Ministério da Justiça

UnB

Centro de Apoio ao Desenvolvimento Tecnológico

latitude
Laboratório de tecnologias da tomada de decisão

Termo de Cooperação/Projeto:

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

Documento:

RT Levantamento e Análise da Legislação de Segurança da Informação

Data de Emissão:

01/09/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA

Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
John Kennedy Férrer Lima
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA

Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alessandro Zimmer
Alysson Fernandes de Chantal
Amanda Almeida Paiva
Andréia Campos Santana
Andreia Guedes Oliveira
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Caio Rondon Botelo de Carvalho
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Eduarda Simões Veloso Freire
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
José Elenilson Cruz
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marcos Vinicius Vieira da Silva
Marco Schaffer
Mirele Maria Cavalcante Rocha
Pedro Augusto Oliveira de Paula
Renata Elisa Medeiros Jordão
Roberto Mariano de Oliveira Soares
Sandro Augusto Pavlik Haddad
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Vinicius de Morais Alves
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
02/10/2014	0.1	Versão inicial.
03/10/2014	0.2	Revisão e implementação de texto e forma.
14/10/2014	0.3	Revisão e implementação de texto e forma.
21/10/2014	0.4	Inclusão item 2 – Revisão de Texto.
04/11/2014	0.5	Revisão e implementação de texto e forma.
11/11/2014	0.6	Revisão e implementação de texto e forma.
15/11/2014	0.7	Inclusão item 3.
25/11/2014	0.8	Inclusão item 4.
04/12/2014	0.9	Revisão e implementação de texto e forma.
08/12/2014	0.10	Revisão e implementação de texto e forma.
09/12/2014	0.11	Revisão e implementação de texto e forma.
15/12/2014	0.12	Revisão e implementação de texto e forma.
08/01/2015	0.13	Revisão e implementação de texto e forma
12/01/2015	0.14	Entrega relatório
01/09/2015	0.15	Revisão após Nota Técnica.

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

Sumário

1. INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura

tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

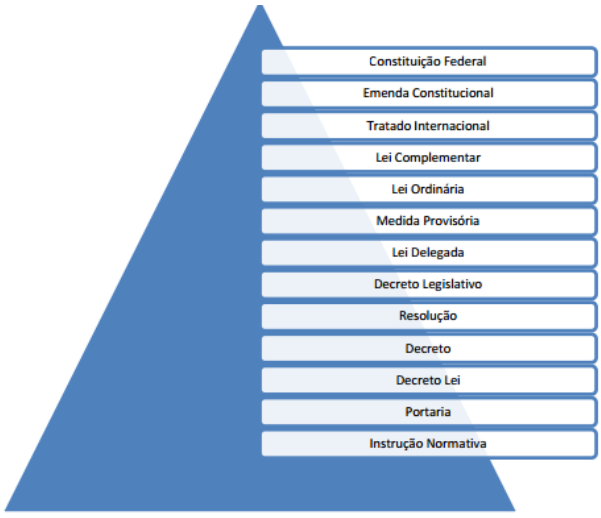
O presente relatório tem como objetivo o levantamento e a análise da legislação brasileira aplicada à segurança da informação, com a finalidade de auferir as regras a serem observadas no gerenciamento dos dados que serão armazenados no Cadastro Nacional do Registro de Identificação Civil – CANRIC com a instituição do número único de Registro de Identidade Civil – RIC, pelo qual cada cidadão brasileiro, nato ou naturalizado, será identificado em suas relações com a sociedade e com os organismos governamentais e privados.

Para tanto, o presente estudo foi organizado em quatro capítulos, sendo o primeiro um estudo acerca da Legislação Federal e suas regulamentações, o segundo abordando a legislação brasileira relacionada à segurança da informação, o terceiro sobre legislação brasileira específica à segurança da informação e o quarto analisando as instruções normativas no âmbito da Administração Pública Federal.

2. INTRODUÇÃO À SISTEMÁTICA DA LEGISLAÇÃO BRASILEIRA

O sistema jurídico brasileiro é composto por três grupos de normas, quais sejam: (i) constitucionais; (ii) infraconstitucionais e (iii) infralegais. As normas constitucionais compreendem a Constituição Federal, incluindo o ADCT – Ato das Disposições Constitucionais Transitórias e os Tratados/Convenções sobre direitos humanos[1]. As normas infraconstitucionais são compostas pelas Leis Complementar e Ordinária, Medida Provisória, Lei Delegada, Decreto Legislativo e Resolução. Por sua vez as normas infralegais são os Decretos, Portarias e as Instruções Normativas.

O quadro abaixo ilustra a hierarquia entre as normas:



A Constituição Federal é a Lei máxima do Estado brasileiro, a qual regula e organiza o seu funcionamento, bem como, limita poderes e define direitos e deveres dos cidadãos. Só pode ser alterada por meio da Emenda Constitucional, a qual deverá ser proposta por no mínimo um terço dos membros da Câmara dos Deputados ou do Senado Federal e será aprovada se obtiver em cada Casa do Congresso Nacional, em dois turnos, três quintos dos votos dos respectivos membros.

Não podem ser objeto de deliberação a Proposta de Emenda Constitucional que vise alterar as Cláusulas Pétreas, quais sejam: I - a forma federativa de Estado; II - o voto direto,

[1] Art. 5º, LXXVIII, §3º da Constituição Federal: os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais.

secreto, universal e periódico; III - a separação dos Poderes; e IV - os direitos e garantias individuais.

A Lei Complementar tem como propósito regulamentar norma prevista na Constituição Federal, sendo necessária para sua aprovação, a maioria absoluta de cada Casa do Congresso Nacional, que é formado pela Câmara dos Deputados e pelo Senado Federal. Por sua vez, a Lei Ordinária versa sobre a organização do poder judiciário e do ministério público, sobre nacionalidade, cidadania, direitos individuais, políticos e eleitorais, planos plurianuais e orçamentos e a todo o direito material e processual, como os códigos civil, penal, tributário e respectivos processos, sendo necessária para sua aprovação, a maioria relativa em cada Casa do Congresso Nacional.

A Medida Provisória é o ato normativo de iniciativa exclusiva do Presidente da República, com força de lei, que pode ser expedido em caso de urgência e relevância. Produz efeitos imediatos, mas depende de aprovação do Congresso Nacional para transformação definitiva em lei, nos termos do art. 62 da Constituição Federal[2].

---

[2] Art. 62. Em caso de relevância e urgência, o Presidente da República poderá adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional.
§ 1º É vedada a edição de medidas provisórias sobre matéria:
I – relativa a:
a) nacionalidade, cidadania, direitos políticos, partidos políticos e direito eleitoral;
b) direito penal, processual penal e processual civil;
c) organização do Poder Judiciário e do Ministério Público, a carreira e a garantia de seus membros;
d) planos plurianuais, diretrizes orçamentárias, orçamento e créditos adicionais e suplementares, ressalvado o previsto no art. 167, § 3º;
II – que vise a detenção ou sequestro de bens, de poupança popular ou qualquer outro ativo financeiro;
III – reservada a lei complementar;
IV – já disciplinada em projeto de lei aprovado pelo Congresso Nacional e pendente de sanção ou veto do Presidente da República.
§ 2º Medida provisória que implique instituição ou majoração de impostos, exceto os previstos nos arts. 153, I, II, IV, V, e 154, II, só produzirá efeitos no exercício financeiro seguinte se houver sido convertida em lei até o último dia daquele em que foi editada.
§ 3º As medidas provisórias, ressalvado o disposto nos §§ 11 e 12 perderão eficácia, desde a edição, se não forem convertidas em lei no prazo de sessenta dias, prorrogável, nos termos do § 7º, uma vez por igual período, devendo o Congresso Nacional disciplinar, por decreto legislativo, as relações jurídicas delas decorrentes.
§ 4º O prazo a que se refere o § 3º contar-se-á da publicação da medida provisória, suspendendo-se durante os períodos de recesso do Congresso Nacional.
§ 5º A deliberação de cada uma das Casas do Congresso Nacional sobre o mérito das medidas provisórias dependerá de juízo prévio sobre o atendimento de seus pressupostos constitucionais.
§ 6º Se a medida provisória não for apreciada em até quarenta e cinco dias contados de sua publicação, entrará em regime de urgência, subsequentemente, em cada uma das Casas do Congresso Nacional, ficando sobrestadas, até que se ultime a votação, todas as demais deliberações legislativas da Casa em que estiver tramitando.
§ 7º Prorrogar-se-á uma única vez por igual período a vigência de medida provisória que, no prazo de sessenta dias, contado de sua publicação, não tiver a sua votação encerrada nas duas Casas do Congresso Nacional.

A Lei Delegada é elaborada pelo Presidente da República, a pedido, e por delegação expressa do Poder Legislativo, mediante resolução que especifica o conteúdo e os termos do exercício dessa prerrogativa. Não pode versar sobre os seguintes tópicos: atos de competência exclusiva do Congresso Nacional; matéria reservada à lei complementar; legislação sobre planos plurianuais, diretrizes orçamentárias e orçamentos; entre outros.

O Decreto Legislativo é uma norma aprovada pelo Congresso Nacional no uso de suas atribuições exclusivas constantes do art. 49 da Constituição Federal[3] com a finalidade de regulamentar os assuntos ali dispostos. Segundo a doutrina, os decretos legislativos são

§ 8º As medidas provisórias terão sua votação iniciada na Câmara dos Deputados.
§ 9º Caberá à comissão mista de Deputados e Senadores examinar as medidas provisórias e sobre elas emitir parecer, antes de serem apreciadas, em sessão separada, pelo plenário de cada uma das Casas do Congresso Nacional.
§ 10. É vedada a reedição, na mesma sessão legislativa, de medida provisória que tenha sido rejeitada ou que tenha perdido sua eficácia por decurso de prazo.
§ 11. Não editado o decreto legislativo a que se refere o § 3º até sessenta dias após a rejeição ou perda de eficácia de medida provisória, as relações jurídicas constituídas e decorrentes de atos praticados durante sua vigência conservar-se-ão por ela regidas.
§ 12. Aprovado projeto de lei de conversão alterando o texto original da medida provisória, esta manter-se-á integralmente em vigor até que seja sancionado ou vetado o projeto.

[3] Art. 49. É da competência exclusiva do Congresso Nacional:
I - resolver definitivamente sobre tratados, acordos ou atos internacionais que acarretem encargos ou compromissos gravosos ao patrimônio nacional;
II - autorizar o Presidente da República a declarar guerra, a celebrar a paz, a permitir que forças estrangeiras transitem pelo território nacional ou nele permaneçam temporariamente, ressalvados os casos previstos em lei complementar;
III - autorizar o Presidente e o Vice-Presidente da República a se ausentarem do País, quando a ausência exceder a quinze dias;
IV - aprovar o estado de defesa e a intervenção federal, autorizar o estado de sítio, ou suspender qualquer uma dessas medidas;
V - sustar os atos normativos do Poder Executivo que exorbitem do poder regulamentar ou dos limites de delegação legislativa;
VI - mudar temporariamente sua sede;
VII - fixar idêntico subsídio para os Deputados Federais e os Senadores, observado o que dispõem os arts. 37, XI, 39, § 4º, 150, II, 153, III, e 153, § 2º, I;
VIII - fixar os subsídios do Presidente e do Vice-Presidente da República e dos Ministros de Estado, observado o que dispõem os arts. 37, XI, 39, § 4º, 150, II, 153, III, e 153, § 2º, I;
IX - julgar anualmente as contas prestadas pelo Presidente da República e apreciar os relatórios sobre a execução dos planos de governo;
X - fiscalizar e controlar, diretamente, ou por qualquer de suas Casas, os atos do Poder Executivo, incluídos os da administração indireta;
XI - zelar pela preservação de sua competência legislativa em face da atribuição normativa dos outros Poderes;
XII - apreciar os atos de concessão e renovação de concessão de emissoras de rádio e televisão;
XIII - escolher dois terços dos membros do Tribunal de Contas da União;
XIV - aprovar iniciativas do Poder Executivo referentes a atividades nucleares;
XV - autorizar referendo e convocar plebiscito;
XVI - autorizar, em terras indígenas, a exploração e o aproveitamento de recursos hídricos e a pesquisa e lavra de riquezas minerais;
XVII - aprovar, previamente, a alienação ou concessão de terras públicas com área superior a dois mil e quinhentos hectares.

"atos destinados a regular matérias de competência exclusiva do Congresso Nacional (artigo 49) que tenham efeitos externos a ele[4].

A resolução é um ato normativo, editada pelo Poder Legislativo, no uso de suas atribuições fixadas pela Constituição Federal, para regular matéria da competência privativa da Casa legislativa, de caráter político, processual, legislativo ou administrativo.

O Decreto é o ato de natureza administrativa da competência privativa do Poder Executivo (Presidente da República, Governadores e Prefeitos) e é usualmente usado pelo chefe do poder executivo para fazer nomeações e regulamentações de leis. O Decreto Lei também é emanado pelo Poder Executivo, contudo, tem força de lei e é, normalmente, uma ferramenta do chefe do Poder Executivo para dar imediata efetividade para um desejo político da administração.

A Portaria é um documento de ato administrativo de qualquer autoridade pública, que contém instruções acerca da aplicação de leis ou regulamentos, recomendações de caráter geral, normas de execução de serviço, nomeações, demissões, punições, ou qualquer outra determinação de sua competência.

E por fim, as instruções normativas são atos normativos expedidos por autoridades administrativas, normas complementares das leis, dos tratados e das convenções internacionais e dos decretos, e não podem transpor, inovar ou modificar o texto das normas que complementam. As instruções normativas visam regulamentar ou implementar o que está previsto nas leis.

3. A LEGISLAÇÃO BRASILEIRA RELACIONADA À SEGURANÇA DA INFORMAÇÃO

A segurança da informação é definida no art. 2º, inciso II, do Decreto n.º 3.505, de 13 de junho de 2000, como a 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, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as

[4] SILVA, José Afonso da. Curso de Direito Constitucional positivo. 33ª ed. Atual. São Paulo. Malheiros, 2010, p. 525.

destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Na legislação brasileira há diversos dispositivos legais esparsos relacionados à segurança da informação, os quais serão abordadas a seguir, divididos nos seguintes tópicos: Constituição Federal; Códigos; Leis Ordinárias e Complementares e Decretos.

3.1. Constituição Federal – CF/88

A Constituição Federal traz como direitos e garantias fundamentais aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, determinando que 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, conforme se depreende do inciso X do art. 5º, donde se conclui ser sigiloso as informações relacionadas à intimidade ou à vida privada do cidadão.

O inciso XII do supracitado artigo garante que 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, razão pela qual se infere o direito à privacidade das comunicações privadas e dos dados telemáticos.

Por sua vez, o inciso XIV garante a todos o acesso à informação e o resguardo do sigilo da fonte, quando necessário ao exercício profissional. O direito à informação e ao acesso aos registros públicos vem descrito no inciso XXXIII, o qual determina que 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. Logo, qualquer cidadão pode ter acesso às informações constantes nos órgãos públicos, com exceção das sigilosas, sendo que a Lei n.º 12.527, de 18 de novembro de 2011, regulamentou este acesso. Salienta-se que a referida lei será tratada oportunamente no presente relatório.

Ainda no que tange a disponibilidade das informações constantes em órgãos públicos, o inciso XXXIV do art. 5º da Constituição Federal garante ao cidadão o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder e ainda a obtenção de certidões em repartições públicas para defesa de direitos e esclarecimento de situações de interesse social.

O art. 23, em seus incisos III e IV, relata que é de competência comum da União, dos Estados, do Distrito Federal e dos Municípios, proteger os documentos, bem como, impedir a evasão e a destruição, assim, cabe ao Estado a proteção da integridade, da autenticidade e da disponibilidade das informações constantes nos órgãos e entidades integrantes da Administração Pública, e ainda, a sua gestão, nos termos do art. 216, §2º da Constituição Federal[5].

A Constituição Federal determina ainda, em seu art. 37, que a Administração Pública deve obedecer aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência, sendo o Estado responsável por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos (§ 6º do art. 37), assim como, que o acesso a informações privilegiadas deve ser regulamentado por lei, que determinará os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que venha a ter acesso a tais dados (§ 7º do art. 37).

3.2. Código Penal - CP

O Código Penal Brasileiro foi instituído pelo Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 e desde então passou por diversas modificações, visando assim, torná-lo mais coerente com as características da sociedade atual. De acordo com Luiz Régis Prado, “O Direito Penal é o setor ou parcela do ordenamento jurídico público que estabelece as ações ou omissões delitivas, cominando-lhes determinadas consequências jurídicas – penas ou medidas de segurança. Enquanto sistema normativo, integra-se por normas jurídicas (mandamentos e proibições) que criam o injusto penal e suas respectivas consequências”[6].

[5] § 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.

[6] PRADO, Luiz Régis. Curso de Direito Penal Brasileiro v.1. São Paulo: RT, 2008. p.55

Dessa forma, o presente tópico visa abordar as condutas delitivas descritas no Código Penal quanto à segurança da informação, a começar pelo art. 151, que descreve o crime de violação de correspondência fechada dirigida a outrem, sonegação ou destruição de correspondência, e violação de comunicação telegráfica, radioelétrica ou telefônica, que é punido com pena de detenção de um a seis meses ou multa.

Por sua vez o art. 152 tipifica o crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial, abusando da condição de sócio ou empregado, determinando uma pena de detenção de três meses a dois anos, para o agente que venha a comete-lo.

O § 1º-A do art. 153 relata que é punível com pena de um a quatro anos e multa, o agente que divulgar, sem justa causa, informações sigilosas ou reservadas contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Já quem revelar a alguém segredo de que tem ciência em razão da função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem, a pena é de detenção, de três meses a um ano ou multa, nos termos do art. 154.

É tipificado como crime no art. 154-A do Código Penal a invasão a dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, cuja pena é de detenção de três meses a um ano e multa.

Cabe ressaltar que se a invasão resultar em prejuízo econômico, a pena é aumentada de um sexto a um terço e se forem obtidos conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, ou o controle remoto não autorizado do dispositivo invadido, a pena será de reclusão, podendo ser aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

No art. 266 é previsto o crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, cuja pena é de detenção, de um a três anos, e multa. Registra-se que incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-

lhe o restabelecimento, sendo aplicada em dobro a pena, se o crime for cometido por ocasião de calamidade pública.

A falsificação de documento público é o crime tipificado no art. 297, e consiste em falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro, punível com reclusão de dois a seis anos, e multa, sendo aumentada a pena de sexta parte, caso o agente for funcionário público e cometer o crime prevalecendo-se do cargo.

O crime de supressão de documento é previsto no art. 305 e traz como conduta a destruição, supressão ou ocultação, em benefício próprio ou de outrem, ou em prejuízo alheio, de documento público ou particular verdadeiro, de que não podia dispor. A pena descrita é de 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.

O uso ou divulgação de conteúdo sigiloso dos certames de interesse público é objeto do crime descrito no art. 311-A[7], que é punível com reclusão de um a seis anos, sendo aumentada em um terço se for cometido por funcionário público.

O crime de inserção de dados falsos em sistema de informações consiste em 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. É tipificado no art. 313-A e tem como pena reclusão, de 2 (dois) a 12 (doze) anos, e multa.

A modificação ou alteração não autorizada de sistema de informações, sem autorização ou solicitação da autoridade competente é delito descrito no art. 313-B, cuja pena é de detenção, de 3 (três) meses a 2 (dois) anos e multa, e serão aumentadas de um terço até

[7] Art. 311-A. Utilizar ou divulgar, indevidamente, com o fim de beneficiar a si ou a outrem, ou de comprometer a credibilidade do certame, conteúdo sigiloso de:
I - concurso público;
II - avaliação ou exame públicos;
III - processo seletivo para ingresso no ensino superior; ou
IV - exame ou processo seletivo previstos em lei:
Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§1º Nas mesmas penas incorre quem permite ou facilita, por qualquer meio, o acesso de pessoas não autorizadas às informações mencionadas no caput.
§2º Se da ação ou omissão resulta dano à administração pública:
Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.
§3º Aumenta-se a pena de 1/3 (um terço) se o fato é cometido por funcionário público.

a metade se da modificação ou alteração resultar dano para a Administração Pública ou para o administrado.

A violação de sigilo profissional, que consiste em revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação é tipificado como crime no art. 325, cuja pena é de detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. Também, incorre nas mesmas penas quem 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; ou se utiliza, indevidamente, do acesso restrito.

Por fim, importante registrar que o Código de Processo Penal, que é o conjunto de regras e princípios destinados à organização da justiça penal e aplicação dos preceitos contidos no Direito Penal, instituído pelo Decreto-Lei n.º 3.689, de 3 de outubro de 1941, garante o sigilo das informações quando necessárias para elucidação do fato ou exigido pelo interesse da sociedade, como por exemplo, na tramitação do inquérito policial (art. 20)[8] e nas diligências que o Juiz entenda necessárias (art. 745)[9].

3.3. Código Tributário Nacional - CTN

A Lei n.º 5.172 de 25 de outubro de 1966, que dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, aos Estados e Municípios, determina em seu art. 198, que 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, salvo quando: (i) for requisitada por autoridade judiciária no interesse da justiça; ou (ii) solicitada por 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.

[8] Art. 20. A autoridade assegurará no inquérito o sigilo necessário à elucidação do fato ou exigido pelo interesse da sociedade.

[9] Art. 745. O juiz poderá ordenar as diligências necessárias para apreciação do pedido, cercando-as do sigilo possível e, antes da decisão final, ouvirá o Ministério Público.

No entanto, importante ressaltar, que é permitido a prestação de assistência e a permuta de informações entre a Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios, com a finalidade de fiscalização dos tributos respectivos, nos termos do art. 199 do Código Tributário Nacional[10].

3.4. Consolidação das Leis do Trabalho - CLT

A Consolidação das Leis do Trabalho, instituída pelo Decreto-Lei n.º 5.452, de 1º de maio de 1943, traz em seu art. 482, alínea "g", que a violação de segredo da empresa, constitui justa causa para rescisão do contrato de trabalho pelo empregador, sendo assim, patente a proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista), haja vista ser considerada falta grave punível com a perda do emprego, sem prejuízo de eventuais indenizações.

3.5. Código de Defesa do Consumidor - CDC

O Código de Defesa do Consumidor, instituído pela Lei n.º 8.078, de 11 de setembro de 1990, trata na Seção VI especificamente sobre bancos de dados e cadastro de consumidores, garantindo o direito de acesso do consumidor às suas informações pessoais arquivadas em bancos de dados (cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele), bem como sobre as suas respectivas fontes, nos termos do art. 43. O mesmo artigo garante em seus §§ 2º e 3º[11] que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" e que "o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção".

---

[10] Art. 199. A Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios prestar-se-ão mutuamente assistência para a fiscalização dos tributos respectivos e permuta de informações, na forma estabelecida, em caráter geral ou específico, por lei ou convênio.
Parágrafo único. A Fazenda Pública da União, na forma estabelecida em tratados, acordos ou convênios, poderá permutar informações com Estados estrangeiros no interesse da arrecadação e da fiscalização de tributos.

[11] § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
3 O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas

Por sua vez o § 4º do supracitado artigo considera os bancos de dados de consumidores algo de caráter público. Desta forma, em uma interpretação integrativa da lei, o acesso aos bancos de dados de registros pessoais das relações de consumo é igualmente assegurado por meio de *habeas data*.

Ademais, o CDC estabeleceu para o consumidor o direito de acesso e retificação de informações suas que sejam armazenadas por fornecedores, além da vedação da manutenção deste registro por mais de 5 anos[12].

Por fim, tem-se que o art. 44 determina que 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. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor, sendo, facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.

Logo, infere-se dos artigos 43 e 44 do Código de Defesa do Consumidor, que as atividades dos bancos de dados e cadastros de consumidores, e as regras para seu funcionamento, determinam que os cadastros e dados devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, razão pela qual não podem fornecer informações dubitáveis sobre o consumidor, pois assim ultrapassam os limites legais que legitimam sua atividade e se sujeitam às penas legais cominadas.

3.6. Código de Alta Conduta da Administração e Código de Ética Profissional do Servidor Público do Poder Executivo Federal

Aprovado em 21 de agosto de 2000, o Código de Conduta da Alta Administração Federal foi instituído com a finalidade de tornar claras as regras éticas de conduta das autoridades da alta Administração Pública Federal sobre conflitos de interesses públicos e privados e limitações às atividades profissionais posteriores ao exercício de cargo público, devendo ser observado por Ministros e Secretários de Estado, titulares de cargos de natureza especial, secretários-executivos, secretários ou autoridades equivalentes e presidentes e diretores de agências nacionais, autarquias, inclusive as especiais,

[12] DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. P. 17

fundações mantidas pelo Poder Público, empresas públicas e sociedades de economia mista.

O art. 3º do Código em questão determina que a autoridade pública, no prazo de dez dias contados de sua posse, enviará à Comissão de Ética Pública – CEP[13] informações sobre sua situação patrimonial que, real ou potencialmente, possa suscitar conflito com o interesse público, indicando o modo pelo qual irá evitá-lo.

A teor do §4º do Art. 5º do mesmo *Códex*, 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.

Outro ponto a ser destacado do Código de Conduta da Alta Administração Federal no que tange a segurança da informação é o inciso II do art. 14, que proíbe a autoridade pública que deixar o cargo a 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, onde se denota a proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

Por sua vez, o Código de Ética do Profissional do Servidor Público do Poder Executivo Federal, aprovado por meio do Decreto n.º 1.171, de 22 de junho de 1994, determina que é vedado ao servidor público alterar ou deturpar o teor de documentos que deva encaminhar para providências, bem como, retirar da repartição pública, sem estar legalmente autorizado, qualquer documento, livro ou bem pertencente ao patrimônio público. (Alínea “h” e “l” do inciso XV da Seção II).

Traz ainda que o Servidor Público deve conferir publicidade a qualquer ato administrativo, como requisito de eficácia e moralidade, ensejando sua omissão comprometimento ético contra o bem comum, imputável a quem a negar, salvo em casos de segurança nacional, investigações policiais ou interesse superior do Estado e da

[13] Comissão de Ética Pública - CEP, criada pelo Decreto de 26 de maio de 1999, do Presidente da República, no uso da atribuição que lhe confere o art. 84, inciso VI da Constituição Federal e publicado no Diário Oficial da União do dia 27 de maio de 1999.

Administração Pública, a serem preservados em processo previamente declarado sigiloso, nos termos da lei.

3.7. Leis Ordinárias e Complementares

A Lei n.º 6.538, de 22 de junho de 1978, que dispõe sobre os serviços postais, em seu art. 5º determina que o sigilo da correspondência é inviolável, sendo punível com pena de detenção de três meses a um ano, ou multa, o profissional do serviço postal que violar o sigilo profissional, nos termos do art. 41 da supracitada legislação.

A proteção das informações sigilosas relacionadas à segurança nacional é tratada pela Lei n.º 7.170, de 14 de dezembro de 1983, que define os crimes contra a segurança nacional, a ordem política e social, e traz em seu art. 13[14], o crime de espionagem ou divulgação de informações sigilosas a grupo estrangeiro, ou a organização ou grupo de existência ilegal, que é punido com reclusão de três a quinze anos.

A Política Nacional de Informática, que tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico, instituída pela Lei n.º 7.232, de 29 de outubro de 1984, traz em seu art. 2º, inciso VIII e IX, que devem ser estabelecidos 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, bem como para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas.

[14] 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 aero fotográfica ou de sensoriamento 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.

Para tanto, foram definidos como instrumentos da Política Nacional de Informática: I - o estímulo ao crescimento das atividades de informática de modo compatível com o desenvolvimento do País; II - a institucionalização de normas e padrões de homologação e certificação de qualidade de produtos e serviços de informática; III - a mobilização e a aplicação coordenadas de recursos financeiros públicos destinados ao fomento das atividades de informática; IV - o aperfeiçoamento das formas de cooperação internacional para o esforço de capacitação do País; V - a formação, o treinamento e o aperfeiçoamento de recursos humanos para o setor; VI - a instituição de regime especial de concessão de incentivos tributários e financeiros, em favor de empresas nacionais, destinados ao crescimento das atividades de informática; VII - as penalidades administrativas pela inobservância de preceitos desta Lei e regulamento; VIII - o controle das importações de bens e serviços de informática por 8 (oito) anos a contar da publicação desta Lei; IX - a padronização de protocolo de comunicação entre sistemas de tratamento da informação; e X - o estabelecimento de programas específicos para o fomento das atividades de informática, pelas instituições financeiras estatais.

Por sua vez, a proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários é o objeto do art. 18 da Lei n.º 7.492, de 16 de junho de 1986, que determina que a violação do 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, resulta na pena de reclusão de um a quatro anos e multa.

A conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas é o objeto da Lei n.º 8.027, de 12 de abril de 1990, que prevê em seu art. 5º, inciso I[15], a pena de demissão para o servidor que se valer ou permitir dolosamente que terceiros tirem proveito de informação obtida em função do cargo, para lograr, proveito pessoal ou de outrem, bem como, que revele segredo de que teve conhecimento em função do cargo ou emprego (inciso V, parágrafo único do art. 5º), com a finalidade de proteger as informações privilegiadas produzidas ou acessadas no exercício de cargo ou função

[15] 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;

pública. Com a mesma intenção há a determinação contida na Lei n.º 8.112, de 11 de dezembro de 1990, em seu art. 116, inciso VIII[16] e o art. 132, inciso IX[17].

O art. 11, inciso III, IV e VII da Lei n.º 8.429, de 2 de junho de 1992, que trata das sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional, também visa a proteção das informações obtidas no exercício da função, relatando que constitui ato de improbidade administrativa revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo; negar publicidade aos atos oficiais; e revelar ou permitir que chegue ao conhecimento de terceiro, antes da respectiva divulgação oficial, teor de medida política ou econômica capaz de afetar o preço de mercadoria, bem ou serviço.

Aos servidores do Tribunal de Contas da União que exercem funções específicas de controle externo é aplicável o disposto no art. 86 da Lei n.º 8.443, de 16 de julho de 1992, onde se infere que este deve guardar sigilo sobre dados e informações obtidos em decorrência do exercício de seus cargos e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.

A proteção da disponibilidade de informações para manutenção da ordem tributária é a matéria tratada na Lei n.º 8.137, de 27 de dezembro de 1990, que define crimes contra a ordem tributária, econômica e contra as relações de consumo, além daqueles contidos no Código Penal, relata no art. 3º, que o crime funcional contra a ordem tributária é punido com pena de três a oito anos e multa, e consiste em 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.

A Lei Complementar n.º 75, de 20 de maio de 1993, em seu art. 8º, incisos II, VIII garante ao Ministério Público da União, no exercício de suas atribuições, ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública e requisitar informações, exames, perícias e documentos de autoridades

[16] Art. 116. São deveres do servidor:
VIII - guardar sigilo sobre assunto da repartição;
[17] Art. 132. A demissão será aplicada nos seguintes casos:
IX - revelação de segredo do qual se apropriou em razão do cargo;

da Administração Pública direta ou indireta. Por sua vez, o § 1º do supracitado artigo, relata que o membro do Ministério Público será civil e criminalmente responsável pelo uso indevido das informações e documentos que requisitar. Cabe ressaltar que o mesmo direito é garantido aos Ministérios Públicos Estaduais, por meio do art. 26, inciso I, alínea b e inciso II da Lei n.º 8.625, de 12 de fevereiro de 1993.

A proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas é o intuito da Lei n.º 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, que em seu art. 72 tipifica como crime, puníveis como reclusão de cinco a dez anos: a) obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; b) 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; c) causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes. O mesmo intuito possui o art. 67, incisos VII e VIII, da Lei n.º 9.100, de 29 de setembro de 1995, que tipifica o crime de fraude eleitoral nas eleições municipais, prevendo a pena de reclusão de três a seis anos.

A Lei n.º 9.296, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, trata do sigilo dos dados e das comunicações privadas, sendo que em seu art. 10 tipifica como 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, cuja pena é de reclusão de dois a quatro anos e multa.

O sigilo das informações também é matéria tratada na Lei n.º 9.472, de 16 de julho 1997, que dispõe sobre a organização dos serviços de telecomunicações, que garante ao usuário dos serviços de telecomunicações, nos termos do art. 3, incisos V, VI e IX: (i) à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas; (ii) à não divulgação, caso o requeira, de seu código de acesso; e (iii) ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço.

Todavia, a Lei n.º 10.703, de 18 de julho de 2003, garante a disponibilidade dos dados cadastrais para fins de investigação criminal, determinando que incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. Os dados constantes do cadastro, salvo motivo justificado, deverão ser imediatamente disponibilizados pelos prestadores de serviços para atender solicitação da autoridade judicial, sob pena de multa por infração cometida.

Por fim, cabe ressaltar que a Lei n.º 10.683, de 28 de maio de 2003, que trata da organização da Presidência da República e dos Ministérios, determina por meio do art. 6º, inciso VI, que a coordenação das atividades de inteligência federal e de segurança da informação compete ao Gabinete de Segurança Institucional da Presidência da República.

3.8. Decretos da Presidência da República.

Rememorando, os Decretos editados pelo Presidente da República regulamentam as Leis e dispõem sobre a organização da administração pública. Desse modo, o Decreto n.º 3.505, de 13 de junho de 2000, institui a Política de Segurança da Informação nos órgãos e 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) a 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 tecnologias sensíveis e duais; (v) criação, desenvolvimento e manutenção de mentalidade de segurança da informação; (vi) capacitação científico-tecnológica 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.

Para tanto, criou o Comitê Gestor da Segurança da Informação, composto por um representante de cada Ministério e órgãos listados no art. 7º do Decreto n.º 3.505/2000[18],

18 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; V - Ministério da Previdência Social; VI -

coordenado pelo Gabinete de Segurança Institucional da Presidência da República, possuindo a finalidade 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 seguintes objetivos:

> I - 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;
>
> 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.

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; X - Ministério da Ciência, Tecnologia e Inovação; XI - Casa Civil da Presidência da República; XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará; XIII - Secretaria de Comunicação Social da Presidência da República; XIV - Ministério de Minas e Energia; XIV - Ministério de Minas e Energia; XV - Controladoria-Geral da União; XVI - Advocacia-Geral da União; XVI - Advocacia-Geral da União; XVII - Secretaria-Geral da Presidência da República.

Com a intuito de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério, inclusive aquelas pertinentes a segurança da informação, foi criada a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, pelo Decreto n.º 4.801, de 6 de agosto de 2003, regulamentando o inciso II do art. 7º da Lei n.º 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios.

Compete a Câmara de Relações Exteriores e Defesa Nacional, presidida pelo Chefe do Gabinete de Segurança Institucional da Presidência da República e integrada pelos Ministros de Estado enumerados no art. 2º do Decreto n.º 4.801/2003[19], aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidas pertinentes a: I - cooperação internacional em assuntos de segurança e defesa; II - integração fronteiriça; III - populações indígenas; IV - direitos humanos; V - operações de paz; VI - narcotráfico e a outros delitos de configuração internacional; VII - imigração; VIII - atividade de inteligência; IX - segurança para as infraestruturas críticas, incluindo serviços; X - segurança da informação; e XI - segurança cibernética.

Por meio do Decreto n.º 5.687, de 31 de janeiro de 2006, foi promulgada a Convenção das Nações Unidas contra a Corrupção, assinada pelo Brasil em 9 de dezembro de 2003, segundo a qual, cada Estado signatário se comprometeu a se esforçar para implementar, entre outras, as seguintes medidas, com o objetivo disponibilizar as informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos:

> 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;

19 Art. 2º A Câmara de Relações Exteriores e Defesa Nacional será integrada pelos seguintes Ministros de Estado: I - Chefe do Gabinete de Segurança Institucional da Presidência da República, que a presidirá; II - Chefe da Casa Civil da Presidência da República; III - da Justiça; IV - da Defesa; V - das Relações Exteriores; VI - do Planejamento, Orçamento e Gestão; VII - do Meio Ambiente; VIII - da Ciência e Tecnologia; IX - da Fazenda; X - Chefe da Secretaria de Assuntos Estratégicos da Presidência da República; XI - da Saúde; XII - das Comunicações; XIII - da Integração Nacional; XIV - de Minas e Energia; e XV - dos Transportes.

b) A simplificação dos procedimentos administrativos, quando proceder, a fim de facilitar o acesso do público às autoridades encarregadas da adoção de decisões;

c) A publicação de informação, o que poderá incluir informes periódicos sobre os riscos de corrupção na administração pública;

d) aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões; e

e) garantir o acesso eficaz do público à informação.

Importante ressaltar que compete ao Gabinete de Segurança Institucional da Presidência da República: (i) coordenar a execução de ações de segurança da informação e comunicações na administração pública federal; (ii) definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal; (iii) operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal; (iv) avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações; e (v) coordenar as atividades relacionadas à segurança e ao credenciamento de pessoas e de empresas no trato de assuntos e documentos sigilosos, nos termos do art. 6º do Decreto n.º 8.100, de 4 de setembro de 2013.

4. LEGISLAÇÃO BRASILEIRA ESPECÍFICA À SEGURANÇA DA INFORMAÇÃO

4.1. Lei n.º 8.159/91, de 08 de janeiro de 1991. Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências

A Política Nacional de Arquivos Públicos e Privados determina que é dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação, definindo como arquivos, 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. 2º da Lei 8.159/91).

Por gestão documental entende-se o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (art. 3º da Lei 8.159/91).

Cabe ressaltar que a Política Nacional de Arquivos Públicos e Privados garante a todos o direito de 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 (art. 4º e 5º da Lei n.º 8.159/91), bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, ficando resguardado o direito de indenização pelo dano material ou moral decorrente da violação do sigilo, sem prejuízo das ações penal, civil e administrativa (art. 6º da Lei n.º 8.159/91), sendo que o acesso a estas informações atualmente é regulado pela Lei de Acesso à Informação (Lei n.º 12.527/2011), que será abordada em tópico especifico.

A administração dos arquivos públicos[20] ou de caráter público compete às instituições arquivistas federais, estaduais, do Distrito Federal e municipais, competindo ao Arquivo

[20] Art. 7º - Os arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias.
§1º - São também públicos os conjuntos de documentos produzidos e recebidos por instituições de caráter público, por entidades privadas encarregadas da gestão de serviços públicos no exercício de suas atividades.

Nacional a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Executivo Federal, bem como preservar e facultar o acesso aos documentos sob sua guarda, e acompanhar e implementar a política nacional de arquivos.

Por sua vez, consideram-se arquivos privados os conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, em decorrência de suas atividades, podendo os arquivos privados serem identificados pelo Poder Público como de interesse público e social, desde que sejam considerados como conjuntos de fontes relevantes para a história e desenvolvimento científico nacional, razão pela qual não poderão ser alienados com dispersão ou perda da unidade documental, nem transferidos para o exterior. Um exemplo de arquivos privados identificados como de interesse público e social são registros civis de arquivos de entidades religiosas produzidos anteriormente à vigência do Código Civil.

Vinculado ao Arquivo Nacional do Ministério da Justiça encontra-se o Conselho Nacional de Arquivos (CONARQ), que tem por finalidade definir a política nacional de arquivos públicos e privados, como órgão central do Sistema Nacional de Arquivos (SINAR) e exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo.

O SINAR é regulamentado pelo Decreto n.º 4.073, de 3 de janeiro de 2002 e integrado pelo: I - Arquivo Nacional; II - os arquivos do Poder Executivo Federal; III - os arquivos do Poder Legislativo Federal; IV - os arquivos do Poder Judiciário Federal; V - os arquivos estaduais dos Poderes Executivo, Legislativo e Judiciário; VI - os arquivos do Distrito Federal dos Poderes Executivo, Legislativo e Judiciário; e VII - os arquivos municipais dos Poderes Executivo e Legislativo.

---

§2º - A cessação de atividades de instituições públicas e de caráter público implica o recolhimento de sua documentação à instituição arquivística pública ou a sua transferência à instituição sucessora.
Art. 8º - Os documentos públicos são identificados como correntes, intermediários e permanentes.
§1º - Consideram-se documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes.
§2º - Consideram-se documentos intermediários aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente.
§3º - Consideram-se permanentes os conjuntos de documentos de valor histórico, probatório e informativo que devem ser definitivamente preservados.
Art. 9º - A eliminação de documentos produzidos por instituições públicas e de caráter público será realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência.
Art. 10 - Os documentos de valor permanente são inalienáveis e imprescritíveis.

Compete aos integrantes do SINAR: (i) promover a gestão, a preservação e o acesso às informações e aos documentos na sua esfera de competência, em conformidade com as diretrizes e normas emanadas do órgão central; (ii) disseminar, em sua área de atuação, as diretrizes e normas estabelecidas pelo órgão central, zelando pelo seu cumprimento; implementar a racionalização das atividades arquivistas, de forma a garantir a integridade do ciclo documental; (iii) garantir a guarda e o acesso aos documentos de valor permanente; apresentar sugestões ao CONARQ para o aprimoramento do SINAR; (iv) prestar informações sobre suas atividades ao CONARQ; apresentar subsídios ao CONARQ para a elaboração de dispositivos legais necessários ao aperfeiçoamento e à implementação da política nacional de arquivos públicos e privados; (v) promover a integração e a modernização dos arquivos em sua esfera de atuação; (vi) propor ao CONARQ os arquivos privados que possam ser considerados de interesse público e social; (vii) comunicar ao CONARQ, para as devidas providências, atos lesivos ao patrimônio arquivístico nacional; (viii) colaborar na elaboração de cadastro nacional de arquivos públicos e privados, bem como no desenvolvimento de atividades censitárias referentes a arquivos; possibilitar a participação de especialistas nas câmaras técnicas, câmaras setoriais e comissões especiais constituídas pelo CONARQ; e (ix) proporcionar aperfeiçoamento e reciclagem aos técnicos da área de arquivo, garantindo constante atualização.

4.2. Lei n.º 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

O *habeas data* é o remédio jurídico que tem como objetivo: (i) 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) a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; e (iii) a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.

Os processos de *habeas data* têm prioridade sobre todos os atos judiciais, exceto *habeas-corpus* e mandado de segurança, sendo isento de custas, tanto no âmbito judicial quanto no procedimento administrativo para acesso a informações e retificação de dados e para anotação de justificação, devendo o prazo para proceder a conclusão do processo não exceder de vinte e quatro horas, a contar da distribuição.

O julgamento do *habeas data* compete originariamente: a) ao Supremo Tribunal Federal, contra atos do Presidente da República, das Mesas da Câmara dos Deputados e do Senado Federal, do Tribunal de Contas da União, do Procurador-Geral da República e do próprio Supremo Tribunal Federal; b) ao Superior Tribunal de Justiça, contra atos de Ministro de Estado ou do próprio Tribunal; c) aos Tribunais Regionais Federais contra atos do próprio Tribunal ou de juiz federal; d) a juiz federal, contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais; e) a tribunais estaduais, segundo o disposto na Constituição do Estado; e f) a juiz estadual, nos demais casos.

4.3. Lei n.º 9.883, de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN e dá outras providências.

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.

Para os efeitos de aplicação da Lei n.º 9.883/1999 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.

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, tendo como órgão central a Agência Brasileira de Inteligência - ABIN, órgão da Presidência da República, a quem compete planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, dentre outras, a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade. Para tanto, objetivando o desempenho de suas atribuições, é facultada a ABIN firmar

convênios, acordos, contratos e quaisquer outros ajustes, observada a legislação e normas pertinentes, nos termos do art. 7º.

A execução da Política Nacional de Inteligência, fixada pelo Presidente da República, será levada a efeito pela ABIN, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, sendo que quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los, pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Cabe ressaltar que a autoridade ou qualquer outra pessoa que tiver conhecimento ou acesso aos documentos, obriga-se a manter o respectivo sigilo, sob pena de responsabilidade administrativa, civil e penal, e, em se tratando de procedimento judicial, fica configurado o interesse público de que trata o art. 155, inciso I, do Código de Processo Civil, devendo qualquer investigação correr, igualmente, sob sigilo.

O Decreto n.º 4.376, de 13 de setembro de 2002, regulamenta a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n.º 9.883, de 7 de dezembro de 1999, determinando em seu art. 4º que este é composto pelos seguintes órgãos:

> I - Casa Civil da Presidência da República, por meio de sua Secretaria-Executiva;
>
> II - Gabinete de Segurança Institucional da Presidência da República, órgão de coordenação das atividades de inteligência federal;
>
> III - Agência Brasileira de Inteligência - ABIN, do Gabinete de Segurança Institucional da Presidência da República, como órgão central do Sistema;
>
> IV - Ministério da Justiça, por meio da Secretaria Nacional de Segurança Pública, da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Departamento de Polícia Rodoviária Federal, do Departamento Penitenciário Nacional e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, da Secretaria Nacional de Justiça;

V - Ministério da Defesa, por meio da Subchefia de Inteligência Estratégica, da Assessoria de Inteligência Operacional, da Divisão de Inteligência Estratégico-Militar da Subchefia de Estratégia do Estado-Maior da Armada, do Centro de Inteligência da Marinha, do Centro de Inteligência do Exército, do Centro de Inteligência da Aeronáutica, e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia;

VI - Ministério das Relações Exteriores, por meio da Secretaria-Geral de Relações Exteriores e da Coordenação-Geral de Combate aos Ilícitos Transnacionais;

VII - Ministério da Fazenda, por meio da Secretaria-Executiva do Conselho de Controle de Atividades Financeiras, da Secretaria da Receita Federal do Brasil e do Banco Central do Brasil;

VIII - Ministério do Trabalho e Emprego, por meio da Secretaria-Executiva;

IX - Ministério da Saúde, por meio do Gabinete do Ministro de Estado e da Agência Nacional de Vigilância Sanitária - ANVISA;

X - Ministério da Previdência Social, por meio da Secretaria-Executiva;

XI - Ministério da Ciência e Tecnologia, por meio do Gabinete do Ministro de Estado;

XII - Ministério do Meio Ambiente, por meio da Secretaria-Executiva e do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis - IBAMA;

XIII - Ministério da Integração Nacional, por meio da Secretaria Nacional de Defesa Civil;

XIV - Controladoria-Geral da União, por meio da Secretaria-Executiva;

XV - Ministério da Agricultura, Pecuária e Abastecimento, por meio de sua Secretaria-Executiva;

XVI - Secretaria de Aviação Civil da Presidência da República, por meio de sua Secretaria-Executiva;

XVII - Ministério dos Transportes, por meio de sua Secretaria-Executiva e do Departamento Nacional de Infraestrutura de Transportes - DNIT;

XVIII - Ministério de Minas e Energia, por meio de sua Secretaria-Executiva; e

XIX - Ministério das Comunicações, por meio de sua Secretaria-Executiva.

Nos termos do art. 6º do supracitado Decreto cabe aos órgãos que compõem o Sistema Brasileiro de Inteligência, no âmbito de suas competências: I - produzir conhecimentos, em atendimento às prescrições dos planos e programas de inteligência, decorrentes da Política Nacional de Inteligência; II - planejar e executar ações relativas à obtenção e integração de dados e informações; III - intercambiar informações necessárias à produção de conhecimentos relacionados com as atividades de inteligência e contra inteligência; IV - fornecer à ABIN, para fins de integração, informações e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais; e V - estabelecer os respectivos mecanismos e procedimentos particulares necessários às comunicações e ao intercâmbio de informações e conhecimentos no âmbito do Sistema, observando medidas e procedimentos de segurança e sigilo, sob coordenação da ABIN, com base na legislação pertinente em vigor.

A ABIN poderá manter, em caráter permanente, representantes dos órgãos componentes do Sistema Brasileiro de Inteligência no Departamento de Integração do Sistema Brasileiro de Inteligência, que tem por atribuição coordenar a articulação do fluxo de dados e informações oportunas e de interesse da atividade de Inteligência de Estado, com a finalidade de subsidiar o Presidente da República em seu processo decisório, sendo que, estes representantes poderão acessar, por meio eletrônico, as bases de dados de seus órgãos de origem, respeitadas as normas e limites de cada instituição e as normas legais pertinentes à segurança, ao sigilo profissional e à salvaguarda de assuntos sigilosos, nos termos do § 4º do Art. 6º-A do Decreto n.º 4.376/2002.

Ao Conselho Consultivo do Sistema Brasileiro de Inteligência, vinculado ao Gabinete de Segurança Institucional compete: I - emitir pareceres sobre a execução da Política Nacional de Inteligência; 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; III - contribuir para o aperfeiçoamento da doutrina de inteligência; IV - opinar sobre propostas de integração de novos órgãos e entidades ao Sistema Brasileiro de Inteligência; V - propor a criação e a extinção de grupos de trabalho para estudar problemas específicos, com atribuições, composição e funcionamento regulados no ato que os instituir; e VI - propor ao seu Presidente o regimento interno.

São membros do Conselho Consultivo do Sistema Brasileiro de Inteligência, presidido pelo Chefe do Gabinete de Segurança Institucional, nos termos do art. 8º, os titulares dos seguintes órgãos:

> I - Gabinete de Segurança Institucional da Presidência da República;
>
> II - Agência Brasileira de Inteligência - ABIN, do Gabinete de Segurança Institucional da Presidência da República;
>
> III - Secretaria Nacional de Segurança Pública, Diretoria de Inteligência Policial do Departamento de Polícia Federal e Departamento de Polícia Rodoviária Federal, todos do Ministério da Justiça;
>
> IV - Subchefia de Inteligência Estratégica, Assessoria de Inteligência Operacional, Divisão de Inteligência Estratégico-Militar da Subchefia de Estratégia do Estado-Maior da Armada, Centro de Inteligência da Marinha, Centro de Inteligência do Exército, Centro de Inteligência da Aeronáutica, e Centro Gestor e Operacional do Sistema de Proteção da Amazônia, todos do Ministério da Defesa;
>
> V - Coordenação-Geral de Combate aos Ilícitos Transnacionais da Subsecretaria-Geral de Assuntos Políticos, do Ministério das Relações Exteriores;
>
> VI - Conselho de Controle de Atividades Financeiras, do Ministério da Fazenda;

Cabe a ABIN na condição de órgão central do Sistema Brasileiro de Inteligência:

> I - estabelecer as necessidades de conhecimentos específicos, a serem produzidos pelos órgãos que constituem o Sistema Brasileiro de Inteligência, e consolidá-las no Plano Nacional de Inteligência;
>
> II - coordenar a obtenção de dados e informações e a produção de conhecimentos sobre temas de competência de mais de um membro do Sistema Brasileiro de Inteligência, promovendo a necessária interação entre os envolvidos;
>
> III - acompanhar a produção de conhecimentos, por meio de solicitação aos membros do Sistema Brasileiro de Inteligência, para assegurar o atendimento da finalidade legal do Sistema;
>
> IV - analisar os dados, informações e conhecimentos recebidos, com vistas a verificar o atendimento das necessidades de conhecimentos estabelecidas no Plano Nacional de Inteligência;

> V - integrar as informações e os conhecimentos fornecidos pelos membros do Sistema Brasileiro de Inteligência;
>
> VI - solicitar dos órgãos e entidades da Administração Pública Federal os dados, conhecimentos, informações ou documentos necessários ao atendimento da finalidade legal do Sistema;
>
> VII - promover o desenvolvimento de recursos humanos e tecnológicos e da doutrina de inteligência, realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência, em coordenação com os demais órgãos do Sistema Brasileiro de Inteligência;
>
> VIII - prover suporte técnico e administrativo às reuniões do Conselho e ao funcionamento dos grupos de trabalho, solicitando, se preciso, aos órgãos que constituem o Sistema colaboração de servidores por tempo determinado, observadas as normas pertinentes; e
>
> IX - representar o Sistema Brasileiro de Inteligência perante o órgão de controle externo da atividade de inteligência.

4.4. Lei Complementar n.º 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

A Lei Complementar n.º 105/2001 determina que as instituições financeiras[21] devem conservar em sigilo suas operações ativas e passivas e serviços prestados, sendo este extensivo ao Banco Central do Brasil, em relação às operações que realizar e às informações que obtiver no exercício de suas atribuições, contudo, relata que não constitui violação do dever de sigilo:

> – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
>
> - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as

[21] São consideradas instituições financeiras, para os efeitos da Lei Complementar n.º 105: I – os bancos de qualquer espécie; II – distribuidoras de valores mobiliários; III – corretoras de câmbio e de valores mobiliários; IV – sociedades de crédito, financiamento e investimentos; V – sociedades de crédito imobiliário; VI – administradoras de cartões de crédito; VII – sociedades de arrendamento mercantil; VIII – administradoras de mercado de balcão organizado; IX – cooperativas de crédito; X – associações de poupança e empréstimo; XI – bolsas de valores e de mercadorias e futuros; XII – entidades de liquidação e compensação; XIII – outras sociedades que, em razão da natureza de suas operações, assim venham a ser consideradas pelo Conselho Monetário Nacional.

normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;

- a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;

- a revelação de informações sigilosas com o consentimento expresso dos interessados;

- a prestação de informações nos termos e condições estabelecidos nos artigos 5º[22], 6º[23], 7º[24] e 9º[25] da Lei Complementar.

No entanto, a supracitada legislação determina que o sigilo, inclusive quanto a contas de depósitos, aplicações e investimentos mantidos em instituições financeiras, não pode ser oposto ao Banco Central do Brasil: (i) no desempenho de suas funções de fiscalização, compreendendo a apuração, a qualquer tempo, de ilícitos praticados por controladores, administradores, membros de conselhos estatutários, gerentes, mandatários e prepostos de instituições financeiras; e (ii) ao proceder o inquérito em instituição financeira submetida a regime especial.

Frisa-se que 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; II – de tráfico ilícito de substâncias entorpecentes ou drogas afins; III – de contrabando ou tráfico de armas, munições ou material destinado a sua produção; IV – de extorsão mediante sequestro; V – contra o sistema financeiro nacional; VI – contra a Administração Pública; VII – contra a

[22] Art. 5º O Poder Executivo disciplinará, inclusive quanto à periodicidade e aos limites de valor, os critérios segundo os quais as instituições financeiras informarão à administração tributária da União, as operações financeiras efetuadas pelos usuários de seus serviços

[23] Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente.

[24] Art. 7º Sem prejuízo do disposto no § 3º do art. 2º, a Comissão de Valores Mobiliários, instaurado inquérito administrativo, poderá solicitar à autoridade judiciária competente o levantamento do sigilo junto às instituições financeiras de informações e documentos relativos a bens, direitos e obrigações de pessoa física ou jurídica submetida ao seu poder disciplinar.

[25] Art. 9º Quando, no exercício de suas atribuições, o Banco Central do Brasil e a Comissão de Valores Mobiliários verificarem a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes, informarão ao Ministério Público, juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos.

ordem tributária e a previdência social; VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores; IX – praticado por organização criminosa.

O Banco Central do Brasil e a Comissão de Valores Mobiliários e as instituições financeiras prestarão as informações ordenadas pelo Poder Judiciário, preservado o seu caráter sigiloso mediante acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide, nos termos do art. 3º. Devem ainda fornecer ao Poder Legislativo Federal, quando se fizerem necessários ao exercício de suas respectivas competências constitucionais e legais (art. 4º).

A quebra de sigilo, fora das hipóteses autorizadas na Lei Complementar, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis.

4.5. Medida Provisória n.º 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

A Medida Provisória n.º 2.200-2 institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para 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 segura.

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão, sendo composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro – AR.

O modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o Instituto Nacional de Tecnologia da Informação, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos[26].

A função de autoridade gestora de políticas é exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco

[26] Disponível em http://www.iti.gov.br/icp-brasil/o-que-e. Acesso em 08 de dezembro de 2014.

representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos órgãos constantes no art. 3º da supracitada legislação[27], competindo a este:

> I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
>
> II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
>
> III - estabelecer a política de certificação e as regras operacionais da AC Raiz;
>
> IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
>
> V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;
>
> VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;
>
> VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e
>
> 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.

[27] Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares: I - Ministério da Justiça; II - Ministério da Fazenda; III - Ministério do Desenvolvimento, Indústria e Comércio Exterior; IV - Ministério do Planejamento, Orçamento e Gestão; V - Ministério da Ciência e Tecnologia; VI - Casa Civil da Presidência da República; e VII - Gabinete de Segurança Institucional da Presidência da República.
§1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.
§2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.
§3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.
§4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

À Autoridade Certificadora 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 Autoridades Certificadoras de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das Autoridades Certificadora e das Autoridades de Registro 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.

As Autoridades Certificadoras, 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 lista de certificados revogados e outras informações pertinentes e manter registro de suas operações. Por sua vez, as Autoridades de Registros, entidades operacionalmente vinculadas a determinada Autoridade Certificadora, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados à Autoridade Certificadora e manter registros de suas operações.

A supracitada legislação determinou ainda que consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos, bem como, que 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.

O Instituto Nacional de Tecnologia da Informação - ITI, autarquia federal criada pela Medida Provisória n.º 2.200-2/2001, vinculada, na forma do Decreto n.º 4.566, de 1º de janeiro de 2003, à Casa Civil da Presidência da República, tem como finalidade ser a Autoridade Certificadora Raiz-AC Raiz, da Infraestrutura de Chaves Públicas Brasileira-ICP-Brasil, possuindo as seguintes competências, conforme descreve o Decreto n.º 4.689, de 7 de maio de 2003:

> I - executar as políticas de certificação e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

II - propor a revisão e a atualização das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

III - gerenciar os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu, incluindo emissão, expedição, distribuição e revogação desses documentos;

IV - gerenciar a lista de certificados emitidos, revogados e vencidos;

V - executar as atividades de fiscalização e de auditoria das Autoridades Certificadoras - AC, Autoridades de Registro - AR e dos prestadores de serviços habilitados na ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;

VI - aplicar sanções e penalidades, na forma da lei;

VII - emitir certificado para o funcionamento das AC, das AR e dos prestadores de serviço de suporte da ICP-Brasil;

VIII - promover o relacionamento com instituições congêneres no País e no exterior;

IX - celebrar e acompanhar a execução de convênios e acordos internacionais de cooperação, no campo das atividades de infraestrutura de chaves públicas e áreas afins, ouvido o Comitê Gestor da ICP-Brasil;

X - estimular a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infraestrutura de chaves públicas;

XI - estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, autenticidade e integridade de informações eletrônicas; e

XI - executar outras atribuições que lhe forem cometidas pelo Comitê Gestor da ICP-Brasil.

Por sua vez, o Decreto n.º 6.605, de 14 de outubro de 2014, regulamenta o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória no 2.200-2, de 24 de agosto de 2001, para exercer a função de autoridade gestora de políticas da ICP-Brasil, ao qual compete:

I - coordenar o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das Autoridades Certificadoras - AC, Autoridades

de Registro - AR, Autoridades de Carimbo de Tempo - ACT e demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - auditar e fiscalizar a AC Raiz e os seus prestadores de serviço de suporte;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificado e regras operacionais das AC, AR e ACT e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, credenciar e autorizar o funcionamento das AC, das AR, das ACT e demais prestadores de serviço de suporte, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de infraestruturas de certificação externas, negociar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais;

VIII - aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil; e

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.

O Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, vinculado à Casa Civil da Presidência da República, é composto por doze membros e respectivos suplentes, sendo cinco representantes da sociedade civil, integrantes de setores interessados, e representantes dos seguintes órgãos: I - Casa Civil da Presidência da República, que o coordenará; II - Gabinete de Segurança Institucional da Presidência da República; III - Ministério da Justiça; IV - Ministério da Fazenda; V - Ministério do Desenvolvimento, Indústria e Comércio Exterior; VI - Ministério do Planejamento, Orçamento e Gestão; e VII - Ministério da Ciência e Tecnologia.

4.6. Lei n.º 12.527 de 18 de novembro de 2011. Lei de Acesso à Informação - LAI.

A Lei de Acesso à Informação dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal, que garante 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, determinando que é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão (art.5º da Lei n.º 12.527/2011), definindo informação como: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (art. 4º, inciso I da Lei n.º 12.527/2011).

Subordinam-se ao regime da Lei de Acesso a Informação os órgãos públicos integrantes da administração direta e indireta dos Poderes Executivo, Legislativo e Judiciário, incluindo as Cortes de Contas, e o Ministério Público, assim como, as demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios, e às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres, cabendo a estes assegurar a:

> I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
>
> II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
>
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Para tanto, define como informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e como informação pessoal: aquela relacionada à pessoa natural identificada ou identificável.

A Lei de Acesso a Informação estabelece que o acesso à informação pública é a regra, e o sigilo, a exceção, razão pela qual a divulgação de informações de interesse público deve ocorrer independentemente de solicitações, por meios de comunicação viabilizados pela tecnologia da informação, visando assim o fomento ao desenvolvimento da cultura de transparência na administração pública e desenvolvimento do controle social da administração pública. O direito ao acesso a informação compreende, entre outros, os direitos de obter:

> I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;
>
> II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;
>
> III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;
>
> IV - informação primária, íntegra, autêntica e atualizada;
>
> V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;
>
> VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e
>
> VII - informação relativa:
>
> a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;
>
> b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

Para garantir o acesso a informação a LAI estipula procedimento, normas e prazos, prevendo a criação, em todos órgãos e entidades do poder público, de um serviço de informações ao cidadão, que caberá: a) atender e orientar o público quanto ao acesso a informações; b) informar sobre a tramitação de documentos nas suas respectivas unidades; e c) protocolizar documentos e requerimentos de acesso a informações.

Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida, cabendo ao órgão ou entidade pública autorizar ou conceder o acesso imediato à informação disponível, ou em até 20 (vinte) dias, prorrogáveis por mais 10 (dez) dias, nos termos dos artigos 10 e 11 da Lei 12.527/2011[28].

O serviço de busca e fornecimento das informações é gratuito, salvo as cópias de documentos, conforme descreve o art. 12, podendo o solicitante ser isento de ressarcir os custos, caso sua situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da Lei n.º 7.115, de 29 de agosto de 1983.

Importante frisar que as informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso, nos termos do art. 21.

Nos casos em que a informação estiver sob algum tipo de sigilo previsto em Lei, é direito do solicitante obter o inteiro teor de decisão de negativa de acesso, por certidão ou cópia. Cabe ressaltar que quando a informação for parcialmente sigilosa, fica assegurado o acesso, por meio de certidão, extrato ou cópia, com a ocultação da parte sob sigilo.

---

[28] Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

Art. 11. O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível.

§1º Não sendo possível conceder o acesso imediato, na forma disposta no caput, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias: I - comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão; II - indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou III - comunicar que não possui a informação, indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

§2º O prazo referido no § 1º poderá ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente.

§3º Sem prejuízo da segurança e da proteção das informações e do cumprimento da legislação aplicável, o órgão ou entidade poderá oferecer meios para que o próprio requerente possa pesquisar a informação de que necessitar.

§4º Quando não for autorizado o acesso por se tratar de informação total ou parcialmente sigilosa, o requerente deverá ser informado sobre a possibilidade de recurso, prazos e condições para sua interposição, devendo, ainda, ser-lhe indicada a autoridade competente para sua apreciação.

§5º A informação armazenada em formato digital será fornecida nesse formato, caso haja anuência do requerente.

§6ºCaso a informação solicitada esteja disponível ao público em formato impresso, eletrônico ou em qualquer outro meio de acesso universal, serão informados ao requerente, por escrito, o lugar e a forma pela qual se poderá consultar, obter ou reproduzir a referida informação, procedimento esse que desonerará o órgão ou entidade pública da obrigação de seu fornecimento direto, salvo se o requerente declarar não dispor de meios para realizar por si mesmo tais procedimentos.

Havendo negativa de acesso a informações, ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da sua ciência, dirigido à autoridade hierarquicamente superior à que exarou a decisão impugnada, que deverá se manifestar no prazo de 5 (cinco) dias. Persistindo a negativa, o solicitante poderá recorrer ao Ministro de Estado da área, ou em caso de descumprimento de procedimentos e prazos, à Controladoria Geral da União, conforme descrevem os artigos 15 e 16 da LAI[29].

Prevê o art. 17, que em última instancia caberá recurso à Comissão Mista de Reavaliação de Informações, que decidirá, no âmbito da administração pública federal, sobre o tratamento e a classificação de informações sigilosas e terá competência para: I - requisitar da autoridade que classificar informação como ultrassecreta e secreta esclarecimento ou conteúdo, parcial ou integral da informação; II - rever a classificação de informações ultrassecretas ou secretas, de ofício ou mediante provocação de pessoa interessada, observado o disposto no art. 7º e demais dispositivos desta Lei; e III - prorrogar o prazo de sigilo de informação classificada como ultrassecreta, sempre por prazo determinado, enquanto o seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional ou à integridade do território nacional ou grave risco às relações internacionais do País.

[29] Art. 15. No caso de indeferimento de acesso a informações ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da sua ciência.
Parágrafo único. O recurso será dirigido à autoridade hierarquicamente superior à que exarou a decisão impugnada, que deverá se manifestar no prazo de 5 (cinco) dias.
Art. 16. Negado o acesso a informação pelos órgãos ou entidades do Poder Executivo Federal, o requerente poderá recorrer à Controladoria-Geral da União, que deliberará no prazo de 5 (cinco) dias se:
I - o acesso à informação não classificada como sigilosa for negado;
II - a decisão de negativa de acesso à informação total ou parcialmente classificada como sigilosa não indicar a autoridade classificadora ou a hierarquicamente superior a quem possa ser dirigido pedido de acesso ou desclassificação;
III - os procedimentos de classificação de informação sigilosa estabelecidos nesta Lei não tiverem sido observados; e
IV - estiverem sendo descumpridos prazos ou outros procedimentos previstos nesta Lei.
§1º O recurso previsto neste artigo somente poderá ser dirigido à Controladoria-Geral da União depois de submetido à apreciação de pelo menos uma autoridade hierarquicamente superior àquela que exarou a decisão impugnada, que deliberará no prazo de 5 (cinco) dias.
§2º Verificada a procedência das razões do recurso, a Controladoria-Geral da União determinará ao órgão ou entidade que adote as providências necessárias para dar cumprimento ao disposto nesta Lei.
§3º Negado o acesso à informação pela Controladoria-Geral da União, poderá ser interposto recurso à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35.

Cabe aqui ressaltar que a Lei n.º 12.527/2011 traz exceções à regra de acesso as informações, quais sejam, os dados pessoais e informações classificadas por autoridades como sigilosa. As informações pessoais relativas à intimidade, vida privada, honra e imagem, terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem e poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem, conforme regula o art. 31.

O consentimento da pessoa não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante.

O § 4º do art. 31 determina que a restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

No que tange a classificação da informação, os artigos 23 ao 30 da LAI dissertam que como princípio geral uma informação só pode ser classificada como sigilosa quando considerada imprescindível à segurança da sociedade ou do Estado, trazendo para tanto três classificações, quais seja: a) Ultrassecreta, cujo prazo de segredo é de 25 anos, renovável uma única vez; b) Secreta, cujo prazo de segredo é de 15 anos; e c) Reservada, cujo prazo de segredo é de 5 anos. A classificação do sigilo de informações no âmbito da administração pública federal é de competência:

> I - no grau de ultrassecreto, das seguintes autoridades:
>
> a) Presidente da República;
>
> b) Vice-Presidente da República;
>
> c) Ministros de Estado e autoridades com as mesmas prerrogativas;

> d) Comandantes da Marinha, do Exército e da Aeronáutica; e
>
> e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
>
> II - no grau de secreto, das autoridades referidas no inciso I, dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista; e
>
> III - no grau de reservado, das autoridades referidas nos incisos I e II e das que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade, observado o disposto nesta Lei.

No âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo é regulamentado pelo Decreto n.º 7.724, de 16 de maio de 2012.

Por sua vez, o Decreto n.º 7.845, de 14 de novembro de 2012, regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, determinando que compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, nos termos do art. 37 da Lei n.º 12.527, de 2011:

> I - habilitar os órgãos de registro nível 1[30] para o credenciamento de segurança[31] de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada[32];
>
> II - habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de informação classificada em qualquer grau de sigilo;
>
> III - habilitar entidade privada que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da

[30] Nos termos do inciso XIII, do art. 1º do Decreto n.º 7.845/2012, considera-se órgão de registro nível 1 - ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;

[31] Nos termos do inciso VII, do art. 1º do Decreto n.º 7.845/2012, considera-se credenciamento de segurança - processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada;

[32] Nos termos do inciso XVIII, do art. 1º do Decreto n.º 7.845/2012, considera-se tratamento da informação classificada - conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Presidência da República para o tratamento de informação classificada;

IV - credenciar pessoa que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada;

V - realizar inspeção e investigação para credenciamento de segurança necessárias à execução do previsto, respectivamente, nos incisos III e IV do caput; e

VI - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada.

O supracitado Decreto criou o Comitê Gestor de Credenciamento de Segurança, integrado por representantes, titular e suplente, dos seguintes órgãos: - Gabinete de Segurança Institucional da Presidência da República, que o coordenará; II - Casa Civil da Presidência da República; III - Ministério da Justiça; IV - Ministério das Relações Exteriores; V - Ministério da Defesa; VI - Ministério da Ciência, Tecnologia e Inovação; VII - Ministério do Planejamento, Orçamento e Gestão; e VIII - Controladoria-Geral da União.

Compete ao Comitê Gestor de Credenciamento de Segurança propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada; definir parâmetros e requisitos mínimos para qualificação técnica de órgãos e entidades públicas e privadas e para credenciamento de segurança e concessão de credencial de segurança para pessoas, nos termos do art. 12[33].

O Decreto n.º 7.845, de 14 de novembro de 2012, traz ainda os procedimentos para habilitação dos órgãos e entidades públicas para o credenciamento de segurança, nos artigos 10 a 16, e sobre da forma de tratamento de informação classificada pelos órgãos e entidades, nos artigos 17 a 49. E por fim, nos artigos 50 a 53, versa sobre a indexação de documento com informação classificada.

[33] Art. 12. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:
I - solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;
II - preenchimento de formulário com dados pessoais e autorização para investigação;
III - aptidão para o tratamento da informação classificada, verificada na investigação; e
IV - declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.

4.7. Decreto n.º 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.

O art. 24, inciso IX da Lei nº 8.666, de 21 de junho de 1993 determina que é dispensável a licitação quando houver possibilidade de comprometimento da segurança nacional, nos casos estabelecidos em decreto do Presidente da República, ouvido o Conselho de Defesa Nacional.

O Decreto n.º 2.295, 04 de agosto de 1997, que regulamenta o supracitado dispositivo, relata que 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; IV - outros casos que possam comprometer a segurança nacional serão submetidos à apreciação do Conselho de Defesa Nacional, para o fim de dispensa de licitação.

Contudo, cabe ressaltar que 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.

4.8. Decreto de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.

O Comitê Executivo do Governo Eletrônico, criado pelo Decreto de 18 de outubro de 2000, tem como 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 integrado pelo:

> I - o Chefe da Casa Civil da Presidência da República, que o presidirá;
>
> II - os Secretários-Executivos dos Ministérios;

III - o Secretário-Geral do Ministério das Relações Exteriores;

IV - o Subchefe do Gabinete de Segurança Institucional da Presidência da República;

V - o Secretário de Organização Institucional do Ministério da Defesa;

VI - o Subsecretário-Geral da Secretaria-Geral da Presidência da República;

VII - o Secretário de Avaliação, Promoção e Normas da Secretaria de Comunicação de Governo da Presidência da República;

VIII – o Procurador-Geral da União;

IX - o Subcorregedor-Geral da Corregedoria-Geral da União; e

X - o Diretor-Presidente do Instituto Nacional de Tecnologia da Informação.

Compete ao Comitê Executivo do Governo Eletrônico:

I - coordenar e articular a implantação de programas e projetos para a racionalização da aquisição e da utilização da infraestrutura, 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.

Atualmente o Governo Eletrônico brasileiro conta oito Comitês Técnicos responsáveis pelo desenvolvimento das políticas e ações definidas nos princípios e diretrizes estabelecidas para toda a Administração Pública Federal. Os Comitês Técnicos instituídos, no âmbito do Comitê Executivo do Governo Eletrônico, por meio do Decreto de 29 de outubro de 2003, têm a finalidade de coordenar e articular o planejamento e a implementação de projetos e ações nas respectivas áreas de competência, com as seguintes denominações: a) Implementação do *Software* Livre; b) Inclusão Digital; c) Integração de Sistemas; d) Sistemas Legados e Licenças de *Software*; e) Gestão de Sítios e Serviços *On-line*; f) Infraestrutura de Rede; g) Governo para Governo (G2g); e h) Gestão de Conhecimentos e Informação Estratégica.

O Decreto de 29 de outubro de 2003 determina ainda que os Comitês Técnicos serão compostos por representantes de órgãos e entidades da administração pública federal, indicados pelos integrantes do Comitê Executivo do Governo Eletrônico.

4.9. Decreto n.º 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O Decreto n.º 3.996, de 31 de outubro de 2001, regulamenta a prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, determinando que 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, que deverão ser providos no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Faculta ao Comitê Executivo do Governo Eletrônico, criado pelo Decreto de 18 de outubro de 2000, 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, desde que, respeitado o padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Por fim, determina que 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, e que 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, conforme reza o art. 3º-A, incluído pelo Decreto n.º 4.414, de 7 de outubro de 2002.

4.10. Decreto n.º 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

O Sistema de Geração e Tramitação de Documentos Oficiais – SIDOF foi criado pelo Decreto n.º 4.522, de 17 de dezembro de 2002, com intuito de organizar 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.

O SIDOF tem a seguinte estrutura: I - órgão central - Casa Civil da Presidência da República, responsável pela formulação de diretrizes, orientação, planejamento, coordenação, supervisão e controle dos assuntos a ele relativos; II - órgãos setoriais - unidades incumbidas especificamente de atividades concernentes ao Sistema nos Ministérios e órgãos integrantes da Presidência da República; III - órgãos seccionais - unidades incumbidas da execução das atividades do SIDOF, nas autarquias e fundações públicas. O art. 3º, determina que participam do SIDOF:

> I - o Presidente da República;
>
> II - os Ministros de Estado e os dirigentes máximos de órgãos integrantes da estrutura da Presidência da República, responsáveis pela proposição de documentos oficiais ao Presidente da República;
>
> III - os titulares dos órgãos de assistência jurídica dos ministérios e da Presidência da República;
>
> IV - o Administrador-Geral do SIDOF, designado pelo Subchefe para Assuntos Jurídicos da Casa Civil da Presidência da República, responsável pela formulação de diretrizes, orientação, planejamento, coordenação, supervisão e controle dos assuntos relativos ao Sistema;
>
> V - o Administrador de Usuários e os responsáveis ou prepostos setoriais e seccionais incumbidos das atividades concernentes ao SIDOF, nos Ministérios e órgãos supervisionados, ou integrantes da Presidência da República;
>
> VI - o órgão responsável pela infraestrutura de tecnologia da informação, a cargo da Diretoria de Tecnologia da Informação da

Secretaria de Administração da Casa Civil da Presidência da República, incumbido da implementação e atualização do SIDOF, abrangendo software básico e aplicações, bem como pela permanente coordenação das aplicações da tecnologia utilizada;

VII - a Coordenação-Geral de Certificação da Secretaria de Administração da Casa Civil como Autoridade Certificadora da Presidência da República; e

VIII - o órgão responsável pela infraestrutura de equipamentos, manutenção e suporte técnico aos usuários do SIDOF, nos órgãos setoriais e seccionais a cargo das respectivas Coordenações de Modernização e Informática, ou equivalentes.

5. INSTRUÇÕES NORMATIVAS SOBRE SEGURANÇA DA INFORMAÇÃO APLICÁVEIS À SEGURANÇA DA INFORMAÇÃO NO ÂMBITO FEDERAL

5.1. Instrução Normativa nº 1 do GSI, de 13 de junho de 2008. - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

A Instrução Normativa n.º 1 do Gabinete de Segurança Institucional da Presidência da República aprova as orientações para Gestão de Segurança da Informação e Comunicações que devem ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Vejamos em sua íntegra.

> Art. 1º Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.
>
> Art. 2º Para fins desta Instrução Normativa, entende-se por:
>
> I - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
>
> II - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
>
> III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
>
> IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
>
> V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
>
> VI - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
>
> VII - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de

incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

Art. 4º Ao Comitê Gestor de Segurança da Informação compete:

I - assessorar o GSI no aperfeiçoamento da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

II - instituir grupos de trabalho para tratar de temas específicos relacionados à segurança da informação e comunicações.

Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações; II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI

Parágrafo único. Para fins do disposto no caput, deverá ser observado o disposto no inciso II do art. 3º desta Instrução Normativa.

Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções

específicas sobre segurança da informação e comunicações;

III – propor alterações na Política de Segurança da Informação e Comunicações; e

IV - propor normas relativas à segurança da informação e comunicações.

Art. 7º Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;
VII - propor normas relativas à segurança da informação e comunicações.

Art. 8º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Art. 9º Esta Instrução Normativa entra em vigor sessenta dias após sua publicação.

Segue abaixo quadro de Normas Complementares à IN n.º 01 GSI/PR/2008 - Segurança da Informação e Comunicações[34]:

Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização. (Publicada no DOU Nº 200, de 15 Out 2008 - Seção 1).
Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1)
Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 Jul. 2009 - Seção 1)
Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 37, de 25 Fev. 2013 - Seção 1)
Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago. 2009 - Seção 1)
Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 223, de 23 Nov. 2009 - Seção 1)
Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1)
Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago. 2010 - Seção 1)
Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da

[34] Disponível no sitio do Gabinete de Segurança Institucional da Presidência da República, ligado ao Departamento de Segurança da Informação e Comunicações em https://dsic.planalto.gov.br/documentos/quadro_legislacao.htm. Acesso em 12 de dezembro de 2014.

Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1)
Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1)
Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1)
Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1)
Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). (Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1)
Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev. 2012 - Seção 1)
Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 Jun. 2012 - Seção 1)
Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de *Software* Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 224, de 21 Nov. 2012 - Seção 1)
Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abr. 2013 - Seção 1)
Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abril 2013 - Seção 1)
Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul. 2014 - Seção 1)
Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1)
Norma Complementar nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1)

5.2. Instrução Normativa nº 2 do GSI, de 05 de fevereiro de 2013. - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

A Instrução Normativa n.º 2 do Gabinete de Segurança Institucional da Presidência da República normatiza os procedimentos do Núcleo de Segurança e Credenciamento – NSC do GSI/PR e expede diretrizes a serem adotadas pelos órgãos e entidades no âmbito do

Poder Executivo Federal, para o Credenciamento de Segurança e o tratamento de informação classificada, em conformidade com os Artigos 36 e 37 da Lei de Acesso a Informação (Lei n.º 12.527, de 2011), cuja integra encontra-se anexa ao presente documento.

Abaixo segue quadro de Normas Complementares à IN n.º 02 GSI/PR/2013 - Credenciamento de Segurança[35]:

Norma Complementar nº 01/IN02/NSC/GSIPR, e seus anexos (Anexo A e Anexo B) Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas. (Publicada no DOU Nº 123, de 28 de junho de 2013 - Seção 1)

5.3. Instrução Normativa nº 3 do GSI, de 06 de março de 2013. - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

A Instrução Normativa n.º 03 do Gabinete de Segurança Institucional da Presidência da República estabelece no âmbito do Poder Executivo Federal, os parâmetros e padrões mínimos para recursos criptográficos baseados em algoritmos de Estado, que deverão ser implementados, pelos órgãos e entidades, na criptografia da informação classificada, em qualquer grau de sigilo, cujo teor encontra-se reproduzido abaixo.

> Art. 3º A Alta Administração dos órgãos e entidades do Poder Executivo Federal, sob pena de responsabilidade, deverá, no âmbito de sua competência, assegurar a implementação e utilização dos parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado, para criptografia da informação classificada, em qualquer grau de sigilo.
>
> Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem seguir o disposto nesta Instrução Normativa e na legislação vigente, sob pena de responsabilidade.

[35] Disponível no sitio do Gabinete de Segurança Institucional da Presidência da República, ligado ao Departamento de Segurança da Informação e Comunicações em https://dsic.planalto.gov.br/documentos/quadro_legislacao.htm. Acesso em 12 de dezembro de 2014.

Art. 4º A cifração e decifração de informações classificadas, em qualquer grau de sigilo, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013, reproduzidos no Anexo desta Instrução Normativa.

Art. 5º O recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade.

§1º Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, previsto no caput poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:

I - seja realizado exclusivamente por meio de Contrato Sigiloso, nos termos dos arts. 48 e 49 do Decreto n.º 7.845, de 14 de novembro de 2012;

II - seja previsto em cláusula contratual que fica vedado ao contratado os direitos de propriedade e de exploração comercial, do recurso criptográfico com algoritmo de estado, objeto do presente contrato;

§2º O não cumprimento do previsto no caput ou nos incisos I e II do § 1º, poderá gerar responsabilidade administrativa, civil e penal, conforme legislação vigente.

Art. 6º À Alta Administração dos órgãos e entidades do Poder Executivo Federal compete:

I - solicitar, quando se fizer necessário, apoio técnico ao GSI/PR, referente ao uso de recurso criptográfico baseado em algoritmo de Estado, para o cumprimento da legislação pertinente;

II - realizar auto avaliação de conformidade relativa ao uso dos recursos criptográficos baseados em algoritmo de Estado, e encaminhar relatório anual ao GSI/PR, conforme previsto no item 5.6.2 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013;

III - adequar os recursos criptográficos, já em uso, às determinações desta Instrução Normativa, e conforme legislação vigente;

IV - prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente Instrução Normativa, sem prejuízo da legislação vigente;V - garantir o previsto no art. 41 do Decreto n.º 7.845, de 14 de novembro de 2012, e encaminhar relatório anual

ao GSI/PR, conforme previsto no item 5.6.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013;

VI - informar ao GSI/PR, tempestivamente, o comprometimento do sigilo de qualquer recurso criptográfico baseado em algoritmo de Estado;

VII - capacitar os Agentes Responsáveis para o uso dos recursos criptográficos, observando as normas vigentes, os procedimentos de credenciamento de segurança, e o tratamento de informação classificada; e

VIII - prever recurso orçamentário para o uso de recursos criptográficos baseados em algoritmos de Estado, conforme necessidade de cada órgão ou entidade.

Art. 7º O GSI/PR acompanhará periodicamente o cumprimento do estabelecido nesta IN pelos órgãos e entidades do Poder Executivo Federal, por meio do disposto no item 5.6 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013, e de visitas técnicas quando se fizer necessário.

Art. 8º O GSI/PR prestará apoio técnico, previsto no art. 56 do Decreto nº 7.845, de 14 de novembro de 2012, devendo os órgãos e entidades do Poder Executivo Federal formalizarem a demanda junto ao GSI/PR no prazo de até cento e oitenta dias, conforme previsto no item 5.9.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de

2013.

Parágrafo único. Vencido o prazo do caput, as necessidades recebidas não serão mais tratadas como demanda específica para o cumprimento do prazo referido no Decreto, e sim, como demanda de caráter ordinário.

Art. 9º Todo recurso criptográfico baseado em algoritmo de Estado constitui material de acesso restrito e requer procedimentos especiais adequados de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente, sob pena de responsabilização da Alta Administração.

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem possuir credencial de segurança, ou excepcionalmente, assinar o Termode Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto n o 7.845, de 14 de novembro de 2012.

Art. 10 Esta Instrução Normativa entra em vigor na data de sua publicação

5.4. Quadro de Normas Técnicas relacionadas à segurança da informação[36]:

Regulamento	Assunto
ISO/IEC TR 13335-3:1998	Esta norma 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.
ISO/IEC GUIDE 51:1999	Esta norma 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 GUIDE 73:2002.	Esta norma 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.
ABNT NBR ISO IEC 17799: 2005.	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 27001:2005.	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 27005:2011.	Esta Norma fornece diretrizes para o processo de gestão de riscos de segurança da informação
ABNT NBR ISO/IEC 27001:2013.	Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
ABNT NBR ISO/IEC 27002:2013.	Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização

[36] Disponível no sitio do Gabinete de Segurança Institucional da Presidência da República, ligado ao Departamento de Segurança da Informação e Comunicações em https://dsic.planalto.gov.br/documentos/quadro_legislacao.htm. Acesso em 12 de dezembro de 2014.

6. CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da SE e da Universidade de Brasília, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas.

Esse trabalho conclui o levantamento da legislação sobre segurança da informação o que permitirá uma maior segurança quanto às regras a serem observadas no gerenciamento dos dados que serão armazenados no Cadastro Nacional do Registro de Identificação Civil – CANRIC com a instituição do número único de Registro de Identidade Civil – RIC.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe do MJ, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

7. BIBLIOGRAFIA

SILVA, José Afonso da. Curso de Direito Constitucional positivo. 33ª ed. Atual. São Paulo. Malheiros, 2010, p. 525.

PRADO, Luiz Régis. Curso de Direito Penal Brasileiro v.1. São Paulo: RT, 2008. p.55.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. P. 17.

Sítio do Instituto Nacional de Tecnologia da Informação. Disponível em: http://www.iti.gov.br/. Acesso em Dez/14 e Jan/15.

Sítio do Gabinete de Segurança Institucional da Presidência da República, ligado ao Departamento de Segurança da Informação e Comunicações. Disponível em: https://dsic.planalto.gov.br/. Acesso em Dez/14 e Jan/15.

Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em Out/14, Nov/14, Dez/14 e Jan/15.

Código Penal Brasileiro. Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em Out/14.

Código Tributário Nacional. Lei n.º 5.172 de 25 de outubro de 1966. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em Out/14.

Consolidação das Leis do Trabalho. Decreto-Lei n.º 5.452, de 1º de maio de 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em Out/14.

Código de Defesa do Consumidor. Lei n.º 8.078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em Dez/14 e Jan/15.

Código de Conduta da Alta Administração Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/codigos/codi_conduta/cod_conduta.htm. Acesso em Nov./14.

Código de Ética do Profissional do Servidor Público do Poder Executivo Federal. Decreto n.º 1.171, de 22 de junho de 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d1171.htm. Acesso em Nov./14.

Lei n.º 6.538, de 22 de junho de 1978. Dispõe sobre os serviços postais. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6538.htm. Acesso em Nov./14.

Lei n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7170.htm. Acesso em Dez/14.

Lei n.º 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7232.htm. Acesso em Dez/14.

Lei n.º 7.492, de 16 de junho de 1986. Define os crimes contra o sistema financeiro nacional, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/l7492.htm. Acesso em Dez/14.

Lei n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8027.htm. Acesso em Dez/14.

Lei n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Acesso em Dez/14.

Lei n.º 8.429, de 2 de junho de 1992. Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8429.htm. Acesso em Dez/14.

Lei n.º 8.443, de 16 de julho de 1992. Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8443.htm. Acesso em Dez/14.

Lei n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em Dez/14.

A Lei Complementar n.º 75, de 20 de maio de 1993. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75.htm. Acesso em Dez/14.

Lei n.º 8.625, de 12 de fevereiro de 1993. Institui a Lei Orgânica Nacional do Ministério Público, dispõe sobre normas gerais para a organização do Ministério Público dos Estados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8625.htm. Acesso em Dez/14.

Lei n.º 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em Dez/14.

Lei n.º 9.100, de 29 de setembro de 1995. Estabelece normas para a realização das eleições municipais de 3 de outubro de 1996, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9100.htm. Acesso em Dez/14.

A Lei n.º 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em Dez/14.

Lei n.º 9.472, de 16 de julho 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. Disponível em: https://www.planalto.gov.br/Ccivil_03/LEIS/L9472.htm. Acesso em Dez/14.

Lei n.º 10.703, de 18 de julho de 2003. Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.703.htm. Acesso em Dez/14.

Lei n.º 10.683, de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.683.htm. Acesso em Dez/14.

Decreto n.º 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em Dez/14.
Decreto n.º 4.801, de 6 de agosto de 2003. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4801.htm. Acesso em Dez/14.

Decreto n.º 5.687, de 31 de janeiro de 2006. Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm. Acesso Dez/14.

Decreto n.º 8.100, de 4 de setembro de 2013. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República; remaneja cargos em comissão e altera o Anexo II ao Decreto nº 6.408, de 24 de março de 2008, que 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, do Gabinete de Segurança Institucional da Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8100.htm. Acesso Dez/14.

Lei n.º 8.159/91, de 08 de janeiro de 1991. Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em Jan/15.

Lei n.º 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em Jan/15.

Lei n.º 9.883, de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm. Acesso em Jan/15.

Decreto n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm. Acesso em Jan/15.

Lei n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm. Acesso em Jan/15.

Lei Complementar n.º 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em Jan/15.

Medida Provisória n.º 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm. Acesso em Jan/15.

Lei n.º 12.527 de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em Jan/15.

Decreto n.º 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. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2295.htm. Acesso em Dez/14.

Decreto de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/dnn/Dnn9067.htm. Acesso em Dez/14.

Decreto n.º 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm. Acesso em Dez/14.

Decreto n.º 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4522.htm. Acesso em Dez/14.

Instrução Normativa nº 1 do GSI, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: https://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas. Acesso em Jan/15.

Instrução Normativa nº 2 do GSI, de 05 de fevereiro de 2013. - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. Disponível em: https://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas. Acesso em Jan/15.

Instrução Normativa nº 3 do GSI, de 06 de março de 2013. - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. Disponível em: https://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas. Acesso em Jan/15.

8. Anexo: Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br

Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013.

Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA – GSI/PR, na condição de SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL, no uso de suas atribuições;

CONSIDERANDO:

- o disposto nos arts. 36 e 37 da Lei nº 12.527, de 18 de novembro de 2011;
- o Decreto nº 3.505, de 13 de junho de 2000;
- o Decreto nº 7.724, de 16 de maio de 2012;
- o Decreto nº 7.845, de 14 de novembro de 2012;
- a necessidade de garantir a segurança da sociedade e do Estado por meio do credenciamento de segurança para acesso a informações classificadas;
- a necessidade de garantir a segurança da informação classificada, observada a sua disponibilidade, autenticidade, integridade e restrição de acesso;
- a necessidade de estabelecer e orientar a condução das diretrizes de salvaguarda das informações classificadas já existentes ou a serem implementadas pelos órgãos e entidades do Poder Executivo Federal;

RESOLVE:

Art. 1º Normatizar os procedimentos do Núcleo de Segurança e Credenciamento - NSC do GSI/PR e expedir diretrizes a serem adotadas pelos órgãos e entidades no âmbito do Poder Executivo Federal, para o Credenciamento de Segurança e o tratamento de informação classificada, em conformidade com os Artigos 36 e 37 da Lei nº 12.527, de 2011, Decreto 7.724, de 2012 e Decreto 7.845, de 2012.

Art. 2º Para fins desta Instrução Normativa entende-se por:

I - **Atos Internacionais**: acordo internacional concluído por escrito entre Estados e regido pelo Direito Internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação específica, conforme o art. 2º, da Convenção de Viena do Direito dos Tratados, de 23 de maio de 1969, promulgada pelo Decreto nº 7.030, de 14 de dezembro de 2009;

II - **Controle de acesso à informação classificada**: realizado através de credencial de segurança e demonstração da necessidade de conhecer;

III - **Credencial de Segurança**: certificado que autoriza pessoa para o tratamento de informação classificada;

IV - **Credenciamento de segurança**: processo utilizado para habilitar órgão ou entidade pública ou privada ou para credenciar pessoa, para o tratamento de informação classificada;

V - **Documentos Classificados**: documento que contenha informação classificada em qualquer grau de sigilo;

VI - **Documentos Controlados – DC**: documento que contenha informação classificada em qualquer grau de sigilo e que, a critério da autoridade classificadora, requer medidas adicionais de controle;

VII - **Gestor de segurança e credenciamento**: responsável pela segurança da informação classificada em qualquer grau de sigilo nos Órgãos de Registro e Postos de Controle.

VIII - **Informação Classificada**: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada;

IX - **Informação Sigilosa**: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

X - **Inspeção para credenciamento de segurança**: averiguação da existência dos requisitos indispensáveis à habilitação de órgãos e entidades para o tratamento de informação classificada;

XI - **Investigação para credenciamento de segurança**: averiguação da existência dos requisitos indispensáveis para a concessão da credencial de segurança à pessoas naturais, para o tratamento de informação classificada;

XII - **Necessidade de conhecer**: condição segundo a qual o conhecimento da informação classificada é indispensavel para o adequado exercício de cargo, função, emprego ou atividade;

XIII - **Órgãos de Registro nível 1**: os Ministérios e os órgãos e entidades públicos de nível equivalente, credenciados pelo Núcleo de Segurança e Credenciamento;

XIV - **Órgãos de Registro nível 2**: os órgãos e entidades públicos vinculados ao Órgão de Registro nível 1 e credenciados pelos mesmos;

XV - **Postos de Controle**: unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo; e

XVI - **Quebra de segurança**: a ação ou omissão, intencional ou acidental, que resulte no comprometimento ou no risco de comprometimento de informação classificada.

Art. 3º Compete ao Núcleo de Segurança e Credenciamento - NSC, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República:

I - habilitar os Órgãos de Registro nível 1 para o Credenciamento de Segurança de órgãos e entidades públicas ou privadas, e de pessoas que com ele mantenham vínculo de qualquer natureza, para o tratamento de informação classificada;

II - habilitar Postos de Controle dos Órgãos de Registro nível 1 para o armazenamento de informação classificada em qualquer grau de sigilo;

III - habilitar entidade privada que mantenha vínculo de qualquer natureza com o GSI/PR para o tratamento de informação classificada;

IV - credenciar pessoa que mantenha vínculo de qualquer natureza com o GSI/PR para o tratamento de informação classificada;

V - realizar inspeção e investigação para Credenciamento de Segurança necessária à execução do previsto nos incisos III e IV, respectivamente;

VI - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada;

VII - assessorar o Ministro-Chefe do GSI/PR nas negociações de tratados, acordos ou atos internacionais relacionados com a troca de informações classificadas;

VIII - assessorar o Ministro-Chefe do GSI/PR nos assuntos relacionados com o credenciamento de segurança de órgãos e entidades públicas ou privadas e pessoas, para o tratamento de informação classificada;

IX - assessorar o Ministro-Chefe do GSI/PR nas funções de autoridade nacional de segurança para tratamento de informação classificada decorrente de tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores.

X - acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança e informar sobre eventuais danos ao país ou à organização internacional de origem, sempre que necessário, pela via diplomática;

XI - prover apoio técnico aos Órgãos de Registro e Posto de Controle, no âmbito do Poder Executivo federal, para a implantação dos mesmos e pleno desenvolvimento das atividades de Credenciamento de Segurança; e,

XII - promover e propor regulamentação de credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações sigilosas.

Art. 4º Compete ao Órgão de Registro nível 1:

I - habilitar Órgão de Registro nível 2 para credenciar pessoa para o tratamento de informação classificada;

II - habilitar Posto de Controle dos órgãos e entidades públicas ou privadas que com ele mantenham vínculo de qualquer natureza, para o armazenamento de informação classificada em qualquer grau de sigilo;

III - credenciar pessoa natural que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada;

IV- realizar a inspeção e investigação para credenciamento de segurança necessárias à execução do previsto no inciso III do caput; e

V - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada, no âmbito de suas competências;

VI - encaminhar periodicamente ao Núcleo de Segurança e Credenciamento, relatórios sobre suas atividades de credenciamento e seu funcionamento, bem como daqueles por ele credenciados;

VII- notificar o Núcleo de Segurança e Credenciamento, imediatamente, quando da quebra de segurança das informações classificadas do próprio e daqueles Órgãos de Registro nível 2 e Postos de Controle por ele credenciados, inclusive as relativas a tratados, acordos ou qualquer outro ato internacional.

Art. 5º Compete ao Órgão de Registro nível 2:

I - realizar investigações para credenciamento e conceder as credenciais segurança apenas às pessoas naturais a eles vinculadas;

II - encaminhar periodicamente relatórios de atividades ao Órgão de Registro nível 1 que o credenciou;

III - notificar o Órgão de Registro que o credenciou, imediatamente, quando da quebra de segurança das informações classificadas;

Art. 6 º Compete ao Posto de Controle:

I - armazenar e controlar as informações classificadas, inclusive as credenciais de segurança, sob sua responsabilidade;

II - manter a segurança lógica e física das informações classificadas, sob sua guarda;

IV - encaminhar, periodicamente, ao Órgão de Registro que o credenciou relatórios de suas atividades;

V - notificar o Órgão de Registro que o credenciou, imediatamente, quando da quebra de segurança das informações classificadas por ele custodiadas;

Art. 7º O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos a pessoas que tenham necessidade de conhecê-la e que tenham Credencial de Segurança segundo as normas fixadas pelo GSI/PR, por intermédio do NSC, sem prejuízo das atribuições de agentes públicos autorizados por Lei.

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo à pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser

permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 7.845, de 2012, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei.

Art. 8º A Credencial de Segurança, emitida pelo NSC e pelos Órgãos de Registro de nível 1 e 2, é considerada material de acesso restrito, sendo pessoal e intransferível, e com validade explícita na mesma.

Art. 9º As autoridades referidas nos incisos I, II e III do art. 30 do Decreto nº 7.724, de 2012, são consideradas credenciadas *ex officio* no exercício de seu cargo dentro de suas competências e nos seus respectivos graus de sigilo, respeitada a necessidade de conhecer.

Parágrafo 1º. Toda autoridade referida nos incisos II e III do art. 30 do Decreto nº 7.724, de 2012, que tenha necessidade de conhecer informação classificada em grau de sigilo superior àquele para o qual são credenciadas *ex officio*, deverá possuir credencial de segurança no respectivo grau de sigilo, a ser concedida pelo órgão de registro ao qual estiver vinculada.

Art. 10 O suplente indicado e agente público ou militar designado para o desempenho de funções junto à Comissão Mista de Reavaliação de Informações Classificadas deverá possuir Credencial de Segurança para tratamento da informação classificada em qualquer grau de sigilo, válida exclusivamente no âmbito dos trabalhos da citada Comissão.

Art. 11 O credenciamento de segurança será realizado de acordo com os procedimentos constantes das normas complementares a serem expedidas pelo GSI/PR.

Art. 12 A verificação da Credencial de Segurança ou de documento similar emitido por outro país, quando se fizer necessária, será realizada pelo GSI/PR por intermédio do NSC.

Art. 13 Os Órgãos de Registro poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas habilitados, para fins de Credenciamento de Segurança, tratamento de informação classificada e realização de inspeção para habilitação ou investigação para Credenciamento de Segurança, observada a legislação vigente.

Art. 14 O ato da habilitação dos Órgãos de Registro e Postos de Controle lhe conferem a competência do previsto no art. 7º, art. 8º e art. 9º do Decreto nº 7.845, de 2012, respectivamente.

Art. 15 As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Parágrafo único. As áreas ou instalações do Posto de Controle de cada órgão de registro e de entidades privadas são consideradas de acesso restrito.

Art. 16 Órgão ou entidade da iniciativa privada somente poderá ser habilitado como Posto de Controle, mediante solicitação ao Órgão de Registro nível 1 com o qual possuir vínculo de qualquer natureza.

Art. 17 Cabe ao Gestor de Segurança e Credenciamento:

I - a manutenção da qualificação técnica necessária à segurança de informação classificada, em qualquer grau de sigilo, no âmbito do órgão ou entidade com a qual mantém vínculo;

II - a implantação, controle e funcionamento dos protocolos de Documentos Controlados - DC e dos documentos classificados;

III - a conformidade administrativa e sigilo dos processos de credenciamento e habilitação dentro da competência do órgão ou entidade com a qual mantém vínculo;

IV - a proposição à Alta Administração de normas no âmbito do órgão ou entidade com a qual mantém vínculo, para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos;

V - a gestão dos recursos criptográficos, das Credenciais de Segurança e dos materiais de acesso restrito;

VI - o assessoramento da Alta Administração do órgão ou entidade com a qual mantém vínculo, para o tratamento de informações classificadas, em qualquer grau de sigilo; e,

VII - a promoção da capacitação dos agentes públicos ou militares responsáveis pelo tratamento de informação classificada, em qualquer grau de sigilo.

Parágrafo único. A gestão de segurança e credenciamento no que se refere ao tratamento de informação classificada, em qualquer grau de sigilo, abrange ações e métodos que visam à integração das atividades de gestão de risco e de continuidade das ações de controle, acesso, credenciamento e suas capacitações.

Art. 18 Os ministérios e órgãos de nível equivalente que demandarem o tratamento de informação classificada, em qualquer grau de sigilo, deverão, tão logo desejarem, solicitar ao GSI/PR a sua habilitação como Órgão de Registro nível 1.

Parágrafo único. Os Órgãos de Registro nível 1 poderão habilitar quantos Órgãos de Registro nível 2 subordinados forem do seu interesse e conveniência.

Art. 19 A fiscalização prevista no inciso VI do art. 3º do Decreto nº 7.845, de 2012, será realizada por intermédio de visitas técnicas de equipe do NSC, quando se fizer necessário,

bem como, por acompanhamento dos relatórios de conformidade a esta Instrução Normativa e respectivas Normas Complementares, que serão periodicamente enviados pelos Órgãos de Registro e Postos de Controle ao NSC.

Art. 20 Cabe a Alta Administração dos órgãos de registro prever recurso orçamentário específico para o custeio das inspeções, investigações, apoios e visitas técnicas, determinadas nos incisos V do art. 3º, IV do art. 7º e art. 8º do Decreto nº 7.845, de 2012, e art. 19 da presente Instrução Normativa.

Art. 21. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo, com país ou organização estrangeira, o credenciamento de segurança no território nacional, se dará somente se houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil.

Art. 22 As tratativas para a consecução de atos internacionais que envolvam troca de informação classificada, após a manifestação do país interessado e da anuência do Ministério das Relações Exteriores, serão encaminhadas ao GSI/PR para articulação e entendimentos para a formalização.

Parágrafo único. A renegociação dos atos internacionais em vigor que envolvam troca de informação classificada deverá seguir os mesmos procedimentos do *caput*.

Art. 23. Os órgãos e entidades poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos ao credenciamento de segurança e ao tratamento de informação classificada em qualquer grau de sigilo.

Art. 24. Toda quebra de segurança de informação classificada, em qualquer grau de sigilo, deverá ser informada, tempestivamente, pela Alta Administração do órgão ou entidade ao GSI/PR, relatando as circunstâncias com o maior detalhamento possível.

Art. 25 Esta Instrução Normativa entra em vigor na data de sua publicação.

JOSÉ ELITO CARVALHO SIQUEIRA