COLETÂNEA DE ACESSO À INFORMAÇÃO

MINISTÉRIO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO

3ª edição, revista e ampliada

MINISTÉRIO DA TRÂNPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO

OUVIDORIA-GERAL DA UNIÃO
SAS, Quadra 01, Bloco A, Edifício Darcy Ribeiro, 9.º andar
70070-905 - Brasília/DF
cguouvidor@cgu.gov.br
Telefone: (61) 2020-6782
Fax: (61) 2020-7249

ÁREA RESPONSÁVEL PELA PUBLICAÇÃO
Ouvidoria-Geral da União

Capa e editoração: Ascom
Disponível no sítio www.cgu.gov.br/ouvidoria

Apresentação

Esta terceira edição revista e ampliada da Coletânea de Acesso à Informação busca oferecer ao usuário os principais normativos que regem a matéria no âmbito do Poder Executivo federal. Além de trazer novos normativos, como o Decreto nº 8.777, de 11 de maio de 2016, que instituiu a Política de Dados Abertos do Poder Executivo federal e criou o processo administrativo de abertura de dados, esta edição também dá especial atenção à gestão da informação, razão pela qual reproduz a Lei de Arquivos e um conjunto representativo de normas do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

Merece atenção, também, a inclusão do documento "Princípios sobre o Direito de Acesso à Informação", do Comitê Jurídico Interamericano, junto ao capítulo dedicado aos Instrumentos Internacionais, que serviu, ao longo destes primeiros anos de Implantação da Lei de Acesso no Brasil, como importante subsídio para a interpretação do princípio da máxima divulgação, reiteradamente evocado nos pareceres e decisões do Poder Executivo federal.

A Ouvidoria-Geral da União espera que esta publicação sirva como importante instrumento para a efetivação da Lei de Acesso, ao auxiliar cidadãos e servidores a compreender e exercer o direito de acesso à informação.

Sumário

CONSTITUIÇÃO FEDERAL

TÍTULO II
DOS DIREITOS E GARANTIAS FUNDAMENTAIS

CAPÍTULO I
DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[...]

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal

[...]

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

[...]

XXII - é garantido o direito de propriedade;

[...]

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

[...]

LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

[...]

§ 3º 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.

CAPÍTULO VII
DA ADMINISTRAÇÃO PÚBLICA

SEÇÃO I
DISPOSIÇÕES GERAIS

Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:

[...]

§ 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:

I - as reclamações relativas à prestação dos serviços públicos em geral, asseguradas a manutenção de serviços de atendimento ao usuário e a avaliação periódica, externa e interna, da qualidade dos serviços;

II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;

CAPÍTULO III
DA EDUCAÇÃO, DA CULTURA E DO DESPORTO

SEÇÃO II
DA CULTURA

Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:

[...]

§ 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

TRATADOS E DECLARAÇÕES INTERNACIONAIS

Declaração Universal dos Direitos Humanos

Art. XIX

Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

Pacto Internacional sobre Direitos Civis e Políticos

(Promulgado por meio do Decreto nº 592, de 6 de julho de 1992)

ARTIGO 19

1. Ninguém poderá ser molestado por suas opiniões.

2. Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha.

3. O exercício do direito previsto no parágrafo 2 do presente artigo implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para:

a) assegurar o respeito dos direitos e da reputação das demais pessoas;

b) proteger a segurança nacional, a ordem, a saúde ou a moral públicas

Convenção Americana sobre Direitos Humanos ou Pacto de San José da Costa Rica

(Promulgada por meio do Decreto nº 678, de 6 de novembro de 1992)

Artigo 13. Liberdade de pensamento e de expressão

1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda nature-

za, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha.

2. O exercício do direito previsto no inciso precedente não pode estar sujeito a censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei e ser necessárias para assegurar:

a. o respeito aos direitos ou à reputação das demais pessoas; ou

b. a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.

3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de freqüências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de idéias e opiniões.

4. A lei pode submeter os espetáculos públicos a censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2.

5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência.

Declaração de Princípios sobre Liberdade de Expressão

(Aprovado pela Comissão Interamericana de Direitos Humanos em seu 108º período ordinário de sessões, celebrado de 16 a 27 de outubro de 2000)

Princípio 4

O acesso à informação em poder do Estado é um direito fundamental do indivíduo. Os Estados estão obrigados a garantir o exercício desse direito. Este princípio só admite limitações excepcionais que devem estar previamente estabelecidas em lei para o caso de existência de perigo real e iminente que ameace a segurança nacional em sociedades democráticas.

Convenção das Nações Unidas contra a Corrupção

(Promulgada por meio do Decreto nº 5.687, de 31 de janeiro de 2006)

Artigo 10
Informação pública

Tendo em conta a necessidade de combater a corrupção, cada Estado Parte, em conformidade com os princípios fundamentais de sua legislação interna, adotará medidas que sejam necessárias para aumentar a transparência em sua administração pública, inclusive no relativo

a sua organização, funcionamento e processos de adoção de decisões, quando proceder. Essas medidas poderão incluir, entre outras coisas:

a) A instauração de procedimentos ou regulamentações que permitam ao público em geral obter, quando proceder, informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais, sobre as decisões e atos jurídicos que incumbam ao público;

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

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

[...]

Artigo 13
Participação da sociedade

1. Cada Estado Parte adotará medidas adequadas, no limite de suas possibilidades e de conformidade com os princípios fundamentais de sua legislação interna, para fomentar a participação ativa de pessoas e grupos que não pertençam ao setor público, como a sociedade civil, as organizações não-governamentais e as organizações com base na comunidade, na prevenção e na luta contra a corrupção, e para sensibilizar a opinião pública a respeito à existência, às causas e à gravidade da corrupção, assim como a ameaça que esta representa. Essa participação deveria esforçar-se com medidas como as seguintes:

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

b) Garantir o acesso eficaz do público à informação;

c) Realizar atividade de informação pública para fomentar a intransigência à corrupção, assim como programas de educação pública, incluídos programas escolares e universitários;

d) Respeitar, promover e proteger a liberdade de buscar, receber, publicar e difundir informação relativa à corrupção. Essa liberdade poderá estar sujeita a certas restrições, que deverão estar expressamente qualificadas pela lei e ser necessárias para: i) Garantir o respeito dos direitos ou da reputação de terceiros; ii) Salvaguardar a segurança nacional, a ordem pública, ou a saúde ou a moral públicas.

2. Cada Estado Parte adotará medidas apropriadas para garantir que o público tenha conhecimento dos órgão pertinentes de luta contra a corrupção mencionados na presente Convenção, e facilitará o acesso a tais órgãos, quando proceder, para a denúncia, inclusive anônima, de quaisquer incidentes que possam ser considerados constitutivos de um delito qualificado de acordo com a presente Convenção.

Convenção Interamericana contra a Corrupção

(Promulgada por meio do Decreto nº 4.410/2002)

Artigo III
Medidas preventivas

Para os fins estabelecidos no artigo II desta Convenção, os Estados Partes convêm em considerar a aplicabilidade de medidas, em seus próprios sistemas institucionais destinadas a criar, manter e fortalecer:

1. Normas de conduta para o desempenho correto, honrado e adequado das funções públicas. Estas normas deverão ter por finalidade prevenir conflitos de interesses, assegurar a guarda e uso adequado dos recursos confiados aos funcionários públicos no desempenho de suas funções e estabelecer medidas e sistemas para exigir dos funcionários públicos que informem as autoridades competentes dos atos de corrupção nas funções públicas de que tenham conhecimento. Tais medidas ajudarão a preservar a confiança na integridade dos funcionários públicos e na gestão pública.

2. Mecanismos para tornar efetivo o cumprimento dessas normas de conduta.

3. Instruções ao pessoal dos órgãos públicos a fim de garantir o adequado entendimento de suas responsabilidades e das normas éticas que regem as suas atividades.

4. Sistemas para a declaração das receitas, ativos e passivos por parte das pessoas que desempenhem funções públicas em determinados cargos estabelecidos em lei e, quando for o caso, para a divulgação dessas declarações.

5. Sistemas de recrutamento de funcionários públicos e de aquisição de bens e serviços por parte do Estado de forma a assegurar sua transparência, equidade e eficiência.

6. Sistemas para arrecadação e controle da renda do Estado que impeçam a prática da corrupção.

7. Leis que vedem tratamento tributário favorável a qualquer pessoa física ou jurídica em relação a despesas efetuadas com violação dos dispositivos legais dos Estados Partes contra a corrupção.

8. Sistemas para proteger funcionários públicos e cidadãos particulares que denunciarem de boa-fé atos de corrupção, inclusive a proteção de sua identidade, sem prejuízo da Constituição do Estado e dos princípios fundamentais de seu ordenamento jurídico interno.

9. Órgãos de controle superior, a fim de desenvolver mecanismos modernos para prevenir, detectar, punir e erradicar as práticas corruptas.

10. Medidas que impeçam o suborno de funcionários públicos nacionais e estrangeiros, tais como mecanismos para garantir que as sociedades mercantis e outros tipos de associações mantenham registros que, com razoável nível de detalhe, reflitam com exatidão a

aquisição e alienação de ativos e mantenham controles contábeis internos que permitam aos funcionários da empresa detectarem a ocorrência de atos de corrupção.

11. Mecanismos para estimular a participação da sociedade civil e de organizações não-governamentais nos esforços para prevenir a corrupção.

12. O estudo de novas medidas de prevenção, que levem em conta a relação entre uma remuneração equitativa e a probidade no serviço público.

[...]

Artigo XVI
Sigilo bancário

1. O Estado Parte requerido não poderá negar-se a proporcionar a assistência solicitada pelo Estado Parte requerente alegando sigilo bancário. Este artigo será aplicado pelo Estado Parte requerido em conformidade com seu direito interno, com suas disposições processuais e com os acordos bilaterais ou multilaterais que o vinculem ao Estado Parte requerente.

2. O Estado Parte requerente compromete-se a não usar informações protegidas por sigilo bancário que receba para propósito algum que não o do processo que motivou a solicitação, salvo com autorização do Estado Parte requerido.

Declaração do Rio sobre Meio Ambiente e Desenvolvimento – ECO-92

Princípio 10

A melhor maneira de tratar as questões ambientais é assegurar a participação, no nível apropriado, de todos os cidadãos interessados. No nível nacional, cada indivíduo terá acesso adequado às informações relativas ao meio ambiente de que disponham as autoridades públicas, inclusive informações acerca de materiais e atividades perigosas em suas comunidades, bem como a oportunidade de participar dos processos decisórios. Os Estados irão facilitar e estimular a conscientização e a participação popular, colocando as informações à disposição de todos. Será proporcionado o acesso efetivo a mecanismos judiciais e administrativos, inclusive no que se refere à compensação e reparação de danos.

Princípios sobre o Direito de Acesso à Informação (CJI/RES. 147 (LXXIII-O/08)

O COMITÊ JURÍDICO INTERAMERICANO:

RECONHECENDO o direito de acesso à Informação como um direito humano fundamental que garante o acesso à informação em posse dos órgãos públicos, incluindo, dentro de um prazo razoável, o acesso aos arquivos históricos;

CONSCIENTE da decisão da Corte Interamericana de Direitos Humanos no caso de Claude Reyes e outros versus Chile de 19 de setembro de 2006, no qual foi decidido que o direito à liberdade de expressão consagrado no artigo 13 da Convenção Interamericana sobre Direitos Humanos inclui o direito de acesso à informação.

LEVANDO EM CONSIDERAÇÃO as resoluções da Assembleia-Geral da OEA intituladas "Acesso à informação pública: fortalecimento da democracia", AG/RES.1932 (XXXIII-O/03), AG/RES.2057 (XXXIV-O/04), AG/RES.2121 (XXXV-O/05), AG/RES.2252 (XXXVI-O/06), AG/RES.2288 (XXXVII-O/07) e AG/RES.2418 (XXXVIII-O/08), bem como o Estudo das Recomendações sobre Acesso à Informação, apresentado à Comissão de Assuntos Jurídicos e Políticos no dia 24 de abril de 2008 (documento CP/CAJP-2599/08), organizado pelo Departamento de Direito Internacional no cumprimento da Resolução AG/RES. 2288 (XXXVIII- O/07);

LEVANDO EM CONTA as principais declarações internacionais sobre o direito de acesso à informação adotadas por vários órgãos intergovernamentais e organizações não-governamentais, incluindo, entre outros, os princípios do Articulo 19, O Direito a Saber do Público; os Princípios de Lima; os Dez Princípios do Direito a Saber do Open Society Justice Initiative; a Declaração de Atlanta e o Plano de Ação para o avanço do direito de acesso à informação, patrocinado pelo Centro Carter;

MANIFESTANDO SUA AUTORIZAÇÃO para a adoção e implementação de leis de acesso à informação por um número cada vez maior de Estados nas Américas, bem como pelos esforços da parte de outros Estados para adotar essas leis;

CONSIDERANDO a necessidade de desenvolver os princípios vinculados ao direito de acesso à informação, particularmente para apoiar a elaboração e a implementação de leis que tornem esse direito efetivo;

RESOLVE:

Adotar os seguintes princípios, os quais estão inter-relacionados e devem ser interpretados de maneira integral:

1. A princípio, toda informação é acessível. O acesso à informação é um direito humano fundamental que estabelece que toda pessoa pode acessar as informações que estejam sob a guarda de órgãos públicos, sujeito apenas um único regime de exceções, em consonância com uma sociedade democrática e proporcionais ao interesse que os justifica. Os Estados devem assegurar o respeito ao direito de acesso à informação, adotando a legislação apropriada e colocando em prática os meios necessários para a sua implementação.

2. O direito de acesso à informação se estende a todos os órgãos públicos em todos os níveis de governo, incluindo os pertencentes aos poderes executivo, legislativo e judiciário, aos órgãos criados por constituições ou por outras leis, órgãos de governo ou

controlado por ele, assim como organizações que operam com fundos públicos ou que desenvolvem funções públicas.

3. O direito de acesso à informação se refere a toda informação significante, cuja definição deve ser ampla, incluindo toda a informação controlada e arquivada em qualquer formato ou meio.

4. Os órgãos públicos devem difundir informações sobre suas funções e atividades – incluindo sua política, oportunidades de consultas, atividades que afetam o público, orçamentos, subsídios, benefícios e contratos – de forma rotineira e proativa, ainda que na ausência de um pedido específica, e de maneira que assegure que a informação seja acessível y compreensível.

5. Devem ser implementadas regras claras, justas, não-discriminatórias e simples quanto ao processo de manuseio de pedidos de informação. Essas regras devem incluir prazos claros e razoáveis, assistência para o solicitante de informação, o acesso gratuito ou de baixo custo e que, nesse caso, não exceda o custo da fotocópia ou envio da informação por correspondência. As regras devem estabelecer que quando o acesso for negado, o órgão em questão deve fornecer as justificativas necessárias para a negativa, em tempo hábil.

6. As exceções ao direito de acesso à informação devem ser estabelecidas pela lei, ser claras y limitadas.

7. A responsabilidade por justificar qualquer negativa de acesso à informação deve recair sobre órgão ao qual a informação foi solicitada.

8. Todo indivíduo tem o direito de recorrer a qualquer negativa ou obstrução de acesso à informação perante uma instância administrativa. Também deve existir o direito de apelar das decisões do órgão em questão perante a justiça.

9. Toda pessoa que intencionalmente negue ou obstrua o acesso à informação violando as regras que garantem esse direito deve ser punida com as medidas cabíveis.

10. Deve-se adotar medidas para promover, implementar e assegurar o direito de acesso à informação incluindo a criação e a manutenção de arquivos públicos de maneira séria e profissional, a capacitação e o treinamento de funcionários públicos, a implementação de programas para divulgar a importância desse direito ao público, o melhoramento dos sistemas de administração e manuseio da informação, assim como a divulgação das medidas tomadas pelos órgãos públicos para implementar o direito de acesso à informação, inclusive em relação ao processamento dos pedidos de acesso à informação.

A presente resolução foi aprovada por unanimidade, na seção do dia 07 de agosto de 2008, pelos seguintes membros: doutores Ricardo Seitenfus, Ana Elizabeth Villalta Vizcarra, Guillermo Fernández de Soto, Jorge Palacios Treviño, Mauricio Herdocia Sacasa, Freddy Castillo Castellanos, Jaime Aparicio, Jean-Paul Hubert e Hyacinth Evadne Lindsay.

LEIS

Lei de Arquivos

LEI Nº 8.159, DE 8 DE JANEIRO DE 1991.

Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências

O PRESIDENTE DA REPÚBLICA, faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º - 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.

Art. 2º - Consideram-se arquivos, para os fins desta Lei, os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

Art. 3º - Considera-se gestão de documentos o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

Art. 4º - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Art. 5º - A Administração Pública franqueará a consulta aos documentos públicos na forma desta Lei.

Art. 6º - Fica resguardado o direito de indenização pelo dano material ou moral decorrente da violação do sigilo, sem prejuízo das ações penal, civil e administrativa.

CAPÍTULO II
DOS ARQUIVOS PÚBLICO

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.

§ 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 freqüentes.

§ 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. 10º - Os documentos de valor permanente são inalienáveis e imprescritíveis.

CAPÍTULO III
DOS ARQUIVOS PRIVADOS

Art. 11 - Consideram-se arquivos privados os conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, em decorrência de suas atividades.

Art. 12 - Os arquivos privados podem ser 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.

Art. 13 - Os arquivos privados identificados como de interesse público e social não poderão ser alienados com dispersão ou perda da unidade documental, nem transferidos para o exterior.

Parágrafo único - Na alienação desses arquivos o Poder Público exercerá preferência na aquisição.

Art. 14 - O acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ser franqueado mediante autorização de seu proprietário ou possuidor.

Art. 15 - Os arquivos privados identificados como de interesse público e social poderão ser depositados a título revogável, ou doados a instituições arquivísticas públicas.

Art. 16 - Os registros civis de arquivos de entidades religiosas produzidos anteriormente à vigência do Código Civil ficam identificados como de interesse público e social.

CAPÍTULO IV
DA ORGANIZAÇÃO E ADMINISTRAÇÃO DE INSTITUIÇÕES ARQUIVÍSTICAS PÚBLICAS

Art. 17 - A administração da documentação pública ou de caráter público compete às instituições arquivísticas federais, estaduais, do Distrito Federal e municipais.

§ 1º - São Arquivos Federais o Arquivo Nacional os do Poder Executivo, e os arquivos do Poder Legislativo e do Poder Judiciário. São considerados, também, do Poder Executivo os arquivos do Ministério da Marinha, do Ministério das Relações Exteriores, do Ministério do Exército e do Ministério da Aeronáutica.

§ 2º - São Arquivos Estaduais os arquivos do Poder Executivo, o arquivo do Poder Legislativo e o arquivo do Poder Judiciário.

§ 3º - São Arquivos do Distrito Federal o arquivo do Poder Executivo, o Arquivo do Poder Legislativo e o arquivo do Poder Judiciário.

§ 4º - São Arquivos Municipais o arquivo do Poder Executivo e o arquivo do Poder Legislativo.

§ 5º - Os arquivos públicos dos Territórios são organizados de acordo com sua estrutura político-jurídica.

Art. 18 - Compete ao Arquivo 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.

Parágrafo único - Para o pleno exercício de suas funções, o Arquivo Nacional poderá criar unidades regionais.

Art. 19 - Competem aos arquivos do Poder Legislativo Federal a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Legislativo Federal no exercício das suas funções, bem como preservar e facultar o acesso aos documentos sob sua guarda.

Art. 20 - Competem aos arquivos do Poder Judiciário Federal a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Judiciário Federal no exercício de suas funções, tramitados em juízo e oriundos de cartórios e secretarias, bem como preservar e facultar o acesso aos documentos sob sua guarda.

Art. 21 - Legislação estadual, do Distrito Federal e municipal definirá os critérios de organização e vinculação dos arquivos estaduais e municipais, bem como a gestão e o acesso aos documentos, observado o disposto na Constituição Federal e nesta Lei.

CAPÍTULO V
DO ACESSO E DO SIGILO DOS DOCUMENTOS PÚBLICOS

[Revogado pela Lei 12.527, de 18 de novembro de 2011)

DISPOSIÇÕES FINAIS

Art. 25 - Ficará sujeito à responsabilidade penal, civil e administrativa, na forma da legislação em vigor, aquele que desfigurar ou destruir documentos de valor permanente ou considerado como de interesse público e social.

Art. 26 - Fica criado o Conselho Nacional de Arquivos (CONARQ), órgão vinculado ao Arquivo Nacional, que definirá a política nacional de arquivos, como órgão central de um Sistema Nacional de Arquivos (SINAR).

§ 1º - O Conselho Nacional de Arquivos será presidido pelo Diretor-Geral do Arquivo Nacional e integrado por representantes de instituições arquivísticas e acadêmicas, públicas e privadas.

§ 2º - A estrutura e funcionamento do conselho criado neste artigo serão estabelecidos em regulamento.

Art. 27 - Esta Lei entra em vigor na data de sua publicação.

Art. 28 - Revogam-se as disposições em contrário.

Brasília, 8 de janeiro de 1991; 170º da Independência e 103º da República.

FERNANDO COLLOR

Jarbas Passarinho

Lei de Acesso à Informação

LEI Nº 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 no8.112, 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

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES GERAIS

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

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Art. 2o Aplicam-se as disposições desta Lei, no que couber, 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.

Parágrafo único. A publicidade a que estão submetidas as entidades citadas no caput refere-se à parcela dos recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas.

Art. 3o Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;

II - divulgação de informações de interesse público, independentemente de solicitações;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

IV - fomento ao desenvolvimento da cultura de transparência na administração pública;

V - desenvolvimento do controle social da administração pública.

Art. 4o Para os efeitos desta Lei, considera-se:

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Art. 5o 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.

CAPÍTULO II
DO ACESSO A INFORMAÇÕES E DA SUA DIVULGAÇÃO

Art. 6o Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, 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.

Art. 7o O acesso à informação de que trata esta Lei 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.

§ 1o O acesso à informação previsto no caput não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

§ 2o Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

§ 3o O direito de acesso aos documentos ou às informações neles contidas utilizados como fundamento da tomada de decisão e do ato administrativo será assegurado com a edição do ato decisório respectivo.

§ 4o A negativa de acesso às informações objeto de pedido formulado aos órgãos e entidades referidas no art. 1o, quando não fundamentada, sujeitará o responsável a medidas disciplinares, nos termos do art. 32 desta Lei.

§ 5o Informado do extravio da informação solicitada, poderá o interessado requerer à autoridade competente a imediata abertura de sindicância para apurar o desaparecimento da respectiva documentação.

§ 6o Verificada a hipótese prevista no § 5o deste artigo, o responsável pela guarda da informação extraviada deverá, no prazo de 10 (dez) dias, justificar o fato e indicar testemunhas que comprovem sua alegação.

Art. 8o É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

§ 1o Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:

I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;

II - registros de quaisquer repasses ou transferências de recursos financeiros;

III - registros das despesas;

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e

VI - respostas a perguntas mais frequentes da sociedade.

§ 2o Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

§ 3o Os sítios de que trata o § 2o deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:

I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;

II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e

VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei no 10.098, de 19 de dezembro de 2000, e do art. 9o da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo no 186, de 9 de julho de 2008.

§ 4o Os Municípios com população de até 10.000 (dez mil) habitantes ficam dispensados da divulgação obrigatória na internet a que se refere o § 2o, mantida a obrigatoriedade de divulgação, em tempo real, de informações relativas à execução orçamentária e financeira, nos critérios e prazos previstos no art. 73-B da Lei Complementar no 101, de 4 de maio de 2000 (Lei de Responsabilidade Fiscal).

Art. 9o O acesso a informações públicas será assegurado mediante:

I - criação de serviço de informações ao cidadão, nos órgãos e entidades do poder público, em local com condições apropriadas para:

a) atender e orientar o público quanto ao acesso a informações;

b) informar sobre a tramitação de documentos nas suas respectivas unidades;

c) protocolizar documentos e requerimentos de acesso a informações; e

II - realização de audiências ou consultas públicas, incentivo à participação popular ou a outras formas de divulgação.

CAPÍTULO III
DO PROCEDIMENTO DE ACESSO À INFORMAÇÃO

Seção I
Do Pedido de Acesso

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.

§ 1o Para o acesso a informações de interesse público, a identificação do requerente não pode conter exigências que inviabilizem a solicitação.

§ 2o Os órgãos e entidades do poder público devem viabilizar alternativa de encaminhamento de pedidos de acesso por meio de seus sítios oficiais na internet.

§ 3o São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público.

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.

§ 6o Caso 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.

Art. 12. O serviço de busca e fornecimento da informação é gratuito, salvo nas hipóteses de reprodução de documentos pelo órgão ou entidade pública consultada, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

Parágrafo único. Estará isento de ressarcir os custos previstos no caput todo aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da Lei no 7.115, de 29 de agosto de 1983.

Art. 13. Quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade, deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original.

Parágrafo único. Na impossibilidade de obtenção de cópias, o interessado poderá solicitar que, a suas expensas e sob supervisão de servidor público, a reprodução seja feita por outro meio que não ponha em risco a conservação do documento original.

Art. 14. É direito do requerente obter o inteiro teor de decisão de negativa de acesso, por certidão ou cópia.

Seção II
Dos Recursos

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.

Art. 17. No caso de indeferimento de pedido de desclassificação de informação protocolado em órgão da administração pública federal, poderá o requerente recorrer ao Ministro de Estado da área, sem prejuízo das competências da Comissão Mista de Reavaliação de Informações, previstas no art. 35, e do disposto no art. 16.

§ 1o O recurso previsto neste artigo somente poderá ser dirigido às autoridades mencionadas depois de submetido à apreciação de pelo menos uma autoridade hierarquicamente superior à autoridade que exarou a decisão impugnada e, no caso das Forças Armadas, ao respectivo Comando.

§ 2o Indeferido o recurso previsto no caput que tenha como objeto a desclassificação de informação secreta ou ultrassecreta, caberá recurso à Comissão Mista de Reavaliação de Informações prevista no art. 35.

Art. 18. Os procedimentos de revisão de decisões denegatórias proferidas no recurso previsto no art. 15 e de revisão de classificação de documentos sigilosos serão objeto de regulamentação própria dos Poderes Legislativo e Judiciário e do Ministério Público, em seus respectivos âmbitos, assegurado ao solicitante, em qualquer caso, o direito de ser informado sobre o andamento de seu pedido.

Art. 19. (VETADO).

§ 1o (VETADO).

§ 2o Os órgãos do Poder Judiciário e do Ministério Público informarão ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público, respectivamente, as decisões que, em grau de recurso, negarem acesso a informações de interesse público.

Art. 20. Aplica-se subsidiariamente, no que couber, a Lei no 9.784, de 29 de janeiro de 1999, ao procedimento de que trata este Capítulo.

CAPÍTULO IV
DAS RESTRIÇÕES DE ACESSO À INFORMAÇÃO

Seção I
Disposições Gerais

Art. 21. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.

Parágrafo único. 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.

Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

Seção II
Da Classificação da Informação quanto ao Grau e Prazos de Sigilo

Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:

I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

III - pôr em risco a vida, a segurança ou a saúde da população;

IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.

§ 1o Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput, vigoram a partir da data de sua produção e são os seguintes:

I - ultrassecreta: 25 (vinte e cinco) anos;

II - secreta: 15 (quinze) anos; e

III - reservada: 5 (cinco) anos.

§ 2o As informações que puderem colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as) serão classificadas como reservadas e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

§ 3o Alternativamente aos prazos previstos no § 1o, poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, desde que este ocorra antes do transcurso do prazo máximo de classificação.

§ 4o Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação tornar-se-á, automaticamente, de acesso público.

§ 5o Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I - a gravidade do risco ou dano à segurança da sociedade e do Estado; e

II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

Seção III
Da Proteção e do Controle de Informações Sigilosas

Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.

§ 1o O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.

§ 2o O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.

§ 3o Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.

Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.

Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei.

Seção IV
Dos Procedimentos de Classificação, Reclassificação e Desclassificação

Art. 27. 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.

§ 1o A competência prevista nos incisos I e II, no que se refere à classificação como ultrassecreta e secreta, poderá ser delegada pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação.

§ 2o A classificação de informação no grau de sigilo ultrassecreto pelas autoridades previstas nas alíneas "d" e "e" do inciso I deverá ser ratificada pelos respectivos Ministros de Estado, no prazo previsto em regulamento.

§ 3o A autoridade ou outro agente público que classificar informação como ultrassecreta deverá encaminhar a decisão de que trata o art. 28 à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35, no prazo previsto em regulamento.

Art. 28. A classificação de informação em qualquer grau de sigilo deverá ser formalizada em decisão que conterá, no mínimo, os seguintes elementos:

I - assunto sobre o qual versa a informação;

II - fundamento da classificação, observados os critérios estabelecidos no art. 24;

III - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, conforme limites previstos no art. 24; e

IV - identificação da autoridade que a classificou.

Parágrafo único. A decisão referida no caput será mantida no mesmo grau de sigilo da informação classificada.

Art. 29. A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, nos termos e prazos previstos em regulamento, com vistas à sua desclassificação ou à redução do prazo de sigilo, observado o disposto no art. 24.

§ 1o O regulamento a que se refere o caput deverá considerar as peculiaridades das informações produzidas no exterior por autoridades ou agentes públicos.

§ 2o Na reavaliação a que se refere o caput, deverão ser examinadas a permanência dos motivos do sigilo e a possibilidade de danos decorrentes do acesso ou da divulgação da informação.

§ 3o Na hipótese de redução do prazo de sigilo da informação, o novo prazo de restrição manterá como termo inicial a data da sua produção.

Art. 30. A autoridade máxima de cada órgão ou entidade publicará, anualmente, em sítio à disposição na internet e destinado à veiculação de dados e informações administrativas, nos termos de regulamento:

I - rol das informações que tenham sido desclassificadas nos últimos 12 (doze) meses;

II - rol de documentos classificados em cada grau de sigilo, com identificação para referência futura;

III - relatório estatístico contendo a quantidade de pedidos de informação recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes.

§ 1o Os órgãos e entidades deverão manter exemplar da publicação prevista no caput para consulta pública em suas sedes.

§ 2o Os órgãos e entidades manterão extrato com a lista de informações classificadas, acompanhadas da data, do grau de sigilo e dos fundamentos da classificação.

Seção V
Das Informações Pessoais

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1o As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - 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

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2o Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3o O consentimento referido no inciso II do § 1o 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.

§ 4o 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.

§ 5o Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:

I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;

IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;

V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;

VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e

VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

§ 1o Atendido o princípio do contraditório, da ampla defesa e do devido processo legal, as condutas descritas no caput serão consideradas:

I - para fins dos regulamentos disciplinares das Forças Armadas, transgressões militares médias ou graves, segundo os critérios neles estabelecidos, desde que não tipificadas em lei como crime ou contravenção penal; ou

II - para fins do disposto na Lei no 8.112, de 11 de dezembro de 1990, e suas alterações, infrações administrativas, que deverão ser apenadas, no mínimo, com suspensão, segundo os critérios nela estabelecidos.

§ 2o Pelas condutas descritas no caput, poderá o militar ou agente público responder, também, por improbidade administrativa, conforme o disposto nasLeis nos 1.079, de 10 de abril de 1950, e 8.429, de 2 de junho de 1992.

Art. 33. A pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto nesta Lei estará sujeita às seguintes sanções:

I - advertência;

II - multa;

III - rescisão do vínculo com o poder público;

IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a 2 (dois) anos; e

V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

§ 1o As sanções previstas nos incisos I, III e IV poderão ser aplicadas juntamente com a do inciso II, assegurado o direito de defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias.

§ 2o A reabilitação referida no inciso V será autorizada somente quando o interessado efetivar o ressarcimento ao órgão ou entidade dos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso IV.

§ 3o A aplicação da sanção prevista no inciso V é de competência exclusiva da autoridade máxima do órgão ou entidade pública, facultada a defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista.

Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.

CAPÍTULO VI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 35. (VETADO).

§ 1o É instituída a 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, observado o prazo previsto no § 1o do art. 24.

§ 2o O prazo referido no inciso III é limitado a uma única renovação.

§ 3o A revisão de ofício a que se refere o inciso II do § 1o deverá ocorrer, no máximo, a cada 4 (quatro) anos, após a reavaliação prevista no art. 39, quando se tratar de documentos ultrassecretos ou secretos.

§ 4o A não deliberação sobre a revisão pela Comissão Mista de Reavaliação de Informações nos prazos previstos no § 3o implicará a desclassificação automática das informações.

§ 5o Regulamento disporá sobre a composição, organização e funcionamento da Comissão Mista de Reavaliação de Informações, observado o mandato de 2 (dois) anos para seus integrantes e demais disposições desta Lei.

Art. 36. O tratamento de informação sigilosa resultante de tratados, acordos ou atos internacionais atenderá às normas e recomendações constantes desses instrumentos.

Art. 37. É instituído, no âmbito do Gabinete de Segurança Institucional da Presidência da República, o Núcleo de Segurança e Credenciamento (NSC), que tem por objetivos:

I - promover e propor a regulamentação do credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações sigilosas; e

II - garantir a segurança de informações sigilosas, inclusive aquelas provenientes de países ou organizações internacionais com os quais a República Federativa do Brasil tenha firmado tratado, acordo, contrato ou qualquer outro ato internacional, sem prejuízo das atribuições do Ministério das Relações Exteriores e dos demais órgãos competentes.

Parágrafo único. Regulamento disporá sobre a composição, organização e funcionamento do NSC.

Art. 38. Aplica-se, no que couber, a Lei no 9.507, de 12 de novembro de 1997, em relação à informação de pessoa, física ou jurídica, constante de registro ou banco de dados de entidades governamentais ou de caráter público.

Art. 39. Os órgãos e entidades públicas deverão proceder à reavaliação das informações classificadas como ultrassecretas e secretas no prazo máximo de 2 (dois) anos, contado do termo inicial de vigência desta Lei.

§ 1o A restrição de acesso a informações, em razão da reavaliação prevista no caput, deverá observar os prazos e condições previstos nesta Lei.

§ 2o No âmbito da administração pública federal, a reavaliação prevista no caput poderá ser revista, a qualquer tempo, pela Comissão Mista de Reavaliação de Informações, observados os termos desta Lei.

§ 3o Enquanto não transcorrido o prazo de reavaliação previsto no caput, será mantida a classificação da informação nos termos da legislação precedente.

§ 4o As informações classificadas como secretas e ultrassecretas não reavaliadas no prazo previsto no caput serão consideradas, automaticamente, de acesso público.

Art. 40. No prazo de 60 (sessenta) dias, a contar da vigência desta Lei, o dirigente máximo de cada órgão ou entidade da administração pública federal direta e indireta designará autoridade que lhe seja diretamente subordinada para, no âmbito do respectivo órgão ou entidade, exercer as seguintes atribuições:

I - assegurar o cumprimento das normas relativas ao acesso a informação, de forma eficiente e adequada aos objetivos desta Lei;

II - monitorar a implementação do disposto nesta Lei e apresentar relatórios periódicos sobre o seu cumprimento;

III - recomendar as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto nesta Lei; e

IV - orientar as respectivas unidades no que se refere ao cumprimento do disposto nesta Lei e seus regulamentos.

Art. 41. O Poder Executivo Federal designará órgão da administração pública federal responsável:

I - pela promoção de campanha de abrangência nacional de fomento à cultura da transparência na administração pública e conscientização do direito fundamental de acesso à informação;

II - pelo treinamento de agentes públicos no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública;

III - pelo monitoramento da aplicação da lei no âmbito da administração pública federal, concentrando e consolidando a publicação de informações estatísticas relacionadas no art. 30;

IV - pelo encaminhamento ao Congresso Nacional de relatório anual com informações atinentes à implementação desta Lei.

Art. 42. O Poder Executivo regulamentará o disposto nesta Lei no prazo de 180 (cento e oitenta) dias a contar da data de sua publicação.

Art. 43. O inciso VI do art. 116 da Lei no 8.112, de 11 de dezembro de 1990, passa a vigorar com a seguinte redação:

"Art. 116. .....

.....

VI - levar as irregularidades de que tiver ciência em razão do cargo ao conhecimento da autoridade superior ou, quando houver suspeita de envolvimento desta, ao conhecimento de outra autoridade competente para apuração;

....." (NR)

Art. 44. O Capítulo IV do Título IV da Lei no 8.112, de 1990, passa a vigorar acrescido do seguinte art. 126-A:

"Art. 126-A. Nenhum servidor poderá ser responsabilizado civil, penal ou administrativamente por dar ciência à autoridade superior ou, quando houver suspeita de envolvimento desta, a outra autoridade competente para apuração de informação concernente à prática de crimes ou improbidade de que tenha conhecimento, ainda que em decorrência do exercício de cargo, emprego ou função pública."

Art. 45. Cabe aos Estados, ao Distrito Federal e aos Municípios, em legislação própria, obedecidas as normas gerais estabelecidas nesta Lei, definir regras específicas, especialmente quanto ao disposto no art. 9o e na Seção II do Capítulo III.

Art. 46. Revogam-se:

I - a Lei no 11.111, de 5 de maio de 2005; e

II - os arts. 22 a 24 da Lei no 8.159, de 8 de janeiro de 1991.

Art. 47. Esta Lei entra em vigor 180 (cento e oitenta) dias após a data de sua publicação.

Brasília, 18 de novembro de 2011; 190o da Independência e 123o da República.

DILMA ROUSSEFF
José Eduardo Cardoso
Celso Luiz Nunes Amorim
Antonio de Aguiar Patriota
Miriam Belchior
Paulo Bernardo Silva
Gleisi Hoffmann
José Elito Carvalho Siqueira
Helena Chagas
Luís Inácio Lucena Adams
Jorge Hage Sobrinho
Maria do Rosário Nunes

DECRETOS DE REGULAMENTAÇÃO DA LEI DE ACESSO À INFORMAÇÃO

DECRETO Nº 7.724, DE 16 DE MAIO DE 2012

Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.

A PRESIDENTA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, caput, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Lei no 12.527, de 18 de novembro de 2011,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1o Este Decreto regulamenta, 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, conforme o disposto na Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.

Art. 2o Os órgãos e as entidades do Poder Executivo federal assegurarão, às pessoas naturais e jurídicas, o direito de acesso à informação, que será proporcionado mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão, observados os princípios da administração pública e as diretrizes previstas na Lei no 12.527, de 2011.

Art. 3o Para os efeitos deste Decreto, considera-se:

I - informação - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - dados processados - dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

III - documento - unidade de registro de informações, qualquer que seja o suporte ou formato;

IV - informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

V - informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

VI - tratamento da informação - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VII - disponibilidade - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VIII - autenticidade - qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

IX - integridade - qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

X - primariedade - qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

XI - informação atualizada - informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam; e

XII - documento preparatório - documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas.

Art. 4o A busca e o fornecimento da informação são gratuitos, ressalvada a cobrança do valor referente ao custo dos serviços e dos materiais utilizados, tais como reprodução de documentos, mídias digitais e postagem.

Parágrafo único. Está isento de ressarcir os custos dos serviços e dos materiais utilizados aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da Lei no 7.115, de 29 de agosto de 1983.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 5o Sujeitam-se ao disposto neste Decreto os órgãos da administração direta, as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e as demais entidades controladas direta ou indiretamente pela União.

§ 1o A divulgação de informações de empresas públicas, sociedade de economia mista e demais entidades controladas pela União que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, estará submetida às normas pertinentes da Comissão de Valores Mobiliários, a fim de assegurar sua competitividade, governança corporativa e, quando houver, os interesses de acionistas minoritários.

§ 2o Não se sujeitam ao disposto neste Decreto as informações relativas à atividade empresarial de pessoas físicas ou jurídicas de direito privado obtidas pelo Banco Central do Brasil, pelas agências reguladoras ou por outros órgãos ou entidades no exercício de atividade de controle, regulação e supervisão da atividade econômica cuja divulgação possa representar vantagem competitiva a outros agentes econômicos.

Art. 6o O acesso à informação disciplinado neste Decreto não se aplica:

I - às hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça; e

II - às informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado, na forma do §1o do art. 7o da Lei no 12.527, de 2011.

CAPÍTULO III
DA TRANSPARÊNCIA ATIVA

Art. 7o É dever dos órgãos e entidades promover, independente de requerimento, a divulgação em seus sítios na Internet de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, observado o disposto nos arts. 7o e 8o da Lei no 12.527, de 2011.

§ 1o Os órgãos e entidades deverão implementar em seus sítios na Internet seção específica para a divulgação das informações de que trata o caput.

§ 2o Serão disponibilizados nos sítios na Internet dos órgãos e entidades, conforme padrão estabelecido pela Secretaria de Comunicação Social da Presidência da República:

I - banner na página inicial, que dará acesso à seção específica de que trata o § 1o; e

II - barra de identidade do Governo federal, contendo ferramenta de redirecionamento de página para o Portal Brasil e para o sítio principal sobre a Lei no12.527, de 2011.

§ 3o Deverão ser divulgadas, na seção específica de que trata o § 1o, informações sobre:

I - estrutura organizacional, competências, legislação aplicável, principais cargos e seus ocupantes, endereço e telefones das unidades, horários de atendimento ao público;

II - programas, projetos, ações, obras e atividades, com indicação da unidade responsável, principais metas e resultados e, quando existentes, indicadores de resultado e impacto;

III - repasses ou transferências de recursos financeiros;

IV - execução orçamentária e financeira detalhada;

V - licitações realizadas e em andamento, com editais, anexos e resultados, além dos contratos firmados e notas de empenho emitidas;

VI - remuneração e subsídio recebidos por ocupante de cargo, posto, graduação, função e emprego público, incluindo auxílios, ajudas de custo, jetons e quaisquer outras vantagens pecuniárias, bem como proventos de aposentadoria e pensões daqueles que estiverem na ativa, de maneira individualizada, conforme ato do Ministério do Planejamento, Orçamento e Gestão;

VII - respostas a perguntas mais frequentes da sociedade; (Redação dada pelo Decreto nº 8.408, de 2015)

VIII - contato da autoridade de monitoramento, designada nos termos do art. 40 da Lei nº 12.527, de 2011, e telefone e correio eletrônico do Serviço de Informações ao Cidadão - SIC; e (Redação dada pelo Decreto nº 8.408, de 2015)

IX - programas financiados pelo Fundo de Amparo ao Trabalhador - FAT. (Incluído pelo Decreto nº 8.408, de 2015)

§ 4o As informações poderão ser disponibilizadas por meio de ferramenta de redirecionamento de página na Internet, quando estiverem disponíveis em outros sítios governamentais.

§ 5o No caso das empresas públicas, sociedades de economia mista e demais entidades controladas pela União que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, aplica-se o disposto no § 1o do art. 5o.

§ 6o O Banco Central do Brasil divulgará periodicamente informações relativas às operações de crédito praticadas pelas instituições financeiras, inclusive as taxas de juros mínima, máxima e média e as respectivas tarifas bancárias.

§ 7o A divulgação das informações previstas no § 3o não exclui outras hipóteses de publicação e divulgação de informações previstas na legislação.

§ 8º Ato conjunto dos Ministros de Estado da Controladoria-Geral da União, do Planejamento, Orçamento e Gestão e do Trabalho e Emprego disporá sobre a divulgação dos programas de que trata o inciso IX do § 3º, que será feita, observado o disposto no Capítulo VII: (Incluído pelo Decreto nº 8.408, de 2015)

I - de maneira individualizada; (Incluído pelo Decreto nº 8.408, de 2015)

II - por meio de informações consolidadas disponibilizadas no sítio na Internet do Ministério do Trabalho e Emprego; e (Incluído pelo Decreto nº 8.408, de 2015)

III - por meio de disponibilização de variáveis das bases de dados para execução de cruzamentos, para fins de estudos e pesquisas, observado o disposto no art. 13. (Incluído pelo Decreto nº 8.408, de 2015)

Art. 8o Os sítios na Internet dos órgãos e entidades deverão, em cumprimento às normas estabelecidas pelo Ministério do Planejamento, Orçamento e Gestão, atender aos seguintes requisitos, entre outros:

I - conter formulário para pedido de acesso à informação;

II - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;

III - possibilitar gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

IV - possibilitar acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

V - divulgar em detalhes os formatos utilizados para estruturação da informação;

VI - garantir autenticidade e integridade das informações disponíveis para acesso;

VII - indicar instruções que permitam ao requerente comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade; e

VIII - garantir a acessibilidade de conteúdo para pessoas com deficiência.

CAPÍTULO IV
DA TRANSPARÊNCIA PASSIVA

Seção I
Do Serviço de Informação ao Cidadão

Art. 9o Os órgãos e entidades deverão criar Serviço de Informações ao Cidadão - SIC, com o objetivo de:

I - atender e orientar o público quanto ao acesso à informação;

II - informar sobre a tramitação de documentos nas unidades; e

III - receber e registrar pedidos de acesso à informação.

Parágrafo único. Compete ao SIC:

I - o recebimento do pedido de acesso e, sempre que possível, o fornecimento imediato da informação;

II - o registro do pedido de acesso em sistema eletrônico específico e a entrega de número do protocolo, que conterá a data de apresentação do pedido; e

III - o encaminhamento do pedido recebido e registrado à unidade responsável pelo fornecimento da informação, quando couber.

Art. 10. O SIC será instalado em unidade física identificada, de fácil acesso e aberta ao público.

§ 1o Nas unidades descentralizadas em que não houver SIC será oferecido serviço de recebimento e registro dos pedidos de acesso à informação.

§ 2o Se a unidade descentralizada não detiver a informação, o pedido será encaminhado ao SIC do órgão ou entidade central, que comunicará ao requerente o número do protocolo e a data de recebimento do pedido, a partir da qual se inicia o prazo de resposta.

Seção II
Do Pedido de Acesso à Informação

Art. 11. Qualquer pessoa, natural ou jurídica, poderá formular pedido de acesso à informação.

§ 1o O pedido será apresentado em formulário padrão, disponibilizado em meio eletrônico e físico, no sítio na Internet e no SIC dos órgãos e entidades.

§ 2o O prazo de resposta será contado a partir da data de apresentação do pedido ao SIC.

§ 3o É facultado aos órgãos e entidades o recebimento de pedidos de acesso à informação por qualquer outro meio legítimo, como contato telefônico, correspondência eletrônica ou física, desde que atendidos os requisitos do art. 12.

§ 4o Na hipótese do § 3o, será enviada ao requerente comunicação com o número de protocolo e a data do recebimento do pedido pelo SIC, a partir da qual se inicia o prazo de resposta.

Art. 12. O pedido de acesso à informação deverá conter:

I - nome do requerente;

II - número de documento de identificação válido;

III - especificação, de forma clara e precisa, da informação requerida; e

IV - endereço físico ou eletrônico do requerente, para recebimento de comunicações ou da informação requerida.

Art. 13. Não serão atendidos pedidos de acesso à informação:

I - genéricos;

II - desproporcionais ou desarrazoados; ou

III - que exijam trabalhos adicionais de análise, interpretação ou consolidação de dados e informações, ou serviço de produção ou tratamento de dados que não seja de competência do órgão ou entidade.

Parágrafo único. Na hipótese do inciso III do caput, o órgão ou entidade deverá, caso tenha conhecimento, indicar o local onde se encontram as informações a partir das quais o requerente poderá realizar a interpretação, consolidação ou tratamento de dados.

Art. 14. São vedadas exigências relativas aos motivos do pedido de acesso à informação.

Seção III
Do Procedimento de Acesso à Informação

Art. 15. Recebido o pedido e estando a informação disponível, o acesso será imediato.

§ 1o Caso não seja possível o acesso imediato, o órgão ou entidade deverá, no prazo de até vinte dias:

I - enviar a informação ao endereço físico ou eletrônico informado;

II - comunicar data, local e modo para realizar consulta à informação, efetuar reprodução ou obter certidão relativa à informação;

III - comunicar que não possui a informação ou que não tem conhecimento de sua existência;

IV - indicar, caso tenha conhecimento, o órgão ou entidade responsável pela informação ou que a detenha; ou

V - indicar as razões da negativa, total ou parcial, do acesso.

§ 2o Nas hipóteses em que o pedido de acesso demandar manuseio de grande volume de documentos, ou a movimentação do documento puder comprometer sua regular tramitação, será adotada a medida prevista no inciso II do § 1o.

§ 3o Quando a manipulação puder prejudicar a integridade da informação ou do documento, o órgão ou entidade deverá indicar data, local e modo para consulta, ou disponibilizar cópia, com certificação de que confere com o original.

§ 4o Na impossibilidade de obtenção de cópia de que trata o § 3o, o requerente poderá solicitar que, às suas expensas e sob supervisão de servidor público, a reprodução seja feita por outro meio que não ponha em risco a integridade do documento original.

Art. 16. O prazo para resposta do pedido poderá ser prorrogado por dez dias, mediante justificativa encaminhada ao requerente antes do término do prazo inicial de vinte dias.

Art. 17. Caso a informação esteja disponível ao público em formato impresso, eletrônico ou em outro meio de acesso universal, o órgão ou entidade deverá orientar o requerente quanto ao local e modo para consultar, obter ou reproduzir a informação.

Parágrafo único. Na hipótese do caput o órgão ou entidade desobriga-se do fornecimento direto da informação, salvo se o requerente declarar não dispor de meios para consultar, obter ou reproduzir a informação.

Art. 18. Quando o fornecimento da informação implicar reprodução de documentos, o órgão ou entidade, observado o prazo de resposta ao pedido, disponibilizará ao requerente Guia de Recolhimento da União - GRU ou documento equivalente, para pagamento dos custos dos serviços e dos materiais utilizados.

Parágrafo único. A reprodução de documentos ocorrerá no prazo de dez dias, contado da comprovação do pagamento pelo requerente ou da entrega de declaração de pobreza

por ele firmada, nos termos da Lei no 7.115, de 1983, ressalvadas hipóteses justificadas em que, devido ao volume ou ao estado dos documentos, a reprodução demande prazo superior.

Art. 19. Negado o pedido de acesso à informação, será enviada ao requerente, no prazo de resposta, comunicação com:

I - razões da negativa de acesso e seu fundamento legal;

II - possibilidade e prazo de recurso, com indicação da autoridade que o apreciará; e

III - possibilidade de apresentação de pedido de desclassificação da informação, quando for o caso, com indicação da autoridade classificadora que o apreciará.

§1o As razões de negativa de acesso a informação classificada indicarão o fundamento legal da classificação, a autoridade que a classificou e o código de indexação do documento classificado.

§ 2o Os órgãos e entidades disponibilizarão formulário padrão para apresentação de recurso e de pedido de desclassificação.

Art. 20. O acesso a documento preparatório ou informação nele contida, utilizados como fundamento de tomada de decisão ou de ato administrativo, será assegurado a partir da edição do ato ou decisão.

Parágrafo único. O Ministério da Fazenda e o Banco Central do Brasil classificarão os documentos que embasarem decisões de política econômica, tais como fiscal, tributária, monetária e regulatória.

Seção IV
Dos Recursos

Art. 21. No caso de negativa de acesso à informação ou de não fornecimento das razões da negativa do acesso, poderá o requerente apresentar recurso no prazo de dez dias, contado da ciência da decisão, à autoridade hierarquicamente superior à que adotou a decisão, que deverá apreciá-lo no prazo de cinco dias, contado da sua apresentação.

Parágrafo único. Desprovido o recurso de que trata o caput, poderá o requerente apresentar recurso no prazo de dez dias, contado da ciência da decisão, à autoridade máxima do órgão ou entidade, que deverá se manifestar em cinco dias contados do recebimento do recurso.

Art. 22. No caso de omissão de resposta ao pedido de acesso à informação, o requerente poderá apresentar reclamação no prazo de dez dias à autoridade de monitoramento de que trata o art. 40 da Lei no 12.527, de 2011, que deverá se manifestar no prazo de cinco dias, contado do recebimento da reclamação.

§ 1o O prazo para apresentar reclamação começará trinta dias após a apresentação do pedido.

§ 2o A autoridade máxima do órgão ou entidade poderá designar outra autoridade que lhe seja diretamente subordinada como responsável pelo recebimento e apreciação da reclamação.

Art. 23. Desprovido o recurso de que trata o parágrafo único do art. 21 ou infrutífera a reclamação de que trata o art. 22, poderá o requerente apresentar recurso no prazo de dez dias, contado da ciência da decisão, à Controladoria-Geral da União, que deverá se manifestar no prazo de cinco dias, contado do recebimento do recurso.

§ 1o A Controladoria-Geral da União poderá determinar que o órgão ou entidade preste esclarecimentos.

§ 2o Provido o recurso, a Controladoria-Geral da União fixará prazo para o cumprimento da decisão pelo órgão ou entidade.

Art. 24. No caso de negativa de acesso à informação, ou às razões da negativa do acesso de que trata o caput do art. 21, desprovido o recurso pela Controladoria-Geral da União, o requerente poderá apresentar, no prazo de dez dias, contado da ciência da decisão, recurso à Comissão Mista de Reavaliação de Informações, observados os procedimentos previstos no Capítulo VI.

CAPÍTULO V
DAS INFORMAÇÕES CLASSIFICADAS EM GRAU DE SIGILO

Seção I
Da Classificação de Informações quanto ao Grau e Prazos de Sigilo

Art. 25. São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam:

I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País;

III - prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

IV - pôr em risco a vida, a segurança ou a saúde da população;

V - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

VI - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

VII - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional, observado o disposto no inciso II do caput do art. 6o;

VIII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

IX - comprometer atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

Art. 26. A informação em poder dos órgãos e entidades, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada no grau ultrassecreto, secreto ou reservado.

Art. 27. Para a classificação da informação em grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I - a gravidade do risco ou dano à segurança da sociedade e do Estado; e

II - o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

Art. 28. Os prazos máximos de classificação são os seguintes:

I - grau ultrassecreto: vinte e cinco anos;

II - grau secreto: quinze anos; e

III - grau reservado: cinco anos.

Parágrafo único. Poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, observados os prazos máximos de classificação.

Art. 29. As informações que puderem colocar em risco a segurança do Presidente da República, Vice-Presidente e seus cônjuges e filhos serão classificadas no grau reservado e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

Art. 30. A classificação de informação é de competência:

I - no grau 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, da Aeronáutica; e

e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;

II - no grau secreto, das autoridades referidas no inciso I do caput, dos titulares de autarquias, fundações, empresas públicas e sociedades de economia mista; e

III - no grau reservado, das autoridades referidas nos incisos I e II do caput e das que exerçam funções de direção, comando ou chefia do Grupo-Direção e Assessoramento Superiores - DAS, nível DAS 101.5 ou superior, e seus equivalentes.

§ 1o É vedada a delegação da competência de classificação nos graus de sigilo ultrassecreto ou secreto.

§ 2o O dirigente máximo do órgão ou entidade poderá delegar a competência para classificação no grau reservado a agente público que exerça função de direção, comando ou chefia.

§ 3o É vedada a subdelegação da competência de que trata o § 2o.

§ 4o Os agentes públicos referidos no § 2o deverão dar ciência do ato de classificação à autoridade delegante, no prazo de noventa dias.

§ 5o A classificação de informação no grau ultrassecreto pelas autoridades previstas nas alíneas "d" e "e" do inciso I do caput deverá ser ratificada pelo Ministro de Estado, no prazo de trinta dias.

§ 6o Enquanto não ratificada, a classificação de que trata o § 5o considera-se válida, para todos os efeitos legais.

Seção II
Dos Procedimentos para Classificação de Informação

Art. 31. A decisão que classificar a informação em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo, e conterá o seguinte:

I - código de indexação de documento;

II - grau de sigilo;

III - categoria na qual se enquadra a informação;

IV - tipo de documento;

V - data da produção do documento;

VI - indicação de dispositivo legal que fundamenta a classificação;

VII - razões da classificação, observados os critérios estabelecidos no art. 27;

VIII - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 28;

IX - data da classificação; e

X - identificação da autoridade que classificou a informação.

§ 1o O TCI seguirá anexo à informação.

§ 2o As informações previstas no inciso VII do caput deverão ser mantidas no mesmo grau de sigilo que a informação classificada.

§ 3o A ratificação da classificação de que trata o § 5o do art. 30 deverá ser registrada no TCI.

Art. 32. A autoridade ou outro agente público que classificar informação no grau ultrassecreto ou secreto deverá encaminhar cópia do TCI à Comissão Mista de Reavaliação de Informações no prazo de trinta dias, contado da decisão de classificação ou de ratificação.

Art. 33. Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento tratamento do grau de sigilo mais elevado, ficando assegurado o acesso às partes não classificadas por meio de certidão, extrato ou cópia, com ocultação da parte sob sigilo.

Art. 34. Os órgãos e entidades poderão constituir Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS, com as seguintes atribuições:

I - opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;

II - assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo;

III - propor o destino final das informações desclassificadas, indicando os documentos para guarda permanente, observado o disposto na Lei no 8.159, de 8 de janeiro de 1991; e

IV - subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na Internet.

Seção III
Da Desclassificação e Reavaliação da Informação Classificada em Grau de Sigilo

Art. 35. A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.

Parágrafo único. Para o cumprimento do disposto no caput, além do disposto no art. 27, deverá ser observado:

I - o prazo máximo de restrição de acesso à informação, previsto no art. 28;

II - o prazo máximo de quatro anos para revisão de ofício das informações classificadas no grau ultrassecreto ou secreto, previsto no inciso I do caput do art. 47;

III - a permanência das razões da classificação;

IV - a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e

V - a peculiaridade das informações produzidas no exterior por autoridades ou agentes públicos.

Art. 36. O pedido de desclassificação ou de reavaliação da classificação poderá ser apresentado aos órgãos e entidades independente de existir prévio pedido de acesso à informação.

Parágrafo único. O pedido de que trata o caput será endereçado à autoridade classificadora, que decidirá no prazo de trinta dias.

Art. 37. Negado o pedido de desclassificação ou de reavaliação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contado da ciência da negativa, ao Ministro de Estado ou à autoridade com as mesmas prerrogativas, que decidirá no prazo de trinta dias.

§ 1o Nos casos em que a autoridade classificadora esteja vinculada a autarquia, fundação, empresa pública ou sociedade de economia mista, o recurso será apresentado ao dirigente máximo da entidade.

§ 2o No caso das Forças Armadas, o recurso será apresentado primeiramente perante o respectivo Comandante, e, em caso de negativa, ao Ministro de Estado da Defesa.

§ 3o No caso de informações produzidas por autoridades ou agentes públicos no exterior, o requerimento de desclassificação e reavaliação será apreciado pela autoridade hierarquicamente superior que estiver em território brasileiro.

§ 4o Desprovido o recurso de que tratam o caput e os §§1o a 3o, poderá o requerente apresentar recurso à Comissão Mista de Reavaliação de Informações, no prazo de dez dias, contado da ciência da decisão.

Art. 38. A decisão da desclassificação, reclassificação ou redução do prazo de sigilo de informações classificadas deverá constar das capas dos processos, se houver, e de campo apropriado no TCI.

Seção IV
Disposições Gerais

Art. 39. As informações classificadas no grau ultrassecreto ou secreto serão definitivamente preservadas, nos termos da Lei no 8.159, de 1991, observados os procedimentos de restrição de acesso enquanto vigorar o prazo da classificação.

Art. 40. As informações classificadas como documentos de guarda permanente que forem objeto de desclassificação serão encaminhadas ao Arquivo Nacional, ao arquivo permanente do órgão público, da entidade pública ou da instituição de caráter público, para fins de organização, preservação e acesso.

Art. 41. As informações sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de classificação em qualquer grau de sigilo nem ter seu acesso negado.

Art. 42. Não poderá ser negado acesso às informações necessárias à tutela judicial ou administrativa de direitos fundamentais.

Parágrafo único. O requerente deverá apresentar razões que demonstrem a existência de nexo entre as informações requeridas e o direito que se pretende proteger.

Art. 43. 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 sejam credenciadas segundo as normas fixadas pelo Núcleo de Segurança e Credenciamento, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, sem prejuízo das atribuições de agentes públicos autorizados por lei.

Art. 44. As autoridades do Poder Executivo federal adotarão as providências necessárias para que o pessoal a elas subordinado conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações classificadas em qualquer grau de sigilo.

Parágrafo único. A pessoa natural ou entidade privada que, em razão de qualquer vínculo com o Poder Público, executar atividades de tratamento de informações classificadas, adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações.

Art. 45. A autoridade máxima de cada órgão ou entidade publicará anualmente, até o dia 1° de junho, em sítio na Internet:

I - rol das informações desclassificadas nos últimos doze meses;

II - rol das informações classificadas em cada grau de sigilo, que deverá conter:

a) código de indexação de documento;

b) categoria na qual se enquadra a informação;

c) indicação de dispositivo legal que fundamenta a classificação; e

d) data da produção, data da classificação e prazo da classificação;

III - relatório estatístico com a quantidade de pedidos de acesso à informação recebidos, atendidos e indeferidos; e

IV - informações estatísticas agregadas dos requerentes.

Parágrafo único. Os órgãos e entidades deverão manter em meio físico as informações previstas no caput, para consulta pública em suas sedes.

CAPÍTULO VI
DA COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES CLASSIFICADAS

Art. 46. A Comissão Mista de Reavaliação de Informações, instituída nos termos do § 1o do art. 35 da Lei no 12.527, de 2011, será integrada pelos titulares dos seguintes órgãos:

I - Casa Civil da Presidência da República, que a presidirá;

II - Ministério da Justiça;

III - Ministério das Relações Exteriores;

IV - Ministério da Defesa;

V - Ministério da Fazenda;

VI - Ministério do Planejamento, Orçamento e Gestão;

VII - Secretaria de Direitos Humanos da Presidência da República;

VIII - Gabinete de Segurança Institucional da Presidência da República;

IX - Advocacia-Geral da União; e

X - Controladoria Geral da União.

Parágrafo único. Cada integrante indicará suplente a ser designado por ato do Presidente da Comissão.

Art. 47. Compete à Comissão Mista de Reavaliação de Informações:

I - rever, de ofício ou mediante provocação, a classificação de informação no grau ultrassecreto ou secreto ou sua reavaliação, no máximo a cada quatro anos;

II - requisitar da autoridade que classificar informação no grau ultrassecreto ou secreto esclarecimento ou conteúdo, parcial ou integral, da informação, quando as informações constantes do TCI não forem suficientes para a revisão da classificação;

III - decidir recursos apresentados contra decisão proferida:

a) pela Controladoria-Geral da União, em grau recursal, pedido de acesso à informação ou de abertura de base de dados, ou às razões da negativa de acesso à informação ou de abertura de base de dados; ou (Redação dada pelo Decreto nº 8.777, de 2016)

b) pelo Ministro de Estado ou autoridade com a mesma prerrogativa, em grau recursal, a pedido de desclassificação ou reavaliação de informação classificada;

IV - prorrogar por uma única vez, e por período determinado não superior a vinte e cinco anos, o prazo de sigilo de informação classificada no grau ultrassecreto, enquanto seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional, à integridade do território nacional ou grave risco às relações internacionais do País, limitado ao máximo de cinquenta anos o prazo total da classificação; e

V - estabelecer orientações normativas de caráter geral a fim de suprir eventuais lacunas na aplicação da Lei no 12.527, de 2011.

Parágrafo único. A não deliberação sobre a revisão de ofício no prazo previsto no inciso I do caput implicará a desclassificação automática das informações.

Art. 48. A Comissão Mista de Reavaliação de Informações se reunirá, ordinariamente, uma vez por mês, e, extraordinariamente, sempre que convocada por seu Presidente.

Parágrafo único. As reuniões serão realizadas com a presença de no mínimo seis integrantes.

Art. 49. Os requerimentos de prorrogação do prazo de classificação de informação no grau ultrassecreto, a que se refere o inciso IV do caput do art. 47, deverão ser encaminhados à Comissão Mista de Reavaliação de Informações em até um ano antes do vencimento do termo final de restrição de acesso.

Parágrafo único. O requerimento de prorrogação do prazo de sigilo de informação classificada no grau ultrassecreto deverá ser apreciado, impreterivelmente, em até três sessões subsequentes à data de sua autuação, ficando sobrestadas, até que se ultime a votação, todas as demais deliberações da Comissão.

Art. 50. A Comissão Mista de Reavaliação de Informações deverá apreciar os recursos previstos no inciso III do caput do art. 47, impreterivelmente, até a terceira reunião ordinária subsequente à data de sua autuação.

Art. 51. A revisão de ofício da informação classificada no grau ultrassecreto ou secreto será apreciada em até três sessões anteriores à data de sua desclassificação automática.

Art. 52. As deliberações da Comissão Mista de Reavaliação de Informações serão tomadas:

I - por maioria absoluta, quando envolverem as competências previstas nos incisos I e IV do caput do art.47; e

II - por maioria simples dos votos, nos demais casos.

Parágrafo único. A Casa Civil da Presidência da República poderá exercer, além do voto ordinário, o voto de qualidade para desempate.

Art. 53. A Casa Civil da Presidência da República exercerá as funções de Secretaria-Executiva da Comissão Mista de Reavaliação de Informações, cujas competências serão definidas em regimento interno.

Art. 54. A Comissão Mista de Reavaliação de Informações aprovará, por maioria absoluta, regimento interno que disporá sobre sua organização e funcionamento.

Parágrafo único. O regimento interno deverá ser publicado no Diário Oficial da União no prazo de noventa dias após a instalação da Comissão.

CAPÍTULO VII
DAS INFORMAÇÕES PESSOAIS

Art. 55. As informações pessoais relativas à intimidade, vida privada, honra e imagem detidas pelos órgãos e entidades:

I - terão acesso restrito a agentes públicos legalmente autorizados e a pessoa a que se referirem, independentemente de classificação de sigilo, pelo prazo máximo de cem anos a contar da data de sua produção; e

II - poderão ter sua divulgação ou acesso por terceiros autorizados por previsão legal ou consentimento expresso da pessoa a que se referirem.

Parágrafo único. Caso o titular das informações pessoais esteja morto ou ausente, os direitos de que trata este artigo assistem ao cônjuge ou companheiro, aos descendentes ou ascendentes, conforme o disposto no parágrafo único do art. 20 da Lei no 10.406, de 10 de janeiro de 2002, e na Lei no 9.278, de 10 de maio de 1996.

Art. 56. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

Art. 57. O consentimento referido no inciso II do caput do art. 55 não será exigido quando o acesso à informação pessoal for necessário:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, vedada a identificação da pessoa a que a informação se referir;

III - ao cumprimento de decisão judicial;

IV - à defesa de direitos humanos de terceiros; ou

V - à proteção do interesse público geral e preponderante.

Art. 58. A restrição de acesso a informações pessoais de que trata o art. 55 não poderá ser invocada:

I - com o intuito de prejudicar processo de apuração de irregularidades, conduzido pelo Poder Público, em que o titular das informações for parte ou interessado; ou

II - quando as informações pessoais não classificadas estiverem contidas em conjuntos de documentos necessários à recuperação de fatos históricos de maior relevância.

Art. 59. O dirigente máximo do órgão ou entidade poderá, de ofício ou mediante provocação, reconhecer a incidência da hipótese do inciso II do caput do art. 58, de forma fundamentada, sobre documentos que tenha produzido ou acumulado, e que estejam sob sua guarda.

§ 1o Para subsidiar a decisão de reconhecimento de que trata o caput, o órgão ou entidade poderá solicitar a universidades, instituições de pesquisa ou outras entidades com notória experiência em pesquisa historiográfica a emissão de parecer sobre a questão.

§ 2o A decisão de reconhecimento de que trata o caput será precedida de publicação de extrato da informação, com descrição resumida do assunto, origem e período do conjunto de documentos a serem considerados de acesso irrestrito, com antecedência de no mínimo trinta dias.

§ 3o Após a decisão de reconhecimento de que trata o § 2o, os documentos serão considerados de acesso irrestrito ao público.

§ 4o Na hipótese de documentos de elevado valor histórico destinados à guarda permanente, caberá ao dirigente máximo do Arquivo Nacional, ou à autoridade responsável pelo arquivo do órgão ou entidade pública que os receber, decidir, após seu recolhimento, sobre o reconhecimento, observado o procedimento previsto neste artigo.

Art. 60. O pedido de acesso a informações pessoais observará os procedimentos previstos no Capítulo IV e estará condicionado à comprovação da identidade do requerente.

Parágrafo único. O pedido de acesso a informações pessoais por terceiros deverá ainda estar acompanhado de:

I - comprovação do consentimento expresso de que trata o inciso II do caput do art. 55, por meio de procuração;

II - comprovação das hipóteses previstas no art. 58;

III - demonstração do interesse pela recuperação de fatos históricos de maior relevância, observados os procedimentos previstos no art. 59; ou

IV - demonstração da necessidade do acesso à informação requerida para a defesa dos direitos humanos ou para a proteção do interesse público e geral preponderante.

Art. 61. O acesso à informação pessoal por terceiros será condicionado à assinatura de um termo de responsabilidade, que disporá sobre a finalidade e a destinação que fundamentaram sua autorização, sobre as obrigações a que se submeterá o requerente.

§ 1o A utilização de informação pessoal por terceiros vincula-se à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa.

§ 2o Aquele que obtiver acesso às informações pessoais de terceiros será responsabilizado por seu uso indevido, na forma da lei.

Art. 62. Aplica-se, no que couber, a Lei no 9.507, de 12 de novembro de 1997, em relação à informação de pessoa, natural ou jurídica, constante de registro ou banco de dados de órgãos ou entidades governamentais ou de caráter público.

CAPÍTULO VIII
DAS ENTIDADES PRIVADAS SEM FINS LUCRATIVOS

Art. 63. As entidades privadas sem fins lucrativos que receberem recursos públicos para realização de ações de interesse público deverão dar publicidade às seguintes informações:

I - cópia do estatuto social atualizado da entidade;

II - relação nominal atualizada dos dirigentes da entidade; e

III - cópia integral dos convênios, contratos, termos de parcerias, acordos, ajustes ou instrumentos congêneres realizados com o Poder Executivo federal, respectivos aditivos, e relatórios finais de prestação de contas, na forma da legislação aplicável.

§ 1o As informações de que trata o caput serão divulgadas em sítio na Internet da entidade privada e em quadro de avisos de amplo acesso público em sua sede.

§ 2o A divulgação em sítio na Internet referida no §1o poderá ser dispensada, por decisão do órgão ou entidade pública, e mediante expressa justificação da entidade, nos casos de entidades privadas sem fins lucrativos que não disponham de meios para realizá-la.

§ 3o As informações de que trata o caput deverão ser publicadas a partir da celebração do convênio, contrato, termo de parceria, acordo, ajuste ou instrumento congênere, serão atualizadas periodicamente e ficarão disponíveis até cento e oitenta dias após a entrega da prestação de contas final.

Art. 64. Os pedidos de informação referentes aos convênios, contratos, termos de parcerias, acordos, ajustes ou instrumentos congêneres previstos no art. 63 deverão ser apresentados diretamente aos órgãos e entidades responsáveis pelo repasse de recursos.

CAPÍTULO IX
DAS RESPONSABILIDADES

Art. 65. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:

I - recusar-se a fornecer informação requerida nos termos deste Decreto, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

II - utilizar indevidamente, subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda, a que tenha acesso ou sobre que tenha conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

III - agir com dolo ou má-fé na análise dos pedidos de acesso à informação;

IV - divulgar, permitir a divulgação, acessar ou permitir acesso indevido a informação classificada em grau de sigilo ou a informação pessoal;

V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;

VI - ocultar da revisão de autoridade superior competente informação classificada em grau de sigilo para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e

VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

§ 1o Atendido o princípio do contraditório, da ampla defesa e do devido processo legal, as condutas descritas no caput serão consideradas:

I - para fins dos regulamentos disciplinares das Forças Armadas, transgressões militares médias ou graves, segundo os critérios neles estabelecidos, desde que não tipificadas em lei como crime ou contravenção penal; ou

II - para fins do disposto na Lei no 8.112, de 11 de dezembro de 1990, infrações administrativas, que deverão ser apenadas, no mínimo, com suspensão, segundo os critérios estabelecidos na referida lei.

§ 2o Pelas condutas descritas no caput, poderá o militar ou agente público responder, também, por improbidade administrativa, conforme o disposto nas Leis no 1.079, de 10 de abril de 1950, e no 8.429, de 2 de junho de 1992.

Art. 66. A pessoa natural ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o Poder Público e praticar conduta prevista no art. 65, estará sujeita às seguintes sanções:

I - advertência;

II - multa;

III - rescisão do vínculo com o Poder Público;

IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a dois anos; e

V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade.

§ 1o A sanção de multa poderá ser aplicada juntamente com as sanções previstas nos incisos I, III e IV do caput.

§ 2o A multa prevista no inciso II do caput será aplicada sem prejuízo da reparação pelos danos e não poderá ser:

I - inferior a R$ 1.000,00 (mil reais) nem superior a R$ 200.000,00 (duzentos mil reais), no caso de pessoa natural; ou

II - inferior a R$ 5.000,00 (cinco mil reais) nem superior a R$ 600.000,00 (seiscentos mil reais), no caso de entidade privada.

§ 3o A reabilitação referida no inciso V do caput será autorizada somente quando a pessoa natural ou entidade privada efetivar o ressarcimento ao órgão ou entidade dos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base no inciso IV do caput.

§ 4o A aplicação da sanção prevista no inciso V do caput é de competência exclusiva da autoridade máxima do órgão ou entidade pública.

§ 5o O prazo para apresentação de defesa nas hipóteses previstas neste artigo é de dez dias, contado da ciência do ato.

CAPÍTULO X
DO MONITORAMENTO DA APLICAÇÃO DA LEI

Seção I
Da Autoridade de Monitoramento

Art. 67. O dirigente máximo de cada órgão ou entidade designará autoridade que lhe seja diretamente subordinada para exercer as seguintes atribuições:

I - assegurar o cumprimento das normas relativas ao acesso à informação, de forma eficiente e adequada aos objetivos da Lei no 12.527, de 2011;

II - avaliar e monitorar a implementação do disposto neste Decreto e apresentar ao dirigente máximo de cada órgão ou entidade relatório anual sobre o seu cumprimento, encaminhando-o à Controladoria-Geral da União;

III - recomendar medidas para aperfeiçoar as normas e procedimentos necessários à implementação deste Decreto;

IV - orientar as unidades no que se refere ao cumprimento deste Decreto; e

V - manifestar-se sobre reclamação apresentada contra omissão de autoridade competente, observado o disposto no art. 22.

Seção II
Das Competências Relativas ao Monitoramento

Art. 68. Compete à Controladoria-Geral da União, observadas as competências dos demais órgãos e entidades e as previsões específicas neste Decreto:

I - definir o formulário padrão, disponibilizado em meio físico e eletrônico, que estará à disposição no sítio na Internet e no SIC dos órgãos e entidades, de acordo com o § 1o do art. 11;

II - promover campanha de abrangência nacional de fomento à cultura da transparência na administração pública e conscientização sobre o direito fundamental de acesso à informação;

III - promover o treinamento dos agentes públicos e, no que couber, a capacitação das entidades privadas sem fins lucrativos, no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública;

IV - monitorar a implementação da Lei no 12.527, de 2011, concentrando e consolidando a publicação de informações estatísticas relacionadas no art. 45;

V - preparar relatório anual com informações referentes à implementação da Lei no 12.527, de 2011, a ser encaminhado ao Congresso Nacional;

VI - monitorar a aplicação deste Decreto, especialmente o cumprimento dos prazos e procedimentos; e

VII - definir, em conjunto com a Casa Civil da Presidência da República, diretrizes e procedimentos complementares necessários à implementação da Lei no12.527, de 2011.

Art. 69. Compete à Controladoria-Geral da União e ao Ministério do Planejamento, Orçamento e Gestão, observadas as competências dos demais órgãos e entidades e as previsões específicas neste Decreto, por meio de ato conjunto:

I - estabelecer procedimentos, regras e padrões de divulgação de informações ao público, fixando prazo máximo para atualização; e

II - detalhar os procedimentos necessários à busca, estruturação e prestação de informações no âmbito do SIC.

Art. 70. Compete ao Gabinete de Segurança Institucional da Presidência da República, observadas as competências dos demais órgãos e entidades e as previsões específicas neste Decreto:

I - estabelecer regras de indexação relacionadas à classificação de informação;

II - expedir atos complementares e estabelecer procedimentos relativos ao credenciamento de segurança de pessoas, órgãos e entidades públicos ou privados, para o tratamento de informações classificadas; e

III - promover, por meio do Núcleo de Credenciamento de Segurança, o credenciamento de segurança de pessoas, órgãos e entidades públicos ou privados, para o tratamento de informações classificadas.

CAPÍTULO XI
DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 71. Os órgãos e entidades adequarão suas políticas de gestão da informação, promovendo os ajustes necessários aos processos de registro, processamento, trâmite e arquivamento de documentos e informações.

Art. 72. Os órgãos e entidades deverão reavaliar as informações classificadas no grau ultrassecreto e secreto no prazo máximo de dois anos, contado do termo inicial de vigência da Lei no 12.527, de 2011.

§ 1o A restrição de acesso a informações, em razão da reavaliação prevista no caput, deverá observar os prazos e condições previstos neste Decreto.

§ 2o Enquanto não transcorrido o prazo de reavaliação previsto no caput, será mantida a classificação da informação, observados os prazos e disposições da legislação precedente.

§ 3o As informações classificadas no grau ultrassecreto e secreto não reavaliadas no prazo previsto no caput serão consideradas, automaticamente, desclassificadas.

Art. 73. A publicação anual de que trata o art. 45 terá inicio em junho de 2013.

Art. 74. O tratamento de informação classificada resultante de tratados, acordos ou atos internacionais atenderá às normas e recomendações desses instrumentos.

Art. 75. Aplica-se subsidiariamente a Lei no 9.784, de 29 de janeiro de 1999, aos procedimentos previstos neste Decreto.

Art. 76. Este Decreto entra em vigor em 16 de maio de 2012.

Brasília, 16 de maio de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Celso Luiz Nunes Amorim
Antonio de Aguiar Patriota
Guido Mantega
Miriam Belchior
Paulo Bernardo Silva
Marco Antonio Raupp
Alexandre Antonio Tombini
Gleisi Hoffmann
Gilberto Carvalho
José Elito Carvalho Siqueira
Helena Chagas
Luis Inácio Lucena Adams
Jorge Hage Sobrinho
Maria do Rosário Nunes

ANEXO
GRAU DE SIGILO:
(idêntico ao grau de sigilo do documento)

<table>
<tr><td colspan="3">TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO</td></tr>
<tr><td colspan="3">ÓRGÃO/ENTIDADE:</td></tr>
<tr><td colspan="3">CÓDIGO DE INDEXAÇÃO:</td></tr>
<tr><td colspan="3">GRAU DE SIGILO:</td></tr>
<tr><td colspan="3">CATEGORIA:</td></tr>
<tr><td colspan="3">TIPO DE DOCUMENTO:</td></tr>
<tr><td colspan="3">DATA DE PRODUÇÃO:</td></tr>
<tr><td colspan="3">FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO:</td></tr>
<tr><td colspan="3">RAZÕES PARA A CLASSIFICAÇÃO:
(idêntico ao grau de sigilo do documento)</td></tr>
<tr><td colspan="3">PRAZO DA RESTRIÇÃO DE ACESSO:</td></tr>
<tr><td colspan="3">DATA DE CLASSIFICAÇÃO:</td></tr>
<tr><td colspan="2">AUTORIDADE CLASSIFICADORA</td><td>Nome:
Cargo:</td></tr>
<tr><td colspan="2">AUTORIDADE RATIFICADORA
(quando aplicável)</td><td>Nome:
Cargo:</td></tr>
<tr><td></td><td>DESCLASSIFICAÇÃO em ____/____/_____
(quando aplicável)</td><td>Nome:
Cargo:</td></tr>
<tr><td></td><td>RECLASSIFICAÇÃO em ____/____/_____
(quando aplicável)</td><td>Nome:
Cargo:</td></tr>
<tr><td></td><td>REDUÇÃO DE PRAZO em ____/____/_____
(quando aplicável)</td><td>Nome:
Cargo:</td></tr>
<tr><td></td><td>PRORROGAÇÃO DE PRAZO em __/ ___/____
(quando aplicável)</td><td>Nome:
Cargo:</td></tr>
<tr><td colspan="3">_____
ASSINATURA DA AUTORIDADE CLASSIFICADORA</td></tr>
</table>

_____

ASSINATURA DA AUTORIDADE RATIFICADORA (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO (quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO
(quando aplicável)

_____

ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO
(quando aplicável)

DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012

Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

A PRESIDENTA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, caput, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto nos arts. 25, 27, 29, 35, § 5o, e 37 da Lei no 12.527, de 18 de novembro de 2011,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1o Este Decreto regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento, conforme o disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011.

Art. 2o Para os efeitos deste Decreto, considera-se:

I - algoritmo de Estado - função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal;

II - cifração - ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

III - código de indexação - código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo;

IV - comprometimento - perda de segurança resultante do acesso não autorizado;

V - contrato sigiloso - ajuste, convênio ou termo de cooperação cujo objeto ou execução implique tratamento de informação classificada;

VI - credencial de segurança - certificado que autoriza pessoa para o tratamento de informação classificada;

VII - credenciamento de segurança - processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada;

VIII - decifração - ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

IX - dispositivos móveis - equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;

X - gestor de segurança e credenciamento - responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle;

XI - marcação - aposição de marca que indica o grau de sigilo da informação classificada;

XII - medidas de segurança - medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XIII - órgão de registro nível 1 - ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;

XIV - órgão de registro nível 2 - órgão ou entidade pública vinculada a órgão de registro nível 1 e por este habilitado;

XV - posto de controle - unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

XVI - quebra de segurança - ação ou omissão que implica comprometimento ou risco de comprometimento de informação classificada em qualquer grau de sigilo;

XVII - recurso criptográfico - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração; e

XVIII - 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.

CAPÍTULO II
DO CREDENCIAMENTO DE SEGURANÇA

Seção I
Dos Órgãos

Art. 3o 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 no 12.527, de 2011:

I - habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada;

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 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 docaput; e

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

Art. 4o Fica criado o Comitê Gestor de Credenciamento de Segurança, integrado por representantes, titular e suplente, dos seguintes órgãos:

I - 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.

§ 1o Os membros titulares e suplentes serão indicados pelos dirigentes máximos dos órgãos representados, e designados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.

§ 2o A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

§ 3o Poderão ser convidados para as reuniões do Comitê representantes de órgãos e entidades públicas e privadas, ou especialistas, para emitir pareceres e fornecer informações.

Art. 5o Compete ao Comitê Gestor de Credenciamento de Segurança:

I - propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada;

II - definir parâmetros e requisitos mínimos para:

a) qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos dos arts. 10 e 11; e

b) concessão de credencial de segurança para pessoas, nos termos do art. 12; e

III - avaliar periodicamente o cumprimento do disposto neste Decreto.

Art. 6o Compete ao Gabinete de Segurança Institucional da Presidência da República:

I - expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada;

II - participar de negociações de tratados, acordos ou atos internacionais relacionados com o tratamento de informação classificada, em articulação com o Ministério das Relações Exteriores;

III - acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança;

IV - informar sobre eventuais danos referidos no inciso III do caput ao país ou à organização internacional de origem, sempre que necessário, pela via diplomática; e

V - assessorar o Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada, inclusive no que se refere a tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores.

Parágrafo único. O Gabinete de Segurança Institucional da Presidência da República exercerá as funções de autoridade nacional de segurança para tratamento de informação classificada decorrente de tratados, acordos ou atos internacionais.

Art. 7o 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 que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada;

IV- realizar 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.

Art. 8o Compete ao órgão de registro nível 2 realizar investigação e credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada.

Parágrafo único. A competência para realização de inspeção e investigação de que trata o inciso IV do caput do art. 7o poderá ser delegada a órgão de registro nível 2.

Art. 9o Compete ao posto de controle:

I - realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza; e

II - garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.

Seção II
Dos procedimentos

Art. 10. A habilitação dos órgãos e entidades públicas para o credenciamento de segurança fica condicionada aos seguintes requisitos:

I - comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo; e

II - designação de gestor de segurança e credenciamento, e de seu substituto.

Art. 11. A concessão de habilitação de entidade privada como posto de controle fica condicionada aos seguintes requisitos:

I - regularidade fiscal;

II - comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo;

III - expectativa de assinatura de contrato sigiloso;

IV - designação de gestor de segurança e credenciamento, e de seu substituto; e

V - aprovação em inspeção para habilitação de segurança.

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.

Art. 13. A habilitação para credenciamento de segurança e a concessão de credencial de segurança resultarão da análise objetiva dos requisitos previstos neste Decreto.

Art. 14. Os órgãos de registro nível 1 e nível 2 poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados, para:

I - credenciamento de segurança e tratamento de informação classificada; e

II - realização de inspeção e investigação para credenciamento de segurança.

Art. 15. Cada órgão de registro terá no mínimo um posto de controle, habilitado.

Art. 16. 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.

CAPÍTULO III
DO TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Seção I
Disposições Gerais

Art. 17. Os órgãos e entidades adotarão providências para que os agentes públicos conheçam as normas e observem os procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Parágrafo único. O disposto no caput se aplica à pessoa ou entidade privada que, em razão de qualquer vínculo com o Poder Público, execute atividade de credenciamento de segurança ou de tratamento de informação classificada.

Art. 18. O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas na forma deste Decreto, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, constante do Anexo I, 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. 19. A decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo observará os procedimentos previstos nos arts. 31 e 32 do Decreto no 7.724 de 16 de maio de 2012, e deverá ser formalizada em decisão consubstanciada em Termo de Classificação de Informação.

Art. 20. A publicação de atos normativos relativos a informação classificada em qualquer grau de sigilo ou protegida por sigilo legal ou judicial poderá limitar-se, quando necessário, aos seus respectivos números, datas de expedição e ementas, redigidos de modo a não comprometer o sigilo.

Seção II
Do Documento Controlado

Art. 21. Para o tratamento de documento com informação classificada em qualquer grau de sigilo ou prevista na legislação como sigilosa o órgão ou entidade poderá adotar os seguintes procedimentos adicionais de controle:

I - identificação dos destinatários em protocolo e recibo específicos;

II - lavratura de termo de custódia e registro em protocolo específico;

III - lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e

IV - lavratura de termo de transferência de custódia ou guarda.

§ 1o O documento previsto no caput será denominado Documento Controlado - DC.

§ 2o O termo de inventário previsto no inciso III do caput deverá conter no mínimo os seguintes elementos:

I - numeração sequencial e data;

II - órgãos produtor e custodiante do DC;

III - rol de documentos controlados; e

IV - local e assinatura.

§ 3o O termo de transferência previsto no inciso IV do caput deverá conter no mínimo os seguintes elementos:

I – numeração sequencial e data;

II - agentes públicos substituto e substituído;

III - identificação dos documentos ou termos de inventário a serem transferidos; e

IV - local e assinatura.

Art. 22. O documento ultrassecreto é considerado DC desde sua classificação ou reclassificação.

Seção III
Da Marcação

Art. 23. A marcação será feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento.

§ 1o As páginas serão numeradas seguidamente, devendo cada uma conter indicação do total de páginas que compõe o documento.

§ 2o A marcação deverá ser feita de modo a não prejudicar a compreensão da informação.

Art. 24. O DC possuirá a marcação de que trata o art. 23 e conterá, na capa e em todas as páginas, a expressão em diagonal "Documento Controlado (DC)" e o número de controle, que indicará o agente público custodiante.

Art. 25. A indicação do grau de sigilo em mapas, fotocartas, cartas, fotografias, quaisquer outros tipos de imagens e meios eletrônicos de armazenamento obedecerá aos procedimentos complementares adotados pelos órgãos e entidades.

Seção IV
Da Expedição, Tramitação e Comunicação

Art. 26. A expedição e a tramitação de documentos classificados deverão observar os seguintes procedimentos:

I - serão acondicionados em envelopes duplos;

II - no envelope externo não constará indicação do grau de sigilo ou do teor do documento;

III - no envelope interno constarão o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo;

IV - o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará remetente, destinatário e número ou outro indicativo que identifique o documento; e

V - será inscrita a palavra "PESSOAL" no envelope que contiver documento de interesse exclusivo do destinatário.

Art. 27. A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem.

Art. 28. A expedição de documento com informação classificada em grau de sigilo secreto ou reservado será feita pelos meios de comunicação disponíveis, com recursos de criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

Art. 29. Cabe aos responsáveis pelo recebimento do documento com informação classificada em qualquer grau de sigilo, independente do meio e formato:

I - registrar o recebimento do documento;

II - verificar a integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e

III - informar ao remetente o recebimento da informação, no prazo mais curto possível.

§ 1o Caso a tramitação ocorra por expediente ou correspondência, o envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.

§ 2o Envelopes internos contendo a marca "PESSOAL" somente poderão ser abertos pelo destinatário.

Art. 30. A informação classificada em qualquer grau de sigilo será mantida ou arquivada em condições especiais de segurança.

§ 1o Para manutenção e arquivamento de informação classificada no grau de sigilo ultrassecreto e secreto é obrigatório o uso de equipamento, ambiente ou estrutura que ofereça segurança compatível com o grau de sigilo.

§ 2o Para armazenamento em meio eletrônico de documento com informação classificada em qualquer grau de sigilo é obrigatória a utilização de sistemas de tecnologia da informação atualizados de forma a prevenir ameaças de quebra de segurança, observado o disposto no art. 38.

§ 3o As mídias para armazenamento poderão estar integradas a equipamentos conectados à internet, desde que por canal seguro e com níveis de controle de acesso adequados ao tratamento da informação classificada, admitindo-se também a conexão a redes de computadores internas, desde que seguras e controladas.

Art. 31. Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao grau de sigilo.

Art. 32. Os agentes responsáveis pela guarda ou custódia de documento controlado o transmitirá a seus substitutos, devidamente conferido, quando da passagem ou transferência de responsabilidade.

Parágrafo único. Aplica-se o disposto neste artigo aos responsáveis pela guarda ou custódia de material de acesso restrito.

Seção V
Da Reprodução

Art. 33. A reprodução do todo ou de parte de documento com informação classificada em qualquer grau de sigilo terá o mesmo grau de sigilo do documento.

§ 1º A reprodução total ou parcial de informação classificada em qualquer grau de sigilo condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

§ 2o As cópias serão autenticadas pela autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

Art. 34. Caso a preparação, impressão ou reprodução de informação classificada em qualquer grau de sigilo for efetuada em tipografia, impressora, oficina gráfica ou similar, essa operação será acompanhada por pessoa oficialmente designada, responsável pela garantia do sigilo durante a confecção do documento.

Seção VI
Da Preservação e da Guarda

Art. 35. A avaliação e a seleção de documento com informação desclassificada, para fins de guarda permanente ou eliminação, observarão o disposto na Lei no 8.159, de 8 de janeiro de 1991, e no Decreto no 4.073, de 3 de janeiro de 2002.

Art. 36. O documento de guarda permanente que contiver informação classificada em qualquer grau de sigilo será encaminhado, em caso de desclassificação, ao Arquivo Nacional ou ao arquivo permanente do órgão público, da entidade pública ou da instituição de caráter público, para fins de organização, preservação e acesso.

Art. 37. O documento de guarda permanente não pode ser desfigurado ou destruído, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

Seção VII
Dos Sistemas de Informação

Art. 38. No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo federal.

§ 1o A transmissão de informação classificada em qualquer grau de sigilo por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

§ 2º A autenticidade da identidade do usuário da rede deverá ser garantida, no mínimo, pelo uso de certificado digital.

§ 3º Os sistemas de informação de que trata o caput deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo.

§ 4o Os sistemas de informação de que trata o caput deverão manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

Art. 39. Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam física ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

Art. 40. A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

Parágrafo único. Compete ao Gabinete de Segurança Institucional da Presidência da República estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação previsto no art. 6o do Decreto no 3.505, de 13 de junho de 2000.

Art. 41. Os procedimentos de tratamento de informação classificada em qualquer grau de sigilo aplicam-se aos recursos criptográficos, atendidas as seguintes exigências:

I - realização de vistorias periódicas, com a finalidade de assegurar a execução das operações criptográficas;

II - manutenção de inventários completos e atualizados do material de criptografia existente;

III - designação de sistemas criptográficos adequados a cada destinatário;

IV - comunicação, ao superior hierárquico ou à autoridade competente, de anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de informações criptografadas; e

V - identificação de indícios de violação, de interceptação ou de irregularidades na transmissão ou recebimento de informações criptografadas.

Seção VIII
Das Áreas, Instalações e Materiais

Art. 42. 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.

Art. 43. Os órgãos e entidades públicas adotarão medidas para definição, demarcação, sinalização, segurança e autorização de acesso às áreas restritas sob sua responsabilidade.

Parágrafo único. As visitas a áreas ou instalações de acesso restrito serão disciplinadas pelo órgão ou entidade responsável pela sua segurança.

Art. 44. Os materiais que, por sua utilização ou finalidade, demandarem proteção, terão acesso restrito às pessoas autorizadas pelo órgão ou entidade.

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

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

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

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

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

V - recursos criptográficos; e

VI - explosivos, líquidos e gases.

Art. 46. Os órgãos ou entidades públicas encarregadas da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto, prova, produção, aquisição, armazenagem ou emprego de material de acesso restrito expedirão instruções adicionais necessárias à salvaguarda dos assuntos a eles relacionados.

Art. 47. O meio de transporte utilizado para deslocamento de material de acesso restrito é de responsabilidade do custodiante e deverá considerar o grau de sigilo das informações.

§ 1º O material de acesso restrito poderá ser transportado por empresas contratadas, adotadas as medidas necessárias à manutenção do sigilo das informações.

§ 2º As medidas necessárias para a segurança do material transportado serão prévia e explicitamente estabelecidas em contrato.

Seção IX
Da Celebração de Contratos Sigilosos

Art. 48. A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura de TCMS e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

I - obrigação de manter sigilo relativo ao objeto e a sua execução;

II - possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

III - obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

IV - identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

V - obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

VI - responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

Art. 49. Aos órgãos e entidades públicas com que os contratantes mantêm vínculo de qualquer natureza caberá adotar procedimentos de segurança da informação classificada em qualquer grau de sigilo ou do material de acesso restrito em poder dos contratados ou subcontratados.

CAPÍTULO IV
DA INDEXAÇÃO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

Art. 50. A informação classificada em qualquer grau de sigilo ou o documento que a contenha receberá o Código de Indexação de Documento que contém Informação Classificada - CIDIC.

Parágrafo único. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada, e será estruturado em duas partes.

Art. 51. A primeira parte do CIDIC será composta pelo Número Único de Protocolo -NUP, originalmente cadastrado conforme legislação de gestão documental.

§ 1o A informação classificada em qualquer grau de sigilo ou o documento que a contenha, quando de sua desclassificação, manterá apenas o NUP.

§ 2o Não serão usadas tabelas de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso à informação classificada em qualquer grau de sigilo, sob pena de pôr em risco sua proteção e confidencialidade.

Art. 52. A segunda parte do CIDIC será composta dos seguintes elementos:

I - grau de sigilo: indicação do grau de sigilo, ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível;

II - categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme Anexo II;

III - data de produção da informação classificada: registro da data de produção da informação classificada, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

IV - data de desclassificação da informação classificada em qualquer grau de sigilo: registro da potencial data de desclassificação da informação classificada, efetuado no ato da classificação, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

V - indicação de reclassificação: indicação de ocorrência ou não, S (sim) ou N (não), de reclassificação da informação classificada, respectivamente, conforme as seguintes situações:

a) reclassificação da informação resultante de reavaliação; ou

b) primeiro registro da classificação; e

VI - indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.

Art. 53. Para fins de gestão documental, deverá ser guardado o histórico das alterações do CIDIC.

CAPÍTULO V
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 54. A implementação do CIDIC deverá ser consolidada até 1o de junho de 2013.

Parágrafo único. Enquanto não implementado o CIDIC, o Termo de Classificação de Informação será preenchido com o NUP.

Art. 55. O documento com informação classificada em qualquer grau de sigilo, produzido antes da vigência da Lei no 12.527, de 2011, receberá o CIDIC para fins do disposto no art. 45 do Decreto nº 7.724, de 16 de maio de 2012.

Art. 56. Os órgãos e entidades deverão adotar os recursos criptográficos baseados em algoritmo de Estado no prazo de um ano a contar da definição dos parâmetros e padrões de que trata o parágrafo único do art. 40.

Parágrafo único. Até o término do prazo previsto no caput, compete ao Gabinete de Segurança Institucional da Presidência da República acompanhar e prestar apoio técnico

aos órgãos e entidades quanto à implementação dos recursos criptográficos baseados em algoritmo de Estado.

Art. 57. Os órgãos e entidades poderão expedir instruções complementares, no âmbito de suas competências, que detalharão os procedimentos relativos ao credenciamento de segurança e ao tratamento de informação classificada em qualquer grau de sigilo.

Art. 58. O Regimento Interno da Comissão Mista de Reavaliação da Informação detalhará os procedimentos de segurança necessários para a salvaguarda de informação classificada em qualquer grau de sigilo durante os seus trabalhos e os de sua Secretaria-Executiva, observado o disposto neste Decreto.

Art. 59. Este Decreto entra em vigor na data de sua publicação.

Art. 60. Ficam revogados:

I - o Decreto no 4.553, de 27 de dezembro de 2002; e

II - o Decreto no 5.301, de 9 de dezembro de 2004.

Brasília, 14 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
Márcia Pelegrini
Celso Luiz Nunes Amorim
Miriam Belchior
Marco Antonio Raupp
José Elito Carvalho Siqueira
Luís Inácio Lucena Adams
Jorge Hage Sobrinho

ANEXO I
TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

[Qualificação: nome, nacionalidade, CPF, identidade (no, data e local de expedição), filiação e endereço], perante o(a) [órgão ou entidade], declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo(a) [órgão ou entidade] e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações classificadas em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito do (da) [órgão ou entidade], salvo autorização da autoridade competente.

Declaro que [recebi] [tive acesso] ao (à) [documento ou material entregue ou exibido ao signatário], e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

[Local, data e assinatura]

[Duas testemunhas identificadas]

ANEXO II
CÓDIGO DE INDEXAÇÃO DE DOCUMENTO
QUE CONTÉM INFORMAÇÃO CLASSIFICADA - CIDIC - CATEGORIAS

CATEGORIAS	CÓDIGO
Agricultura, extrativismo e pesca	01
Ciência, Informação e Comunicação	02
Comércio, Serviços e Turismo	03
Cultura, Lazer e Esporte	04
Defesa e Segurança	05
Economia e Finanças	06
Educação	07
Governo e Política	08
Habitação, Saneamento e Urbanismo	09
Indústria	10
Justiça e Legislação	11
Meio ambiente	12
Pessoa, família e sociedade	13
Relações internacionais	14
Saúde	15
Trabalho	16
Transportes e trânsito	17

Obs.:

1. Categorias: representam os aspectos ou temas correlacionados à informação classificada em grau de sigilo, e serão indicadas pela Autoridade Classificadora. Para tanto deverá ser usado, exclusivamente, o primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), definidos no Padrão de Interoperabilidade do Governo Eletrônico (e-Ping), conforme quadro acima.

2. Composição no CIDIC: 2 dígitos = código numérico

DECRETO Nº 8.777, DE 11 DE MAIO DE 2016

Institui a Política de Dados Abertos do Poder Executivo federal.

A PRESIDENTA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, caput, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Lei nº 12.527, de 18 de novembro de 2011, e no art. 24, caput, incisos V e VI, da Lei nº 12.965, de 23 de abril de 2014,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Dados Abertos do Poder Executivo federal, com os seguintes objetivos:

I - promover a publicação de dados contidos em bases de dados de órgãos e entidades da administração pública federal direta, autárquica e fundacional sob a forma de dados abertos;

II - aprimorar a cultura de transparência pública;

III - franquear aos cidadãos o acesso, de forma aberta, aos dados produzidos ou acumulados pelo Poder Executivo federal, sobre os quais não recaia vedação expressa de acesso;

IV - facilitar o intercâmbio de dados entre órgãos e entidades da administração pública federal e as diferentes esferas da federação;

V - fomentar o controle social e o desenvolvimento de novas tecnologias destinadas à construção de ambiente de gestão pública participativa e democrática e à melhor oferta de serviços públicos para o cidadão;

VI - fomentar a pesquisa científica de base empírica sobre a gestão pública;

VII - promover o desenvolvimento tecnológico e a inovação nos setores público e privado e fomentar novos negócios;

VIII - promover o compartilhamento de recursos de tecnologia da informação, de maneira a evitar a duplicidade de ações e o desperdício de recursos na disseminação de dados e informações; e

IX - promover a oferta de serviços públicos digitais de forma integrada.

Art. 2º Para os fins deste Decreto, entende-se por:

I - dado - sequência de símbolos ou valores, representados em qualquer meio, produzidos como resultado de um processo natural ou artificial;

II - dado acessível ao público - qualquer dado gerado ou acumulado pelo Governo que não esteja sob sigilo ou sob restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011;

III - dados abertos - dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte;

IV - formato aberto - formato de arquivo não proprietário, cuja especificação esteja documentada publicamente e seja de livre conhecimento e implementação, livre de patentes ou qualquer outra restrição legal quanto à sua utilização; e

V - Plano de Dados Abertos - documento orientador para as ações de implementação e promoção de abertura de dados de cada órgão ou entidade da administração pública federal, obedecidos os padrões mínimos de qualidade, de forma a facilitar o entendimento e a reutilização das informações.

Art. 3º A Política de Dados Abertos do Poder Executivo federal será regida pelos seguintes princípios e diretrizes:

I - observância da publicidade das bases de dados como preceito geral e do sigilo como exceção;

II - garantia de acesso irrestrito às bases de dados, as quais devem ser legíveis por máquina e estar disponíveis em formato aberto;

III - descrição das bases de dados, com informação suficiente para a compreensão de eventuais ressalvas quanto à sua qualidade e integridade;

IV - permissão irrestrita de reuso das bases de dados publicadas em formato aberto;

V - completude e interoperabilidade das bases de dados, as quais devem ser disponibilizadas em sua forma primária, com o maior grau de granularidade possível, ou referenciar as bases primárias, quando disponibilizadas de forma agregada;

VI - atualização periódica, de forma a garantir a perenidade dos dados, a padronização de estruturas de informação e o valor dos dados à sociedade e atender às necessidades de seus usuários; e

VII - designação clara de responsável pela publicação, atualização, evolução e manutenção de cada base de dado aberta, incluída a prestação de assistência quanto ao uso de dados.

CAPÍTULO II
DA LIVRE UTILIZAÇÃO DE BASES DE DADOS

Art. 4º Os dados disponibilizados pelo Poder Executivo federal, bem como qualquer informação de transparência ativa, são de livre utilização pelo Governo federal e pela sociedade.

Parágrafo único. Na divulgação de dados protegidos por direitos autorais pertencentes a terceiros, fica o Poder Executivo federal obrigado a indicar o seu detentor e as condições de utilização por ele autorizadas.

CAPÍTULO III
DA GOVERNANÇA

Art. 5º A gestão da Política de Dados Abertos do Poder Executivo federal será coordenada pelo Ministério do Planejamento, Orçamento e Gestão, por meio da Infraestrutura Nacional de Dados Abertos - INDA.

§ 1º A INDA contará com mecanismo de governança multiparticipativa, transparente, colaborativa e democrática, com caráter gerencial e normativo, na forma de regulamento.

§ 2º A implementação da Política de Dados Abertos ocorrerá por meio da execução de Plano de Dados Abertos no âmbito de cada órgão ou entidade da administração pública federal, direta, autárquica e fundacional, o qual deverá dispor, no mínimo, sobre os seguintes tópicos:

I - criação e manutenção de inventários e catálogos corporativos de dados;

II - mecanismos transparentes de priorização na abertura de bases de dados, os quais obedecerão os critérios estabelecidos pela INDA e considerarão o potencial de utilização e reutilização dos dados tanto pelo Governo quanto pela sociedade civil;

III - cronograma relacionado aos procedimentos de abertura das bases de dados, sua atualização e sua melhoria;

IV - especificação clara sobre os papeis e responsabilidades das unidades do órgão ou entidade da administração pública federal relacionados com a publicação, a atualização, a evolução e a manutenção das bases de dados;

V - criação de processos para o engajamento de cidadãos, com o objetivo de facilitar e priorizar a abertura da dados, esclarecer dúvidas de interpretação na utilização e corrigir problemas nos dados já disponibilizados; e

VI - demais mecanismos para a promoção, o fomento e o uso eficiente e efetivo das bases de dados pela sociedade e pelo Governo.

§ 3º A INDA poderá estabelecer normas complementares relacionadas com a elaboração do Plano de Dados Abertos, bem como relacionadas a proteção de informações pessoais na publicação de bases de dados abertos nos termos deste Decreto.

§ 4º A autoridade designada nos termos do art. 40 da Lei nº 12.527, de 2011, será responsável por assegurar a publicação e a atualização do Plano de Dados Abertos, e exercerá as seguintes atribuições:

I - orientar as unidades sobre o cumprimento das normas referentes a dados abertos;

II - assegurar o cumprimento das normas relativas à publicação de dados abertos, de forma eficiente e adequada;

III - monitorar a implementação dos Planos de Dados Abertos; e

IV - apresentar relatórios periódicos sobre o cumprimento dos Planos de Dados Abertos, com recomendações sobre as medidas indispensáveis à implementação e ao aperfeiçoamento da Política de Dados Abertos.

CAPÍTULO IV
DA SOLICITAÇÃO DE ABERTURA DE BASES DE DADOS

Art. 6º Às solicitações de abertura de bases de dados da administração pública federal aplicam-se os prazos e os procedimentos previstos para o processamento de pedidos de acesso à informação, nos termos da Lei nº 12.527, de 2011, e do Decreto nº 7.724, de 16 de maio de 2012.

Parágrafo único. A decisão negativa de acesso de pedido de abertura de base de dados governamentais fundamentada na demanda por custos adicionais desproporcionais e não previstos pelo órgão ou pela entidade da administração pública federal deverá apresentar análise sobre a quantificação de tais custos e sobre a viabilidade da inclusão das bases de dados em edição futura do Plano de Dados Abertos.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 7º O Decreto nº 7.724, de 16 de maio de 2012, passa a vigorar com as seguintes alterações:

"Art. 47. .....

.....

III - .....

a) pela Controladoria-Geral da União, em grau recursal, pedido de acesso à informação ou de abertura de base de dados, ou às razões da negativa de acesso à informação ou de abertura de base de dados; ou

....." (NR)

Art. 8º Consideram-se automaticamente passíveis de abertura as bases de dados do Governo federal que não contenham informações protegidas nos termos dos art. 7, § 3º, art. 22, art. 23 e art. 31 da Lei nº 12.527, de 2011.

Parágrafo único. Aplica-se o disposto no caput a bases de dados que contenham informações protegidas, no que se refere às informações não alcançadas por essa proteção.

Art. 9º Os Planos de Dados Abertos dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional deverão ser elaborados e publicados em sítio eletrônico no prazo de sessenta dias da data de publicação deste Decreto.

§ 1º Os Planos de Dados Abertos dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional deverão priorizar a abertura dos dados de interesse público listados no Anexo, os quais deverão ser publicados em formato aberto no prazo de cento e oitenta dias da data de publicação deste Decreto.

§ 2º Os Planos de Dados Abertos dos demais órgãos e entidades da administração pública federal direta, autárquica e fundacional serão publicados conforme cronograma publicado em ato conjunto do Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União.

Art. 10. Compete à Controladoria-Geral da União monitorar a aplicação do disposto neste Decreto e o cumprimento dos prazos e procedimentos.

Art. 11. Este Decreto entra em vigor na data de sua publicação.

Brasília, 11 de maio de 2016; 195o da Independência e 128o da República.

DILMA ROUSSEFF
Eugênio José Guilherme de Aragão
Valdir Moysés Simão
Luiz Navarro

ANEXO

SISTEMA/ÓRGÃO RESPONSÁVEL	DADOS DE INTERESSE PÚBLICO PARA PRIORIZAÇÃO
Casa Civil da Presidência da República	Texto das publicações do Diário Oficial da União
Controladoria-Geral da União	Ocupantes de cargos de gerência e direção em empresas estatais e subsidiárias
Órgãos e entidades que não utilizam o Sistema Integrado de Administração de Recursos Humanos - Siape	Dados relativos a servidores inativos e aposentados e relativos à empregados e servidores públicos das entidades da administração indireta que órgãos e entidades que não utilizam o Siape
Ministério da Fazenda	Dados do Sistema Integrado de Administração Financeira - Siafi
Ministério da Fazenda	Informações sobre o quadro societário das empresas, a partir do Cadastro Nacional de Pessoas Jurídicas
Ministério do Planejamento, Orçamento e Gestão	Dados relacionados ao Plano Plurianual, incluindo metas físicas.
Ministério do Planejamento, Orçamento e Gestão	Dados relativos a servidores inativos e aposentados.
Ministério do Planejamento, Orçamento e Gestão	Bens móveis e de patrimônio registrados no Sistema Integrado de Administração de Serviços - Siads
Ministério do Planejamento, Orçamento e Gestão	Dados relacionados ao Sistema Integrado de Administração de Serviços Gerais - Siasg / Comprasnet.
Ministério do Planejamento, Orçamento e Gestão	Dados referentes ao Portal de Convênios/ Siconv.
Ministério do Planejamento, Orçamento e Gestão	Informações cadastrais e relacionadas ao controle da execução de emendas parlamentares.
Ministério do Planejamento, Orçamento e Gestão	Propriedades e imóveis do Governo federal.
Sistema Nacional de Informações de Registro Civil - SIRC	Dados sobre nascimentos, casamentos, divórcios e óbitos.

PORTARIAS

PORTARIA INTERMINISTERIAL Nº 233, DE 25 DE MAIO DE 2012

OS MINISTROS DE ESTADO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, CHEFE DA CONTROLADORIA-GERAL DA UNIÃO, DA DEFESA E DA FAZENDA, no uso das atribuições que lhes confere o inciso II do parágrafo único do art. 87 da Constituição Federal, e tendo em vista o disposto no inciso VI do § 3º do art. 7º e no inciso I do art. 69 do Decreto nº 7.724, de 16 de maio de 2012, resolvem:

Art. 1º Esta Portaria disciplina, no âmbito do Poder Executivo federal, o modo de divulgação da remuneração e subsídio recebidos por ocupante de cargo, posto, graduação, função e emprego público, incluindo auxílios, ajudas de custo, jetons e quaisquer outras vantagens pecuniárias, bem como proventos de aposentadoria e pensões daqueles que estiverem na ativa, conforme disposto no inciso VI do § 3º do art. 7º do Decreto nº 7.724, de 16 de maio de 2012.

§ 1º As informações previstas no caput serão encaminhadas pelos órgãos e entidades responsáveis até o 10º (décimo) dia útil de cada mês à Controladoria-Geral da União - CGU, em formato por ela definido, para fins de publicação mensal no Portal da Transparência.

§ 2º A CGU deverá publicar as informações recebidas até o último dia útil de cada mês, no Portal da Transparência.

Art. 2º As informações referentes a valores percebidos pelo pessoal civil serão extraídas do Sistema Integrado de Administração de Recursos Humanos - SIAPE, pela Secretaria de Gestão Pública do Ministério do Planejamento, Orçamento e Gestão - SEGEP/MP, e encaminhados à CGU no prazo do §1º do art. 1º.

§ 1º Os valores previstos no caput abrangem parcelas remuneratórias e indenizatórias, salvo, neste último caso, as verbas indenizatórias constantes exclusivamente do Sistema Integrado de Administração Financeira do Governo Federal - SIAFI, que serão encaminhadas diretamente pela Secretaria do Tesouro Nacional do Ministério da Fazenda à CGU.

§ 2º Os órgãos e entidades que não utilizam o SIAPE enviarão diretamente as informações referentes à remuneração dos seus servidores à CGU, no prazo previsto no § 1º do art. 1º.

§ 3º Aplica-se o disposto no caput às informações referentes à remuneração dos policiais militares oriundos dos extintos Territórios Federais e aos contratados por tempo determinado nos termos da Lei nº 8.745, de 9 de dezembro de 1993.

Art. 3º As informações referentes à remuneração percebida por servidores públicos federais em razão da participação como representantes da União em Conselhos de Administração e Fiscal ou órgãos equivalentes de empresas controladas direta ou indiretamente pela União (jetons) serão consolidadas pelo Departamento de Coordenação e Governança das Empresas Estatais do Ministério do Planejamento, Orçamento e Gestão - DEST/SE/MP e encaminhadas à CGU, no prazo do §1º do art. 1º.

§ 1º A responsabilidade pelo conteúdo e envio das informações de que trata o caput deste artigo é das empresas nele referidas, cabendo-lhes a atualização, até o 5º (quinto) dia útil do mês subsequente ao do pagamento do jetom, no Sistema de Informação das Empresas Estatais - SIEST.

§ 2º As informações referentes à remuneração de servidores públicos federais em Conselhos de Administração e Fiscal ou em órgãos equivalentes, em empresas em que a União ou empresas estatais participam minoritariamente no capital, na condição de acionista ordinário ou preferencialista, (jetons) deverão ser encaminhadas à CGU pelo Ministério que fez a indicação do servidor até o 10º (décimo) dia útil do mês subsequente ao do pagamento do jetom.

Art. 4º As informações referentes a valores percebidos pelo pessoal militar das Forças Armadas serão encaminhadas pelo Ministério da Defesa à CGU, no prazo do §1º do art. 1º.

Art. 5º Os órgãos e entidades deverão adequar seus sítios eletrônicos de modo a disponibilizar mecanismo de redirecionamento de página para o Portal da Transparência, de que trata o § 1º do art. 1º.

Art. 6º As empresas públicas, sociedades de economia mista e demais entidades controladas pela União que não atuam em regime de concorrência, não sujeitas ao disposto no art. 173 da Constituição, deverão disponibilizar as informações de seus empregados e administradores em seus sítios na Internet, não sendo necessária a publicação no Portal da Transparência de que trata o § 1º do art. 1º.

Parágrafo único. A primeira disponibilização das informações de que trata este artigo deverá ser feita até 30 de julho de 2012.

Art. 7º Com exceção do disposto no art. 6º, a primeira disponibilização das informações de que trata esta Portaria no Portal da Transparência deverá ser feita até:

I - 30 de junho de 2012, no caso das verbas remuneratórias dos servidores civis, dos contratados por tempo determinado, dos policiais militares oriundos de exTerritórios Federais e jetons das participações em conselhos;

II - 30 de julho de 2012, no caso das verbas remuneratórias percebidas pelo pessoal militar das Forças Armadas; e

III - 30 de agosto de 2012, no caso das verbas indenizatórias do pessoal civil e do pessoal militar das Forças Armadas.

Parágrafo único. A publicação que trata o caput não prejudica o pedido de acesso a informação previsto nos art. 11 e seguintes do Decreto nº 7.724, de 2012.

Art. 8º Esta Portaria Interministerial entra em vigor na data de sua publicação.

MIRIAM BELCHIOR
Ministra de Estado do Planejamento, Orçamento e Gestão
JORGE HAGE SOBRINHO
Ministro de Estado Chefe da Controladoria-Geral da União
GUIDO MANTEGA
Ministro de Estado da Fazenda
CELSO AMORIM
Ministro de Estado da Defesa

PORTARIA INTERMINISTERIAL Nº-1.254, DE 18 DE MAIO DE 2015

Institui o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC) no âmbito do Poder Executivo federal.

O MINISTRO DE ESTADO CHEFE DA CONTROLADORIA-GERAL DA UNIÃO E O MINISTRO DE ESTADO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, no uso das atribuições que lhes conferem o art. 87, parágrafo único, inciso II, da Constituição, e o art. 69 do Decreto nº 7.724, de 16 de maio de 2012, e tendo em vista o disposto na Lei nº 12.527, de 18 de novembro de 2011, resolvem:

Art. 1º Fica instituído o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC), no âmbito dos órgãos e entidades do Poder Executivo federal, como sistema centralizado para o tratamento de pedidos de acesso à informação amparados pela Lei nº 12.527, de 2011.

§ 1º Entende-se por tratamento, para fins desta Portaria, o registro do pedido de acesso à informação, bem como o fornecimento da respectiva resposta, a interposição de recursos e o registro das respectivas decisões.

§ 2º Os pedidos de acesso à informação poderão ser recebidos por outros meios, desde que atendam os seguintes requisitos, previstos no art. 12 do Decreto nº 7.724, de 2012:

I - nome do requerente;

II - número de documento de identificação válido;

III - especificação, de forma clara e precisa, da informação requerida; e

IV - endereço físico ou eletrônico do requerente, para recebimento de comunicações ou da informação requerida.

Art. 2º A utilização do e-SIC é obrigatória para órgãos da administração direta, autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União.

Parágrafo único. A obrigatoriedade do e-SIC não exclui a possibilidade de utilização, pelos órgãos e entidades, de outros sistemas para organização dos fluxos internos de tratamento dos pedidos de acesso à informação.

Art. 3º Compete à Controladoria-Geral da União:

I - promover a disponibilização, a gestão, a manutenção e a atualização do e-SIC; e

II - orientar os órgãos e entidades do Poder Executivo federal quanto aos procedimentos referentes à utilização do e-SIC.

Art. 4º Compete aos órgãos e entidades do Poder Executivo federal:

I - garantir o acesso à informação, resguardando, sob pena de responsabilização, nos termos do artigo 34 da Lei nº 12.527, de 2011:

a) as informações pessoais relacionadas à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

b) as informações classificadas, nos termos dos arts. 23 e 24 da Lei nº 12.527, de 2011;

c) as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado, na forma do §1º do art. 7º da Lei nº 12.527, de 2011; e

d) as hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça, conforme inciso I do art. 6º do Decreto nº 7.724, de 2012.

II - garantir que todos os pedidos de acesso à informação direcionados a seu órgão ou entidade, no ato de seu recebimento, sejam registrados no e-SIC, bem como as respectivas respostas, os recursos, as reclamações e as decisões;

III - disponibilizar acesso ao e-SIC em seus sítios eletrônicos;

IV - efetuar o cadastramento de seus Serviços de Informações ao Cidadão junto à Controladoria-Geral da União e mantê-lo atualizado;

V - criar e administrar o perfil dos servidores cadastrados no e-SIC, responsabilizando-se por sua atualização;

VI - manter os dados e informações relativos ao cumprimento da legislação de acesso à informação atualizados no e-SIC, conforme orientações da Controladoria-Geral da União; e

VII - seguir as orientações quanto aos procedimentos referentes à utilização do e-SIC emitidas pela Controladoria-Geral União.

Parágrafo único. As informações fornecidas pelos órgãos e entidades são de sua responsabilidade exclusiva, não cabendo à Controladoria-Geral da União, como gestora do e-SIC, a responsabilidade por eventuais danos decorrentes de uso indevido, ainda que por terceiros não autorizados.

Art. 5º Os casos omissos serão resolvidos pela Controladoria-Geral da União.

Art. 6º Esta Portaria entra em vigor na data de sua publicação.

VALDIR MOYSÉS SIMÃO
Ministro de Estado Chefe da Controladoria-Geral da União
NELSON BARBOSA
Ministro de Estado do Planejamento, Orçamento e Gestão

RESOLUÇÕES

RESOLUÇÕES DA COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES

Resolução nº 01, de 21 de dezembro de 2012

Aprova o Regimento Interno da Comissão Mista de Reavaliação de Informações.

A COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES, tendo em vista o disposto no art. 54 do Decreto nº 7.724, de 16 de maio de 2012,

RESOLVE:

Art. 1º Fica aprovado o Regimento Interno da Comissão Mista de Reavaliação de Informações, na forma do Anexo, que dispõe sobre sua organização e funcionamento, observado o disposto no Decreto nº 7.724, de 16 de maio de 2012.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

ANEXO

CAPÍTULO I

DA NATUREZA E DAS COMPETÊNCIAS DA COMISSÃO

Art. 1º A Comissão Mista de Reavaliação de Informações é o órgão colegiado interministerial que tem por finalidade exercer as competências que lhe foram atribuídas pela Lei nº 12.527, de 18 de novembro de 2011, quanto ao tratamento e classificação de informações sigilosas no âmbito da administração pública federal, notadamente:

I - rever, de ofício ou mediante provocação, a classificação de informação no grau ultrassecreto ou secreto ou sua reavaliação, no máximo a cada quatro anos;

II - requisitar da autoridade que classificar informação no grau ultrassecreto ou secreto esclarecimento ou conteúdo, parcial ou integral, da informação, quando as informações constantes do Termo de Classificação de Informação - TCI não forem suficientes para a revisão da classificação;

III - decidir recursos apresentados contra decisão proferida:

a) pela Controladoria-Geral da União, em grau recursal, a pedido de acesso à informação ou às razões da negativa de acesso à informação; ou

b) pelo Ministro de Estado ou autoridade com a mesma prerrogativa, em grau recursal, a pedido de desclassificação ou reavaliação de informação classificada;

IV - prorrogar por uma única vez, e por período determinado não superior a vinte e cinco anos, o prazo de sigilo de informação classificada no grau ultrassecreto, enquanto seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional, à integridade do território nacional ou grave risco às relações internacionais do País, limitado ao máximo de cinquenta anos o prazo total da classificação; e

V - estabelecer orientações normativas de caráter geral a fim de suprir eventuais lacunas na aplicação do Decreto nº 7.724, de 2012, e da Lei nº 12.527, de 2011.

CAPÍTULO II
DA ORGANIZAÇÃO

Art. 2º Comissão será integrada pelos titulares dos seguintes órgãos:

I - Casa Civil da Presidência da República, que a presidirá;

II - Ministério da Justiça;

III - Ministério das Relações Exteriores;

IV - Ministério da Defesa;

V - Ministério da Fazenda;

VI - Ministério do Planejamento, Orçamento e Gestão;

VII - Gabinete de Segurança Institucional da Presidência da República;

VIII - Advocacia-Geral da União;

IX - Controladoria-Geral da União; e

X - Secretaria de Direitos Humanos da Presidência da República.

Parágrafo único. Cada integrante indicará suplente a ser designado por ato do Presidente da Comissão.

Art. 3º São atribuições do Presidente da Comissão:

I - dirigir os trabalhos da Comissão;

II - adotar as providências administrativas necessárias ao seu regular funcionamento;

III - representar a Comissão perante outros órgãos e entidades;

IV- convocar e presidir as sessões ordinárias e extraordinárias;

V - votar, na condição de membro, e, em caso de empate, proferir o voto de qualidade;

VI- requisitar ad referendum da Comissão esclarecimento ou conteúdo, parcial ou integral, de informação classificada, nos termos do inciso II do caput do art. 1º;e

VII - desempenhar outras atribuições estabelecidas neste Regimento.

Art. 4º A Casa Civil da Presidência da República exercerá as funções de Secretaria-Executiva da Comissão.

§ 1º O Secretário-Executivo será designado livremente pelo Ministro de Estado Chefe da Casa Civil da Presidência da República.

§ 2º Os demais integrantes da Secretaria-Executiva serão designados pelo Ministro de Estado Chefe da Casa Civil da Presidência da República entre servidores públicos ocupantes de cargo efetivo, militares da ativa das Forças Armadas ou empregados públicos, para a realização de atividades técnicas e administrativas da Comissão e tratamento da informação sigilosa". (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

Art. 5º Compete à Secretaria-Executiva:

I - secretariar, em caráter permanente, os trabalhos da Comissão;

II - receber os recursos e demais expedientes, e deles dar ciência aos integrantes da Comissão;

III - custodiar os Termos de Classificação de Informações, deles dar ciência aos integrantes da Comissão, para revisão de ofício ou reavaliação, e propor sua inclusão na pauta, em atenção aos prazos previstos na legislação;

IV - organizar as pautas, registrar as deliberações das reuniões, e expedir as convocações e notificações necessárias;

V - elaborar as atas das reuniões e, após aprovação pela Comissão, dar-lhes publicidade;

VI - adotar as medidas e os procedimentos necessários de segurança e de proteção da informação sigilosa e de informação pessoal, observada sua disponibilidade, autenticidade, integridade e eventual restrição de acesso;

VII - comunicar aos requerentes e ao órgão ou entidade interessado as decisões da Comissão, por meio eletrônico, no prazo de quinze dias, contado da data de reunião em que foi tomada a decisão;

VIII - assessorar tecnicamente a Comissão, inclusive na elaboração de propostas de instrumentos deliberativos de que trata o art. 10;

IX - monitorar o cumprimento dos prazos previstos nos §§ 1º, inciso III, 2º e 3o do art. 35 da Lei nº 12.527, de 2011;

X - elaborar relatório anual com informações sobre os trabalhos da Comissão;

XI - encaminhar à Controladoria-Geral da União, até 10 de março de cada ano, informações sobre o trabalho da Comissão, para subsidiar a preparação do relatório previsto no inciso V do caput do art. 68 do Decreto nº 7.724, de 2012; e

XII- exercer outras competências conferidas pela Comissão ou por sua Presidência.

CAPÍTULO III
DAS DELIBERAÇÕES

Art. 6º A Comissão deliberará em reuniões presenciais ou por meio do uso de tecnologia de informação e comunicação apropriada.

Parágrafo único. A Secretaria-Executiva enviará com antecedência a pauta da reunião e os documentos necessários para deliberação.

Art. 7º A Comissão deliberará:

I - por maioria absoluta, quando envolverem as competências previstas nos incisos I e IV do caput do art. 1º; e

II - por maioria simples, nos demais casos.

Art. 8º A Comissão se reunirá, ordinariamente, uma vez por mês e, extraordinariamente, sempre que convocada por seu Presidente.

§ 1º As reuniões serão realizadas com a participação de no mínimo seis integrantes.

§ 2º Quando não houver quórum mínimo para as atividades da Comissão, a reunião será considerada como não realizada, e não contará para efeitos dos prazos previstos neste Regimento.

Art. 9º Em caso de pedido de vista, o membro que o formular deverá apresentar seu voto até a reunião ordinária subsequente.

Art. 10º As deliberações do plenário da Comissão terão a forma de:

I - decisão, quando se tratar de matérias previstas nos incisos I a IV do caput do art. 1º;

II- resolução, quando se tratar de:

a) orientação normativa de caráter geral de que trata o inciso V do caput do art. 1º; e

b) aprovação e alteração do Regimento Interno; e

III - súmula, constituída de enunciado que sintetize entendimento resultante de reiteradas decisões, para consolidar interpretação adotada pela Comissão, ou encerrar divergência administrativa.

Parágrafo único. Será dada publicidade às deliberações da Comissão por meio do Portal de Acesso à Informação.

Art. 11º A edição ou revisão de enunciado de súmula ou de orientação normativa ocorrerá mediante proposta apresentada por qualquer dos membros da Comissão.

§ 1º A Comissão deliberará sobre a admissibilidade da proposta por maioria simples dos votos.

§ 2º O presidente designará relator para apresentação da proposta admitida e sua deliberação ocorrerá em sessão subsequente.

CAPÍTULO IV
DOS RECURSOS À COMISSÃO

Art. 12º Em caso de negativa de acesso à informação, ou às razões da negativa do acesso, desprovido o recurso pela CGU, o requerente poderá apresentar, no prazo de dez dias, contado da ciência da decisão, recurso à Comissão.

Parágrafo único. Os recursos interpostos à Comissão com base no caput serão protocolados na Controladoria-Geral da União para instrução.

Art. 13º A Controladoria-Geral da União instruirá o recurso com os seguintes documentos:

I - pedido de acesso a que se refere o recurso;

II - manifestações proferidas nas instâncias anteriores, tais como a resposta ao pedido, os recursos e as respostas aos recursos;

III - a decisão proferida pela Controladoria-Geral da União como instância recursal, incluídas as informações prestadas pelo órgão e a análise técnica do mérito, quando couber; e

IV - manifestação quanto ao conhecimento do recurso interposto à Comissão.

Parágrafo único. A Controladoria-Geral da União encaminhará o recurso instruído à Secretaria-Executiva da Comissão com antecedência mínima de dez dias da reunião seguinte à sua interposição.

Art. 14º O recurso não será conhecido quando interposto:

I - fora do prazo;

II - fora das competências da Comissão;

III - por quem não seja legitimado; ou

IV - em situações não previstas no Decreto nº 7.724, de 2012.

Art. 15-A. A decisão de classificação, desclassificação, reclassificação, prorrogação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, nos termos do Decreto no 7.724, de 2012. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

Art. 15-B. A cópia do TCI de informações classificadas no grau ultrassecreto ou secreto será encaminhada à Secretaria-Executiva da Comissão por meio de sistema eletrônico, que utilizará recursos criptográficos adequados ao grau de sigilo, observadas as medidas destinadas a garantir o sigilo, a inviolabilidade, a integridade e a autenticidade da informação, cuja segurança será sistematicamente aferida e atestada pelo Gabinete de Segurança Institucional da Presidência da República. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

§ 1º Somente servidores credenciados para o tratamento de informações classificadas, na forma do Decreto no 7.845, de 14 de novembro de 2012, poderão utilizar ou ter acesso ao sistema eletrônico de que trata o caput. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

§ 2º O sistema eletrônico de que trata o caput deverá manter controle e registro dos acessos e das transações realizadas. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

§ 3º A cifração e a decifração de informação classificada em qualquer grau de sigilo utilizarão recurso criptográfico baseado em algoritmo de Estado. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

§ 4º A Secretaria-Executiva informará ao remetente o recebimento do TCI por meio eletrônico. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

§ 5º Para harmonizar e coordenar os trabalhos da Comissão, o sistema eletrônico deverá permitir pesquisa estruturada nos campos do TCI. (alterado pela Resolução CMRI nº 1, de 24 de maio de 2013)

Art. 15-C. A informação referente ao TCI será armazenada em equipamentos seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Gabinete de Segurança Institucional da Presidência da República. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

Art. 15-D. Identificados, a qualquer tempo, indícios de irregularidade das informações constantes do TCI, estes serão imediatamente comunicados ao remetente para adoção de medidas cabíveis. (redação da Resolução CMRI nº 1, de 24 de maio de 2013)

CAPÍTULO V
DA REAVALIAÇÃO, PRORROGAÇÃO DE PRAZO E DESCLASSIFICAÇÃO DE INFORMAÇÕES SIGILOSAS

Art. 16º A Secretaria-Executiva dará ciência à Comissão do recebimento do Termo de Classificação de Informação - TCI de que trata o art. 32 do Decreto nº 7.724, de 2012.

Parágrafo único. Qualquer dos membros da Comissão poderá propor a revisão da classificação realizada pelo órgão ou entidade nos casos previstos no caput, devendo apresentar as razões aos demais integrantes do colegiado, no mínimo, dez dias antes da reunião da Comissão.

Art. 17º A revisão de ofício da informação classificada no grau ultrassecreto ou secreto será apreciada em até três sessões anteriores à data de sua desclassificação automática.

Art. 18º A Secretaria-Executiva poderá solicitar ao órgão ou entidade informações adicionais sobre a necessidade de manutenção do sigilo, antes da revisão de ofício de que trata o inciso II do parágrafo único do art. 35 do Decreto nº 7.724, de 2012.

Parágrafo único. As informações solicitadas nos termos do caput deverão ser encaminhadas à Secretaria-Executiva da Comissão no prazo por ela estabelecido, e conterão:

I - razões para a manutenção da classificação;

II - histórico das prorrogações relativas à informação classificada; e

III - eventual esclarecimento ou conteúdo, parcial ou integral, da informação requisitada ao órgão ou entidade, nos termos do inciso II do caput do art. 1º.

Art. 19º Os requerimentos de prorrogação do prazo de classificação de informação no grau ultrassecreto a que se refere o inciso IV do caput do art. 1º deverão ser encaminhados à Comissão em até um ano antes do vencimento do termo final de restrição de acesso.

Parágrafo único. O requerimento de que trata o caput deverá ser apreciado, impreterivelmente, em até três sessões subsequentes à data de seu recebimento pela Secretaria-Executiva, ficando sobrestadas, até que se ultime a votação, todas as demais deliberações da Comissão.

Art. 20º O requerimento de que trata o art. 19 deverá indicar as razões que justificam a manutenção da classificação e será encaminhado à Secretaria-Executiva da Comissão.

Parágrafo único. A autoridade classificadora instruirá o pedido de prorrogação com os seguintes documentos:

I - razões para a manutenção da classificação;

II- eventual esclarecimento ou conteúdo, parcial ou integral, da informação requisitada ao órgão ou entidade, nos termos do inciso II do caput do art. 1º; e

III - manifestação quanto à observância do prazo previsto no art. 19.

Art. 21º Em caso de recurso interposto contra decisão proferida em pedido de desclassificação ou reavaliação de informação classificada, a autoridade recorrida enviará à Secretaria-Executiva da Comissão o recurso instruído com os seguintes documentos:

I - razões para a manutenção da classificação; e

II - eventual esclarecimento ou conteúdo, parcial ou integral, da informação requisitada ao órgão ou entidade, nos termos do inciso II do caput do art. 1º.

Parágrafo único. Os recursos interpostos à Comissão com base no caput serão protocolados no órgão que indeferiu o pedido de desclassificação ou de reavaliação, para a instrução.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Art. 22º O Serviço de Informação ao Cidadão - SIC da Casa Civil da Presidência da República receberá os pedidos de acesso a informação em poder da Comissão.

§ 1º Quando houver negativa de acesso a informação em poder da Comissão, ou não fornecimento das razões da negativa do acesso, o recurso de que trata o caput do art. 21 do Decreto nº 7.724, de 2012, será dirigido ao Presidente da Comissão.

§ 2º Para o recurso previsto no parágrafo único do art. 21 do Decreto no 7.724, de 2012, considera-se autoridade máxima o pleno da Comissão.

§ 3º Não cabe recurso da decisão de desprovimento proferida pelo pleno da Comissão.

Art. 23º Compete à autoridade de monitoramento, designada nos termos do art. 67 do Decreto nº 7.724, de 2012, acompanhar a implementação das decisões proferidas no âmbito da Comissão Mista de Reavaliação de Informações.

§ 1º A autoridade referida no caput deste artigo dará ciência do cumprimento das decisões proferidas pela CMRI à Controladoria Geral da União - CGU a cada trimestre e, eventualmente, em prazo específico determinado na própria decisão.

§2º Comprovado perante a CMRI o descumprimento de decisão de que trata o caput, caberá a CGU instaurar ou determinar a instauração de procedimento administrativo a fim de apurar a responsabilidade de quem deu causa, nos termos do art. 65 do Decreto nº 7.724, de 2012.

Art. 24º A Casa Civil da Presidência da República proverá o suporte administrativo necessário ao funcionamento da Comissão.

Art. 25º As normas deste Regimento Interno aplicam-se imediatamente aos processos em curso na Comissão e não atingem os atos processuais já praticados em período anterior à sua vigência.

Brasília, 21 de dezembro de 2012.

RESOLUÇÃO Nº 2, DE 30 DE MARÇO DE 2016

Dispõe sobre a publicação do rol de informações desclassificadas, nos termos do art. 45, inciso I, do Decreto nº 7.724, de 16 de maio de 2012.

A COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES, no exercício da competência que lhe atribui o inciso V do art. 47 do Decreto nº 7.724, de 16 de maio de 2012,

RESOLVE:

Art. 1º O rol das informações desclassificadas, ao qual se refere o art. 45, inciso I, do Decreto nº 7.724, de 16 de maio de 2012, deverá apresentar, no mínimo, a descrição das seguintes informações:

I – dados que identifiquem o documento desclassificado, a exemplo do Número Único de Protocolo - NUP, do Código de Indexação de Documento que contém Informação Classificada - CIDIC, ou outro;

II – grau de sigilo ao qual o documento desclassificado ficou submetido;

III – breve resumo do documento desclassificado.

Art. 2º Os órgãos e entidades do Poder Executivo federal deverão manter em transparência ativa todas as listas anuais de desclassificação produzidas a partir da vigência desta Resolução, em formato eletrônico aberto e não proprietário nos moldes em que tenham sido originalmente publicadas, conforme modelo anexo.

Art. 3º Caberá à Controladoria-Geral da União o monitoramento da execução do disposto nesta Resolução.

Art. 4º Esta resolução entra em vigor a partir na data de sua publicação.

ANEXO I

INFORMAÇÕES DESCLASSIFICADAS – Art. 45 do Decreto 7.724, de 16 de maio de 2012.
PERÍODO DE DESCLASSIFICAÇÃO: dd/mm/aaaa – dd/mm/aaaa

IDENTIFICAÇÃO DO DOCUMENTO	GRAU DE SIGILO	BREVE RESUMO DO DOCUMENTO

RESOLUÇÃO Nº 3, DE 30 DE MARÇO DE 2016

Dispõe sobre o procedimento de revisão de ofício de informação classificada em grau de sigilo secreto e ultrassecreto de que trata o art. 47, inciso I, e art. 51 do Decreto nº 7.724, de 16 de maio de 2012.

A COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES, no exercício das competências que lhe atribuem os incisos I, II e V do art.47 do Decreto nº 7.724, de 16 de maio de 2012,

RESOLVE:

Art. 1º A revisão de ofício da classificação de informação no grau ultrassecreto ou secreto ocorrerá quadrienalmente no prazo previsto pelo art. 35, §3º, da Lei nº 12.527, de 18 de novembro de 2011.

Art. 2º Caberá às autoridades elencadas no art. 27, incisos I e II, da Lei nº 12.527, de 2011, podendo se valer das Comissões Permanentes de Avaliação de Documentos Sigilosos (CPADS) de que trata o art. 34 do Decreto 7.724, de 16 de maio de 2012, a revisão prévia de todas as informações classificadas em grau de sigilo secreto e ultrassecreto no âmbito dos órgãos e entidades do Poder Executivo federal, a fim de pronunciarem-se acerca da necessidade de desclassificação, reclassificação ou manutenção do grau de classificação das informações analisadas por meio de Relatório de Avaliação de Documentos Sigilosos.

§1º Para a revisão prévia de que trata o caput, as autoridades acima deverão considerar, pelo menos:

I – a existência de outra espécie de sigilo disciplinada em Lei a incidir sobre a informação classificada, tal como previsto no Anexo B da Norma Complementar nº 20 da Instrução Normativa nº 1 do Departamento de Segurança da Informação e Comunicações, de 15 de julho de 2014,situação em que deverá opinar por sua desclassificação, nos termos da Lei 12.527, de 18 de novembro de 2011;

II – a existência de informação protegida nos termos do art. 31 da Lei nº 12.527, de 2011, situação em que deverá opinar por sua desclassificação; e

III – a permanência, no tempo, das razões determinantes da classificação em grau de sigilo de que trata o art. 23 da Lei nº 12.527, de 2011, situação em que deverá opinar pela manutenção da classificação ou alteração de seu grau ou prazo de restrição de acesso.

§2º O Relatório de Avaliação de Documentos Sigilosos deverá ser encaminhado à Comissão Mista de Reavaliação de Informações, nos moldes e prazos previstos nos Anexos I e

II desta Resolução, respectivamente, e será classificado em grau de sigilo compatível com as informações que contiver.

§ 3º No exercício da atribuição que lhe confere o inciso I do art.47 do Decreto nº 7.724, de 2012, a Comissão Mista de Reavaliação de Informações (CMRI) se manifestará, até o prazo estabelecido no art. 1º desta Resolução, sobre aprovação, aprovação parcial ou rejeição do parecer opinativo do Relatório de Avaliação de Documentos Sigilosos.

§4º Para os fins previstos no §2º do presente, poderá a CMRI requerer:

I - esclarecimentos adicionais sobre os documentos sujeitos à reavaliação; e

II - solicitar acesso à íntegra dos documentos sujeitos à avaliação, os quais deverão ser disponibilizados no prazo previsto na requisição.

Art. 3º A revisão da classificação de informação no grau ultrassecreto ou secreto, ou da sua reavaliação, ocorrerá em reuniões especiais convocadas pela Presidência da CMRI, a qual designará relatores para análise de conjuntos de informações previstas para as revisões em curso.

§ 1º É vedado ao membro da CMRI atuar como relator na revisão de informações do órgão ou entidade a que represente ou a que tenha vínculo funcional.

§2º A CMRI deliberará sobre as revisões de que trata esta Resolução, informando aos órgãos e entidades do Poder Executivo federalinteressados e publicando a ata da respectiva reunião.

§ 3º Os órgãos e entidades do Poder Executivo federal farão constar nos respectivos Termos de Classificação de Informação (TCIs) os dados referentes à conclusão das revisões.

§ 4º As reuniões previstas no caput não contarão para os prazos previstos nos arts. 15 e 19 da Resolução CMRI nº 1, de 21 de dezembro de 2012.

Art. 4º Inexistindo CPADS constituídas, os órgãos e entidades do Poder Executivo federal poderão se valer de comissão interna congênere ou de agente público determinado, observadas as normas de salvaguardas estabelecidas na Lei nº 12.527, de 2011, e em sua regulamentação.

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

Brasília, 30 de Março de 2016

ANEXO I

IDENTIFICAÇÃO DO DOCUMENTO	GRAU DE SIGILO	BREVE RESUMO DO DOCUMENTO	RAZÃO PARA A MANUTENÇÃO DO SIGILO	PARECER DA AUTORIDADE RATIFICADORA DA CLASSIFICAÇÃO

ANEXO II

PRAZO DE ENVIO	RELATÓRIOS SOBRE DOCUMENTOS SECRETOS E ULTRASSECRETOS A SEREM ENCAMINHADOS
Último dia útil de maio de 2016	Documentos ultrassecretos com vencimento de classificação no ano de 2016 e 2017
Último dia útil de maio de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2018
Último dia útil de junho de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2019
Último dia útil de julho de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2020
Último dia útil de agosto de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2021
Último dia útil de setembro de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2022
Último dia útil de outubro de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2023
Último dia útil de novembro de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2024
Último dia útil de dezembro de 2016	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2025
Último dia útil de janeiro de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2026
Último dia útil de fevereiro de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2027
Último dia útil de março de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2028
Último dia útil de abril de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2029
Último dia útil de maio de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2030
Último dia útil de junho de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2031
Último dia útil de julho de 2017	Documentos secretos e ultrassecretos com vencimento de classificação no ano de 2032

Último dia útil de agosto de 2017	Documentos ultrassecretos com vencimento de classificação no ano de 2033
Último dia útil de setembro de 2017	Documentos ultrassecretos com vencimento de classificação no ano de 2034
Último dia útil de outubro de 2017	Documentos ultrassecretos com vencimento de classificação no ano de 2035
Último dia útil de novembro de 2017	Documentos ultrassecretos com vencimento de classificação no ano de 2036
Último dia útil de dezembro de 2017	Documentos ultrassecretos com vencimento de classificação no ano de 2037
Último dia útil de janeiro de 2018	Documentos ultrassecretos com vencimento de classificação no ano de 2038
Último dia útil de fevereiro de 2018	Documentos ultrassecretos com vencimento de classificação no ano de 2039
Último dia útil de março de 2018	Documentos ultrassecretos com vencimento de classificação no ano de 2040
Último dia útil de abril de 2018	Documentos ultrassecretos com vencimento de classificação no ano de 2041

RESOLUÇÃO Nº 4, 27 DE ABRIL DE 2016

Dispõe sobre o Termo de Classificação de Informações de que trata o art. 31 do Decreto 7.724, de 16 de maio de 2012.

A COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES, no exercício da competência que lhe atribuem os incisos I, II e V do art.47 do Decreto nº 7.724, de 16 de maio de 2012,

RESOLVE:

Art. 1º Na elaboração dos Termos de Classificação de Informações, as autoridades classificadoras deverão observar a necessidade de motivar adequadamente o ato classificatório no campo "razões para a classificação", a fim de subsidiar de modo apropriado a revisão de que trata a Resolução nº 3 da Comissão Mista de Reavaliação de Informações, de 30 de março de 2016.

Paragrafo único - O preenchimento do campo “razões para a classificação” de que trata o caput, deverá conter as informações necessárias e suficientes à avaliação da classificação, incluindo a descrição da informação classificada.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Brasília, 27 de abril de 2016.

SÚMULAS DA CMRI

Súmula CMRI nº 1/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 1/2015

"PROCEDIMENTO ESPECÍFICO - Caso exista canal ou procedimento específico efetivo para obtenção da informação solicitada, o órgão ou a entidade deve orientar o interessado a buscar a informação por intermédio desse canal ou procedimento, indicando os prazos e as condições para sua utilização, sendo o pedido considerado atendido."

Justificativa

Esta súmula visa a consolidar entendimento firmado no âmbito da CMRI no sentido de que, na existência de canal ou procedimento específico e efetivo para obtenção da informação solicitada, presume-se satisfativa a resposta que o indique. Esta presunção, no entanto, poderá ser afastada caso o interessado comprove em seu pedido ou em sede recursal a ausência de efetividade do canal indicado. Desse modo, sempre que o órgão ou entidade demandado não disponha de procedimento em efetivo funcionamento — seja porque não haja prazos e condições pré-determinados ou porque reste demonstrada a inobservância destes —, deverá o pedido ser processado na forma de solicitação de acesso a informação.

Portanto, em que pese a natureza autônoma e não subsidiária da Lei 12.527/2011, o processo administrativo de acesso à informação não prejudicou formas específicas já constituídas de relacionamento entre Administração e administrados, devendo estas prevalecerem sempre que existentes e efetivas, em respeito ao princípio da eficiência e economicidade.

Tal entendimento foi expresso nas Decisões 11/2014 (ref. Proc. nº **12649.010650/2013-50**) e 165/2014 (ref. Proc. nº **37400.002346/2014-53**), nos quais se afirmou que o processo de acesso à informação não constitui meio idôneo para solicitar retificação de dados pessoais em processo administrativo e tampouco para a retificação de direito previdenciário, respectivamente, quando não comprovada a inexistência, ineficácia ou exaurimento dos canais específicos de relacionamento entre Administração e administrado.

Súmula CMRI nº 2/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 2/2015

"INOVAÇÃO EM FASE RECURSAL– É facultado ao órgão ou entidade demandado conhecer parcela do recurso que contenha matéria estranha: i) ao objeto do pedido inicial ou; ii) ao objeto do recurso que tiver sido conhecido por instância anterior - devendo o órgão ou entidade, sempre que não conheça a matéria estranha, indicar ao interessado a necessidade de formulação de novo pedido para apreciação da matéria pelas instâncias administrativas iniciais."

Justificativa

Esta súmula apresenta regra geral para o conhecimento de recursos interpostos no âmbito do processo administrativo de acesso à informação, segundo a qual somente deverá ser objeto de apreciação por instância superior matéria que já haja sido apreciada pela instância inferior. Nesse sentido, a alteração da matéria do pedido de acesso à informação ao longo dos recursos, quando leve ao aumento do seu escopo ou à sua mudança de assunto, poderá não ser objeto de apreciação pela instância superior, em respeito ao princípio do duplo grau de jurisdição, uma vez que o conhecimento de matéria estranha ao objeto inicial, quando

levado à apreciação somente da última instância administrativa, pode levar à sua supressão, em prejuízo do administrado.

Esta regra, no entanto, merece ser harmonizada com os princípios da instrumentalidade, da eficiência, da economicidade e da tutela da legítima confiança dos administrados. Por esta razão, diz-se que o órgão ou entidade demandada poderá optar por conhecer de parcelas de recursos que apresentem esta natureza. Assim, quando à matéria estranha ao pedido inicial corresponder questão de acesso à informação sobre cujo mérito possa o órgão ou entidade demandado facilmente se manifestar, deverá ele assim proceder, em respeito aos princípios administrativos da eficiência e da economicidade.

Ademais, a fim de resguardar a legítima confiança dos administrados, o órgão deverá sempre manifestar-se na primeira oportunidade sobre o eventual não conhecimento de parcela do recurso que contenha matéria estranha ao pedido. Assim, não poderá o órgão deixar de conhecer de matéria que tenha sido objeto de apreciação por instância inferior sob o pretexto de que tal matéria não conste no pedido original. Nesse sentido, admite-se que a apreciação da matéria poderá levar tanto ao conhecimento expresso quanto ao conhecimento tácito da parcela do recurso objeto de inovação.

Ressalta-se que a decisão pelo não conhecimento de parcela do pedido deverá conter orientação para que o interessado interponha novo pedido de informação sobre a matéria estranha ao pedido original. Além disso, naquilo que o recurso não inovar, deve o órgão ou a entidade conhecer do recurso, processando o pedido conforme determina a Lei de Acesso e seu decreto regulamentador.

Nesse sentido, já se pronunciou a CMRI expressamente por meio das Decisões nos 151/2014 (ref. Proc. nº99902.001989/2013-03), 158/2014 (ref. Proc. nº 00077.000039/2014-47), 167/2014 (ref. Proc. nº72550.000110/2014-60), 170/2014 (ref. Proc. nº 46800.004216/2013-52), 248/2014 (ref. Proc. nº99923.001372/2014-12) e 259/2014 (ref. Proc. nº 50650.002221/2014-40). Em todos estes casos, a Comissão optou por não conhecer de parcelas de recursos que inovavam em relação à matéria tratada em instâncias anteriores.

Súmula CMRI nº 3/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 3/2015

"EXTINÇÃO POR CLASSIFICAÇÃO DA INFORMAÇÃO – Observada a regularidade do ato administrativo classificatório, extingue-se o processo cujo objeto tenha sido classificado durante a fase de instrução processual, devendo o órgão fornecer ao interessado o respectivo Termo de Classificação de Informação, mediante obliteração do campo 'Razões da Classificação'."

Justificativa

Esta súmula trata dos efeitos da mudança essencial de circunstâncias decorrente da classificação da informação no curso do processo administrativo de acesso à informação. A classificação regular da informação constitui fato superveniente, cujo mérito não pode ser objeto de avaliação no curso do processo de acesso à informação. Em decorrência disso, deve o processo ser extinto, nos termos do art. 52 da Lei 9.784/1999, de aplicação subsidiária ao Decreto 7.724/2012, por força de seu art.75, afim de que o interessado possa ingressar com pedido específico de desclassificação de informação, que segue rito próprio.

É dever dos órgãos cumprir os requisitos formais e materiais para a regular classificação da informação, conforme previstos pelo Decreto nº 7.724, de 2012. Nesse sentido, se, no curso da instrução processual, a informação for irregularmente classificada, pode a CGU ou a CMRI solicitar que o órgão ou a entidade sane a irregularidade, sob pena de anulação do ato classificatório e disponibilização da informação solicitada, conforme expressado nos autos do processo nº 59900.000286/2012-74.

Tal entendimento foi expresso na Decisão 225/2014 (ref. Proc. nº 23480.034646/2013-63), na qual a CMRI, acompanhando a posição da CGU, decidiu pelo não conhecimento de recurso interposto contra decisão que extinguia processo em razão de classificação superveniente, no curso da instrução.

Súmula CMRI nº 4/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 4/2015

"PROCEDIMENTO PARA DESCLASSIFICAÇÃO – O pedido de desclassificação não se confunde com o pedido de acesso à informação, sendo ambos constituídos por ritos distintos e autuados em processos apartados. Nos termos dos artigos 36 e 37 do Decreto 7.724, de 2012, o interessado na desclassificação da informação deve apresentar o seu pedido à autoridade classificadora, cabendo recurso, sucessivamente, à autoridade máxima do órgão ou entidade classificador e, em última instância, à CMRI."

Justificativa

Esta súmula consolida entendimento segundo o qual não é possível ao interessado, no curso do processo administrativo de acesso à informação, solicitar a conversão de seu pedido de acesso em pedido de desclassificação de informação. Além de constituir-se, por si, em inovação no objeto do pedido, ambos possuem ritos distintos e não conciliáveis, visto que, se no primeiro caso o Decreto 7.724/2012, ao regulamentar a Lei 12.527/2011, estabeleceu quatro instâncias recursais, sendo duas internas e duas externas ao órgão ou entidade demandado, no segundo caso este mesmo decreto estabeleceu apenas três instâncias recursais, sendo duas internas – e não necessariamente coincidentes com aquelas previstas para o processo de acesso –, e apenas uma externa ao órgão ou entidade demandado. Desta forma, a simples conversão de uma espécie de pedido em outra acarretaria evidentes supressão de instâncias,em prejuízo da Administração, e violação ao princípio da isonomia, em prejuízo dos administrados.

Tal entendimento aplica-se, igualmente, a casos de classificação superveniente, no curso da instrução, quando então, nos termos da Súmula CMRI nº 3/2015, a autoridade decisória deverá declarar extinto o processo de acesso à informação, sem promover, de ofício ou por provocação, a sua conversão em processo de desclassificação.

O processo de desclassificação de informação deve ser protocolado pelo interessado junto ao Serviço de Informação do órgão ou entidade demandado por meio de formulário próprio, não sendo ainda possível fazê-lo, em tempo presente, por meio do Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC).

Assim já decidiu a CMRI em diversas oportunidades, conforme Decisões nºs 017/2013 (ref. Proc. nº**00075.001292/2012-76**), 191/2014 (ref. Proc. nº**00077.000106/2014-23**), 207/2014 (ref. Proc. nº**00083.000243/2014-89**), 210/2014 (Ref. Proc. nº **00077.000700/2014-14**),

213/2014 (ref. Proc. nº **08850.002175/2014-66**), 209/2014 (ref. Proc. nº **08850.002132/2014-81**), 212/2014 (ref. Proc. nº **00083.000236/2014-87**), 206/2014 (ref. Proc. nº **08850.002133/2014-25**), 2014/2014 (ref. Proc. nº **00077.000680/2014-81**), 211/2014 (ref. Proc. nº **00077.000679/2014-57**) e 215/2014 (ref. Proc. nº **00075.000816/2014-73**).

Súmula CMRI nº 5/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 5/2015

"CONHECIMENTO - AUTORIDADE QUE PROFERE DECISÃO – Poderão ser conhecidos recursos em instâncias superiores, independente da competência do agente que proferiu a decisão anterior, de modo a não cercear o direito fundamental de acesso à informação.

Justificativa

Esta súmula visa a tutelar a legítima confiança do interessado cujo recurso seja apreciado por autoridade incompetente no âmbito de processo administrativo de acesso à informação, a fim de que este não sofra limitação ao direito de revisão da decisão. Desta forma, os princípios da razoabilidade, da instrumentalidade das formas e da eficiência respaldam interpretação segundo a qual o interessado não poderá ter seu direito de acesso à informação prejudicado por ato irregular da Administração.

Neste mesmo sentido, em respeito à segurança jurídica, tampouco poderá o órgão ou entidade alegar a nulidade do ato em proveito próprio.

Tal posicionamento tem prevalecido desde o início da atuação da CMRI, estando implícito, dentre numerosas decisões, nas Decisões nos 197/2013 (ref. Proc. **00077.000613/2013-86**), em que redirecionamento irregular levou a que autoridade incompetente se manifestasse acerca de recurso, 042/2013 (ref. Proc.**60502.001471/2012-58**), em que se conheceu de recurso interposto contra decisão "apócrifa" e 119/2014 (ref. Proc. nº **16853.000448/2014-**

36), em que se conheceu de recurso contra decisão de autoridade de competência controversa à luz do Decreto 7.724/2012.

Súmula CMRI nº 6/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES**, tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 6/2015

"INEXISTÊNCIA DE INFORMAÇÃO – A declaração de inexistência de informação objeto de solicitação constitui resposta de natureza satisfativa; caso a instância recursal verifique a existência da informação ou a possibilidade de sua recuperação ou reconstituição, deverá solicitar a recuperação e a consolidação da informação ou reconstituição dos autos objeto de solicitação, sem prejuízo de eventuais medidas de apuração de responsabilidade no âmbito do órgão ou da entidade em que tenha se verificado sua eliminação irregular ou seu descaminho."

Justificativa

Esta súmula consolida entendimento segundo o qual as respostas que certifiquem a inexistência de informação objeto de solicitação de acesso.

De forma diversa, caso a instância recursal verifique que a informação estava disponível ou poderia ser recuperada, esta deverá manifestar-se sobre o mérito do recurso interposto em face da declaração de inexistência para, quando possível, opinar pelo seu provimento e determinar a produção da informação ou a reconstituição de processos e documentos perdidos ou irregularmente eliminados. Caso a produção da informação ou reconstituição de seu suporte ocorra no curso da instrução, considerar-se-á satisfeito o pleito do interessado, dando ensejo à perda do objeto do recurso.

Todavia, quando não se mostrar possível a recuperação ou consolidação da informação e a reconstituição de seu suporte, a instância revisora dará essa ciência ao interessado.

Havendo indícios da ocorrência de destruição irregular ou no descaminho do documento ou informação, deverá a instância revisora encaminhar os autos do processo à área ou aos órgãos responsáveis pela apuração de eventuais responsabilidades para fim de apuração disciplinar.

Tal entendimento foi expresso na Decisão nº 238/2014 (ref. Proc. nº **00075.000670/2014-66**), na qual a CMRI optou por não conhecer de recurso interposto por cidadã que desejava obter informações declaradas inexistentes a seu respeito. Já na Decisão nº 268/2014, (ref. Proc. nº **60502.002541/2014-57**), a CMRI declarou perdido o objeto de recurso após solicitar que o órgão demandado produzisse a informação considerada necessária ao exercício de suas competências legais.

Súmula CMRI nº 7/2015

A **COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES,** tendo em vista o disposto no inciso III do art. 10 do seu Regimento Interno, aprovado por meio da Resolução nº 1, de 21 de dezembro de 2012,

RESOLVE:

Art. 1º Fica aprovada a seguinte Súmula:

Súmula CMRI nº 7/2015

"CONSELHOS PROFISSIONAIS – Não são cabíveis os recursos de que trata o art. 16 da Lei nº 12.527, de 2011, contra decisão tomada por autoridade máxima de conselho profissional, visto que estes não integram o Poder Executivo Federal, não estando sujeitos, em consequência, à disciplina do Decreto nº 7.724/2012."

Justificativa

Votos-vista do Ministério do Planejamento, Orçamento e Gestão (MPOG) que apreciaram os recursos relativos aos processos nº 00217.000583/2014-47 e nº 00217.000302/2014-56, interpostos à Comissão Mista de Reavaliação de Informações (CMRI) na forma do art. 24 do Decreto nº 7.724 , de 16 de maio de 2012, mediante o qual os recorrentes requerem a revisão das decisões proferidas em pedidos de acesso à informação dirigidos ao Conselho Regional de Medicina Veterinária do Paraná (CRMV-PR) e ao Conselho Regional

de Química da Nona Região (CRQ/IX), respectivamente, aprovados por unanimidade pela CMRI na 30ª Reunião, ocorrida no dia 25 de março de 2015:

"Tenho a opinião de que os conselhos profissionais não integram a estrutura do Poder Executivo federal não estando a sua administração vinculada ao Estado. Acerca da questão, o Parecer Jurídico nº 0911-7.14/2014/AGD/CGU/AGU, expedido pela Consultoria Jurídica junto ao Ministério do Planejamento, Orçamento e Gestão, órgão encarregado da organização administrativa do Governo Federal (Decreto nº 8.189, de 21/01/2014), assim discorreu:

"No entanto, os conselhos profissionais não se constituem com a participação do Estado em seu órgão dirigente, que é composto integralmente por representantes da própria classe disciplinada pela entidade, eleitos por seus associados, e consequentemente são estes que também elaboram os regulamentos a serem seguidos na área de atuação da entidade. A Administração Pública não influencia suas decisões. Além disso, os recursos de que dispõe são oriundos das contribuições pagas pela respectiva categoria, não lhes sendo destinados recursos orçamentários nem fixadas despesas pela lei orçamentária anual.

Em razão das características acima apontadas, a Lei nº 9.649, de 1998 admitiu a delegação da atividade de fiscalização profissional a entidades de direito privado. Contudo, o Supremo Tribunal Federal, na Ação Direta de Inconstitucionalidade nº 1.717/DF, julgou inconstitucional o disposto no art. 58 do referido ato normativo, por entender indelegável a uma entidade privada a atividade típica de Estado, que abrange o poder de polícia, o de tributar e o de punir, no que concerne ao exercício de atividades profissionais regulamentadas, verbis:

EMENTA: DIREITO CONSTITUCIONAL E ADMINISTRATIVO. AÇÃO DIRETA DE INCONSTITUCIONALIDADE DO ART. 58 E SEUS PARÁGRAFOS DA LEI FEDERAL Nº 9.649, DE 27.05.1998, QUE TRATAM DOS SERVIÇOS DE FISCALIZAÇÃO DE PROFISSÕES REGULAMENTADAS. 1. Estando prejudicada a Ação, quanto ao § 3º do art. 58 da Lei nº 9.649, de 27.05.1998, como já decidiu o Plenário, quando apreciou o pedido de medida cautelar, a Ação Direta é julgada procedente, quanto ao mais, declarando-se a inconstitucionalidade do "caput" e dos § 1º, 2º, 4º, 5º, 6º, 7º e 8º do mesmo art. 58. 2. Isso porque a interpretação conjugada dos artigos 5º, XIII, 22, XVI, 21, XXIV, 70, parágrafo único, 149 e 175 da Constituição Federal, leva à conclusão, no sentido da indelegabilidade, a uma entidade privada, de atividade típica de Estado, que abrange até poder de polícia, de tributar e de punir, no que concerne ao exercício de atividades profissionais regulamentadas, como ocorre com os dispositivos impugnados. 3. Decisão unânime.

É importante atentar que o precedente em tela se trata de decisão proferida em processo objetivo, no qual, portanto, não foram analisadas todas as peculiaridades inerentes ao regime jurídico a ser considerado em relação aos conselhos de fiscalização profissional, bem como a

análise da constitucionalidade do modelo já posto, restringindo-se o âmbito de discussão, neste julgamento, à matéria disposta no art. 58, caput e §§ 1º, 2º, 4º, 5º, 6º, 7º e 8º da lei impugnada.

Segundo Carlos Ari Sundfeld e Jacintho Arruda Câmara:

"Para classificar tais entidades de modo adequado é necessário considerar todas as suas características. O equívoco que se observa em boa parte das propostas de interpretação está em privilegiar um tipo de característica em detrimento de outro. Como não se encontra, entre as categorias tradicionais de classificação, um modelo que apresente as peculiaridades das entidades de fiscalização profissional, acaba-se estabelecendo uma dicotomia, na qual só restaria como opção enquadrá-las como parte da Administração indireta ou como entidade privada.

A superação desse impasse se dá com a separação de duas realidades distintas: a natureza pública, de um lado, e a estatal, de outro. Todavia, por vezes esta distinção é esquecida. De um modo geral se pretende vincular a natureza de direito público à estrutura burocrática que integra o Estado. A premissa da qual se parte é a de que, por ser público, o ente também seria, necessariamente, estatal. A recíproca também é tida como verdadeira. Desta outra forma entende-se que se não for estatal, o ente só poderia ostentar natureza jurídica de direito privado.

Acontece que não há relação necessária entre possuir natureza de direito público e integrar a estrutura estatal. Deveras, não é todo ente estatal que apresenta regime jurídico de direito público, bem como não é necessário que todo ente público faça parte da estrutura estatal.

(...)

Referidas entidades são públicas por determinação da própria lei que as instituiu. A razão para atribuir esse regime jurídico é fácil de identificar. Algumas das funções para as quais essas entidades foram criadas envolvem o exercício de poder de autoridade, atributo típico de Poder Público. Tais competências dizem respeito, por exemplo, à habilitação de pessoas para o exercício profissional, à edição de regulamentos sobre práticas profissionais, à aplicação de sanções disciplinares, entre outras.

Prerrogativas e sujeições tipicamente públicas também lhes foram atribuídas. As entidades são autorizadas por lei a cobrar anuidades de seus membros, podendo, no caso de inadimplência, lançar mão de execução fiscal; gozam de imunidade de impostos; sujeitam-se a controle do Tribunal de Contas, para citar alguns exemplos de aplicação mais freqüente e incontroversa do regime jurídico de direito público.

Nada disso, porém, significa dizer que as entidades de fiscalização profissional foram tratadas por lei como parte integrante da Administração. Muito pelo contrário. Acompanhando uma tendência presente no direito comparado, a regulação das atividades profissionais no Brasil foi atribuída a entidades de caráter corporativo, com personalidade de direito público, mas visivelmente destacadas da estrutura burocrática estatal."[1]

Com efeito, os conselhos profissionais são regidos por um regime jurídico especial que os diferencia das típicas autarquias. Isto porque, ao contrário destas, são dotados, como aduz Diogo

de Figueiredo Moreira Neto, de "total autonomia em relação à entidade política matriz".[2] No ponto, vale citar a lição de Lucas Rocha Furtado, que reconhece, assim como Carlos Ari Sundfeld e Jacintho Arruda Câmara, que as entidades em comento não integram a Administração Pública:

"Dado que são autarquias, a elas se aplica o Direito Público, porém, em função de particularidades que lhes são próprias, de forma mitigada. A Constituição Federal dispõe, por exemplo, que a criação de cargos, empregos ou funções públicas depende de lei. Seria, portanto, necessária a aprovação de lei federal para criar um emprego de secretária ou ascensorista ou qualquer outro para o Conselho de Educação Física, por exemplo?

Parece-nos que a observância das normas públicas não pode ocorrer de forma plena ou absoluta sob pena de se mostrar, por vezes, totalmente absurda.

São autarquias especiais. A sua especialidade – e neste ponto não podem ser confundidas com as autarquias em regime especial – está no fato de que não integram a Administração Pública. Elas não se subordinam ou vinculam a nenhuma outra entidade. No desempenho de suas atribuições, devem dispor de plena e absoluta liberdade administrativa, gerencial, financeira, orçamentária, tendo como limite a lei que as criou e os princípios constitucionais."[3]

Veja-se que a particular disciplina a que se submetem os conselhos de fiscalização profissional não é idêntica àquela das típicas autarquias públicas, mas é outra, de natureza híbrida, em que até lhe são aplicáveis algumas normas de direito público, mas sem lhes retirar a característica essencial da ampla independência, autonomia e atuação desatrelada da administração pública federal, o que as aproxima das entidades paraestatais. Pode-se afirmar, portanto, que os conselhos profissionais não se submetem às mesmas normas que regem as entidades que tradicionalmente integram administração pública indireta.

Nesse sentido, transcrevo alguns trechos do voto do Ministro Maurício Corrêa, por ocasião do julgamento do MS nº 21.797/RJ:

"Mesmo que esses Conselhos sejam autarquias, segundo a definição de uns, porém nunca deixarão de ser **autarquias corporativas peculiares**, em seu sentido particularíssimo, contudo, jamais aquelas especiais integrantes indiretas do Serviço Público, como tal organizado em carreira à imagem do estampado dogmaticamente na Constituição.

(...)

Seria um contra-senso que a ação estatal **se fizesse em setor de exclusiva atuação da iniciativa privada**, para impor o cumprimento de certo regime para os seus empregados, de que defluiriam prerrogativas, privilégios, ônus e encargos, que ao Estado não é dado constranger ao ente paraestatal a que o faça. Nenhuma lei criou cargos públicos em Conselhos Profissionais, e seria absolutamente inadmissível, inconcebível e ininteligível mesmo, que por uma interpretação analógica e ampliativa, viesse o Estado a exigir que essa categoria de empregados se convertesse em servidores públicos, circunstância que por si só já acarretaria a ele mesmo, pesados ônus, decorrentes das conseqüências dessa absurda metamorfose."

Em posição semelhante, dispôs o Tribunal de Contas da União, no recurso de reconsideração do Conselho Regional de Nutrição da 5ª Região, TC 010.983/2000-6, contra a decisão prolatada na sessão de 31.10.2000 (relação nº 80/2000), Acórdão nº 042/2002, 1ª Câmara: "...a posição reiterada dessa Corte tem sido no sentido de que os conselhos profissionais encontram-se obrigados a promover concurso publico previamente à contratação de pessoal. No sentido dessas decisões, concurso público é, dentre outras características, aquele amplamente divulgado ao conhecimento público, no qual restem pública e previamente estabelecidos os requisitos para candidatura e a sistemática de avaliação dos candidatos, e garantam objetividade na avaliação. Não há como considerar que meros processos seletivos de publicidade e isonomia limitados, atendem aos ditames constitucionais incidentes sobre entidades regidas pelo direito público (art. 37, inciso II, da CF). Ressalto, aqui, não se estar afirmando que os conselhos devem promover concurso público nos moldes da Lei n. 8.112/90, mas sim conforme determinação e princípios constitucionais, nos moldes, por exemplo, daqueles já promovidos por diversas empresas estatais."

Pode-se concluir que o regime a que estão submetidos os conselhos profissionais não se adequam completamente às prescrições constitucionais pertinentes ao regime jurídico das entidades de direito público que integram a Administração Pública, bem como não se compatibiliza com a disciplina prevista no Decreto-Lei nº 200/67.

Os conselhos de fiscalização profissional não foram concebidos como entes vinculados ao Estado, e dessa forma se desenvolveram, sem qualquer ingerência estatal em relação à estrutura, administração, com seus dirigentes eleitos diretamente pelos próprios associados, o mesmo ocorrendo quanto à sua receita, não estando submetidas a qualquer controle por parte da administração centralizada, apenas ao controle externo, ligado aos poderes Judiciário e Legislativo, mas sem vincular-se ou subordinar-se a qualquer órgão público, portanto, sem admitir qualquer influência do Estado na sua administração.

Com efeito, seu desenvolvimento como entidades corporativas fechadas, com estrutura e funcionamento completamente apartado da administração pública federal, demonstra ainda uma independência ampla do Estado, não apenas nos seus aspectos estruturais, ligados à sua organização, completamente alheios à disciplina prevista no Decreto-Lei nº 200, de 1967, mas também quanto ao regime jurídico aplicado em relação aos seus bens, receitas, despesas, finanças, contabilidade, compras, contratos e pessoal."

Pelos fundamentos expostos, a natureza pública das entidades de fiscalização profissional não implica que integrem a estrutura do Estado nem tampouco que façam parte do Poder Executivo federal.

Em consequência, o Decreto nº 7.724, de 2012, que regula os procedimentos de garantia do acesso às informações no âmbito do Poder Executivo federal, é inaplicável no caso concreto.

No que toca à aplicabilidade da Lei nº 12.527, de 2011 aos conselhos profissionais, embora seu art. 1º, que trata de sua abrangência subjetiva, não tenha feito menção expressa a estes órgãos, declara que se trata do regulamento legal do inciso XXXIII do art. 5º da Constituição Federal que dispõe acerca do direito à informação a ser obtida perante os órgãos de natureza pública. Portanto, entendo pela aplicabilidade das regras legais aos conselhos profissionais que detém autonomia para regular seus procedimentos internos na forma como entenderem cabível."

Assim, apesar de geralmente constituídas sob a forma de autarquias, o que resulta na submissão ao regime de acesso à informação previsto na Lei de Acesso a Informação, a natureza pública singular das entidades de fiscalização profissional não implica que integrem a estrutura do Estado nem tampouco que façam parte do Poder Executivo federal, de modo que não cabe atribuir à CGU e à CMRI o poder revisional das respostas a pedidos de acesso às informações proferidas por conselhos profissionais.

Diante disso, a CMRI entende ser aplicável a Lei de Acesso à Informação (Lei nº 12.527/2012) aos conselhos profissionais, não sendo aplicável, contudo, os recursos de que tratam o art. 16 da Lei às decisões exaradas pelas autoridades máximas dos conselhos profissionais. Igualmente inaplicável a esses órgãos é o Decreto nº 7.724, de 2012, que regulamenta, no âmbito do Poder Executivo federal, a Lei de Acesso a Informação.

_____

[1] SUNDFELD, Carlos Ari; CÂMARA, Jacintho Arruda. Conselhos de fiscalização profissional: entidades públicas não-estatais, in RDE – Revista de Direito do Estado, SP, nº 4, out/dez/06, p. 321/33.

[2] MOREIRA NETO, Diogo de Figueiredo. Curso de Direito Administrativo. Rio de janeiro: Forense, 2014, p. 284.

[3] FURTADO, Lucas Rocha. Curso de Direito Administrativo. Belo Horizonte: Editora Forum, 2012, p. 160.

INSTRUÇÕES NORMATIVAS E NORMAS COMPLEMENTARES

INSTRUÇÕES NORMATIVAS E NORMAS COMPLEMENTARES DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - DSIC

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

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

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

Art. 3 º 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; Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013.

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 Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013. 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. 8 º 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. 9 º 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. Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013.

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

Norma Complementar nº 01/IN02/NSC/GSI/PR, DE 27 DE JUNHO DE 2013

Disciplina o Credenciamento de Segurança de pessoas naturais, órgãos e entidades públicas e privadas para o trâmite de informações classificadas.

1 OBJETIVO

Disciplinar o processo de credenciamento de segurança de pessoas naturais, bem como de órgãos e entidades públicas e privadas, como órgãos de registro e postos de controle,

para o tratamento de informações classificadas, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

2 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no caput do art. 37 e inciso I da Lei nº 12.527, de 2011 e no caput do art. 6º e inciso I do Decreto nº 7.845, de 2012, compete ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR, por meio do Núcleo de Segurança e Credenciamento - NSC, na qualidade de Órgão de Registro Central, promover e propor a regulamentação do credenciamento de segurança de pessoas naturais para o tratamento de informações classificadas, em qualquer grau de sigilo.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar, aplicam-se os seguintes termos e definições:

3.1 Ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.
3.2 Credencial de segurança: certificado que autoriza pessoa para o tratamento de informação classificada;
3.3 Credenciamento de segurança: processo utilizado para habilitar órgão ou entidade, pública ou privada, ou ainda para credenciar pessoas para o tratamento de informação classificada.
3.4 Gestor de Segurança e Credenciamento - GSC: responsável pela segurança da informação classificada em qualquer grau de sigilo nos órgãos de registro e postos de controle, devidamente credenciado.
3.5 Gestão de riscos de segurança da informação e comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
3.6 Habilitação de segurança: condição atribuída a um órgão ou entidade pública ou privada, que lhe confere a aptidão para o tratamento da informação classificada em determinado grau de sigilo.

3.7 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.
3.8 Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.
3.9 Inspeção para habilitação de segurança: averiguação da existência dos requisitos indispensáveis à habilitação de segurança de órgãos e entidades para o tratamento de informação classificada.
3.10 Investigação para credenciamento de segurança: averiguação da existência dos requisitos indispensáveis para a concessão da credencial de segurança às pessoas naturais, para o tratamento de informação classificada.
3.11 Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa tenha acesso à informação classificada, em qualquer grau de sigilo;
3.12 Núcleo de Segurança e Credenciamento - NSC: Órgão de Registro Central, instituído no Gabinete de Segurança Institucional da Presidência da República;
3.13 Órgão de Registro Nível 1 - ORN1: ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento.
3.14 Órgão de Registro Nível 2 - ORN2: órgão ou entidade pública vinculada a órgão de registro nível 1 e por este habilitado.
3.15 Posto de Controle - PC: unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento e controle de informação classificada em qualquer grau de sigilo, no âmbito de sua atuação.
3.16 Quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento ou no risco de comprometimento de informação classificada em qualquer grau de sigilo.
3.17 Tratamento da informação classificada: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do processo de credenciamento de segurança de pessoas naturais, de órgãos e entidades públicas e privadas, como órgãos de registro e postos de controle para o tratamento de informações classificadas devem considerar, priorita-

riamente, os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do órgão ou entidade do Poder Executivo Federal, além do que, devem necessariamente estar alinhadas à Instrução Normativa GSI/PR nº 02, de 2013, ao Decreto nº 7.724, de 2012, ao Decreto nº 7.845, de 2012 e às normas em vigor que tratem do assunto.

4.2 O processo de credenciamento de segurança deve subsidiar o órgão ou entidade do Poder Executivo Federal a fim de conhecer, valorizar, proteger e manter seus ativos de informação classificadas, em conformidade com os requisitos legais e do negócio.

4.3 O processo de credenciamento de segurança deve produzir subsídios tanto para a gestão de riscos aos ativos de informação classificada, quanto para a continuidade das ações, nos aspectos relacionados à segurança da informação e comunicações.

4.4 Os órgãos e entidades públicas poderão ser habilitados para o tratamento de informação classificada, em qualquer grau de sigilo, pelo Núcleo de Segurança e Credenciamento ou pelos Órgãos de Registro Nível 1, com os quais possuam vínculo.

4.5 As entidades privadas poderão ser habilitadas como postos de controle para o tratamento de informação classificada, em qualquer grau de sigilo, pelo Núcleo de Segurança e Credenciamento ou pelos Órgãos de Registro Nível 1, desde que possuam vínculo de qualquer natureza com os mesmos.

4.6 Quando o tratamento da informação classificada em qualquer grau de sigilo, envolver país ou organização estrangeira, a habilitação de segurança da empresa privada brasileira somente poderá ser realizada se houver algum tratado, acordo, memorando de entendimentos ou ajuste técnico, específico para troca de informação classificada, firmado entre o país ou organização estrangeira e a República Federativa do Brasil, conforme previsto no art. 16 do Decreto nº 7.845, de 2012.

5 CREDENCIAMENTO DE SEGURANÇA DE PESSOAS NATURAIS

O credenciamento de segurança de pessoas naturais é um processo que será realizado pelo Núcleo de Segurança e Credenciamento e pelos órgãos de registro.

5.1 A credencial de segurança será concedida para pessoa natural somente nos casos em que houver a necessidade de conhecer informações classificadas, em qualquer grau de sigilo, conforme estabelecido em normatização interna do órgão ou entidade do Poder Executivo Federal ao qual a pessoa a ser credenciada estiver vinculada.

5.2 A credencial de segurança estará sempre associada à informação classificada que a pessoa natural tem necessidade de conhecer e com prazo de validade preestabelecido, não superior a dois anos, levando-se em consideração as informações contidas no documento de indicação, citadas no item 5.5.1.2 desta Norma.

5.3 A pessoa natural poderá receber credencial de segurança, desde que atendidos ainda os seguintes requisitos:

5.3.1 Solicitação formal por qualquer autoridade referida no art. 9º da Instrução Normativa GSI/PR nº 02, de 2013, ou no § 2º do art. 30 do Decreto nº 7.724, de 2012, ao Gestor de Segurança e Credenciamento do órgão de registro da autoridade solicitante.

5.3.1.1 O Gestor de Segurança e Credenciamento poderá também dar início ao processo de credenciamento das pessoas naturais vinculadas ao seu respectivo órgão de registro, uma vez detectada a necessidade de conhecer.

5.3.1.2 Quando a pessoa natural for de entidade privada, a solicitação formal deverá ser realizada pelo diretor estatutário ou Gestor de Segurança e Credenciamento da mesma, ao GSC do Órgão de Registro Nível 1 com o qual mantenha vínculo de qualquer natureza.

5.3.2 Preenchimento do Formulário Individual de Dados para Credenciamento - FIDC, conforme modelo constante do Anexo A desta Norma, devidamente assinado.

5.3.3 Ser aprovada na investigação para credenciamento pelo órgão de registro com o qual mantenha vínculo de qualquer natureza.

5.4 Quando a necessidade de conhecer estiver relacionada à troca ou tratamento de informação classificada em qualquer grau de sigilo com país ou organização estrangeira, o credenciamento de segurança da pessoa natural somente poderá ser realizado se houver algum tratado, acordo, memorando de entendimentos ou ajuste técnico, específico para troca de informação classificada, firmado entre o país ou organização estrangeira e a República Federativa do Brasil, conforme previsto no art. 16 do Decreto nº 7.845, de 2012.

5.5 O processo de credenciamento de pessoas naturais deverá seguir as seguintes fases:

5.5.1 Fase da indicação

5.5.1.1 A fase de indicação do processo de credenciamento inicia-se com a solicitação formal citada no item 5.3.1 desta Norma, com a identificação por parte da autoridade indicadora, da pessoa que tem necessidade de conhecer.

5.5.1.2 No documento de indicação deverão constar o grau de acesso à informação classificada pretendido, o documento referido no item 5.3.2 desta Norma, as atividades/funções a serem desenvolvidas pelo indicado que demandem o acesso à informação classificada, o prazo estimado de exercício, bem como a justificativa da autoridade indicadora para a necessidade de conhecer documentos classificados por parte da pessoa a ser credenciada e outras informações julgadas pertinentes.

5.5.1.3 O documento de indicação passa a compor o processo de credenciamento de segurança e será considerado documento pessoal, tratado conforme Seção V,

do Capítulo IV, da Lei nº 12.527, de 2011 e Seção IV, do Capítulo III, do Decreto nº 7.845, de 2012.

5.5.1.4 O órgão de registro, de posse da demanda de credenciamento, verificará a conformidade e pertinência do processo e poderá então iniciar a fase de investigação de segurança.

5.5.2 Fase da investigação de segurança

5.5.2.1 A investigação de segurança tem como objetivo identificar o nível do risco potencial de quebra de segurança ao se permitir que a pessoa indicada acesse informação classificada no grau de sigilo indicado.

5.5.2.2 A investigação de segurança deverá ser realizada por órgão ou entidade pública competente para tal, integrante ou não da própria estrutura organizacional do órgão de registro solicitante, observado o disposto no parágrafo único do art. 8º e art. 14 do Decreto nº 7.845, de 2012.

5.5.2.3 De posse do processo de credenciamento encaminhado pelo órgão de registro solicitante, o órgão encarregado da investigação para credenciamento dará início a esta fase após conferir a documentação recebida e constatar a expressa autorização do indicado para realizar a investigação para o credenciamento.

5.5.2.4 O relatório de investigação será anexado ao processo de credenciamento de segurança, também tratado como informação pessoal, no qual constará parecer do responsável técnico, fundamentado no perfil do indicado, por intermédio de análise dos autos da investigação, indicando, em função do nível do risco potencial de quebra de segurança constatado, se o indicado está apto ou não para o credenciamento de segurança no grau solicitado.

5.5.2.5 Os autos e peças componentes da investigação serão realizados por servidor público ocupante de cargo efetivo ou militar de carreira, com competência profissional comprovada para atuar na área de inteligência, por policial ou por perito criminal, ou ainda, por profissionais de saúde, no caso de pareceres técnicos específicos desta área, a critério do responsável pelo relatório da investigação.

5.5.2.6 A investigação deverá avaliar, no mínimo, dados dos seguintes aspectos pessoais do indicado:

a) envolvimento com pessoas ou organizações associadas ao crime, terrorismo, tráfico, sabotagem e espionagem;

b) situação fiscal;

c) dados relacionados à situação criminal, cível e administrativa; e

d) situação eleitoral e do serviço militar.

5.5.2.7 Os autos da investigação deverão ser arquivados no órgão encarregado da investigação e tratados como documento pessoal, conforme Seção V, do Capítulo IV da Lei nº 12.527, de 2011, e Seção IV do Capítulo III do Decreto nº 7.845, de 2012.

5.5.2.8 O Relatório de Investigação - RI deverá ser anexado ao processo de credenciamento e encaminhado ao órgão de registro demandante, sendo tratado como documento pessoal, conforme Seção V do Capítulo IV da Lei nº 12.527, de 2011 e Seção IV do Capítulo III do Decreto nº 7.845, de 2012.

5.5.3 Fase do credenciamento

5.5.3.1 O ato do credenciamento é a homologação da permissão para o tratamento da informação classificada no grau solicitado, contudo, não exime o credenciado das responsabilidades administrativas, cíveis e penais quanto à manutenção da segurança dos ativos de informação classificada tratados, conforme legislação pertinente.

5.5.3.2 A credencial de segurança é concedida pela alta administração do órgão de registro, podendo ser delegado o ato de concessão, a critério da mesma, para o Gestor de Segurança e Credenciamento do órgão de registro, sendo vedada a subdelegação.

5.5.3.3 Com base no RI e em outras informações que se fizerem úteis, o órgão de registro poderá expedir a credencial solicitada, considerando o risco à segurança, o grau de acesso, o tempo de acesso e a necessidade de conhecer.

5.5.3.4 Conforme estabelecido por normatização interna do órgão de registro, a credencial de segurança, poderá ser publicada em ato administrativo do órgão, ou ainda, se necessária a sua materialização, expedida na forma impressa ou eletrônica, sendo neste caso considerada como material de acesso restrito.

5.5.3.5 Quando a atividade do credenciado for externa ao órgão ou entidade ao qual pertence e caso haja exigência de comprovação do credenciamento, poderá ser expedido um Certificado de Credencial de Segurança - CCS, conforme modelo constante do Anexo B a esta Norma, do qual constarão os dados previstos no item **5.5.3.8** com a aplicação do Selo Nacional sobre a assinatura.

5.5.3.6 A credencial de segurança deverá ser numerada em sequência anual, no âmbito do órgão de registro emissor.

5.5.3.7 O órgão de registro deverá informar a concessão da credencial de segurança à autoridade solicitante.

5.5.3.8 A credencial de segurança deverá conter no mínimo os seguintes dados:

a) número da credencial;

b) nome completo, número de registro ou de identidade e número de inscrição no Cadastro de Pessoas Físicas do Ministério da Fazenda (CPF) do credenciado;

c) órgão ou entidade com o qual o credenciado mantém vínculo;

d) cargo ou função do credenciado;

e) grau de acesso à informação classificada (Reservado, Secreto ou Ultrassecreto);
f) finalidade da credencial;
g) data prevista para o término de validade da credencial;
h) data de expedição da credencial; e
i) identificação da autoridade que emitiu a credencial.

5.5.3.9 A credencial de segurança, juntamente com o seu respectivo processo, deverá ser armazenada no órgão de registro que a emitiu, sendo facultativo o uso de ferramentas de tecnologia da informação para este fim, desde que atendidos os requisitos mínimos de segurança previstos na legislação vigente.

5.6 A credencial de segurança poderá ser renovada ao término de sua validade, desde que obedecido o processo descrito nos itens 5.5.1, 5.5.2 e 5.5.3 da presente norma, sendo vedada a sua prorrogação.

5.6.1 É admitida a antecipação do processo de renovação da credencial de segurança, a critério do órgão de registro, para evitar a descontinuidade do credenciamento com o término de sua validade.

5.7 Os postos de controle deverão manter os registros atualizados de todas as credenciais de segurança emitidas para as pessoas naturais sob sua responsabilidade.

6 HABILITAÇÃO DE SEGURANÇA DE ÓRGÃO DE REGISTRO NÍVEL 1

6.1 A habilitação de segurança será concedida pelo NSC, para os ministérios ou órgãos públicos de nível equivalente que identificarem a necessidade de tratamento de informações classificadas, em qualquer grau de sigilo, mediante demanda a qualquer tempo.

6.2 A alta administração dos ministérios ou dos órgãos públicos de nível equivalente, requisitante da habilitação de segurança, formalizará sua intenção ao Gabinete de Segurança Institucional da Presidência da República – GSI/PR, incluindo a designação do Gestor de Segurança e Credenciamento, bem como seu suplente, conforme inciso II do art. 10 do Decreto nº 7.845, de 2012.

6.3 A designação do Gestor de Segurança e Credenciamento, e respectivo suplente, será considerada como documento de indicação para o credenciamento segurança, no grau ultrassecreto, dos indicados.

6.4 O NSC realizará o primeiro credenciamento de segurança do Gestor de Segurança e Credenciamento, e seu suplente, conforme processo previsto no item 5 desta Norma Complementar.

6.4.1 Os servidores designados para Gestor de Segurança e Credenciamento e suplente deverão encaminhar ao NSC o Formulário Individual de Dados para Credenciamento - FIDC, constante do Anexo A desta Norma, devidamente preenchido e assinado.

6.4.2 Após a habilitação de segurança do ORN1, os Gestores de Segurança e Credenciamento e suplentes subsequentes serão credenciados pelo próprio órgão de registro, conforme estabelecido por normatização interna do órgão e entidade do Poder Executivo Federal, observando a legislação específica em vigor.

6.4.3 A substituição do Gestor de Segurança e Credenciamento dos ORN1, por qualquer motivo, deve ser informada ao NSC, identificando o substituto e seus respectivos dados de contato.

6.5 O NSC informará ao órgão demandante a homologação da credencial de segurança do Gestor de Segurança e Credenciamento e seu suplente.

6.6 O GSC credenciado dará então prosseguimento ao credenciamento de segurança do seu Órgão de Registro Nível 1 solicitando a habilitação do posto de controle de acordo com o item 8 desta Norma.

7 HABILITAÇÃO DE SEGURANÇA DE ÓRGÃO DE REGISTRO NÍVEL 2

7.1 A habilitação de segurança será concedida pelo ORN1, para seus órgãos e entidades públicas vinculadas que necessitarem tratar informações classificadas em qualquer grau de sigilo. A habilitação de segurança poderá ser concedida mediante demanda a qualquer tempo do órgão interessado ou por determinação do ORN1, por intermédio do credenciamento de segurança.

7.2 A alta administração do órgão requisitante do credenciamento de segurança formalizará a intenção de habilitação de segurança para a alta administração do ORN1, incluindo a designação do respectivo Gestor de Segurança e Credenciamento e seu suplente, conforme inciso II do art. 10 do Decreto nº 7.845, de 2012, bem como a respectiva categoria de credencial de segurança pretendida para os mesmos.

7.2.1 No caso da determinação de habilitação de segurança como ORN2, a alta a dministração do órgão a ser habilitado designará o Gestor de Segurança e Credenciamento e seu suplente e informará ao ORN1 para anuência e prosseguimento do processo.

7.3 A designação do Gestor de Segurança e Credenciamento, e respectivo suplente, será considerada como documento de indicação para o credenciamento de segurança dos indicados, no grau de acesso solicitado.

7.4 O ORN1 realizará o credenciamento de segurança do primeiro Gestor de Segurança e Credenciamento, titular e suplente, conforme previsto no item 5 desta Norma Complementar.

7.4.1 Os servidores designados para Gestor de Segurança e Credenciamento, titular e suplente, deverão encaminhar ao ORN1 o Formulário Individual de Dados para Credenciamento, constante do Anexo A desta Norma Complementar, devidamente preenchido e assinado.

7.4.2 O Órgão de Registro Nível 1 informará ao Órgão de Registro Nível 2 a homologação da credencial de segurança do Gestor de Segurança e Credenciamento e seu suplente.

7.4.3 Após a habilitação de segurança do ORN2, os Gestores de Segurança e Credenciamento, titulares e suplentes subsequentes, serão credenciados pelo próprio ORN2, conforme estabelecido por normatização interna do órgão ou entidade do Poder Executivo Federal, observando a legislação específica em vigor.

7.4.4 A substituição do Gestor de Segurança e Credenciamento do ORN2, por qualquer motivo, deve ser informada imediatamente ao ORN1, identificando o substituto e seus respectivos dados de contato.

7.5 O GSC credenciado dará então prosseguimento ao credenciamento de segurança do ORN2 solicitando a habilitação de segurança do posto de controle de acordo com o item 8 desta Norma.

8 HABILITAÇÃO DE SEGURANÇA DE POSTO DE CONTROLE DE ÓRGÃO OU ENTIDADE PÚBLICA.

8.1 A habilitação de segurança de Posto de Controle será concedida, a critério dos órgãos de registro e em sua área de atuação, para os órgãos e entidades públicas que com eles mantenham vínculo de qualquer natureza e que tratarem informações classificadas, em qualquer grau de sigilo.

8.2 Cada órgão de registro deverá possuir pelo menos um Posto de Controle.

8.3 O primeiro PC de cada Órgão de Registro Nível 1 será habilitado pelo NSC, e os postos de controle subsequentes, quando necessários, serão habilitados pelos próprios ORN1.

8.4 Os Postos de Controle de ORN2 serão sempre habilitados por um ORN1 com o qual mantenha vínculo de qualquer natureza.

8.5 O Posto de Controle deverá possuir a seguinte qualificação técnica mínima:

a) estar localizado em área de acesso restrito, conforme disposto nos artigos 42, 43, 44 e 45 do Decreto nº 7.845, de 2012 ;

b) possuir meios de armazenamento de documentos físicos e eletrônicos com nível de segurança compatível com os graus de sigilo e volume;

c) possuir estrutura física adequada para o armazenamento e preservação dos documentos físicos e eletrônicos;

d) possuir planos e procedimentos de contingência de forma a assegurar a continuidade dos processos essenciais no caso de falhas ou sinistros;

e) possuir meios de comunicação segura compatível com os graus de sigilo;

f) possuir suas redes de dados e seus sistemas de tecnologia da informação adequadamente protegidos de ataques eletrônicos;
g) possuir sistemas alternativos de proteção da infraestrutura crítica relacionada com os ativos de informação e materiais de acesso restrito sob sua responsabilidade de armazenamento e controle;
h) atender aos princípios de disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação e materiais de acesso restrito sob sua responsabilidade;
i) possuir protocolo exclusivo para documentos classificados, e quando necessário, de Documentos Controlados;
j) possuir restrição ao uso de máquinas fotográficas, gravadores de vídeo e áudio, ou similares, tais como câmeras de dispositivos móveis no interior das instalações do PC;
k) possuir quadro de pessoal capacitado para o tratamento de informação classificada; e
l) possuir recurso criptográfico para armazenamento e transmissão da informação classificada em conformidade com a Instrução Normativa GSI/PR nº 3, de 2013.

8.6 O processo de habilitação de segurança do primeiro Posto de Controle de Órgão de Registro Nível 1 é iniciado por solicitação do seu GSC, previamente credenciado, ao NSC. Os demais postos de controle, quando necessários, serão habilitados pelo próprio ORN1.

8.7 O processo de habilitação de segurança de Posto de Controle de Órgão de Registro Nível 2 é iniciado por solicitação do seu GSC, previamente credenciado, ao ORN1 com o qual mantém vínculo de qualquer natureza.

8.8 O documento de solicitação deverá indicar o endereço do Posto de Controle, meios de contato, bem como a declaração expressa da total aderência às qualificações técnicas necessárias à segurança da informação classificada, previstas no item 8.5 desta Norma, e ainda, quando o PC estiver geograficamente afastado do órgão de registro, os dados do responsável pelo mesmo, previamente credenciado.

8.9 O Gestor de Segurança e Credenciamento do órgão a ser habilitado é o responsável pela verificação da qualificação técnica prevista no item 8.5 desta Norma, sob pena de responsabilidade.

8.10 O NSC e os Órgãos de Registro Nível 1 prestarão o apoio técnico necessário para a implementação e funcionamento dos postos de controle vinculados, incluindo visitas técnicas mediante solicitação do órgão interessado.

8.11 O NSC e órgãos de registro poderão, a seu critério, realizar inspeções para a verificação da qualificação técnica, a qualquer tempo, nos Postos de Controle por eles habilitados.

8.12 O documento de solicitação citado no item 8.8 desta Norma comporá o processo de habilitação de segurança do Posto de Controle.

8.13 O NSC ou o Órgão de Registro Nível 1, com base na análise do processo de habilitação de segurança e outras informações julgadas pertinentes, poderá homologar

a habilitação de segurança dos Postos de Controle a eles vinculados, ou diligenciar para a adequação do processo.

8.14 O NSC ou o ORN1, conforme o caso, informará a habilitação de segurança do PC ao órgão solicitante.

8.15 O processo de habilitação de segurança será arquivado no Posto de Controle do órgão de registro que homologou a habilitação.

9 HABILITAÇÃO DE SEGURANÇA DE ENTIDADE PRIVADA.

9.1 O Órgão de Registro Nível 1 concederá a habilitação de segurança para entidade privada com a qual mantenha vínculo de qualquer natureza e que necessite tratar informação classificada em qualquer grau de sigilo, bem como, possua expectativa de assinatura de contrato sigiloso, previsto na Seção IX do Capítulo III do Decreto nº 7.845, de 2012, protocolo ou carta de intenções firmada com órgãos ou entidades públicas em sua área de atuação.

9.2 A direção estatutária da entidade privada formalizará a intenção de habilitação de segurança de sua empresa ao GSC do órgão ou entidade pública, com o qual mantenha vínculo de qualquer natureza, encaminhando ao mesmo os seguintes documentos probatórios da regularidade fiscal e expectativa de assinatura de contrato sigiloso, previstos nos incisos I e III do art. 11 do Decreto nº 7.845, de 2012:

a) prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ) atualizado;

b) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

c) organograma atualizado ou documento que identifique os reais controladores da empresa;

d) Certidão Negativa de Débitos de Tributos e Contribuições Federais (Receita Federal);

e) certidão quanto à Dívida Ativa da União (Procuradoria-Geral da Fazenda Nacional);

f) Certidão Negativa de Débitos (INSS);

g) certidão de regularidade do FGTS (Caixa Econômica Federal);

h) prova de inscrição no cadastro de contribuintes estadual e municipal, se houver, relativo ao domicílio ou sede da empresa;

i) prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede da empresa;

j) protocolo ou carta de intenções, contendo o objeto do contrato, duração e grau de sigilo envolvido; e

k) a natureza da informação classificada, bem como a necessidade do seu tratamento.

9.3 A direção estatutária da entidade privada deverá também designar as pessoas que atuarão como GSC, titular e suplente, da empresa, conforme estabelecido no inciso IV do art. 11 do Decreto nº 7.845, de 2012, providenciando o credenciamento de segurança das mesmas, conforme previsto no item 5 desta Norma.
9.4 A substituição do Gestor de Segurança e Credenciamento titular ou suplente da empresa, por qualquer motivo, deverá ser informada imediatamente ao ORN1, para fins de credenciamento de segurança do substituto, conforme previsto no item 5 desta Norma.
9.5 Após conferência, análise e aprovação dos documentos probatórios apresentados, o ORN1 proporá à entidade privada um período para a realização da inspeção para habilitação de segurança na empresa.
9.6 O Órgão de Registro Nível 1 designará uma equipe de inspeção para habilitação de segurança da empresa que será acompanhada pelo Gestor de Segurança e Credenciamento da mesma.
9.7 A equipe de inspeção para habilitação de segurança verificará, em loco, as instalações destinadas para o Posto de Controle da entidade privada quanto ao atendimento da qualificação técnica mínima necessária ao tratamento de informação classificada, previsto no inciso II do art. 11 do Decreto nº 7.845, de 2012, de acordo com o item 8.5 desta Norma.
9.8 A inspeção será finalizada com relatório substanciado, anexado ao processo de habilitação de segurança, no qual constará parecer fundamentado na análise dos autos da inspeção, indicando, em função do nível do risco potencial de quebra de segurança constatado, se a empresa está aprovada ou não na habilitação de segurança.
9.9 O relatório de inspeção deverá ser exarado por servidor público ocupante de cargo efetivo ou militar de carreira, credenciado e será anexado ao processo de habilitação de segurança.
9.10 Com base no relatório de inspeção, nos autos do processo e em outras informações que se fizerem úteis, o ORN1 poderá então expedir a habilitação de segurança solicitada, considerando o risco à segurança, o período de vigência do contrato e a necessidade de tratamento da informação classificada.
9.11 A habilitação de segurança de entidades privadas, observado o disposto no item 9.10 e a critério da alta administração do ORN1 com o qual a mesma mantém vínculo de qualquer natureza, terá validade não superior a dois anos.
9.12 O processo de habilitação de segurança será arquivado no ORN1, com o qual a entidade privada mantém vínculo de qualquer natureza.
9.13 O Órgão de Registro Nível 1, a seu critério, e em qualquer tempo, poderá realizar visita de inspeção à entidade privada que recebeu a habilitação de segurança, para a verificação do cumprimento da legislação de segurança da informação e comunicações em vigor.

9.14 A entidade privada que for desabilitada, por término de validade, fim do contrato ou a critério do Órgão de Registro Nível 1 que a habilitou, é responsável pela transferência imediata para o órgão de registro de todos os ativos de informação classificada pertencentes ao órgão ou entidade pública armazenadas no seu Posto de Controle, observando a legislação e as normas de segurança da informação classificada em vigor, sob pena da Lei.
9.15 Quando a entidade privada mantiver vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República, os procedimentos previstos nesta Norma para Órgão de Registro Nível 1, poderão, a critério da alta administração do GSI/PR, serem realizados pelo NSC, conforme previsto no Inciso III do art. 3º do Decreto nº 7.845, de 2012.

10 DESCREDENCIAMENTO

10.1 O descredenciamento da pessoa natural poderá ocorrer em virtude de um dos seguintes motivos: término de validade da credencial de segurança, falecimento, cessar a necessidade de conhecer, transferência de órgão ou entidade, aposentadoria, passagem para a reserva ou inatividade, licenciamento, suspeita ou quebra de segurança, ou ainda, a critério do órgão de registro ao qual estiver vinculada.
10.2 O descredenciamento de órgão ou entidade pública poderá ocorrer, em qualquer tempo, a pedido, ou quando o mesmo incorrer nos seguintes casos: extinção, fusão, secção, mudança de subordinação, cessar a necessidade de tratar informação classificada, suspeita ou quebra de segurança, ou ainda, a critério do órgão de registro que homologou a habilitação.
10.3 O descredenciamento de entidade privada poderá ocorrer, em qualquer tempo, a pedido, ou quando a mesma incorrer nos seguintes casos: extinção, falência, fusão, aquisição, secção, cessar a necessidade de tratar informação classificada, suspeita ou quebra de segurança, ou ainda, a critério do órgão de registro que a habilitou.
10.4 A solicitação de descredenciamento de pessoa natural, órgão ou entidade pública ou privada, quando se fizer necessária, deverá ser encaminhada pela autoridade que solicitou o credenciamento de segurança ao órgão de registro com o qual mantenha vínculo de qualquer natureza.
10.5 O descredenciamento por término da validade se dará de forma automática, independente de solicitação ou processo, devendo ser homologado pelo órgão de registro com o qual a pessoa natural ou entidade privada mantenha vínculo de qualquer natureza.
10.6 O órgão de registro deverá informar a homologação do descredenciamento da pessoa natural ao órgão ou entidade pública ou privada, a que a mesma estiver vinculada.

10.7 O NSC ou o Órgão de Registro Nível 1 deverá informar a homologação do descredenciamento ao órgão ou entidade pública ou privada, desabilitado.
10.8 Nos caso de extinção, falência, fusão, divisão ou aquisição da entidade privada, sua direção estatutária deverá comunicar formal e imediatamente tal fato ao órgão de registro que a habilitou, para fins de descredenciamento.

11 RESPONSABILIDADES

11.1 Cabe à alta administração dos órgãos e entidades do Poder Executivo Federal, habilitados como órgão de registro:

11.1.1 aprovar as diretrizes gerais e o processo de credenciamento de segurança no âmbito de sua atuação; e

11.1.2 prever os recursos orçamentários necessários para a implementação e manutenção do processo de credenciamento de segurança no âmbito de sua atuação.

11.2 O Gestor de Segurança e Credenciamento de órgão ou entidade pública, no âmbito de suas atribuições, é responsável por promover a gestão da segurança e do credenciamento dos órgãos de registros, dos postos de controle e das pessoas naturais sob sua responsabilidade, no que se refere às informações classificadas, bem como, por gerir, acompanhar e avaliar as atividades previstas na competência do seu órgão ou entidade, conforme disposto nos artigos 4°, 5°, 6°, 7° e 17 da Instrução Normativa GSI/PR nº 02, de 2013.
11.3 O Gestor de Segurança e Credenciamento da entidade privada, no âmbito de suas atribuições, é responsável por promover a gestão da segurança de todos os ativos de informação classificada da empresa, bem como, por gerir, acompanhar, e avaliar as atividades previstas na competência de sua empresa, conforme disposto nos artigos 6° e 17 da Instrução Normativa GSI/PR nº 2, de 2013.
11.4 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.
11.5 Casos omissos ou excepcionais relacionados ao tratamento da informação classificada em qualquer grau de sigilo por órgão ou entidade pública ou privada, bem como ao credenciamento de segurança das pessoas naturais, ou decorrentes de tratados, acordos ou atos internacionais, serão tratados pelo Gabinete de Segurança Institucional da Presidência da República na qualidade de Autoridade Nacional de Segurança, em decorrência do previsto no parágrafo único do art. 6º do Decreto nº 7.845, de 2012, sem prejuízo das atribuições do Ministério das Relações Exteriores e demais órgãos competentes.

12 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

NORMA COMPLEMENTAR Nº 20/IN01/DSIC/GSI/PR

Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública federal.

1 OBJETIVO

Estabelecer diretrizes de Segurança da Informação e Comunicações (SIC) para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

2 CONSIDERAÇÕES INICIAIS

Os órgãos e entidades da APF produzem e tratam informação diariamente na rotina de trabalho de seus agentes públicos, ocupando relevância fundamental para a gestão da máquina pública e o processo de tomada de decisões quanto às políticas públicas federais.

Neste sentido, a presente Norma dispõe acerca de diretrizes a serem cumpridas no âmbito dos órgãos e entidades da APF quanto ao adequado tratamento da informação durante as fases do ciclo de vida.

Esta Norma configura instrumento complementar as políticas, procedimentos e regras regulamentados por atos normativos que norteiam o tratamento da informação nos órgãos e entidades da APF. Por essa razão, ressalta-se a importância da observação, por parte dos agentes públicos, dos dispositivos estabelecidos na legislação relativa a temas como SIC, gestão documental e arquivística, gestão da informação, acesso à informação, e sigilo da informação.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF.

Ciclo de vida da informação: ciclo formado pelas fases da Produção e Recepção; Organização; Uso e Disseminação; e Destinação.

Custodiante da informação: refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de SIC comunicadas pelo proprietário da informação.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação classificada em grau de sigilo: 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.

Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Metadados: conjunto de dados estruturados que descrevem informação primária.

Proprietário da informação: refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação.

Sanitização de dados: eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

4 DIRETRIZES GERAIS

4.1 Toda informação institucional dos órgãos e entidades da APF em qualquer suporte, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio do Estado brasileiro e deve ser tratada segundo as diretrizes descritas nesta Norma Complementar e nos termos da legislação pertinente em vigência.

4.2 O tratamento da informação ao longo de seu ciclo de vida deve ser realizado de modo ético e responsável pelos agentes públicos dos órgãos e entidades da APF.

4.3 O tratamento da informação deve ser feito conforme atos normativos de SIC, assegurando-se os requisitos da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação em todo seu ciclo de vida.
4.4 A informação institucional dos órgãos e entidades da APF deve ser tratada visando as suas funções administrativas, informativas, probatórias e comunicativas, e considerados os princípios de acesso a informação dispostos pela Lei nº 12.527/2011 e seus Decretos nº 7.724/2012 e nº 7.845/2012.
4.5 É dever do agente público salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal.
4.6 As medidas e os procedimentos relacionados ao tratamento da informação a ser realizado com apoio de empresa terceirizada, em qualquer fase do ciclo de vida da informação, devem ser estabelecidos contratualmente para que se assegure o cumprimento das diretrizes previstas nesta Norma, bem como em legislações vigentes.
4.7 Os órgãos e entidades da APF devem promover ações para conscientização dos agentes públicos visando à disseminação das diretrizes de tratamento da informação.
4.8 Os órgãos e entidades da APF devem identificar o proprietário e o custodiante da informação.
4.9 O proprietário da informação deve assumir, no mínimo, as seguintes atividades:
a) descrever a informação;
b) definir as exigências de SIC da informação;
c) comunicar as exigências de SIC da informação a todos os custodiantes e usuários;
d) buscar assegurar o cumprimento das exigências de SIC por meio de monitoramento; e
e) indicar os riscos que podem afetar a informação.
4.10 O custodiante da informação deve aplicar os níveis de controles de segurança conforme as exigências de SIC, comunicadas pelo proprietário da informação, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

5 CICLO DE VIDA DA INFORMAÇÃO

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

Para efeito desta Norma, o conjunto das ações referentes ao tratamento da informação está agrupado nas seguintes fases:

5.1 Produção e Recepção: refere-se à fase inicial do ciclo de vida, e compreende a produção, recepção ou custódia e classificação da informação.

5.2 Organização: refere-se ao armazenamento, arquivamento e controle da informação.

5.3 Uso e Disseminação: refere-se à utilização, acesso, reprodução, transporte, transmissão e distribuição da informação.

5.4 Destinação: refere-se a fase final do ciclo de vida da informação, e compreende a avaliação, destinação ou eliminação da informação.

6 DIRETRIZES ESPECÍFICAS DE SIC

Os órgãos e entidades da APF devem seguir as diretrizes específicas relativas às fases do ciclo de vida da informação, conforme apresentado, a seguir, nos subitens 6.1, 6.2, 6.3 e 6.4.

As diretrizes específicas representam o mínimo a ser implementado pelos órgãos e entidades da APF, e os respectivos normativos internos devem observar a legislação vigente e todos os normativos de SIC para a APF.

6.1 Produção e Recepção

6.1.1 Os processos de produção, recepção e custódia da informação devem ser planejados e implementados considerando-se:

a) os interesses da APF;

b) o período previsto para a retenção da informação; e

c) os custos com recursos materiais, financeiros e pessoas.

6.1.2 A informação produzida e custodiada pelos órgãos e entidades da APF deve ser mantida disponível e acessível aos agentes públicos que dela necessitarem para o desempenho de suas atribuições.

6.1.3 Com vistas a garantir as condições essenciais ao aprofundamento da democratização do acesso a informação no âmbito interno e externo aos órgãos e entidades da APF, deve-se priorizar a produção de informação em linguagem clara e precisa independentemente de seu formato ou suporte.

6.1.4 Os órgãos e entidades da APF devem verificar se a informação por eles produzida, recebida ou custodiada se enquadra em quaisquer hipóteses de sigilo, a fim de adotar as medidas cabíveis quanto ao seu tratamento (Anexo A).

6.1.5 Os órgãos e entidades da APF devem garantir que a produção, a recepção e a custódia de informação sejam feitas com a devida proteção da informação pessoal (Anexo A).

6.1.6 Nas reuniões em que é produzida e recebida informação sigilosa e pessoal, devem ser adotados controles de segurança para acesso ao ambiente, aos documentos, as anotações, as mídias e aos demais recursos utilizados.
6.1.7 Quando a produção, recepção e custódia de informação sigilosa e pessoal exigir impressão em tipografias, impressoras, oficinas gráficas ou similares, a operação deve ser acompanhada por pessoa oficialmente designada, responsável pela execução das medidas de salvaguarda necessárias à garantia do sigilo durante todo o processo.
6.1.8 Quando a produção, recepção e custódia de informação sigilosa classificada, em qualquer grau de sigilo, exigir impressão em tipografias, impressoras, oficinas gráficas ou similares, a operação deve ser acompanhada por pessoa credenciada, ou excepcionalmente, que tenha assinado o Termo de Compromisso de Manutenção de Sigilo (TCMS).
6.1.9 Recomenda-se que a informação produzida, recepcionada ou custodiada seja identificada por metadados.
6.1.10 O registro do documento descreve o seu conteúdo e deve, no mínimo, incluir número sequencial de identificação do documento, identificação da origem do documento, ano de produção, assunto, classificação e indicação de sigilo, quando couber.
6.1.11 Para toda informação classificada em qualquer grau de sigilo, os órgãos e entidades da APF devem adotar o Código de Indexação de Documento que contém Informação Classificada (CIDIC).
6.1.12 Os órgãos e entidades da APF, por meio de normas e procedimentos internos, podem estabelecer código de indexação para o caso de informação pessoal e demais hipóteses de sigilo previstas em lei.
6.1.13 A informação classificada deve ser produzida e custodiada utilizando criptografia baseada em algoritmo de Estado compatível com o grau de sigilo, conforme padrões mínimos estabelecidos na NC 09 DSIC/GSI/PR.
6.1.14 Para a classificação da informação, os órgãos e entidades da APF devem observar a legislação pertinente que trata dos procedimentos gerais para utilização de protocolo na APF.

6.2 Organização

6.2.1 Devem ser considerados para o armazenamento, o arquivamento e controle da informação:

a) as características físicas do suporte e do ambiente;
b) o volume e estimativa de crescimento;
c) o período previsto para a retenção da informação;
d) a proteção contra incidentes de SIC;
e) as eventuais necessidades de classificação e preservação da informação conforme atos normativos correlatos;
f) as perdas por destruição, furto ou sinistro;

g) a frequência de uso; e

h) os custos relativos ao armazenamento, arquivamento e o controle da informação.

6.2.2 É dever do agente público a manutenção dos registros de documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas.

6.2.3 Recomenda-se a observância dos padrões de interoperabilidade do Governo Eletrônico.

6.2.4 Devem ser mantidos controles sobre cópias de segurança da informação, zelando por seu adequado armazenamento e garantindo sua rastreabilidade e restauração.

6.2.5 Devem ser realizadas as marcações e adotadas as demais medidas de salvaguarda da informação sigilosa e da pessoal nos termos dos Decretos 7.724/2012 e 7.845/2012 ou de outras legislações específicas.

6.2.6 A informação classificada em grau de sigilo deve ser armazenada utilizando criptografia compatível conforme padrões mínimos para recurso criptográfico baseado em algoritmo de Estado estabelecido na NC 09 DSIC/GSI/PR.

6.2.7 No armazenamento de informação classificada em grau de sigilo secreto ou ultrassecreto, deve ser utilizado cofre ou estrutura que ofereça segurança equivalente.

6.2.8 A informação sigilosa e pessoal deve ser armazenada e arquivada em ambiente com acesso restrito e controlado.

6.2.9 A informação deve ser armazenada em servidores de arquivos e sistemas corporativos instalados em ambiente seguro. Na comunicação de dados da APF, o armazenamento e a recuperação de dados deve ser realizada em centro de processamento de dados fornecido por órgãos e entidades da APF, conforme legislação vigente.

6.2.10 Devem ser estabelecidas ações de Segurança da Informação e Comunicações para a Gestão de Continuidade de Negócio (GCN).

6.2.11 Em face de um cenário híbrido, que envolva ao mesmo tempo documentos em diferentes suportes e meios, devem ser estabelecidos requisitos de armazenamento que atendam às necessidades de sua preservação.

6.2.12 Recomenda-se criteriosa e periódica avaliação na especificação de mídias de armazenamento adequadas à necessidade de preservação, atentando-se para a compatibilidade com as novas tecnologias.

6.2.13 No uso de computação em nuvem devem ser observados os normativos de SIC e a legislação vigente.

6.3 Uso e disseminação

6.3.1 A utilização, o acesso, a reprodução, o transporte, a transmissão e a distribuição da informação devem seguir os princípios da disponibilidade, integridade, confidencialidade e autenticidade, conforme normativos de SIC e legislação vigente, bem

como orientações específicas que garantam a salvaguarda de informação sigilosa e pessoal, bem como a divulgação de informação ostensiva.

6.3.2 Nas reuniões em que é tratada informação sigilosa e pessoal, devem ser adotados controles de segurança para acesso ao ambiente, aos documentos, as anotações, as mídias e aos demais recursos utilizados.

6.3.3 A informação deve ser utilizada para atender os interesses dos órgãos e entidades da APF, não devendo ser usada para propósito pessoal de agente público ou privado.

6.3.4 A informação a ser disponibilizada por meio da transparência ativa e passiva deve ser objeto de prévia análise a fim de que se identifiquem parcelas da informação com restrição de acesso.

6.3.5 A publicação de informação institucional deve ser realizada prioritariamente por meio dos canais oficiais do órgão e entidade da APF.

6.3.6 Recomenda-se que os recursos de Tecnologia da Informação e Comunicação (TIC) franqueados ao público estejam isolados da rede corporativa.

6.3.7 A concessão de acessos lógicos e físicos ou o uso de informação institucional em dispositivos móveis corporativos e particulares devem observar a legislação de SIC vigente.

6.3.8 Recomenda-se regulamentação interna para o uso de impressoras e copiadoras, definindo as diretrizes para a impressão/cópia de documentos que contenham informação sigilosa e pessoal.

6.3.9 Recomenda-se a realização periódica de testes de restauração da informação contida nas mídias de cópias de segurança, a fim de garantir a utilização quando da ocorrência de incidentes de SIC.

6.3.10 No transporte, transmissão e distribuição de documentos em suporte físico que for realizado por empresa terceirizada, cabe ao órgão e entidade da APF estabelecer contratualmente as medidas e procedimentos de SIC adequados.

6.3.11 Os órgãos e entidades da APF devem planejar e dimensionar seus sistemas e canais de comunicação de forma a garantir a disponibilidade, a integridade, a confidencialidade e autenticidade da informação distribuída e divulgada.

6.3.12 A salvaguarda da informação sigilosa e pessoal deve ser observada na utilização, acesso, reprodução, transporte, transmissão e distribuição, conforme legislação vigente.

6.3.13 O acesso às áreas, instalações e materiais que contenham informação classificada em qualquer grau de sigilo, de acesso restrito, ou que demande proteção, deve ser normatizado internamente.

6.3.14 No transporte, transmissão e distribuição de mídias que contenham informação sigilosa deve ser aplicado controle de acesso e uso de criptografia baseada em algoritmo registrado. No caso da informação classificada em qualquer grau de sigilo deve-se utilizar criptografia baseada em algoritmo de Estado.

6.3.15 Devem ser definidos medidas e procedimentos específicos de SIC no transporte, transmissão e distribuição de documentos que contenham informação sigilosa e pessoal, em qualquer suporte ou meio.

6.3.16 É vedada a expedição de documento ultrassecreto por meio postal.

6.4 Destinação

6.4.1 Deve ser constituída a Comissão Permanente de Avaliação de Documentos (CPAD) para orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor, conforme legislação vigente.

6.4.2 Pode ser constituída a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) para assessorar sobre a classificação quanto ao grau de sigilo, desclassificação, reclassificação ou reavaliação da informação, propor o destino final da informação desclassificada e subsidiar a elaboração do rol anual das informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na Internet.

6.4.3 A disponibilidade, integridade, confidencialidade e autenticidade devem ser observadas na avaliação, destinação, arquivamento ou eliminação da informação, conforme legislação vigente. A avaliação e a seleção de documento com informação desclassificada, para fins de guarda permanente ou eliminação, observarão o disposto na Lei no 8.159/1991 e no Decreto no 4.073/2002.

6.4.4 A destinação de informação que conste de sítios eletrônicos institucionais e de repositórios internos, deve observar as legislações vigentes sobre o assunto e, nos casos necessários, ser objeto de normatização complementar pelos órgãos e entidades da APF, para que se garanta a preservação de conteúdos relevantes para o exercício de suas competências e a preservação da memória institucional.

6.4.5 Na eliminação de informação em meio eletrônico deve ser realizada sanitização dos dados nas mídias de armazenamento, tais como dispositivos móveis, discos rígidos, memórias das impressoras, scanners, multifuncionais, entre outros dispositivos, antes do descarte, a fim de evitar a recuperação irregular e indevida de dados.

7 IMPLEMENTAÇÃO

A adoção de mecanismos de gestão dos processos e procedimentos envolvidos no tratamento da informação ao longo do ciclo de vida é fundamental para a implementação das diretrizes determinadas por esta Norma.

Recomenda-se que a Alta Administração dos órgãos e entidades da APF estabeleça metodologia de gestão de tratamento da informação, observando no mínimo, as etapas de planejamento, execução, avaliação e desenvolvimento de ações de melhoria, conforme a seguir apresentado:

7.1 Planejamento

7.1.1 A Alta Administração dos órgãos e entidades da APF deve assegurar que a Política de Segurança da Informação e Comunicações (POSIC) estabeleça diretrizes gerais de tratamento da informação ao longo do ciclo de vida.

7.1.2 As normas e procedimentos internos de tratamento da informação devem ser elaborados com participação do Gestor de Segurança da Informação e Comunicações do órgão e entidade da APF, aprovados no âmbito do respectivo Comitê de Segurança da Informação e Comunicações, e submetidos à Alta Administração, para aprovação e publicação.

7.1.3 Devem ser identificadas em normativos internos ações necessárias ao aprimoramento do processo de tratamento da informação, a serem implementadas na etapa de execução.

7.2 Execução

As normas e procedimentos internos de tratamento da informação devem garantir a sua implementação em todo ciclo de vida da informação, atentando para:

a) promoção de capacitação;
b) mudança de cultura;
c) estímulo de boas práticas em todas as fases do ciclo de vida da informação; e
d) adoção de metodologias e tecnologias adequadas e atuais.

7.3 Avaliação

7.3.1 Devem ser realizados procedimentos de avaliação periódica do processo de tratamento da informação, identificando-se as revisões e alterações pertinentes.

7.3.2 Após a realização da avaliação, devem ser elaborados os ajustes e as alterações cabíveis ao processo de tratamento da informação instituído.

7.4 Ações de Melhoria

Devem ser desenvolvidas continuamente ações de melhoria visando aumentar o nível de maturidade do processo de tratamento da informação no âmbito da SIC do órgão ou entidade da APF.

8 RESPONSABILIDADES

8.1 Cabe à Alta Administração do órgão ou entidade da APF, no âmbito de suas atribuições, aprovar as diretrizes estratégicas de SIC que norteiam o tratamento da informação.

8.2 Cabe ao Gestor de SIC, no âmbito de suas atribuições no Comitê de SIC, propor, avaliar, realizar periódica análise de melhorias de normas e procedimentos internos de tratamento da informação.

8.3 Cabe a todos os agentes públicos observar o disposto nesta Norma, nos demais normativos internos de SIC do órgão e entidade da APF, bem como nos Decretos nº 7.724/2012 e nº 7845/2012.

9 VIGÊNCIA

Esta Norma entra em vigor na data da sua publicação.

10 ANEXO

A - Quadro exemplificativo de tipos de informação

ANEXO A

Quadro exemplificativo de tipos de informação

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

INSTRUÇÃO NORMATIVA CONJUNTA Nº 01 CRG/OGU, 24 DE JUNHO DE 2014.

Estabelece normas de recebimento e tratamento de denúncias anônimas e estabelece diretrizes para a reserva de identidade do denunciante.

O **CORREGEDOR-GERAL DA UNIÃO** e o **OUVIDOR-GERAL DA UNIÃO** Substituto no uso de suas atribuições, tendo em vista o disposto nos artigos 14, inciso I e 15, inciso I, do Anexo I ao Decreto nº 8.109, de 17 de setembro de 2013, bem como nos artigos 2º, inciso I e 4º, inciso I do Decreto nº 5.480, de 30 de junho de 2005, e no art. 13 do Decreto nº 8.243, de 23 de maio de 2014;

Considerando a necessidade de uniformizar o tratamento de denúncias anônimas e pedidos de reserva de identidade nos órgãos e entidades do Poder Executivo Federal;

Considerando as orientações consolidadas pelo Supremo Tribunal Federal sobre o tratamento de denúncias anônimas, bem como a proteção outorgada pela Lei n. 12.527, de 18 de novembro de 2001, às informações de caráter pessoal;

R E S O L V E M:

Art. 1º. Esta Instrução Normativa regulamenta o tratamento de manifestações anônimas e solicitações de reserva de identidade no âmbito dos órgãos de controle do Poder Executivo federal.

§ 1º Para fins desta instrução normativa, considera-se:

I - denúncia anônima: manifestação que chega aos órgãos e entidades públicas sem identificação;

II - reserva de identidade: hipótese em que o órgão público, a pedido ou de ofício, oculta a identificação do manifestante.

Art. 2º. Apresentada denúncia anônima frente a ouvidoria do Poder Executivo federal, esta a receberá e a tratará, devendo encaminhá-la aos órgãos responsáveis pela apuração desde que haja elementos suficientes à verificação dos fatos descritos.

§1º Recebida a denúncia anônima, os órgãos apuratórios a arquivarão e, se houver elementos suficientes, procederão, por iniciativa própria, à instauração de procedimento investigatório preliminar.

§ 2º O procedimento investigatório preliminar mencionado no parágrafo anterior não poderá ter caráter punitivo.

Art. 3º. Sempre que solicitado, a ouvidoria deve garantir acesso restrito à identidade do requerente e às demais informações pessoais constantes das manifestações recebidas.

§ 1º A ouvidoria, de ofício ou mediante solicitação de reserva de identidade, deverá encaminhar a manifestação aos órgãos de apuração sem o nome do demandante, hipótese em que o tratamento da denúncia será o previsto no art. 2º deste normativo;

§ 2º. Caso indispensável à apuração dos fatos, o nome do denunciante será encaminhado ao órgão apuratório, que ficará responsável a restringir acesso à identidade do manifestante à terceiros.

§ 3º A restrição de acesso estabelecida no caput deste dispositivo não se aplica caso se configure denunciação caluniosa (art. 339 do Decreto-lei n. 2.848/40 – Código Penal) ou flagrante má-fé por parte do manifestante.

§ 4º A restrição de acesso estabelecida no caput deste dispositivo encontra fundamento no art. 31 da Lei n. 12.527/11, devendo perdurar pelo prazo de 100 (cem) anos.

Art. 4º Esta instrução normativa entra em vigor na data de sua publicação.

Acesso à Informação

MINISTÉRIO DA
TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO

BRASIL
GOVERNO FEDERAL