AUTORIDADE NACIONAL DE SEGURANÇA
PARA TRATAMENTO DE
INFORMAÇÃO CLASSIFICADA

COLETÂNEA DE NORMAS DE SEGURANÇA DA INFORMAÇÃO CLASSIFICADA

Atualizada até janeiro de 2026

GABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

AUTORIDADE NACIONAL DE SEGURANÇA
PARA TRATAMENTO DE
INFORMAÇÃO CLASSIFICADA

COLETÂNEA DE NORMAS DE SEGURANÇA DA INFORMAÇÃO CLASSIFICADA

Atualizada até janeiro de 2026

NSC | Núcleo de Segurança e Credenciamento

Créditos

Marcos Antonio Amaro dos Santos
Ministro-Chefe do GSI/PR

André Luiz Bandeira Molina
Secretário de Segurança da Informação e Cibernética

Departamento de Segurança da Informação
Danielle Jacon Ayres Pinto
Diretora do Departamento de Segurança da Informação

Guilherme Bruscato Portella
Coordenador-Geral do Núcleo de Segurança e Credenciamento

Organização da Coletânea
Guilherme Bruscato Portella
Josemar Andrade Fraga

Edição e Revisão
Secretaria de Segurança da Informação e Cibernética Departamento de Segurança da Informação
Coordenação-Geral do Núcleo de Segurança e Credenciamento

Editoração e Formatação eletrônica
Liele Rodrigues da Silva
Moisés Wendell Fernandes Rodrigues

Dados Internacionais de Catalogação na Publicação (CIP)

B823c Brasil. Presidência da República. Gabinete de Segurança Institucional.
Coletânea de normas de segurança da informação classificada: atualizada até janeiro de 2026 / Gabinete de Segurança Institucional. – Brasília : Presidência da República, 2026.
269 p.

ISBN 978-65-86360-37-0

1. Segurança da Informação - Leis. 2. Classificação da Informação. 3. Credenciamento. 4. Tratamento de Informação Classificada. 5. Tratados Internacionais de Segurança da Informação. I. Título.

CDU 004.056

Bibliotecária: Lorena Flávia Santos Nolasco – CRB-1/3222

SUMÁRIO

DECRETOS

INSTRUÇÕES NORMATIVAS

PORTARIAS MINISTERIAIS

MENSAGEM DA DIRETORA DE SEGURANÇA DA INFORMAÇÃO

É com satisfação que apresento esta Coletânea de Normas de Segurança da Informação e do Tratamento de Informações Sigilosas, concebida para apoiar de forma prática e consistente, a atuação dos órgãos e entidades da Administração Pública Federal. Em um cenário de transformação digital acelerada, de ampliação do uso intensivo de tecnologias da informação e de crescente complexidade do ambiente de ameaças, a segurança da informação constitui elemento essencial para a governança, a continuidade institucional, a soberania nacional e a proteção dos interesses do Estado. Esta Coletânea reúne os principais instrumentos legais e infralegais que orientam o credenciamento de segurança, a proteção de dados sensíveis, a gestão documental e o tratamento de informações classificadas, oferecendo referência segura e atualizada para gestores, equipes técnicas, autoridades competentes e para toda a sociedade.

À Diretoria de Segurança da Informação compete planejar e coordenar a atividade nacional de segurança da informação, abrangendo a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas, em articulação com órgãos e entidades competentes. Cabe-lhe, ainda, elaborar normativos e requisitos metodológicos, promover a capacitação de recursos humanos, fomentar a cultura de segurança da informação e cibernética, atuar como órgão central de credenciamento de segurança e fiscalizar os respectivos processos. No âmbito internacional, a Diretoria assiste o Gabinete de Segurança Institucional no exercício da Autoridade Nacional de Segurança, bem como, propõe, implementa e acompanha tratados, acordos e outros atos relacionados ao intercâmbio e à proteção de informações sigilosas.

O Núcleo de Segurança e Credenciamento (NSC), está no centro da execução dessas atribuições sendo a unidade responsável dentro do Departamento de Segurança da Informação do GSI por operacionalizar as políticas e diretrizes relativas ao credenciamento de segurança. O NSC atua na habilitação e no credenciamento de pessoas físicas e jurídicas, órgãos e entidades, na definição e aplicação de critérios técnicos de segurança, na orientação aos órgãos da Administração Pública Federal e no acompanhamento da conformidade dos procedimentos adotados para o acesso e o tratamento de informações classificadas. Sua atuação contribui diretamente para o fortalecimento dos mecanismos de controle, rastreabilidade e proteção das informações sensíveis do Estado.

Nesse sentido, essa Coletânea reflete, os projetos em curso no âmbito da Diretoria de Segurança da Informação e do NSC, voltados à modernização e ao fortalecimento do ecossistema nacional de segurança da informação. Destacam-se, entre eles, a atualização e consolidação do arcabouço normativo, o aprimoramento dos processos de credenciamento e fiscalização, o desenvolvimento de critérios para certificação e acreditação de ambientes e sistemas destinados ao tratamento de informações classificadas, a ampliação das ações de capacitação e de promoção da cultura de segurança, bem como o fortalecimento da cooperação nacional e internacional para o intercâmbio seguro de

informações.

Ao disponibilizar este acervo normativo de forma organizada e de fácil acesso, reafirmamos o compromisso com a segurança jurídica, a padronização de procedimentos e a adoção de boas práticas na proteção da informação. Espera-se que este material sirva como instrumento de referência permanente e de apoio à tomada de decisão, contribuindo para a atuação coordenada dos órgãos e entidades e para o fortalecimento da segurança da informação no âmbito do Estado brasileiro.

Danielle Jacon Ayres Pinto
Diretora de Segurança da Informação
Gabinete de Segurança Institucional da Presidência da República

[...] 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: [...]

[...] 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; [...]

[...] LX a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem; [...]

[...] LXXIX é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. [...]

[...] Art. 22. Compete privativamente à União legislar sobre: [...]

[...] XXVIII defesa territorial, defesa aeroespacial, defesa marítima, defesa civil e mobilização nacional; [...]

[...] XXX proteção e tratamento de dados pessoais. [...]

[...] 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: […]

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

[...] 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. [...]

LEI Nº 8.159, DE 8 DE JANEIRO DE 1991

VERSÃO PUBLICADA

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 Considerase 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 PÚBLICOS

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. Regulamento

§ 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 Consideramse documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas freqüentes.

§ 2º Consideramse 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 Consideramse 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 Consideramse arquivos privados os conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, em decorrência de suas atividades.(Regulamento)

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.(Regulamento)

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. (Regulamento)

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. (Regulamento)

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

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. (Regulamento).

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 políticojurídica.

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

~~Art. 22 É assegurado o direito de acesso pleno aos documentos públicos.~~ (Revogado pela Lei nº 12.527, de 2011)

~~Art 23. Decreto fixará as categorias de sigilo que deverão ser obedecidas pelos órgãos públicos na classificação dos documentos por eles produzidos. Regulamento~~ (Revogado pela Lei nº 12.527, de 2011)

~~§ 1º Os documentos cuja divulgação ponha em risco a segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas são originariamente sigilosos.~~ (Revogado pela Lei nº 12.527, de 2011)

~~§ 2º O acesso aos documentos sigilosos referentes à segurança da sociedade e do Estado será restrito por um prazo máximo de 30 (trinta) anos, a contar da data de sua produção, podendo esse prazo ser prorrogado, por uma única vez, por igual período.~~ (Revogado pela Lei nº 12.527, de 2011)

~~§ 3º O acesso aos documentos sigilosos referente à honra e à imagem das pessoas será restrito por um prazo máximo de 100 (cem) anos, a contar da sua data de produção.~~ (Revogado pela Lei nº 12.527, de 2011)

~~Art. 24. Poderá o Poder Judiciário, em qualquer instância, determinar a exibição reservada de qualquer documento sigiloso, sempre que indispensável à defesa de direito próprio ou esclarecimento de situação pessoal da parte.~~ (Revogado pela Lei nº 12.527, de 2011)

~~*Parágrafo único* Nenhuma norma de organização administrativa será interpretada de modo a, por qualquer forma, restringir o disposto neste artigo.~~ (Revogado pela Lei nº 12.527, 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 DiretorGeral 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 Revogamse as disposições em contrário.

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

FERNANDO COLLOR
Jarbas Passarinho

Este texto não substitui o publicado no DOU de 9.1.1991 e retificado em 28.1.1991

VERSÃO PUBLICADA

Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências

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. Subordinamse 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 Aplicamse 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 destinamse 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, considerase:

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, garantindose 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.

VIII (VETADO). (Incluído pela Lei nº 14.345, de 2022)

§ 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 comunicarse, 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. 73B 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, serlhe 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 de fornecimento de informação é gratuito. (Redação dadapela Lei nº 14.129, de 2021) (Vigência)

§ 1º O órgão ou a entidade poderá cobrar exclusivamente o valor necessário ao ressarci-mento dos custos dos serviços e dos materiais utilizados, quando o serviço de busca e de for-necimento da informação exigir reprodução de documentos pelo órgão ou pela entidade pública consultada. (Incluído pela Lei nº 14.129, de 2021) (Vigência)

§ 2º Estará isento de ressarcir os custos previstos no § 1º deste artigo 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.(Incluído pela Lei nº 14.129, de 2021) (Vigência)

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 III
DO PROCEDIMENTO 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. (Regulamento)

§ 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 procedimentosde 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: (Regulamento)

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. (Regulamento)

§ 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 deocultação 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 nas Leis 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 ouinformações 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. (Regulamento)

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: (Regulamento)

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

Este texto não substitui o publicado no DOU de 18.11.2011 - Edição extra

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

VERSÃO PUBLICADA

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019)

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

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços

ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD; (Redação dada pela Medida Provisória nº 1.317, de 2025)

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados,

reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

XIX - autoridade nacional: entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Medida Provisória nº 1.317, de 2025)

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios

ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)Vigência

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios

previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou(Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.(Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando

exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III

Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o §

1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV

Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os

quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3 (VETADO) (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder

Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de

consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a

garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4 (VETADO).(Incluído pela Lei nº 13.853, de 2019) Vigência

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as

instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos

princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de

monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Promulgação partes vetadas)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.(Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.(Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.(Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. (Vigência)

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

CAPÍTULO IX
(REDAÇÃO DADA PELA MEDIDA PROVISÓRIA Nº 1.317, DE 2025)
DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Agência Nacional de Proteção de Dados

Art. 55. (VETADO).

Art. 55-A. Fica criada a Agência Nacional de Proteção de Dados – ANPD, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia

funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal, nos termos do disposto na Lei nº 13.848, de 25 de junho de 2019. (Redação dada pela Medida Provisória nº 1.317, de 2025)

§ 1 (Revogado pela Lei nº 14.460, de 2022)

§ 2 (Revogado pela Lei nº 14.460, de 2022)

§ 3 (Revogado pela Lei nº 14.460, de 2022)

Art. 55-B.(Revogado pela Lei nº 14.460, de 2022)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - (revogado); (Redação dada pela Lei nº 14.460, de 2022)

V-A - Procuradoria; (Redação dada pela Medida Provisória nº 1.317, de 2025)

V-B - Auditoria; e (Incluído pela Medida Provisória nº 1.317, de 2025)

VI - unidades administrativas e unidades especializadas. (Redação dada pela Medida Provisória nº 1.317, de 2025)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea ‘f’ do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo

administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a

apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;(Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento, (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências

regulatória, fiscalizatória e punitiva da ANPD (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação(Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: (Incluído pela Lei nº 14.460, de 2022)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e (Incluído pela Lei nº 14.460, de 2022)

II - que venha a adquirir ou a incorporar. (Incluído pela Lei nº 14.460, de 2022)

Art. 56. (VETADO).

Art. 5 7. (VETADO).

Seção II

Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº

13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a prote-ção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais pre-vistos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto nº§ 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de ban-cos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexi-dade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordena-mento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor: (Redação dada pela Medida Provisória nº 869, de 2018)

I. dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e(Incluído pela Lei nº 13.853, de 2019)

I.A. dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II. 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília, 14 de agosto de 2018; 197o da Independência e 130o da República.

MICHEL TEMER

Torquato Jardim

Aloysio Nunes Ferreira Filho

Eduardo Refinetti Guardia

Esteves Pedro Colnago Junior

Gilberto Magalhães Occhi Gilberto Kassab

Wagner de Campos Rosário Gustavo do Vale Rocha

Ilan Goldfajn Raul Jungmann Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra

VERSÃO PUBLICADA

[…] Divulgação de segredo

Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis.

§ 1° Somente se procede mediante representação.

§ 1° A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

§ 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

[…]

[…] Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vanta-gem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I. Presidente da República, governadores e prefeitos;

II. Presidente do Supremo Tribunal Federal

III. Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV. dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessio-nárias de serviços públicos. […]

[…] Violação de sigilo funcional

Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:

Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

§ 1º Nas mesmas penas deste artigo incorre quem:

I. permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;

II. se utiliza, indevidamente, do acesso restrito.

§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:

Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

[…] Espionagem

Art. 359-K. Entregar a governo estrangeiro, a seus agentes, ou a organização criminosa estrangeira, em desacordo com determinação legal ou regulamentar, documento ou informação classificados como secretos ou ultrassecretos nos termos da lei, cuja revelação possa colocar em perigo a preservação da ordem constitucional ou a soberania nacional:

Pena - reclusão, de 3 (três) a 12 (doze) anos.

§ 1º Incorre na mesma pena quem presta auxílio a espião, conhecendo essa circunstância, para subtraí-lo à ação da autoridade pública.

§ 2º Se o documento, dado ou informação é transmitido ou revelado com violação do dever de sigilo:

Pena - reclusão, de 6 (seis) a 15 (quinze) anos.

§ 3º Facilitar a prática de qualquer dos crimes previstos neste artigo mediante atribuição, fornecimento ou empréstimo de senha, ou de qualquer outra forma de acesso de pessoas não autorizadas a sistemas de informações:

Pena - detenção, de 1 (um) a 4 (quatro) anos.

§ 4º Não constitui crime a comunicação, a entrega ou a publicação de informações ou de documentos com o fim de expor a prática de crime ou a violação de direitos humanos. […]

Rio de Janeiro, 7 de dezembro de 1940; 119º da Independência e 52º da República.

GETÚLIO VARGAS
Francisco Campos

Este texto não substitui o publicado no DOU de 31.12.1940 e retificado em 3.1.1941

EXTRATO DA LEI Nº 8.429, DE 2 DE JUNHO DE 1992 LEI DE IMPROBIDADE ADMINISTRATIVA

VERSÃO PUBLICADA

[…]CAPÍTULO II

DOS ATOS DE IMPROBIDADE ADMINISTRATIVA[…]

Seção III

Dos Atos de Improbidade Administrativa que Atentam Contra os Princípio da Administração Pública

Art. 11. Constitui ato de improbidade administrativa que atenta contra os princípios da administração pública a ação ou omissão dolosa que viole os deveres de honestidade, de imparcialidade e de legalidade, caracterizada por uma das seguintes condutas: (Redação dada pela Lei nº 14.230, de 2021)[…]

[…] III - revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo, propiciando beneficiamento por informação privilegiada ou colocando em risco a segurança da sociedade e do Estado; […]

CAPÍTULO III

DAS PENAS

Art. 12. Independentemente do ressarcimento integral do dano patrimonial, se efetivo, e das sanções penais comuns e de responsabilidade, civis e administrativas previstas na legislação específica, está o responsável pelo ato de improbidade sujeito às seguintes cominações, que podem ser aplicadas isolada ou cumulativamente, de acordo com a gravidade do fato: (Redação dada pela Lei nº 14.230, de 2021)[…]

III.na hipótese do art. 11 desta Lei, pagamento de multa civil de até 24 (vinte e quatro) vezes o valor da remuneração percebida pelo agente e proibição de contratar com o poder público ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, ainda que por intermédio de pessoa jurídica da qual seja sócio majoritário, pelo prazo não superior a 4 (quatro) anos; (Redação dada pela Lei nº 14.230, de 2021)[…]

IV.(Revogado). (Redação dada pela Lei nº 14.230, de 2021)

Parágrafo único. (Revogado). (Redação dada pela Lei nº 14.230, de 2021)

§ 1º A sanção de perda da função pública, nas hipóteses dos incisos I e II do *caput* deste artigo, atinge apenas o vínculo de mesma qualidade e natureza que o agente público ou político detinha com o

poder público na época do cometimento da infração, podendo o magistrado, na hipótese do inciso I do *caput* deste artigo, e em caráter excepcional, estendê-la aos demais vínculos, consideradas as circunstâncias do caso e a gravidade da infração. (Redação dada pela Lei nº 14.230, de 2021) (Vide ADI 7236)

§ 2º A multa pode ser aumentada até o dobro, se o juiz considerar que, em virtude da situação econômica do réu, o valor calculado na forma dos incisos I, II e III do *caput* deste artigo é ineficaz para reprovação e prevenção do ato de improbidade. (Incluído pela Lei nº 14.230, de 2021)

§ 3º Na responsabilização da pessoa jurídica, deverão ser considerados os efeitos econômicos e sociais das sanções, de modo a viabilizar a manutenção de suas atividades. (Incluído pela Lei nº 14.230, de 2021)

§ 4º Em caráter excepcional e por motivos relevantes devidamente justificados, a san-ção de proibição de contratação com o poder público pode extrapolar o ente público lesado pelo ato de improbidade, observados os impactos econômicos e sociais das sanções, de for-ma a preservar a função social da pessoa jurídica, conforme disposto no § 3º deste artigo. (Incluído pela Lei nº 14.230, de 2021)

§ 5º No caso de atos de menor ofensa aos bens jurídicos tutelados por esta Lei, a sanção limitar-se-á à aplicação de multa, sem prejuízo do ressarcimento do dano e da perda dos valores obtidos, quando for o caso, nos termos do *caput* deste artigo. (Incluído pela Lei nº 14.230, de 2021)

§ 6º Se ocorrer lesão ao patrimônio público, a reparação do dano a que se refere esta Lei deverá deduzir o ressarcimento ocorrido nas instâncias criminal, civil e administrativa que tiver por objeto os mesmos fatos. (Incluído pela Lei nº 14.230, de 2021)

§ 7º As sanções aplicadas a pessoas jurídicas com base nesta Lei e na Lei nº 12.846, de 1º de agosto de 2013, deverão observar o princípio constitucional do non bis in idem. (Incluído pela Lei nº 14.230, de 2021)

§ 8º A sanção de proibição de contratação com o poder público deverá constar do Cadas-tro Nacional de Empresas Inidôneas e Suspensas (CEIS) de que trata a Lei nº 12.846, de 1º de agosto de 2013, observadas as limitações territoriais contidas em decisão judicial, conforme disposto no § 4º deste artigo. (Incluído pela Lei nº 14.230, de 2021)

§ 9º As sanções previstas neste artigo somente poderão ser executadas após o trânsito em julgado da sentença condenatória. (Incluído pela Lei nº 14.230, de 2021)

§ 10. Para efeitos de contagem do prazo da sanção de suspensão dos direitos políticos, computar-se-á retroativamente o intervalo de tempo entre a decisão colegiada e o trânsito em julgado da sentença condenatória. (Incluído pela Lei nº 14.230, de 2021) (Vide ADI 7236)[…]

Rio de Janeiro, 2 de junho de 1992; 171° da Independência e 104° da República.

FERNANDO COLLOR

Célio Borja

Este texto não substitui o publicado no DOU de 3.6.1992.

VERSÃO PUBLICADA

Acordo de Segurança Relativo à Troca de Informações Classificadas e Protegidas entre o Governo da República Federativa do Brasil e o Governo da República Francesa

Observação: o Acordo de 1974 foi emendado em 2016 para ajustar as equivalências entre os graus de sigilo aos preceitos da Lei nº 12.527/2011 (Lei de Acesso à Informação). Em 2024, devido a mudanças na legislação france-sa, foi assinado novo Acordo de Segurança Relativo à Troca de Informações Classificadas e Protegidas entre o Governo da República Federativa do Brasil e o Governo da República Francesa, que ainda não está em vigor. Mais informações neste link

ACORDO DE SEGURANÇA RELATIVO A TROCAS DE INFORMAÇÃO DE CARÁTER SIGILOSO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA REPÚBLICA FRANCESA

O Governo da República Federativa do Brasil

e

O Governo da República Francesa

desejosos de assegurar a proteção das informações de caráter sigiloso que, no interesse da segurança nacional, são trocadas entre as autoridades competentes dos dois Estados, ou fornecidas no quadro de pedidos ou encomendas governamentais a estabelecimentos brasileiros ou franceses, convieram nas seguintes disposições:

Artigo 1º

Disposições Gerais

O presente Acordo constitui o regulamento de segurança comum aos diferentes acordos de cooperação que impliquem comunicação de informações de caráter sigiloso, concluídos entre o Governo brasileiro e o Governo francês.

A autoridade governamental responsável pela segurança no quadro desta colaboração é:

pelo Brasil:

Ministro de Estado responsável pela execução do acordo de cooperação.

pela França:

o Secretário Geral da Defesa Nacional.

Anexos de segurança, em que serão especialmente definidos, por cada uma das duas par-tes contratantes, os elementos sigilosos sujeitos à salvaguarda que cada qual comunicar, bem como as informações que possam levar ao conhecimento desses segredos, serão juntados aos acordos particulares relativos aos diferentes setores de cooperação.

Entender-se-á por informação todo conhecimento, sob qualquer forma que seja expresso: informação, documento, material, invenção, procedimento, etc.

Nos acordos de cooperação a que se refere o presente Acordo de Segurança, as informações transferidas a um dos Governos por um terceiro país poderão ser igualmente comunicadas ao outro Governo, se não houver objeção por parte do referido terceiro país.

As informações trocadas só podem ser utilizadas para os fins que digam respeito à aplicação dos acordos de cooperação estabelecidos.

As informações de caráter sigiloso não podem ser transferidas a uma terceira Parte, ou a cidadão dessa terceira Parte, sem prévia autorização da Parte contratante da qual provenham estas informações.

A salvaguarda dos direitos de propriedade, inclusive dos de propriedade industrial, será re-gulada em cada acordo de cooperação. Em nenhum caso, poderão tais direitos ser transmitidos a terceiro país, ou a cidadão de outro Estado, sem a aprovação da outra Parte.

Artigo 2º
Segurança Geral das Informações

A proteção que os dois Governos se comprometem a garantir pelo presente Acordo de Segurança se estende ao conjunto das informações de caráter sigiloso Comunicadas ou surgidas durante toda a duração de cada um dos acordos de cooperação, incluídos os contratos e subcontratos ajustados em virtude desses acordos.

Os anexos de segurança poderão ser completados, por consentimento mútuo, no decurso da execução dos acordos, ou modificados:

- na ocasião da. descoberta ou da apresentação de informações que uma das duas partes contratantes considere que devam ser mantidas em sigilo;

- quando o país em que a informação teve origem comunicar que ela perdeu seu caráter sigiloso e não necessita mais de proteção particular.

As informações só podem ser trocadas em virtude de disposições baixadas pelos representantes oficiais dos dois Governos, partes dos acordos de cooperação e por eles acordadas. Com o fim de obter normas de segurança comparáveis para as informações sigilosas, as autoridades governamentais

responsáveis se comprometem a fornecer, a pedido da outra parte, as modalidades de execução das medidas de segurança prescritas por sua regulamentação nacional, especialmente as condições de proteção previstas pelas diferentes classificações ou menções de proteção.

As características sigilosas dos acordos particulares a serem concluídos figurarão em um anexo de segurança. A autoridade governamental responsável definirá igualmente, de maneira tão precisa quanto possível, o grau de salvaguarda a atribuir às informações, sob qualquer forma em que elas se apresentem, fornecidas à outra parte. Cabe às autoridades governamentais destinatárias outorgar-lhes o mesmo grau de proteção, levando em conta o quadro de equivalência das classificações e das menções de proteção, adotado de comum acordo e indicado a seguir:

	Brasil	França
Classificações (segredo de segurança nacional)	Secreto "Documento Controlado"	Secret défense
Menções de Proteção (discrição profissional)	Confidencial Reservado	Condifentiel défense Diffusion restreinte

Se um documento que contenha informações sigilosas for reproduzido, ou traduzido, total ou parcialmente, as marcas de segurança serão apostas sobre as reproduções ou traduções que devam receber o mesmo grau de sigilo que o documento de origem.

Artigo 3º

Responsabilidade das Autoridades Governamentais

A fim de garantir a segurança das informações sigilosas, as autoridades governamentais assumirão plena responsabilidade, em seu território nacional, pela aplicação das prescrições do presente Acordo de segurança em matéria:

- de licenciamento dos estabelecimentos associados à execução dos acordos de cooperação;
- de decisões individuais concernentes à habilitação das pessoas que deverão conhecer as informações sigilosas;
- de definição das medidas materiais de proteção a serem tomadas, assim como do controle de sua aplicação e de sua eficácia, notadamente nos estabelecimentos associados à execução dos acordos.
-

Na expressão "autoridades governamentais" estão compreendidas as autoridades civis ou militares com a delegação dos Ministros responsáveis pela execução do acordo.

Por "estabelecimento associado" entender-se-á todo organismo alheio à Administração direta e

às Forças Armadas.

Artigo 4º

Licenciamento Dos Estabelecimentos Associados

Nenhum estabelecimento poderá associar-se à execução dos acordos de cooperação, por contrato, convenção ou transação que diga respeito direta ou indiretamente a um dos elementos sigilosos, sem consentimento prévio da autoridade governamental responsável pela aplicação dos acordos.

O consentimento será também necessário para a participação nos estudos preparatórios para a conclusão de contratos, convenções ou transações. Será igualmente exigido para os eventuais subcontratantes ou subempreiteiros que devam receber comunicação ou fornecer informação sigilosa constantes dos anexos de segurança.

O licenciamento só será dado após investigação sobre a capacidade técnica e as condições de segurança. Em particular, deverá ser controlada no local a capacidade material dos estabelecimentos para aplicar as prescrições relativas à segurança das informações sigilosas.

Essas prescrições serão objeto de textos oficiais comunicados aos interessados pela autoridade governamental. As responsabilidades individuais e as dos estabelecimentos em matérias de proteção do sigilo, assim como as sanções aplicáveis, em caso de infração, serão claramente definidas nesses textos.

Artigo 5º

Habilitação das pessoas

Nenhuma pessoa poderá tomar conhecimento de uma informação sigilosa se não satisfizer as condições abaixo discriminadas:

- ter, em consequência de suas funções ou seu cargo, a necessidade de conhecê-las;
- ter sido habilitada por decisão emanada de autoridade governamental responsável.

As modalidade de habilitação dessas pessoas em cada país contratante serão comunicadas à outra parte.

Artigo 6º

Medidas materiais de segurança

A natureza e a extensão das medidas materiais a serem tomadas estão definidas nos regulamentos nacionais de salvaguarda com observância do quadro de. equivalência que figura no artigo segundo deste Acordo e das prescrições particulares baixadas nos anexos de segurança elaborados para a aplicação dos acordos.

Em caso de desaparecimento de documento ou de material sigiloso, recebido nos termos de um acordo de cooperação, ou de suspeita de comprometimento, cada parte deverá informar o Governo de origem, que receberá igualmente comunicação dos resultados da investigação imediatamente providenciada, a fim de estabelecer as circunstâncias do desaparecimento e as possibilidades de comprometimento.

Artigo 7º

Segurança dos transportes fora das fronteiras

a) Encaminhamento de documentos sigilosos

O transporte de documentos sigilosos será efetuado de Governo a Governo, por via diplomática ou militar.

Esta regra não terá nenhuma exceção no que diz, respeito ao encaminhamento das informações sigilosas por meios de telecomunicação. O emprego desses meios será objeto de disposições especiais que figurarão nos anexos de segurança; as duas partes contratantes se comprometem a respeitá-los estritamente, a fim de garantir a segurança de toda informação que se refira direta ou indiretamente aos elementos sigilosos comunicados.

Em caso de urgência claramente comprovada, o acompanhamento dos documentos entre o Brasil e a França poderá ser excepcionalmente confiado a uma pessoa habilitada que represente um estabelecimento associado na execução do acordo, com a condição de esta pessoa estar munida de uma autorização pessoal, expedida para esse efeito pela autoridade governamental responsável e devidamente instruída dos deveres que lhe incumbem.

Esse procedimento deve ser de caráter excepcional e somente poderá ser autorizado quando o encaminhamento dos documentos por via diplomática ou militar provocar atrasos incompatíveis com os prazos de execução do programa.

b) Encaminhamento de materiais sigilosos

Todo transporte de material sigiloso será submetido à aprovação das autoridades nacionais interessadas, tanto no que toca à operação em si mesma quanto às datas, aos meios utilizados, às modalidades de execução e ao pessoal empregado.

Caberá ao expedidor de material sigiloso dar a conhecer em tempo hábil sua intenção de transporte, para obter as autorizações necessárias das autoridades nacionais competentes.

O pessoal encarregado de todas as etapas no transporte, desde o estabelecimento de origem até final destino, deverá ter sido submetido previamente a uma investigação de segurança, e estar munido de autorização e instruções escritas.

Artigo 8º

Visitas e estágios

a) Visitas

As autorizações de visita aos estabelecimentos associados na execução do acordo de cooperação só serão expedidas pelas autoridades que tenham recebido delegação para esse fim do Ministro responsável pela segurança no âmbito do Acordo.

A autorização de visita às zonas reservadas só poderá ser dada aos nacionais das partes contratantes, titulares de um certificado de segurança de nível pelo menos igual ao mais alto grau das informações elaboradas ou guardadas no estabelecimento.

A autorização fixará a data ou período da visita e o grau das informações sigilosas que poderão ser comunicadas.

A menos que previamente autorizados pela autoridade competente, os visitantes não poderão retirar materiais ou documentos a que tiverem acesso durante as visitas, nem usar meios de reprodução de qualquer natureza com respeito às discussões, materiais ou documentos relativos às informações sigilosas.

As visitas de cidadãos de nações outras que não as duas partes contratantes só poderão ser autorizadas com o acordo prévio do Governo que tenha fornecido as informações sigilosas manipuladas ou guardadas no estabelecimento.

b) Estágios

As visitas de duração superior a dois dias são chamadas estágios.

c) Relações com a imprensa

A regulamentação geral concernente às visitas será aplicada integralmente aos represen-tantes da imprensa escrita, falada ou televisada.

Não poderá ser autorizada a visita de representantes da imprensa às zonas reservadas. Só poderão ser comunicadas à imprensa informações não sigilosas e mediante prévia autorização da autoridade responsável pela execução do Acordo.

Artigo 9º

Controle governamental e visitas de verificação a estabelecimentos associados

Sob a responsabilidade das autoridades governamentais de cada Estado contratante, em seu

respectivo país, serão efetuados controles para verificar a aplicação e a eficácia de medidas materiais de segurança.

Nos estabelecimentos associados à execução dos acordos de cooperação, cada uma das Partes contratantes poderá solicitar à outra Parte que à autorize a participar de visitas de veri-ficação.

Esta solicitação deverá ser apresentada com uma antecedência de pelo menos 30 dias às autoridades governamentais antes da visita pretendida.

Os gastos ocasionados pelas visitas de verificação estarão a cargo da Parte que as requerer.

Tais visitas terão como exclusivo propósito verificar a aplicação das regras de segurança relativas às informações sigilosas que constituem o objeto do presente Acordo.

Artigo 10º

Execução do Acordo

Cada acordo de cooperação que vier a ser concluído, implicando comunicação entre o Brasil e a França de informações de caráter sigiloso, conterá obrigatoriamente um anexo de segurança que se refira ao presente Acordo e que o complete pelas disposições específicas ao objeto do Acordo.

O presente Acordo entrará em vigor na data de sua assinatura.

É concluído por um período de dois anos e será renovado por recondução tácita, exceto denúncia formulada três meses antes de expirar tal período. Após sua renovação, poderá ser denunciado a qualquer momento, mediante aviso prévio de 3 meses. Em caso de denúncia, as informações de caráter sigiloso, comunicadas nos termos do presente Acordo, continuarão a ser regidas pelas disposições aqui estabelecidas.

EM FÉ DO QUE

Os representantes dos dois Governos, devidamente autorizados para este efeito, assinam o presente Acordo e apõem o seu respectivo selo.

Feito em Brasília, em dois de setembro de 1974.

Em dois exemplares nas línguas portuguesa e francesa, fazendo fé ambos os textos.

EMENDA AO ACORDO DE SEGURANÇA RELATIVO À TROCA DE INFORMAÇÃO DE CARÁTER SIGILOSO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA REPÚBLICA FRANCESA, ASSINADO EM 2 DE OUTUBRO DE 1974

O Governo da República Federativa do Brasil e

O Governo da República Francesa; doravante denominados "Partes";

Desejosos de alterar certas disposições do Acordo de Segurança Relativo à Troca de Informação de Caráter Sigiloso entre o Governo da República Federativa do Brasil e o Governo da República Francesa, assinado em 2 de outubro de 1974 (doravante denominado " Acordo de Segurança");

Acordam as seguintes disposições:

Artigo 1º

Autoridades Nacionais de Segurança

No artigo 1º do Acordo de Segurança, a expressão "Secretário Geral da Defesa Nacional" será substituída por "Secretário Geral da Defesa e da Segurança Nacional" e a expressão "Ministro de Estado responsável pela execução do Acordo de cooperação" será substituída por "Casa Militar da Presidência da República".

Artigo 2º

Grau de Proteção

No artigo 2º do Acordo de Segurança, a tabela de equivalência será alterada como segue:

	República Francesa	República Federativa do Brasil
Classificações (segredo de segurança nacional)	SECRET DEFENSE	Ultrassecreto
	CONFIDENTIEL DEFENSE	Secreto (a)
Menções de Proteção (discrição profissional)	DIFFUSION RESTREINTE	Reservado

Artigo 3º

Transmissão Eletrônica

Ao final do artigo 2º do Acordo de Segurança, será aditado o seguinte parágrafo:

"A transmissão eletrônica de informações sigilosas é feita em forma criptografada com os métodos e dispositivos criptográficos aprovados por comum acordo pelas autoridades gover-namentais

responsáveis de ambas as Partes.

”

Artigo 4º

Vigência

A presente Emenda entra em vigor no primeiro dia do terceiro mês após a data de sua assinatura.

Em fé do que, os representantes de seus respectivos Governos, devidamente autorizados para tanto, assinaram a presente Emenda.

FEITA em , em 2016, em dois exemplares originais, nos idiomas francês e português, sendo ambos os textos igualmente autênticos.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

Mauro Vieira

Ministro das Relações Exteriores

PELO GOVERNO DA REPÚBLICA FRANCESA

Laurent Bili

Embaixador da França no Brasil

VERSÃO PUBLICADA

Aprova o texto do Acordo para a Proteção de Informação Classificada entre a República Fede-rativa do Brasil e a República Portuguesa, assina-do na cidade do Porto, em 13 de outubro de 2005.

Observação: as equivalências entre os graus de sigilo não estão atualizadas, pois o acordo é anterior à Lei nº 12.527/2011 (Lei de Acesso à Informação). Texto da emenda, embora assinado, ainda não está em vigor. Mais informações neste

O Congresso Nacional decreta:

Art. 1º Fica aprovado o texto do Acordo para a Proteção de Informação Classificada entre a República Federativa do Brasil e a República Portuguesa, assinado na cidade do Porto, em 13 de outubro de 2005.

Parágrafo único. Ficam sujeitos à aprovação do Congresso Nacional quaisquer atos que possam resultar em revisão do referido Acordo, bem como quaisquer ajustes complementares que, nos termos do inciso I do *caput* do art. 49 da Constituição Federal, acarretem encargos ou compromissos gravosos ao patrimônio nacional.

Art. 2º Este Decreto Legislativo entra em vigor na data de sua publicação.

Senado Federal, em 18 de setembro de 2008.

Senador GARIBALDI ALVES FILHO

Presidente do Senado Federal

ACORDO PARA A PROTEÇÃO DE INFORMAÇÃO CLASSIFICADA ENTRE A REPÚBLICA FEDERATIVA DO BRASIL E A REPÚBLICA PORTUGUESA

A República Federativa do Brasil e

A República Portuguesa doravante designadas por "Partes",

Reconhecendo a necessidade das Partes de garantir a proteção de Informação Classifica-da trocada entre as Partes, pessoas singulares ou coletivas, no âmbito de acordos de cooperação ou contratos celebrados ou a celebrar;

Desejando estabelecer um conjunto de regras sobre a proteção mútua da Informação Classificada trocada entre as Partes,

Acordam o seguinte:

Artigo 1º

Objetivo

O presente Acordo estabelece as regras de segurança aplicáveis a todos os acordos de cooperação ou contratos que prevejam a transmissão de competentes das Partes ou por pes-soas singulares ou coletivas autorizadas para esse efeito.

Artigo 2º

Âmbito de aplicação

1. O presente Acordo estabelece os procedimentos a adotar para a proteção de Informação Classificada trocada entre as Partes.

2. O presente Acordo não é aplicável à cooperação direta entre os serviços de informações.

Artigo 3º

Definições

Para os efeitos do presente Acordo:

a) "Informação Classificada" designa a informação, os documentos e materiais, independentemente da sua forma, natureza e meios de transmissão, aos quais tenha sido atribuído um grau de classificação de segurança e que requeiram proteção contra divulgação não autorizada;

b) "Entidade Nacional de Segurança" designa a entidade designada por cada Parte como responsável pela aplicação e supervisão do presente Acordo;

c) "Parte Transmissora" designa a Parte que entrega ou transmite Informação Classificada à outra Parte;

d) "Parte Destinatária" designa a Parte à qual é entregue ou transmitida Informação Classificada pela Parte Transmissora;

e) "Terceira Parte" designa qualquer organização internacional ou Estado incluindo osseus cidadãos e pessoas coletivas, e que não é Parte no presente Acordo;

f) "Contratante" designa uma pessoa singular ou coletiva possuidora de capacidade jurídica para celebrar contratos;

g) "Contrato Classificado" designa qualquer acordo entre dois ou mais Contratantes que estabelece e define direitos e obrigações entre eles e que contém ou envolve Informação Classificada;

h) "Credenciamento de Segurança de Pessoa Singular" designa a determinação feita pela Entidade Nacional de Segurança ou outra entidade competente, em resultado de procedimento de investigação para credenciamento, de que um indivíduo está habilitado para ter acesso a Informação Classificada, de acordo com o Direito interno;

i) "Credenciamento de Segurança de Pessoa Coletiva" designa a determinação feita pela Entidade Nacional de Segurança ou outra entidade competente de que, sob o ponto de vista da segurança, uma entidade tem capacidade física e organização para manusear e guardar informação Classificada, de acordo com o respectivo Direito interno;

j) "Necessidade de Conhecer" designa que o acesso à Informação Classificada que só pode ser concedido à pessoa que tenha comprovada necessidade de a conhecer, ou de a possuir, para cumprimento das suas funções oficiais e profissionais, de acordo com o propósito para o qual a informação foi entregue ou transmitida à Parte Destinatária;

k) "Instrução de Segurança do Projeto" designa uma compilação de requisitos de segurança, que são aplicados a um determinado projecto para garantir a uniformização nos procedimentos de segurança;

l) "Guia de Classificação de Segurança do Projeto" designa a parte da Instrução de Segurança do Projeto que identifica os elementos do projeto que são classificados, especificando os respectivos níveis de classificação de segurança.

Artigo 4º

Entidades Nacionais de Segurança

I. As Entidades Nacionais de Segurança responsáveis pela aplicação do presente Acordo são:

Pela República Portuguesa:

Autoridade Nacional de Segurança

Presidência do Conselho de Ministros

Av. Ilha da Madeira, 1

1400-204 Lisboa

Portugal

Pela República Federativa do Brasil:

Gabinete de Segurança Institucional Presidência da República

Esplanada dos Ministérios

Brasília

Brasil

II. As Partes informar-se-ão mutuamente, por via diplomática, de qualquer alteração rela-tiva às suas Entidades Nacionais de Segurança.

Artigo 5º

Princípios de Segurança

1. A proteção e utilização de Informação Classificada trocada entre as Partes regem-se pelos seguintes princípios:

a) As Partes atribuirão a toda a Informação Classificada transmitida, produzida ou de-senvolvida o mesmo grau de segurança atribuído à sua própria Informação Classificada de grau equivalente.

b) O acesso à Informação Classificada é limitado às pessoas que tenham Necessida-de de Conhecer e que, no caso de informação classificada como CONFIDENCIAL ou superior, estejam habilitadas com um Credenciamento de Segurança de Pessoa Singular emitida pelas autoridades competentes. 2. Com o objetivo de se obterem e manterem padrões de segurança comparáveis, as Entidades Nacionais de Segurança deverão, sempre que solicitado, disponibilizar mutuamente informação sobre os seus padrões de segurança, procedimentos e práticas para a proteção de Informação Classificada.

Artigo 6º

Classificação de segurança

1. As Partes acordam que os graus de classificação de segurança seguintes são equiva-lentes e correspondem aos graus de classificação de segurança especificados no respectivo Direito interno de cada uma das Partes:

República Portuguesa	República Federativa do Brasil

MUITO SECRETO	ULTRA SECRETO
SECRETO	SECRETO
CONFIDENCIAL	CONFIDENCIAL
RESERVADO	RESERVADO

2. A Parte Destinatária marcará a Informação Classificada recebida com as suas próprias marcas de classificação de segurança equivalentes, em conformidade com as equivalências referidas no número 1 do presente Artigo.

3. As Partes informa-se-ão mutuamente sobre as alterações ulteriores dos graus de classificação da Informação Classificada transmitida.

4. A Parte Destinatária não poderá baixar o grau de classificação de segurança ou desclas-sificar a Informação Classificada recebida, sem prévia autorização escrita da Parte Transmissora.

Artigo 7º

Credenciamento de segurança

1. Se solicitado, as Partes, através das suas Entidades Nacionais de Segurança, tendo em conta o respectivo Direito interno, colaboração entre si no decurso dos procedimentos para o credenciamento de segurança das suas pessoas singulares ou coletivas que residam ou estejam localizadas no território da outra Parte, precedendo a emissão do Credenciamento de Segurança de Pessoa Singular e do Credenciamento de Segurança de Pessoa Coletiva.

2. Cada Parte reconhecerá o Credenciamento de Segurança de Pessoa Singular e o Credenciamento de Segurança de Pessoa Coletiva emitidas de acordo com o Direito interno da outra Parte. A equivalência dos graus de classificação de segurança será feita em conformidade com o Artigo 6º do presente Acordo.

3. As Entidades Nacionais de Segurança informar-se-ão mutuamente sobre quaisquer alterações relativas ao Credenciamento de Segurança de Pessoa Singular e ao Credenciamento de Segurança de Pessoa Coletiva, designadamente no caso de cancelamento ou abaixamento do grau de classificação de segurança atribuído.

Artigo 8º

Reprodução e destruição

1. A Informação Classificada marcada como SECRETO ou superior, só poderá ser reproduzida após autorização escrita da Entidade Nacional de Segurança da Parte Transmissora.

2. As reproduções de Informação Classificada deverão obedecer aos seguintes procedimentos:

a) As pessoas envolvidas deverão ser titulares de Credenciamento de Segurança de Pessoa Singular de acordo com o Artigo 5º;

b) As reproduções serão marcadas e protegidas da mesma forma que a informação original;

c) O número de cópias a efetuar deverá ser limitado ao requerido para uso oficial;

3. A Informação Classificada marcada como MUITO SECRETO/ULTRA SECRETO não poderá ser destruída, devendo ser devolvida à Entidade Nacional de Segurança da Parte Transmissora.

4. A destruição de Informação Classificada marcada como SECRETO será notificada à Entidade Nacional de Segurança da Parte Transmissora.

5. A Informação Classificada marcada até CONFIDENCIAL, inclusive, deverá ser destruída de acordo com o respectivo Direito interno.

6. No caso de uma situação de crise que torne impossível proteger ou devolver Informação Classificada criada ou transferida de acordo com o presente Acordo, esta deverá ser destruída imediatamente. A Parte Destinatária deverá notificar a Autoridade Entidade Nacional de Segu-rança da Parte Transmissora acerca da destruição da Informação Classificada com a maior brevidade possível.

Artigo 9º

Transmissora de Informação Classificada

1. A Informação Classificada será transmitida entre as Partes através de canais aprovados conjuntamente pelas Entidades Nacionais de Segurança.

2. As Partes podem transmitir Informação Classificada por meios electrônicos, de acordo com os procedimentos de segurança aprovados conjuntamente pelas Entidades Nacionais de Segurança.

3. A transmissão de Informação Classificada volumosa ou em grande quantidade será aprovada em cada caso por ambas as Entidades Nacionais de Segurança.

4. A Entidade Nacional de Segurança da parte Destinatária confirmará, por escrito, a recepção de Informação Classificada.

Artigo 10º

Uso e cumprimento

1. A Informação Classificada transmitida só poderá ser utilizada para os fins a que foi transmitida.

2. Cada Parte informará as suas pessoas singulares e coletivas da existência do presente Acordo, sempre que esteja envolvida Informação Classificada.

3. Cada Parte assegurará que todas as pessoas singulares e coletivas, que recebam Informação Classificada, respeitem as obrigações do presente Acordo.

4. A Parte Destinatária não transmitirá Informação Classificada a uma Terceira Parte sem autorização prévia escrita da Parte Transmissora.

Artigo 11º

Medidas de segurança para Contratos Classificados

1. Uma Parte que pretenda celebrar um Contrato Classificado com um Contratante da outra Parte, ou que pretenda autorizar um dos seus Contratantes a efetuar um Contrato Classificado no território da outra Parte, no âmbito de um projeto classificado, obterá, através da respectiva Entidade Nacional de Segurança, garantia escrita prévia da Entidade Nacional de Segurança da outra Parte, em como o Contratante é detentor de um Credenciamento de Segurança de Pessoa Coletiva com o grau de classificação de segurança adequado.

2. Devem constar em instrumento jurídico apropriado, nos termos do presente Acordo e do Direito interno de cada Parte, as se-guintes obrigações para o Contratante:

a) Assegurar que as suas instalações estão em condições de proteger corretamente a Informação Classificada;

b) Estar habilitado com a classificação de segurança apropriada;

c) Garantir o grau de classificação de segurança do pessoal adequado às pessoas que necessitem ter acesso a uma dada Informação Classificada;

d) Assegurar que todas as pessoas que tenham acesso a Informação Classificada es-tejam informadas das suas responsabilidades sobre proteção de Informação Classificada, em conformidade com o Direito interno;

e) Permitir inspeções de segurança às suas instalações.

3. Qualquer sub-contratante deverá cumprir as mesmas obrigações de segurança que o Contratante.

4. A Entidade Nacio-nal de Segurança detém a competência para assegurar o cumprimento pelo Contratante das disposições previstas no parágrafo 2 do presente Artigo.

5. Logo que sejam desencadeadas negociações pré-contratuais entre pessoas singulares ou coletivas que residam ou estejam situadas no território de uma das Partes e outras pessoas singulares ou coletivas que residam ou estejam situadas no território da outra Parte para a celebração de atos contratuais classifi-cados, a Entidade Nacional de Segurança ou a entidade responsável pela classificação em cujo território será cumprido o contrato informará a outra Parte sobre a classificação de segurança atribuída à Informação Classificada relacionada com o contrato em negociação.

6. Qualquer Contrato Classificado celebrado entre pessoas singulares ou coletivas das Partes, nos termos do presente Acordo, deverá incluir uma Instrução de Segurança do Projecto identificando os seguintes aspectos:

a) Guia de Classificação de Segurança do Projeto e lista da Informação Classificada;

b) Procedimentos para a comunicação de alterações à classificação de segurança de Informação Classificada;

c) Canais de comunicação e meios de transmissão electrônica;

d) Procedimento para o transporte de Informação Classificada;

e) Entidades responsáveis pela coordenação e salvaguarda de Informação Classificada relacionada com o Contrato Classificado;

f) Obrigatoriedade de notificação de qualquer comprometimento ou suspeita de comprometimento de Informação Classificada.

7. Deverá ser enviada cópia da Instrução de Segurança do Projeto de qualquer Contrato Classificado à Entidade Nacional de Segurança da Parte em cujo território o Contrato Classificado será cumprido, de forma a garantir adequada supervisão de segurança e controle.

8. Os representantes das Entidades Nacionais de Segurança podem efetuar visitas mútuas a fim de verificarem a eficácia das medidas adotadas pelo Contratante na proteção de Informa-ção Classificada relativa ao Contrato Classificado. O aviso da visita deverá ser efetuado com uma antecedência mínima de trinta dias.

Artigo 12º
Visitas

1. As visitas que envolvam acesso a Informação Classificada por nacionais de uma Parte à outra Parte estão sujeitas a autorização prévia escrita conferida pela Entidade Nacional de Segurança da Parte anfitriã, de acordo com o respectivo Direito interno.

2. As visitas que envolvam acesso a Informação Classificada serão autorizadas por uma Parte aos visitantes da outra Parte, apenas se estes:

a) Possuírem Credenciamento de Segurança de Pessoa Singular apropriada concedida pela Entidade Nacional de Segurança ou outra autoridade relevante da parte visitante; e

b) Estiverem autorizados a receber ou a ter acesso à Informação Classificada fundamentado na Necessidade de Conhecer, de acordo com o Direito interno.

c) Entidade Nacional de Segurança da Parte visitante notificará a visita planejada à Entidade competente da Parte anfitriã, endereçando um pedido de visita com uma antecedência mínima de trinta dias à data prevista para a visita.

3. Em casos urgentes, o pedido de visita poderá ser efectuado com uma antecedência mínima de sete dias. 5.

4. O pedido de visita deverá incluir:

a) O nome e o sobrenome do visitante, a data e o local de nascimento, nacionalidade e o número do passaporte ou bilhete de identidade;

b) O nome da entidade que o visitante representa ou a que pertence;

c) Nome e endereço da entidade a visitar;

d) Certificação do Credenciamento de Segurança de Pessoa Singular do visitante e a respectiva validade;

e) Objeto e propósito da visita ou visitas;

f) A data prevista para a visita ou visitas e respectiva duração, e, em caso de visitas recorrentes, deverá ser referido o período total das visitas;

g) Nome e número de telefone do contacto da instituição ou instalação a visitar, os contactos prévios e quaqluer outra informação que seja útil para justificar a visita ou visitas;

h) A data, a assinatura e a aposição do selo oficial da Entidade Nacional de Segurança competente.

5. A Entidade Nacional de Segurança da Parte que recebe o pedido de visita examinará e decidirá sobre o pedido e informará de sua decisão a Entidade Nacional de Segurança da Parte requerente.

6. As visitas de pessoas de uma Terceira Parte que impliquem acesso a Informação Classificada da Parte Transmissora apenas serão autorizadas mediante consentimento escrito da Entidade Nacional de Segurança da Parte Transmissora.

7. Uma vez aprovada a visita, a Entidade Nacional de Segurança da parte anfitriã fornecerá cópia do pedido de visita ao encarregado de segurança da organização a ser visitada.

8. A validade da autorização da visita não deverá exceder os doze meses.

9. Para qualquer projeto ou contrato, as Entidades Nacionais de Segurança poderão acordar em elaborar listas de pessoas autorizadas a efetuar visitas recorrentes. Essas listas são válidas por um período inicia de doze meses.

10. Após aprovação das listas pelas Entidades Nacionais de Segurança, os termos das visitas específicas serão diretamente acordados com os representantes das entidades a serem visitadas, nos termos do presente Acordo.

Artigo 13º

Comprometimento da Informação Classificada

1. Em caso de quebra de segurança que resulte em comprometimento ou suspeita de comprometimento de Informação Classificada com origem ou recebida da outra Parte, a Enti-dade Nacional de Segurança da Parte onde ocorra a quebra de segurança ou comprometimento de Informação Classificada informará prontamente a Entidade Nacional de Segurança da outra Parte e instaurará a correspondente investigação.

2. Se a quebra de segurança ou comprometimento de Informação Classificada ocorrer num outro Estado que não o das Partes, a Entidade Nacional de Segurança da Parte transmissora atuará em conformidade com o parágrafo 1 do presente Artigo.

3. A outra Parte, se necessário, colaborará na investigação.

4. Em qualquer caso, a outra Parte será informada, por escrito, dos resultados da investi-gação, incluindo a indicação das razões da quebra e comprometimento de segurança, a extensão dos danos e as conclusões da investigação.

Artigo 14º

Encargos

Cada Parte assumirá os encargos que para si advenham da aplicação e supervisão do Presente Acordo.

Artigo 15º

Solução de controvérsias

Qualquer diferendo sobre a interpretação ou a aplicação das medidas previstas no presente Acordo será resolvido por via diplomática.

Artigo 16º

Revisão

1. O presente Acordo pode ser objecto de revisão a pedido de qualquer das Partes.
2. As emendas entrarão em vigor nos termos previstos no Artigo 18º do presente Acordo.

Artigo 17º

Vigência e denúncia

1. O presente Acordo permanecerá em vigor por um período indeterminado.
2. Qualquer das Partes poderá, a qualquer momento, denunciar o presente Acordo.
3. A denúncia deverá ser notificada, por escrito e por via diplomática, produzindo efeitos seis meses após a data da recepção da respectiva notificação.
4. Em caso de denúncia, a Informação Classificada trocada na vigência do presente Acordo continuará a ser tratada em conformidade com as disposições do mesmo, até que a Parte Transmissora dispense a Parte Destinatária dessa obrigação.

Artigo 18º

Entrada em vigor

1. Cada uma das Partes notificará a outra, por escrito e por via diplomática, que todos os pro-cedimentos internos necessários para a entrada em vigor do presente Acordo foram cumpridos.
2. O presente Acordo entrará em vigor no trigésimo dia após a recepção da última das notificações referidas no número 1 do presente Artigo.

Em fé do que, os signatários, devidamente autorizados para o efeito, assinam o presente Acordo.

Feito na Cidade do Porto em 13 de Outubro de 2005, em dois originais em língua portuguesa.

PELA REPÚBLICA FEDERATIVA DO BRASIL

Samuel Pinheiro Guimarães
Ministro de Estado, interino, das Relações Exteriores

PELA REPÚBLICA PORTUGUESA

João Gomes Cravinho
Secretário de Estado dos Negócios Estrangeiros e Cooperação

VERSÃO PUBLICADA

Aprova o texto do Acordo entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia sobre Proteção Mútua de Informações Classificadas, assinado em Moscou, em 13 de agosto de 2008.

Observação: as equivalências entre os graus de sigilo não estão atualizadas, pois o acordo é anterior à Lei nº 12.527/2011 (Lei de Acesso à Informação). Texto da emenda, embora assinado, ainda não está em vigor. Mais informações neste link.

Faço saber que o Congresso Nacional aprovou, e eu, José Sarney, Presidente do Senado Federal, nos termos do *Parágrafo único* do art. 52 do Regimento Comum e do inciso XXVIII do art. 48 do Regimento Interno do Senado Federal, promulgo o seguinte

DECRETO LEGISLATIVO Nº 802, DE 2010

Aprova o texto do Acordo entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia sobre Proteção Mútua de Informações Classificadas, assinado em Moscou, em 13 de agosto de 2008.

O Congresso Nacional decreta:

Art. 1º Fica aprovado o texto do Acordo entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia sobre Proteção Mútua de Informações Classificadas, assinado em Moscou, em 13 de agosto de 2008.

Parágrafo único. Ficam sujeitos à aprovação do Congresso Nacional quaisquer atos que possam resultar em revisão do referido Acordo, bem como quaisquer ajustes complementares que, nos termos do inciso I do art. 49 da Constituição Federal, acarretem encargos ou compro-missos gravosos ao patrimônio nacional.

Art. 2º Este Decreto Legislativo entra em vigor na data de sua publicação.

Senado Federal, em 20 de dezembro de 2010.

Senador JOSÉ SARNEY

Presidente do Senado Federal

ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA FEDERAÇÃO DA RÚSSIA SOBRE PROTEÇÃO

MÚTUA DE INFORMAÇÕES CLASSIFICADAS

O Governo da República Federativa do Brasil e

O Governo da Federação da Rússia (doravante denominados "Partes"),

Reconhecendo o interesse mútuo em garantir a proteção das informações classificadas trocadas no âmbito da cooperação política, técnico-militar, econômica e outras, de conformidade com as respectivas legislações da República Federativa do Brasil e da Federação da Rússia,

Acordam o que se segue:

Artigo 1

Definições

Para os fins do presente Acordo:

a) "informação classificada" significa qualquer dado, independentemente de sua forma, protegido em conformidade com as respectivas legislações da República Federativa do Brasil e da Federação da Rússia, transmitido ou recebido na forma estabelecida pelo presente Acordo, cujo acesso ou divulgação não autorizados pode causar dano à segurança ou aos interesses da República Federativa do Brasil ou da Federação da Rússia;

b) "meios de armazenamento de informações classificadas" significam os objetos materiais, inclusive meios físicos nos quais as informações classificadas são expressas na forma de símbolos, imagens, sinais, soluções técnicas e processos;

c) "marcação de classificação" significa a marcação, colocada no próprio meio de armazenamento ou na documentação que o acompanha, identificadora do grau de sigilo dos dados contidos nesse meio de armazenamento;

d) "credencial de segurança" significa a autorização para acesso a informações classificadas concedida a indivíduos ou organizações;

e) "organizações credenciadas" significam os órgãos governamentais ou outras organizações credenciados pelas Partes para transmitir, receber, guardar, proteger e utilizar as infor-mações classificadas;

f) "contrato" significa o acordo concluído entre organizações credenciadas, o qual prevê a transmissão de informações classificadas no decorrer da cooperação;

g) "Parte transmissora" significa a Parte que transmite as informações classificadas à outra Parte;

h) "Parte receptora" significa a Parte à qual são transmitidas as informações classificadas.

Artigo 2

Órgãos Competentes

1. Os órgãos competentes, responsáveis pela implementação do presente Acordo (doravante denominados "órgãos competentes") são os seguintes:

a) na República Federativa do Brasil, o Gabinete de Segurança Institucional da Presidência da República;

b) na Federação da Rússia, o Serviço Federal de Segurança da Federação da Rússia.

2. As Partes deverão notificar de imediato à outra Parte, por via diplomática, sobre quaisquer alterações de seus órgãos competentes.

Artigo 3

Equivalência dos Graus de Sigilo

As Partes concordam que os seguintes graus de sigilo são equivalentes da seguinte forma:

Na República Federativa do Brasil	Na Federação da Rússia
SECRETO (Secret)	Cobepmehho cekpetho (Top Secret)
CONFIDENCIAL (Confidential)	Cekpetho (Secret)

Artigo 4

Proteção das Informações Classificadas

1. As Partes, em conformidade com as respectivas legislações da República Federativa do Brasil e da Federação da Rússia, deverão:

a) assegurar a proteção das informações classificadas;

b) aplicar, com relação às informações classificadas, as mesmas medidas de proteção prevista relativamente às próprias informações classificadas, de grau de sigilo equivalente, em conformidades com o Artigo 3 do presente Acordo;

c) utilizar as informações classificadas recebidas da organização credenciada da outra Parte exclusivamente para os fins previstos na sua transmissão;

d) não permitir a uma terceira parte o acesso às informações classificadas, sem prévia concordância por escrito da Parte transmissora.

2. O acesso às informações classificadas deverá ser permitido apenas às pessoas cujo conhecimento das mencionadas informações seja necessário para o cumprimento das obrigações funcionais e para os fins previstos em sua transmissão, possuidoras de apropriada credencial de segurança.

Artigo 5

Transmissão das Informações Classificadas

1. Caso uma organização credenciada de uma Parte tencione transmitir informações classificadas a uma organização credenciada da outra Parte, ela deverá solicitar previamen-te à autoridade competente de sua Parte uma confirmação por escrito de que a organização credenciada da outra Parte possui a correspondente credencial de segurança para acesso a informações classificadas.A autoridade competente da Parte deverá solicitar à autoridade competente da outra Parte uma confirmação por escrito da existência de credencial de segurança apropriada pela organização daquela Parte.

2. Em cada caso especifico, a decisão de transmitir informações classificadas deverá ser tomada em conformidade com a respectiva legislação da República Federativa do Brasil ou da Federação da Rússia.

3. Os meios de armazenamento de informações classificadas deverão ser transmitidos por via diplomática ou por outros métodos acordados entre as Partes. A organização credenciada da Parte receptora deverá confirmar o recebimento das informações classificadas.

4. Com a finalidade de transmitir meios de armazenamento de informações classificadas de grande volume, as autoridades competentes deverão acordar sobre o método e a rota de transporte, bem como sobre a forma de escolta.

5. As informações classificadas poderão ser transmitidas por meios técnicos protegidos, mediante entendimento entre as autoridades competentes das Partes.

Artigo 6

Tratamento das Informações Classificadas

1. Ao receber os meios de armazenamento de informações classificadas, a organização credenciada responsável por sua recepção deverá, complementarmente, promover a marcação de classificação correspondente ao grau de sigilo equivalente, conforme definido no Artigo 3 do presente Acordo.

2. A obrigação de marcação de classificação deverá ser aplicada nos meios de armazena-mento de informações classificadas obtidas como resultado de tradução, cópia ou reprodução.

3. As informações classificadas geradas com base em informações classificadas recebi-das da outra Parte deverão possuir grau de sigilo não inferior ao grau de sigilo das informações classificadas recebidas.

4. As informações classificadas deverão ser submetidas a tratamento em conformidade com as exigências previstas nas respectivas legislações da Respectiva Federativa do Brasil e da Federação da Rússia.

5. Os meios de armazenamento de informações classificadas deverão ser devolvidos ou destruídos mediante autorização por escrito da organização credenciada da Parte transmissora.

6. A destruição dos meios de armazenamento de informações classificadas deverá ser documentada, sendo que o processo de destruição deverá excluir qualquer possibilidade de reprodução ou restauração das informações.

7. A organização credenciada da Parte transmissora deverá ser informada, por escrito, sobre a devolução ou a destruição dos meios de armazenamento de informações classificadas.

8. A marcação de classificação dos meios de armazenamento de informações classifi-cadas recebidas somente poderá ser alterada pela organização credenciada da Parte receptora após autorização por escrito da organização credenciada da Parte transmissora.A organização credenciada da Parte transmissora deverá notificar a organização cre-denciada da Parte receptora, por escrito, sobre quaisquer alterações do grau de sigilo das infor-mações classificadas.

Artigo 7
Contratos

Os contratos firmados entre as organizações credenciadas deverão conter uma seção es-pecifica com os seguintes itens:

a) relação das informações classificadas e seu grau de sigilo;

b) particularidades sobre proteção e tratamento dos meios de armazenamento de infor-

c) mações classificadas;

d) procedimentos de resolução de controvérsias sobre o tratamento das informações classificadas, eventualmente surgidas no decorres da implementação do contrato;

e) procedimento de reparação de possível dano resultante da divulgação não autorizada das informações classificadas.

Artigo 8
Visitas

1. Visitas de representantes de organização credenciada de uma Parte, com previsão de seu acesso a informações classificadas deverão ser sujeitas a prévia autorização por escrito, concedida pela autoridade competente da outra Parte após consultar a organizar a ser visitada. A autorização para tal visita deverá ser concedida apenas às pessoas mencionadas no parágrafo 2 do Artigo 4 do presente

Acordo.

2. O requerimento sobre a possibilidade de realização da visita deverá ser submetido pela autoridade competente da Parte visitante à autoridade competente da Parte anfitriã no mínimo trinta (30) dias antes da data da visita pretendida.

3. A autoridade competente da Parte anfitriã deverá notificar à autoridade competente da Parte visitante sobre os resultados do processo de consulta, no mínimo dez (10) dias antes da visita pretendida.

4. O requerimento para a visita pretendida deverá ser formalizado em conformidade com as respectivas legislações da República Federativa do Brasil e da Federação da Rússia e deverá conter os seguintes dados:

a) nome completo da pessoa visitante, data e local de nascimento, nacionalidade, número do passaporte, ocupação ou função, local de trabalho e seu grau de credencial de segurança;

b) períodos previstos para a visita, razão social e endereço da organização credenciada a ser visitada, bem como nome completo e função da pessoa a ser visitada;

c) objetivo e fundamentos da visita, assim como natureza das questões a serem discutidas.

5. Durante a visita, os representantes da organização credenciada da Parte visitante deverão conter as regras relativas ao tratamento das informações classificadas da Parte anfitriã.

Artigo 9º
Violação das Exigências Relativas à Proteção das Informações Classificadas

1. Qualquer violação das exigências relativas à proteção das informações classificadas que tenha resultado ou possa resultar no acesso ou na divulgação não autorizada de informações classificadas, identificada por uma organização credenciada ou pela autoridade competente de uma das partes, deverá ser imediatamente notificada à autoridade competente da outra Parte.

2. A autoridade competente da Parte que notificou a violação deverá realizar a investigação do incidente e informar à autoridade competente da outra Parte sobre os resultados de tal investigação e sobre as devidas medidas corretivas adotadas.

3. Os procedimentos de reparação do dano ocasionado pela violação das exigências relativas à proteção das informações classificadas deverão ser definidos em cada caso concreto, por acordo entre as organizações credenciadas e, quando necessário, com a participação das autoridades competentes das Partes.

Artigo 10
Despesas

Cada Parte assumirá as próprias despesas relacionadas à implementação do presente Acordo.

Artigo 11

Consultas

As autoridades competentes, para os fins de implementação do presente Acordo, realizarão consultas a pedido de uma delas.

Artigo 12

Relação com Outros Acordos

Os dispositivos relativos à proteção das informações classificadas contidos em outros acor-dos e entendimentos firmados entre as Partes, bem como entre as autoridades competentes e organizações credenciais das Partes, continuarão em vigor, desde que não contradigam os dispositivos do presente Acordo.

Artigo 13

Solução de Controvérsias

1. Quaisquer controvérsias relativas à interpretação e à aplicação dos dispositivos do presen-te Acordo que possam ocorrer entre as Partes deverão ser resolvidas por meio de negociações e de consultas entre as autoridades competentes e, quando necessário, por via diplomática.

2. Durante a resolução das controvérsias, as Partes continuarão a cumprir todas suas obri-gações previstas no presente Acordo.

Artigo 14

Emendas

O presente Acordo poderá ser objeto de emendas por consentimento mútuo expresso por escrito entre as Partes.

Artigo 15

Disposições Finais

1. O presente Acordo entrará em vigor trinta (30) dias após a data de recebimento, por via diplomática, da última notificação escrita sobre o cumprimento, pelas Partes, dos respectivos procedimentos internos necessários para sua entrada em vigor.

2. O presente Acordo terá vigência por prazo indeterminado.

3. Qualquer das Partes poderá denunciar o presente Acordo, por meio do envio à outra Parte, por via diplomática, de notificação escrita sobre sua intenção denunciá-lo. Nesse caso, a vigência do presente Acordo cessará ao fim de seis (6) meses contados a partir da data de recebimento de tal notificação.

4. No caso de denúncia do presente Acordo, continuarão a ser aplicadas com relação às informações classificadas as medidas para sua proteção previstas no presente Acordo, até que essas informações sejam desclassificadas de acordo com a forma estabelecida.

Feito em Moscou, aos 13 de agosto de 2008, em dois exemplares originais, em portu-guês, russo e inglês, sendo todos os textos igualmente autênticos. Em caso de divergência na interpretação do presente Acordo, prevalecerá o texto em inglês.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

JORGE ARMANDO FÊLIX
Ministro-chefe do Gabinete de Segurança Institucional da Presidência da República

PELO GOVERNO DA FEDERAÇÃO DA RÚSSIA

SERGUEI MIKHAILOVITCH SMIRNOV
Primeiro Vice-Diretor do Serviço Federal de Segurança da Rússia

DECRETO Nº 9.273, DE 31 DE JANEIRO DE 2018 (ESPANHA)

VERSÃO PUBLICADA

Promulga o Acordo entre a República Fede-rativa do Brasil e o Reino da Espanha Relativo à Troca e Proteção Mútua de Informações Classi-ficadas, firmado em Brasília, em 15 de abril de 2015.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 84, *caput* , inciso IV, da Constituição, e

Considerando que o Acordo entre a República Federativa do Brasil e o Reino da Espanha Relativo à Troca e Proteção Mútua de Informações Classificadas foi firmado em Brasília, em 15 de abril de 2015;

Considerando que o Congresso Nacional aprovou o Acordo por meio do Decreto Legislativo nº 82, de 25 de maio de 2017; e

Considerando que o Acordo entrou em vigor para a República Federativa do Brasil, no plano jurídico externo, em 6 de agosto de 2017, nos termos de seu Artigo 12;

DECRETA :

Art. 1º Fica promulgado o Acordo entre a República Federativa do Brasil e o Reino da Espanha Relativo à Troca e Proteção Mútua de Informações Classificadas, firmado em Brasília, em 15 de abril de 2015, anexo a este Decreto.

Art. 2º São sujeitos à aprovação do Congresso Nacional atos que possam resultar em revisão do Acordo e ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional, nos termos do inciso I do *caput* do art. 49 da Constituição.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Brasília, 31 de janeiro de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Aloysio Nunes Ferreira Filho

Este texto não substitui o publicado no DOU de 1º.2.2018

ACORDO ENTRE A REPÚBLICA FEDERATIVA DO BRASIL E O REINO DA ESPANHA RELATIVO À TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÕES CLASSI-FICADAS

A República Federativa do Brasil e

O Reino da Espanha

(doravante denominados “Partes”),

Reconhecendo a necessidade de garantir a segurança das Informações Classificadas troca-das no âmbito de instrumentos de cooperação ou contratos celebrados entre as mesmas, suas pessoas físicas, órgãos e entidades credenciadas; e

Desejando estabelecer um conjunto de regras e procedimentos sobre segurança de Infor-mações Classificadas em conformidade com o ordenamento jurídico da República Federativa do Brasil e do Reino de Espanha;

Acordam o seguinte:

Artigo 1
Objeto e âmbito de aplicação

1. O presente Acordo estabelece regras e procedimentos para a segurança de InformaçõesClassificadas trocadas entre as Partes, suas pessoas físicas, órgãos e entidades credenciadas.

2. Nenhuma das Partes poderá invocar o presente Acordo com o objetivo de obter Informação Classificada que a outra Parte tenha recebido de uma Terceira Parte.

Artigo 2
Definições

Para efeitos do presente Acordo:

a) “Autoridade Nacional de Segurança – ANS” designa a autoridade indicada pelas Partes para a implementação do presente Acordo;

b) “Comprometimento da segurança” designa qualquer ato ou omissão, intencional ou aci-dental, do qual resulte comprometimento ou risco de comprometimento da Informação Classi-ficada;

c) “Contrato Sigiloso” designa qualquer ajuste, convênio ou acordo de cooperação cujo objeto ou execução implique no tratamento de Informações Classificadas;

d) “Habilitação Pessoal de Segurança” na Espanha e “Credencial de Segurança” no Brasil designa à garantia por parte da Autoridade Nacional de Segurança de que uma pessoa atende aos requisitos para ter acesso à Informação Classificada, em conformidade com as respectivas legislações

nacionais;

e) “Habilitação de Segurança de Estabelecimento” na Espanha e “Habilitação de Segurança” no Brasil designa a garantia por parte da Autoridade Nacional de Segurança de que um órgão ou entidade possui, do ponto de vista da segurança, capacidade material e organizacional para produzir e gerir Informações Classificadas, em conformidade com as respectivas legislações nacionais;

f) “Informação Classificada” designa qualquer informação ou material, independente de sua forma, natureza ou método de transmissão, que contenha dados que as Partes qualifiquem como Informação Classificada e que, conforme as respectivas legislações, seja marcada como tal;

g) “Instrução de Segurança de Projeto” designa os procedimentos e medidas de segurança aplicáveis a um determinado projeto ou Contrato Sigiloso;

h) “Necessidade de Conhecer” designa o princípio segundo o qual somente será dado acesso à Informação Classificada a uma pessoa que tenha necessidade comprovada de fazê-lo em razão de suas funções oficiais, com amparo no qual a informação foi transferida à Parte Receptora;

i) “Parte de Origem” designa a Parte que transmite a Informação Classificada à outra Parte;

j) “Parte Receptora” designa a Parte para a qual é transmitida a Informação Classificada;

k) “Terceira Parte” designa qualquer organização internacional ou Estado que não seja Parte no presente Acordo;

l) “Tratamento” designa a recepção, produção, reprodução, tradução, utilização, acesso, transporte, transmissão, distribuição, armazenamento e controle de Informações Classificadas.

Artigo 3

Autoridades Nacionais de Segurança

1. As Autoridades Nacionais de Segurança de cada Parte responsáveis pela aplicação e implementação do presente Acordo são:

Pela República Federativa do Brasil:

Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República (GSIPR)

Pelo Reino da Espanha:

Secretário de Estado, Diretor do Centro Nacional de Inteligência (CNI).

2. As Autoridades Nacionais de Segurança informar-se-ão mutuamente sobre a respectiva legislação em vigor que regulamenta a segurança de Informações Classificadas.

3. Com vistas a assegurar uma estreita cooperação na aplicação do presente Acordo, as Autoridades Nacionais de Segurança poderão consultar-se sempre que solicitado por uma delas.

4. Representantes da Autoridade Nacional de Segurança de uma Parte poderão efetuar visitas aos estabelecimentos da Autoridade Nacional de Segurança da outra Parte com a finalidade de conhecer procedimentos e medidas de segurança aplicáveis às Informações Classificadas.

5. Se solicitado, as Partes, por meio das suas Autoridades Nacionais de Segurança, tendo em conta o respectivo Direito interno em vigor, colaborarão entre si no decurso dos procedimentos necessários ao Credenciamento de Segurança de suas pessoas físicas que tenham residido ou residam no território da outra Parte.

6. As Autoridades Nacionais de Segurança assegurarão que as pessoas físicas, órgãos e entidades credenciadas de seu país cumprirão as obrigações do presente Acordo.

Artigo 4

Graus de Classificação de Sigilo

1. As Partes acordam que os seguintes graus de sigilo são equivalentes:

República Federativa do Brasil (Português)	Reino da Espanha (Espanhol)
ULTRASSECRETO	SECRETO
SECRETO	RESERVADO
	CONFIDENCIAL
RESERVADO	DIFUSIÓN LIMITADA

2. Parte Receptora concederá à Informação Classificada recebida o grau de sigilo equivalente ao expressamente concedido pela Parte de Origem, em conformidade com o disposto no parágrafo 1 deste artigo.

3. A Parte Receptora não poderá reclassificar ou desclassificar a Informação Classificada recebida sem a prévia autorização escrita da Autoridade Nacional de Segurança da Parte de Origem.

4. A Parte de Origem informará à Parte Receptora sobre a reclassificação ou desclassificação da Informação Classificada transmitida.

Artigo 5

Tratamento da Informação Classificada

1. O acesso à Informação Classificada será limitado às pessoas que tenham Necessidade de Conhecer e que sejam possuidoras de uma Habilitação Pessoal de Segurança ou uma Cre-dencial de Segurança.

2. As Partes reconhecerão reciprocamente as Credenciais de Segurança emitidas de acordo com a Legislação da outra Parte.

3. A Informação Classificada transmitida somente poderá ser utilizada para os fins para os quais foi transmitida.

4. As traduções e reproduções de Informações Classificadas serão efetuadas em conformidade com os seguintes procedimentos:

a) os tradutores deverão estar credenciados no nível correspondente ao grau de sigilo da Informação Classificada a ser traduzida;

b) as traduções e reproduções deverão estar marcadas com o mesmo grau de sigilo da Informação Classificada original;

c) as traduções e reproduções serão controladas pelas Partes;

d) as traduções deverão conter uma indicação apropriada, no idioma para o qual foram traduzidas, de que contêm Informação Classificada recebida da Parte de Origem; e

e) o número de reproduções e cópias se limitará ao requerido para os fins oficiais.

5. Nenhuma Informação Classificada poderá ser destruída e deverá ser devolvida à Parte de Origem quando não mais for necessária.

6. A Informação Classificada marcada como ULTRASSECRETO no Brasil ou SECRETO na Es-panha, somente poderá ser traduzida ou reproduzida mediante autorização escrita da Autoridade Nacional de Segurança da Parte de Origem.

Artigo 6

Transmissão entre as Partes

1. A Informação Classificada será transmitida entre as Partes por via diplomática ou pessoas físicas, órgãos ou entidades devidamente credenciados e autorizados pela Parte de Origem.

2. .A Informação Classificada poderá ser transmitida por meio de sistemas de comunicação protegidos, redes ou outros meios eletromagnéticos aprovados por ambas as Partes.

3. A transmissão de Informação Classificada volumosa ou em grande quantidade será aprovada, em cada caso, por ambas as Autoridades Nacionais de Segurança.

4. A Autoridade Nacional de Segurança da Parte Receptora confirmará, por escrito, o recebimento de Informação Classificada.

5. A Parte Receptora não transmitirá Informação Classificada a uma Terceira Parte, ou a qualquer pessoa física, órgão ou entidade que tenha a nacionalidade de um terceiro Estado, sem autorização prévia, por escrito, da Parte de Origem.

Artigo 7

Contratos Sigilosos

1. No caso de Contratos Sigilosos celebrados ou a celebrar que prevejam a transmissão de Informações Classificadas será exigido o Credenciamento de Segurança dos contratantes pelas

Autoridades Nacionais de Segurança das Partes.

2. Qualquer subcontratado também deverá ser credenciado, obrigando-se pela segurança das Informações Classificadas.

3. Os Contratos Sigilosos deverão conter cláusulas que contemplem os seguintes aspectos:

a) identificação das Informações Classificadas;

b) previsão de uma instrução de Segurança do Projeto que defina um conjunto de procedimentos e medidas de segurança aplicáveis às Informações Classificadas;

c) responsabilização pelos danos decorrentes de qualquer Comprometimento de Segurança;

d) obrigação de informar qualquer Comprometimento de Segurança à sua Autoridade Nacional de Segurança;

e) vedação de subcontratação total ou parcial do objeto sem expressa autorização do outrocontratante;

f) previsão dos canais de comunicação e meios para transmissão das Informações Classificadas;

g) obrigação de que o contratado, seus empregados, gerentes ou representantes, mantenham o correspondente sigilo;

h) necessidade de que as pessoas que terão acesso às Informações Classificadas, estejam identificadas; e

i) responsabilização pelo não cumprimento dos procedimentos e medidas de segurança aplicáveis às Informações Classificadas.

4. Uma cópia do Contrato Sigiloso deverá ser remetida à Autoridade Nacional de Segurança da Parte onde o Contrato Sigiloso será cumprido para verificação do cumprimento das Cláusulas de Segurança.

Artigo 8
Visitas

1. As visitas que envolvam acesso à Informação Classificada por nacionais de uma Parte à outra Parte estarão sujeitas à autorização prévia, por escrito, das Autoridades Nacionais de Segurança.

2. O pedido de visita será apresentado por intermédio das Autoridades Nacionais de Segurança com um prazo de antecedência mínimo de 30 (trinta) dias à data prevista para a visita.

3. As visitas serão autorizadas por uma Parte aos visitantes da outra Parte, somente se estes:

a) possuírem Habilitação de Segurança ou Credencial de Segurança válida concedida pelo seu país de origem; e

b) estiverem autorizados a receber ou a ter acesso à Informação Classificada fundamentado

na Necessidade de Conhecer.

4. O pedido de visita será apresentado por intermédio das Autoridades Nacionais de Segurança, devendo incluir as seguintes informações:

a) dados pessoais do visitante: nome e sobrenome, data e local de nascimento, nacionalidade, passaporte ou outra cédula de identidade;

b) indicação do órgão ou da entidade à qual o visitante pertence;

c) dados relacionados à visita: período da visita, objeto e propósito da visita, indicação da entidade que pretende visitar;

d) indicação de um contato no órgão ou entidade que pretende visitar, com nome e sobrenome e número de telefone;

e) indicação do grau de sigilo da informação que se pretende acessar; e

f) certificação da posse de uma Habilitação de Segurança ou uma Credencial de Segurança do visitante, na qual conste o grau de sigilo, o prazo de validade e qualquer limitação que conste na mesma.

5. A Autoridade Nacional de Segurança do país anfitrião notificará a Autoridade Nacional de Segurança do país do visitante de sua decisão com um prazo de antecedência mínima de 10 (dez) dias à data prevista para a visita.

6. Uma vez autorizada a visita, a Autoridade Nacional de Segurança do país anfitrião enviará uma cópia do pedido de visita à entidade a ser visitada.

7. Nos casos de projetos ou contratos que exijam visitas recorrentes, poderão ser elaboradas listas das pessoas autorizadas. Tais listas não poderão ter validade superior a 12 (doze) meses.

Artigo 9
Comprometimento de Segurança

1. Em caso de Comprometimento de Segurança relacionado à Informação Classificada que envolva as Partes do presente Acordo, a Autoridade Nacional de Segurança da Parte onde ocorre o Comprometimento de Segurança informará, prontamente, a Autoridade Nacional de Segurança da outra Parte.

2. A Parte onde ocorre o Comprometimento de Segurança deverá investigar ou colaborar com a investigação do incidente e informar, tão logo possível à outra Parte, sobre o resultado da investigação e as medidas de correção aplicadas.

Artigo 10
Custos

1. O presente Acordo não prevê a geração de qualquer custo.

2. Caso ocorra algum custo, cada uma das Partes arcará com as suas próprias despesas decorrentes da aplicação e supervisão de todos os aspectos do presente Acordo, em conformidade com suas legislações.

Artigo 11

Solução de Controvérsia

1. Qualquer controvérsia sobre a interpretação ou a implementação do presente Acordo será resolvida por via diplomática com a participação das Autoridades Nacionais de Segurança.

2. Durante o período de resolução das controvérsias o Acordo deverá continuar sendo cumprido.

Artigo 12

Entrada em vigor

O presente Acordo entrará em vigor 30 (trinta dias) após a recepção da última notificação, por escrito e por via diplomática, informando que foram cumpridos os requisitos internos das Partes.

Artigo 13

Revisão

1. O presente Acordo poderá ser emendado com base no consentimento mútuo, por escrito, das Partes.

2. As emendas entrarão em vigor nos termos do artigo 12 do presente Acordo.

Artigo 14

Vigência e Denúncia

1. O presente Acordo permanecerá em vigor por um período indeterminado.

2. As Partes poderão, a qualquer momento, denunciar o presente Acordo.

3. A denúncia deverá ser notificada por escrito e por via diplomática com no mínimo 6 (seis) meses de antecedência.

4. Não obstante a denúncia, toda Informação Classificada trocada em virtude do presente Acordo continuará a ser protegida em conformidade com as disposições do mesmo, até que a Parte de Origem dispense a Parte Receptora dessa obrigação.

Em fé do que, os representantes devidamente autorizados por seus respectivos governos, assinam este Acordo, em Brasília, no dia 15 do mês de abril do ano de 2015, em duas vias ori-ginais, nas versões em língua portuguesa e espanhola, sendo ambas igualmente autênticas.

PELA REPÚBLICA
FEDERATIVA DO BRASIL
General de Exército José Elito Carvalho Siqueira
Ministro de Estado
Chefe do Gabinete de Segurança Institucional da
Presidência da Repúblicada República

PELO REINO DA ESPANHA

D. José de Blas Jiménez
Diretor do Escritório Nacional de Segurança

DECRETO Nº 10.307, DE 2 DE ABRIL DE 2020 (SUÉCIA)

VERSÃO PUBLICADA

Promulga o Acordo entre a República Federativa do Brasil e o Reino da Suécia sobre Troca e Proteção Mútua de Informação Classificada, firmado em Estocolmo, em 3 de abril de 2014.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, *caput*, inciso IV, da Constituição, e

Considerando que o Acordo entre a República Federativa do Brasil e o Reino da Suécia sobre Troca e Proteção Mútua de Informação Classificada foi firmado em Estocolmo, em 3 de abril de 2014;

Considerando que o Congresso Nacional aprovou o Acordo por meio do Decreto Legislativo nº 181, de 19 de dezembro de 2018; e

Considerando que o Acordo entrou em vigor para a República Federativa do Brasil, no plano jurídico externo, em 11 de outubro de 2019, nos termos do seu Artigo 15;

DECRETA:

Art. 1º Fica promulgado o Acordo entre a República Federativa do Brasil e o Reino da Suécia sobre Troca e Proteção Mútua de Informação Classificada, firmado em Estocolmo, em 3 de abril de 2014, anexo a este Decreto.

Art. 2º São sujeitos à aprovação do Congresso Nacional atos que possam resultar em revisão do Acordo e ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional, nos termos do inciso I do *caput* do art. 49 da Constituição.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

JAIR MESSIAS BOLSONARO

Ernesto Henrique Fraga Araújo

Este texto não substitui o publicado no DOU de 3.4.2020

ACORDO ENTRE A REPÚBLICA FEDERATIVA DO BRASILE O REINO DA SUÉCIA SOBRE TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Federativa do Brasil, e

O Reino da Suécia,

(doravante denominados “Partes” ou se separadamente como “Parte”),

No interesse da segurança nacional e com a finalidade de assegurar a proteção de Informa-ções Classificadas trocadas no âmbito de instrumentos de cooperação ou contratos celebrados entre as Partes, seus indivíduos credenciados, bem como órgãos e entidades públicas e privadas;

Desejando estabelecer um conjunto de regras e procedimentos sobre a segurança de Infor-mação Classificada, em conformidade com o ordenamento jurídico das Partes em vigor,

Acordam o seguinte:

Artigo 1

Definições

Para os efeitos do presente Acordo, o termo:

a) Contrato Sigiloso - designa um contrato ou subcontrato, incluindo qualquer negociação pré-contratual, cujo objeto contenha ou envolva Informações Classificadas;

b) Informação Classificada - significa informação, independentemente da sua forma e características, trocada entre, ou produzida pelas Partes ou por qualquer entidade pública ou privada sob a jurisdição das Partes, e que, de acordo com a legislação de cada uma das Partes, foi classificada como tal e requer proteção contra perda, divulgação não autorizada ou outro comprometimento;

c) Autoridade Competente de Segurança - CSA - significa uma autoridade de segurança de uma da Parte que é responsável pela implementação dos requisitos de segurança abrangidos pelo presente Acordo;

d) Comprometimento - designa qualquer forma de utilização indevida, dano ou acesso não autorizado, alteração, divulgação ou destruição de informação classificada, bem como qualquer outra ação ou omissão, que possa resultar em perda de sua confidencialidade, integridade ou disponibilidade;

e) Autoridades de Defesa - designa as autoridades do Reino da Suécia, para as quais se aplicam os regulamentos de segurança das Forças Armadas da Suécia;

f) Habilitação de Segurança - significa a determinação por uma Autoridade de Segurança Competente de uma das Partes de que uma entidade pública ou privada localizada em seu país possui habilitação de segurança e atende as necessárias medidas de segurança dentro de uma instalação específica para o tratamento da Informação Classificada, de acordo com a legislação nacional em vigor;

g) Necessidade de conhecer - designa a condição segundo a qual o acesso à Informação

Classificada pode ser concedido a um indivíduo, para o adequado exercício de cargo, função, emprego ou atividade;

h) Parte de Origem - significa a Parte, bem como qualquer entidade pública ou privada sob sua jurisdição, que envia a Informação Classificada à Parte Receptora nos termos deste Acordo;

i) Outras Autoridades - Autoridades no Reino da Suécia, para as quais se aplicam as regras de segurança do Conselho da Polícia Nacional;

j) Credencial de Segurança Pessoal - significa uma determinação por uma Autoridade de Segurança Competente de uma das Partes de que um indivíduo tenha recebido uma credencial de segurança para o Tratamento de Informação Classificada, de acordo com a sua legislação nacional em vigor;

k) Parte Receptora - designa a Parte, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição, que recebe Informações Classificadas da outra Parte, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição, nos termos deste Acordo;

l) Credenciamento de Segurança - designa o processo de emissão de uma Habilitação de Segurança ou de uma Credencial de Segurança Pessoal por uma Autoridade de Segurança Com-petente, em conformidade com a legislação nacional das Partes;

m) Terceiros - designa os Estados, qualquer organização internacional, governos ou indivíduos que representam organismos estatais ou organizações, que não sejam Partes do presente Acordo; e

n) Tratamento da Informação Classificada - designa um conjunto de ações referentes à produ-ção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da Informação Classificada, em qualquer grau de sigilo.

Artigo 2
Níveis de Classificação de Sigilo

1. As Partes, de acordo com sua legislação nacional, concordam que os níveis de classificação de sigilo correspondem entre si e são considerados como equivalentes:

a) Para Informações Classificadas fornecidas pelas Autoridades de Defesa do Reino da Suécia:

No Reino da Suécia Autoridades de Defesa	Na República Federativa do Brasil

HEMLIG/TOP SECRET	ULTRASSECRETO
HEMLIG/SECRET	SECRETO
HEMLIG/CONFIDENTIAL	SECRETO
HEMLIG/RESTRICTED	RESERVADO

b) Para Informações Classificadas fornecidas por Outras Autoridades do Reino da Suécia:

No Reino da Suécia Autoridades de Defesa	Na República Federativa do Brasil
HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	ULTRASSECRETO
HEMLIG	SECRETO

c) Para Informações Classificadas fornecidas por República Federativa do Brasil:

Na República Federativa do Brasil	No Reino da Suécia	
	Autoridades de Defesa	Outras Autoridades
ULTRASSECRETO	HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
SECRETO	HEMLIG/SECRET	HEMLIG

2. Qualquer Informação Classificada fornecida com base no presente Acordo deverá ser marcada com o nível de classificação de sigilo adequado de acordo com a legislação nacional da Parte de Origem e, onde for apropriado, possuir estampado o nome do país detentor e forne-cedor da Informação Classificada.

3. As Partes deverão marcar todas as Informações Classificadas recebidas da outra Parte com o nível de classificação equivalente, de acordo com o parágrafo 1 deste Artigo.

4. As Partes deverão comunicar uma à outra quaisquer modificações na legislação nacional

relacionadas às marcas de classificação de sigilo.

5. A Parte de Origem deverá:

a) tão logo possível, notificar a Parte Receptora sobre qualquer alteração na classificação de sigilo das informações classificadas fornecidas;

b) informar a Parte Receptora sobre quaisquer condições de liberação ou limitações quanto ao uso das Informações Classificadas fornecidas.

Artigo 3

Proteção da Informação Classificada

1. As Partes tomarão todas as medidas apropriadas, em conformidade com suas respectivas legislações nacionais, para assegurar que o nível de proteção atribuído à Informação Classifi-cada recebida esteja de acordo com o nível de classificação de sigilo equivalente, conforme estabelecido no artigo 2º do presente Acordo.

2. Nada neste Acordo deve prejudicar o previsto na legislação nacional das Partes, em relação ao direito dos indivíduos de obter acesso a documentos públicos ou informações de caráter público, à proteção dos dados pessoais ou à proteção de Informações Classificadas.

3. Em conformidade com a legislação nacional, cada Parte assegurará que medidas apropria-das serão implementadas para a proteção de Informações Classificadas processadas, armazenadas ou transmitidas em sistemas de comunicações e informações, enquanto for necessário para garantir a confidencialidade, integridade, disponibilidade e, quando aplicável, o não repúdio e autenticidade da Informação Classificada, bem como um nível apropriado de responsabilidade e rastreabilidade de ações em relação a essas informações.

Artigo 4º

Divulgação e Uso de Informação Classificada

1. Cada Parte deverá assegurar que as Informações Classificadas fornecidas ou trocadas no âmbito do presente Acordo não sejam:

a) desclassificados ou reclassificadas com nível de sigilo inferior, sem o prévio consentimento por escrito da Parte de Origem;

b) utilizadas para fins diferentes dos estabelecidos pela Parte de Origem;

c) divulgada a terceiros sem o prévio consentimento por escrito da Parte de Origem, e sem que haja um acordo ou convênio apropriado para a proteção da Informação Classificada com a terceira parte envolvida.

2. O princípio do consentimento da Parte de Origem deve ser respeitado por cada uma das

Partes, de acordo com as suas normas constitucionais e sua legislação nacional.

Artigo 5º

Acesso à Informação Classificada

1. Cada Parte deverá assegurar que o acesso à Informação Classificada somente será concedido com base no princípio da "Necessidade de Conhecer".

2. Cada Parte deverá assegurar que todos os indivíduos que tiverem acesso à Informação Classificada estejam informados da sua responsabilidade de proteção dessas informações, de acordo com as normas de segurança em vigor.

3. As Partes deverão assegurar que o acesso à Informação Classificada somente será concedido aos indivíduos que possuam uma Credencial de Segurança Pessoal apropriada ou que estejam devidamente autorizados por força das suas funções, em conformidade com a legis-lação nacional.

4. De acordo com sua legislação nacional, cada Parte deverá assegurar que qualquer entidade sob a sua jurisdição que possa receber ou gerar Informação Classificada possua a apropriada Habilitação de Segurança e seja capaz de proporcionar proteção adequada, conforme previsto no § 1 do artigo 3 do presente Acordo, no nível de segurança adequado.

Artigo 6º

Tradução, Reprodução e Destruição de Informação Classificada

1. Todas as traduções e reproduções de Informações Classificadas devem possuir as apropriadas marcas de classificação de sigilo e devem ser protegidas e controladas pelas Partes, em conformidade com o original.

2. Todas as traduções de Informações Classificadas deverão conter uma anotação adequada, na língua para a qual foram traduzidas, indicando que contêm Informação Classificada da Parte de Origem.

3. De acordo com o artigo 5º § 3 do presente Acordo, os tradutores devem possuir uma Credencial de Segurança Pessoal no nível de sigilo da Informação Classificada a ser traduzida.

4. A Informação Classificada marcada como ULTRASSECRETO/HEMLIG/TOP SECRET/HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET somente poderá ser traduzida ou reproduzida mediante autorização prévia por escrito da Parte de Origem.

5. A Informação Classificada recebida nos termos deste Acordo, marcada como ULTRASSE-CRETO/HEMLIG/TOP SECRET/ HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET não poderá ser destruída. Quando já não for considerada necessária pela Parte Receptora, deverá ser devolvida à Parte de Origem.

6. A Informação Classificada recebida nos termos deste Acordo marcada como SECRETO, RESERVADO, HEMLIG/SECRET, HEMLIG/CONFIDENCIAL ou HEMLIG/RESTRICTED não poderá ser destruída. Quando já não for considerada necessária pela Parte Receptora, deverá ser devolvida à Parte de Origem, salvo acordo em contrário entre as Partes.

Artigo 7º

Transferência de Informação Classificada

1. As Informações Classificadas deverão ser transferidas entre as Partes, em conformidade com as legislações nacionais da respectiva Parte, por via diplomática ou de outro modo mutu-amente aprovado pelas Autoridades Competentes de Segurança das Partes.

2. Na implementação do presente Acordo, as Partes poderão firmar um acordo de segurança das comunicações, com o objetivo de regular a transmissão segura de Informações Classificadas e a comunicação segura entre elas.

Artigo 8º

Visitas

1. As visitas às instalações onde as Informações Classificadas são manuseadas ou armazenadas estão sujeitas à aprovação prévia por parte da Autoridade Competente de Segurança da Parte anfitriã, a menos que de outra forma mutuamente aprovada.

2. A solicitação da visita deverá ser submetida à Parte anfitriã e deverá conter os seguintes dados, que serão utilizados somente para o propósito da visita:

a) nome do visitante, data e local de nascimento, nacionalidade e número de cartão de identificação/passaporte;

b) cargo ou função do visitante, com a especificação do empregador que o visitante representa;

c) especificação do projeto no qual o visitante trabalha;

d) validade e nível da Credencial de Segurança Pessoal do visitante, se necessário;

e) nome, endereço, número de telefone/fax, e-mail e ponto de contato das instalações aserem visitadas;

f) objetivo da visita, incluindo o mais alto nível de classificação de segurança de Informação Classificada envolvida;

g) data e duração da visita. Para visitas recorrentes, deve ser indicado o período total das visitas;

h) outros dados, se acordado entre as Autoridades Competentes de Segurança, e

i) data e assinatura.

3. O pedido de visita deverá ser apresentado pelo menos 20 (vinte) dias antes da visita, a menos que de outra forma mutuamente aprovada pelas Autoridades Competentes de Segurança.

4. Qualquer Informação Classificada liberada para um visitante será considerada como Informação Classificada recebida nos termos deste Acordo. O visitante deverá cumprir as normas de segurança da Parte anfitriã.

5. As Autoridades Competentes de Segurança poderão acordar sobre uma lista de visitantes com direito a visitas recorrentes. A lista será válida por um período inicial não superior a 12 (doze) meses, podendo ser prorrogado por mais um período de tempo não superior a 12 (doze) meses. O pedido para visitas recorrentes deverá ser apresentado em conformidade com o § 3º deste artigo. Uma vez aprovada a lista, as visitas poderão ser organizadas diretamente entre as instalações envolvidas.

Artigo 9

Contratos Sigilosos

1. Se a Autoridade Competente de Segurança da Parte de Origem tenciona permitir negocia-ções para a celebração de um Contrato Sigiloso com um contratante sob a jurisdição da Parte Receptora, ele deverá, mediante pedido, de acordo com a sua legislação nacional, obter todas as Habilitações de Segurança e Credenciais de Segurança Pessoais relevantes, da Autoridade Competente de Segurança da Parte Receptora.

2. Cada Parte poderá solicitar à outra Parte a realização de uma verificação de segurança em uma instalação sob sua jurisdição para garantir a conformidade com os padrões de segurança estabelecidos neste Acordo.

3. Um Contrato Sigiloso deverá conter disposições relativas aos requisitos de segurança e sobre a classificação de cada aspecto ou elemento do Contrato Sigiloso. Uma cópia destas disposições deverá ser submetida às Autoridades Competentes de Segurança das Partes, para permitir a supervisão de segurança.

Artigo 10

Autoridades Competentes de Segurança e Cooperação de Segurança

1. Para efeitos do presente Acordo, as Autoridades Competentes de Segurança são:

Na República Federativa do Brasil:

Gabinete de Segurança Institucional da Presidência da República - GSI/PR (Autoridade Nacional de Segurança)

No Reino da Suécia:

As Forças Armadas Suecas, Serviço de Segurança Militar

(Autoridade Nacional de Segurança)

A Administração de Material de Defesa Sueca (Autoridade de Segurança Designada)

2. Cada Parte deverá fornecer à outra os dados de contato necessários de suas respectivas Autoridades Competentes de Segurança, por escrito.

3. As Partes deverão informar uma à outra, por escrito, qualquer alteração que venha a ocorrer em suas respectivas Autoridades Competentes de Segurança.

4. Com o objetivo de assegurar uma estreita cooperação na execução do presente Acordo, as Autoridades Competentes de Segurança poderão ser consultadas sempre que for solicitado por uma delas. As Partes reconhecem mutuamente as Credenciais de Segurança e devem informar imediatamente uma à outra quaisquer alterações nas Habilitações de Segurança e Credenciais de Segurança Pessoais mutuamente reconhecidas.

5. Para alcançar e manter níveis comparáveis de segurança, as Autoridades Competentes de Segurança deverão, quando solicitadas, fornecer umas às outras informações sobre suas normas e padrões de segurança, procedimentos e práticas para a proteção de Informação Classifica-da. Para esta finalidade, as Autoridades Competentes de Segurança poderão realizar reuniões regulares.

6. As Autoridades Competentes de Segurança deverão informar uma à outra sobre os riscos de segurança específicos que possam pôr em perigo a Informação Classificada liberada, quando aplicável.

7. A pedido, as Partes deverão prestar mútua assistência no processo de concessão das Credenciais de Segurança.

8. Se qualquer Autoridade Competente de Segurança suspende ou toma medidas no sentido de revogar o acesso à Informação Classificada que tenha sido concedido a um cidadão da outra Parte com base em um Credenciamento de Segurança, a outra Parte deverá ser notificada e informada sobre as razões para tal ação.

Artigo 11

Perda ou Comprometimento da Informação Classificada

1. As Partes tomarão todas as medidas apropriadas, em conformidade com sua respectiva legislação nacional, para investigar os casos em que se sabe, ou quando existam motivos ra-zoáveis para suspeitar, que as Informações Classificadas foram perdidas ou comprometidas.

2. A Parte que descobrir uma perda ou comprometimento deve, através dos canais apropriados, informar imediatamente a Parte de Origem sobre tal ocorrência e, posteriormente, informar a Parte de Origem sobre os resultados finais da investigação referida no § 1º deste artigo e das medidas corretivas tomadas para evitar a reincidência. A pedido, a Parte de Origem poderá prestar assistência na

investigação.

Artigo 12

Custos

Cada Parte deverá arcar com os custos de suas próprias despesas decorrentes da aplicação do presente Acordo.

Artigo 13

Solução de Controvérsias

1. Qualquer controvérsia que possa surgir entre as Partes sobre a interpretação ou aplicação do presente Acordo, ou qualquer assunto relacionado, deverá ser resolvida por meio de consultas e negociações entre apenas as Partes, por via diplomática.

2. Durante o período de resolução das controvérsias do Acordo, as Partes continuarão a cumprir com as suas obrigações nos termos deste Acordo.

Artigo 14º

Comunicações

Todas as comunicações entre as Partes relacionadas com a implementação do presente Acordo serão feitas por escrito, em Inglês.

Artigo 15º

Comunicações

O presente Acordo entrará em vigor 30 (trinta) dias após a recepção da última notificação, por intermédio da qual as Partes tenham informado uma à outra, por via diplomática, que os seus requisitos legais internos necessários para sua entrada em vigor foram cumpridos.

Artigo 16º

Emendas

1. O presente Acordo poderá ser alterado a qualquer momento, por escrito, por consentimento mútuo das Partes.

2. As emendas entrarão em vigor nos termos estabelecidos no artigo 15 do presente Acordo.

Artigo 17º

Vigência e Denúncia

1. O presente Acordo permanecerá em vigor por tempo indeterminado.

2. Qualquer uma das Partes poderá, a qualquer momento, denunciar o presente Acordo mediante notificação por escrito à outra Parte.

3. A denúncia deve ser notificada por via diplomática e surtirá efeito seis (6) meses após a data em que o aviso de denúncia for recebido pela outra Parte.

4. Em caso de denúncia, quaisquer Informações Classificadas trocadas nos termos do presente Acordo continuarão a ser protegidas em conformidade com as disposições aqui estabelecidas, a menos que a Parte de Origem isente a Parte Receptora dessa obrigação.

Artigo 18º

Disposições Finais

As Partes deverão imediatamente notificar uma à outra quaisquer alterações em sua res-pectiva legislação nacional que afete a proteção de Informações Classificadas fornecidas com base no presente Acordo. No caso de tais alterações, as Partes deverão se consultar e consi-derar a possibilidade de realizar alterações neste Acordo. Nesse meio tempo, as Informações Classificadas continuarão a ser protegidas como descrito aqui, salvo pedido em contrário da Parte de Origem, por escrito.

Feito em Estocolmo, em 3 de abril de 2014, em dois exemplares originais, nos idiomas sueco, português e inglês, sendo todos os textos igualmente autênticos. Em caso de divergência de interpretação, o texto em Inglês prevalecerá.

Em testemunho do qual, as Partes assinam este Acordo com o selo a partir do dia e ano acima mencionados.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL
General-de-Exército
José Elito Carvalho Siqueira
Ministro de Estado
Chefe do Gabinete de Segurança Institucional da Presidência da República

PELO GOVERNO DO REINO DA SUÉCIA

General Gunnar Karlson Diretor de Inteligência Militar e Serviço de Segurança

VERSÃO PUBLICADA

Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo do Grão-Ducado de Luxemburgo sobre Troca e Proteção Mútua de Informação Classificada, firmado em Nova Iorque, em 25 de setembro de 2018.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84,*caput*, inciso IV, da Constituição, e

Considerando que o Acordo entre o Governo da República Federativa do Brasil e o Governo do Grão-Ducado de Luxemburgo sobre Troca e Proteção Mútua de Informação Classificada foi firmado em Nova Iorque, em 25 de setembro de 2018;

Considerando que o Congresso Nacional aprovou o Acordo por meio do Decreto Legislativo nº 13, de 13 de abril de 2022; e

Considerando que o Acordo entrou em vigor para a República Federativa do Brasil, no plano jurídico externo, em 1º de julho de 2022, nos termos de seu Artigo 17;

DECRETA :

Art. 1º Fica promulgado o Acordo entre o Governo da República Federativa do Brasil e o Governo do Grão-Ducado de Luxemburgo sobre Troca e Proteção Mútua de Informação Classificada, firmado em Nova Iorque, em 25 de setembro de 2018, anexo a este Decreto.

Art. 2º São sujeitos à aprovação do Congresso Nacional atos que possam resultar em revisão do Acordo e ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional, nos termos do art. 49,*caput*, inciso I, da Constituição.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Belém, 13 de novembro de 2025; 204º da Independência e 137º da República.

LUIZ INÁCIO LULA DA SILVA

Mauro Luiz Iecker Vieira

ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DO GRÃO DUCADO DE LUXEMBURGO SOBRE TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República Federativa do Brasil, e

O Governo do Grão Ducado de Luxemburgo

A seguir denominados conjuntamente "Partes" ou individualmente como "Parte",

No interesse da segurança nacional e com a finalidade de assegurar a proteção de informações classificadas trocadas no âmbito dos tratados de cooperação ou acordos celebrados entre si, seus indivíduos, órgãos, assim como entidades públicas ou privadas credenciadas;

Desejando estabelecer um conjunto de regras e procedimentos sobre a proteção de Informações classificadas de acordo com as leis e regulamentos nacionais das Partes;

Confirmando que este Acordo não afetará os compromissos de ambas as Partes decorrentes de outros acordos internacionais e que não deve ser usado contra os interesses, segurança e integridade territorial de outros Estados.

Acordam o seguinte:

Artigo 1

Objeto e âmbito de aplicação

O presente Acordo estabelece regras e procedimentos para a proteção de Informação classificada trocada e gerada no processo de cooperação, em relação aos seus interesses e segurança nacionais, entre as Partes mencionadas, seus indivíduos, agências e entidades credenciadas.

Artigo 2

Definições

Para os fins do presente Acordo, o termo:

a) Contrato classificado:significa qualquer contrato ou subcontrato, incluindo as negociações pré-contratuais, entre dois ou mais Contratantes criando e definindo direitos e obrigações exigíveis entre eles, que contém ou fornece acesso a informação classificada;

b) Informação Classificada:é a informação, independentemente da sua forma, natureza e meios de transmissão, definida de acordo com as respectivas leis e regulamentos de ambas as Partes, protegida contra acesso ou divulgação não autorizados, que foi classificada e for trocada ou gerada pelas Partes;

c) Autoridade de Segurança Competente (CSA): significa uma entidade competente

autorizada, de acordo com as leis e regulamentos nacionais das Partes, responsável pela implementação dos requisitos de segurança abrangidos pelo presente Acordo;

d) Comprometimento:designa qualquer forma de uso indevido, danos ou acesso não autorizado, alteração, divulgação ou destruição de Informação Classificada, bem como qualquer outra ação ou inatividade, devido a uma violação de segurança, resultando em perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;

e) Contratante:significa um indivíduo, agência ou entidade com capacidade legal para celebrar contratos;

f) Habilitação de Segurança de Instalação (FSC): significa uma habilitação fornecida por uma Autoridade de Segurança Competente de uma Parte, que uma entidade pública ou privada localizada no seu país está autorizada e possui medidas de segurança apropriadas dentro de uma instalação específica para o Tratamento de Informação Classificada, de acordo com as leis e regulamentos nacionais;

g) Autoridade Nacional de Segurança (NSA): designa o órgão estatal especificado pela legislação nacional das Partes, especialmente autorizado no âmbito da proteção da Informação Classificada;

h) Necessidade de conhecer:designa a condição pela qual o acesso à Informação Classificada pode ser concedido a um indivíduo que tenha a real necessidade de conhecimento ou posse de tais informações para poder desempenhar funções e tarefas oficiais;

i) Parte Originária:significa a Parte, incluindo qualquer empresa pública ou privada sob sua jurisdição, a partir da qual a Informação Classificada é produzida;

j) Credencial de Segurança Pessoal (PSC): significa a autorização fornecida pela Autoridade de Segurança Competente de uma Parte que um indivíduo recebeu a credencial de segurança para o tratamento da informação classificada, de acordo com as leis e regulamentos nacionais, baseado na condição de que esse indivíduo está autorizado a ter acesso e manipular informação classificada até o nível definido na respectiva credencial.

k) Parte Receptora:significa a Parte, incluindo quaisquer entidades públicas ou privadas sob a sua jurisdição, para a qual Informação Classificada é transmitida;

l) Acreditação de Segurança:designa a qualificação positiva de entidades e órgãos públicos ou privados, bem como de pessoas físicas que, em virtude de procedimento de fiscalização ou de investigação de segurança, em conformidade com a legislação nacional, tenham sido autorizadas para o tratamento de Informações Classificadas para um certo nível de sigilo;

m) Violação de Segurança:significa a ação ou omissão, seja intencional ou acidental, que resulta no comprometimento real ou possível da Informação Classificada;

n) Grau de Sigilo da Informação Classificada: significa categoria, de acordo com as leis e regulamentos nacionais das Partes, que caracteriza a importância da Informação Classificada, o nível

de restrição de seu acesso e o nível de sua proteção pelas Partes, e também a categoria com base na qual as informações são identificadas;

o) Habilitação de segurança: designa o processo de emissão de um FSC ou PSC por uma Autoridade de Segurança Competente, em conformidade com as leis e regulamentos nacionais das Partes;

p) Terceira Parte: designa os Estados, qualquer organização internacional, governos ou indivíduos que representem organismos ou organizações estatais, incluindo quaisquer entidades públicas e privadas que não sejam Partes do presente Acordo;

q) Tratamento da Informação Classificada: designa o conjunto de ações relativas à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivo, armazenamento, liberação, avaliação, destinação ou controle da Informação Classificada em qualquer Grau de Sigilo; e

r) Visita:significa qualquer acesso a entidades públicas e privadas, para efeitos deste presente Acordo, que inclui o tratamento de Informação Classificada.

Artigo 3
Graus de Sigilo da Informação Classificada

1. De acordo com as leis e regulamentos nacionais, as Partes concordam que os Graus de Sigilo da Informação Classificada devem corresponder uns aos outros e serem considerados equivalentes da seguinte forma:

No Grão Ducado de Luxemburgo (Francês)	Equivalente em Inglês	Na República Federativa do Brasil (Português)
TRES SECRET LUX	Top Secret	Ultrassecreto
SECRET LUX	Secret	SECRETO
CONFIDENTIEL LUX	Confidential	
RESTREINT LUX	Restricted	Reservado

2. Qualquer Informação Classificada fornecida sob este Acordo deve ser identificada com o Grau de Sigilo apropriado às leis e regulamentos nacionais da Parte Originária e, quando apro-priado, ser prefixado com o nome do país de origem que fornecer a Informação Classificada.

3. As Partes devem marcar toda a Informação Classificada recebida da outra Parte com o Grau de Sigilo equivalente, de acordo com o parágrafo 1 deste Artigo.

4. As Partes devem notificar uma a outra sobre quaisquer alterações nos Graus de Sigilo da Informação Classificada, conforme especificado no parágrafo 1, e sobre todas as alterações de

classificação subsequentes relativas à Informação Classificada transmitida.

5. A Parte Originária deve:

a) sem demora, notificar a Parte Receptora de quaisquer alterações no Grau de Sigilo da Informação Classificada transmitida;

b) informar à Parte Receptora quaisquer condições de divulgação ou limitações no uso de Informação Classificada.

Artigo 4
Proteção da Informação Classificada

1. As Partes tomarão todas as medidas adequadas, de acordo com as respectivas leis e regulamentos nacionais, para garantir que o nível de proteção concedido à Informação Classifi-cada recebida, esteja em conformidade com o Grau de Sigilo equivalente, conforme estabelecido no Artigo 3 deste Acordo.

2. Nada neste Acordo prejudicará as leis ou regulamentos nacionais das Partes em relação aos direitos das pessoas físicas para obter acesso a documentos públicos ou acesso a informa-ções de caráter público, proteção de dados pessoais ou proteção da Informação Classificada.

3. De acordo com suas leis e regulamentos nacionais, cada Parte deve assegurar que se-jam implementadas medidas adequadas para a proteção da Informação Classificada que seja processada, armazenada ou transmitida em sistemas de comunicação e informação, até onde forem necessárias. Tais medidas devem assegurar a confidencialidade, a integridade, a dispo-nibilidade e, quando aplicável, o não repúdio e a autenticidade da Informação Classificada, bem como um nível apropriado de responsabilização e rastreabilidade de ações em relação a essa informação.

Artigo 5
Divulgação e uso da Informação Classificada

1. Cada Parte deve garantir que a Informação Classificada fornecida ou trocada sob este Acordo não seja:

a) Desclassificada ou reclassificada para um Grau de Sigilo da Informação Classificada inferior sem o prévio consentimento por escrito da Parte Originária;

b) usada para propósitos diferentes dos estabelecidos pela Parte Originária;

c) divulgada a qualquer Terceira Parte sem o prévio consentimento por escrito da Parte Originária e sem um apropriado acordo ou contrato para proteção de Informação Classificada esteja em vigor com a referida Terceira Parte.

2. Cada Parte, de acordo com seus requisitos constitucionais e legislação nacional, deve

respeitar o princípio do consentimento do originador.

Artigo 6

Acesso a Informação Classificada

1. Cada Parte deve garantir que o acesso à Informação Classificada seja concedido combase no princípio da "Necessidade de Conhecer".

2. Cada Parte deve garantir que todos os indivíduos que tenham acesso à Informação Classificada sejam informados sobre suas responsabilidades para proteger essa informação de acordo com os regulamentos de segurança apropriados.

3. As Partes assegurarão que o acesso às Informação Classificada seja concedido apenas a indivíduos que possuam um PSC apropriado ou que estejam devidamente autorizados em virtude de suas funções de acordo com a legislação nacional.

4. De acordo com suas leis e regulamentos nacionais, cada Parte deverá garantir que qual-quer entidade sob sua jurisdição que possa receber ou gerar Informação Classificada seja devi-damente habilitada e seja capaz de fornecer proteção adequada, conforme previsto no parágrafo 1 do Artigo 4 deste Acordo, no nível de segurança apropriado.

Artigo 7

Tradução, reprodução e destruição de Informação Classificada

1. Todas as traduções e reproduções de Informação Classificada devem conter os Graus de Sigilo equivalente e serem protegidas e controladas adequadamente pelas Partes assim como o original.

2. Todas as traduções de Informação Classificada devem conter uma anotação adequada, na língua para a qual foi traduzida, indicando que elas contêm Informação Classificada da Parte Originária.

3. De acordo com o parágrafo 3 do Artigo 6 deste Acordo, os tradutores devem ter PSC apropriada ao Grau de Sigilo da Informação Classificada a ser traduzida.

4. A Informação Classificada como TOP SECRET/TRES SECRET LUX/ULTRASSECRETO deve ser traduzida ou reproduzida apenas mediante autorização prévia por escrito da Parte Originária.

5. A Informação Classificada recebida sob este Acordo não deverá ser destruída. A informa-ção deverá ser devolvida à Parte Originária quando não for mais necessária à Parte Receptora.

6. A Informação Classificada não será reproduzida pela Parte Receptora sem a aprovação prévia por escrito da Parte Originária.

Artigo 8

Transmissão entre as Partes

1. A Informação Classificada deverá ser transmitida entre as Partes pela via diplomática ou conforme acordado entre as Partes.

2. A informação Classificada deve ser transmitida por meio de sistemas de comunicação protegidos, redes ou outros meios eletromagnéticos aprovados por ambas as Partes. Tais trans-missões devem ser protegidas por meios criptográficos mutuamente aceitos pelas Autoridades Nacionais de Segurança, de acordo com as leis e regulamentos nacionais.

3. Informação Classificada como TOP SECRET/TRES SECRET LUX/ULTRASSECRETO deve ser enviada apenas pela via diplomática.

4. Informação classificada como RESTRICTED/RESTREINT LUX/RESERVADO também po-derá ser postada ou utilizado outro serviço de entrega, de acordo com as leis e regulamentos nacionais.

5. Em caso de transmissão de grandes remessas contendo Informação Classificada, os procedimentos de transporte devem ser acordados e avaliados conjuntamente, caso a caso, pelas Autoridades Nacionais de Segurança das Partes.

Artigo 9

Visitas

1. As visitas às instalações onde a Informação Classificada é tratada ou armazenada de-vem estar sujeitas a aprovação prévia pela Autoridade Nacional de Segurança da Parte anfitriã, a menos que, de outra forma, seja aprovada mutuamente.

2. O pedido de visita deverá ser submetido à Autoridade Nacional de Segurança da Parte anfitriã e deve incluir os seguintes dados, os quais deverão ser usados unicamente para o pro-pósito da visita:

a) nome do visitante, data e local de nascimento, nacionalidade e número do cartão de identificação/passaporte;

b) posição e função do visitante, bem como o nome e endereço da instalação onde ele é empregado;

c) especificação do projeto em que o visitante está participando;

d) a validade e o nível do PSC do visitante;

e) o nome, endereço, número de telefone, e-mail e ponto de contato da instalação a ser visitada;

f) o objetivo da Visita, incluindo a entidade que pretendem visitar e o mais alto Grau

de Sigilo da Informação Classificada envolvida;

g) a data e a duração da visita. Para visitas recorrentes, o período total coberto pelas visitas deve ser indicado;

h) outros dados, se acordados pelas Autoridades Nacionais de Segurança; e

i) data e assinatura.

3. O pedido de Visita deverá ser submetido pelo menos 30 (trinta) dias antes da data prevista da visita, a menos que seja previamente aprovado mutuamente pelas Autoridades de Segurança Competentes.

4. Qualquer Informação Classificada divulgada a um visitante deve ser considerada como Informação Classificada recebida segundo as regras deste Acordo. Todo visitante deve cumprir com os regulamentos de segurança da Parte anfitriã.

5. As visitas somente poderão ser autorizadas por uma Parte aos visitantes da outra Parte se estes:

a) possuírem a PSC válida emitida pelo país de origem; e

b) estiverem autorizados a receber ou ter acesso a Informação Classificada sob o princípio da necessidade de conhecer.

6. Uma vez autorizada a Visita, a Autoridade Nacional de Segurança do país anfitrião deve notificar a Autoridade Nacional de Segurança do país do visitante sobre sua autorização, com um aviso mínimo de 10 (dez) dias, até a data prevista da Visita, e fornecer uma cópia do pedido para a entidade a ser visitada.

7. As Autoridades de Segurança Competentes podem concordar com uma lista de visitantes com direito a visitas recorrentes. A lista deve ser válida por um período inicial não superior a 12 (doze) meses e pode ser prorrogada por mais um período não superior a 12 (doze) meses. Um pedido de Visitas recorrentes deve ser apresentado de acordo com o parágrafo 3º deste Artigo. Assim que a lista for aprovada, as visitas podem ser organizadas diretamente entre as instalações envolvidas.

Artigo 10

Contratos Classificados relacionados a este Acordo

1. No caso de Contratos Classificados firmados e implementados no território de uma das Partes, a NSA ou CSA da outra Parte deve obter uma garantia escrita prévia de que o contratado proposto possui FSC e PSCs necessárias no Grau de Sigilo apropriado.

2. O Contratante compromete-se a:

a) assegurar que suas instalações tenham condições adequadas para o Tratamento de

b) Informação Classificada;

c) possuir Habilitação de Segurança;

d) assegurar que todas as pessoas com acesso a Informação Classificada tenham PSC apropriada e sejam informadas sobre suas responsabilidades em relação à sua proteção, de acordo com leis e regulamentos;

e) permitir inspeções de segurança de suas instalações.

3. Para cada Contrato adjudicado, a Parte Originária informará a Parte Receptora o Grau de Sigilo da Informação Classificada transferida.

4. Os Contratos Classificados também devem fornecer os seguintes termos adicionais:

a) responsabilidade pelo descumprimento dos procedimentos e medidas de segurança

b) aplicáveis à Informação Classificada;

c) obrigação de informar qualquer Violação de Segurança ou comprometimento de informação classificada para sua CSA;

d) responsabilidade pelos danos resultantes de Violações de Segurança.

5. Qualquer subcontratado deve cumprir as mesmas obrigações de segurança que o Contratado.

Artigo 11

Autoridades Nacionais de Segurança e Cooperação de Segurança

1. As Autoridades Nacionais de Segurança responsáveis pela implementação e supervisão do presente Acordo serão:

Na República Federativa do Brasil

Gabinete de Segurança Institucional da Presidência da República – GSI/PR Autoridade Nacional de Segurança

(National Security Authority)

No Grão Ducado de Luxemburgo:

Service de Renseignement de l'Etat Autorité nationale de Sécurité (National Security Authority)

2. Cada Parte deve fornecer à outra os dados de contato de sua respectiva Autoridade Nacional de Segurança por escrito.

3. As Autoridades Nacionais de Segurança devem informar-se mutuamente sobre suas respectivas leis e regulamentos nacionais vigentes que regulam a segurança da Informação Classificada.

4. As Autoridades Nacionais de Segurança devem informar-se mutuamente sobre quaisquer modificações a respeito delas mesmas ou sobre modificações das Credenciais ou Habilitações de Segurança de indivíduos, agências e entidades.

5. Com o objetivo de assegurar uma cooperação estreita na aplicação do presente Acordo, as Autoridades Nacionais de Segurança podem ser consultadas sempre que solicitado por uma delas.

6. Os representantes da Autoridade Nacional de Segurança de uma Parte podem visitar os

estabelecimentos da Autoridade Nacional de Segurança da outra Parte com a intenção de adquirir conhecimento de procedimentos de segurança e medidas aplicáveis à Informação Classificada.

7. As Partes, por intermédio das suas Autoridades Nacionais de Segurança, devem informar-se mutuamente, a qualquer momento, sobre quaisquer alterações no título de tais órgãos ou transferência de suas competências para outros órgãos.

8. Se solicitado, as Partes, por meio das suas Autoridades Nacionais de Segurança, tendo em conta as respectivas leis e regulamentos nacionais, devem colaborar entre si no decorrer dos procedimentos necessários para a emissão da Credencial de Segurança Pessoal de seus indivíduos que viveram ou vivem no território da outra Parte.

9. As Partes reconhecem mutuamente as PSC e as FSC, e devem informar à outra Parte prontamente sobre quaisquer mudanças nas mesmas.

10. Para alcançar e manter padrões de segurança compatíveis, as Autoridades de Segurança Competentes devem, sob demanda, fornecer uma à outra informações sobre os seus padrões nacionais de segurança, procedimentos e práticas para a proteção de Informação Classificada. Se necessário, as Autoridades Nacionais Competentes podem realizar reuniões regulares.

11. Sob demanda, as Partes devem prestar assistência mútua à concessão de PSCs.

Artigo 12

Assistência para Procedimentos de Habilitação e Credenciamento de Segurança

1. A pedido, as Autoridades Nacionais de Segurança das Partes, levando em consideração suas respectivas leis e regulamentos nacionais, devem auxiliar-se mutuamente durante os procedimentos de Habilitação e Credenciamento de Segurança.

2. As Partes devem reconhecer as Habilitações e Credenciais de Segurança emitidas de acordo com as leis e regulamentos da outra Parte.

Artigo 13

Violação de Segurança

1. No caso de uma violação de segurança relacionada a Informação Classificada que envolva as Partes deste Acordo, a Autoridade Nacional de Segurança da Parte onde a Violação de Segurança ocorreu deverá informar imediatamente a Autoridade Nacional de Segurança da outra Parte.

2. Quando a violação de Segurança ocorrer em uma Terceira Parte, a Autoridade Nacional de Segurança da Parte Originária deverá informar à Autoridade Nacional de Segurança da outra Parte, o mais rápido possível, e assegurar a investigação apropriada.

3. A Parte competente deve tomar todas as medidas em conformidade com as leis e regu-

lamentos nacionais, a fim de limitar as consequências da violação a que se refere o parágrafo 1 deste Artigo e evitar violações futuras. A pedido, a outra Parte deve prestar assistência adequada; devendo ser informada do resultado do processo e das medidas tomadas pela violação.

4. A Parte onde a Violação de Segurança ocorrer deve investigar ou acompanhar a investigação do incidente e, ao final, informar imediatamente a outra Parte sobre o resultado da inves-tigação e as medidas corretivas aplicadas.

5. A outra Parte, se necessário, deverá cooperar na investigação.

Artigo 14

Custos

Cada Parte deve arcar com os custos das suas próprias despesas resultantes da implemen-tação e supervisão de todos os aspectos do presente Acordo.

Artigo 15

Disputas

1. Qualquer disputa que surja entre as Partes sobre a interpretação ou aplicação do presente Acordo, ou qualquer assunto relacionado, deve ser resolvida mediante consultas e negociações entre as Partes, por meio da via diplomática.

2. Durante o período de resolução da disputa, ambas as Partes devem continuar a cum-prir todas as suas obrigações nos termos do presente Acordo.

Artigo 16º

Comunicações

Todas as comunicações entre as Partes relativas à implementação deste Acordo serão feitas por escrito, em inglês.

Artigo 17º

Entrada em Vigor

O presente Acordo deve entrar em vigor no primeiro dia do segundo mês após a recepção da última notificação, mediante a qual as Partes se informaram, por meio da via diplomática, de que os seus requisitos legais internos necessários para sua entrada em vigor foram cumpridos.

Artigo 18º

Alterações

1. O presente Acordo pode ser alterado em qualquer momento, por escrito, por consentimento mútuo das Partes.

2. As alterações entrarão em vigor nos termos estabelecidos no Artigo 17 do presente Acordo.

Artigo 19º

Validade e Denúncia

1. O presente Acordo permanecerá em vigor indefinidamente.

2. Qualquer Parte poderá, em qualquer momento, denunciar o presente Acordo mediante notificação escrita à outra Parte.

3. A rescisão deve ser notificada pela via diplomática e entrará em vigor após 6 (seis) meses a partir da data em que a outra Parte tenha recebido a notificação de denúncia.

4. Em caso de denúncia, qualquer Informação Classificada trocada nos termos do presente Acordo deve continuar a ser protegida de acordo com as disposições aqui estabelecidas, a menos que a Parte Originária isente a Parte Receptora dessa obrigação.

Artigo 20º

Disposições Finais

As Partes devem notificar-se prontamente sobre quaisquer alterações às respectivas leis ou aos regulamentos nacionais que afetem a proteção da Informação Classificada compartilha-das no âmbito deste Acordo. No caso de tais mudanças, as Partes consultarão para considerar possíveis mudanças neste Acordo. Enquanto isso, a Informação Classificada continuará a ser protegida conforme descrito neste documento, a menos que requisitado por escrito pela Parte Originária.

PARA O GOVERNO DA
REPÚBLICA FEDERATIVA
DO BRASIL
Aloysio Nunes Ferreira
Ministro de Estado das Relações Exteriores

PARA O GOVERNO DO GRÃO
DUCADO DE LUXEMBURGO
Jean Asselborn
Ministro dos Negócios Estrangeiros e Europeus

Feito em Nova York em de setembro de 2018, em dois originais, cada um na língua portuguesa, francesa e inglesa, sendo todos os textos igualmente autênticos. Em caso de diver-gências de interpretação, o texto em inglês deverá prevalecer.

VERSÃO PUBLICADA

Aprova o texto do Acordo entre o Governo da República Federativa do Brasil e o Governo do Estado de Israel sobre Proteção de Informação Classificada e Materiais, assinado em Tel Aviv, em 24 de novembro de 2010, e o texto de sua Emenda, firmada em Tel Aviv e Brasília, em 6 de junho de 2018.

O Congresso Nacional decreta:

Art. 1 Ficam aprovados o texto do Acordo entre o Governo da República Federativa do Brasil e o Governo do Estado de Israel sobre Proteção de Informação Classificada e Materiais, assinado em Tel Aviv, em 24 de novembro de 2010, e o texto de sua Emenda, firmada em Tel Aviv e Brasília, em 6 de junho de 2018.

Parágrafo único. Nos termos do inciso I do *caput* do art. 49 da Constituição Federal, ficam sujeitos à aprovação do Congresso Nacional quaisquer atos que possam resultar em revisão do referido Acordo ou de sua Emenda, bem como quaisquer ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional.

Art. 2 Este Decreto Legislativo entra em vigor na data de sua publicação.

Senado Federal, em 5 de outubro de 2022

Senador RODRIGO PACHECO

Presidente do Senado Federal

ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DO ESTADO DE ISRAEL SOBRE PROTEÇÃO DE INFORMAÇÃO CLASSIFICADA E MATERIAIS

O Governo da República Federativa do Brasil (Representado pelo Gabinete de Segurança Institucional da Presidência da República)

e

O Governo do Estado de Israel (representado pelo Ministério da Defesa do Estado de Israel) (doravante denominados "Partes"),

Considerando que pretendem cooperar em projetos conjuntos relacionados a questões de defesa e segurança que podem envolver o intercâmbio de informação e materiais classificados; e

Considerando que desejam proteger informações e materiais classificados relativos a projetos de segurança e intercambiados entre si da divulgação não autorizada;

Considerando que concordam que a celebração de acordo de proteção da informação classificada é essencial e de interesse mútuo; e

Considerando que as Partes deste Acordo sobre Proteção de Informação Classificada e Matérias concordam que a mera existência da relação entre as Partes concernente à Informação Classificada e Matérias relacionadas a projetos militares e de defesa não são classificadas. O conteúdo classificado das relações, no entanto, não serão expostos a terceiros sem o consen-timento prévio e por escrito da outra Parte,

Acordam o seguinte:

Artigo I
Objeto e Aplicabilidade

O presente Acordo estabelece regras e procedimentos para a segurança de informações classificadas trocadas entre as Partes, seus indivíduos, agências e entidades.

Artigo II
Definições

Para os fins do presente Acordo

a) "informações e materiais classificados" abrangem informações e materiais de qualquer tipo ou forma que, no interesse da segurança nacional do Governo transmissor e de acordo com suas leis e regulamentos aplicáveis, requeiram proteção contra divulgação não autorizada e que tenham sido classificados conforme estabelecido no Artigo IV, parágrafo 1, deste Acordo pelas devidas

autoridades nacionais de segurança. Especificamente:

i.o termo "informações" abrange quaisquer informações classificadas, sob qualquer forma, incluindo visual, oral e escrita;

ii.o termo "materiais" abrange qualquer documento, produto ou substância nos quais informações possam ser gravadas, ou aos quais informações possam ser incorporadas, independentemente de seu caráter físico, incluindo, mas não se limitando a, escritos, hardware, equipamentos, maquinários, aparelhos, dispositivos, maquetes, fotografias, gravações, repro-duções, mapas e cartas, bem como outros produtos, substâncias ou itens a partir dos quais se possa obter informação.

b) "autoridade de segurança" significa a entidade indicada por cada Parte para a implementação do presente Acordo;

c) "necessidade de conhecer" designa o acesso a informação e materiais classificados a ser garantido apenas ao indivíduo que tenha tanto a necessidade de conhecê-la, quanto as credenciais de segurança apropriadas, para que possa desempenhar suas funções oficiais e profissionais;

d) "credencial de segurança" designa a qualificação de indivíduos, agências e entidades para o tratamento de informações e materiais classificados.

Artigo III
Implementação deste Acordo

1. Este Acordo será considerado parte integrante de qualquer contrato a ser feito ou assinado no futuro entre as Partes, ou entre quaisquer entidades, agências e unidades autorizadas, relacionadas a informações e materiais classificados de projetos de segurança entre as Partes, no tocante aos seguintes assuntos:

a) cooperação entre as Partes ou quaisquer entidades, agências e unidades autorizadas

b) relacionadas a projetos de defesa;

c) cooperação ou troca de informações classificadas em qualquer área entre as Partes ou

d) quaisquer entidades, agências e unidades;

e) cooperação, troca de informações classificadas, parcerias, contratos ou quaisquer outras relações entre as Partes, ou quaisquer entidades governamentais, entidades públicas ou privadas, agências e unidades autorizadas pelas Partes no tocante a projetos de segurança;

f) venda de equipamentos e conhecimento, incluindo informação e materiais classificados relacionados a projetos de defesa;

g) transferência de informações classificadas entre as Partes por intermédio de qualquer representante, empregado ou consultor (privado ou outro) referente a projetos de defesa.

2. Cada Parte notificará entidades, agências e unidades relevantes em seu país da existência deste Acordo, após levar em conta a classificação de segurança dos respectivos contratos a serem assinados no futuro.

3. Os dispositivos deste Acordo vincularão e serão devidamente observados por todas as entidades, agências e unidades das respectivas Partes.

4. As autoridades de segurança informarão uma à outra de suas respectivas legislações em vigor que regulem a segurança de informações classificadas, bem como quaisquer modificações nelas introduzidas.

5. Cada Parte será responsável por informações e materiais classificados a partir do momento de sua recepção. Essa responsabilidade sujeitar-se-á aos dispositivos e práticas relevantes deste Acordo.

Artigo IV

Classificação de Segurança e Divulgação

1. Informações e materiais poderão ser classificados em uma das seguintes categorias de segurança:

Classificação israelense	Inglês	Classificação brasileira
Sodi Beyoter	(Top Secret)	Ultra-Secreto
Sodi	(Secret)	Secreto
Shamur	(Confidential)	Confidencial
Shamur	(Restricted)	Reservado

2. As Partes não divulgarão informações e materiais classificados cobertos por este Acordo a terceiros, sem o consentimento prévio e escrito da Parte transmissora. Se essa divulgação for autorizada pela Parte transmissora, terceiros utilizarão essas informações e materiais classificados somente para os propósitos especificados, conforme vier a ser acordado entre as Partes.

3. De acordo com suas leis, regulamentos e práticas nacionais, ambas as Partes tomarão as medidas apropriadas para proteger informações e materiais classificados. As Partes aplicarão a informações e materiais classificados recebidos o mesmo nível de proteção de segurança de suas informações e materiais classificados em categoria equivalente, conforme estabelecido no parágrafo 1 deste Artigo.

4. O acesso a informações e materiais classificados será facultado somente a pessoas quetenham necessidade de conhecer e que tenham sido credenciadas e autorizadas por sua Parte de

origem.

5. Cada Parte abster-se-á de realizar publicações de qualquer tipo, relativas às áreas de cooperação e às atividades mútuas cobertas por este Acordo. Sem prejuízo ao acima exposto, qualquer anúncio ou desmentido relevante por qualquer das Partes a ser feito no futuro deverá ser submetido à consulta e a consentimento mútuo.

6. A credencial de segurança para informações e materiais classificados será restrita àqueles com necessidade de conhecer.

7. As Partes reconhecem mutuamente credenciais de segurança emitidas nos termos da legislação da outra Parte.

8. Informações e materiais classificados como ultra-secretos não serão traduzidos, reproduzidos ou destruídos, salvo autorização expressa, por escrito, pela autoridade nacional de segurança da Parte transmissora.

Artigo Vº
Classificação de Segurança e Divulgação

1. O acesso a informações e materiais classificados e a instalações onde projetos de segurança sejam realizados será concedido por uma Parte a qualquer pessoa nacional da outra Parte, desde que seja obtida permissão prévia da autoridade nacional de segurança competente da Parte anfitriã. Essa autorização será concedida somente com base em pedidos de visitas a pessoas que tenham obtido credencial de segurança e que tenham sido autorizadas a lidar com informações e materiais classificados (doravante denominados “Visitantes”).

2. A autoridade de segurança da Parte visitante deverá notificar a autoridade nacional de segurança da Parte anfitriã acerca de visitantes previstos, com pelo menos quatro semanas de antecedência em relação à visita planejada. No caso de necessidades especiais, a credencial de segurança será concedida, assim que possível, sujeita à coordenação prévia.

3. Os pedidos de visita deverão incluir pelo menos os seguintes dados:

a) nome do visitante, data e local de nascimento, nacionalidade e número do passaporte;

b) cargo oficial do visitante e o nome das entidades, agências e unidades, fábrica ou organização por ele representada;

c) grau da credencial de segurança do visitante, dada por suas autoridades nacionais de segurança;

d) data planejada para a visita;

e) objetivo da visita;

f) nome das entidades, agências e unidades que se pretende visitar;

g) nome das pessoas na Parte anfitriã a serem visitadas, unidades.

4. Pedidos de visita serão entregues por meio dos canais apropriados, de acordo com o que for acordado pelas Partes.

5. Sem prejuízo ao disposto nesse Artigo, os requisitos estipulados no parágrafo 3 acima se aplicam a todas as atividades mencionadas no Artigo III, parágrafo 1.

6. A autoridade nacional de segurança da Parte anfitriã deverá notificar a autoridade nacional de segurança da Parte visitante sobre a aprovação da visita com antecedência mínima de 10 (dez) dias da data planejada para a visita.

7. Após aprovação pela autoridade nacional de segurança, a autorização para a visita será concedida pelo período específico que ser fizer necessário para o projeto específico. Autorizações para múltiplas visitas serão concedidas para períodos que não excedam 12 meses.

8. A Parte anfitriã deverá tomar todas as medidas e os procedimentos de segurança necessários para garantir a segurança física dos visitantes no seu território.

9. As autoridades nacionais de segurança da Parte anfitriã deverão coordenar-se com as autoridades nacionais de segurança da Parte visitante em todos os assuntos relativos à segurança física dos visitantes.

10. Sem prejuízo às obrigações acima mencionadas, a Parte anfitriã deverá:

a) notificar a Parte visitante de quaisquer alertas específicos sobre possíveis hostilidades, incluindo atos terroristas que possam por em risco seu pessoal visitante ou ameaçar a segurança desses;

b) em caso de qualquer alerta aqui especificado, tomar todas as medidas e os procedimentos de segurança adequados, incluindo medidas de proteção e evacuação de visitantes em áreas de risco no seu território.

Artigo VIº
Transferência de Informações e Materiais Classificados

1. Informações e materiais classificados serão requisitados e transmitidos entre as Partes por via diplomática ou por indivíduos, agências ou entidades com credenciais de segurança próprias e autorizadas pela Parte transmissora.

2. As informações e materiais classificados serão transmitidos através de sistemas de comunicação, redes ou mídias eletromagnéticas protegidos, mediante acordo prévio entre as Partes.

3. Caso a Parte receptora queira utilizar informações e materiais classificados recebidos fora de seu território, tanto a transferência quanto o uso deverão ser previamente coordenados com a Parte transmissora.

Artigo VIIº

Medidas em Caso de Falha na Proteção de Informações e Materiais Classificados

1. Em caso de falha na proteção de informações e materiais classificados, a Parte receptora:

a) informará imediatamente a autoridade nacional de segurança da Parte transmissora sobre o caso conhecido ou suspeito em que informações e materiais classificados recebidos possam ter sido perdidos ou divulgados a pessoas não autorizadas, por meio de sua autoridade nacional de segurança;

b) investigará o caso conhecido ou suspeito;

c) informar à Parte transmissora, oportunamente, os pormenores de qualquer ocorrência, assim como o resultado final da investigação e as ações corretivas tomadas de forma a evitar a reincidência.

2. A Parte que realizar a investigação deve arcar com todos os custos decorrentes sendo que eles não serão objeto de reembolso pela outra Parte.

Artigo VIII

Autoridade Nacional de Segurança

1. Cada Parte designará uma autoridade competente de seu estado como autoridade nacional de segurança para supervisionar a implementação deste Acordo em todos os seus aspectos.

Pela Parte israelense – A Diretoria de Segurança para o Apa

Pela Parte brasileira – O Diretor do Departamento da Segurança da Informação e Comunicação

1. As autoridades de segurança das Partes deverão estabelecer planos de segurança para a troca de informações e materiais classificados, em conformidade com o estipulado no presente Acordo.

2. Ambas as autoridades nacionais de segurança, cada uma em seu âmbito territorial, prepararão e distribuirão instruções de segurança e procedimentos para a proteção de informações e materiais classificados, como estipulado no Artigo II deste Acordo.

3. As Partes coordenarão, previamente, o estabelecimento de provisões, instruções, procedimentos e práticas relativas à implementação do presente Acordo, assim como de todos os contratos entre entidades e agências públicas e privadas devidamente autorizadas, contratadas pelas Partes.

4. Cada uma das Partes poderá convidar especialistas em segurança da outra Parte para visitar as instalações de sua autoridade nacional de segurança e das entidades, agências e unida-des autorizadas, quando mutuamente conveniente, para discutir procedimentos e infraestrutura para a proteção de informações e materiais classificados.

Artigo IX

Divulgação de Informações e Materiais Classificados

para Entidades, Agências e Unidades Autorizadas

1. No caso de uma das Partes ou suas entidades, agências e unidades adjudicar um contrato relacionado aos assuntos referidos no Artigo III, parágrafo 1, a ser executado no território da outra Parte, e esse contrato envolver informações e materiais classificados, então a Parte em cujo território o contrato for executado responsabilizar-se-á pela aplicação das medidas de segurança para a proteção de informações e materiais classificados, conforme seus próprios padrões e requisitos.

2. Antes da transmissão de informações e materiais classificados por uma Parte a provedores ou prováveis provedores da outra, a Parte receptora:

a) garantirá que cada provedor ou provável provedor e suas instalações tenham condições para proteger as informações e materiais classificados;

b) emitirá, para efeito da alínea a deste parágrafo, credencial de segurança apropriada às instalações envolvidas;

c) emitirá credenciais de segurança apropriadas ao pessoal que necessite ter acesso a

d) informações e materiais classificados para o cumprimento de suas funções;

e) garantirá que todas as pessoas com acesso a informações e materiais classificados tenham conhecimento de suas responsabilidades no sentido de proteger tais informações, de acordo com a legislação vigente;

f) executará inspeções de segurança periódicas nas instalações credenciadas.

Artigo X
Custos e Apoio

1. Cada uma das Partes arcará com os respectivos custos de implementação do presente Acordo, incluindo os decorrentes de qualquer violação de segurança.

2. Cada Parte prestará apoio ao pessoal da outra Parte que estiver realizando serviços no seu país ou exercendo os direitos estabelecidos neste Acordo no território da outra Parte.

Artigo XI
Resolução de Controvérsias

1. Em relação a qualquer controvérsia que possa surgir entre as Partes deste Acordo, relativa tanto à interpretação deste Acordo quanto da execução dos termos aqui presentes ou qualquer matéria relacionada, as Parte, em primeira instância, envidarão esforços para chegar a uma solução amigável.

2. Nos casos em que as Partes não cheguem a solução amigáveis, as Partes submeterão a

controvérsia ao Diretor de Segurança do Aparato de Defesa de Israel e ao Diretor do Departa-mento de Segurança da Informação e Comunicação do Brasil.

3. Durante a controvérsia, ambas as Partes continuarão a cumprir suas obrigações no âmbito deste Acordo.

Artigo XII

Comunicações

Todas as comunicações entre as Partes, relativas à implementação deste Acordo, serão feitas por escrito, em inglês, sujeitas a restrições de segurança, e encaminhadas aos seguintes destinatários:

Estado de Israel – Ministério da Defesa Diretor de Segurança das Informações

Diretoria de Segurança para o Estabelecimento da Defesa

República Federativa do Brasil – Gabinete de Segurança Institucional da Presidência da República

Coordenador Geral de Gestão de Segurança e Credenciamento Departamento de Segurança das Informações e Comunicações

Artigo XIII

Vigência, Emendas e Aplicação

1. Este Acordo entrará em vigor no trigésimo dia após a data da última notificação, por escrito ou por via diplomática, de que foram cumpridos os requisitos de direito interno das Partes, necessários para a sua entrada em vigor.

2. O presente Acordo poderá ser emendado por consentimento mútuo entre as Partes, por meio de canais diplomáticos. Emendas entrarão em vigor conforme disposto no parágrafo 1 do presente Artigo.

3. Este Acordo será complementado por planos de trabalho que regularão o “MODUS OPERANDI” de cada projeto de defesa entre as Partes.

Artigo XIV

Validade e Denúncia

1. O presente Acordo vigorará por tempo indeterminado.

2. Qualquer Parte poderá informar a outra, a qualquer momento, por via diplomática, de sua decisão de denunciar o presente Acordo. A denúncia surtirá efeitos seis (6) meses após a data da notificação.

3. Em caso de denúncia, quaisquer informações e materiais classificados trocados nos termos do presente Acordo continuarão a ser protegidos pela Parte receptora, salvo caso a Parte transmissora autorize, expressamente, a Parte receptora a se escusar dessa obrigação.

Feito em Tel Aviv, em 24 de novembro de 2010, em dois originais, nos idiomas português e inglês, sendo ambos os textos igualmente autênticos.

Em testemunho do que, as Partes subscrevem e assinam este Acordo no dia e ano acima mencionados.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

Jorge Armando Felix
Ministro de Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

PELO GOVERNO DO ESTADO DE ISRAEL

Ehud Barak
Ministro da Defesa

Amir Kain
Diretor de Segurança para o Estabelecimento da Defesa

EMENDA AO ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DO ESTADO DE ISRAEL (MINISTÉRIO DA DEFESA) SOBRE PROTEÇÃO DE INFORMAÇÕES CLASSIFICADAS E MATERIAIS ASSINADO EM TEL AVIV EM 24 DE NOVEMBRO DE 2010

O Governo da República Federativa do Brasil (Representado pelo Gabinete de Segurança Institucional da Presidência da República)

e

O Governo do Estado de Israel (representado pelo Ministério da Defesa do Estado de Israel) (doravante denominados "Partes"),

Desejosos de alterar certas disposições do Acordo para a Proteção de Informações Classi-ficadas e de Materiais entre o Governo da República Federativa do Brasil e o Governo do Estado de Israel (Ministério da Defesa), assinado em Tel Aviv, em 24 de novembro de 2010 (doravante designado por "Acordo de Segurança")

Artigo I

Objeto

1. A presente Emenda tem por objetivo atualizar o Acordo de Segurança devido à mudanças na legislação nacional da Parte Brasileira.

2. Por consentimento mútuo das Partes, esta Emenda torna-se parte do Acordo de Segurança assinado em Tel Aviv, em 24 de novembro de 2010.

Artigo II

Autoridade Nacional de Segurança

No parágrafo 1º do Artigo VIII do Acordo de Segurança, o trecho: "O Diretor do Departamento de Segurança da Informação e Comunicação" será alterado para: "Gabinete de Segurança Institucional da Presidência da República".

Artigo III

Classificação de Segurança da Informação

A tabela de equivalência de categorias, no parágrafo 1o do Artigo IV do Acordo de Segurança, será alterada da seguinte forma:

Para ambas as partes, a Informação classificada será protegida de acordo com a legislação

nacional conforme segue:

Classificação no Brasil	Inglês	Classificação em Israel
ULTRASSECRETO	Top Secret	SODI BEYOTER
SECRETO	Secret	SODI
RESERVADO	Restricted	SHAMUR

Artigo IV
Material

1. Para todos os contextos relacionados a este Acordo, qualquer material classificado israelense será considerado Material de Acesso Restrito para a parte brasileira, conforme estabele-cido na regulamentação brasileira, e será tratado de acordo com as medidas e procedimentos apropriados que estejam em conformidade com seu nível equivalente de classificação de se-gurança de Israel, conforme estabelecido no Artigo III desta Emenda.

2. Qualquer Material contendo informações sigilosas originado pela Parte Brasileira e considerado por ela como Material de Acesso Restrito, será categorizado pela Parte Israelense de acordo com mais alto grau de classificação da informação que ele contém, de acordo com o Artigo III desta Emenda.

3. Qualquer Material que não contenha informação sigilosa, originado pela Parte Brasileira e considerado por ela como Material de Acesso Restrito, será categorizado como “RESERVADO” pela Parte Israelense.

Artigo V
Entrada em vigor, Emendas e Aplicação

Esta Emenda entrará em vigor de acordo com o parágrafo 1 do Artigo XIIII do Acordo de Segurança.

Feito em Tel Aviv/Brasília, em 6 de junho de 2018, em duas cópias originais, na versão em língua portuguesa e na versão em língua inglesa, com textos igualmente autênticos. No caso de divergências, o texto em inglês deverá prevalecer.

Em testemunho do que, as Partes subscrevem, apertam as mãos e assinam esta

Emenda no dia e ano acima mencionados.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

Sergio Westphalen Etchegoyen Ministro do Gabinete de Segurança Institucional da Presidência da República

PELO GOVERNO DO ESTADO DE ISRAEL

Nir Ben-Moshe
Diretor do DSDE

Avigdor Liberman
Ministro da Defesa do Estado de Israel

DECRETO Nº 11.609, DE 19 DE JULHO DE 2023 (EMIRADOS ÁRABES UNIDOS)

VERSÃO PUBLICADA

Aprova o texto do Acordo entre a República Federativa do Brasil e os Emirados Árabes Uni-dos sobre Troca e Proteção Mútua de Informação Classificada e Material, assinado em Abu Dhabi, em 27 de outubro de 2019.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, no uso da atribuição que lhe confere o art. 84, *caput*, inciso IV, da Constituição, e

Considerando que o Acordo entre a República Federativa do Brasil e os Emirados Árabes Unidos sobre Troca e Proteção Mútua de Informação Classificada e Material foi firmado em Abu Dhabi, em 27 de outubro de 2019;

Considerando que o Congresso Nacional aprovou o Acordo por meio do Decreto Legislativo nº 153, de 19 de outubro de 2022; e

Considerando que o Acordo entrou em vigor para a República Federativa do Brasil, no plano jurídico externo, em 19 de abril de 2023, nos termos do seu Artigo XVII;

DECRETA:

Art. 1º Fica promulgado o Acordo entre a República Federativa do Brasil e os Emirados Árabes Unidos sobre Troca e Proteção Mútua de Informação Classificada e Material, firmado em Abu Dhabi, em 27 de outubro de 2019, anexo a este Decreto.

Art. 2º São sujeitos à aprovação do Congresso Nacional atos que possam resultar em revisão do Acordo e ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional, nos termos do inciso I do *caput* do art. 49 da Constituição.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Brasília, 19 de julho de 2023; 202º da Independência e 135º da República.

GERALDO JOSÉ RODRIGUES ALCKMIN FILHO

Mauro Luiz Iecker Vieira

ACORDO ENTRE A REPÚBLICA FEDERATIVA DO BRASIL E OS EMIRADOS ÁRABES UNIDOS SOBRE TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA E MATERIAL

A República Federativa do Brasil, e

Os Emirados Árabes Unidos

(doravante denominados “Partes” ou se separadamente como “Parte”),

No interesse da segurança nacional e com a finalidade de assegurar a proteção das Infor-mações Classificadas e de Material trocados dentro da esfera de tratados de cooperação ou contratos firmados entre as Partes, seus indivíduos, órgãos e entidades credenciados, bem como entidades públicas ou privadas;

Desejando estabelecer um conjunto de regras e procedimentos sobre a proteção de Infor-mações Classificadas e Materiais de acordo com as leis e regulamentos nacionais das Partes;

Confirmando que este Acordo não afetará os compromissos de ambas as Partes, decorrentes de outros acordos internacionais, e que não será utilizado contra os interesses, a segurança e a integridade territorial de outros Estados, acordam o seguinte:

Artigo I
Objeto e escopo de aplicação

O presente Acordo estabelece regras e procedimentos para a proteção de Informações Classificadas e Material trocados e gerados no processo de cooperação, em relação a seus interesses e segurança nacionais, entre as Partes anteriormente mencionadas, seus indivíduos, agências e entidades credenciadas.

Artigo II
Definições

Para os efeitos do presente Acordo, o termo:

a) Contrato Classificado: significa qualquer contrato ou subcontrato incluindo as negocia-ções pré-contratuais, entre dois ou mais Contratantes que criem e definam direitos e obrigações aplicáveis entre eles, que contenha ou preveja o acesso à Informação Classificada;

b) Informação Classificada: significa a informação, independentemente da sua forma, natu-reza e meio de transmissão, determinada de acordo com as respectivas Leis e Regulamentos de ambas as Partes, protegida contra acesso ou divulgação não autorizados, que tenha sido classificada e for trocada ou gerada pelas partes;

c) Comprometimento: designa qualquer forma de uso indevido, dano ou acesso não autorizado, alteração, divulgação ou destruição de Informação Classificada, bem como qualquer outra ação ou inação, devido a uma quebra de segurança, resultando em perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;

d) Contratante: significa um indivíduo, agência ou entidade que possui capacidade legal para celebrar contratos;

e) Habilitação de Segurança de Instalação (FSC): significa uma habilitação fornecida pela Autoridade Nacional de Segurança de uma Parte que uma entidade pública ou privada locali-zada em seu país está autorizada e possui medidas de segurança apropriadas dentro de uma instalação específica para o Tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais;

f) Autoridade Nacional de Segurança (NSA): designa o órgão de Estado especificado pela legislação nacional das Partes, especialmente autorizado na esfera de proteção de Informação Classificada;

g) Necessidade de Conhecer: designa a condição pela qual o acesso à Informação Classificada pode ser concedido a um indivíduo que tenha um requisito verificado para conhecimento ou posse de tais informações, a fim de ser capaz de desempenhar funções e tarefas oficiais;

h) Parte de Origem: significa a Parte, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição, que criou a informação classificada;

i) Credencial de Segurança Pessoal (PSC): significa a autorização fornecida pela Autoridade de Segurança Nacional de uma Parte de que um indivíduo tenha sido credenciado para o Trata-mento de Informações Classificadas, de acordo com suas leis e regulamentos nacionais; onde o indivíduo está autorizado a ter acesso e a lidar com as Informações Classificadas até o nível definido na autorização;

j) Parte Receptora: significa a Parte, incluindo quaisquer entidades públicas ou privadas sob sua jurisdição, que recebe Informação Classificada;

k) Violação de Segurança: significa a ação ou omissão, seja intencional ou acidental, que resulta no real ou possível comprometimento da Informação Classificada;

l) Nível de Classificação de Segurança: significa a categoria, de acordo com as leis e regulamentos nacionais das Partes, que caracteriza a importância da Informação Classificada, o nível de restrição de acesso a ela e o nível de sua proteção pelas Partes, e também a categoria com base na qual a informação é marcada;

m) Credenciamento de Segurança: designa o processo de emissão de um FSC ou PSC pela Autoridade Nacional de Segurança, em conformidade com as leis e regulamentos nacionais das Partes;

n) Terceira Parte: designa os Estados, qualquer organização internacional, governos ou in-

divíduos que representam órgãos ou organizações estaduais, incluindo quaisquer entidades públicas e privadas, que não sejam Partes deste Acordo;

o) Tratamento da Informação Classificada: designa um conjunto de ações relacionadas à produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, distribui-ção, arquivamento, armazenamento, descarte, avaliação, destino ou controle de Informação Classificada em qualquer Nível de Classificação de Segurança; e

p) Visita: significa qualquer acesso a entidade pública ou privada, para efeitos do presente Acordo, que inclua o Tratamento de Informação Classificada.

Artigo III
Níveis de Classificação de Segurança

1. De acordo com as leis e regulamentos nacionais, as Partes concordam que os Níveis de Classificação de Segurança devem corresponder entre si da seguinte forma e são considerados equivalentes:

Nos Emirados Árabes Unidos (linguagem correspondente)	Equivalente em Inglês	Na República Federativa do Brasil (Português)
قياغلل يرس	Top Secret	Ultrassecreto
يرس	Secret	SECRETO
موتكم	Confidential	
روظحم	Restricted	Reservado

2. Qualquer Informação Classificada fornecida sob este Acordo deverá ser marcada com o Nível de Classificação de Segurança apropriado de acordo com as leis e regulamentos nacionais da Parte Originadora.

3. As Partes deverão identificar toda Informação Classificada recebida da outra Parte com um Nível de Classificação de Segurança equivalente, de acordo com o parágrafo 1 deste Artigo.

4. As Partes notificar-se-ão mutuamente sobre quaisquer alterações aos Níveis de Classificação de Segurança especificados no parágrafo 1 e sobre todas as alterações de classificação subsequentes à Informação Classificada transmitida.

5. A Parte de Origem deverá notificar a Parte Receptora, sem atrasos, sobre quaisquer mudanças no Nível de Classificação de Segurança das Informações Classificadas transmitidas.

Artigo IV

Proteção da Informação Classificada

1. As Partes tomarão todas as medidas apropriadas para assegurar que o nível de proteção concedido à Informação Classificada recebida esteja de acordo com o Nível de Classificação de Segurança equivalente ao estabelecido no Artigo III deste Acordo;

2. Nenhuma disposição do presente Acordo prejudica a legislação ou regulamentação nacional das Partes no que diz respeito aos direitos das pessoas físicas de obterem acesso a documentos públicos ou acesso a informação de caráter público, à proteção de dados pessoais ou à proteção de Informação Classificada;

3. De acordo com as leis e os regulamentos nacionais, cada Parte deverá assegurar que sejam implementadas medidas apropriadas para tratamento e proteção da Informação Classificada.

Artigo V

Divulgação e uso da Informação Classificada

1. Cada Parte deverá assegurar que a Informação Classificada fornecida ou trocada sob o presente Acordo não será:

a) desclassificada ou reclassificada com nível de sigilo inferior, sem o prévio consentimento por escrito da Parte de Origem;

b) utilizada para fins diferentes dos estabelecidos pela Parte de Origem;

c) divulgada a qualquer Terceira Parte sem o consentimento prévio por escrito da Parte de Origem. Neste caso, deve vigorar um acordo apropriado ou contrato para proteção da Informação Classificada com a referida Terceira Parte.

Artigo VI

Acesso à Informação Classificada

1. Cada Parte deverá assegurar que o acesso à informação classificada somente será concedido com base no princípio da “Necessidade de Conhecer”.

2. Cada Parte deverá assegurar que todos os indivíduos que tiverem acesso à Informação Classificada estejam informados da sua responsabilidade de proteção dessas informações, de acordo com as normas de segurança em vigor.

3. As Partes deverão assegurar que o acesso à Informação Classificada somente será concedido aos indivíduos que possuam uma Credencial de Segurança Pessoal apropriada ou que estejam devidamente autorizados por força das suas funções, em conformidade com a legis-lação nacional em

vigor.

4. De acordo com suas leis e regulamentos nacionais, cada Parte deverá garantir que qualquer entidade sob sua jurisdição que possa receber ou gerar Informação Classificada possua a apropriada Habilitação de Segurança e seja capaz de proporcionar proteção adequada à mesma, conforme disposto no parágrafo 1 do Artigo IV deste Acordo, no Nível de Classificação de Sigilo apropriado.

Artigo VII

Tradução, Reprodução e Destruição de Informação Classificada

1. Todas as traduções e reproduções de Informação Classificada devem possuir as apropriadas marcas de Nível de Classificação de Segurança e devem ser protegidas e controladas pelas Partes, como os originais;

2. Todas as traduções de informações classificadas deverão conter uma anotação adequada, na língua para a qual foram traduzidas, indicando que contêm informação classificada da Parte de Origem;

3. De acordo com o Artigo VI parágrafo 3 deste Acordo, os tradutores devem possuir uma Credencial de Segurança Pessoal no nível de sigilo da Informação Classificada a ser traduzida;

4. A Informação Classificada marcada como ULTRASSECRETO somente poderá ser traduzida ou reproduzida mediante autorização prévia por escrito da Parte de Origem.

5. O número de reproduções deve ser limitado ao mínimo necessário para sua finalidade oficial, e deve ser feito apenas por indivíduos com Credencial de Segurança Pessoal apropriado e Necessidade de Conhecer.

6. As informações classificadas recebidas nos termos deste Acordo não serão destruídas. Quando não for mais considerado necessário pela Parte Receptora, será devolvido à Parte de Origem.

Artigo VIII

Transmissão entre as Partes

1. A Informação Classificada será transmitida entre as Partes através dos canais diplomáticos ou conforme acordado pelas Partes.

2. A Informação Classificada deve ser transmitida através de sistemas de comunicações protegidos, redes ou outros meios eletromagnéticos protegidos que tenham sido acordados por ambas as Partes.

3. A Informação Classificada marcada como ULTRASSECRETA deve ser enviada somente por canais diplomáticos.

4. A Parte Receptora não transmitirá Informação Classificada a Terceira Parte, sem a prévia

aprovação por escrito da ANS da Parte de Origem.

Artigo IX
Visitas

1. Visitas às instalações onde a Informação Classificada é manuseada ou armazenada estarão sujeitas à aprovação prévia da Autoridade de Segurança Nacional da Parte anfitriã, a menos que de outra forma mutuamente aprovada.

2. O pedido de visita deve ser submetido à Autoridade de Segurança Nacional da Parte anfitriã e deve incluir os seguintes dados a serem utilizados apenas para a finalidade da visita:

a) o nome do visitante, data e local de Nascimento, nacionalidade e número de carteira de

b) identidade/passaporte;

c) cargo e função do visitante, bem como o nome e endereço da instalação onde ele/ela

d) está empregado;

e) especificação do projeto em que o visitante está participando;

f) a validade e o nível da Credencial de Segurança Pessoal do visitante;

g) o nome, endereço, número de telefone, e-mail e ponto de contato das instalações a serem

h) visitadas;

i) o objetivo da visita, incluindo a entidade que se pretende visitar e o nível mais alto de classificação de sigilo de informação classificada envolvida;

j) a data e a duração da visita. Para visitas recorrentes, deve ser indicado o período total das visitas; e

k) Identificação da autoridade requerente.

3. O pedido de visita deverá ser apresentado pelo menos 30 (trinta) dias antes da visita, a menos que de outra forma mutuamente aprovada pelas Autoridades Nacionais de Segurança.

4. Qualquer Informação Classificada compartilhada para o visitante será considerada como Informação Classificada recebida nos termos deste Acordo. O visitante deverá cumprir as normas de segurança da Parte anfitriã.

5. As visitas serão autorizadas por uma das Partes aos visitantes da outra Parte, apenas se esses:

a) possuírem Credencial de Segurança Pessoal válida concedida por seu país de origem; e

b) estiverem autorizados a receberem ou terem acesso à Informação Classificada de acordo com o Princípio da Necessidade de Conhecer.

6. Uma vez autorizada a Visita, a Autoridade Nacional de Segurança do país anfitrião deverá notificar a Autoridade de Segurança Nacional do país do visitante sobre sua autorização com antecedência mínima de 10 (dez) dias da visita prevista e fornecerá uma cópia do pedido e da autorização

à entidade a ser visitada.

Artigo X

Contratos Classificados relacionados a este Acordo

1. No caso de Contratos Classificados celebrados e implementados no território de uma das Partes, a NSA da outra Parte deverá obter uma garantia prévia por escrito de que o Contratado proposto detém as FSC e PSC necessárias ao nível apropriado.

2. O Contratante compromete-se, sob a supervisão da respectiva Autoridade, a:

a) possuir a devida Habilitação de Segurança de Instalação;

b) garantir que todas as pessoas com acesso a Informação Classificada possuam Credencial de Segurança Pessoal apropriada e sejam informadas de sua responsabilidade em relação à sua proteção, de acordo com as leis e regulamentos; e

c) não divulgar ou permitir a divulgação da Informação Classificada a um terceiro não expressamente autorizado por escrito pela Parte de Origem.

3. Para cada contrato adjudicado, a Parte de Origem informará a Parte Receptora do Nível de Classificação de Segurança da Informação transferida.

4. Os Contratos Classificados também devem fornecer estes termos adicionais:

a) responsabilidade pelo não cumprimento dos procedimentos e medidas de segurança

b) aplicáveis à Informação Classificada;

c) obrigação de informar qualquer Violação de Segurança ou comprometimento de Informa-

d) ção Classificada à sua Autoridade Nacional de Segurança;

e) responsabilidade pelos danos resultantes de Violação de Segurança.

5. Qualquer subcontratante deve cumprir as mesmas obrigações de segurança que o Contratante.

Artigo XI

Material

1. Para todos os contextos relacionados a este Acordo, qualquer material classificado nos Emirados Árabes Unidos será considerado pela Parte Brasileira como “Material de Acesso Restrito”, conforme estabelecido na regulamentação brasileira, e será tratado de acordo com as medidas e procedimentos apropriados que devem estar em conformidade com o seu nível equivalente de classificação de segurança dos Emirados Árabes Unidos, conforme estabelecido no Artigo III deste Acordo.

2. Qualquer Material que contenha Informação Classificada, originada pela Parte Brasileira e por ela considerado “Material de Acesso Restrito”, será categorizado pela Parte dos Emirados Árabes Unidos, segundo o mais alto nível de classificação de segurança das informações nele contida, conforme estabelecido no Artigo III deste Acordo.

3. Qualquer Material que não contenha Informação Classificada, originado por qualquer das Partes e considerado “Material de Acesso Restrito”, será categorizado como restrito pela outra Parte.

Artigo XII

Autoridades Nacionais de Segurança e Cooperação em Segurança

1. As Autoridades Nacionais de Segurança responsáveis pela implementação e supervisão do presente acordo serão:

Na República Federativa do Brasil:

Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da

República Federativa do Brasil

Nos Emirados Árabes Unidos:

As Forças Armas dos Emirados Árabes Unidos

2. Cada Parte fornecerá à outra, por escrito, os dados de contato de suas respectivas Autoridades de Segurança Nacional.

3. As Autoridades de Segurança Nacional deverão informar mutuamente sobre suas respectivas leis e regulamentos nacionais em vigor que regulam a segurança da Informação Classificada.

4. As Autoridades de Segurança Nacional deverão informar mutuamente sobre quaisquer alterações que lhes digam respeito ou sobre as Credenciais de Segurança de indivíduos, agências e entidades.

5. Com o objetivo de assegurar uma estreita cooperação na aplicação do presente Acordo, as Autoridades Nacionais de Segurança podem ser consultadas sempre que solicitado por uma delas.

6. Representantes da Autoridade Nacional de Segurança de uma Parte poderão visitar os estabelecimentos da Autoridade Nacional de Segurança da outra Parte com o intuito de adquirir conhecimento dos procedimentos e medidas de segurança aplicáveis à Informação Classificada.

7. As Partes, por intermédio das suas Autoridades Nacionais de Segurança, deverão informar mutuamente, e tempestivamente, de quaisquer alterações no título desses organismos ou das transferências das suas competências para outros órgãos.

8. Se solicitado, as Partes, por meio de suas Autoridades Nacionais de Segurança, levando em conta as respectivas leis e regulamentos nacionais, colaborarão entre si durante os procedimentos necessários para o Credenciamento de Segurança de Pessoas que viveram ou vivem em território da outra parte.

9. As Partes reconhecem mutuamente as Credenciais de Segurança de Pessoas e as Habilitações de Segurança de Instalações emitidas.

10. As Partes deverão prontamente informar mutuamente acerca de qualquer mudança quanto ao reconhecimento de Credenciais de Segurança de Pessoas e as Habilitações de Segurança de Instalações.

11. Para alcançar e manter os padrões comparáveis de segurança, as Autoridades Nacionais de Segurança deverão, mediante solicitação, prestar informações mútuas sobre seus procedimentos nacionais de segurança, normas e práticas de segurança para a proteção de Informação Classificada. Se necessário, as Autoridades Nacionais de Segurança poderão realizar reuniões regulares.

12. Mediante solicitação, as Partes fornecerão assistência mútua na realização de Credenciamento de Segurança de Pessoas.

Artigo XIII
Violação de Segurança

1. No caso de uma Violação de Segurança relacionada a Informação Classificada que envolva as Partes deste Acordo, a Autoridade de Segurança Nacional da Parte em que a Violação de Segurança ocorrer informará imediatamente à Autoridade de Segurança Nacional da outra Parte.

2. Quando a Violação de Segurança ocorrer com uma Terceira Parte, a Autoridade de Segurança Nacional da Parte de Origem informará à Autoridade de Segurança Nacional da outra Parte, o mais breve possível, e garantirá uma apropriada investigação.

3. A Parte competente tomará todas as medidas de acordo com as leis e regulamentos nacionais, de modo a limitar as consequências da Violação mencionada no Parágrafo 1 deste Artigo e evitar futuras violações. Mediante pedido, a outra Parte prestará assistência adequada; deverá ser informado o resultado do processo e das medidas tomadas em virtude da Violação de Segurança.

4. A Parte onde a Violação de Segurança acontecer deverá investigar ou acompanhar a investigação do incidente e, no final, informar imediatamente a outra Parte sobre o resultado da investigação e as medidas corretivas aplicadas.

5. A outra Parte deverá, quando demandada, cooperar com a investigação.

Artigo XIV
Custos

Cada Parte deverá arcar com os custos de suas próprias despesas resultantes da implementação e supervisão de todos os aspectos do presente Acordo.

Artigo XV

Solução de Controvérsias

1. Qualquer controvérsia que surgir entre as Partes em relação à interpretação ou aplicação do presente Acordo, ou qualquer assunto relacionado, deverá ser resolvida, se necessário, por meio de consultas e negociações entre as Partes, por meio de canais diplomáticos. As Partes poderão acordar em iniciar as negociações no prazo de 30 (trinta) dias, ou menos, a partir da data em que uma das Partes receber uma notificação por escrito da outra Parte.

2. Nenhuma controvérsia ou discordância poderá ser encaminhada a qualquer tribunal internacional ou Terceira Parte para solução.

3. Os procedimentos de resolução de controvérsias entre ambas as Partes serão conduzidos com base no princípio da confidencialidade.

4. Durante o período de resolução de controvérsia, ambas as Partes continuarão a cumprir todas as suas obrigações no âmbito do presente Acordo.

Artigo XVI

Comunicações

Todas as comunicações entre as Partes relacionadas à implementação deste Acordo deverãoser feitas por escrito, em inglês.

Artigo XVII

Entrada em vigor

O presente Acordo entrará em vigor 30 (trinta) dias após o recebimento da última notificação, por qual das Partes tenham informado uma à outra, por via diplomática, de que os seus requisitos legais internos necessários para sua entrada em vigor foram cumpridas.

Artigo XVIII

Emendas

1. O presente Acordo poderá ser alterado a qualquer momento, por escrito, por consentimento mútuo das Partes.

2. As emendas entrarão em vigor de acordo com os termos estabelecidos no Artigo XVII do presente Acordo.

Artigo XIX

Vigência e Rescisão

1. O presente Acordo permanecerá em vigor por tempo indeterminado.

2. Qualquer uma das Partes poderá, a qualquer momento, denunciar o presente Acordo mediante notificação por escrito à outra Parte.

3. A rescisão deverá ser notificada por via diplomática e deverá entrar em vigor após 6 (seis) meses da data em que a outra Parte tenha recebido a notificação de rescisão.

4. Em caso de rescisão, qualquer Informação Classificada trocada nos termos do presente Acordo, continuará a ser protegida em conformidade com as disposições aqui estabelecidas, a menos que a Parte de Origem isente a Parte Receptora dessa obrigação.

Artigo XX

Disposições Finais

As Partes deverão imediatamente notificar uma à outra, quaisquer alterações em sua respectiva legislação nacional que afete a proteção de Informação Classificada fornecida com base no presente Acordo. No caso de tais alterações, as Partes deverão se consultar e considerar a possibilidade de realizar alterações neste Acordo. Nesse meio tempo, a informação classificada continuará a ser protegida como aqui descrito, salvo pedido em contrário da Parte de Origem, por escrito.

Feito em Abu Dhabi, em 27 de outubro de 2019, em dois originais, nos idiomas Árabe, Português e Inglês, sendo todos os textos igualmente idênticos. Em caso de divergência de inter-pretação, o texto em Inglês prevalecerá.

Em testemunho do mesmo, as Partes assinam este Acordo no dia e ano acima mencionados.

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

Ernesto Araújo
Ministro das Relações Exteriores
Augusto Heleno Ribeiro Pereira Ministro Chefe do Gabinete de Segurança Institucional

PELOS EMIRADOS ÁRABES UNIDOS

Mohammed Bin Ahmed Al Bawardi Ministro de Estado para Negócios de Defesa.

DECRETO Nº 4.073, DE 3 DE JANEIRO DE 2002

VERSÃO PUBLICADA

Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e tendo em vista o disposto na Lei no 8.159, de 8 de janeiro de 1991,

DECRETA:

CAPÍTULO I
DO CONSELHO NACIONAL DE ARQUIVOS

Art. 1º O Conselho Nacional de Arquivos - CONARQ, órgão colegiado instituído no âmbito do Arquivo Nacional, criado pelo art. 26 da Lei nº 8.159, de 8 de janeiro de 1991, tem por finalidade definir a política nacional de arquivos públicos e privados. (Redação dada pelo Decreto nº 10.148, de 2019)

Art. 2º Compete ao CONARQ:

I. estabelecer diretrizes e orientações técnicas para o funcionamento do Sistema Nacional de Arquivos – SINAR, com vistas à gestão, à preservação e ao acesso aos documentos de ar-quivos; (Redação Dada Pelo Decreto Nº 12.599, De 2025)

II. promover o inter-relacionamento de arquivos públicos, privados e comunitários, com vistas ao intercâmbio e à integração sistêmica das atividades arquivísticas; (Redação dada pelo Decreto nº 12.599, de 2025)

III. propor à Ministra de Estado da Gestão e da Inovação em Serviços Públicos atos norma-tivos necessários à implementação, ao monitoramento e ao aprimoramento da política nacional de arquivos, com vistas a ampliar o processo de participação social sobre a referida política; (Redação dada pelo Decreto nº 12.599, de 2025)

IV. zelar pelo cumprimento dos dispositivos constitucionais e legais que norteiam o funcio-namento e o acesso aos arquivos públicos;

V. subsidiar a elaboração de planos nacionais de desenvolvimento de arquivos e monitorar a sua execução, com a proposição de metas e de prioridades da política nacional de arquivos; (Redação dada pelo Decreto nº 12.599, de 2025)

VI. estimular a integração e a modernização das instituições integrantes do SINAR; (Redação dada pelo Decreto nº 12.599, de 2025)

VII. identificar os arquivos privados e comunitários de interesse público e social, nos termos do

disposto no art. 12 da Lei nº 8.159, de 8 de janeiro de 1991; (Redação dada pelo Decreto nº 12.599, de 2025).

VIII. analisar e reconhecer os arquivos privados e comunitários de interesse público e social;(Redação dada pelo Decreto nº 12.599, de 2025)

IX. propor à Ministra de Estado da Gestão e da Inovação em Serviços Públicos a declaração de interesse público e social de arquivos privados e comunitários; (Redação dada pelo Decreto nº 12.599, de 2025)

X. estimular a capacitação técnica inicial e continuada de profissionais de arquivos nas

XI. instituições integrantes do SINAR; (Redação dada pelo Decreto nº 12.599, de 2025)

XII. promover a atualização do cadastro nacional de arquivos e desenvolver as atividades

XIII. censitárias referentes a esse processo; (Redação dada pelo Decreto nº 12.599, de 2025)

XIV. propor ao Arquivo Nacional ações de articulação com outros órgãos do Poder Público e instituições responsáveis pela formulação de políticas nacionais nas áreas de educação, cul-tura, informação, ciência, tecnologia, inovação, transformação digital, meio ambiente e direitos humanos; e (Redação dada pelo Decreto nº 12.599, de 2025)

XV. apresentar e aprovar proposta de atualização do regimento interno do CONARQ. (Redação dada pelo Decreto nº 12.599, de 2025)

Art. 3º São membros conselheiros do CONARQ:

I. o Diretor-Geral do Arquivo Nacional, que o presidirá;

II. um da Secretaria-Geral da Presidência da República; (Redação dada pelo Decreto nº 12.599, de 2025)

III. um do Ministério da Cultura; (Redação dada pelo Decreto nº 12.599, de 2025)

IV. um do Ministério da Gestão e da Inovação em Serviços Públicos; (Redação dada pelo Decreto nº 12.599, de 2025)

V. um do Ministério da Justiça e Segurança Pública; (Redação dada pelo Decreto nº 12.599, de 2025)

VI. um da Advocacia-Geral da União; (Redação dada pelo Decreto nº 12.599, de 2025)

VII. dois do Congresso Nacional; (Redação dada pelo Decreto nº 12.599, de 2025)

VIII. dois do Poder Judiciário federal; (Redação dada pelo Decreto nº 12.599, de 2025)

IX. dois de Arquivos Públicos Estaduais e do Distrito Federal; (Redação dada pelo Decreto nº 12.599, de 2025)

X. dois de Arquivos Públicos Municipais; (Incluído pelo Decreto nº 12.599, de 2025)

XI. dois de Arquivos Privados; (Incluído pelo Decreto nº 12.599, de 2025)

XII. dois de Arquivos Comunitários; (Incluído pelo Decreto nº 12.599, de 2025)

XIII. quatro de organizações e instituições de ensino e pesquisa com atuação nas áreas de arquivologia, biblioteconomia, ciência da informação, ciências sociais, comunicação, educação,

história, museologia e patrimônio, ou de tecnologia e inovação;

XIV. três de associações de profissionais de arquivos; e (Incluído pelo Decreto nº 12.599, de 2025)

XV. três personalidades de notório saber sobre arquivos, gestão de documentos e acesso à informação e à memória. (Incluído pelo Decreto nº 12.599, de 2025)

§ 1º Cada membro do CONARQ terá um suplente, que o substituirá em suas ausências e seus impedimentos, exceto os referidos no inciso XVII do *caput*. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 2º Os membros do CONARQ de que tratam os incisos II a VI do *caput* e os respectivos suplentes serão indicados em ato da autoridade máxima dos respectivos órgãos do Poder Exe-cutivo federal. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 3º Os membros do CONARQ de que trata o inciso VII do *caput* e os respectivos suplentes serão indicados em ato do Presidente do Congresso Nacional.

§ 4º O membro do CONARQ de que trata o inciso VIII do *caput* e o respectivo suplente serão indicados em ato do Presidente do Supremo Tribunal Federal. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 5º Os membros do CONARQ de trata o inciso XI do *caput* e os respectivos suplentes se-rão indicados pela Rede de Arquivos Públicos Estaduais e do Distrito Federal dos respectivos Poderes Executivos no âmbito do SINAR. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 6º Ato da Ministra de Estado da Gestão e da Inovação em Serviços Públicos estabelecerá requisitos para o processo seletivo dos membros de que tratam os incisos XII a XVII do *caput* e dos respectivos suplentes, o qual: (Incluído pelo Decreto nº 12.599, de 2025)

I. será aberto às entidades cuja finalidade esteja relacionada à política nacional de arquivos; (Incluído pelo Decreto nº 12.599, de 2025)

II. observará critérios relacionados à comprovada experiência com a temática de arquivos e preservação da memória; e (Incluído pelo Decreto nº 12.599, de 2025)

III. promoverá a equidade de gênero, étnico-racial e regional. (Incluído pelo Decreto nº 12.599, de 2025)

§ 7º Os membros do CONARQ e os respectivos suplentes serão designados em ato da Ministra de Estado da Gestão e da Inovação em Serviços Públicos. (Incluído pelo Decreto nº 12.599, de 2025)

§ 8º Os membros do CONARQ e os respectivos suplentes terão mandato de dois anos, permitida uma recondução. (Incluído pelo Decreto nº 12.599, de 2025)

§ 9º Os membros do CONARQ e os respectivos suplentes não poderão exercer mais de dois mandatos, ainda que na representação de outro órgão, organização, instituição, associa-ção profissional, e demais hipóteses previstas no *caput*, exceto após o decurso de quatro anos. (Incluído pelo Decreto nº 12.599, de 2025)

§ 10. A restrição prevista no § 9º não se aplica a quem exercer a Presidência do CONARQ.

(Incluído pelo Decreto nº 12.599, de 2025)

§ 11. O Presidente do CONARQ terá um suplente, que o substituirá em suas ausências e seus impedimentos. (Incluído pelo Decreto nº 12.599, de 2025)

Art. 4º Caberá ao Arquivo Nacional dar o apoio técnico e administrativo ao CONARQ, por meio da Secretaria-Executiva do CONARQ. (Redação dada pelo Decreto nº 12.599, de 2025)

Art. 5º O Plenário, órgão superior de deliberação do CONARQ, se reunirá, em caráter or-dinário, uma vez a cada quatro meses e, em caráter extraordinário, mediante convocação do Presidente ou requerimento de dois terços de seus membros. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 1º O CONARQ funcionará vinculado ao Arquivo Nacional. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 2º As reuniões do CONARQ serão realizadas preferencialmente por meio de videoconfe-rência. (Redação dada pelo Decreto nº 10.148, de 2019)

Art. 6º O quórum de reunião do CONARQ é de maioria absoluta dos membros e o quórum de aprovação é de maioria simples. (Redação dada pelo Decreto nº 10.148, de 2019)

Parágrafo único. Além do voto ordinário, o Presidente do CONARQ terá o voto de qualidade em caso de empate. (Incluído pelo Decreto nº 10.148, de 2019)

Art. 7º O CONARQ poderá instituir subcolegiados nos formatos de grupos de trabalho ou câmaras técnicas consultivas temporárias, com a finalidade de auxiliar o Conselho a elaborar estudos e propostas normativas, de modo a apresentar soluções para questões referentes à implementação da política nacional de arquivos e ao funcionamento do SINAR. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 1º Os subcolegiados: (Redação dada pelo Decreto nº 12.599, de 2025)

I. serão instituídos e compostos na forma de ato do CONARQ; (Incluído pelo Decreto nº 12.599, de 2025)

II. serão compostos por, no máximo, sete membros; (Incluído pelo Decreto nº 12.599, de 2025)

III. estarão limitados a, no máximo, sete em operação simultânea; e (Incluído pelo Decreto nº 12.599, de 2025)

IV. terão caráter temporário e duração não superior a um ano. (Incluído pelo Decreto nº 12.599, de 2025)

§ 2º O CONARQ poderá convidar especialistas de outros órgãos e entidades para compor os subcolegiados. (Redação dada pelo Decreto nº 12.599, de 2025)

Art. 7º- A Fica instituída a Câmara Técnica de Avaliação de Arquivos Privados e Comunitários, no âmbito do CONARQ, como subcolegiado e de caráter permanente, à qual compete: (Redação dada pelo Decreto nº 12.599, de 2025)

I. receber as propostas de declaração de interesse público e social de acervos privados e comunitários e instruir o processo de avaliação; (Redação dada pelo Decreto nº 12.599, de 2025)

II. convidar especialistas para análise dos acervos privados e comunitários, quando neces-sário; (Redação dada pelo Decreto nº 12.599, de 2025)

III. emitir parecer conclusivo sobre o interesse público e social dos acervos privados e co-munitários para apreciação do Plenário do CONARQ; e (Redação dada pelo Decreto nº 12.599, de 2025)

IV. subsidiar o monitoramento dos acervos declarados como de interesse público e social pelo Poder Executivo federal. (Incluído pelo Decreto nº 10.148, de 2019)

§ 1º Para fins do disposto neste Decreto, consideram-se: (Redação dada pelo Decreto nº 12.599, de 2025)

I. arquivos privados - os conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, nos termos do disposto no art. 11 da Lei nº 8.159, de 8 de janeiro de 1991; e (Incluído pelo Decreto nº 12.599, de 2025)

II. arquivos comunitários - os conjuntos de documentos produzidos, recebidos, acumulados e organizados por coletividades no exercício de suas atividades, e as instituições formadas por essas coletividades para custodiar, preservar e promover o acesso a esses acervos, com o objetivo de afirmar suas memórias, identidades e trajetórias sociais. (Incluído pelo Decreto nº 12.599, de 2025)

§ 2º A Comissão de Avaliação de Acervos Privados e Comunitários terá de três a cinco membros e respectivos suplentes, nos termos do disposto em ato do CONARQ. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 3º Os membros da Comissão de Avaliação de Acervos Privados e Comunitários e os res-pectivos suplentes, incluído o seu Presidente: (Redação dada pelo Decreto nº 12.599, de 2025)

I. poderão ser conselheiros do CONARQ ou especialistas convidados; e (Incluído pelo Decreto nº 12.599, de 2025)

II. serão designados pelo Presidente do CONARQ, ad referendum do Conselho. (Incluído pelo Decreto nº 12.599, de 2025)

§ 4º A Comissão de Avaliação de Acervos Privados e Comunitários se reunirá, em cará-ter ordinário, mediante solicitação para análise de acervo privado ou comunitário e, em cará-ter extraordinário, mediante convocação de seu Presidente ou solicitação de seus membros. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 5º O quórum de reunião da Comissão de Avaliação de Acervos Privados e Comunitários é de maioria absoluta e o quórum de aprovação é de maioria simples. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 6º Na hipótese de empate, além do voto ordinário, o Presidente da Comissão de Avaliação de Acervos Privados e Comunitários terá o voto de qualidade. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 7º A Secretaria-Executiva da Comissão de Avaliação de Acervos Privados e Comunitários será exercida pelo Arquivo Nacional. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 8º Os membros da Comissão de Avaliação de Acervos Privados e Comunitários se reuni-rão, preferencialmente, por meio de videoconferência. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 9º A participação na Comissão de Avaliação de Acervos Privados e Comunitários será considerada prestação de serviço público relevante, não remunerada." (NR)

Art. 8º-A A participação no CONARQ será considerada prestação de serviço público rele-vante, não remunerada. (Incluído pelo Decreto nº 12.599, de 2025)

Art. 9º A aprovação do regimento interno do CONARQ é de competência da Ministra de Es-tado da Gestão e da Inovação em Serviços Públicos. (Redação dada pelo Decreto nº 12.599, de 2025)

CAPÍTULO II
DO SISTEMA NACIONAL DE ARQUIVOS

Art. 10. O SINAR tem por finalidade implementar a política nacional de arquivos públicos e privados, visando à gestão, à preservação e ao acesso aos documentos de arquivo.

Art. 11. O SINAR tem como órgão central o CONARQ.

Art. 12. Integram o SINAR:

I. o Arquivo Nacional;

II. os arquivos do Poder Executivo Federal;

III. os arquivos do Poder Legislativo Federal;

IV. os arquivos do Poder Judiciário Federal;

V. os arquivos estaduais dos Poderes Executivo, Legislativo e Judiciário;

VI. os arquivos municipais dos Poderes Executivo e Legislativo; e (Redação dada pelo Decreto nº 12.599, de 2025)

VII. os arquivos pessoais, privados e comunitários cadastrados no CONARQ, nos termos do disposto no § 2º. (Redação dada pelo Decreto nº 12.599, de 2025)

§ 1º Os arquivos referidos nos incisos II a VII, quando organizados sistemicamente, passam a integrar o SINAR por intermédio de seus órgãos centrais.

§ 2º As pessoas físicas e jurídicas de direito privado, detentoras de arquivos pessoais, privados e comunitários, poderão integrar o SINAR mediante cadastro no CONARQ. (Redação dada pelo Decreto nº 12.599, de 2025)

Art. 13. Compete aos integrantes do SINAR:

I. promover a gestão, a preservação e o acesso às informações e aos documentos na sua esfera de competência, em conformidade com as diretrizes e normas emanadas do órgão central;

II. disseminar, em sua área de atuação, as diretrizes e normas estabelecidas pelo órgão central, zelando pelo seu cumprimento;

III. implementar a racionalização das atividades arquivísticas, de forma a garantir a integri-dade do

ciclo documental;

IV. garantir a guarda e o acesso aos documentos de valor permanente;

V. apresentar sugestões ao CONARQ para o aprimoramento do SINAR;

VI. prestar informações sobre suas atividades ao CONARQ;

VII. apresentar subsídios ao CONARQ para a elaboração de dispositivos legais necessários ao aperfeiçoamento e à implementação da política nacional de arquivos públicos e privados;

VIII. promover a integração e a modernização dos arquivos em sua esfera de atuação;

IX. propor ao CONARQ os arquivos privados que possam ser considerados de interesse público e social;

X. comunicar ao CONARQ, para as devidas providências, atos lesivos ao patrimônio arqui-vístico nacional;

XI. colaborar na elaboração de cadastro nacional de arquivos públicos e privados, bem como no desenvolvimento de atividades censitárias referentes a arquivos;

XII. possibilitar a participação de especialistas de órgãos e entidades, públicos e privados, nas câmaras técnicas e na Comissão de Avaliação de Acervos Privados; e (Redação dada pelo Decreto nº 12.599, de 2025)

XIII. proporcionar aperfeiçoamento e reciclagem aos técnicos da área de arquivo, garantindo constante atualização.

Art. 14. Os integrantes do SINAR seguirão as diretrizes e normas emanadas do CONARQ, sem prejuízo de sua subordinação e vinculação administrativa.

CAPÍTULO III
DOS DOCUMENTOS PÚBLICOS

Art. 15. São arquivos públicos os conjuntos de documentos:

I. produzidos e recebidos por órgãos e entidades públicas federais, estaduais, do Distriton Federal e municipais, em decorrência de suas funções administrativas, legislativas e judiciárias;

II. produzidos e recebidos por agentes do Poder Público, no exercício de seu cargo ou fun-ção ou deles decorrente;

III. produzidos e recebidos pelas empresas públicas e pelas sociedades de economia mista;

IV. produzidos e recebidos pelas Organizações Sociais, definidas como tal pela Lei no 9.637, de 15 de maio de 1998, e pelo Serviço Social Autônomo Associação das Pioneiras Sociais, ins-tituído pela Lei no 8.246, de 22 de outubro de 1991.

Parágrafo único. A sujeição dos entes referidos no inciso IV às normas arquivísticas do CONARQ constará dos Contratos de Gestão com o Poder Público.

Art. 16. Às pessoas físicas e jurídicas mencionadas no art. 15 compete a responsabilidade pela

preservação adequada dos documentos produzidos e recebidos no exercício de atividades públicas.

Art. 17. Os documentos públicos de valor permanente, que integram o acervo arquivístico das empresas em processo de desestatização, parcial ou total, serão recolhidos a instituições arquivísticas públicas, na sua esfera de competência.

§ 1º O recolhimento de que trata este artigo constituirá cláusula específica de edital nos processos de desestatização.

§ 2º Para efeito do disposto neste artigo, as empresas, antes de concluído o processo de desestatização, providenciarão, em conformidade com as normas arquivísticas emanadas do CONARQ, a identificação, classificação e avaliação do acervo arquivístico.

§ 3º Os documentos de valor permanente poderão ficar sob a guarda das empresas men-cionadas no § 2o, enquanto necessários ao desempenho de suas atividades, conforme disposto em instrução expedida pelo CONARQ.

§ 4º Os documentos de que trata o *caput* são inalienáveis e não são sujeitos a usucapião, nos termos do art. 10 da Lei no 8.159, de 1991.

§ 5º A utilização e o recolhimento dos documentos públicos de valor permanente que in-tegram o acervo arquivístico das empresas públicas e das sociedades de economia mista já desestatizadas obedecerão às instruções do CONARQ sobre a matéria.

CAPÍTULO IV
DA GESTÃO DE DOCUMENTOS
DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Seção II
Da Entrada de Documentos Arquivísticos Públicos no Arquivo Nacional

Art. 19. Os documentos arquivísticos públicos de âmbito federal, ao serem transferidos ou recolhidos ao Arquivo Nacional, deverão estar avaliados, organizados, higienizados e acondi-cionados, bem como acompanhados de instrumento descritivo que permita sua identificação e controle.

Parágrafo único. As atividades técnicas referidas no *caput*, que precedem à transferência ou ao recolhimento de documentos, serão implementadas e custeadas pelos órgãos e entidades geradores dos arquivos.

Art. 20. Após nomeação dos inventariantes, liquidantes ou administradores de acervos para órgãos e entidades extintos, o Ministério da Economia solicitará ao Ministro de Estado da Justiça e Segurança Pública a assistência técnica do Arquivo Nacional para a orientação necessária à preservação e à destinação do patrimônio documental acumulado, nos termos do disposto nº§ 2º do art. 7º da Lei nº 8.159, de 1991. (Redação dada pelo Decreto nº 10.148, de 2019)

Art. 21. O Ministro de Estado da Justiça e Segurança Pública, mediante proposta do Arquivo Nacional, editará instrução a respeito dos procedimentos a serem observados pelos órgãos e pelas entidades da administração pública federal, para a execução das medidas constantes desta Seção. (Redação dada pelo Decreto nº 10.148, de 2019)

CAPÍTULO V
DA DECLARAÇÃO DE INTERESSE PÚBLICO E SOCIAL DE ARQUIVOS PRIVADOS

Art. 22. Os arquivos privados de pessoas físicas ou jurídicas que contenham documen-tos relevantes para a história, a cultura e o desenvolvimento nacional podem ser declarados de interesse público e social por ato do Ministro de Estado da Justiça e Segurança Pública.(Redação dada pelo Decreto nº 10.148, de 2019)

§ 1o A declaração de interesse público e social de que trata este artigo não implica a transferência do respectivo acervo para guarda em instituição arquivística pública, nem exclui a responsabilidade por parte de seus detentores pela guarda e a preservação do acervo.

§ 2o São automaticamente considerados documentos privados de interesse público e social:

I. os arquivos e documentos privados tombados pelo Poder Público;

II. os arquivos presidenciais, de acordo com o art. 3º da Lei no 8.394, de 30 de dezembro de 1991;

III. os registros civis de arquivos de entidades religiosas produzidos anteriormente à vigên-cia da Lei nº 3.071, de 1o de janeiro de 1916, de acordo com o art. 16 da Lei no 8.159, de 1991.

Art. 23. A Comissão de Avaliação de Acervos Privados, por iniciativa própria ou mediante provocação, encaminhará solicitação relativa à declaração de interesse público e social de ar-quivos privados, acompanhada de parecer, para deliberação do Conselho Nacional de Arquivos. (Redação dada pelo Decreto nº 10.148, de 2019)

§ 1º O parecer será instruído com avaliação técnica da Comissão de Avaliação de Acervos Privados de que trata o art. 7º-A.(Redação dada pelo Decreto nº 10.148, de 2019)

§ 2º Da decisão do CONARQ caberá recurso ao Ministro de Estado da Justiça e Segurança Pública, na forma prevista na Lei nº 9.784, de 29 de janeiro de 1999. (Redação dada pelo Decreto nº 10.148, de 2019)

Art. 24. O proprietário ou detentor de arquivo privado declarado de interesse público e social deverá comunicar previamente ao CONARQ a transferência do local de guarda do arquivo ou de quaisquer de seus documentos, dentro do território nacional.

Art. 25. A alienação de arquivos privados declarados de interesse público e social deve ser precedida de notificação à União, titular do direito de preferência, para que manifeste, no prazo máximo de sessenta dias, interesse na aquisição, na forma do *Parágrafo único* do art. 13 da Lei nº 8.159, de 1991.

Art. 26. Os proprietários ou detentores de arquivos privados declarados de interesse público e social devem manter preservados os acervos sob sua custódia, ficando sujeito à responsa-bilidade penal, civil e administrativa, na forma da legislação em vigor, aquele que desfigurar ou destruir documentos de valor permanente.

Art. 27. Os proprietários ou detentores de arquivos privados declarados de interesse público e social poderão firmar acordos ou ajustes com o CONARQ ou com outras instituições, objeti-vando o apoio para o desenvolvimento de atividades relacionadas à organização, preservação e divulgação do acervo.

Art. 28. A perda acidental, total ou parcial, de arquivos privados declarados de interesse público e social ou de quaisquer de seus documentos deverá ser comunicada ao CONARQ, por seus proprietários ou detentores.

CAPÍTULO VI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 29. Este Decreto aplica-se também aos documentos eletrônicos, nos termos da lei.

Art. 30. O Ministro de Estado da Justiça e Segurança Pública poderá editar normas com-plementares à execução do disposto neste Decreto. (Redação dada pelo Decreto nº 10.148, de 2019)

Art. 32. Este Decreto entra em vigor na data de sua publicação.Art. 33. Ficam revogados os Decretos nos 1.173, de 29 de junho de 1994, 1.461, de 25 de abril de 1995, 2.182, de 20 de março de 1997, e 2.942, de 18 de janeiro de 1999.

Brasília, 3 de janeiro de 2002; 181o da Independência e 114o da República.

FERNANDO HENRIQUE CARDOSO

Silvano Gianni

Este texto não substitui o publicado no DOU 4.1.2002

DECRETO Nº 7.724, DE 16 DE MAIO DE 2012

VERSÃO PUBLICADA

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, observa-dos 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 infor-mação;

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 identificá-vel, relativa à intimidade, vida privada, honra e imagem;

VI. tratamento da informação - conjunto de ações referentes à produção, recepção, clas-sificação, 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, recebidaou modificada por determinado indivíduo, equipamento ou sistema;

IX. integridade - qualidade da informação não modificada, inclusive quanto à origem, trânsitoe 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 docu-mentos, 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 autar-quias, 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 empre-sarial 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 ser-viços no mercado de capitais, comercial, profissional, industrial e segredo de justiça; e

II. às informações referentes a projetos de pesquisa e desenvolvimento científicos ou tec-nológicos 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 8 º 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 L ei nº 12.527, 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 finan-ceira 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, incluídos os auxílios, as ajudas de custo, os jetons e outras vantagens pecuni-árias, além dos proventos de aposentadoria e das pensões daqueles servidores e empregados públicos que estiverem na ativa, de maneira individualizada, conforme estabelecido em ato do Ministro de Estado da Economia;

(Redação dada pelo Decreto nº 9.690, de 2019).

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 a rt. 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 De-creto nº 8.408, de 2015)

§ 4º As informações poderão ser disponibilizadas por meio de ferramenta de redireciona-mento 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 a rt. 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 publi-cação e divulgação de informações previstas na legislação.

§ 8º Ato conjunto dos Ministros de Estado da Controladoria-Geral da União e da Economia disporá sobre a divulgação dos programas de que trata o inciso IX do § 3º , que será feita, ob-servado o disposto no Capítulo VII: (Redação dada pelo Decreto nº 9.690, de 2019)

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

II. por meio de informações consolidadas disponibilizadas no sítio eletrônico do Ministério da Economia; e (Redação dada pelo Decreto nº 9.690, de 2019)

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

IV. Art. 8º Os sítios eletrônicos dos órgãos e das entidades, em cumprimento às normas estabe-lecidas pelo Ministério da Economia, atenderão aos seguintes requisitos, entre outros. (Redação dada pelo Decreto nº 9.690, de 2019)

V. conter formulário para pedido de acesso à informação;

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

VII. 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;

VIII. possibilitar acesso automatizado por sistemas externos em formatos abertos, estruturados e

legíveis por máquina;

IX. divulgar em detalhes os formatos utilizados para estruturação da informação; VI - garantir autenticidade e integridade das informações disponíveis para acesso;

X. indicar instruções que permitam ao requerente comunicar-se, por via eletrônica ou te-lefônica, com o órgão ou entidade; e

XI. 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 pedi-

III. dos de acesso à informação.

IV. *Parágrafo único*. Compete ao SIC:

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

VI. 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

VII. o encaminhamento do pedido recebido e registrado à unidade responsável pelo forne-cimento 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 rece-bimento 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 proto-colo 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 II

Do Pedido 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, comcertificação de que confere com o original.

§ 4º Na impossibilidade de obtenção de cópia de que trata o § 3º , o requerente poderá so-licitar 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 jus-tificativa 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 ór-gão 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.

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 se-gurança 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 tec-nológico, 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 estran-geiras e seus familiares; ou

IX. comprometer atividades de inteligência, de investigação ou de fiscalização em anda-mento, 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 inte-resse

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 Repú-blica, 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 autar-quias, 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 exer-çam 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. (Repristinado pelo Decreto nº 9.716, de 2019)

§ 2º O dirigente máximo do órgão ou entidade poderá delegar a competência para classi-ficação no grau reservado a agente público que exerça função de direção, comando ou chefia. (Repristinado pelo Decreto nº 9.716, de 2019)

§ 3º É vedada a subdelegação da competência de que trata o § 2º . (Repristinado pelo De-creto nº 9.716, de 2019)

§ 4º Os agentes públicos referidos no § 2º deverão dar ciência do ato de classificação à autoridade delegante, no prazo de noventa dias. (Repristinado pelo Decreto nº 9.716, de 2019)

§ 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;-

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

III. 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 pra-ticada 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 cre-denciadas 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 1ºde 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 IV
DA TRANSPARÊNCIA PASSIVA

Art. 46. A Comissão Mista de Reavaliação de Informações, instituída nos termos do § 1º do art. 35 da Lei nº12.527, de 18 de novembro 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 da Justiça e Segurança Pública; (Redação dada pelo Decreto nº 9.690, de 2019)

IV. Ministério das Relações Exteriores;

V. Ministério da Defesa;

VI. Ministério da Economia; (Redação dada pelo Decreto nº 9.690, de 2019)

VII. Ministério da Mulher, da Família e dos Direitos Humanos; (Redação dada pelo Decreto nº 9.690, de 2019)

VIII. Gabinete de Segurança Institucional da Presidência da República ; (Redação dada pelo Decreto nº 9.690, de 2019)

IX. Advocacia-Geral da União; e (Redação dada pelo Decreto nº 9.690, de 2019)

X. Controladoria-Geral da União. (Redação dada pelo Decreto nº 9.690, de 2019)

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 ultrasse-creto ou secreto ou sua reavaliação, no máximo a cada quatro anos;

II. requisitar da autoridade que classificar informação no grau ultrassecreto ou secreto es-clarecimento 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, a 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 9.690, de 2019)

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 Co-missão 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 classifi-cada no grau ultrassecreto deverá ser apreciado, impreterivelmente, em até três sessões sub-sequentes 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 pre-vistos 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-Execu-tiva 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 deti-das pelos órgãos e entidades:

I. terão acesso restrito a agentes públicos legalmente autorizados e a pessoa a que se refe-rirem, 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. I - comprovação do consentimento expresso de que trata o inciso II do *caput* do art. 55, por meio de procuração;

II. 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.

Parágrafo único . As entidades com personalidade jurídica de direito privado constituídas sob a forma de serviço social autônomo, destinatárias de contribuições, são diretamente responsáveis por fornecer as informações referentes à parcela dos recursos provenientes das contribuições e dos demais recursos públicos recebidos. (Redação dada pelo Decreto nº 9.781, de 2019) (Vigência)

Art. 64 - A . As entidades com personalidade jurídica de direito privado constituídas sob a forma de serviço social autônomo, destinatárias de contribuições, divulgarão, independentemente de requerimento, as informações de interesse coletivo ou geral por elas produzidas ou custodiadas,

inclusive aquelas a que se referem os incisos I ao VIII do § 3º do art. 7º, em local de fácil visualização em sítios oficiais na internet. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

§ 1º A publicidade a que estão submetidas as entidades citadas no *caput* refere-se à parcela dos recursos provenientes das contribuições e dos demais recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

§ 2º A divulgação das informações previstas no *caput* não exclui outras hipóteses de publicação e divulgação de informações previstas na legislação, inclusive na Lei de Diretrizes Orçamentárias. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

§ 3º A divulgação de informações atenderá ao disposto no § 1º do art. 7º e no art. 8º. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

Art. 64 - B . As entidades com personalidade jurídica de direito privado constituídas sob a forma de serviço social autônomo, destinatárias de contribuições, também deverão criar SIC, observado o disposto nos arts. 9º ao art. 24. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

Parágrafo único. A reclamação de que trata o art. 22 será encaminhada à autoridade máxima da entidade solicitada. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

Art. 64 - C . As entidades com personalidade jurídica de direito privado constituídas sob a forma de serviço social autônomo, destinatárias de contribuições, estarão sujeitas às sanções e aos procedimentos de que trata o art. 66, hipótese em que a aplicação da sanção de declaração de inidoneidade é de competência exclusiva da autoridade máxima do órgão ou da entidade da administração pública responsável por sua supervisão. (Incluído pelo Decreto nº 9.781, de 2019) (Vigência)

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 L ei 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 nº 12.527, de 2011.

Art. 69. Compete à Controladoria-Geral da União e ao Ministério da Economia, observadas as competências dos demais órgãos e entidades e as previsões específicas deste Decreto, por meio de ato conjunto: (Redação dada pelo Decreto nº 9.690, de 2019)

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, promo-vendo 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 ul-trassecreto 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 início 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

Este texto não substitui o publicado no DOU de 16.5.2012 - Edição extra e retificado em 18.5.2012

ANEXO GRAU DE SIGILO

(Redação dada pelo Decreto nº 11.527, de 2023)

<table>
<tr><td colspan="3">TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO - TCI</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">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">ASSUNTO DA INFORMAÇÃO CLASSIDICADA:</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

VERSÃO PUBLICADA

Regulamenta procedimentos para credencia-mento 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. 1 º 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, desenvol-vido 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 infor-mação 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, respon-sável 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 infor-mação 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 clas-sificada;

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

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

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

Art. 4º (Revogado pelo Decreto nº 9.832, de 2019)

Art. 5º Compete ao Comitê Gestor da Segurança da Informação instituído pelo Decreto nº 9.637, de 26 de dezembro de 2018 : (Redação dada pelo Decreto nº 9.832, de 2019)

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 decorren-tes 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 trata-dos, 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 exe-cução 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 condi-cionada 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;

V. aprovação em inspeção para habilitação de segurança.

Art. 12. A concessão de credencial de segurança a uma pessoa fica condicionada aos se-guintes

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 nacio-nal 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 conhe-çam 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 compro-meter 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 se-guintes 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 infor-mação 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 se-guintes 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 re-metente, 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 somen-te será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.

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

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

§ 1º Para manutenção e arquivamento de informação classificada no grau de sigilo ultrasse-creto 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 trata-mento 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 trans-mitirá 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 hierarquica-mente superior com igual prerrogativa.

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

Art. 34. Caso a preparação, impressão ou reprodução de informação classificada em qual-quer grau de sigilo for efetuada em tipografia, impressora, oficina gráfica ou similar, essa opera-ção 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 qual-quer 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 infor-mação 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.

§ 4 º Os sistemas de informação de que trata o *caput* deverão manter controle e registro dosacessos 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 infor-mação 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 Repú-blica 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 opera-ções 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 re-lativa 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 transmis-são 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, armaze-nagem 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 pro-tocolo 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:

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

I. possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

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

III. 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;

IV. obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

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

VI. Art. 49. Aos órgãos e entidades públicas com que os contratantes mantêm vínculo de qual-quer natureza caberá adotar procedimentos de segurança da informação classificada em qual-quer 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 re-classificação 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, exclusiva-mente, 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 al-goritmo 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 Segu-rança 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

Este texto não substitui o publicado no DOU de 16.11.2012

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

d) classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

e) 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 NUMÉRICO
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 12.572, DE 4 DE AGOSTO DE 2025

VERSÃO PUBLICADA

Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal.

O PRESIDENTE 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 nº12.527, de 18 de novembro de 2011, e na Lei nº 13.709, de 14 de agosto de 2018,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política Nacional de Segurança da Informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no País.

Art. 2º Para fins do disposto neste Decreto, a segurança da informação abrange a segurança:

I. dos dados, dos ativos de informação e dos processos organizacionais;

II. do ambiente físico e eletrônico que contenha ativos de informação; e

III. do pessoal envolvido no ciclo de vida da informação.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º São princípios da Política Nacional de Segurança da Informação:

I. a soberania nacional e a priorização dos interesses nacionais;

II. a responsabilidade do poder público na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;

III. a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a privacidade e o acesso à informação, ressalvadas as hipóteses de sigilo previstas em lei;

IV. a educação como instrumento para o desenvolvimento da cultura de segurança da informação;

V. a atuação colaborativa entre os órgãos e as entidades da administração pública federal; e

VI. o foco na gestão de riscos.

CAPÍTULO III
DOS OBJETIVOS

Art. 4º São objetivos da Política Nacional de Segurança da Informação:

I - contribuir para a segurança da informação, observados os direitos e as garantias fundamentais, especialmente em relação:

a) à proteção de dados pessoais, observada a legislação específica;

b) à segurança dos dados custodiados por órgãos e entidades públicos federais e entidades privadas prestadoras de serviços públicos; e

c) à gestão e à proteção adequadas do conhecimento sensível e das informações com restrição de acesso;

II - salvaguardar as infraestruturas críticas e os serviços essenciais;

III - estimular a gestão de riscos, a proteção e o controle da informação;

IV - incentivar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;

V - aprimorar continuamente o arcabouço normativo relacionado à segurança da informação;

VI - incentivar a qualificação dos recursos humanos necessários à segurança da informação, com a promoção da inclusão e da diversidade;

VII - fortalecer a cultura e a educação em segurança da informação na sociedade;

VIII - construir uma rede abrangente, colaborativa, sistêmica e interoperacional relacionada à segurança da informação; e

IX - desenvolver a cooperação internacional em segurança da informação.

CAPÍTULO IV
DA ESTRUTURA DE GOVERNANÇA

Art. 5º O Gabinete de Segurança Institucional da Presidência da República coordenará as ações do Governo federal relativas à segurança da informação.

Art. 6º O Gabinete de Segurança Institucional instituirá, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, o Comitê Gestor da Segurança da Informação, com a finalidade de acompanhar a implementação e a evolução da Política Nacional de Segurança da Informação.

Parágrafo único. O Comitê Gestor da Segurança da Informação será composto pelos gestores de segurança da informação dos órgãos e das entidades da administração pública federal.

CAPÍTULO V
DOS INSTRUMENTOS

Art. 7 São instrumentos da Política Nacional de Segurança da Informação:

I - a Estratégia Nacional de Segurança da Informação;

II - o Plano Nacional de Segurança da Informação; e

III - os normativos sobre segurança da informação editados pelo Gabinete de Segurança Institucional.

CAPÍTULO VI
DAS COMPETÊNCIAS

Art. 8 Competem ao Gabinete de Segurança Institucional os seguintes temas relacionados à segurança da informação:

I - coordenar as atividades de segurança da informação e das comunicações, inclusive quanto à formulação de políticas públicas;

II - elaborar diretrizes, estratégias, planos, normativos, requisitos metodológicos e recomendações;

III - promover programas destinados à formação e à qualificação de recursos humanos;

IV - coordenar e realizar ações destinadas à promoção da cultura de segurança da informação;

V - acompanhar a evolução tecnológica e as melhores práticas, em âmbito nacional e internacional; e

VI - estimular a cooperação internacional, em coordenação com o Ministério das Relações Exteriores.

Art. 9 Compete ao Sistema de Controle Interno do Poder Executivo Federal auditar a execução das ações da Política Nacional de Segurança da Informação de responsabilidade dos órgãos

e das entidades da administração pública federal.

Art. 10 Compete aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação:

I - implementar a Política Nacional de Segurança da Informação;

II - instituir comitê interno de segurança da informação ou estrutura equivalente;

III - designar o gestor de segurança da informação;

IV - elaborar, publicar, implementar e revisar regularmente suas políticas de segurança da informação e suas normas internas de segurança da informação, observados os normativos sobre segurança da informação editados pelo Gabinete de Segurança Institucional;

V - estimular ações de conscientização e de capacitação de pessoas que atuem nos órgãos e nas entidades da administração pública federal em temas relacionados à segurança da informação;

VI - realizar a avaliação de conformidade com as normas relativas à segurança da informação;

VII - aplicar as ações corretivas e administrativas cabíveis nos casos de violação de sua política de segurança da informação, nos termos do disposto neste Decreto e na legislação;

VIII - coordenar as atividades desenvolvidas pelo gestor de segurança da informação, pelo encarregado pelo tratamento de dados pessoais, pelo gestor de segurança e credenciamento e pelo titular da unidade de tecnologia da informação;

IX - assegurar a transmissão do conhecimento e das responsabilidades por ocasião da substituição do gestor de segurança da informação; e

X - planejar e destinar recursos orçamentários para ações de segurança da informação.

Parágrafo único. Ao órgão de que trata o inciso II do caput compete propor a elaboração e as revisões da política de segurança da informação e das normas internas de segurança da informação do seu órgão ou da sua entidade.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 11 O Ministro de Estado Chefe do Gabinete de Segurança Institucional poderá editar atos complementares necessários à aplicação do disposto neste Decreto.

Art. 12. Ficam revogados:

I – o Decreto nº 9.637, de 26 de dezembro de 2018;

II – o art. 1º do Decreto nº 9.832, de 12 de junho de 2019;

III – o Decreto nº 10.641, de 2 de março de 2021; e

IV – o Decreto nº 10.849, de 28 de outubro de 2021.

Art. 13 Este Decreto entra em vigor na data de sua publicação.

Brasília, 4 de agosto de 2025; 204º da Independência e 137º da República.

LUIZ INÁCIO LULA DA SILVA
Marcos Antonio Amaro dos Santos

Este texto não substitui o publicado no DOU de 5.8.2025.

INSTRUÇÃO NORMATIVA GSI/PR Nº 2, DE 5 DE FEVEREIRO DE 2013.

VERSÃO PUBLICADA

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 classi-ficada, em conformidade com os Artigos 36 e 37 da Lei nº 12.527, de 2011, Decreto 7.724, de 2012 e Decreto 7.845, de 2012.

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

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

II. Controle de acesso à informação classificada: realizado através de credencial de segu-rança e demonstração da necessidade de conhecer;

III. Credencial de Segurança: certificado que autoriza pessoa para o tratamento de infor-mação 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 qual-quer 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 adicio-nais 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 públi-cas, 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 requi-sitos indispensáveis para a concessão da credencial de segurança à pessoas naturais, para o tratamento de informação classificada;

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

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

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

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

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

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

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

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

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

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

V. realizar inspeção e investigação para Credenciamento de Segurança necessária à exe-cução 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 credencia-mento 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 internacio-nais, observadas as competências do Ministério das Relações Exteriores.

X. acompanhar averiguações e processos de avaliação e recuperação dos danos decor-rentes 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 informa-ção classificada;

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

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

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

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

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

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;

III. encaminhar, periodicamente, ao Órgão de Registro que o credenciou relatórios de suas atividades;

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

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

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo à pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto no 7.845, de 2012, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei.

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

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

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

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

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

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

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

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

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

Art. 17 Cabe ao Gestor de Segurança e Credenciamento:

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

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

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

IV. a proposição à Alta Administração de normas no âmbito do órgão ou entidade com a qual

mantém vínculo, para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos;

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

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

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

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

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

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

Art. 19 A fiscalização prevista no inciso VI do art. 3o do Decreto no 7.845, de 2012, será realizada por intermédio de visitas técnicas de equipe do NSC, quando se fizer necessário, bem como, por acompanhamento dos relatórios de conformidade a esta Instrução Normativa e respectivas Normas Complementares, que serão periodicamente enviados pelos Órgãos de Registro e Postos de Controle ao NSC.

Art. 20 Cabe a Alta Administração dos órgãos de registro prever recurso orçamentário específico para o custeio das inspeções, investigações, apoios e visitas técnicas, determinadas nos incisos V do art. 3o, IV do art. 7 º e art. 8 º 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

INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 06 DE MARÇO DE 2013

VERSÃO PUBLICADA

Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA - GSI/PR, no uso de suas atribuições;

CONSIDERANDO:

- o disposto nos incisos II do art. 37 da Lei n° 12.527, de 18 de novembro de 2011;
- o disposto no Decreto n° 3.505, de 13 de junho de 2000;
- o disposto no inciso II do *caput* do art. 70 do Decreto n° 7.724, de 16 de maio de 2012;
- o disposto no art. 40 e seu *Parágrafo único* e no art. 56 do Decreto n° 7.845, de 14 de novembro de 2012;
- o disposto na Instrução Normativa GSI/PR n° 1, de 13 de junho de 2008;
- o disposto na Norma Complementar - NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 fevereiro de 2013; e
- a necessidade de orientar a condução de políticas de segurança da informação classificada, já existentes, ou a serem implementadas pelos órgãos e entidades do Poder Executivo Federal;

RESOLVE:

Art. 1° Estabelecer, no âmbito do Poder Executivo Federal, os parâmetros e padrões mínimos para recursos criptográficos baseados em algoritmos de Estado, que deverão ser implementados, pelos órgãos e entidades, na criptografia da informação classificada, em qualquer grau de sigilo.

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

I. Agente Responsável: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade do Poder Executivo Federal e possuidor de credencial de segurança;

II. 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;

III. Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração

IV. ou decifração;

V. Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis por pessoas não

autorizadas a conhecê-la;

VI. Credencial de Segurança: certificado que autoriza pessoa para o tratamento da informa-ção classificada;

VII. Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

VIII. Gestor de Segurança da Informação e Comunicações: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade do Poder Executivo Federal;

IX. 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, classificada como ultrassecreta, secreta ou reservada; e

X. Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

Art. 3° A Alta Administração dos órgãos e entidades do Poder Executivo Federal, sob pena de responsabilidade, deverá, no âmbito de sua competência, assegurar a implementação e utilização dos parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado, para criptografia da informação classificada, em qualquer grau de sigilo;

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem seguir o disposto nesta Instrução Normativa e na legislação vigente, sob pena de responsabilidade.

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

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

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

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

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

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

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

I. solicitar, quando se fizer necessário, apoio técnico ao GSI/PR, referente ao uso de recurso

criptográfico baseado em algoritmo de Estado, para o cumprimento da legislação pertinente;

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

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

IV. prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente Instrução Normativa, sem prejuízo da legislação vigente;

V. garantir o previsto no art. 41 do Decreto n° 7.845, de 14 de novembro de 2012, e encaminhar relatório anual ao GSI/PR, conforme previsto no item 5.6.3 da NC 09/IN01/DSIC/GSI/ PR (Revisão 01), de fevereiro de 2013;

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

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

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

Art. 8° O GSI/PR prestará apoio técnico, previsto no art. 56 do Decreto n° 7.845, de 14 de novembro de 2012, devendo os órgãos e entidades do Poder Executivo Federal formalizarem a demanda junto ao GSI/PR no prazo de até cento e oitenta dias, conforme previsto no item 5.9.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013.

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

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

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

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

JOSÉ ELITO CARVALHO SIQUEIRA

VERSÃO PUBLICADA

Dispõe sobre os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 87, *Parágrafo único*, inciso II, da Constituição, e tendo em vista o disposto na Lei nº 12.527, de 18 de novembro de 2011; no art. 8º,*caput*, inci-sos IV e V, da Lei nº 14.600, de 19 de junho de 2023; no art. 6º, *caput*, inciso I, do Decreto nº 7.845, de 14de novembro de 2012; no art. 8º, *caput*, inciso II, do Decreto nº 12.572, de 4 de agosto de 2025;

RESOLVE:

Art. 1º Ficam dispostos os requisitos mínimos de segurança da informação para tratamento deinformação classifi cada em computação em nuvem.

Art. 2º Para os fins desta Instrução Normativa, entende-se como nuvem para tratamento de informação classificada a infraestrutura de computação em nuvem privada ou comunitária gerida exclusivamente por órgãos de registro ou por empresas habilitadas como postos de controle.

CAPÍTULO I
DOS REQUISITOS PARA TRATAMENTO DE INFORMAÇÃO CLASSIFICADA EM COMPUTAÇÃO EM NUVEM

Art. 3º O tratamento de informação classificada em computação em nuvem deverá observar os seguintes requisitos, além dos previstos nos arts. 10 a 19 da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021:

I. utilizar procedimentos de segmentação de rede, baseados em arquiteturas e técnicas adequadas ao ambiente computacional e aos riscos associados, para isolar os ambientes de processamento e armazenamento de informações classificadas;

II. utilizar tecnologias de virtualização com certificações de segurança que garantam o isolamento entre as máquinas virtuais alocadas a cada órgão de registro que utilize o serviço;

III. caso sejam utilizados contêineres, possuir mecanismos que possibilitem implementar controles de isolamento, além de ferramentas de segurança específicas para contêineres;

IV. criptografar todas as informações classificadas em grau de sigilo, tanto as arquivadas ou armazenadas quanto aquelas em transporte ou transmissão, utilizando-se algoritmos de Estado;

V. garantir que as chaves criptográficas sejam gerenciadas exclusivamente pelos órgãos de registro;

VI. implementar um processo de gestão de backup e recuperação de dados, realizando os backups criptografados em infraestrutura local, com garantia de recuperação em caso de desastre;

VII. exigir a utilização de autenticação multifatorial para todos os acessos aos sistemas que armazenam ou processam informações classificadas;

VIII. implementar políticas e controles de acesso que garantam que somente pessoal credenciado e com necessidade de conhecer poderá acessar as informações classificadas;

IX. realizar o registro detalhado e imutável de todos os acessos ao ambiente de nuvem para tratamento de informação classificada, especialmente, mas não limitado a, contas administrativas, contas de usuários, contas de aplicativos e contas de serviço, com auditorias periódicas conduzidas por equipe independente;

X. implementar mecanismos automatizados de alertas para atividades suspeitas;

XI. utilizar sistema centralizado de gestão de identidades, permissões e revogação de acessos com governança completa do ciclo de vida, desde a criação até a desativação, com o registro de todas as operações realizadas;

XII. implementar a gestão do controle de acesso, utilizando tanto o modelo de controle de acesso com base em papéis (role-based access control - RBAC) como o modelo de controle de acesso com base em atributos (attribute-based access control- ABAC), de acordo com a necessidade, com revisão, no mínimo, a cada seis meses; e

XIII. implementar controles técnicos e administrativos que impeçam o acesso do provedor de nuvem ao conteúdo das informações.

Art. 4º As informações classificadas em grau de sigilo reservado ou secreto e seus documentos preparatórios deverão ser transitados em redes localizadas exclusivamente em território nacional, preferencialmente em infraestruturas tecnológicas sob controle direto de órgãos da administração pública federal, direta e indireta, bem como de empresas públicas.

§ 1º É permitido o trânsito da informação de que trata o *caput* fora do território nacional,- mediante uso de meios criptográficos compatíveis com o grau de sigilo, exclusivamente nas seguintes hipóteses:

I. comunicações com representantes diplomáticos, consulares ou de adidâncias de órgãos de registro; e

II. em demais missões oficiais, mediante autorização da alta administração do órgão de registro.

§ 2º O trânsito de dados de que trata o *caput* e o § 1º somente poderá ocorrer em redes que permitam, no mínimo, a aplicação de mecanismos de rastreabilidade, registro e monitoração integral de todos os pacotes de dados recebidos e enviados, e incluam, no mínimo, metadados de origem, destino, horário, tamanho e protocolo utilizado.

§ 3º A implementação dos mecanismos previstos no § 2º é de responsabilidade do provedor do

serviço de nuvem, devendo estar prevista em contrato, garantindo-se o acesso irrestrito aos logs pela equipe de segurança do órgão de registro contratante.

Art. 5º As informações classificadas em grau de sigilo reservado ou secreto e seus documentos preparatórios deverão ser armazenados e processados em datacenters localizados exclusivamente em território nacional, preferencialmente em infraestruturas tecnológicas sob controle direto de órgãos da administração pública federal, direta e indireta, bem como de empresas públicas, observadas as disposições constantes dos tratados e convenções internacionais de que o Brasil seja signatário.

Parágrafo único. É vedada replicação ou backup das informações de que trata o *caput* fora do território nacional, bem como a execução de qualquer outra ação que resulte na saída de informações do território nacional.

Art. 6º As informações classificadas em grau de sigilo ultrassecreto e seus documentos preparatórios não poderão ser tratados em computação em nuvem.

CAPÍTULO II
DOS REQUISITOS MÍNIMOS PARA PROVEDOR DE SERVIÇO DE NUVEMPARA TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Art. 7º O provedor de serviço de nuvem para tratamento de informação classifica cada, além de observar os requisitos previstos nos arts. 10 e 11 do Decreto nº 7.845, de 14 de novembro de 2012, e no art.20 da Instrução Normativa nº 5, de 30 de agosto de 2021, do Gabinete de Segurança Institucional da Presidência da República, deverá, no mínimo:

I. estar estabelecido no Brasil, ter situação cadastral ativa e ter como principal atividade econômica provimento de serviços de tecnologia da informação;

II. possuir certificação vigente nas seguintes normas:

a) ABNT NBR ISO/IEC 27001;

b) ABNT NBR ISO/IEC 27017;

c) ABNT NBR ISO/IEC 27018;

d) ABNT NBR ISO/IEC 27701; e

e) ABNT NBR ISO/IEC 22237;

III. demonstrar que todos os recursos físicos necessários, tais como servidores, equipamentos de armazenamento, equipamentos de rede e outros, estão localizados em data centers em território nacional;

IV. disponibilizar infraestrutura física dedicada, sem compartilhamento com clientes ou entidades não autorizados pelo órgão de registro contratante;

V. disponibilizar infraestrutura projetada para alta disponibilidade, com redundância e planos de recuperação de desastres;

VI. possuir mecanismos capazes de implementar medidas para proteger os dados armazénados contra acessos não autorizados por parte de ameaças persistentes avançadas;

VII. demonstrar ser capaz de atender aos requisitos previstos no art. 3º; e

VIII. providenciar, junto ao órgão de registro contratante, o credenciamento de segurança de pessoas físicas com acesso à infraestrutura.

IX. *Parágrafo único*. Auditoria técnica do órgão de registro contratante avaliará o cumprimento dos requisitos de que trata o *caput*, especialmente os previstos nos incisos III e VII.

Art. 8º O provedor de serviço de nuvem para tratamento de informação classificada deverá ser habilitado como órgão de registro ou posto de controle nos termos dos arts. 10 e 11 do Decreto nº 7.845, de14 de novembro de 2012.

Parágrafo único. O Gabinete de Segurança Institucional da Presidência da República poderá realizar a habilitação de que trata o *caput* dos órgãos e entidades vinculados a outros Ministérios não habilitados como órgãos de registro nível 1, desde que haja anuência expressa do respetivo Ministro de Estado.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 9º Compete aos órgãos de registro contratantes de serviços de nuvem para tratamento de informação classificada, além dos requisitos previstos na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021:

I. estabelecer contrato sigiloso para a prestação de serviços de nuvem para tratamento de informação classificada, nos termos do art. 48 do Decreto nº 7.845, de 14 de novembro de 2012, com expressa previsão de que a contratada deverá observar as disposições desta Instrução Normativa;

II. monitorar e auditar, no mínimo anualmente, o cumprimento das normas de segurança pelo provedor de serviço de nuvem para tratamento de informação classificada, com definição prévia de escopo técnico mínimo, periodicidade e critérios de conformidade;

III. realizar o credenciamento de segurança, conforme a legislação vigente, de todas as pessoas que tenham necessidade de acessar e operar a infraestrutura de nuvem para tratamento de informação classificada;

IV. capacitar periodicamente equipe de pessoal com acesso às informações classificadas, com conteúdo atualizado sobre proteção de dados, segurança da informação e incidentes cibernéticos;

V. apurar eventual infração nos casos de suspeita de descumprimento, por parte da contratada, de qualquer dispositivo do contrato previsto no inciso I ou das normas de segurança da informação classificada; e

VI. adotar imediatamente as ações necessárias nos casos de suspeita de comprometimento de

segurança, o que poderá incluir a suspensão do acesso às informações armazenadas ou processadas pelo provedor.

Art. 10. Compete ao provedor de serviço em nuvem para tratamento de informação classificada:

I. garantir a conformidade com as normas e padrões de segurança estabelecidos nesta Instrução Normativa;

II. fornecer ao órgão de registro contratante relatório, no mínimo anual, sobre a segurança das informações classificadas sob sua guarda, contemplando, no mínimo, aspectos de segurança cibernética, segurança de rede, segurança de nuvem, segurança de aplicações e segurança de dados;

III. cooperar com as autoridades competentes em investigações relacionadas a incidentes de segurança;

IV. preservar e entregar os indícios e evidências relacionadas a incidentes de segurança,-quando necessário à apuração de ilícitos penais, cíveis ou administrativos; e

V. impedir que pessoas não autorizadas pelo órgão de registro contratante tenham acesso aos recursos e instalações onde estão armazenadas as informações classificadas.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 11. A Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, passa a vigorar com a seguinte alteração:

"Art. 17 .....

.....

II –informação classificada em grau de sigilo e seus documentos preparatórios poderão ser tratados em ambiente de computação em nuvem nos termos da regulamentação específica; e

. ....." (NR)

Art. 12. Esta Instrução Normativa entra em vigor na data de sua publicação.

MARCOS ANTONIO AMARO DOS SANTOS

VERSÃO PUBLICADA

Homologa a Revisão 02 da Norma Complementar nº 09/IN01/DSIC/GSIPR.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso de suas atribuições, resolve:

Art. 1º Fica homologada a Norma Complementar nº 01/ IN02/NSC/GSI/PR que disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas, no âmbito do Poder Executivo Federal.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

JOSÉ ELITO CARVALHO SIQUEIRA

DISCIPLINA O CREDENCIAMENTO DE SEGURANÇA DE PESSOAS NATURAIS, ÓRGÃOS E ENTIDADES PÚBLICAS E PRIVADAS PARA O TRATAMENTO DE INFORMAÇÕES CLASSIFICADAS

ORIGEM

Núcleo de Segurança e Credenciamento.

REFERÊNCIA NORMATIVA

- Lei nº 12.527, de 18 de novembro de 2011; Decreto nº 7.724, de 16 de maio de 2012;
- Decreto nº 7.845, de 14 de novembro de 2012;
- Instrução Normativa GSI/PR nº 01 , de 13 de junho de 2008; Instrução Normativa GSI/PR nº 02 , de 5 de fevereiro de 2013; Instrução Normativa GSI/PR nº 03, de 06 de março de 2013;
- Norma Complementar nº 07/IN01/DSIC/GSIPR, de 06 de maio de 2010; Norma Complementar nº 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012;
- Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01), de 15 de fevereiro de 2013; e Norma Complementar nº 09/IN01/DSIC/GSIPR (Revisão 01), de 15 de fevereiro de 2013.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito do Poder Executivo Federal.

SUMÁRIO

5. Credenciamento de segurança de pessoas naturais
6. Habilitação de segurança de Órgão de Registro Nível 1
7. Habilitação de segurança de Órgão de Registro Nível 2
8. Habilitação de segurança de Posto de Controle de Órgão ou Entidade Pública
9. Habilitação de Segurança de Entidade Privada
10. Descredenciamento
11. Responsabilidades
12. Vigência
13. Anexos

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR

Diretor do Departamento de Segurança da Informação e Comunicações

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, prioritariamente, 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 ano 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 76 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,
b) sabotagem e espionagem;
c) situação fiscal;
d) dados relacionados à situação criminal, cível e administrativa; e
e) 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 administração 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.

7.4.5. 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.

13. ANEXOS

A - Formulário Individual de Dados para Credenciamento - FIDC.

B - Modelo de Certificado de Credencial de Segurança.

ANEXO A

INFORMAÇÃO PESSOAL ACESSO RESTRITO

(QUANDO PREENCHIDO)

FORMULÁRIO INDIVIDUAL DE DADOS PARA CREDENCIAMENTO - FIDC

Ministério/Secretaria/Órgão/Autarquia

INSTRUÇÕES PARA O PREENCHIMENTO:

- Responda de forma precisa às questões apresentadas;
- Preferencialmente digite os dados diretamente no Formulário ou preencha o mesmo **em letra de forma** com **caneta azul ou preta**;
- Se não tiver resposta a dar a alguma(s) questão(ões), escreva a expressão **"NADA A RELATAR "**;
- Os dados informados serão tratados como informações pessoais;
- **Rubricar** todas as folhas e **Assinar a Última.**
- **Poderá ser Assinada Eletrônicamente**, desde que se possa conferir a autenticidade do documento e, neste caso, é dispensado a sua rubrica.

Foto 3x4
(atual)
Rosto frontal e fundo branco.
Digitalizada ou não.

1. DADOS PESSOAIS:

Nome completo:

Data de nascimento: / /

Local de nascimento: - UF: - País: - Nacionalidade(s):

Estado Civil:

Documento de identificação nº: - Tipo: [ ] Civil [ ] Militar

Órgão Expedidor: Data de expedição: / / - Local de expedição: –

UF:

Identidade Funcional nº: Órgão: - SIGEP nº:

Cadastro de Pessoas Físicas (CPF) nº: - Cadastro INSS nº:

Título de Eleitor nº: - Zona: - Seção:

Carteira Nacional de Habilitação nº: Emissão: / / - UF:

Passaporte nº: - País Emissor: Validade: / /

Passaporte Oficial nº: - País Emissor: Validade: / /

2. DADOS DE RESIDÊNCIA HABITUAL:

Endereço:

CEP: - Cidade: – UF: – País:

Telefones residenciais: ( )

Telefones celulares: ( )

Telefones funcionais: ( )

E-mails:

E-mails funcional:

---

3. DADOS PROFISSIONAIS:

Cargo/Função/Emprego:

Órgão/Empresa:

Endereço:

CEP - Cidade: - UF: - País:

Data de admissão: / /

---

4. DADOS DO PAI:

Nome completo:

Data de nascimento: / / - Cadastro de Pessoas Físicas (CPF) nº:

Local de nascimento: - UF: - País - Nacionalidade(s):

Endereço:

CEP - Cidade: - UF: - País: Convive atualmente: Sim [ ] Não [ ]

---

5. DADOS DA MÃE:

Nome completo:

Data de nascimento: / / - Cadastro de Pessoas Físicas (CPF) nº:

Local de nascimento: - UF: - País - Nacionalidade(s):

Endereço:

CEP - Cidade: - UF: - País: Convive atualmente: Sim [ ] Não [ ]

---

6. DADOS DO CÔNJUGE OU COMPANHEIRO(A):

Nome completo:

Data de nascimento: / / - Cadastro de Pessoas Físicas (CPF) nº:

Local de nascimento: - UF: - País - Nacionalidade(s):

Endereço:

CEP - Cidade: - UF: - País:

Convive atualmente: Sim [ ] Não [ ]

---

7. RESIDÊNCIAS ANTERIORES (Endereços residenciais do solicitante nos últimos dez anos):

Desde	Até	Endereço - Cidade – UF – CEP – País

---

8. VIAGENS: SE VISITOU ALGUM PAÍS ESTRANGEIRO NOS ÚLTIMOS 10 ANOS, PREENCHA O QUADRO ABAIXO:

Data		País	Motivo
Início	Fim		

---

9. PESSOAS DE SEU CONVÍVIO QUE TENHAM RESIDIDO NO EXTERIOR POR MAIS DE DOIS ANOS, NOS ÚLTIMOS DEZ ANOS:

Nome	De/Até	País	Motivo

10. POSSUI ALGUMA ENFERMIDADE? Sim [ ] Não [ ]

10.1 CASO POSITIVO, QUAL?

_____

_____

11. FAZ USO DE ALGUM MEDICAMENTO CONTROLADO? Sim [ ] Não [ ]

11.1 CASO POSITIVO, RELACIONE :

_____

_____

12. FORMAÇÃO PROFISSIONAL (Relacionar os cursos realizados após o ensino médio):

Data de conclusão	Instituição e País	Título

13. DADOS SOBRE EMPREGOS ANTERIORES (Relacionar os empregos anteriores ao que está sendo exercido atualmente):

Período	Empresa ou entidade	Endereço	Cargo/Emprego

14. RELAÇÕES INTERNACIONAIS (Relatar se manteve relações com governos estrangeiros, organismos ou programas internacionais esclarecendo as funções desempenhadas ou tipo de relação mantida):

Organismo/Programa	Tipo de relação e período	País

15. REFERÊNCIAS PESSOAIS:

Nome	Telefones com DDD

16. OBSERVAÇÕES FINAIS (Relate qualquer fato que julgue necessário e oportuno para o processo de credenciamento):

_____

_____

_____

_____

17. DECLARAÇÃO PESSOAL:

B. Eu, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx, devidamente qualificado no item 1 (um) deste Formulário, **declaro para os fins deste Credenciamento de Segurança, que**:

C.

A. Tudo que foi manifestado por mim, neste questionário, é pura expressão da verdade;

D. Reconheço que qualquer falsidade declarada (por omissão, engano, inexatidão ou tergiversação de algum dado) será motivo para negação ou anulação da Credencial de Segurança, sem prejuízo de outras responsabilidades;

C. Comprometo-me a comunicar imediatamente ao Órgão de Registro credenciador, durante a Investigação de Segurança ou durante o período de validade da Credencial de Segurança, qualquer alteração posterior dos dados assinalados neste questionário;

D. Conheço a legislação em vigor e as normas relacionadas à Segurança da Informação, especialmente, aquelas relativas à Informação Classificada;

E. Tenho ciência de que o tratamento de dados pessoais a ser realizado neste formulário e no Processo de Credenciamento de Segurança, para concessão de Credencial de Segurança para o Tratamento de informações Classificada, não é abrangido pela Lei nº 13.709, de 14 de agosto de 2018, Lei

de Proteção de Dados (LGPD), conforme prevê o inciso III, letras “a”, “b”, “c” e “d” do seu art. 4º.

F. A partir dos dados deste formulário, atendendo ao prescrito no inciso II do art. 55 do Decreto nº 7.724, de 16 de maio de 2012, autorizo a Investigação de Segurança para Credenciamento de Segurança sobre minha pessoa, a fim de verificar se existe algum registro que possa indicar risco à Segurança da Informação, em especial às Informações Classificadas;

G. Aceito a condição de ser ou não aprovado na Investigação de Segurança, reconhecendo que o meu Credenciamento, para o Tratamento de Informação Classificada, dependerá desse resultado.

Local - UF, _____ de _____ de _____.

_____

Nome: **Xxxxxxxxxxx xxxxxxxxxxx**

ANEXO B

Material de Acesso Restrito Art. 45 Dec. nº 7845/2012 (Quando preenchido)

MODELO DE CERTIFICADO DE CREDENCIAL DE SEGURANÇA (CCS)

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade expedidora)

CERTIFICADO DE CREDENCIAL DE SEGURANÇA Nº XXX/201X.

CERTIFICO que o Sr.(a)___, identidade nº , emitida em / / pelo(a) , vinculado aos quadros do(a) (Órgão ou entidade de vínculo do credenciado), onde exerce o cargo/função de (Cargo ou função do credenciado), está credenciado para o tratamento de informações classificadas no grau (em letra maiúscula, entre aspas e em vermelho: "ULTRASSECRETO" ou "SECRETO"ou "RESERVADO"), para (Descrição sucinta da finalidade para qual se destina a Credencial).

Esta Credencial de Segurança é válida até___de____de____.

,_____de____de____.

(Local) (Data)

Selo Nacional

(Assinatura e carimbo da Autoridade responsável pelo Credenciamento)

Material de Acesso Restrito

Art. 45 Dec.nº 7845/2012

(Quando preenchido)

(Quando preenchido)

Nome:	
Nº da Credencial:	
RG/Idt:	
CPF:	
Órgão de Vínculo:	
Cargo/Função:	
Finalidade:	
Data da Expedição:	
Validade:	
Autoridade Emitente:	
Observações:	

Material de Acesso Restrito

Art. 45 Dec.nº 7845/2012

(Quando preenchido)

PORTARIA Nº 23, DE 15 JULHO DE 2014

VERSÃO PUBLICADA

Homologa a Revisão 02 da Norma Complementar nº 09/IN01/DSIC/GSIPR.

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

Art. 1º Fica homologada a Revisão 02 da Norma Complementar nº 09/IN01/DSIC/GSIPR que estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

JOSÉ ELITO CARVALHO SIQUEIRA

ORIENTAÇÕES ESPECÍFICAS PARA O USO DE RECURSOS CRIPTOGRÁFICOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- Lei nº 12.527, de 18 de novembro de 2011
- Decreto nº 3.505, de 13 de junho de 2000
- Decreto nº 7.724, de 16 de maio de 2012
- Decreto nº 7.845, de 14 de novembro de 2012
- Instrução Normativa GSI nº 01 de 13 de junho de 2008 e suas respectivas Normas Complementares publicadas no DOU pelo DSIC/GSIPR.

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

5. Orientações Específicas

6. Controle

7. Dispositivos Transitórios

8. Vigência

9. Anexos A e B

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR

Diretor do Departamento de Segurança da Informação e Comunicações

1. OBJETIVO

Normatizar o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma complementar, aplicam-se os seguintes termos e definições:

2.1. Agente Responsável: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da APF, direta ou indireta, possuidor de credencial de segurança;

2.2. Algoritmo de Estado: função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável;

2.3. Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

2.4. Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

2.5. Credencial de Segurança: certificado que autoriza pessoa para o tratamento de informação classificada;

2.6. Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

2.7. Empresa Estratégica de Defesa (EED) do setor de Tecnologia de Informação e Comunicação (TIC): toda pessoa jurídica do setor de Tecnologia de Informação e Comunicação (TIC) devidamente credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das condições previstas no inciso IV do art. 2º da Lei nº 12.598, de 22 de março de 2012.

2.8. Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de

segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

2.9. 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, classificada como ultrassecreta, secreta ou reservada;

2.10. Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria;

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

2.12. Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Com fulcro no previsto pelo inciso II do art. 3º da Instrução Normativa nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República – GSI/PR, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas defi-nindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da APF, direta e indireta.

4. RESPONSABILIDADES

4.1. A Alta Administração dos órgãos e entidades da APF, direta e indireta, é responsável:

4.1.1. Pela utilização dos recursos criptográficos para a segurança das informações, principalmente as sigilosas, em conformidade com esta norma;

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

4.1.3. Por prever recurso orçamentário para o uso de recursos criptográficos, conforme necessidade de cada órgão ou entidade.

4.2. O Gestor de Segurança da Informação e Comunicações dos órgãos e entidades da APF, direta e indireta, é responsável pela implementação dos procedimentos relativos ao uso de recursos criptográficos, em conformidade com as orientações contidas nesta norma e deve possuir credencial de segurança; e,

4.3. Todo Agente Responsável usuário de recurso criptográfico é encarregado pela sua operação e sigilo, deve possuir credencial de segurança e assinar o respectivo Termo de Uso de Recursos Criptográficos, conforme modelo constante no Anexo A.

5. ORIENTAÇÕES ESPECÍFICAS

Para fins de utilização de recursos criptográficos pelos órgãos e entidades da APF, direta e

indireta, além da legislação aplicável, deverão ser observados os seguintes procedimentos:

5.1. Algoritmo de Estado:

5.1.1. Toda a informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deverá obrigatoriamente ser protegida com recurso criptográfico baseado em algoritmo de Estado.

5.1.2. A cifração e decifração de informações classificadas, em qualquer grau de sigilo, utilizará exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos no Anexo B desta norma.

5.1.3. O transporte e a recepção de documento com informação classificada em grau de sigilo ultrassecreto serão efetuados pessoalmente por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia previsto no Anexo B, vedada sua postagem.

5.1.4. O canal de comunicação seguro (Rede Privada Virtual - VPN) que interligue redes dos órgãos e entidades da APF, direta e indireta, objetivando a troca de informações classificadas, deve utilizar recurso criptográfico baseado em algoritmo de Estado.

5.1.5. A utilização de recurso criptográfico, baseado em algoritmo de Estado, para cifração e decifração das informações não classificadas é opcional.

5.1.6. O Agente Responsável pela cifração ou decifração, no exercício do cargo, função, emprego ou atividade, utilizará recurso criptográfico baseado em algoritmo adotado pelo órgão ao qual está vinculado;

5.1.7. O uso de recurso criptográfico baseado em algoritmo de Estado é restrito ao Agente Responsável e requer treinamento e credenciamento de segurança, sob responsabilidade dos órgãos e entidades da APF, direta e indireta;

5.1.8. O credenciamento de estrangeiros para uso de recurso criptográfico baseado em algoritmo de Estado deve ser submetido ao GSI/PR;

5.1.9. O GSI/PR é o órgão responsável pelo apoio técnico no tocante a atividades de caráter científico e tecnológico relacionadas ao recurso criptográfico baseado em algoritmo de Estado.

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

5.1.11. Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.1.10 poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:

a) seja uma Empresa Estratégica de Defesa do setor de Tecnologia de Informação e Comunicação e utilize tecnologia nacional, não sendo aceito empresas que apenas forneçam recursos criptográficos com tecnologia estrangeira;

b) seja realizado exclusivamente por meio de Contrato Sigiloso, nos termos dos arts. 48 e

49 do Decreto no 7.845, de 14 de novembro de 2012; e

c) seja previsto em cláusula contratual que fica vedado ao contratado os direitos de propriedade e de exploração comercial do recurso criptográfico com algoritmo de Estado objeto do referido contrato.

5.1.12. O não cumprimento do previsto no item 5.1.10 ou nas letras a, b e c do item 5.1.11, poderá gerar responsabilidade administrativa, civil e penal, conforme legislação vigente.

5.1.13. A Alta Administração dos órgãos e entidades da APF deverá prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente norma, sem prejuízo da legislação vigente.

5.1.14. Além do disposto nesta norma, os recursos criptográficos baseados em algoritmo de Estado podem ser objeto de regulamentação específica.

5.2. Algoritmo Registrado:

5.2.1. A cifração e decifração das informações sigilosas não classificadas deve utilizar recurso criptográfico, no mínimo, baseado em algoritmo registrado, desde que atendidas obrigatoriamente as seguintes condições:

a) O desenvolvimento ou obtenção do algoritmo registrado deverá ser realizado levando-se em consideração a necessidade de proteção da informação sigilosa, bem como as possíveis ameaças à sua exposição, cabendo tal responsabilidade a alta administração do órgão que o empregará; e

b) O algoritmo deverá ser registrado no GSI/PR, que manterá sob sua guarda e controle o

c) banco de registros;

d) O órgão deverá manter sob sua guarda o código fonte e método de processos do algoritmo, bem como implementar os controles adequados, inclusive quanto à auditoria;

5.3. Toda informação sigilosa – classificada ou não –, independente do algoritmo de criptografia utilizado, somente poderá ser armazenada em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal, conforme legislação em vigor.

5.4. É vedado ao Agente Responsável por recurso criptográfico nos órgãos e entidades da APF, direta e indireta:

5.4.1. utilizar recursos criptográficos em desacordo com esta norma, bem como, com a legislação em vigor; e

5.4.2. utilizar recursos criptográficos diferentes dos parâmetros e padrões mínimos definidos pelo órgão ou entidade da APF, direta e indireta, a que pertence.

6. CONTROLE

6.1. Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente.

6.2. A Alta Administração dos órgãos e entidades da APF deverá:

6.2.1. enviar para o GSI/PR relatório de conformidade relativo à aderência a presente norma de todos os recursos criptográficos baseados em algoritmo de Estado sob sua responsabilidade, ao serem adquiridos, quando solicitado e com periodicidade estabelecida por aquele Gabinete;

6.2.2. enviar para o GSI/PR relatório relativo aos procedimentos aplicados no tratamento de informação classificada previstos no art. 41 do Decreto 7.845, de 14 de novembro de 2012, quando solicitado e com periodicidade estabelecida por aquele Gabinete ou, oportunamente, por iniciativa do próprio órgão, quando ocorrer o previsto nos incisos IV e V do mesmo artigo;

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

7. DISPOSITIVOS TRANSITÓRIOS:

7.1. A Alta Administração dos órgãos e entidades da APF, direta e indireta, providenciará a adequação dos recursos criptográficos já em uso, no prazo máximo de 180 dias, contados a partir da publicação do guia técnico de recursos criptográficos previsto no item 7.3;

7.2. Os órgãos e entidades deverão adotar os recursos criptográficos baseados em algoritmo de Estado com parâmetros e padrões de que trata o Anexo B no prazo de um ano a contar da publicação da presente norma;

7.3. O GSI/PR coordenará a elaboração, em 90 (noventa) dias, prorrogáveis por igual período, de um guia técnico de recursos criptográficos como orientações de como proceder para cumprir o previsto no item 5.2.

8. VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

9. ANEXOS

A - Modelo de Termo de Uso de Recurso Criptográfico

B - Padrões mínimos para recurso criptográfico baseado em algoritmo de Estado

ANEXO A

Modelo de Termo de Uso de Recurso Criptográfico

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade da APF)

TERMO DE USO DE RECURSO CRIPTOGRÁFICO

Pelo presente instrumento, eu_____, CPF , identidade__, expedida pelo___, em _____, e lotado no(a)_____deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis e nos termos da_____(legislação vigente) que TENHO conhecimento sobre o uso do recurso criptográfico sob minha responsabilidade, sendo vedado seu uso:

I. para fins diversos dos funcionais ou institucionais;

II. para interceptar ou tentar interceptar transmissão de dados ou informações não destinados ao seu próprio acesso por quaisquer meios;

III. para tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio por quaisquer meios;

IV. para violar ou tentar violar os recursos de segurança dos equipamentos que utilizem recursos criptográficos;

V. para cifração ou decifração de informações ilícitas, entre os quais, materiais obscenos, ofensivos, ilegais, não éticos, ameaças, difamação, injúria, racismo ou quaisquer que venham a causar molestamento, tormento ou danos a terceiros;

VI. de forma inadequada, expondo-o a choques elétricos ou magnéticos, líquidos ou outros fatores que possam vir a causar-lhes danos, incluindo testes de invasão/intrusão/penetração, teste de quebra de senhas, teste de quebra de cifração, e teste de técnicas de invasão e defesa entre outros;

Local, UF,____de_____de_____.

Assinatura

_____

Nome do usuário e seu setor organizacional

ANEXO B

Padrões mínimos para recurso criptográfico baseado em algoritmo de Estado

TABELA I - Tamanho da chave:

Nível de Segurança da Informação	RSA/LD	Curvas Elípticas
Reservado	2048	224
Secreto	3248	256
Ultrassecreto	Não recomendado	Não recomendado

TABELA II - Algoritmos de bloco:

Classificação	Algoritmo	
	Chave	Bloco
Reservado	192	128
Secreto	256	128
Ultrassecreto	Não recomendado	

TABELA III - Algoritmos sequenciais:

Classificação	Algoritmo
Reservado	192
Secreto	256
Ultrassecreto	Não recomendado

TABELA IV – Sistema de Chave Única:

Classificação	Algoritmo
Ultrassecreto	Sequência aleatória

PORTARIA Nº 49, DE 12 DEZEMBRO DE 2014

VERSÃO PUBLICADA

Homologa a Revisão 01 da Norma Complementar nº 20/IN01/DSIC/GSIPR.

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

Art. 1 Fica homologada a Revisão 01 da Norma Complementar nº 20/IN01/DSIC/GSIPR que estabelece Diretrizes de Segurança das Informação e Comunicações (SIC) para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal (APF).

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

JOSÉ ELITO CARVALHO SIQUEIRA

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. Uso e Disseminação: refere-se à utilização, acesso, reprodução, transporte, transmissão e distribuição da informação.

5.3. 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 desclassi-ficada 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 Decretono 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.

PRESIDÊNCIA DA REPÚBLICA

GSI

GABINETE DE SEGURANÇA INSTITUCIONAL

NSC | Núcleo de Segurança e Credenciamento

GABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO DO BRASIL

DO LADO DO POVO BRASILEIRO