.	Poder Executivo	Art. 29. São atribuições do Cargo de Analista de Informações: I - planejar, executar, coordenar, supervisionar e controlar: d)as atividades de pesquisa e desenvolvimento científico ou tecnológico, direcionadas à obtenção e análise de dados e à segurança da informação;
Medida Provisória nº 103, de 1º de Janeiro de 2003	Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências	Poder Executivo	Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação, (...).
Medida Provisória nº 42, de 25 de Junho de 2002	Dispõe sobre a estruturação da Carreira de Inteligência, a remuneração dos integrantes do Quadro de Pessoal da Agência Brasileira de Inteligência – ABIN.	Poder Executivo	Art. 29. Os ocupantes do cargo de Analista de Informações têm por atribuições: d)as atividades de pesquisa e desenvolvimento científico ou tecnológico, direcionadas à obtenção e análise de dados e à segurança da informação;
Medida Provisória Nº 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.	Poder Executivo	Art. 4o Compete ao Comitê Gestor da ICP-Brasil: VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança. Art. 5o À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas. Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final. Art. 6o Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações. Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento. Art. 7o Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações. Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória. § 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil. § 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional. Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira. Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei. Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.
Medida Provisória nº 2.216-37, de 31 de Agosto de 2001	Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. *Obs.: este medida provisória foi reeditada 14 vezes desde setembro de 2000*.	Poder Executivo	Art. 1º. A Lei nº 9.649, de 27 de maio de 1998, passa a vigorar com as seguintes alterações: "Art. 6º. Ao Gabinete de Segurança Institucional da Presidência da República compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional, realizar o assessoramento pessoal em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação (...)".

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos

Decretos	Ementa	Origem	Artigos Segurança Informação
Decreto nº 6.868, de 04.06.2009	Institui o Programa de Apoio à Pesquisa, Desenvolvimento e Inovação em Tecnologias Digitais de Informação e Comunicação (ProTIC) e dispõe sobre a composição de seu Comitê Gestor.	Poder Executivo	Art.1 Fica instituído o Programa de Apoio à Pesquisa, Desenvolvimento e Inovação em Tecnologias Digitais de Informação e Comunicação (ProTIC), com a finalidade de incentivar, apoiar, coordenar e avaliar atividades e projetos de pesquisa, desenvolvimento e inovações, de formação de recursos humanos em decorrência dessas atividades e projetos, de eventos técnico-científicos e de programas de cooperação internacionais, inclusive na produção de conteúdos, na área de tecnologias digitais de informação e comunicação, em particular na promoção do Sistema Brasileiro de Televisão Digital Terrestre - SBTVD-T.
Decreto nº 6.605, de 14 de Outubro de 2008.	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC	Poder Executivo	Art. 1 º O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória n o 2.200-2, de 24 de agosto de 2001 , exerce a função de autoridade gestora de políticas da referida Infra-Estrutura. Art. 3o Compete ao CG da ICP-Brasil: IX - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, de modo a garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança;
Decreto nº 6.504, de 04/07/2008	Institui o Projeto Computador Portátil para Professores, no âmbito do Programa de Inclusão Digital, e dá outras providências.	Poder Executivo	Art. 1° Fica instituído, no âmbito do Programa de Inclusão Digital, o Projeto Computador Portátil para Professores, com o objetivo de promover a inclusão digital de professores ativos da rede pública e privada de educação básica, profissional e superior, nos termos da Lei nº 9.394, de 20 de dezembro de 1996, mediante a aquisição de soluções de informática constituídas de computadores portáteis (notebooks), programas de computador (softwares) neles instalados e de suporte e assistência técnica necessários ao seu funcionamento, observadas as definições, especificações e características técnicas mínimas estabelecidas em ato do Ministro de Estado da Ciência e Tecnologia.
Decreto nº 6.424, de 04/04/2008	Altera e acresce dispositivos ao Anexo do Decreto nº 4.769, de 27/06/2003, que aprova o Plano Geral de Metas para a Universalização do Serviço Telefônico Fixo Comutado prestado no Regime Público - PGMU.	Poder Executivo	Art.5º Compete à ANATEL estabelecer, mediante regulamento, parâmetros para a aferição do cumprimento das metas previstas no PGMU.
Decreto nº 6.408, de 24 de Março de 2008	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Gratificações de Exercício em Cargo de Confiança e das Gratificações de Representação da Agência Brasileira de Inteligência - ABIN, do Gabinete de Segurança Institucional da Presidência da República.	Poder Executivo	Art. 12. Ao Departamento de Pesquisa e Desenvolvimento Tecnológico compete: III - apoiar a Secretaria-Executiva do Conselho de Defesa Nacional, no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.
Decreto nº 6.371, de 12 de Fevereiro de 2008	Dá nova redação ao art. 1º do Decreto nº 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.	Poder Executivo	Art. 1º O art. 1º do Decreto nº 4.801, de 6 de agosto de 2003, passa a vigorar com a seguinte redação: "Art. 1º (...) X - segurança da informação, definida no art. 2º, inciso II, do Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 6.320, de 20 de Dezembro de 2007	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Ministério da Educação, e dá outras providências.	Poder Executivo	Art. 7º À Diretoria de Tecnologia da Informação compete: III - estabelecer e coordenar a execução da política de segurança da informação, no âmbito do Ministério;
Decreto nº 6.319, de 20 de Dezembro de 2007	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Fundo Nacional de Desenvolvimento da Educação - FNDE,.	Poder Executivo	Art. 9º À Diretoria de Administração e Tecnologia compete: IV - planejar, coordenar e acompanhar a execução das atividades inerentes à gestão de tecnologia de informação e da segurança da informação no âmbito do FNDE;
Decreto nº 6.219, de 04 de Outubro de 2007	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas da Superintendência do Desenvolvimento do Nordeste - SUDENE, e dá outras providências.	Poder Executivo	Art. 16. À Diretoria de Administração compete: II - planejar, coordenar e acompanhar a execução das atividades inerentes à gestão e à segurança da informação no âmbito da SUDENE;
Decreto nº 6.218, de 04 de Outubro de 2007	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas da Superintendência do Desenvolvimento da Amazônia – SUDAM.	Poder Executivo	Art. 16. À Diretoria de Administração compete: II - planejar, coordenar e acompanhar a execução das atividades inerentes à gestão e à segurança da informação no âmbito da SUDAM;
Decreto nº 6.138, de 28 de Junho de 2007	Institui, no âmbito do Ministério da Justiça, a Rede de Integração Nacional de Informações de Segurança Pública, Justiça e Fiscalização - Rede Infoseg, e dá outras providências.	Poder Executivo	Art. 6º O fornecimento de informações de monitoramento e controle da Rede Infoseg e de seus usuários é condicionado à instauração e à instrução de processos administrativos ou judiciais, sendo o atendimento da solicitação de responsabilidade exclusiva do chefe do setor de inteligência dos órgãos integrantes da rede, observados, nos casos concretos, os procedimentos de segurança da informação e de seus usuários.
Decreto nº 6.132, de 22 de Junho de 2007	Aprova o Estatuto da Caixa Econômica Federal - CEF e dá outras providências.	Poder Executivo	Art. 38. O Comitê de Tecnologia da Informação, fórum deliberativo e consultivo, é o órgão de orientação superior da área de tecnologia da informação e tem por finalidade propor ao Conselho Diretor, nos limites de suas atribuições, as prioridades em relação aos serviços de tecnologia da informação que necessitem ser implementados para a sustentação dos negócios da CEF, alinhadas às melhores práticas de segurança da informação, às diretrizes e ao planejamento estratégico.
Decreto nº 6.084, de 19 de Abril de 2007	Promulga o Acordo Quadro de Cooperação em Matéria de Defesa entre a República Federativa do Brasil e a Argentina, celebrado em Puerto Iguazú, em 30 de novembro de 2005.	Poder Executivo	ARTIGO 7 1.A segurança da informação e do material trocado ou produzido em decorrência deste Acordo será estabelecida entre as Partes por meio de um Acordo Complementar de proteção dos mesmos.
Decreto nº 6.029, de 1º de fevereiro de 2007.	Institui Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências	Poder Executivo	Art. 1o Fica instituído o Sistema de Gestão da Ética do Poder Executivo Federal com a finalidade de promover atividades que dispõem sobre a conduta ética no âmbito do Executivo Federal, competindo-lhe: II - contribuir para a implementação de políticas públicas tendo a transparência e o acesso à informação como instrumentos fundamentais para o exercício de gestão da ética pública; Art. 22. A Comissão de Ética Pública manterá banco de dados de sanções aplicadas pelas Comissões de Ética de que tratam os incisos II e III do art. 2o e de suas próprias sanções, para fins de consulta pelos órgãos ou entidades da administração pública federal, em casos de nomeação para cargo em comissão ou de alta relevância pública
Decreto nº 5.973, de 29 de Novembro de 2006	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Fundo Nacional de Desenvolvimento da Educação – FNDE.	Poder Executivo	Art. 9º À Diretoria de Administração e Tecnologia compete: IV - planejar, coordenar e acompanhar a execução das atividades inerentes à gestão de tecnologia de informação e da segurança da informação no âmbito do FNDE;
Decreto nº 5.906, de 26 de Setembro de 2006	Regulamenta o art. 4º da Lei nº 11.077, de 30 de dezembro de 2004, os arts. 4º, 9º, 11 e 16-A da Lei nº 8.248, de 23 de outubro de 1991, e os arts. 8º e 11 da Lei nº 10.176, de 11 de janeiro de 2001, que dispõem sobre a capacitação e competitividade do setor de tecnologias da informação.	Poder Executivo	Art. 8º Para fazer jus à isenção ou redução do IPI, as empresas de desenvolvimento ou produção de bens e serviços de informática e automação deverão investir, anualmente, em atividades de pesquisa e desenvolvimento em tecnologias da informação a serem realizadas no País, no mínimo, cinco por cento do seu faturamento bruto no mercado interno, decorrente da comercialização dos produtos contemplados com a isenção ou redução do imposto, deduzidos os tributos correspondentes a tais comercializações, nestes incluídos a Contribuição para o Financiamento da Seguridade Social - COFINS e a Contribuição para o PIS/PASEP, bem como o valor das aquisições de produtos contemplados com isenção ou redução do IPI, nos termos do art. 4º da Lei no 8.248, de 1991, ou do art. 2º da Lei nº 8.387, de 30 de dezembro de 1991, conforme projeto elaborado pelas próprias empresas, a partir da apresentação da proposta de projeto de que trata o art. 22. § 1º No mínimo dois inteiros e três décimos por cento do faturamento bruto mencionado no caput deste artigo deverão ser aplicados como segue: III - sob a forma de recursos financeiros, depositados trimestralmente no Fundo Nacional de Desenvolvimento Científico e Tecnológico - FNDCT, devendo, neste caso, ser aplicado percentual não inferior a cinco décimos por cento. § 2º Os recursos de que trata o inciso III do § 1º destinam-se, exclusivamente, à promoção de projetos estratégicos de pesquisa e desenvolvimento em tecnologias da informação, inclusive em segurança da informação.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Origem	Artigos Segurança Informação
Decreto nº 5.772, de 08 de Maio de 2006	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências.	Poder Executivo	Art. 1º O Gabinete de Segurança Institucional, órgão essencial da Presidência da República, tem como área de competência os seguintes assuntos: IV - coordenação das atividades de inteligência federal e de segurança da informação. Art. 2º O Gabinete de Segurança Institucional tem a seguinte estrutura organizacional: I - órgãos de assistência direta e imediata ao Ministro de Estado: c)Subchefia-Executiva: 3. Departamento de <<Segurança da Informação>> e Comunicações; Art. 3º À Assessoria Especial compete: IV - assessorar o Ministro de Estado sobre os assuntos pertinentes à segurança da informação e comunicação. Art. 5º À Subchefia-Executiva compete: XIII - exercer a supervisão das atividades de <<segurança da informação>> e comunicações ligadas a sua área de competência, na administração pública federal; Art. 8º Ao Departamento de <<Segurança da Informação>> e Comunicações compete: I - adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos; II - planejar e coordenar a execução das atividades de <<segurança da informação>> e comunicações na administração pública federal; III - definir requisitos metodológicos para implementação da <<segurança da informação>> e comunicações pelos órgãos e entidades da administração pública federal; IV - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal; V - estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança da informação e comunicações; e VI - avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações.
Decreto nº 5.687, de 31 de janeiro de 2006.	Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003	Poder Executivo	ANEXO -Artigo 10 .Tendo em conta a necessidade de combater a corrupção, cada Estado Parte, em conformidade com os princípios fundamentais de sua legislação interna, adotará medidas que sejam necessárias para aumentar a transparência em sua administração pública, inclusive no relativo a sua organização, funcionamento e processos de adoção de decisões, quando proceder. Essas medidas poderão incluir, entre outras coisas: a) A instauração de procedimentos ou regulamentações que permitam ao público em geral obter, quando proceder, informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais, sobre as decisões e atos jurídicos que incumbam ao público; b) A simplificação dos procedimentos administrativos, quando proceder, a fim de facilitar o acesso do público às autoridades encarregadas da adoção de decisões; e c) A publicação de informação, o que poderá incluir informes periódicos sobre os riscos de corrupção na administração pública.
Decreto nº 5.644, de 28/12/2005	Dispõe sobre a atuação integrada e o intercâmbio de informações entre a Secretaria da Receita Federal e a Secretaria da Receita Previdenciária e dá outras providências.	Poder Executivo	Art. 1° A Secretaria da Receita Federal, órgão do Ministério da Fazenda, e a Secretaria da Receita Previdenciária, órgão do Ministério da Previdência Social, deverão atuar de forma integrada, com o compartilhamento de informações de interesse para a execução das respectivas competências, com vistas ao aumento da eficiência das atividades de fiscalização, arrecadação e cobrança dos tributos que administram.
Decreto nº 5.584, de 18 de novembro de 2005	Dispõe sobre o recolhimento ao arquivo nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.	Poder Executivo	Art. 1º Os documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN, deverão ser recolhidos ao Arquivo Nacional, até 31 de dezembro de 2005, observados os termos do § 2º do art. 7º da Lei no 8.159, de 8 de janeiro de 1991. Art. 7º Para acesso e manuseio dos documentos referidos no art. 1o, os integrantes dos Grupos Supervisor e Técnico firmarão termo de manutenção de sigilo e receberão credencial de segurança no grau de sigilo correspondente ao dos documentos. Art. 10. Recolhidos ao Arquivo Nacional, os documentos referidos no art. 1o deverão ser disponibilizados para acesso público, resguardadas a manutenção de sigilo e a restrição ao acesso de documentos que se refiram à intimidade da vida privada de pessoas ou cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do Decreto no 4.553, de 2002.
Decreto nº 5.563, de 11 de outubro de 2005.	Regulamenta a Lei no 10.973, de 2 de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo.	Poder Executivo	Art. 2o Para os efeitos deste Decreto, considera-se: V - Instituição Científica e Tecnológica - ICT: órgão ou entidade da administração pública que tenha por missão institucional, dentre outras, executar atividades de pesquisa básica ou aplicada de caráter científico ou tecnológico.
Decreto nº 5.495, de 20 de Julho de 2005	Acresce incisos ao art. 7º do Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da administração pública federal.	Poder Executivo	Art. 1º. O art. 7º do Decreto nº 3.505, de 13 de junho de 2000, passa a vigorar acrescido dos seguintes incisos: "XIV - Ministério de Minas e Energia; XV - Controladoria-Geral da União; e XVI - Advocacia-Geral da União." (NR)
Decreto nº 5.482, de 30 de junho de 2005.	Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores - Internet.	Poder Executivo	Art. 1º O Portal da Transparência do Poder Executivo Federal, sítio eletrônico à disposição na Rede Mundial de Computadores - Internet, tem por finalidade veicular dados e informações detalhados sobre a execução orçamentária e financeira da União, compreendendo, entre outros, os seguintes procedimentos: I - gastos efetuados por órgãos e entidades da administração pública federal; II - repasses de recursos federais aos Estados, Distrito Federal e Municípios; III - operações de descentralização de recursos orçamentários em favor de pessoas naturais ou de organizações não-governamentais de qualquer natureza; e IV - operações de crédito realizadas por instituições financeiras oficiais de fomento.
Decreto nº 5.450, de 31 de Maio de 2005	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências	Poder Executivo	Art. 1º. A modalidade de licitação pregão, na forma eletrônica, de acordo com o disposto no § 1º do art. 2º da Lei nº 10.520, de 17 de julho de 2002, destina-se à aquisição de bens e serviços comuns, no âmbito da União, e submete-se ao regulamento estabelecido neste Decreto. Art. 2º. O pregão, na forma eletrônica, como modalidade de licitação do tipo menor preço, realizar-se-á quando a disputa pelo fornecimento de bens ou serviços comuns for feita à distância em sessão pública, por meio de sistema que promova a comunicação pela internet.
Decreto nº 5.420, de 14 de Abril de 2005	Dispõe sobre o remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, altera o Anexo II ao Decreto nº 4.689, de 7 de maio de 2003, o art. 2º e o caput do art. 8º do Anexo I e o Anexo II ao Decreto nº 5.135, de 7 de julho de 2004.	Poder Executivo	ANEXO II A) Quadro demonstrativo dos cargos em comissão do instituto nacional de tecnologia da informação.
Decreto nº 5.408, de 1º de Abril de 2005	Altera dispositivos da Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República, aprovada pelo Decreto nº 5.083, de 17 de maio de 2004.	Poder Executivo	Art. 1º. Os arts. 4º e 22 da Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República, aprovada pelo Decreto nº 5.083, de 17 de maio de 2004, passam a vigorar com a seguinte redação: "Art. 4º. (...) XIV - implementar, com a assessoria do Comitê Gestor de Segurança da Informação - CGSI e em articulação com os demais órgãos e entidades, a Política de Segurança da Informação da Administração Pública Federal;"
Decreto nº 5.301, de 09 de dezembro de 2004.	Regulamenta o disposto na Medida Provisória nº 228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no inciso XXXIII do art. 5º da Constituição, e dá outras providências. Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.	Poder Executivo	Art. 1o Este Decreto regulamenta a Medida Provisória no 228, de 9 de dezembro de 2004, e institui a Comissão de Averiguação e Análise de Informações Sigilosas. Art. 2o Nos termos da parte final do inciso XXXIII do art. 5o da Constituição, o direito de receber dos órgãos públicos informações de interesse particular, ou de interesse coletivo ou geral, só pode ser ressalvado no caso em que a atribuição de sigilo seja imprescindível à segurança da sociedade e do Estado. Art. 3 Os documentos públicos que contenham informações imprescindíveis à segurança da sociedade e do Estado poderão ser classificados no mais alto grau de sigilo. Parágrafo único. Para os fins deste Decreto, entende-se por documentos públicos qualquer base de conhecimento, pertencente à administração pública e às entidades privadas prestadoras de serviços públicos, fixada materialmente e disposta de modo que se possa utilizar para informação, consulta, estudo ou prova, incluindo áreas, bens e dados. Art. 4o Fica instituída, no âmbito da Casa Civil da Presidência da República, a Comissão de Averiguação e Análise de Informações Sigilosas, com a finalidade de decidir pela aplicação da ressalva prevista na parte final do inciso XXXIII do art. 5o da Constituição.
Decreto nº 5.110, de 18 de Junho de 2004	Acresce inciso ao art. 7º do Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública.	Poder Executivo	Art. 1º. O art. 7º do Decreto nº 3.505, de 13 de junho de 2000, passa a vigorar acrescido do seguinte inciso: "XIII - Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República." (NR)
Decreto nº 4.896, de 25 de novembro de 2003.	Dispõe sobre a institucionalização do Sistema de Informações Organizacionais do Governo Federal - SIORG	Poder Executivo	Art. 1º Fica institucionalizado o Sistema de Informações Organizacionais do Governo Federal - SIORG, com a finalidade de dotar os órgãos e entidades do Poder Executivo Federal de instrumento para: I - elaboração e controle sistêmico das estruturas regimentais, estatutos, regulamentos e regimentos internos; II - manutenção e normalização sistemática das denominações, subordinação hierárquica entre unidades, competências e atribuições institucionais; III - remanejamento de cargos comissionados e funções de confiança; e IV - nomeação, exoneração, designação e dispensa de cargos e funções comissionadas, em integração com o Sistema Integrado de Administração de Recursos Humanos - SIAPE.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Origem	Artigos Segurança Informação
Decreto de 29 de Outubro de 2003	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico (CEGE) e dá outras providências.	Poder Executivo	Art. 1º Ficam instituídos Comitês Técnicos, no âmbito do Comitê Executivo do Governo Eletrônico, criado pelo Decreto de l8 de outubro de 2000, com a finalidade de coordenar e articular o planejamento e a implementação de projetos e ações nas respectivas áreas de competência, com as seguintes denominações: I - Implementação do Software Livre; II - Inclusão Digital; III - Integração de Sistemas; IV - Sistemas Legados e Licenças de Software; V - Gestão de Sítios e Serviços On-line; VI - Infra-Estrutura de Rede; VII - Governo para Governo - G2G; e VIII - Gestão de Conhecimentos e Informação Estratégica.
Decreto nº 4.829, de 03 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.	Poder Executivo	Art. 1° Fica criado o Comitê Gestor da Internet no Brasil - CGIbr, que terá as seguintes atribuições:
Decreto nº 4.801, de 6 de agosto de 2003.	Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.	Poder Executivo	Art. 1o Fica criada a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério, inclusive aquelas pertinentes a: X - segurança da informação, definida no art. 2o, inciso II, do Decreto no 3.505, de 13 de junho de 2000. (Incluído pelo Decreto nº 6.371, de 2008)
Decreto nº 4.689, de 07 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação – ITI, e dá outras providências	Poder Executivo	Estrutura.
Decreto s/n°, de 12 de maio de 2003.	Designa membro para compor Comitê Gestor da ICP-Brasil.	Poder Executivo	Membros.
Decreto s/n, de 27 de maio de 2002	Designa membro para compor Comitê Gestor da ICP-Brasil.	Poder Executivo	Membros.
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.	Poder Executivo	Art. 2º São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. Parágrafo único. O acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer. Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, 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. Art. 44. Aplicam-se aos programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança previstas neste Decreto para os documentos sigilosos controlados e os seguintes procedimentos: I - realização de vistorias periódicas, com a finalidade de assegurar uma perfeita execução das operações criptográficas; II - manutenção de inventários completos e atualizados do material de criptografia existente; III - designação de sistemas criptográficos adequados a cada destinatário; IV - comunicação, ao superior hierárquico ou à autoridade competente, de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de dados ou informações criptografados; e V - identificação de indícios de violação ou interceptação ou de irregularidades na transmissão ou recebimento de dados e informações criptografados. Parágrafo único. Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos pela Infra-Estrutura de Chaves Públicas Brasileira (ICP Brasil). Art. 45. Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo ultra-secreto só poderão estar ligados a redes de computadores seguras, e que sejam física e logicamente isoladas de qualquer outra. Art. 46. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento. Art. 47. Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo secreto, confidencial e reservado só poderão integrar redes de computadores que possuam sistemas de criptografia e segurança adequados a proteção dos documentos. Art. 48. O armazenamento de documentos sigilosos, sempre que possível, deve ser feito em mídias removíveis que podem ser guardadas com maior facilidade.
Decreto nº 4.522, 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.	Poder Executivo	Art. 1º Ficam organizadas sob a forma de sistema, com a designação de Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, as atividades de elaboração, redação, alteração, controle, tramitação, administração e gerência das propostas de atos normativos a serem encaminhadas ao Presidente da República pelos Ministérios e órgãos integrantes da estrutura da Presidência da República. Art. 4º Incumbe ao órgão central do SIDOF: III - quanto à certificação digital dos participantes, sob a responsabilidade da Autoridade Certificadora da Presidência da República: a) identificar e cadastrar os participantes do Sistema na presença destes; b) emitir, expedir, distribuir, revogar e gerenciar os certificados digitais; e c) assegurar à assinatura eletrônica, irretratabilidade, integridade e autenticidade pessoal.
Decreto nº 4.414, de 07 de outubro de 2002.	Altera o Decreto no 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.	Poder Executivo	Art. 1º O Decreto no 3.996, de 31 de outubro de 2001 passa a vigorar acrescido do seguinte artigo: "Art. 3º -A. As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil." (NR)
Decreto nº 4376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências.	Poder Executivo	Art. 2º Para os efeitos deste Decreto, entende-se como inteligência a atividade de obtenção e análise de dados e informações e de produção e difusão de conhecimentos, dentro e fora do território nacional, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório, a ação governamental, a salvaguarda e a segurança da sociedade e do Estado. Art. 3º Entende-se como contra-inteligência a atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem.
Decreto nº 4.376, de 13 de Setembro de 2002	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências.	Poder Executivo	Art. 7º. Fica instituído, vinculado ao Gabinete de Segurança Institucional, o Conselho Consultivo do Sistema Brasileiro de Inteligência, ao qual compete: II - propor normas e procedimentos gerais para o intercâmbio de conhecimentos e as comunicações entre os órgãos que constituem o Sistema Brasileiro de Inteligência, inclusive no que respeita à segurança da informação;
Decreto de 21 de Junho de 2002	Acresce inciso ao art. 2º do Decreto de 18 de outubro de 2000, que cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico (CEGE).	Poder Executivo	Art. 1o O art. 2º do Decreto de 18 de outubro de 2000, que cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, passa a vigorar acrescido do seguinte inciso: "X – o Diretor-Presidente do Instituto Nacional de Tecnologia da Informação." (NR)

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Origem	Artigos Segurança Informação
Decreto de 15 de Março de 2002	Altera o Decreto de 18 de Outubro de 2000, que cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico (CEGE).	Poder Executivo	Art. 1º O art. 2º do Decreto de 18 de outubro de 2000, que cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, passa a vigorar acrescido do seguinte inciso: "IX - o Subcorregedor-Geral da Corregedoria-Geral da União." (NR)
Decreto nº 4.118, de 07 de Fevereiro de 2002	Dispõe sobre a organização da Presidência da República e dos Ministérios.	Poder Executivo	Art. 6º. Ao Gabinete de Segurança Institucional da Presidência da República compete: IV - coordenar as atividades de inteligência federal e de segurança da informação;
Decreto nº 4.073, de 03 de janeiro de 2002.	Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.	Poder Executivo	Art. 1o O Conselho Nacional de Arquivos - CONARQ, órgão colegiado, vinculado ao Arquivo Nacional, criado pelo art. 26 da Lei no 8.159, de 8 de janeiro de 1991, tem por finalidade definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo. Art. 2o Compete ao CONARQ: I - estabelecer diretrizes para o funcionamento do Sistema Nacional de Arquivos - SINAR, visando à gestão, à preservação e ao acesso aos documentos de arquivos; VIII - estimular a integração e modernização dos arquivos públicos e privados; XV - articular-se com outros órgãos do Poder Público formuladores de políticas nacionais nas áreas de educação, cultura, ciência, tecnologia, informação e informática. Art. 18. Em cada órgão e entidade da Administração Pública Federal será constituída comissão permanente de avaliação de documentos, que terá a responsabilidade de orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor.
Decreto s/nº de 04 de Dezembro de 2001	Cria, no âmbito do Comitê Executivo do Governo Eletrônico (CEGE), o Subcomitê da Rede Brasil.gov, e dá outras providências.	Poder Executivo	Art.1º Fica criado, no âmbito do Comitê Executivo do Governo Eletrônico, o Subcomitê da Rede Brasil.gov, composto por um representante, titular e suplente, de cada órgão e entidade participante da rede, com o objetivo de coordenar as ações necessárias para que essas redes sigam um plano de evolução, que contemple regras de integração, compartilhamento de meios, aquisição conjunta de serviços de telecomunicações, troca de tráfego e utilização comum de pontos de acesso, dentro de modelo de gestão compartilhada. Art. 2º Compete ao Subcomitê: I - planejar e deliberar sobre a execução, a operação e a evolução das etapas do projeto de integração das diversas redes de comunicação de dados do Governo Federal, de acordo com o plano de trabalho aprovado pelos órgãos e entidades participantes; II - gerenciar a implantação do ambiente compartilhado; III - homologar os produtos e serviços da rede compartilhada; IV - dimensionar os recursos da rede compartilhada; V - normatizar e adequar as políticas de segurança e endereçamento; VI - definir as rotas primárias e alternativas; VII - normatizar e adequar a redundância da rede física e lógica, considerando os recursos do ambiente central; VIII - estabelecer indicadores, mecanismos e padrões de controle do projeto; IX - normatizar e expedir regras de utilização da rede compartilhada, com vistas à uniformização de conceitos e de procedimentos; X - elaborar sistemáticas de avaliação e de auditoria sobre o desempenho, nível de serviço e custo dos serviços da Rede Brasil.gov; XI - analisar e aprovar a forma de participação das diversas redes da Administração Pública Federal na rede Brasil.gov; e XII - baixar normas reguladoras de suas atribuições.
Decreto nº 4.036, de 28/11/2001	Dá nova redação ao art 1o e acresce inciso ao Anexo do Decreto no 3.280, de 8 de dezembro de 1999, que dispõe sobre a vinculação de entidades integrantes da Administração Pública Federal indireta.	Poder Executivo	Dá nova redação ao art 1º e acresce inciso ao Anexo do Decreto nº 3.280, de 08/12/1999. O decreto dispõe sobre a vinculação do Instituto Nacional de Tecnologia da Informação, AC RAiz da ICP-Brasil, à Casa Civil da Presidência da República.
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.	Poder Executivo	Art. 3o A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil. Art. 3o-A. As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil. (Incluído pelo Decreto nº 4.414, de 7.10.2002)
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.	Poder Executivo	Art. 2o Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital. § 1o Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil. § 2o Respeitado o disposto no § 1o, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.
Decreto no 2.910, de 29 de dezembro de 1998	Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, e dá outras providências.	Poder Executivo	Art . 1º As medidas de segurança relativas a documentos produzidos, em qualquer suporte, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, que digam respeito à garantia da sociedade e do Estado, serão aplicadas em conformidade com o disposto neste Decreto. Art . 36. As normas gerais para a implementação das ações necessárias à segurança das comunicações e dos sistemas de informação dos órgãos do Governo Federal serão baixadas pela Secretaria-Geral do Conselho de Defesa Nacional, com vista a padronizar critérios e procedimentos..
Decreto nº 3.714, de 3 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto no 2.954, de 29 de janeiro de 1999.	Poder Executivo	Art. 2o A transmissão dos documentos a que se refere este Decreto, assinados eletronicamente pela autoridade competente, far-se-á por sistema que lhes garanta a segurança, a autenticidade e a integridade de seu conteúdo, bem como a irretratabilidade ou irrecusabilidade de sua autoria.
Decreto s/nº de 18 de Outubro de 2000	Define os objetivos, a composição e as competências do Comitê Executivo do Governo Eletrônico (CEGE) bem como, sua secretaria executiva;	Poder Executivo	Art. 1º Fica criado, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, com o objetivo de formular políticas, estabelecer diretrizes, coordenar e articular as ações de implantação do Governo Eletrônico, voltado para a prestação de serviços e informações ao cidadão. Art. 3º Compete ao Comitê: I - coordenar e articular a implantação de programas e projetos para a racionalização da aquisição e da utilização da infra-estrutura, dos serviços e das aplicações de tecnologia da informação e comunicações no âmbito da Administração Pública Federal; II - estabelecer as diretrizes para a formulação, pelos Ministérios, de plano anual de tecnologia da informação e comunicações; III - estabelecer diretrizes e estratégias para o planejamento da oferta de serviços e de informações por meio eletrônico, pelos órgãos e pelas entidades da Administração Pública Federal; IV - definir padrões de qualidade para as formas eletrônicas de interação; V - coordenar a implantação de mecanismos de racionalização de gastos e de apropriação de custos na aplicação de recursos em tecnologia da informação e comunicações, no âmbito da Administração Pública Federal; VI - estabelecer níveis de serviço para a prestação de serviços e informações por meio eletrônico; e VII - estabelecer diretrizes e orientações e manifestar-se, para fins de proposição e revisão dos projetos de lei do Plano Plurianual, de Diretrizes Orçamentárias e do Orçamento Anual, sobre as propostas orçamentárias dos órgãos e das entidades da Administração Pública Federal, relacionadas com a aplicação de recursos em investimento e custeio na área de tecnologia da informação e comunicações. Parágrafo único. Em casos de relevância e urgência, o Presidente poderá expedir resolução ad referendum do Comitê, obtida previamente a concordância dos demais membros. (Incluído pelo Decreto de 24.7.2001)
Decreto nº 3.587, de 05 de Setembro de 2000	Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov. e dá outras providências.	Poder Executivo	Art. 19. Compete ao Comitê Gestor de Segurança da Informação e concepção, a especificação e a coordenação da implementação da ICP-Gov, conforme disposto no art. 4º, inciso XIV, do Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.	Poder Executivo	Art. 1º Os programas de computador poderão, a critério do titular dos respectivos direitos, ser registrados no Instituto Nacional da Propriedade Industrial - INPI.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Origem	Artigos Segurança Informação
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.	Poder Executivo	Art. 1º. Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos: I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição; II - proteção de assuntos que mereçam tratamento especial; III - capacitação dos segmentos das tecnologias sensíveis; IV - uso soberano de mecanismos de <<segurança da informação>>, com o domínio de tecnologia sensíveis e duais; V - criação, desenvolvimento e manutenção de mentalidade de <<segurança da informação>>; VI - capacitação científico-tecnologia do País para uso da criptografia na segurança e defesa do Estado; e VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade. Art. 2º. Para efeitos da Política de <<Segurança da Informação>>, ficam estabelecidas as seguintes conceituações: I - Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal; II - <<Segurança da Informação>>: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abragendo, inclusive, a segurança dos recirsos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. Art. 3º. São objetivos da Política da Informação: I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnologia e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis; II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação; III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em <<segurança da informação>>; IV - estabelecer normas jurídicas necessárias à efetiva implementação da <<segurança da informação>>; V - promover as ações necessárias à implementação e manutenção da <<segurança da informação>>; VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de <<segurança da informação>>; VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a <<segurança da informação>>; e VIII - assegurar a interoperabilidade entre os sistemas de <<segurança da informação>>. Art. 4º. Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da <<Segurança da Informação>> de que trata o art. 6º, adotar as seguintes diretrizes: I - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal; II - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da <<segurança da informação>>; III - propor regulamentação sobre matérias afetas à <<segurança da informação>> nos órgãos e nas entidades da Administração Pública Federal; IV - estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; V - acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à <<segurança da informação>>; VI - orientar a condução da Política de <<Segurança da Informação>> já existente ou a ser implementada; VII - realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de <<segurança da informação>>, no intuito de aferir o nível de segurança dos respectivos sistemas de informação; VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de <<Segurança da Informação>>; IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional; X - estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais; XI - estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos; XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações; XIII - estabelecer as normas relativas à implementação dos Sistemas de <<Segurança da Informação>>, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; e XIV - conceber, especificar e coordenar a implementação da infra-estrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal. Art. 5º. A Agencia Brasileira de Inteligência - ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC, competirá: I - apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à <<segurança da informação>>; e II - integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento. Art. 6º. Fica instituído o Comitê Gestor da <<Segurança da Informação>>, com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de <<Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto. Art. 7º. O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados: I - Ministério da Justiça; II - Ministério da Defesa; III - Ministério das Relações Exteriores; IV - Ministério da Fazenda; V - Ministério da Previdência e Assistência Social; VI - Ministério da Saúde; VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior; VIII - Ministério do Planejamento, Orçamento e Gestão; IX - Ministério das Comunicações; X - Ministério da Ciência e Tecnologia; XI - Casa Civil da Presidência da República; e XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará. XIII - Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República. (Incluído pelo Decreto nº 5.110, de 2004) XIV - Ministério de Minas e Energia; (Incluído pelo Decreto nº 5.495, de 2005) XV - Controladoria-Geral da União; e (Incluído pelo Decreto nº 5.495, de 2005) XVI - Advocacia-Geral da União. (Incluído pelo Decreto nº 5.495, de 2005) § 1º Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados. § 2º Os membros do Comitê Gestor não poderão participar de processos similares de iniciativa do setor privado, exceto nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República.
Decreto nº 3.294, de 15 de dezembro de 1999	Institui o Programa Sociedade da Informação, com o objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira	Poder Executivo	Art. 1o Fica instituído o Programa Sociedade da Informação, com o objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira. Art. 2o O Ministério da Ciência e Tecnologia será o responsável pela coordenação das atividades e da execução do Programa.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Origem	Artigos Segurança Informação
Decreto nº 2.295, 04 de agosto de 1997.	Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.	Poder Executivo	Art 1º Ficam dispensadas de licitação as compras e contratações de obras ou serviços quando a revelação de sua localização, necessidade, característica do seu objeto, especificação ou quantidade coloque em risco objetivos da segurança nacional, e forem relativas à: I - aquisição de recursos bélicos navais, terrestres e aeroespaciais; II - contratação de serviços técnicos especializados na área de projetos, pesquisas e desenvolvimento científico e tecnológico; III - aquisição de equipamentos e contratação de serviços técnicos especializados para a área de inteligência. Parágrafo único. As dispensas de licitação serão necessariamente justificadas, notadamente quanto ao preço e à escolha do fornecedor ou executante, cabendo sua ratificação ao titular da pasta ou órgão que tenha prerrogativa de Ministro de Estado.
Decreto nº 1.048, de 21 de janeiro de 1994.	Dispõe sobre o Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências.	Poder Executivo	Art. 1° Ficam organizados, sob a forma de Sistema, com a denominação de Sistema de Administração dos Recursos de Informação e Informática SISP, o planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de informação e informática dos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, em articulação com os demais sistemas que atuam direta ou indiretamente na gestão da informação pública federal. Art. 2° O Sistema de Administração dos Recursos de Informação e Informática tem por finalidade: I - assegurar ao Governo Federal suporte de informação adequado, dinâmico, confiável e eficaz; II - facilitar aos interessados a obtenção das informações disponíveis, resguardados os aspectos de sigilo e restrições administrativas ou previstas em dispositivos legais; III - promover a integração entre programas de governo, projetos e atividades, visando à definição de políticas, diretrizes e normas relativas à gestão dos recursos do Sistema; IV - estimular o uso racional dos recursos de informação e informática, no âmbito da Administração Pública Federal, visando à melhoria da qualidade e da produtividade do ciclo da informação; V - estimular o desenvolvimento, a padronização, a integração, a normalização dos serviços de produção e disseminação de informações, de forma desconcentrada e descentralizada; VI - propor adaptações institucionais necessárias ao aperfeiçoamento dos mecanismos de gestão dos recursos de informação e informática; VII - estimular e promover a formação, o desenvolvimento e o treinamento dos servidores que atuam na área de informação e informática.
Decreto nº 893, de 12 de agosto de 1993	Aprova o Regulamento do Conselho de Defesa Nacional.	Poder Executivo	Art. 1° É aprovado o regulamento, que com este baixa, do Conselho de Defesa Nacional, criado pelo art. 91 da Constituição Federal, e de organização e funcionamento regulados pela Lei n° 8.183, de 11 de abril de 1991.
Decreto nº 97.859, de 23 de junho de 1989	Extingue a Divisão de Segurança e Informações do Ministério das Relações Exteriores	Poder Executivo	Art. 1º - Fica extinta a Divisão de Segurança e Informações do Ministério das Relações Exteriores, criada pelo Decreto nº 60.940, de 4 de julho de 1967.
Decreto nº 88.082, de 02 de Fevereiro de 1983	Dispõe sobre a criação de empregos na Tabela Permanente da Superintendência da Borracha - SUDHEVEA e dá outras providências.	Poder Executivo	Art. 1º. Ficam criados na forma do Anexo deste decreto, nas Categorias Funcionais de Agente Administrativo e Datilógrafo, do Grupo Serviços Auxiliares, código: LT-AS-800; e Analista de Informações e Analista de Segurança Nacional e Mobilização, do Grupo Segurança e Informações, código: LT-SI-1400, da Tabela Permanente da Superintendência da Borracha, os empregos a serem preenchidos na forma regulamentar, observada a legislação específica.
Decreto nº 77.815, de 15 de Junho de 1976	Dispõe sobre a Assessoria Especial de Segurança e Informação (AESI-INPS) do Instituto Nacional de Previdência Social e dá outras providências.	Poder Executivo	Art. 1º. O Instituto Nacional de Previdência Social (INPS) terá uma Assessoria Especial de Segurança e Informações (AESI/INPS), com organização e atribuições definidas em Regulamento próprio. Art. 2º. O quadro de lotação da Assessoria Especial de Segurança e Informações do Instituto Nacional de Previdência Social será o constante do Anexo a este decreto. Art. 3º. A Assessoria Especial de Segurança e Informações do INPS terá consignada, no orçamento do Instituto Nacional de Previdência Social, a dotação própria necessária ao desempenho de suas atribuições.
Decreto nº 67.325, de 02 de Outubro de 1970	Aprova o regulamento das Divisões de Segurança e Informações dos Ministérios Civis.	Poder Executivo	Art. 1º. Fica aprovado o Regulamento das Divisões de Segurança e Informações dos Ministérios Civis, que com êste baixa.
Decreto nº 60.636, de 26 de Abril de 1967	Dispõe sôbre medidas relacionadas com a implantação da Reforma Administrativa.	Poder Executivo	Art. 4º A escolha do ocupante do cargo de dirigente da Divisão de Segurança e Informação de cada Ministério Civil deverá ser prèviamente submetida à aprovação do Secretário do Conselho de Segurança Nacional.
Decreto nº 60.463, de 14 de Março de 1967	Aprova e manda executar o Regimento Interno da Divisão de Segurança e Informações do Ministério das Relações Exteriores.	Poder Executivo	Art. 1º Fica aprovado o Regimento Interno da Divisão de Segurança e Informações do Ministério das Relações Exteriores, que com êste baixa, assinado pelo Ministro de Estado das Relações Exteriores.
Decreto Legislativo nº 348, de 18 de maio de 2005	Aprova o Texto da Convenção das Nações Unidas Contra a Corrupção, Adotada pela Assembleia-geral da Organização das Nações Unidas em Outubro de 2003.	Poder Legislativo	O Congresso Nacional decreta: Art. 1º Fica aprovado o texto da Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral da Organização das Nações Unidas - ONU em outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003, em Mérida, no México, na Conferência de Alto Nível, realizada sob os auspícios do Escritório das Nações Unidas contra Drogas e Crimes e do Governo do México. Parágrafo único. Ficam sujeitos à aprovação do Congresso Nacional quaisquer atos que alterem a referida Convenção, assim como quaisquer ajustes complementares que, nos termos do inciso I do art. 49 da Constituição Federal, acarretem encargos ou compromissos gravosos ao patrimônio nacional. Art. 2º Este Decreto Legislativo entra em vigor na data de sua publicação. Senado Federal, em 18 de maio de 2005
Decreto-lei nº 4.657, de 4 de setembro de 1942.	Lei de Introdução ao Código Civil Brasileiro	Poder Executivo	Art. 4° Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito. Art. 5° Na aplicação da lei, o juiz atenderá aos fins sociais a que ela se dirige e às exigências do bem comum.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Portarias

Portarias	Ementa	Origem	Artigos Segurança Informação
Portaria ITI nº 07, de 16 de Fevereiro de 2009.	Instituir o Comitê Estratégico de Tecnologia da Informação, no âmbito do Instituto Nacional de Tecnologia da Informação.	Poder Executivo Presidência da República. Casa Civil. Instituto Nacional de Tecnologia da Informação.ITI	Art. 1º Instituir o Comitê Estratégico de Tecnologia da Informação - CETI, no âmbito do Instituto Nacional de Tecnologia da Informação, vinculado ao Diretor-Presidente, observadas as diretrizes estabelecidas na Política de Tecnologia da Informação do Órgão Central do SISP e do Comitê Executivo do Governo Eletrônico. Art. 2º O Comitê Estratégico de Tecnologia da Informação tem a seguinte finalidade: I - estabelecer as políticas e diretrizes de tecnologia da informação alinhadas às estratégias do Instituto; II - aprovar o Plano Diretor de Tecnologia da Informação - PDTI, e submetê-lo à homologação do Diretor-Presidente; III - aprovar o plano de ações e de investimentos em tecnologia da informação para o Instituto, e submetê-lo à homologação do Diretor-Presidente; IV - definir prioridades de execução de projetos de tecnologia da informação; e V - definir as diretrizes para a aquisição de bens e contratação de serviços de tecnologia da informação.
Portaria SLTI nº 11 de 30 de Dezembro de 2008	Aprova a Estratégia Geral de Tecnologia da Informação (EGTI) no âmbito do Sistema de Administração dos Recursos de Informação e Informática - SISP na versão de 2008.	Poder Executivo Ministério do Planejamento, Orçamento e Gestão Secretaria de Logística e Tecnologia da Informação SLTI	Art. 2º A versão 2008 da Estratégia Geral de Tecnologia da Informação também será publicada no Portal das Comunidades Virtuais do Governo Federal, na comunidade denominada Sistema de Administração dos Recursos de Informação e Informática (SISP), no endereço eletrônico http://catir.softwarepublico.gov.br/ver-comunidade?community_id=1144612, cujo cadastramento é facultado à servidores públicos de órgãos integrantes do SISP, assim como a especialistas convidados da área de Tecnologia da Informação. Art. 3º Os órgãos integrantes do SISP terão até o dia 30 de janeiro de 2009 para cadastrar informações solicitadas no formulário online denominado Auto-diagnóstico e Plano de Metas disponível na comunidade virtual do SISP, no endereço eletrônico acima citado.
Portaria Nr 23 - SE/GSI, de 28 de agosto de 2008	Homologa o Regimento Interno do Comitê Gestor da Segurança da Informação - CGSI.	Presidência da República. Gabinete de Segurança Institucional. GSI	Art. 1o Fica homologado o Regimento Interno do Comitê Gestor da Segurança da Informação - CGSI, em anexo, aprovado em reunião plenária realizada no dia 13 de agosto de 2008.
Portaria de 07 de agosto de 2007 – SE/GSI	Instituir, no âmbito do Comitê Gestor da Segurança da Informação – CGSI, um Grupo de Trabalho de Metodologia.	Presidência da República. GSI	Art. 1º Instituir, no âmbito do Comitê Gestor de Segurança da Informação – CGSI, um Grupo de Trabalho de Metodologia com o objetivo de aperfeiçoar e propor a padronização de normas e procedimentos de Gestão da Segurança da Informação e Comunicações aplicável aos órgãos e entidades da Administração Pública Federal – APF.
Portaria SLTI nº 03 de 07 de Maio de 2007	Institucionaliza o Modelo de Acessibilidade em Governo Eletrônico – e-MAG no âmbito do Sistema de Administração dos Recursos de Informação e Informática – SISP.	Ministério do Planejamento, Orçamento e Gestão - SLTI	Art. 1º O planejamento, implantação, desenvolvimento ou atualização de portais e sítios eletrônicos, sistemas, equipamentos e programas em Tecnologia da Informação e Comunicação – TIC no âmbito da Administração Pública Federal direta, autárquica e fundacional reger-se-á por políticas, diretrizes e especificações que visem assegurar de forma progressiva a acessibilidade de serviços e sistemas de Governo Eletrônico. §1º As políticas, diretrizes e especificações técnicas de acessibilidade serão sistematizadas na forma de um modelo denominado "Modelo de Acessibilidade em Governo Eletrônico – e-MAG", de adoção compulsória pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Informação e Informática – SISP de que trata o Decreto nº 1.048, de 21 de janeiro de 1994, a partir da data da publicação desta Portaria. §2º O e-MAG será amplamente divulgado e a sua disseminação será ativamente promovida por meio da adesão voluntária a ser obtida junto aos órgãos e entidades das administrações públicas estaduais, municipais e distrital e às pessoas jurídicas de direito privado que mantenham relacionamento por meio eletrônico com a Administração Pública Federal.
Portaria normativa nº 05 de 14 de Julho de 2005	Institucionaliza os Padrões de Interoperabilidade de Governo Eletrônico - e-PING, no âmbito do Sistema de Administração dos Recursos de Informação e Informática – SISP, cria sua Coordenação, definindo a competência de seus integrantes e a forma de atualização das versões do Documento.	Ministério do Planejamento, Orçamento e Gestão - SLTI	Art. 1º O planejamento da implantação, desenvolvimento ou atualização de sistemas, equipamentos e programas em Tecnologia da Informação e Comunicação – TIC, no âmbito da Administração Pública Federal direta, autárquica e fundacional, técnicas, reger-se-á, por políticas, diretrizes e especificações, visando assegurar de forma progressiva a interoperabilidade de serviços e sistemas de Governo Eletrônico. § 1º As políticas, diretrizes e especificações técnicas de interoperabilidade serão sistematizadas na forma de uma arquitetura denominada Padrões de Interoperabilidade de Governo Eletrônico – e-PING e adotadas de forma compulsória, com fulcro nas disposições do inciso IV do art. 6o, e inciso I do art. 7°, do Decreto n° 1.048, de 21 de janeiro de 1994, pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Informação e Informática - SISP, a partir da sua publicação.
Portaria conjunta de 08 de Março de 2004	Designa os coordenadores dos Comitês Técnicos no âmbito do Comitê-Executivo do Governo Eletrônico.	Casa Civil e Ministério do Planejamento, Orçamento e Gestão	Nomes dos coordenadores
Portaria nº 992, de 08/09/2004	Estabelece a Política de Segurança da Informação, para orientação estratégica das ações de segurança a serem executadas pelos órgãos da Previdência Social.	Ministério da Previdência Social	Art. 1º Estabelecer a Política de Segurança da Informação, conforme as diretrizes do Anexo, para orientação estratégica das ações de segurança a serem executadas pelos órgãos da Previdência Social.
Portaria Nr 17 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Análise de Normas Técnicas.	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho de Normas de Segurança da Internet no Governo Federal, para, até 31 de dezembro de 2003, propor normas e procedimentos visando a disponibilização e o uso da Internet no Governo Federal.
Portaria Nr 16 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Política Nacional de Telecomunicações voltado para Defesa Nacional	Presidência da República. GSI	Art.1º Instituir, no âmbito do CGSI, um Grupo de Trabalho de Política Nacional de Telecomunicações voltado para Defesa Nacional, para, até 31 de dezembro de 2003, analisar e apresentar proposta de normatização da Política Nacional de Telecomunicações e os serviços de valor agregado de interesse da Defesa Nacional.
Portaria Nr 15- CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Sistema Operacionais de Fonte Aberta	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho de Sistema Operacionais de Fonte Aberta para, até 31 de dezembro de 2003, analisar e propor soluções baseadas em sistemas operacionais de fonte aberta voltados para aplicações críticas e de interesse da segurança da informação, em parceria com a Câmara de Implementação de Software Livre do Governo Eletrônico.
Portaria Nr 14 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Legislação	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho de Legislação para, até 31 de dezembro de 2003, analisar, estudar, avaliar e, se for o caso, sugerir medidas objetivando o aprimoramento normativo pertinente a matérias afetas à segurança da informação.
Portaria Nr 13 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Criptografia Comercial	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho de Criptografia Comercial para, até 31 de dezembro de 2003, estudar e propor normas para o emprego e exploração de recursos criptográficos comerciais.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Portarias	Ementa	Origem	Artigos Segurança Informação
Portaria Nr 12 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho do Centro de Emergência de Computação	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho do Centro de Emergência de Computação para, até 31 de dezembro de 2003, estudar e propor as medidas necessárias para a criação e implantação de um centro de emergência de computação do Governo Federal.
Portaria Nr 11 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho do Programa de Proteção ao Conhecimento e Segurança da Informação	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho do Programa de Proteção ao Conhecimento e Segurança da Informação para, até 31 de dezembro de 2003, desenvolver e propor um programa de proteção ao conhecimento e segurança da informação para aplicação nos diversos órgãos da Administração Pública Federal.
Portaria Nr 10 - CH/GSI, de 27 de junho de 2003	Instituir, no âmbito do CGSI, um Grupo de Trabalho de Análise de Normas Técnicas	Presidência da República. GSI	Art. 1° Instituir, no âmbito do CGSI, um Grupo de Trabalho de Análise de Normas Técnicas para, até 31 de dezembro de 2003, analisar e opinar, sugerindo medidas julgadas pertinentes, a respeito de normas e regulamentos técnicos de interesse da Segurança das Informações.
Portaria SLTI nº 02 de 13 de Março de 2002	Delega competências a servidor do Departamento de Serviços de Rede para estabelecer a negociação, planejamento e execução das ações necessárias a garantir a participação dos órgãos federais na FENASOFT 2002.	Ministério do Planejamento, Orçamento e Gestão - SLTI	Delegar competência.
Portaria ITI nº 1, de 12 de dezembro de 2001.	Publica o conteúdo do certificado auto-assinado da AC-Raiz da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Tornou público a geração do par de chaves assimétricas e a emissão do certificado da AC-Raiz.
Portaria da Casa Civil nº 21, de 26 de julho de 2001.	Designa os membros para compor a Comissão Técnica Executiva - COTEC do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira - CGICP-Brasil.	Presidência da República. Casa Civil	Designa membros.
Portaria da Casa Civil nº 23 de 12 de maio de 2000	Estabelece metas do Programa Sociedade da Informação.	Presidência da República. Casa Civil	
Portaria nº 16 - CH/GSI, de 22 de janeiro de 2001	Aprova o Regimento Interno do Comitê Gestor da Segurança da Informação (CGSI)	Presidência da República. GSI	Art. 1º O Comitê Gestor da Segurança da Informação, neste documento denominado por CGSI, instituído pelo Art. 6 do Decreto nº 3.505, de 13 de junho de 2000, publicado no Diário Oficial da União de 14 de junho de 2000, é um órgão de assessoramento da Secretaria Executiva do Conselho de Defesa Nacional a qual se subordina.
Portaria Interministerial MC/MCT nº 147, de 31/05/1995	Cria o Comitê Gestor Internet do Brasil. (Vide Resoluções nº 01/98 e 02/98-CG e Acordo Registro.br)	Ministério das Comunicações e Ministério de Ciência e Tecnologia	O Ministro de Estado das Comunicações e o Ministro de Estado da Ciência e Tecnologia, no uso das atribuições que lhes confere o artigo 87, parágrafo único, inciso II, da Constituição, e com o objetivo de assegurar qualidade e eficiência dos serviços ofertados, justa e livre competição entre provedores, e manutenção de padrões de conduta de usuários e provedores, e considerando a necessidade de coordenar e integrar todas as iniciativas de serviços Internet no país, resolvem: Art. 1°. Criar o Comitê Gestor Internet do Brasil, que terá como atribuições:

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Resoluções

Resoluções	Ementa	Origem	Artigos Segurança Informação
Resolução STF nº 350, de 29/11/2007	Dispõe sobre o recebimento de Petição Eletrônico com Certificação Digital no âmbito do Supremo Tribunal Federal e dá outras providências.	Poder Judiciário Superior Tribunal Federal - STF	Art. 1º Fica instituído o peticionamento eletrônico com certificação digital para a prática de atos processuais nos autos que tramitam, por meio físico ou eletrônico, no âmbito do Supremo Tribunal Federal. Parágrafo único. Considera-se certificação digital a assinatura realizada por meio de certificado obtido perante Autoridade Certificadora credenciada junto à Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil, instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001.
Resolução nº 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.	Poder Judiciário Supremo Tribunal Federal - STF	Art. 2º São considerados sigilosos os documentos e processos em qualquer suporte: I – cujo conhecimento irrestrito ou divulgação possa acarretar risco à segurança da sociedade e do Estado; II – necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.
Resolução nº 22.718/08 do TSE, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.	Poder Judiciário Tribunal Superior Eleitoral -TSE	Art. 4º É vedada, desde 48 horas antes até 24 horas depois da eleição, a veiculação de qualquer propaganda política na Internet, no rádio ou na televisão – incluídos, entre outros, as rádios comunitárias e os canais de televisão que operam em UHF, VHF e por assinatura –, e, ainda, a realização de comícios ou reuniões públicas (Código Eleitoral, art. 240, p. único).
Resolução nº 22.038, de 08 de Julho de 2005	Dispõe sobre apuração, totalização dos votos e divulgação dos resultados no Referendo de 23 de outubro de 2005.	Poder Judiciário Tribunal Superior Eleitoral - TSE	CAPÍTULO IX - DA SEGURANÇA DA INFORMAÇÃO Art. 88. Diariamente deverão ser providenciadas cópias de segurança dos dados relativos aos sistemas do referendo, durante toda a fase oficial, sempre que houver alteração na base de dados, mantendo-se a guarda das três últimas cópias, devidamente identificadas e acondicionadas. Art. 89. Todos os meios de armazenamento de dados utilizados na apuração e totalização dos votos, bem como as cópias de segurança dos dados, serão identificados e mantidos em condições apropriadas, conforme orientação do respectivo Tribunal Regional Eleitoral, até sessenta dias após a proclamação do resultado do referendo pelo Tribunal Superior Eleitoral. Art. 90. A desinstalação dos sistemas de totalização - preparação e gerenciamento, e do sistema gerador de mídias somente poderá ser efetuada sessenta dias após a proclamação do resultado do referendo pelo Tribunal Superior Eleitoral, desde que não haja recurso envolvendo procedimentos a eles inerentes. Art. 91. Encerrada a votação, as urnas deverão permanecer com os respectivos lacres até sessenta dias após a proclamação do resultado do referendo. Art. 92. Não sendo interposto recurso contra a votação ou apuração, a qualquer tempo, as urnas poderão ser ligadas para que seja verificado se funcionaram como uma de contingência ou de votação.
Resolução STJ nº 01/2009, de 06/02/2009	Regulamenta o processo judicial eletrônico no âmbito do Superior Tribunal de Justiça.	Poder Judiciário Superior Tribunal de Justiça	Art. 1°. Instituir, no âmbito do Superior Tribunal de Justiça, o *e*-STJ, meio eletrônico de tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais, nos termos da Lei n. 11.419/2006 e desta resolução.
Resolução STJ nº 11, de 11/12/2007	Altera o art. 5º da Resolução n. 8, de 20/09/2007, que institui o Diário da Justiça Eletrônico do Superior Tribunal de Justiça - DJ on-line.	Poder Judiciário Superior Tribunal de Justiça	Art. 1º O art. 5º da Resolução n. 8, de 20 de setembro de 2007, publicada no Diário da Justiça do dia 1º de outubro do corrente ano, Seção I, página 114, passa a vigorar com a seguinte redação: "Art. 5º O Superior Tribunal de Justiça manterá publicação impressa e eletrônica até 29 de fevereiro de 2008."

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Resoluções	Ementa	Origem	Artigos Segurança Informação
Resolução STJ nº 9, de 05/11/2007	Altera o art. 1º da Resolução nº 2, de 24/04/2007, que dispõe sobre o recebimento de Petição Eletrônica no âmbito do Superior Tribunal de Justiça.	Poder Judiciário Superior Tribunal de Justiça	Art. 1º Instituir o recebimento de petição eletrônica, no âmbito do Superior Tribunal de Justiça, que permite aos credenciados utilizar a Internet para a prática de atos processuais, independente de petição escrita, nos processos de competência originária do Presidente, nos Habeas Corpus e nos Recursos em Habeas Corpus. Parágrafo único. O recebimento de petições é um serviço de uso facultativo, disponível na Internet, no portal oficial do Superior Tribunal de Justiça.
Resolução nº 01, de 8 de Março de 2001	Implantação ou aperfeiçoamento de sistemas de gestão destinados ao uso compartilhado por todos os órgãos e entidades da Administração Pública Federal	Poder Executivo Presidência da República. Conselho de Governo. Comitê Executivo do Governo Eletrônico - CEGE	Art. 1º A Administração Pública Federal, por intermédio do Ministério do Planejamento, Orçamento e Gestão, promoverá a implantação ou aperfeiçoamento de sistemas de gestão destinados ao uso compartilhado por todos os órgãos e entidades, nas áreas de administração de recursos humanos, gestão e acompanhamento de obras, controle e acompanhamento de processos administrativos (protocolo) e documentos não processuais, sistemas para controle do inventário de equipamentos e software.
Resolução nº 02, de 30 de Julho de 2001	Modificações nos sistemas de informação gerenciados no âmbito do Sistema de Serviços Gerais (SISG).	Presidência da República. Conselho de Governo. CEGE	Art. 1º A implementação de modificações nos sistemas de informação gerenciados no âmbito do Sistema de Serviços Gerais - SISG deverá ser precedida de avaliação sobre possíveis impactos nos demais sistemas e a eles integrados, de modo que não prejudiquem a eficiência e funcionalidade da integração; Art. 4º Esta Resolução se aplica a todos os órgãos e entidades da Administração Pública Federal no âmbito do SISG.
Resolução nº 03, de 20 de Dezembro de 2001	Autorizada a Empresa Brasileira de Correios e Telégrafos – ECT paraa implantação da AC-Correios	Presidência da República. Conselho de Governo. CEGE	Art. 1º Fica autorizada a Empresa Brasileira de Correios e Telégrafos – ECT a realizar as contratações necessárias à implantação de seu projeto "Solução Integrada para Serviços de Certificação Digital – AC-Correios", conforme documentação apresentada a este Comitê em 18 de dezembro de 2001. Art. 2º O início das atividades de certificação digital da AC-Correios fica sujeita, na forma do art. 2º, §1º do Decreto nº 3.996, de 31 de outubro de 2001, ao seu credenciamento na Infra Estrutura de Chaves Públicas Brasileira – ICP-Brasil e à respectiva certificação pela Autoridade Certificadora Raiz – AC Raiz da ICP-Brasil.
Resolução nº 04, de 8 de Março de 2002	Participação do Governo Federal na FENASOFT 2002.	Presidência da República. Conselho de Governo. CEGE	Art. 1º Fica designada a Secretaria de Logística e Tecnologia da Informação para estabelecer a negociação, o planejamento e a execução das ações necessárias a garantir a participação dos órgãos federais no evento FENASOFT 2002.
Resolução nº 05, de 27 de Março de 2002	Autoriza a implantação da AC-SERPRO	Presidência da República. Conselho de Governo. CEGE	Art. 1º Fica autorizada a Presidência da República e o Serviço Federal de Processamento de Dados – SERPRO a realizar as contratações e tomar as medidas necessárias à implantação de seus projetos de certificação digital.
Resolução nº 05-a, de 15 de Julho de 2002	Obrigatoriedade de autorização do CEGE para prestar ou contratar serviços de certificação digital.		Art. 1º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico (CEGE), os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital; Art. 2º A contratação de serviços de certificação digital fica condicionada a que sejam prestados no âmbito da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.; Art. 3º A autorização aos órgãos e às entidades da Administração Pública Federal para a prestação de serviços de certificação digital fica condicionada ao seu credenciamento junto ao Instituto Nacional de Tecnologia da Informação – ITI.
Resolução nº 6, de 22 de julho de 2002	Cria no âmbito do CEGE o subcomitê de Certificação Digital.	Presidência da República. Conselho de Governo. CEGE	Art. 1º cria esse subcomitê com o objetivo de gerenciar as ações de implantação, manutenção e normatização do uso de certificação digital no Governo Federal; Art. 2º apresenta as competências: I, a) normas e padrões para o uso de certificados digitais nas aplicações, serviços e infra-estruturas da Administração Pública Federal; III - estabelece os procedimentos necessários para a salvaguarda da segurança, nos relacionamentos entre os sistemas de informação governamentais, considerando o controle de perfis e permissões estabelecidos;
Resolução nº 7, de 29 de julho de 2002	Estabelece regras e diretrizes para os sítios na internet da Administração Pública Federal.	Presidência da República. Conselho de Governo. CEGE	Art. 1º A estruturação, a elaboração, a manutenção e a administração dos sítios na internet dos órgãos e entidades da Administração Pública Federal regem-se por esta Resolução; Art. 3º A elaboração de um sítio governamental deverá ser precedida pela: I - definição clara do propósito e abrangência do sítio; II - definição do público-alvo do sítio; III - mensuração do valor que o sítio agregará à Administração Pública Federal; e IV - verificação da existência de sítios com igual propósito; Art. 19. A segurança do sítio deve ser permanentemente atualizada de modo a resistir aos ataques que exploram vulnerabilidades para as quais já existam correções; AArt. 25. O ambiente da rede do sítio do órgão ou entidade deve contar com planos de contingência implementados e atualizados, visando ao pronto restabelecimento do ambiente e dos serviços, assim como o não comprometimento da imagem da Administração Pública Federal; Art. 32. Devem ser adotados conceitos e procedimentos de auditoria interna que permitam análise do ambiente computacional; Art. 39. Os órgãos e entidades da Administração Pública Federal deverão, até o final de 2002, adaptar todos seus sítios na internet ao disposto nesta Resolução.
Resolução nº 08, de 4 de Setembro de 2002	Cria o Subcomitê de Integração de Sistemas Administrativos – SISA no âmbito do CEGE.	Presidência da República. Conselho de Governo. CEGE	Art. 1º cria o subcomitê e destaca seu objetivo de coordenar as ações necessárias para o desenvolvimento, implantação e manutenção da integração de dados e processos entre os sistemas administrativos informatizados e deles com os demais sistemas corporativos, dentro do modelo de gestão compartilhada.
Resolução nº 09, de 4 de Outubro de 2002	Institui o Portal Governo como ambiente virtual de interação interna dos órgãos da Administração Pública Federal.	Presidência da República. Conselho de Governo. CEGE	Art. 1º Institui o ambiente virtual para melhoria da gestão interna; Art. 3º determina as Coordenações Gerais de Modernização e Informática de cada Ministério, ou órgãos equivalentes a responsabilidade pelo suporte, instalação e gerenciamento de seus usuários.
Resolução nº 10, de 11 de Outubro de 2002	Autoriza a Caixa Econômica Federal a realizar contratações e tomar as medidas necessárias para que aquela instituição se torne autoridade Certificadora.	Presidência da República. Conselho de Governo. CEGE	Art. 1º descreve a autorização.
Resolução nº 11, de 14 de Outubro de 2002	Autoriza a contratação de serviços de Certificação Digital para órgão do Ministério das Minas e Energia por intermédio da Autoridade Certificadora do Serviço Federal de Processamento de Dados – SERPRO.	Presidência da República. Conselho de Governo. CEGE	Art. 1º autoriza a contratação de serviços de Certificação Digital pelo Departamento Nacional de Produção Mineral.
Resolução nº 12, de 14 de Novembro de 2002	Institui o Portal de Serviços e Informações de Governo E-Gov.	Presidência da República. Conselho de Governo. CEGE	Art. 1º Institui o portal e aponta os endereços na internet do E-Gov; Art. 2º Esse portal deverá apresentar conexão para todos os serviços e informações disponíveis nos sítios mantidos pelos órgãos e entidades da Administração Pública Federal; Art. 3º A gestão desse portal cabe a Secretaria-Executiva do Comitê Executivo do Governo Eletrônico.
Resolução nº 13, de 25 de Novembro de 2002	Institui o Sistema de Acompanhamento de Processos do Governo Federal - PROTOCOLO.NET.	Presidência da República. Conselho de Governo. CEGE	Art. 1º institui o sistema; Art. 2º aborda a gestão operacional e as ações necessárias para promover, implantar e manter o sistema; Art. 3º Os órgãos competentes pela gestão da tecnologia da informação em cada Ministério, autarquia ou fundação, respondem pela atualização contínua das informações sob sua guarda.; Art. 4º Até 31 de dezembro de 2002, todas as informações deverão estar disponíveis no sistema.
Resolução nº 14, de 6 de Dezembro de 2002	Institui o Inventário de Recursos de Tecnologia da Informação e de Comunicação – INVENTIC.	Presidência da República. Conselho de Governo. CEGE	Art. 1º Institui o INVENTIC com o objetivo de reunir as informações quantitativas a respeito de equipamentos, sistemas operacionais básicos, aplicativos de apoio, informações sobre redes locais e segurança, dos órgãos da Administração Pública Federal; Art. 3º Cabe à Secretaria Executiva do CEGE a gestão operacional desse sistema; Art. 4º Os órgãos responsáveis pela gestão da tecnologia da informação em cada Ministério respondem pela atualização contínua das informações sob sua guarda.; Art. 5º Até o dia 30 de novembro de 2002 as informações de que trata o art. 1º deverão estar disponibilizadas nesse sistema.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Resoluções	Ementa	Origem	Artigos Segurança Informação
Resolução ICP n° 3, de 25 de setembro de 2001	Designa Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços.	Presidência da República. Casa Civil. ITI	Comissão designada.
Resolução ICP n° 5, de 22 de novembro de 2001	Aprova o relatório de auditoria da AC Raiz.	Presidência da República. Casa Civil. ITI	Aprovar o relatório de auditoria apresentado pela Comissão designada pela Resolução No 3, de 25 de setembro de 2001, em anexo, homologar a Autoridade Certificadora Raiz - AC Raiz e o Serviço Federal de Processamento de Dados - SERPRO como seu prestador de serviço, bem como autorizar à Autoridade Certificadora Raiz - AC Raiz a gerar seu par de chaves assimétricas e a emitir o seu certificado.
Resolução ICP n° 15, de 10 de junho de 2002	Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Fica constituído Grupo de Tiabalho, no âmbito da Comissão Técnica Executiva - COTEC de que trata o Decreto No 3.872, de 18 de julho de 2001, com a finalidade de estudar e apresentar proposições sobre sincronismo de tempo e certificação de data e hora para a ICP-Brasil no prazo de noventa dias de sua designação a ser procedida pelo Coordenador do Comitê Gestor da ICP-Brasil.
Resolução ICP n° 16, de 10 de junho de 2002.	Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º A hora a ser utilizada pelas entidades integrantes da Infra-Estrutura de Chaves Públicas Brasileira - ICPBrasil, será a oficial fornecida pelo Observatório Nacional. Art. 2º Os sinais primários para sincronização de freqüência e de tempo serão distribuídos pelo Observatório Nacional de forma segura, conforme as normas de segurança de rede em vigor na ICP-Brasil.
Resolução ICP n° 20, de 08 de maio de 2003	Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz.	Presidência da República. Casa Civil. ITI	Art. 1º Determinar à AC Raiz o desenvolvimento de uma plataforma aberta (*hardware* e *software*) voltada à execução das funções criptográficas da AC Raiz da ICP-Brasil, garantida a auditagem plena desta plataforma e dos sistemas embarcados presentes nos *hardwares*. Parágrafo único. Poderão ser celebrados convênios, acordos, ajustes ou outros instrumentos congêneres de cooperação técnica com órgãos ou entidades da administração púbica direta ou indireta para consecução do estabelecido no *caput*.
Resolução ICP n° 29, de 29 de janeiro de 2004	Designa Comissão para realizar auditoria pré-operacional da AC Raiz	Presidência da República. Casa Civil. ITI	Considerando que a Autoridade Certificadora Raiz – AC Raiz da ICP-Brasil, o Instituto Nacional de Tecnologia da Informação, passa a dispor de ambiente próprio, devidamente provido de recursos físicos e lógicos necessários à operacionalização de suas atividades; Considerando a necessidade de transferência das instalações de segurança (backup) do ambiente de seu atual prestador de serviços de suporte, o Serviço Federal de Processamento de Dados – SERPRO, para seu ambiente próprio.
Resolução ICP n° 33, de 21 de outubro de 2004	Delega à AC Raiz da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências.	Presidência da República. Casa Civil. ITI	Art. 1º Delegar à AC Raiz a atribuição para, por meio de Instruções Normativas, suplementar as normas do Comitê Gestor. Art. 2º A AC Raiz poderá, também, emitir Instruções para orientação quanto à aplicação das Resoluções expedidas pelo Comitê Gestor.
Resolução ICP n° 36, de 21 de outubro de 2004	Aprova o Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no âmbito da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar o regulamento para homologação de sistemas e equipamentos de Certificação digital no âmbito da ICP-Brasil em anexo
Resolução ICP n° 39, de 18 de Abril de 2006.	Aprova a versão 2.0 da Política de Segurança da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 da Política de Segurança da ICPBrasil, em anexo,
Resolução ICP n° 41, de 18 de Abril de 2006.	Aprova a versão 2.0 dos Requisitos Mínimos para as POLÍTICAS DE CERTIFICADO na ICP-Brasil	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 dos requisitos mínimos para as políticas de certificado na ICP Brasil (DOCICP04), em anexo. Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICPBrasil nº 07, de 02 de dezembro de 2001, nº 11, de 14 de fevereiro de 2002, nº 28, de 11 de novembro de 2003 e nº 35, de 21 de outubro de 2004 e convalidados os atos praticados durante as vigências desses normativos.
Resolução ICP n° 42, de 18 de Abril de 2006.	Aprova a versão 2.0 dos Requisitos Mínimos para as DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO das Autoridades Certificadoras da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 dos requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICPBRASIL (DOCICP05), em anexo. Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICPBrasil nº 08, de 02 de dezembro de 2001; nº 09, de 12 de dezembro de 2001; nº 13, de 26 de abril de 2002; nº 21, de 29 de agosto de 2003; nº 23, de 29 de agosto de 2003; nº 26, de 24 de outubro de 2003; nº 30, de 29 de janeiro de 2004; nº 31, de 29 de janeiro de 2004, nº 34, de 21 de outubro de 2004 e nº 37, de 21 de outubro de 2004 e convalidados os atos praticados durante as vigências desses normativos.
Resolução ICP n° 43, de 18 de Abril de 2006.	Aprova a versão 2.0 das Diretrizes da POLÍTICA TARIFÁRIA da Autoridade Certificadora Raiz da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 das diretrizes da política tarifária do Instituto Nacional De Tecnologia Da Informação – ITI (DOCICP06), em anexo. Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICP Brasil nº 10, de 14 de fevereiro de 2002 e nº 18, de 10 de outubro de 2002 e convalidados os atos praticados durante suas vigências. REVOGADA.
Resolução ICP n° 44, de 18 de Abril de 2006.	Aprova a versão 2.0 dos Critérios e Procedimentos para Realização de AUDITORIAS NAS ENTIDADES nas Entidades da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 dos critérios e procedimentos para realização de auditorias nas entidades da ICP-Brasil (DOCICP08), em anexo. Art. 2º Fica revogada a Resolução do Comitê Gestor da ICPBrasil nº 24, de 29 de agosto de 2003 e convalidados os atos praticados durante sua vigência.
Resolução ICP n° 45, de 18 de Abril de 2006.	Aprova a versão 2.0 dos Critérios e Procedimentos para FISCALIZAÇÃO das Entidades Integrantes da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 2.0 dos critérios e procedimentos para fiscalização das entidades integrantes da ICP-Brasil (DOCICP09), em anexo. Art. 2º Fica revogada a Resolução do Comitê Gestor da ICPBrasil nº 25, de 24 de outubro de 2003 e convalidados os atos praticados durante sua vigência.
Resolução ICP n° 47, de 03 de Dezembro de 2007.	Aprova a versão 3.0 dos Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 3.0 dos critérios e procedimentos para credenciamento das entidades integrantes da ICPBrasil (DOCICP03), em anexo. Art. 2º Fica revogada a Resolução do Comitê Gestor da ICPBrasil nº 40, de 18 de abril de 2006 e convalidados os atos praticados durante sua vigência.
Resolução ICP n° 48, de 03 de Dezembro de 2007.	Altera os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICPBrasil.	Presidência da República. Casa Civil. ITI.	Art. 1º O subitem 3.1.10.2 do Anexo da Resolução nº 42, do Comitê Gestor da ICPBrasil, de 18 de abril de 2006, passa a vigorar com a seguinte redação:
Resolução ICP n° 49, de 03 de Junho de 2008. Retificação da Resolução n° 49, de 15 de Dezembro de 2008	Aprova a versão 3.0 da Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 3.0 da Declaração de práticas de certificação da autoridade certificadora raiz da ICP-Brasil, em anexo. Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICP-Brasil nº 38, de 18 de abril de 2006 e nº 46, de 03 de dezembro de 2007, estando convalidados os atos praticados durante sua vigência. Retificação das Resoluções 49, 52, 53, 56 e 57 do Comitê Gestor da ICP-BRASIL.
Resolução ICP n° 50, de 28 de Novembro de 2008.	Altera a Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução n° 49, do Comitê Gestor da ICP-Brasil, de 03 de junho de 2008, passa a vigorar com a seguinte redação: Art. 2º Fica aprovada a versão 4.0 da Declaração de práticas de certificação da Autoridade Certificadora Raiz da ICP-BRASIL (DOC-ICP-01), que incorpora as alterações do artigo anterior.
Resolução n° 51, de 28 de Novembro de 2008.	Altera a Política de Segurança da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução n° 39, de 18 de abril de 2006, passa a vigorar com a seguinte redação:
Resolução ICP n° 52, de 28 de Novembro de 2008. Retificação da Resolução n° 52, de 15 de Dezembro de 2008.	Altera os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução do Comitê Gestor da ICP-Brasil n° 47, de 03 de dezembro de 2007, passa a vigorar acrescido dos seguintes itens: Retificação das Resoluções 49, 52, 53, 56 e 57 do Comitê Gestor Da ICP-BRASIL.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Resoluções	Ementa	Origem	Artigos Segurança Informação
Resolução ICP n° 53, de 28 de Novembro de 2008. Retificação da Resolução n° 53, de 15 de Dezembro de 2008.	Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução n° 41 do Comitê Gestor da ICP-Brasil, de 18 de abril de 2006, passa a vigorar com a seguinte redação: Retificação das Resoluções 49, 52, 53, 56 e 57 do Comitê Gestor Da ICP-BRASIL.
Resolução ICP n° 54, de 28 de Novembro de 2008.	Altera os requisitos mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução n° 42 do Comitê Gestor da ICP-Brasil, de 18 de abril de 2006, passa a vigorar acrescido dos seguintes itens:
Resolução ICP n° 55, de 28 de Novembro de 2008.	Aprova a versão 3.0 das diretrizes da política tarifária da Autoridade Certificadora Raiz da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 3.0 das da Política Tarifária Do Instituto Nacional de Tecnologia da Informação – ITI (DOC-ICP-06), em anexo. Art. 2º Fica revogada a Resolução do Comitê Gestor da ICP-Brasil nº 43, de 18 de abril de 2006 e convalidados os atos praticados durante sua vigência.
Resolução ICP n° 56, de 28 de Novembro de 2008. Retificação da Resolução n° 56, de 15 de Dezembro de 2008.	Altera os critérios e procedimentos para realização de auditorias nas entidades da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução do Comitê Gestor da ICP-Brasil n° 44 , de 18 de abril de 2006, passa a vigorar dos seguintes itens: Retificação das Resoluções 49, 52, 53, 56 e 57 do Comitê Gestor Da ICP-BRASIL.
Resolução ICP n° 57, de 28 de Novembro de 2008. Retificação da Resolução n° 57, de 15 de Dezembro de 2008.	Altera os critérios e procedimentos para fiscalização das entidades integrantes da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º O Anexo da Resolução Comitê Gestor da ICP-Brasil n°45, de 18 de abril de 2006, passa a vigorar com a seguinte redação: Retificação das Resoluções 49, 52, 53, 56 e 57 do Comitê Gestor Da ICP-BRASIL.
Resolução ICP n° 58, de 28 de Novembro de 2008.	Aprova a versão 1.0 do documento Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 1.0 da Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil (DOC-ICP-11 em anexo.).
Resolução ICP n° 59, de 28 de Novembro de 2008.	Aprova a versão 1.0 do documento Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 1.0 dos requisitos mínimos para as declarações de práticas das autoridades de carimbo do tempo da ICP-Brasil (DOC-ICP-12 em anexo).
Resolução ICP n° 60, de 28 de Novembro de 2008.	Aprova a versão 1.0 do documento Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 1.0 dos requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil (DOC-ICP-13 em anexo).
Resolução ICP n° 61, de 28 de Novembro de 2008.	Aprova a versão 1.0 do documento Procedimentos para Auditoria do Tempo na ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar a versão 1.0 dos procedimentos para auditoria do tempo na ICP-Brasil (DOC-ICP-14 em anexo).
Resolução ICP n° 62, de 9 de Janeiro de 2009.	Aprova a versão 1.0 do documento Visão Geral sobre Assinaturas Digitais na ICP-Brasil.	Presidência da República. Casa Civil. ITI	Art 1º. Aprovar a versão 1.0 do documento visão geral sobre assinaturas digitais na ICP-Brasil (DOC-ICP-15), que estabelece formatos e políticas para Assinatura Digital de documentos eletrônicos.
Resolução ICP n° 63, de 1º de Abril de 2009.	Aprova o Regimento Interno do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).	Presidência da República. Casa Civil. ITI	Art. 1º Aprovar o Regimento Interno do Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil.
Resolução nº 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.	Poder Executivo Instituto Nacional da Propriedade Industrial - INPI (autarquia federal vinculada ao Ministério do Desenvolvimento, Indústria e Comércio Exterior)	O PRESIDENTE DO INPI, no uso de suas atribuições, RESOLVE estabelecer normas e procedimentos relativos ao registro de programas de computador, na forma da Leinº 9.609, de 19 de fevereiro de 1998, do Decreto nº 2.556, de 20 de abril de 1998 e da Resolução nº 057, de 06 de julho de 1988, do Conselho Nacional de Direito Autoral
Resolução nº 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.	Poder Executivo INPI	Estabelecer normas e procedimentos relativos ao recolhimento das retribuições relativas aos serviços específicos de registro de programas de computador, de acordo com as disposições do artigo 3º da Lei nº 9.609, de 19 de fevereiro de 1998; do artigo 5º do Decreto nº 2.556, de 20 de abril de 1998 e do artigo 20 da Lei nº 9.610, de 19 de fevereiro de 1998.

Fonte: Presidência da República. Casa Civil. Disponível em: <http://www.planalto.gov.br>. Acesso em: 30 ago. 2009.

Projetos de Lei

Projetos de Lei	Assunto	Origem	Autoria
Proposta de emenda à Constituição nº 00072, de 2003	Altera o artigo 52 da Constituição Federal, atribuindo competência ao Senado Federal para aprovar atos relevantes à defesa nacional e à proteção ambiental da fronteira.	Poder Legislativo	Senador Mozarildo Cavalcanti
Projeto de resolução do Senado nº 00023, de 2002	Acrescenta inciso ao artigo 103 do Regimento Interno. (Dispõe sobre a emissão de parecer conclusivo à proposta de criação de Grupo Parlamentar pela Comissão de Relações Exteriores e Defesa Nacional do Senado Federal, para promover a política de intercâmbio parlamentar na ordem econômica e política mundial)	Poder Legislativo	Senador Carlos Wilson
Projeto de Lei nº 3.773/2008.	Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet.	Poder Legislativo	Senado Federal - Comissão Parlamentar de Inquérito – Pedofilia.
Projeto de Lei nº 4.036/2008.	Altera as Leis nºs 4.878, de 3 de dezembro de 1965, 8.112, de 11 de dezembro de 1990, e o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, para dispor sobre sanções administrativas e penais aplicáveis em casos de interceptação de comunicações e de violação de sigilo, e dá outras providências. Aumenta a pena para conduta abusiva de interceptação ilegal, "grampo telefônico".	Poder Executivo.	Presidente da República
Projeto de Lei nº 3.272/2008.	Normatiza a quebra de sigilo das comunicações telefônicas para fins de investigação criminal e instrução processual penal. Revoga a Lei nº 9.296, de 1996; altera o Decreto-Lei nº 2.848, de 1940 e o Decreto-Lei nº 3.689, de 1941. Regulamenta a Constituição Federal de 1988.	Poder Executivo.	Presidente da República
Projeto de Lei nº 2.899/2008.	Obriga as operadoras de telefonia fixa e móvel ao pagamento de multa em razão de danos decorrentes da ineficiência em garantir a privacidade de seus usuários.	Poder Legislativo	Deputado William Woo.
Projeto de Lei nº 398/2007.	Prevê o aumento de pena no caso de crime contra a honra praticado pela Internet.	Poder Legislativo	Senador Expedito Júnior.
Projeto de lei nº 00016, de 2007	Cria o Acordo de Proteção de Informações Sigilosas, adjeto ao contrato de trabalho, para a proteção de segredo comercial e de informações confidenciais e regulamenta sua aplicação.	Poder Legislativo	Senador Marcelo Crivella
Projeto de Lei nº 1.704/2007.	Tipifica a conduta de violação de comunicação eletrônica.	Poder Legislativo	Deputado Rodovalho.
Projeto de Lei nº 1.230/2007.	Torna obrigatória a identificação biométrica para acesso a bancos de dados da administração pública direta, indireta e fundacional onde sejam armazenados dados sensíveis.	Poder Legislativo	Deputado Eduardo Gomes.
Projeto de lei nº 00323, de 2006	Autoriza a utilização da internet como veículo de comunicação oficial	Poder Legislativo	Senador Demóstenes Torres
Projeto de lei nº 00269, de 2006	Altera a Lei nº 8.666, de 21 junho de 1993, que institui normas para licitações e contratos da administração pública, para garantir a preservação de segredos científicos, tecnológicos, industriais ou estratégicos.	Poder Legislativo	Senador Marcelo Crivella
Projeto de lei nº 00317, de 2005	Dispõe sobre a tarifa telefônica nas ligações interurbanas a provedores de Internet.	Poder Legislativo	Senador Romero Jucá
Projeto de lei n° 100, de 2005	Altera a Lei nº 9.504, de 30 de setembro de 1997 (Lei Eleitoral), para ampliar a segurança e a fiscalização do voto eletrônico mediante a emissão de comprovante físico do voto e adoção de programas de computador abertos.	Poder Legislativo	Senador Augusto Botelho
Projeto de lei nº 00191, de 2004	Acrescenta parágrafo ao Art. 2º da Lei nº 8.560, de 29 de dezembro de 1992. (Dispõe sobre a competência do juízo da Vara da Família, assegurado o segredo de família, relativas à investigação de paternidade de filhos havidos fora do casamento).	Poder Legislativo	Senador a Patrícia Saboya
Projeto de Lei nº 21/2004.	Proíbe envio de mensagens não solicitadas (spam); estabelece multa; estabelece como nova modalidade do crime de falsidade ideológica a conduta de impedir a identificação do remetente ou o bloqueio automático de mensagens eletrônicas não solicitadas, inserir declaração falsa ou diversa da que deveria constar, com o fim de impossibilitar a identificação da origem ou o rastreamento da mensagem.	Poder Legislativo	Senador Duciomar Costa.
Projeto de Decreto Legislativo (SF) Nº 00390, de 2004	Susta a aplicação do Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança e do Estado, no âmbito da Administração Pública Federal.	Poder Legislativo	Senador Valdir Raupp
Projeto de lei nº 00095, de 2003	Dispõe sobre a privacidade na Internet.	Poder Legislativo	Senador Valmir Amaral
Projeto de lei nº 00463, de 2003	Obriga os provedores de hospedagem da Rede Mundial de Computadores (Internet) a fornecer relação das páginas sob seu domínio, e dá outras providências	Poder Legislativo	Senador Serys Slhessarenko
Projeto de Lei nº 89 de 2003	Altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 - Código Penal e a Lei nº 9296, de 24 de julho de 1996, e dá outras providências. (Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial). (Processo Especial)	Poder Legislativo	Deputado Luiz Piauhylino
Projeto de Lei nº 7.316/2002.	Regulamenta o uso de assinaturas eletrônicas e a prestação de serviços de certificação.	Poder Executivo.	Presidente da República
Projeto de lei nº 00234, de 2002	Dispõe sobre requisitos e condições para o registro de nomes de domínio na rede internet no Brasil.	Poder Legislativo	Senador Waldeck Ornelas
Projeto de lei nº 00088, de 2002	Altera o artigo 225 do Decreto-Lei nº 2848, de 7 de dezembro de 1940 - Código Penal, para adotar a ação pública e segredo de justiça nos crimes contra os costumes.	Poder Legislativo	Senador Lúcio Alcântara
Projeto de Lei nº 3.494/2000.	Altera a lei do *habeas data* (Lei nº 9.507, de 12 de novembro de 1997).	Poder Legislativo	Senado Federal.
Projeto de lei nº 00151, de 2000	Dispõe sobre acesso a informações da Internet, e dá outras providências.	Poder Legislativo	Senador Luiz Estevão
Projeto de lei nº 137 de 2000	Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.	Poder Legislativo	Senador Leomar Quintanilha
Projeto de lei nº 76 de 2000	Define e tipifica os delitos informáticos, e dá outras providências.	Poder Legislativo	Senador Renan Calheiros
Projeto de lei nº 75, de 2000	Dispõe sobre a divulgação, através da Internet, dos dados e informações relativos a licitações realizadas pelos órgãos dos poderes Executivo, Legislativo e Judiciário, em todos os níveis da administração pública.	Poder Legislativo	Deputado Aloizio Mercadante
Projeto de Lei nº 84/1999.	Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.	Poder Legislativo	Deputado Luiz Piauhylino.
Projeto de lei nº 00183, de 1999	Acrescenta artigo ao Código de Processo Penal, determinando os casos de segredo de justiça.	Poder Legislativo	Senador Luzia Toledo
Projeto de lei nº 00674, de 1999	Altera a Lei nº 8666, de 21 de junho de 1993, que dispõe sobre licitações e contratos administrativos, para o fim de determinar aos órgãos e entidades da Administração Pública, sempre que possível, o uso da INTERNET no processo licitatório.	Poder Legislativo	Senador Maria do Carmo Alves
Projeto de Lei nº 1.025/1995.	Acrescenta artigo à Lei nº 8.159/91 e dispõe sobre a administração de arquivos públicos federais relacionados à repressão política.	Poder Legislativo	Deputado Aldo Arantes e outros dois.
Projeto de resolução do senado nº 00084, de 1990	Autoriza a República Federativa do Brasil a ultimar contratação de operação de credito externo, no valor de us 135,000,000.00, (cento e trinta e cinco milhões de dolares norte-americanos), junto ao Banco Interamericano de Desenvolvimento - BID, destinada ao financiamento parcial do projeto hidreletrico de segredo, da companhia paranaense de energia - copel.	Poder Legislativo	Senado Federal - Comissão Assuntos Econômicos

Fonte: Câmara dos Deputados; e Senado. Disponível em: <http://www.camara.gov.br> ; <http://www.senado.gov.br>. Acesso em: 30 ago. 2009.

APÊNDICE B – Normas Relacionadas à Segurança da Informação: Canadá

Constituição Federal

Consolidation of Constitution	Ementa	Origem	Artigos Constituição IAC, 1982	Tradução
Consolidation of Constitution Acts, 1867 to 1982: *Constitution* ACT, 1867 29 mar. 1867 *Constitution* IAC, 1982 Assented a 29 mar. 1982	This consolidation contains the text of the Constitution Act, 1867 (formerly the British North America Act, 1867), together with amendments made to it since its enactment, and the text of the Constitution Act, 1982, as amended since its enactment. The Constitution Act, 1982 contains the Canadian Charter of Rights and Freedoms and other new provisions, including the procedure for amending the Constitution of Canada. Esta consolidação contém o texto da text of the *Constitution Act, 1867* (anteriormente *British North America Act, 1867),* juntamente com as alterações feitas a ela desde a sua promulgação, o texto da *Constitution Act, de 1982*, alterada desde a sua promulgação. A *Constitution Act de 1982* contém a *Carta Canadense dos Direitos e Liberdades* e outras novas disposições, incluindo o processo de alteração da Constituição do Canadá.	Coroa do Reino Unido da Grã-Bretanha e Irlanda Rainha Victoria (UK) e Parlamento Canadense	Canadian Charter of Rights and Freedoms Rights and freedoms in Canada 1. The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.	Carta Canadense dos Direitos e Liberdades. Garantia dos direitos e liberdades 1. A Carta Canadense de Direitos e Liberdades garante os direitos e liberdades em limites razoáveis prescritos por lei como podem ser comprovadamente justificadom em uma sociedade livre e democrática.
			Fundamental freedoms 2. Everyone has the following fundamental freedoms: (a) freedom of conscience and religion; (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; (c) freedom of peaceful assembly; and (d) freedom of association.	Das liberdades fundamentais 2. Toda a pessoa tem as seguintes liberdades fundamentais: (A) liberdade de consciência e de religião; (B) liberdade de pensamento, crença, opinião e de expressão, incluindo a liberdade de imprensa e outros meios de comunicação; (C) à liberdade de reunião pacífica, e (D) à liberdade de associação.
			18. (1) The statutes, records and journals of Parliament shall be printed and published in English and French and both language versions are equally authoritative.	18. (1) Os estatutos (leis), registros e revistas do Parlamento deve ser impresso e publicado em Inglês e Francês e ambas as versões lingüísticas são igualmente oficiais.
			20. (1) Any member of the public in Canada has the right to communicate with, and to receive available services from, any head or central office of an institution of the Parliament or government of Canada in English or French, and has the same right with respect to any other office of any such institution where (a) there is a significant demand for communications with and services from that office in such language; or (b) due to the nature of the office, it is reasonable that communications with and services from that office be available in both English and French.	20. (1) Qualquer membro do público, no Canadá tem o direito de se comunicar com, e para receber os serviços disponíveis a partir de, qualquer órgão ou escritório central de uma instituição do Parlamento ou do governo do Canadá, em Inglês ou Francês, e tem o mesmo direito com relação a qualquer outro cargo de qualquer instituição em que (A) exista uma demanda significativa para comunicações e serviços de escritório nessa linguagem, ou (B) devido à natureza do mandato, é razoável que as comunicações e serviços estejam disponíveis em Inglês e Francês.
			Enforcement of guaranteed rights and freedoms 24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances. Exclusion of evidence bringing administration of justice into disrepute (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.	Execução das liberdades e direitos garantidos 24. (1) Qualquer pessoa cujos direitos ou liberdades, tal como garantidos pela presente Carta, forem violados ou negados pode recorrer a um tribunal de jurisdição competente para a obtenção da solução que o tribunal considere apropriada e justa naquelas circunstâncias. Exclusão das provas levando administração da justiça em descrédito (2) Quando, no âmbito de um litígio na subsecção (1), o tribunal concluiu que as provas foram obtidas de uma forma que violou ou negou quaisquer direitos ou liberdades garantidos pela presente Carta, a prova será excluída, se se provar que, tendo em conta todas as circunstâncias, a admissão de que, no processo traria à administração da justiça em descrédito.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Códigos

Códigos	Ementa	Tradução	Origem	Aspecto da Segurança Informação	Tradução
Criminal Code (R.S., 1985, c. C-46) -Act current to January 1st, 2003	An Act respecting the Criminal Law 1. This Act may be cited as the Criminal Code.	Uma lei respeitando o Direito Penal 1. Esta Lei pode ser citada como o *Código Penal.*	Parlamento	"terrorism offence" means (a) an offence under any of sections 83.02 to 83.04 or 83.18 to 83.23, (b) an indictable offence under this or any other Act of Parliament committed for the benefit of, at the direction of or in association with a terrorist group, (c) an indictable offence under this or any other Act of Parliament where the act or omission constituting the offence also constitutes a terrorist activity, or (d) a conspiracy or an attempt to commit, or being an accessory after the fact in relation to, or any counselling in relation to, an offence referred to in paragraph (a), (b) or (c); 140. (1) Every one commits public mischief who, with intent to mislead, causes a peace officer to enter on or continue an investigation by (a) making a false statement that accuses some other person of having committed an offence; (b) doing anything intended to cause some other person to be suspected of having committed an offence that the other person has not committed, or to divert suspicion from himself; (c) reporting that an offence has been committed when it has not been committed; or (d) reporting or in any other way making it known or causing it to be made known that he or some other person has died when he or that other person has not died "electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing; Interception	"ataque terrorismo" significa (A) um delito ao abrigo de quaisquer das secções 83.02 a 83.04 ou 83.18 a 83.23, (B) um delito ao abrigo da presente ou qualquer outra lei do Parlamento cometido em benefício de, no sentido de ou em associação com um grupo terrorista, (C) um delito ao abrigo da presente ou qualquer outra lei do Parlamento em que o ato ou omissão constitutivos da infração constitui também uma atividade terrorista, ou (D) uma conspiração ou uma tentativa de cometer, ou ser um acessório após o fato, em relação a, ou em relação a qualquer aconselhamento, uma infração prevista no parágrafo (a), (b) ou (c); 140. (1) Todo servidor comete dano público, com intenção de enganar, alterar a tranqüilidade do serviço para entrar em ou continuar uma investigação por (a) fazer uma falsa declaração que acusa alguma outra pessoa de ter cometido um delito; b) fazer qualquer coisa com pretensão de gerar suspeita de que outra pessoa cometeu sem tê-lo feito, ou desviar suspeita dele; (c) informar que um delito ocorreu quando não ocorreu; ou (d) informar ou fazer com que se torne conhecido que ele ou alguma outra pessoa morreram quando ele ou aquela outra pessoa não morreram. "eletro-magnéticos", acústico, mecânico ou outros dispositivos, qualquer dispositivo ou equipamento que é usado ou é susceptível de ser utilizado para interceptar uma comunicação privada, mas não inclui uma prótese utilizada para corrigir subnormal audição do usuário a não mais superior a audição normal; Intercepção 184. (1) Toda pessoa que, por meio de qualquer meio eletro-magnéticos, acústico, mecânico ou outro dispositivo, deliberadamente intercepta uma comunicação privada é culpado de um delito acusável e passíveis de prisão por um período não superior a cinco anos.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Códigos	Ementa	Tradução	Origem	Aspecto da Segurança Informação	Tradução
				184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years. ELECTRONIC DOCUMENTS Definitions 841. The definitions in this section apply in this section and in sections 842 to 847. "data" means representations of information or concepts, in any form. "electronic document" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print-out or other output of the data and any document, record, order, exhibit, notice or form that contains the data. Dealing with data in court 842. Despite anything in this Act, a court may create, collect, receive, store, transfer, distribute, publish or otherwise deal with electronic documents if it does so in accordance with an Act or with the rules of court. Transfer of data 843. (1) Despite anything in this Act, a court may accept the transfer of data by electronic means if the transfer is made in accordance with the laws of the place where the transfer originates or the laws of the place where the data is received. Time of filing (2) If a document is required to be filed in a court and the filing is done by transfer of data by electronic means, the filing is complete when the transfer is accepted by the court. Documents in writing 844. A requirement under this Act that a document be made in writing is satisfied by the making of the document in electronic form in accordance with an Act or the rules of court. Signatures 845. If this Act requires a document to be signed, the court may accept a signature in an electronic document if the signature is made in accordance with an Act or the rules of court. Oaths 846. If under this Act an information, an affidavit or a solemn declaration or a statement under oath or solemn affirmation is to be made by a person, the court may accept it in the form of an electronic document if (a) the person states in the electronic document that all matters contained in the information, affidavit, solemn declaration or statement are true to his or her knowledge and belief; (b) the person before whom it is made or sworn is authorized to take or receive informations, affidavits, solemn declarations or statements and he or she states in the electronic document that the information, affidavit, solemn declaration or statement was made under oath, solemn declaration or solemn affirmation, as the case may be; and (c) the electronic document was made in accordance with the laws of the place where it was made. Copies 847. Any person who is entitled to obtain a copy of a document from a court is entitled, in the case of a document in electronic form, to obtain a printed copy of the electronic document from the court on payment of a reasonable fee determined in accordance with a tariff of fees fixed or approved by the Attorney General of the relevant province. Condition for remote appearance 848. Despite anything in this Act, if an accused who is in prison does not have access to legal advice during the proceedings, the court shall, before permitting the accused to appear by a means of communication that allows the court and the accused to engage in simultaneous visual and oral communication, be satisfied that the accused will be able to understand the proceedings and that any decisions made by the accused during the proceedings will be voluntary.	DOCUMENTOS ELETRÔNICOS Definições 841. As definições nesta seção aplicam nesta seção e nas seções 842 a 847. "dados" significa representações de informações ou conceitos, em qualquer forma. "documento eletrônico" significa dados que são registrados ou armazenaram em qualquer meio em ou por um sistema de computador ou outro dispositivo semelhante e podendo ser lido ou percebido por uma pessoa ou um sistema de computador ou outro dispositivo semelhante. Inclui uma exibição, impressão ou outra produção dos dados e qualquer documento, registro, ordem, exibição, notificação ou forma que contêm os dados. Lidando com dados no tribunal 842. Sem prejuízo desta lei, um tribunal pode criar, colecionar, receber, armazenar, transferir, distribuir, publicar ou tratar documentos eletrônicos se assim fizer conforme uma lei ou com as regras de tribunal. Transferência de dados 843. (1) Sem prejuízo desta lei, um tribunal pode aceitar a transferência de dados através de meios eletrônicos se a transferência é feita conforme as leis do lugar onde a transferência origina ou as leis do lugar onde os dados são recebidos. Arquivamento (2) se um documento é exigido ser arquivado em um tribunal e o arquivamento é feito por transferência de dados através de meios eletrônicos, o arquivamento estará completo quando a transferência é aceita pelo tribunal. Documentos por escrito 844. Uma exigência desta lei de um documento por escrito pode ser satisfeito por documento em forma eletrônica conforme a lei ou as regras de tribunal. Assinaturas 845. Se esta lei exigir assinatura de um documento, o tribunal pode aceitar uma assinatura em um documento eletrônico se a assinatura é feita conforme a lei ou as regras de tribunal. Juramentos 846. Se ao abrigo desta lei uma informação, uma atestação ou uma declaração solene ou uma declaração sob juramento ou afirmação solene feitas por uma pessoa, o tribunal pode aceitar isto na forma de um documento eletrônico se (a) a pessoa declara no documento eletrônico que todos os assuntos contiveram na informação, atestação, declaração solene ou declaração são verdadeiros para conhecimento e convicção; (b) a pessoa antes de quem é feito ou é jurado é autorizado levar ou receber informações, atestações, declarações solenes ou declarações e ele ou ela declaram no documento eletrônico que foram feitas a informação, atestação, declaração solene ou declaração sob juramento, declaração solene ou afirmação solene, como pode ser o caso; e (c) o documento eletrônico foi feito conforme as leis do lugar onde foi feito. Cópias 847. Qualquer pessoa que é intitulada para obter uma cópia de um documento de um tribunal é intitulada, no caso de um documento em forma eletrônica, obter uma cópia impressa do documento eletrônico do tribunal em pagamento de uma taxa razoável determinada por uma tarifa de fixa ou aprovada pelo Advogado Geral da província pertinente. Condição de acesso remoto 848. Sem prejuízo desta lei, se um acusado que está em prisão não tiver acesso a aconselhamento legal durante os procedimentos, o tribunal deve, antes de permitir que o acusado apareça por um meio de comunicação que permite para o tribunal e para o acusado terem comunicação visual e oral simultâneas, os acusados poderão entender os procedimentos e qualquer decisão de acusação durante os procedimentos será voluntário.
Não há código civil, leis esparsas, direito comum. Exceção da província Québec.					

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Leis

Leis	Ementa	Tradução	Origem	Artigos Segurança Informação	Tradução
Public Safety Act, 2002 (2004, c. 15) -Assented to May 6th, 2004 -Act current to May 27th, 2009	An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Public Safety Act, 2002.	Uma Lei que emenda outras leis do Canadá, e ordenar medidas de implementação da Convenção de Armas Tóxicas e Biológicas para aumentar segurança pública. A Majestade, por e com o conselho e consentimento do Senado e da Câmara dos Comuns do Canadá, ordena: 1. Esta Lei pode ser citada como Lei de Segurança Pública, 2002.	Parlamento	PART 17 PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 98. [Amendments]	PART 17 LEI DE PROTEÇÃO À INFORMAÇÃO PESSOAL E DOCUMENTOS ELETRÔNICOS 98. [Emendas]
Public Service Employment Act (2003, c. 22, ss. 12, 13) Assented to November 7th, 2003 Act current to May 27th, 2009	An Act respecting employment in the public service Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Public Service Employment Act.	Uma lei sobre emprego no serviço público Sua Majestade, pelo e com o conselho e consentimento do Senado e da Câmara dos Comuns do Canadá, estabelece o seguinte: 1. Esta Lei pode ser citada como Lei do Serviço Público	Parlamento	Access to Facilities and Information Access by Commission 135. Deputy heads and employees shall provide the Commission with any facilities, assistance, information and access to their respective offices that the Commission may require for the performance of its duties.	Acesso aos Recursos e Informação Acesso pela Comissão 135. Chefes Adjuntos e funcionários devem fornecer à Comissão todas as facilidades, dar assistência, e acesso às informações dos respectivos cargos que a Comissão necessite para o desempenho das suas funções.
Anti-terrorism Act (2001, c. 41) -Assented to December 18th, 2001 -Act current to May 27th, 2009	An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Anti-terrorism Act.	Uma lei que altera o Código Penal, a Lei de Ato Secreto, e a Lei de Evidências do Canadá, a Lei de Processo Penal (Lavagem de Dinheiro) e outras leis, e medidas para registrar instituições de caridade, a fim de combater o terrorismo Sua Majestade, pelo e com o conselho e consentimento do Senado e da Câmara dos Comuns do Canadá, estabelece o seguinte: 1. Esta Lei pode ser citada como a Lei Anti-terrorismo.	Parlamento	PART 6 REGISTRATION OF CHARITIES — SECURITY INFORMATION 113. The Charities Registration (Security Information) Act is enacted as follows: [See Charities Registration (Security Information) Act]	PARTE 6 REGISTO DE INSTITUIÇÃO CARIDADE - SEGURANÇA INFORMAÇÃO 113. A Lei de Registro de Instituições de Caridade (Segurança da Informação) é promulgada como se segue: [Ver Lei de Registro de Instituições de Caridade (Segurança da Informação)]
Personal Information Protection and Electronic Documents Act (2000, c. 5) -Assented to April 13th, 2000 -Act current to June 2nd, 2009 (Ato atual 2 de junho de 2009)	An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Personal Information Protection and Electronic Documents Act.	Uma Lei para apoiar e promover o comércio eletrônico com proteção das informações pessoais que são recolhidas, utilizadas ou divulgadas, em certas circunstâncias, prevendo a utilização de meios eletrônicos para transmitir ou gravar informações ou transações, emendando a Lei de Evidências do Canadá, a Lei de Instrumentos Estatutário e a Lei de Revisão de Estatuto Sua Majestade, por e com o conselho e consentimento do Senado e Câmara dos Comuns de Canadá, ordena como segue: 1. Esta Lei pode ser citada como Lei de Proteção à Informação Pessoal e Documentos Eletrônicos.	Parlamento	"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. 4. (1) This Part applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities; or (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. (2) This Part does not apply to (a) any government institution to which the Privacy Act applies; (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.	"informação pessoal" é uma informação que torna identificável um indivíduo, mas não inclui o nome, títulos ou endereço profissional ou número de telefone de emprego em uma organização. 3. O propósito desta Parte é o de estabelecer, em uma era na qual a tecnologia facilita a circulação e troca de informação, regras para administrar o armazenamento, uso e revelação de informação pessoal até os limites do direito à privacidade de indivíduos em relação à informação pessoal e a necessidade de organizações para armazenar, usar ou descobrir informação pessoal para propósitos que uma pessoa mediana consideraria apropriada nas circunstâncias. 4. (1) esta Parte aplica a toda organização em relação à informação pessoal que (a) a organização armazena, usa ou descobre no curso de atividades comerciais; ou (b) é sobre um empregado da organização e que a organização armazena, usa ou descobre com relação à operação de um trabalho federal, empreendimento ou negócio. (2) esta Parte não aplica (a) à instituição de governo para a qual a Lei de Privacidade se aplica; (b) à informação pessoal que o indivíduo armazena, usa ou descobre para propósitos pessoais ou domésticos e não armazena, usa ou descobre para qualquer outro propósito; ou (c) à informação pessoal que a organização armazena, usa ou descobre para propósitos jomalísticos, artísticos ou literários e não armazena, usa ou descobre para qualquer outro propósito.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Leis	Ementa	Tradução	Origem	Artigos Segurança Informação	Tradução
Public Servants Disclosure Protection Act (2005, c. 46) Assented to November 25th, 2005 Act current to May 20th, 2009	An Act to establish a procedure for the disclosure of wrongdoings in the public sector, including the protection of persons who disclose the wrongdoings Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Public Servants Disclosure Protection Act.	Uma Lei para estabelecer um procedimento para a revelação de erros no setor público, inclusive a proteção de pessoas que revelam os erros, Sua Majestade dela, por e com o conselho e consentimento do Senado e Casa de Câmara dos Comuns de Canadá, ordena: 1. Esta Lei pode ser citada como Lei de Proteção à Revelação de Servidores Públicos.	Parlamento	CONSEQUENTIAL AMENDMENTS Access to Information Act 55. [Amendment] 55.1 [Amendment] Canada Evidence Act 56. [Amendment] Federal Courts Act 56.1 [Amendment] Financial Administration Act 56.2 [Amendment] 56.3 [Amendment] 56.4 [Amendment] Official Languages Act 56.5 [Amendment] Personal Information Protection and Electronic Documents Act 57. [Amendment] Privacy Act	EMENDAS CONSEQÜENTES Lei de Acesso à Informação 55. [Emenda] 55.1 [emenda] Canadá Evidência Ato 56. [Emenda] Lei dos Tribunais Federais 56.1 [emenda] Lei de Administração Financeira 56.2 [emenda] 56.3 [emenda] 56.4 [emenda] Lei de Idioma Oficial 56.5 [emenda] Lei de Proteção de Informação Pessoal e de Documentos Eletrônicos 57. [Emenda] Lei de Privacidade
Canada Elections Act (2000, c. 9) -Assented to May 31st, 2000 -Act current to May 27th, 2009	An Act respecting the election of members to the House of Commons, repealing other Acts relating to elections and making consequential amendments to other Acts Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Canada Elections Act.	Uma lei correspondente à eleição dos membros da Câmara dos Comuns; revoga e emenda outras leis relativas a eleições. Sua Majestade, por e com o conselho e consentimento do Senado e da Câmara dos Comuns do Canadá, ordena: 1. Esta lei pode ser citada como Lei de Eleições do Canadá	Parlamento	Electronic voting process 18.1 The Chief Electoral Officer may carry out studies on voting, including studies respecting alternative voting means, and may devise and test an electronic voting process for future use in a general election or a by-election. Such a process may not be used for an official vote without the prior approval of the committees of the Senate and of the House of Commons that normally consider electoral matters. 44. (1) The Chief Electoral Officer shall maintain a register of Canadians who are qualified as electors, to be known as the Register of Electors. 46.1 For the purpose of assisting the Chief Electoral Officer in updating the Register of Electors, the Minister of National Revenue may, on a return of income referred to in subsection 150(1) of the Income Tax Act, request that an individual who is filing a return of income under paragraph 150(1)(d) of that Act indicate in the return whether he or she is a Canadian citizen. 540. (1)…Documents relating to Register of Electors:(2) The Chief Electoral Officer shall, for at least two years after receiving them, retain in his or her possession, on film or in electronic form, all documents that relate to the updating of the Register of Electors.	Processo de votação eletrônico 18.1 o Chefe do Cartório Eleitoral pode fazer estudos de votação, inclusive estudos com respeito a meios de votação alternativas, e podendo inventar e testar processos de votação eletrônico para uso futuro em uma eleição geral ou por eleição. Esse processo não poderá ser usado como voto oficial sem a aprovação anterior dos comitês do Senado e da Casa de Câmara dos Comuns que normalmente consideram assuntos eleitorais. 44. (1) O Chefe do Cartório Eleitoral manterá um registro dos eleitores canadenses, conhecido como Registro de Eleitores. 46.1 A fim de ajudar o Chefe do Cartório Eleitoral a atualizar o Registro de Eleitores, o Ministro Nacional de Imposto de Renda pode, sobre a declaração de renda referida na subseção 150(1) da Lei de Imposto de Renda, arquivar sobre na declaração se o indivíduo é ou cidadão canadense. 540. (1) Documentos relativos ao Registro de Eleitores (2) o Chefe do Cartório Eleitoral deve, durante pelo menos dois anos depois de receber, reter, em microfilme ou em forma eletrônica, todos os documentos que relacionam à atualização do Registro de Eleitores.
Telecommunications Act (1993, c. 38) -Assented a 23. De junho de 1993 -Act current to May 27th, 2009	Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows: 1. This Act may be cited as the Telecommunications Act.	Sua Majestade, pelo e com o consentimento do Senado e da Câmara dos Comuns do Canadá, estabelece o seguinte: 1. Esta Lei pode ser citada como a Lei das Telecomunicações	Parlamento	"intelligence" « information » "intelligence" means signs, signals, writing, images, sounds or intelligence of any nature; "telecommunications" means the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system; 7. It is hereby affirmed that telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty and that the Canadian telecommunications policy has as its objectives (a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions; (f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective; (i) to contribute to the protection of the privacy of persons.	"inteligência" «Informação» "inteligência" significa sinais, escrita, imagens, sons ou informações de qualquer natureza; "telecomunicações", a emissão, transmissão ou recepção de informações por qualquer fio, cabo, rádio, meios ópticos ou outros meios sistema eletromagnéticos, ou por qualquer outro sistema técnico; 7. É afirmado por este meio que telecomunicações desempenham um papel essencial na manutenção da identidade e da soberania do Canadá e que as políticas das telecomunicações canadenses têm como objetivos (A) facilitar o desenvolvimento ordenado em todo o Canadá de um sistema de telecomunicações que sirva para proteger, enriquecer e fortalecer o tecido social e econômico do Canadá e as suas regiões; (F) favorecer o crescente mercado para a prestação de serviços de telecomunicações e garantir que a regulamentação, quando necessária, seja eficiente e eficaz; (I) contribuir para a proteção da privacidade dos indivíduos.
Security of Information Act (R.S., 1985, c. O-5) Act current to May 27th, 2009	An Act respecting the security of information 1. This Act may be cited as the Security of Information Act	Uma lei relacionada à segurança das informações 1. Esta Lei pode ser citada como a Lei de Segurança da Informação.	Parlamento	2. (1) In this Act, (4) For greater certainty, subsection 83.01(2) of the Criminal Code applies for the purposes of the definitions "terrorist activity" and "terrorist group" in subsection (1). 3. (1) For the purposes of this Act, a purpose is prejudicial to the safety or interests of the State if a person (a) commits, in Canada, an offence against the laws of Canada or a province that is punishable by a maximum term of imprisonment of two years or more in order to advance a political, religious or ideological purpose, objective or cause or to benefit a foreign entity or terrorist group; (b) commits, inside or outside Canada, a terrorist activity; (c) causes or aggravates an urgent and critical situation in Canada that (i) endangers the lives, health or safety of Canadians, or (ii) threatens the ability of the Government of Canada to preserve the sovereignty, security or territorial integrity of Canada; (d) interferes with a service, facility, system or computer program, whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada;	2. (1) Na presente Lei (4) Para maior segurança, subsecção 83.01 (2) do Código Penal será aplicada para os efeitos das definições "atividade terrorista" e de "grupo terrorista" na subsecção (1). 3. (1) Para efeitos da presente Lei, é um efeito prejudicial para a segurança ou interesses do Estado, se uma pessoa (A) comete, no Canadá, um crime contra as leis do Canadá ou de uma província que é punível com uma pena máxima de prisão de dois anos ou mais, por incentivar objetivos ou causas política, religiosa ou ideológica, ou beneficiar uma entidade estrangeira ou grupo terrorista; (B) comete, dentro ou fora do Canadá, uma atividade terrorista; (C) causa ou agrava uma situação crítica e urgente que no Canadá (i) coloque em perigo a vida, a saúde ou a segurança dos canadenses, ou (ii) ameace a capacidade do Governo do Canadá para preservar a soberania, a segurança ou a integridade territorial do Canadá; (D) interferir com um serviço, função, sistema ou programa de computador, quer sejam públicos ou privados, ou o seu funcionamento, de uma forma que tenha impacto negativo significativo sobre a saúde, segurança ou atividades econômicas ou financeiras no bem-estar do povo de Canadá ou no funcionamento de qualquer governo no Canadá;

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Leis	Ementa	Tradução	Origem	Artigos Segurança Informação	Tradução
Security of Information Act (R.S., 1985, c. O-5) Act current to May 27th, 2009				(g) impairs or threatens the military capability of the Canadian Forces, or any part of the Canadian Forces; (h) interferes with the design, development or production of any weapon or defence equipment of, or intended for, the Canadian Forces, including any hardware, software or system that is part of or associated with any such weapon or defence equipment; (i) impairs or threatens the capabilities of the Government of Canada in relation to security and intelligence; 4.(3) Every person who receives any secret official code word, password, sketch, plan, model, article, note, document or information, knowing, or having reasonable ground to believe, at the time he receives it, that the code word, password, sketch, plan, model, article, note, document or information is communicated to him in contravention of this Act, is guilty of an offence under this Act, unless he proves that the communication to him of the code word, password, sketch, plan, model, article, note, document or information was contrary to his desire.	(G) prejudicar ou ameaçar a capacidade militar ou qualquer parte das Forças Canadenses. (H) interferir na concepção, desenvolvimento ou produção de qualquer arma ou equipamento de defesa, ou destinados às Forças Canadenses, incluindo hardware, software ou sistema que seja parte ou associada a qualquer arma ou equipamento de defesa; (I) prejudicar ou ameaçar a capacidade do Governo do Canadá em matéria de segurança e de inteligência (informação); 4. (3) Toda pessoa que recebe qualquer código secreto oficial, palavra, senha, esboço, plano, modelo, artigo, nota, documento ou informação, sabendo ou tendo motivos razoáveis para crer, no momento em que recebeu que o código, palavra, senha, esboço, plano, modelo, artigo, nota, documento ou informação que lhe é comunicada, em violação da presente lei, é culpado de uma infração, nos termos desta Lei, salvo se provar que a comunicação com o código, palavra, senha, esboço, plano, modelo, artigo, nota, documento ou informação era contrário ao seu desejo.
Canadian Security Intelligence Service Act (R.S., 1985, c. C-23) Act current to May 27th, 2009	An Act to establish the Canadian Security Intelligence Service 1. This Act may be cited as the Canadian Security Intelligence Service Act.	Uma lei para estabelecer o Serviço de Inteligência e Segurança Canadense 1. Esta Lei pode ser citada como Serviço de Inteligência (Informação) e Segurança Canadense	Parlamento	2. In this Act, "threats to the security of Canada" means (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage. 19. (1) Information obtained in the performance of the duties and functions of the Service under this Act shall not be disclosed by the Service except in accordance with this section.	2. Na presente lei, "ameaças à segurança do Canadá" significa (A) espionagem ou sabotagem contra o Canadá ou prejudicial para os interesses do Canadá ou atividades dirigidas em apoio dessa espionagem ou sabotagem. 19. (1) As informações obtidas no desempenho das atribuições e funções do Serviço de acordo com esta lei não devem ser divulgadas pelo Serviço exceto em conformidade com esta secção.
Access to Information Act (R.S., 1985, c. A-1) Act current to May 27th, 2009	An Act to extend the present laws of Canada that provide access to information under the control of the Government of Canada 1. This Act may be cited as the Access to Information Act. PURPOSE OF ACT 2. (1) The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government. (2) This Act is intended to complement and not replace existing procedures for access to government information and is not intended to limit in any way access to the type of government information that is normally available to the general public.	Uma lei que expande as leis do Canadá sobre acesso à informação,sob o controle do Governo do Canadá 1. Esta Lei pode ser citada como Lei de Acesso à Informação OBJETIVO DO ACTO 2. (1) o propósito desta Lei é estender as leis do Canadá para prover o direito de acesso à informação em registros sob o controle de uma instituição de governo conforme os princípios que as informações de governo devem estar disponíveis ao público, que exceções necessárias ao direito de acesso devem ser limitadas e específica e que as decisões sobre a divulgação de informações da administração devem ser revistas independentemente do governo. (2) Esta lei se destina a complementar e não substitui os procedimentos existentes para o acesso a informações governamentais e não se destina a limitar de forma alguma o acesso ao tipo de informação que o governo normalmente dispõe para o público em geral.	Parlamento	4. (1) Subject to this Act, but notwithstanding any other Act of Parliament, every person who is (a) a Canadian citizen, or (b) a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act, has a right to and shall, on request, be given access to any record under the control of a government institution. Extension of right by order (2) The Governor in Council may, by order, extend the right to be given access to records under subsection (1) to include persons not referred to in that subsection and may set such conditions as the Governor in Council deems appropriate. 6. A request for access to a record under this Act shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution with a reasonable effort to identify the record. 16. (1) The head of a government institution may refuse to disclose any record requested under this Act that contains (b) information relating to investigative techniques or plans for specific lawful investigations; 20. (1) Subject to this section, the head of a government institution shall refuse to disclose any record requested under this Act that contains (a) trade secrets of a third party; (b) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party; (c) information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party; or (d) information the disclosure of which could reasonably be expected to interfere with contractual or other negotiations of a third party.	4. (1) É sujeito a essa Lei, mas sem prejuízo de qualquer outra Lei do Parlamento, toda pessoa que é (A) cidadão canadense, ou (B) residente permanente, na acepção da subsecção 2 (1) do *Immigration and Refugee Protection Act*, tem o direito de, e devem, requerer, acesso a qualquer registro sob o controle de uma instituição governamental. Extensão do direito, por despacho (2) O Governador em Conselho pode, ordenar, extensão do direito de acesso aos registros na subsecção (1) para incluir as pessoas não mencionados na referida subseção e pode definir as condições que considere adequadas. 6. O pedido de acesso a um registro ao abrigo desta lei deve ser feito por escrito à instituição governamental que tem controle do registro e deve fornecer detalhes suficientes para permitir que o funcionário da instituição possa identificar o registro. 16. (1) O chefe de uma instituição governamental pode se recusar a divulgar qualquer registro solicitado ao abrigo desta lei que contenha (B) as informações relativas às técnicas investigativas ou planos para investigações legais específicas; 20. (1) Sujeito a esta seção, o chefe de uma instituição governamental deve se recusar a divulgar qualquer registro solicitado ao abrigo desta Lei que contenha (A) segredos comerciais de um terceiro; (B) informação financeira, comercial, científica ou técnica confidencial fornecida a uma instituição governamental por um terceiro, e é tratada de maneira consistente em formato confidencial pelo terceiro; (C) a divulgação de informações que razoavelmente possam resultar em perda financeira ou material, prejudicar a posição competitiva de um terceiro; ou (D) a divulgação de informações que possam interferir em direitos contratuais ou de outras negociações de um terceiro.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Leis	Ementa	Tradução	Origem	Artigos Segurança Informação	Tradução
Privacy Act (R.S., 1985, c. P-21) Act current to May 27th, 2009	An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves 1. This Act may be cited as the Privacy Act. 2. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.	Uma lei que expande as leis do Canadá sobre proteção da privacidade das pessoas e que dêem a elas o direito de acesso às informações pessoais sobre si mesmos. 1. Esta Lei pode ser citada como a Lei de Privacidade. 2. O objetivo desta lei é expandir as atuais leis do Canadá que protegem a privacidade das pessoas no que diz respeito às informações pessoais sobre si próprias guardadas em instituição governamental e que forneçam ás mesmas o direito de acesso a essas informações.	Parlamento	3. In this Act, "personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, 4. No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution. 5. (2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected. 6. (1) Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information. (2) A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible. (3) A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information. 7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2). 12. (1) Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution. 17. (1) Subject to any regulations made under paragraph 77(1)(o), where an individual is to be given access to personal information requested under subsection 12(1), the government institution shall (a) permit the individual to examine the information in accordance with the regulations; or (b) provide the individual with a copy thereof. 26. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) about an individual other than the individual who made the request, and shall refuse to disclose such information where the disclosure is prohibited under section 8.	3. Na presente Lei, "informações pessoais" são as informações que identificam um indivíduo, gravada em qualquer suporte, incluindo, sem limitar a generalidade do exposto acima, (A) informações relativas à raça, nacionalidade ou origem étnica, cor, religião, idade ou estado civil do indivíduo, (B) informações relativas à educação ou a saúde, criminal ou histórico de emprego do indivíduo ou de informações relativas às operações financeiras em que o indivíduo tem se envolvido, (C) qualquer número de identificação, símbolo ou outro especial atribuído ao indivíduo, (D) o endereço, impressões digitais ou tipo de sangue do indivíduo, 4. Nenhuma informação pessoal é recolhida por uma instituição governamental, salvo se relacionada diretamente a um programa ou atividade operacional da instituição. 5. (2) Uma instituição governamental deve informar qualquer indivíduo que a instituição recolhe informações pessoais sobre ele e a finalidade dessa ação. 6. (1) As informações pessoais que tenham sido utilizadas por uma instituição governamental para uma finalidade administrativa, devem ser mantidas pela instituição por um período de tempo após utilizadas como pode ser prescrito pelo regulamento que o indivíduo a quem se refere a informação tem possibilidade razoável de obter o acesso à informação. (2) A instituição do governo tomará todas as medidas razoáveis para assegurar que as informações pessoais que são utilizadas para uma finalidade administrativa é precisa, atualizada e completa quanto possível. (3) A instituição do governo deve dispor de informações pessoais sob o controlo da instituição, de acordo com os regulamentos e de acordo com as diretrizes emitidas pelo ministro designado em relação à eliminação dessa informação. 7. As informações pessoais sob o controle de uma instituição governamental, não deve, sem o consentimento da pessoa a quem se refere, ser utilizado pela instituição, exceto (A) para a finalidade para a qual a informação foi obtida ou compilados pela instituição ou para uma utilização coerente com essa finalidade, ou (B) para uma finalidade para a qual a informação pode ser divulgada para a instituição na subsecção 8 (2). 12. (1) Sem prejuízo do disposto na presente Lei, todo indivíduo que é um cidadão canadense ou residente permanente na acepção da subsecção 2 (1) do Immigration and Refugee Protection Act tem o direito de, e devem, a pedido, ter acesso (A) a quaisquer informações pessoais sobre o indivíduo contidas em um banco, e (B) quaisquer outras informações pessoais sobre o indivíduo sob o controlo de uma instituição governamental em relação à qual o indivíduo é fornece informações específicas sobre a localização das informações de modo a tomá-lo razoavelmente restaurável pelo governo instituição. 17. (1) Sem prejuízo de quaisquer regulamentos feitos nos termos do n. º 77 (1) (o), quando um indivíduo está a ser dado acesso a informações pessoais solicitadas na subsecção 12 (1), a instituição governamental deve (A) permitir ao indivíduo a analisar as informações em conformidade com os regulamentos, ou (B) fornecer o indivíduo com uma cópia. 26. O chefe de uma instituição governamental pode recusar-se a divulgar qualquer informação pessoal solicitada na subsecção 12 (1) sobre um indivíduo que não seja a pessoa que fez o pedido, e deve recusar-se a divulgar tais informações sempre que a divulgação seja proibida nos termos da secção 8.
Radiocommunication Act (R.S., 1985, c. R-2) Act current to May 27th, 2009 Atual Lei de 27. De maio de 2009	An Act respecting radiocommunication in Canada 1. This Act may be cited as the Radiocommunication Act.	Uma lei sobre radiocomunicação no Canadá 1. Esta Lei pode ser citada como a Lei de Radiocomunicações.	Parlamento	2. In this Act, "radiocommunication" or "radio" means any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by means of electromagnetic waves of frequencies lower than 3 000 GHz propagated in space without artificial guide; 9. (1) No person shall (a) knowingly send, transmit or cause to be sent or transmitted any false or fraudulent distress signal, message, call or radiogram of any kind; (b) without lawful excuse, interfere with or obstruct any radiocommunication;	2. Na presente lei, "radiocomunicações" ou "rádio" é qualquer transmissão, emissão ou recepção de sinais, sinais, escrita, imagens, sons ou informações de qualquer natureza por meio de ondas eletromagnéticas de freqüências inferiores a 3 000 GHz que se propagam pelo espaço sem guias artificiais; 9. (1) Nenhuma pessoa deve (A) inadvertidamente enviar, transmitir ou provocar o envio ou transmissão de qualquer sinal, mensagem, chamada ou radiograma falso ou fraudulento de qualquer espécie; (B) sem justificativa legal, obstruir ou interferir qualquer radiocomunicação;

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Leis	Ementa	Tradução	Origem	Artigos Segurança Informação	Tradução
National Defence Act (R.S., 1985, c. N-5) Act current to May 27th, 2009	An Act respecting national defence 1. This Act may be cited as the National Defence Act.	Uma lei sobre defesa nacional 1. Esta Lei pode ser citada como a Lei de Defesa Nacional.	Parlamento	"foreign intelligence" means information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security. "global information infrastructure" includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks. 75. Every person who (a) improperly holds communication with or gives intelligence to the enemy, (b) without authority discloses in any manner whatever any information relating to the numbers, position, materiel, movements, preparations for movements, operations or preparations for operations of any of Her Majesty's Forces or of any forces cooperating therewith, (c) without authority discloses in any manner whatever any information relating to a cryptographic system, aid, process, procedure, publication or document of any of Her Majesty's Forces or of any forces cooperating therewith, (e) gives a parole, watchword, password, countersign or identification signal different from that which he received, (j) does or omits to do anything with intent to prejudice the security of any of Her Majesty's Forces or of any forces cooperating therewith, is guilty of an offence and on conviction, if the person acted traitorously, shall be sentenced to imprisonment for life, and in any other case, is liable to imprisonment for life or to less punishment. 273.64 (1) The mandate of the Communications Security Establishment is (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.	"inteligência estrangeira" significa dados ou informações sobre as capacidades, intenções ou atividades de um indivíduo estrangeiro, estado, organização ou grupo terrorista relacionados com assuntos internacionais, defesa ou segurança. "informação global das infra-estruturas" inclui emissões eletromagnéticas, sistemas de comunicações, sistemas de tecnologia da informação e redes, bem como quaisquer dados ou informação técnica exercida, contidas ou relacionadas com essas emissões, sistemas ou redes. 75. Toda pessoa que (a) inadvertidamente mantém comunicação com ou dá informação ao inimigo, (b) sem autoridade descobre qualquer maneira qualquer informação relativa aos números, posição, material, movimentos, preparações para movimentos, operações ou preparações para operações de quaisquer das Forças da Majestade ou de qualquer força que coopera, (c) sem autoridade descobre qualquer informação relativa a um sistema de criptografia, ajuda, processo, procedimento, publicação ou documento de quaisquer das Forças da Majestade ou de qualquer força que coopera, (e) dá uma liberdade condicional, senha, contra-senha, contra-senha ou sinal de identificação diferente do que ele recebeu, (j) faz ou omite qualquer coisa com intenção de prejudicar a segurança de quaisquer das Forças da Majestade ou de qualquer força que coopera, é culpado de um crime e em convicção, se a pessoa agiu traiçoeiramente, será condenada a prisão ou pena mais leve. 273.64 (1) Cabe ao Comitê de Comunicações de Segurança (A) adquirir e usar informação de infra-estrutura global para fornecer inteligência estrangeira, de acordo com prioridades de inteligência do Governo do Canadá; (B) aconselhar, orientar e ajudar a garantir serviços para a proteção de informação eletrônica e de informação infra-estruturas de grande importância para o Governo do Canadá, e (C) prestar assistência técnica e operacional para a aplicação da lei federal e agências de segurança no desempenho das suas funções legais.
Copyright Act (R.S., 1985, c. C-42) -Act current to May 27th, 2009	An Act respecting copyright 1. This Act may be cited as the Copyright Act.	Uma lei sobre direitos autorais 1. Esta Lei pode ser citada como Lei de Direitos Autorais.	Parlamento	2. (1) In this Act, "computer program" means a set of instructions or statements, expressed, fixed, embodied or stored in any manner, that is to be used directly or indirectly in a computer in order to bring about a specific result;	2. (1) Na presente lei "programa de computador" significa um conjunto de instruções ou declarações, expressas, fixos, incorporados ou armazenadas sob qualquer forma, para ser usado diretamente ou indiretamente em um computador, a fim de trazer um resultado específico;

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Decretos (Regulamentos)

Decretos	Ementa	Tradução	Origem	Artigos Segurança Informação	
Electronic Alternatives Regulations for the Purposes of Subsection 254(1) of the Canada Labour Code (SOR/2008-115) Registration April 17, 2008	Electronic Alternatives Regulations for the Purposes of Subsection 254(1) of the Canada Labour Code The Minister of Labour, as the responsible authority for the Canada Labour Code in accordance with the definition "responsible authority" in subsection 31(1) of the Personal Information Protection and Electronic Documents Act, pursuant to section 50 of that Act, hereby makes the annexed Electronic Alternatives Regulations for the Purposes of Subsection 254(1) of the Canada Labour Code.	Regulamento de Alternativas Eletrônicas para efeitos da subsecção 254 (1) do Código do Trabalho do Canadá O ministro do Trabalho, como autoridade responsável pelo Código do Trabalho do Canadá, em conformidade com a definição de "autoridade responsável" na subsecção 31 (1) Lei de Proteção de Informações Pessoais e Documentos Eletrônicos, nos termos do § 50 da referida lei, decide Regulamentar Alternativas Eletrônicas, em anexo, para efeitos da subsecção 254 (1) do Código do Trabalho do Canadá.	Ministro do Trabalho	ELECTRONIC DOCUMENTS 2. For the purposes of the application of section 41 of the Personal Information Protection and Electronic Documents Act and the application of that section to subsection 254(1) of the Canada Labour Code, in order to satisfy the requirement that a pay statement shall be in writing, an electronic document must satisfy the following conditions: (a) the document must be provided to the employee by making it available only to the employee through an electronic source, such as a web site, that is accessible to the employee and whose location is made known to the employee; (b) for a period of at least three years from the day on which the document is first provided to the employee, the document must be readable and printable on a computer and printer to which the employer shall provide the employee with private access.	Documentos Eletrônicos 2. Para efeitos da aplicação do artigo 41 da Lei de Proteção de Informações Pessoais e Documentos Eletrônicos e à aplicação dessa seção para subsecção 254 (1) do Código do Trabalho do Canadá, a fim de satisfazer a exigência de que a declaração de pagamento será por escrito, satisfeita em documento eletrônico conforme as condições: (A) o documento deve ser fornecido ao empregado, tornando-o disponível apenas para o trabalhador por meio de uma fonte eletrônica, tais como um Web site, que é acessível ao trabalhador e cuja localização é conhecida pelo trabalhador; (B) para um período de pelo menos três anos a partir do dia em que o primeiro documento é fornecido ao empregado, o documento deve ser lido e impresso de um para o empregador fornecer ao trabalhador acesso privativo.
Secure Electronic Signature Regulamentos (SOR/2005-30) -Registration February 1, 2005 -Regulation current to May 27th, 2009	Personal Information Protection and Electronic Documents Act Secure Electronic Signature Regulations Her Excellency the Governor General in Council, on the recommendation of the Treasury Board, pursuant to subsection 48(1) of the Personal Information Protection and Electronic Documents Acta and paragraph 31.4(a)b of the Canada Evidence Act, hereby makes the annexed Secure Electronic Signature Regulations.	Sobre Lei de Proteção de Informações Pessoais e Documentos Eletrônicos Regulamento de Segurança das Assinaturas Eletrônicas Sua Excelência o Governador Geral do Conselho, sob recomendação do Conselho do Tesouro, em conformidade com a subseção 48 (1) Lei de Proteção de Informações Pessoais e Documentos Eletrônicos e parágrafo e 31,4 (a) b da Lei de Evidências do Canadá decide, em anexo, Regulamentar a Segurança das Assinaturas Eletrônicas	Governador Geral	"asymmetric cryptography" means a cryptographic system that relies on key pairs. "certification authority" means a person or entity that issues digital signature certificates and that has been listed as such on the website of the Treasury Board Secretariat. (autorité de certification) "digital signature certificate", in respect of a person, means an electronic document that (a) identifies the certification authority that issued it and is digitally signed by that certification authority; (b) identifies, or can be used to identify, the person; and (c) contains the person's public key. "entity" includes any federal department, branch, office, board, agency, commission, corporation or body for the administration of the affairs of which a minister of the Crown is accountable to Parliament. "key pair" means a pair of keys held by or for a person that includes a private key and a public key that are mathematically related to, but different from, each other. "private key" means a string of data that (a) is used in asymmetric cryptography to encrypt data contained in an electronic document; and (b) is unique to the person who is identified in, or can be identified through, a digital signature certificate and corresponds only to the public key in that certificate. "public key" means a string of data contained in a digital signature certificate that (a) is used in asymmetric cryptography to decrypt data contained in an electronic document that was encrypted through the application of the private key in the key pair; and (b) corresponds only to the private key in the key pair. 3. (1) A digital signature certificate is valid if, at the time when the data contained in an electronic document is digitally signed in accordance with section 2, the certificate (a) is readable or perceivable by any person or entity who is entitled to have access to the digital signature certificate; and (b) has not expired or been revoked. 4. (1) Before recognizing a person or entity as a certification authority, the President of the Treasury Board must verify that the person or entity has the capacity to issue digital signature certificates in a secure and reliable manner within the context of these Regulations and paragraphs 48(2)(a) to (d) of the Act. (2) Every person or entity that is recognized as a certification authority by the President of the Treasury Board shall be listed on the website of the Treasury Board Secretariat.	"criptografia assimétrica", um sistema criptográfico que dependa chaves pares. "autoridade certificadora", uma pessoa ou entidade que emite certificados de assinatura digital e que tem sido indicados como tal no site da Secretaria do Tesouro Câmara. (Autoridade de certificação) "certificado de assinatura digital", no que diz respeito a uma pessoa, significa que um documento eletrônico que (A) identifica a autoridade certificadora que o emitiu, e é assinado digitalmente por essa autoridade de certificação; (B) identifica, ou pode ser usada para identificar a pessoa, e (C) contém a chave pública da pessoa. "entidade" inclui qualquer departamento federal, sucursal, escritório, administração, agência, comissão, empresa ou entidade responsável pela administração dos assuntos de que um ministro da Coroa é responsável perante o Parlamento. "chave par" significa um par de chaves realizado por ou para uma pessoa, que inclui uma chave privada e uma chave pública que são matematicamente relacionadas, mas diferentes. "chave privada", uma seqüência de dados (A) utilizada em criptografia assimétrica para criptografar os dados contidos em um documento eletrônico e (B) é único para a pessoa que é identificado, ou pode ser identificado através de um certificado de assinatura digital e corresponde apenas à chave pública nesse certificado. "chave pública" é uma seqüência de dados contidos em um certificado de assinatura digital que (A) é utilizado em criptografia assimétrica para descriptografar os dados contidos em um documento eletrônico que foi codificado através da aplicação da chave privada de um par de chaves, e (B) corresponde apenas à chave privada de um par de chaves. 3. (1) A assinatura digital certificado é válido se, no momento em que os dados contidos em um documento eletrônico assinado digitalmente, de acordo com a secção 2, o certificado (A) é legível ou perceptível por qualquer pessoa ou entidade que tenha direito a ter acesso ao certificado de assinatura digital, e (B) não tenha expirado ou sido revogada. 4. (1) Antes de reconhecer uma pessoa ou entidade como uma autoridade de certificação, o Presidente da Câmara do Tesouro deve verificar se a pessoa ou entidade possui a capacidade para emitir certificados de assinatura digital em uma maneira segura e confiável, no âmbito destes regulamentos e os parágrafos 48 (2) (a) a (d) da lei. (2) Qualquer pessoa ou entidade que é reconhecida como uma autoridade de certificação pelo Presidente da Câmara do Tesouro será listada no site da Secretaria do Tesouro Câmara.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Tradução	Origem	Artigos Segurança Informação	
Protection of Privacy Regulations (C.R.C., c. 440) CRIMINAL CODE - Regulation current to May 27th, 2009	1. These Regulations may be cited as the Protection of Privacy Regulations.	1. Estes regulamentos podem ser citados como Regulamento de Proteção da Privacidade.	Parlamento	2. For the purposes of subsection 178.23(1) of the Criminal Code, the Attorney General of a province who gave a notice required to be given by that subsection, or the Solicitor General of Canada where the notice was given by him, shall certify to the court that issued the authorization that such notice was given by filing with a judge of the court a certificate signed by the person who gave the notice specifying (a) the name and address of the person who was the object of the interception; (b) the date on which the authorization and any renewal thereof expired; (c) if any delay for the giving of notice was granted under section 178.23 or subsection 178.12(3) of the Criminal Code, the period of such delay; and (d) the date, place and method of the giving of the notice.	2. Para efeitos do disposto na subsecção 178,23 (1) do Código Penal, o procurador-geral de uma província que requereu aviso da subsecção, ou o Advogado Geral do Canadá deu o aviso, deve certificar ao tribunal que emitiu a autorização que tal aviso foi dado por depósito com um juiz do tribunal de um certificado assinado pela pessoa que deu o aviso especificando (A) o nome e endereço da pessoa que foi o objeto da intercepção; (B) a data em que a renovação desta autorização, bem como qualquer expirado; (C) se houver demora para a concessão de aviso prévio foi concedido ao abrigo da secção 178,23 ou 178,12 subsecção (3) do Código Penal, esse período de atraso; e (D) a data, local e método de dar o do anúncio.
Electronic Payments Regulations (SOR/98-129) -Registration February 23, 1998 -Regulation current to May 27th, 2009	Electronic Payments Regulations The Treasury Board, pursuant to paragraph 10(f) of the Financial Administration Act, hereby makes the annexed Electronic Payments Regulations.	Regulamento de Pagamentos Eletrônicos A Câmara do Tesouro, nos termos do parágrafo 10 (f), da Lei de Administração Financeira, em anexo, regulamenta os pagamentos eletrônicos.	Câmara do Tesouro	4. The Receiver General shall take all necessary measures to ensure (a) the security of the system used for the transmission of electronic instructions for payment to financial institutions; (b) the confidentiality, authenticity and integrity of the data while it is under the control of the Receiver General or being transmitted to a financial institution; and (c) the security, integrity and safekeeping of the media used to issue an electronic instruction for payment while the media are under the control of the Receiver General or in transit to a financial institution for processing. (3) Every electronic instruction for payment issued by on-line transfer shall be acknowledged by the financial institution that receives it and every electronic authorization shall be verified by the financial institution to ensure the integrity of the instruction.	4. O Receptor Geral tomará todas as medidas necessárias para assegurar (A) a segurança do sistema utilizado para a transmissão eletrônica de instruções de pagamento a instituições financeiras; (B) a confidencialidade, autenticidade e integridade dos dados enquanto ele estiver sob o controle do Receptor Geral ou ser transmitidos a uma instituição financeira, e (C) a segurança, a integridade e a segurança dos meios de comunicação utilizado para emitir uma instrução de pagamento eletrônica, enquanto os meios de comunicação estão sob o controle do Receptor Geral ou em trânsito para uma instituição financeira para a transformação. (3) Todas as instruções de pagamentos eletrônicos emitidos por transferência on-line devem ser reconhecidas pela instituição financeira que recebê-lo e cada autorização eletrônica deve ser verificada pela instituição financeira para assegurar a integridade da instrução.
Royal Canadian Mounted Police External Review Committee Security and Confidentiality Regulations (SOR/88-397) Registration July 21, 1988 Regulation current to May 27th, 2009	Royal Canadian Mounted Police External Review Committee Security and Confidentiality Regulations Her Excellency the Governor General in Council, decide to make the annexed Regulations respecting the security and confidentiality of information to which members of the Royal Canadian Mounted Police External Review Committee and persons employed by the Royal Canadian Mounted Police External Review Committee may have access in the performance of their duties.	Comitê de Revisão de Segurança do Royal Canadian Mounted Police External e Regulamentos de Confidencialidade Sua Excelência o Governador Geral do Conselho, decide em anexo, respeitando os regulamentos de segurança e confidencialidade das informações a quais os membros do Comitê de Revisão da Polícia Externa Montada Real Canadense e seus empregados podem ter acesso no exercício das suas funções.	Governador Geral	2. Every member of the Committee and every person employed by the Committee who is required to receive or obtain information relating to any matter under the Royal Canadian Mounted Police Act shall, in the performance of their duties, comply with any security and confidentiality requirements applicable to individuals who normally have access to and use of that information and shall take the oath of secrecy or the affirmation of secrecy set out in the schedule.	2. Qualquer membro da Comissão e de cada pessoa empregada pela Comissão que é necessário para receber ou obter informações relativas a qualquer questão sob a Royal Canadian Mounted Police Act deve, no desempenho das suas funções, cumprir quaisquer requisitos de segurança e de confidencialidade para pessoas que normalmente têm acesso e uso da informação e que tomará o juramento de sigilo ou a afirmação de sigilo estabelecidos no cronograma.
Canadian Telecommunications Common Carrier Ownership and Control Regulations (SOR/94-667) Registration October 25, 1994	His Excellency the Governor General in Council, on the recommendation of the Minister of Industry, Science and Technology, pursuant to section 22 of the Telecommunications Act, is pleased hereby to make the annexed Regulations respecting the ownership and control of canadian telecommunications common carriers.	Sua Excelência o Governador Geral do Conselho, por recomendação do ministro da Indústria, Ciência e Tecnologia, nos termos do artigo 22 a Lei de Telecomunicações congratula-se decide a fazer respeitar os regulamentos, em anexo, a propriedade e o controle de telecomunicações canadense comuns.	Governador Geral	2. (1) In this Regulations, "intermediary" means a person or entity, excluding a depository and trustee, that holds a security on behalf of another person or entity; (intermédiaire)	2. (1) No presente regulamento, "intermediário", uma pessoa ou entidade, exceto um depositário e administrador, que detém uma segurança em nome de outra pessoa ou entidade; (intermédio)
Fingerprinting, Palmprinting and Photography Order (SI/92-131) Registration July 29, 1992	Identification of Criminals Act	Identificação de criminosos	Governor General	His Excellency the Governor General in Council, on the recommendation of the Minister of Justice and pursuant to paragraph 2(1)(b) of the Identification of Criminals Act, is pleased hereby (a) to revoke Order in Council P.C. 1954-1109 of July 22, 1954*; and (b) for the purposes of the Identification of Criminals Act, to sanction the measurements, processes and operations of fingerprinting, palmprinting and photography.	Sua Excelência o Governador Geral do Conselho, por recomendação do ministro da Justiça e nos termos do n º 2 (1) (b) da lei de identificação de criminosos, decide (A) revogar a Ordem PC 1954-1109 no Conselho de 22 de julho de 1954 *; e (B) Para efeitos da Lei de identificação de criminosos, sancionar as medidas, processos e operações de impressão digital, palmprinting e fotografia.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Decretos	Ementa	Tradução	Origem	Artigos Segurança Informação	
Access to Information Regulations (SOR/83-507) Regulation current to May 27th, 2009	Access to Information Regulations 1. These Regulations may be cited as the Access to Information Regulations.	Regulamento de Acesso à Informação 1. Estes regulamentos podem ser citados como Regulamentos de acesso à informação.		2. In these Regulations, "Access to Information Request Form" means the form prescribed by the designated Minister pursuant to paragraph 70(1)(b) of the Act for the purpose of requesting access to records under the control of a government institution; 4. A request for access to a record under the Act shall be made by forwarding to the appropriate officer of the government institution that has control of the record, together with the required application fee.	2. Nestes regulamentos, "Pedido de Acesso à Informação", a forma prescrita pelo Ministro designado nos termos do n º 70 (1) (b) da Lei, a fim de solicitar o acesso a registros sob o controle de uma instituição governamental; 4. O pedido de acesso a um registro ao abrigo da lei deve ser feita pelo encaminhamento adequado para o funcionário da instituição governamental que tem o controlo do registro, juntamente com a aplicação necessária taxa.
Privacy Act Extension Order No. 1 (SOR/83-553)	Order extending the right to be given access to personal information under subsection 12(1) of the privacy act 1. This Order may be cited as the Privacy Act Extension Order No. 1.	Ordem estendendo o direito de obter o acesso a informações pessoais na subsecção 12 (1) da lei de privacidade 1. Este decreto pode ser citado como Extensão Despacho n º 1 da Lei de Privacidade.		2. The right to be given access to personal information under subsection 12(1) of the Privacy Act is hereby extended to include an inmate within the meaning of Part I of the Corrections and Conditional Release Act who is not a Canadian citizen or a permanent resident within the meaning of the Immigration Act, 1976.	2. O direito a ter acesso a informações pessoais na subsecção 12 (1) da lei de privacidade é alargado para incluir um recluso, na acepção da parte I da Lei Correções e Liberdade Condicional, que não é um cidadão canadense ou residente permanente, na acepção do Lei de Imigração de 1976.
Privacy Act Extension Order, No. 2 (SOR/89-206)	Order extending the right to be given access to personal information under subsection 12(1) of the privacy act 1. This Order may be cited as the Privacy Act Extension Order, No. 2.	Ordem estendendo o direito de obter o acesso a informações pessoais na subsecção 12 (1) da lei de privacidade 1. Este decreto pode ser citado como Extensão Despacho, n º 2 da Lei de Privacidade.		2. The right to be given access to personal information under subsection 12(1) of the Privacy Act is hereby extended to include all individuals present in Canada to whom that right has not been extended previously.	2. O direito a ter acesso a informações pessoais na subsecção 12 (1) da lei de privacidade é alargado para incluir todas as pessoas presentes no Canadá, para quem esse direito não tenha sido prorrogado anteriormente.
Privacy Act Heads of Government Institutions Designation Order (SI/83-114)	Order respecting the designation of the heads of government institutions for the purposes of the privacy act 1. This Order may be cited as the Privacy Act Heads of Government Institutions Designation Order.	Ordem respeitando a designação dos chefes das instituições governamentais para efeitos da lei de privacidade 1. Este decreto pode ser citada como Ordem de Designação para Instituições de Chefes de Governo da Lei de Privacidade.		2. The person holding a position set out in Column II of an item of the schedule is hereby designated, for the purposes of the Privacy Act, as the head of the government institution set out in Column I of that item	2. A pessoa que detém uma posição definida na Coluna II de um item do calendário é designado, para efeitos da lei de privacidade, como o chefe da instituição governamental fixados na coluna I desse item.
Privacy Regulations (SOR/83-508)	Privacy Regulations 1. These Regulations may be cited as the Privacy Regulations.	Regulamentos de Privacidade 1. Estes regulamentos podem ser citados como os regulamentos de privacidade.		2. In these Regulations, "Access to Personal Information Request Form" means the form prescribed by the designated Minister pursuant to paragraph 71(1)(c) of the Act for the purpose of requesting access to personal information under the control of a government institution; 4. (1) Personal information concerning an individual that has been used by a government institution for an administrative purpose shall be retained by the institution (a) for at least two years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal; and (b) where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his rights under the Act.	2. Nestes regulamentos, "Formulário de Acesso a Informações Pessoais " é a forma prescrita pelo Ministro designado nos termos do n º 71 (1) (c) da lei com a finalidade de solicitar o acesso a informações pessoais sob o controle de uma instituição governamental; 4. (1) As informações pessoais relativas a uma pessoa que tenha sido utilizado por uma instituição governamental para uma finalidade administrativa, devem ser mantidas pela instituição (A) por, pelo menos, dois anos após a última vez que as informações pessoais foram usadas para uma finalidade administrativa, a menos que a pessoa procurada consinta na sua disposição e (B) quando um pedido de acesso à informação ter sido recebido, até ao momento em que o indivíduo tenha tido a oportunidade de exercer todos os seus direitos ao abrigo da lei.

Fonte: *Department of Justice Canada*. Disponível em: <http://laws.justice.gc.ca/>. Acesso em: 30 ago. 2009.

Projetos de Lei

Projetos de Lei	Assunto	Tradução	Origem	Autoria
LS-443E Bill C-15: Lobbyists Registration Act Act Revised 28 May 2003	Bill C-15: An Act To Amend The Lobbyists Registration Act (Revised 19 March 2003). On 25 October 2002 it was referred for study prior to second reading to the House of Commons Standing Committee on Industry, Science and Technology. In June 2001, the Committee reported on its five-year statutory review of the *Lobbyists Registration Act*. The report, entitled *Transparency in the Information Age: The Lobbyists Registration Act in the 21Century* made several recommendations aimed at improving the operation of the Act. The Act defines lobbyists as individuals paid to make representations with the goal of "influencing" federal public office holders. The Act requires lobbyists to register and disclose certain information, which is made public through a computerized registry system.	Bill C-15, uma lei para alterar a Lei de Registro de Lobistas. Em 25 de Outubro de 2002, foi encaminhado para estudo prévio para a segunda leitura na Câmara dos Comuns pelo Comitê Permanente da Indústria, Ciência e Tecnologia. Em Junho de 2001, a comissão relatou em seus cinco anos de revisão legal da Lei de Registro de Lobistas. O relatório, intitulado *Transparência na Era da Informação: A Lei de Registro de Lobistas no século* XXI fez várias recomendações destinadas ao melhor funcionamento da lei. A lei define como lobistas indivíduos pagos para fazer representações com o objetivo de "influenciar" os titulares de funções públicas federais. A lei exige que lobistas registrem e divulguem certas informações, tornadas públicas através de um sistema de registro computadorizado.	Poder Legislativo	Câmara dos Comuns Message sent to House of Commons: 28 May 2003 Concurrence in Senate amendments: 6 June 2003 Royal Assent: 11 June 2003 Statutes of Canada 2003, c. 10
LS-446E Bill C-23: Sex Offender Information Registration Act Revised 11 March 2003	Bill C-23, An Act respecting the registration of information relating to sex offenders, to amend the Criminal Code and to make consequential amendments to other Acts (the Sex Offender Information Registration Act), was introduced in the House of Commons on 11 December 2002. The Bill's purpose is to help police services investigate crimes of a sexual nature by requiring the registration of certain information relating to sex offenders. This is mainly done through the addition of a number of sections to the Criminal Code.(1) The Bill also makes consequential amendments to the Access to Information Act(2) and the Criminal Records Act,(3) along with coordinating amendments to the Criminal Code to make it consistent with the provisions of the Youth Criminal Justice Act(4) and Bill C-20, An Act to amend the Criminal Code (protection of children and other vulnerable persons) and the Canada Evidence Act.	Bill C-23, um ato de respeito ao registro das informações relativas aos ofensores sexuais, no sentido de alterar o Código Penal e fazer as conseqüentes alterações a outros atos (o Sex Offender Registration Information Act), foi introduzida na Câmara dos Comuns em 11 de Dezembro de 2002 . O projeto tem por objetivo ajudar os serviços policiais investigar crimes de natureza sexual, exigindo o registo de determinadas informações relativas a criminosos sexuais. Este é essencialmente feito através da adição de um número de seções para o Código Penal. (1) O Bill também faz as conseqüentes alterações à Lei do Acesso à Informação (2) e os registros criminais Lei, (3), juntamente com a coordenação das alterações ao Código Penal, para tomá-lo compatível com as disposições da Juventude Criminal Justice Act (4) e Bill C-20, uma lei para alterar o Código Penal (proteção de crianças e outras pessoas vulneráveis) e do Canadá Provas lei.	Poder Legislativo	Câmara dos Comuns First Reading: 11 December 2002 Second Reading: 8 April 2003
LS-450E Bill C-25: Public Service Modernization Act	The Public Service Modernization Act (13 March 2003). On 6 February 2003, Bill C-25, the Public Service Modernization Act,(1) was introduced in the House of Commons. Bill C-25 contains four main public service reform initiatives. 1) It will repeal the current Public Service Staff Relations Act and enact a new Public Service Labour Relations Act to govern labour relations in the federal public service. 2) It will repeal the existing Public Service Employment Act and enact a new Public Service Employment Act to regulate appointments to the public service. 3) It will amend the Financial Administration Act to transfer certain human resources management powers from the Treasury Board to deputy heads. 4) It will amend the Canadian Centre for Management Development Act to pave the way for the amalgamation of the Canadian Centre for Management Development, and Training and Development Canada, into the new Canada School of the Public Service.	Em 6 de Fevereiro de 2003, o projeto de lei C-25, Lei de Modernização da Administração Pública, (1) foi introduzida na Câmara dos Comuns. Bill C-25 contém quatro principais iniciativas de reforma dos serviços públicos. 1) Irá revogar a atual Lei de Relações de Trabalho de Serviço Público e promulgar uma nova lei de Relações de Trabalho do Serviço Público para reger as relações de trabalho no serviço público federal. 2) Irá revogar a atual Lei de Emprego de Serviço Público e promulgar uma nova lei Serviço Público de Emprego para regulamentar as nomeações para o serviço público. 3) Irá revogar a atual Lei da Administração Financeira para transferir certas competências de gestão dos recursos humanos da Câmara do Tesouro para comando do deputado. 4) Irá revogar a atual Lei de Centro de Desenvolvimento e Gerenciamento Canadense para preparar o caminho de fusão do Centro de Desenvolvimento e Gerenciamento Canadense, e do Treinamento e Desenvolvimento do Canadá, na nova Escola do Serviço Público do Canadá.	Poder Legislativo	Câmara dos Comuns First Reading: 6 February 2003
LS-419E Bill C-42: The Public Safety Act 21 December 2001	Bill C-42 is one of three in the government's legislative response to the events of September 11 in the United States. Bill C-36, the Anti-terrorism Act, received Royal Assent on 18 December 2001. On 28 November 2001, the House of Commons unanimously consented on a motion to delete from Bill C-42 section 4.83 in clause 5 amending the Aeronautics Act. The same day, that section was introduced as Bill C-44 in order to provide for speedier passage than consideration as part of Bill C-42 would have allowed for. It received Royal Assent on 18 December 2001. Bill C-42 amends 19 existing Acts, and enacts a new statute to implement the Biological and Toxin Weapons Convention, which entered into force on 26 March 1975. Proposed section 4.82 is a totally new provision that authorizes the Minister to require prescribed passenger information from air carriers and others who operate aviation reservation systems.	O projeto de lei C-42 é um dos três no governo legislativa da resposta aos acontecimentos de 11 de Setembro nos Estados Unidos. Bill C-36, a Lei Anti-terrorismo, Royal recebeu parecer favorável em 18 de Dezembro de 2001. Em 28 de Novembro de 2001, a Câmara dos Comuns consentido por unanimidade sobre uma proposta de excluir da lei C-42 secção 4,83 na cláusula 5, que altera a Lei Aeronáutica. No mesmo dia, que a secção foi introduzida como Bill C-44, a fim de prever a passagem rápida do que considerar como parte da lei C - teria permitido para 42. Recebeu Royal Assent em 18 de Dezembro de 2001. Bill C-42 altera 19 leis existentes, e aprova uma nova lei para implementar a Convenção sobre Armas Biológicas e Tóxicas, que entrou em vigor em 26 de Março de 1975. Proposta de 4,82 é uma nova disposição que autoriza o Ministro a exigir informações sobre passageiros às transportadoras aéreas que operam aviação e outros sistemas de reserva.	Poder Legislativo	Câmara dos Comuns First Reading: 22 November 2001
LS-344E Bill C-6: Personal Information Protection and Electronic Documents Act Revised 15 May 2000	Bill C-6 would introduce measures to protect personal information in the private sector, create an electronic alternative for doing business with the federal government, and clarify how the courts would assess the reliability of electronic records used as evidence. The bill passed report stage on 20 October 1999 and is currently at third reading in the House of Commons. Bill C-6 is a one of several components of the Canadian Electronic Commerce Strategy announced by Prime Minister Chrétien on 22 September 1998, which is aimed at "recreating in cyberspace the same expectations of trust, confidence and reliability that now exist in everyday commerce." The government's stated goal is for Canada to become a world leader in electronic commerce by the year 2000; this bill is one of the measures to be used to achieve this goal. The bill contains six parts, the most prominent of which is Part 1, "Protection of Personal Information in the Private Sector." Together with Schedule 1, which contains the CSA Model Code, Part 1 would establish rules governing the collection, use and disclosure of, as well as access to, personal information in the private sector. Part 2, entitled "Electronic Documents," would provide for the use of electronic alternatives where federal laws now contemplate the use of paper to record or communicate information. The other parts would provide amendments to other federal statutes to facilitate the use and legal recognition of electronic documents.(2)	Bill C-6 iria introduzir medidas para proteger a informação pessoal no setor privado, criar uma alternativa eletrônica para fazer negócios com o governo federal, e esclarecer a forma como os tribunais iriam avaliar a confiabilidade dos registros eletrônicos utilizados como provas. A lei aprovada relatório fase em 20 de Outubro de 1999 e está atualmente na terceira leitura na Câmara dos Comuns. Bill C-6 é um dos vários componentes do Comércio Eletrônico canadense Estratégia anunciado pelo Primeiro-Ministro Chrétien, em 22 de Setembro de 1998, que visa "recriar no ciberespaço as mesmas expectativas de confiança, a confiança e fiabilidade que já existem na vida cotidiana do comércio. " O objetivo declarado do governo é para o Canadá se tornar um líder mundial no comércio eletrônico; até ao ano 2000, este projeto é uma das medidas a serem utilizados para atingir esse objetivo. O projeto contém seis partes, a mais importante das quais é a parte 1, "Proteção de Dados Pessoais no sector privado." Juntamente com o quadro 1, que contém o Código Modelo CSA, Parte 1 estabeleceria regras que regulam a coleta, uso e divulgação, bem como o acesso, de informação pessoal no sector privado. Parte 2, intitulada "Documentos Eletrônicos", que prevêem a utilização de alternativas eletrônicas onde leis federais já contemplam o uso de papel para registrar ou comunicar informações. As outras partes proporcionariam a alteração de outras leis federais a fim de facilitar a utilização e o reconhecimento legal de documentos eletrônicos. (2)	Poder Legislativo	Câmara dos Comuns First Reading: 15 October 1999 Second Reading: 15 October 1999 Committee Report:15 October 1999 Report Stage: 20 October 1999 Third Reading: 26 October 1999 Senado First Reading: 2 November 1999 Second Reading: 6 December 1999 Committee Report: 7 December 1999 Report Stage: 7 December 1999 Third Reading: 9 December 1999

Fonte: PARLIAMENT. Disponível em: <http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/ls-e.html>. Acesso em: 30 ago. 2009.

Projetos de Lei	Assunto	Tradução	Origem	Autoria
LS-400E Bill C-16: Charities Registration (Security Information) Act Revised 16 October 2001	2. (1) The purpose of this Act is to show Canada's commitment to participate in concerted international efforts to deny support to those who engage in terrorism, to protect the integrity of the registration system for charities under the Income Tax Act and to maintain the confidence of Canadian taxpayers that the benefits of charitable registration are made available only to organizations that operate exclusively for charitable purposes. The bill implements Canada's G-8 commitments to: investigate charitable organizations where it is believed that an organization is being used by terrorists to cover for other activities; and take steps to prevent the financing of terrorist organizations indirectly through organizations that have, or claim to have, charitable goals. It also responds to a 1999 Report of the Special Senate Committee on Security and Intelligence, which observed that groups with terrorist affiliations conduct fund-raising activities in Canada, often using benevolent or philanthropic organizations as fronts.	2. (1) O objetivo da presente lei é para mostrar o empenho do Canadá em concentrar esforços internacionais para negar apoio a todos envolvidos no terrorismo, a fim de proteger a integridade do sistema de registro de caridade da Lei de Imposto de Renda e para manter a confiança dos contribuintes canadenses que o registro de caridade são disponibilizados apenas para organizações que operam exclusivamente para fins de caridade. O projeto implementado pelo Canadá é compromisso com G-8 para: investigar as organizações caritativas utilizadas por terroristas para acobertar atividades, e tomar medidas para prevenir o financiamento de organizações terroristas indiretamente através de organizações que têm, ou reivindicam beneficência. Ele também responde a um relatório de 1999 da Comissão Especial do Senado sobre a Segurança e Inteligência, o qual observou que os grupos terroristas com filiações em atividades de angariação de fundos, no Canadá, muitas vezes utilizavam a beneficência ou organizações filantrópicas como frentes.	Poder Legislativo	Câmara dos Comuns First Reading: 15 March 2001 Referred to Committee before Second Reading: 1 May 2001* * The order of reference to the Standing Committee on Finance was discharged and the bill was withdrawn by a motion adopted with the unanimous consent of the House of Commons: 15 October 2001
C-15 C-15A C-15B amend the Criminal Code and to amend other Acts Jan. 29, 2001 - Sept. 16, 2002	*An Act to amend the Criminal Code and to amend other Acts*". (a) adding offences and other measures that provide additional protection to children from sexual exploitation, including sexual exploitation involving use of the Internet; 11. (1) The portion of paragraph 163.1(1)(a) of the French version of the Act before subparagraph (i) is replaced by the following: a) de toute représentation photographique, filmée, vidéo ou autre, réalisée ou non par des moyens mécaniques ou électroniques. (3) Every person who transmits, makes available , distributes, sells, imports, exports or possesses for the purpose of transmission, making available , distribution, sale or exportation any child pornography is guilty of 12. Subsection 164(4) of the Act is replaced by the following: (4) If the court is satisfied, on a balance of probabilities, that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it may make an order declaring the matter forfeited to Her Majesty in right of the province in which the proceedings take place, for disposal as the Attorney General may direct.	Uma lei de alteração do Código Penal e alterar outras leis". (a) adicionando as infracções e outras medidas que proporcionam uma protecção adicional para as crianças da exploração sexual, incluindo a exploração sexual que envolva o uso da Internet; Cláusula 11: (1) A parcela relevante da subsecção 163,1 (1) tem a seguinte redacção: 163,1 (1) Nesta secção, a pornografia infantil"significa `` (A) uma fotografia, cinema, vídeo ou outra representação visual, ou não foi feito por meio eletrônico ou mecânico, (3) Toda pessoa que importa, distribui, vende ou possuir, para efeitos de distribuição ou qualquer venda de pornografia infantil é culpado de Cláusula 12: subsecção 164 (4) tem a seguinte redação: (4) Se o tribunal considerar que a publicação, a representação ou de material escrito, referido na subsecção (1), é obsceno, quadrinhos ou de um crime de pornografia infantil, ela deve fazer um despacho que declara a matéria perdida a Sua Majestade, em razão da província em que o processo tenha lugar, para a eliminação como o Procurador-Geral pode fazer.	Poder Legislativo	Câmara dos Comuns First Reading: March 14, 2001 Debate(s) at 2nd Reading May 3, 2001; May 7, 2001; September 20, 2001 Second Reading: September 26, 2001 Committee Justice and Human Rights October 2, 2001 (22); October 3, 2001 (23); October 4, 2001 (24)
LS-337E Bill C-54: Personal Information Protection and Electronic Documents Act Revised 20 April 1999	Bill C-54, introduced in the House of Commons on 1 October 1998, was referred to the Standing Committee on Industry after second reading. The Committee held hearings commencing 1 December 1998 and ending 18 March 1999. On 12 April, the bill was reported back to the House of Commons, with 39 amendments. On 19 April, during the report stage, the Minister of Industry proposed 10 further amendments to the bill. Part 1 of Bill C-54 contains clauses 2 to 30. The provisions in Part 1 contain definitions, the purpose of Part 1, scope of application, a "purposes limitation" requirement, and the exemptions whereby an organization could collect, use and disclose personal information without the knowledge or consent of the individual concerned. Part 1 also contains provisions regarding access by individuals to their personal information, grounds for refusing an access request, the manner in which a complaint could be brought forward, the Commissioner's powers of investigation and audit, the Commissioner's report, court hearing and remedies, other duties and powers of the Commissioner, the regulation and order-making powers of the Governor in Council, "whistleblower protection," an offences and punishment clause, and a transitional clause.	Bill C-54 iria introduzir medidas para proteger a informação pessoal no sector privado, criar uma alternativa eletrônica para fazer negócios com o governo federal e esclarecer a forma como os tribunais iria avaliar a fiabilidade dos registros eletrônicos utilizados como provas. Parte 1 de lei C-54 contém cláusulas 2 a 30. O disposto na parte 1 contêm definições, o objetivo da Parte 1, o âmbito de aplicação, uma "limitação efeitos" exigência, bem como as isenções em que uma organização pode coletar, usar e divulgar informações pessoais sem o conhecimento ou consentimento da pessoa em causa. Parte 1 contém igualmente disposições relativas ao acesso dos indivíduos às suas informações pessoais, motivos para a recusa de um pedido de acesso, a maneira em que uma queixa pode ser apresentada, ao Comissário de inquérito e de auditoria, o relatório do comissário, em audiência e soluções, outras funções e competências do Comissário, o regulamento e a forma de tomada de poder do governador no Conselho, "denunciante defesa," uma cláusula crimes e castigos, e uma cláusula transitória.	Poder Legislativo	Câmara dos Comuns First Reading: 1 October 1998 Second Reading: 3 November 1998 Committee Report: 13 April 1999

Fonte: PARLIAMENT. Disponível em: <http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/ls-e.html>. Acesso em: 30 ago. 2009.

APÊNDICE C – Normas Técnicas Internacionais

Normas Técnicas Internacionais

Normas	Ementa	Origem	Assunto
AS/NZS 4360	Trata-se de uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza.	*Standards Australia e Standards New Zealand*	Publicada em 1995 e revisada em 1999 e em 2004. Foi a primeira norma internacional sobre Sistemas de Gestão de Riscos Empresariais. Propõe um processo estruturado para o gerenciamento dos mais diversos tipos de riscos, como: os relacionados à segurança, ao meio ambiente e às políticas públicas.
CobiT	*Control Objectives for Information and related Technology*. 4. ed. Rolling Meadows: ITGI, 2005.	ITGI. *Information Technology Governance Institute*.	Conjunto de orientações internacionalmente aceitas em matérias de governança de TI. Rresultou na criação de uma família crescente de publicações e produtos concebidos para ajudar na implementação de TI eficaz para controle e administração em toda uma empresa ou organização.
ITIL (*Infrastructure Technology Information Library*)	O ITIL contempla as áreas de gestão de incidentes, problemas, configuração, implantação de suporte de *software*.	Governo do Reino Unido	Criada no final da década de 1980 para registrar as melhores práticas na área de gestão de serviços de tecnologia da informação. Embora não represente exatamente um padrão de segurança da informação, colaborou para a padronização e a melhoria da qualidade do serviço ofertado pela área de tecnologia de informação, e para o alcance dos objetivos de segurança da informação
ISO/IEC 27005:2008	Norma fornece as diretrizes para o processo de Gestão de Riscos de Segurança da Informação.	ISO/ IEC (*International Standardization Organization /International Electrotechnical Commission*)	Criada para apoiar o entendimento das especificações e conceitos estabelecidos pela norma ISO/IEC 27001, esta nova norma define as melhores práticas em gestão de riscos de segurança da informação e pode ser aplicada a organizações de todos os portes e segmentos. Esta Norma substitui a série de normas ISO/IEC TR 13335 – *Management of Information and Communications Technology Security* (MICTS).
ISO 27001:2006	Gestão da segurança da informação. Parte 2 do padrão BS 7799 define o Sistema de Gestão de Segurança da Informação (ISMS, de *Information Security Management System*). Especifica uma série de processos voltados para garantir a avaliação e o tratamento dos riscos.	ISO, *International Standardization Organization*	A norma ISO 27001 é a principal referência internacional para gestão da segurança da informação. A certificação envolve uma auditoria do ISMS para verificar se a organização dispõe de processos adequados para gerenciar riscos, manter o sistema atualizado e garantir o desenvolvimento da segurança da informação. Essas normas consistem no tratamento da informação como um patrimônio, que deve ser protegido como qualquer outro ativo, de acordo com a classificação prévia de seu grau de confidencialidade, integridade, disponibilidade e privacidade.
ISO 27002: 2005	Código de Práticas para a Gestão da Segurança da Informação. Parte 1 do padrão BS 7799.	ISO	Proteção de dados e da privacidade de informações pessoais, salvaguarda de registros organizacionais e dos direitos de propriedade intelectual. Formalização da política de segurança da informação, definição das responsabilidades na segurança, educação e treinamento em segurança, relatório dos incidentes e gestão da continuidade.
ISO/IEC GUIDE 73:2002	Gestão de Riscos. Define 29 termos da Gestão de Riscos, agrupados nas categorias: a) básicos; b) pessoas ou organizações afetadas por riscos; c) avaliação de riscos; d) tratamento e controle de riscos.	ISO/ IEC (*International Electrotechnical Commission*)	Publicada em 2002, fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.
ISO/IEC GUIDE 51:1999.	Normas com recomendações para a inclusão dos aspectos de segurança.	ISO/IEC	Fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).
ISO/IEC TR 13335-3:1998.	*Management of Information and Communications Technology Security* (MICTS). Gestão de segurança na área de tecnologia da informação.	ISO/IEC	Fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.
ABNT NBR ISO/IEC-27001:2006	Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.Especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes. O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.	ABNT, Associação Brasileira de Normas Técnicas.	Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.
ABNT NBR ISO IEC 17799: 2005.	Código de Práticas para a Gestão da Segurança da Informação. Parte 1 do padrão BS 7799.	ABNT	Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.
ABNT NBR ISO/IEC-17779:2001	Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.Os objetivos definidos provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.	ABNT	Norma Regulatória.
ABNT NBR 12964:1993	Descreve quatro modos de operação para um algoritmo de cifração de blocos que opere sobre blocos-em-claro de p bites, gerando blocos-cifrados de q bites, onde p menor igual q, do tipo algoritmo de chave secreta.	ABNT	Norma Regulatória.
ABNT NBR 12896:1993	Fixa procedimentos a serem adotados para reduzir a vulnerabilidade das senhas nestas circunstâncias.	ABNT	Norma Regulatória.
ABNT NBR 12517:1993	Estabelece símbolos gráficos utilizados para projetos de controle de acesso físico de instalações de processamento de dados em áreas de segurança.	ABNT	Norma Regulatória.
ABNT NBR 11584:1991	Fixa condições exigíveis para proteção física de microcomputadores e terminais.	ABNT	Norma Regulatória. Em cancelamento
ABNT NBR 11515:1990	Fixa as condições ambientais exigíveis de acordo com cada meio de armazenamento de dados, em arquivo, operação ou transporte, bem como em situação de emergência. Aplica-se integralmente, ou em partes, a todos os usuários de processamento eletrônico de dados, bem como microfilmagem.	ABNT	Norma Regulatória.
ABNT NBR 11514:1990	Fixa condições exigíveis para a segurança de áreas delimitadas, edifícios, salas de computadores e de arquivo, centrais de instalações e equipamentos auxiliares, por meio de Controle de Acesso Físico.	ABNT	Norma Regulatória. Em cancelamento

Fonte: ABNT - Associação Brasileira de Normas Técnicas; e ISO - *International Organization for Standardization*. Disponível em: <http://www.abnt.org.br> e <http://www.iso.org/iso/home.htm>. Acesso em: 30 ago. 2009.