Gabinete de Segurança Institucional da Presidência da República

Departamento de Segurança da Informação e Comunicações

Coordenação-Geral do Núcleo de Segurança e Credenciamento

Legislação relacionada

à

Lei do Acesso à Informação

ÍNDICE

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.

Mensagem de veto

Vigência

Regulamento

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. Subordinam-se ao regime desta Lei:

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

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

Art. 2º Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.

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

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

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

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

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

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

V - desenvolvimento do controle social da administração pública.

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

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

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

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

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

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

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

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

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

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

Art. 5º É dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

CAPÍTULO II

DO ACESSO A INFORMAÇÕES E DA SUA DIVULGAÇÃO

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

I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter:

I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;

III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;

IV - informação primária, íntegra, autêntica e atualizada;

V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;

VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e

VII - informação relativa:

a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;

b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

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

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

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

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

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

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

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

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

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

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

III - registros das despesas;

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

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

VI - respostas a perguntas mais frequentes da sociedade.

§ 2º Para cumprimento do disposto no **caput**, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo

obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

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

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

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

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

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

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

VI - manter atualizadas as informações disponíveis para acesso;

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

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

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

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

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

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

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

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

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

CAPÍTULO III

DO PROCEDIMENTO DE ACESSO À INFORMAÇÃO

Seção I

Do Pedido de Acesso

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

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

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

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

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

§ 1º Não sendo possível conceder o acesso imediato, na forma disposta no **caput**, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias:

I - comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;

II - indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou

III - comunicar que não possui a informação, indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

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

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

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

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

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

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

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

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

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

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

Seção II

Dos Recursos

Art. 15. No caso de indeferimento de acesso a informações ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da sua ciência.

Parágrafo único. O recurso será dirigido à autoridade hierarquicamente superior à que exarou a decisão impugnada, que deverá se manifestar no prazo de 5 (cinco) dias.

Art. 16. Negado o acesso a informação pelos órgãos ou entidades do Poder Executivo Federal, o requerente poderá recorrer à Controladoria-Geral da União, que deliberará no prazo de 5 (cinco) dias se:

I - o acesso à informação não classificada como sigilosa for negado;

II - a decisão de negativa de acesso à informação total ou parcialmente classificada como sigilosa não indicar a autoridade classificadora ou a hierarquicamente superior a quem possa ser dirigido pedido de acesso ou desclassificação;

III - os procedimentos de classificação de informação sigilosa estabelecidos nesta Lei não tiverem sido observados; e

IV - estiverem sendo descumpridos prazos ou outros procedimentos previstos nesta Lei.

§ 1º O recurso previsto neste artigo somente poderá ser dirigido à Controladoria-Geral da União depois de submetido à apreciação de pelo menos uma autoridade hierarquicamente superior àquela que exarou a decisão impugnada, que deliberará no prazo de 5 (cinco) dias.

§ 2º Verificada a procedência das razões do recurso, a Controladoria-Geral da União determinará ao órgão ou entidade que adote as providências necessárias para dar cumprimento ao disposto nesta Lei.

§ 3º Negado o acesso à informação pela Controladoria-Geral da União, poderá ser interposto recurso à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35.

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

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

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

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

Art. 19. (VETADO).

§ 1º (VETADO).

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

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

CAPÍTULO IV

DAS RESTRIÇÕES DE ACESSO À INFORMAÇÃO

Seção I

Disposições Gerais

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

Parágrafo único. As informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso.

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

Seção II

Da Classificação da Informação quanto ao Grau e Prazos de Sigilo

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

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

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

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

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

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

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

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

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

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

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

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

II - secreta: 15 (quinze) anos; e

III - reservada: 5 (cinco) anos.

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

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

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

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

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

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

Seção III

Da Proteção e do Controle de Informações Sigilosas

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

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

Seção IV

Dos Procedimentos de Classificação, Reclassificação e Desclassificação

Art. 27. A classificação do sigilo de informações no âmbito da administração pública federal é de competência: (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 de ocultação de ato ilegal cometido por si ou por outrem;

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

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

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

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

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

§ 2º Pelas condutas descritas no **caput**, poderá o militar ou agente público responder, também, por improbidade administrativa, conforme o disposto 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 ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

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

CAPÍTULO VI

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 35. (VETADO).

§ 1º É instituída a Comissão Mista de Reavaliação de Informações, que decidirá, no âmbito da administração pública federal, sobre o tratamento e a classificação de informações sigilosas e terá competência para:

I - requisitar da autoridade que classificar informação como ultrassecreta e secreta esclarecimento ou conteúdo, parcial ou integral da informação;

II - rever a classificação de informações ultrassecretas ou secretas, de ofício ou mediante provocação de pessoa interessada, observado o disposto no art. 7º e demais dispositivos desta Lei; e

III - prorrogar o prazo de sigilo de informação classificada como ultrassecreta, sempre por prazo determinado, enquanto o seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional ou à integridade do território nacional ou grave risco às relações internacionais do País, observado o prazo previsto no § 1º do art. 24.

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

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

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

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

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

DECRETO Nº 7.724, DE 16 DE MAIO DE 2012

Vigência

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

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

DECRETA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Este Decreto regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do **caput** do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO II

DA ABRANGÊNCIA

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

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

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

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

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

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

CAPÍTULO III

DA TRANSPARÊNCIA ATIVA

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

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

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

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

II - barra de identidade do Governo federal, contendo ferramenta de redirecionamento de página para o Portal Brasil e para o sítio principal sobre a Lei 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 financeira detalhada;

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

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

VII - respostas a perguntas mais frequentes da sociedade; e

VIII - contato da autoridade de monitoramento, designada nos termos do art. 40 da Lei nº 12.527, de 2011, e telefone e correio eletrônico do Serviço de Informações ao Cidadão - SIC.

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

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

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

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

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

I - conter formulário para pedido de acesso à informação;

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

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

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

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

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

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

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

CAPÍTULO IV

DA TRANSPARÊNCIA PASSIVA

Seção I

Do Serviço de Informação ao Cidadão

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

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

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

III - receber e registrar pedidos de acesso à informação.

Parágrafo único. Compete ao SIC:

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

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

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

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

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

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

Seção II

Do Pedido de Acesso à Informação

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

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

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

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

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

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

I - nome do requerente;

II - número de documento de identificação válido;

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

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

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

I - genéricos;

II - desproporcionais ou desarrazoados; ou

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

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

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

Seção III

Do Procedimento de Acesso à Informação

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Parágrafo único. A reprodução de documentos ocorrerá no prazo de dez dias, contado da comprovação do pagamento pelo requerente ou da entrega de declaração de pobreza por ele firmada, nos termos da Lei nº 7.115, de 1983, ressalvadas hipóteses justificadas em que, devido ao volume ou ao estado dos documentos, a reprodução demande prazo superior.

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

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

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

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

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

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

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

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

Seção IV

Dos Recursos

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

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

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

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

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

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

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

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

Art. 24. No caso de negativa de acesso à informação, ou às razões da negativa do acesso de que trata o **caput** do art. 21, desprovido o recurso pela Controladoria-Geral da União, o requerente poderá apresentar, no prazo de dez

dias, contado da ciência da decisão, recurso à Comissão Mista de Reavaliação de Informações, observados os procedimentos previstos no Capítulo VI.

CAPÍTULO V

DAS INFORMAÇÕES CLASSIFICADAS EM GRAU DE SIGILO

Seção I

Da Classificação de Informações quanto ao Grau e Prazos de Sigilo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I - grau ultrassecreto: vinte e cinco anos;

II - grau secreto: quinze anos; e

III - grau reservado: cinco anos.

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

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

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

I - no grau ultrassecreto, das seguintes autoridades:

a) Presidente da República;

b) Vice-Presidente da República;

c) Ministros de Estado e autoridades com as mesmas prerrogativas;

d) Comandantes da Marinha, do Exército, da Aeronáutica; e

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

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

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

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

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

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

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

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

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

Seção II

Dos Procedimentos para Classificação de Informação

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

I - código de indexação de documento;

II - grau de sigilo;

III - categoria na qual se enquadra a informação;

IV - tipo de documento;

V - data da produção do documento;

VI - indicação de dispositivo legal que fundamenta a classificação;

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

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

IX - data da classificação; e

X - identificação da autoridade que classificou a informação.

§ 1º O TCI seguirá anexo à informação.

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

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

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

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

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

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

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

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

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

Seção III

Da Desclassificação e Reavaliação da Informação Classificada em Grau de Sigilo

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

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

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

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

III - a permanência das razões da classificação;

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

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

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

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

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

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

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

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

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

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

Seção IV

Disposições Gerais

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

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

Art. 41. As informações sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não

poderão ser objeto de classificação em qualquer grau de sigilo nem ter seu acesso negado.

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

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

Art. 43. O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam credenciadas segundo as normas fixadas pelo Núcleo de Segurança e Credenciamento, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, sem prejuízo das atribuições de agentes públicos autorizados por lei.

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

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

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

I - rol das informações desclassificadas nos últimos doze meses;

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

a) código de indexação de documento;

b) categoria na qual se enquadra a informação;

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

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

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

IV - informações estatísticas agregadas dos requerentes.

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

CAPÍTULO VI

DA COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES CLASSIFICADAS

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

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

II - Ministério da Justiça;

III - Ministério das Relações Exteriores;

IV - Ministério da Defesa;

V - Ministério da Fazenda;

VI - Ministério do Planejamento, Orçamento e Gestão;

VII - Secretaria de Direitos Humanos da Presidência da República;

VIII - Gabinete de Segurança Institucional da Presidência da República;

IX - Advocacia-Geral da União; e

X - Controladoria Geral da União.

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

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

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

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

III - decidir recursos apresentados contra decisão proferida:

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

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

IV - prorrogar por uma única vez, e por período determinado não superior a vinte e cinco anos, o prazo de sigilo de informação classificada no grau ultrassecreto,

enquanto seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional, à integridade do território nacional ou grave risco às relações internacionais do País, limitado ao máximo de cinquenta anos o prazo total da classificação; e

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO VII

DAS INFORMAÇÕES PESSOAIS

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

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

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

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

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

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

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

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

III - ao cumprimento de decisão judicial;

IV - à defesa de direitos humanos de terceiros; ou

V - à proteção do interesse público geral e preponderante.

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

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

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

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

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

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

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

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

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

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

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

II - comprovação das hipóteses previstas no art. 58;

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

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

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

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

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

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

CAPÍTULO VIII

DAS ENTIDADES PRIVADAS SEM FINS LUCRATIVOS

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

I - cópia do estatuto social atualizado da entidade;

II - relação nominal atualizada dos dirigentes da entidade; e

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

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

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

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

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

CAPÍTULO IX

DAS RESPONSABILIDADES

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

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

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

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

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

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

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

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

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

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

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

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

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

I - advertência;

II - multa;

III - rescisão do vínculo com o Poder Público;

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

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

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

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

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

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

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

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

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

CAPÍTULO X

DO MONITORAMENTO DA APLICAÇÃO DA LEI

Seção I

Da Autoridade de Monitoramento

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

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

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

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

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

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

Seção II

Das Competências Relativas ao Monitoramento

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

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

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

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

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

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

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

VII - definir, em conjunto com a Casa Civil da Presidência da República, diretrizes e procedimentos complementares necessários à implementação da Lei nº 12.527, de 2011.

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

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

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

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

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

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

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

CAPÍTULO XI

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

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

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

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

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

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

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

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

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

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

Decreto nº 7.724, de 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

Decreto nº 7.724, de 16 de maio de 2012

ANEXO

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

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

DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012

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

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

DECRETA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

XVIII - tratamento da informação classificada - conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

CAPÍTULO II

DO CREDENCIAMENTO DE SEGURANÇA

Seção I

Dos Órgãos

Art. 3º Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, nos termos do art. 37 da Lei nº12.527, de 2011:

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

II - habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de informação classificada em qualquer grau de sigilo;

III - habilitar entidade privada que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada;

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

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

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

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

I - Gabinete de Segurança Institucional da Presidência da República, que o coordenará;

II - Casa Civil da Presidência da República;

III - Ministério da Justiça;

IV - Ministério das Relações Exteriores;

V - Ministério da Defesa;

VI - Ministério da Ciência, Tecnologia e Inovação;

VII - Ministério do Planejamento, Orçamento e Gestão; e

VIII - Controladoria-Geral da União.

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

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

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

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

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

II - definir parâmetros e requisitos mínimos para:

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

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

III - avaliar periodicamente o cumprimento do disposto neste Decreto.

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

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

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

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

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

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

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

Art. 7º Compete ao órgão de registro nível 1:

I - habilitar órgão de registro nível 2 para credenciar pessoa para o tratamento de informação classificada;

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

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

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

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

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

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

Art. 9º Compete ao posto de controle:

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

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

Seção II

Dos procedimentos

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

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

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

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

I - regularidade fiscal;

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

III - expectativa de assinatura de contrato sigiloso;

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

V - aprovação em inspeção para habilitação de segurança.

Art. 12. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:

I - solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;

II - preenchimento de formulário com dados pessoais e autorização para investigação;

III - aptidão para o tratamento da informação classificada, verificada na investigação; e

IV - declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.

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

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

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

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

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

Art. 16. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo com país ou organização estrangeira, o credenciamento de segurança no território nacional se dará somente se houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil.

CAPÍTULO III

DO TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Seção I

Disposições Gerais

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

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

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

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, constante do Anexo I, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei**.**

Art. 19. A decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo observará os procedimentos previstos nos arts. 31 e 32 do Decreto nº 7.724 de 16 de maio de 2012, e deverá ser formalizada em decisão consubstanciada em Termo de Classificação de Informação.

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

Seção II

Do Documento Controlado

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

I - identificação dos destinatários em protocolo e recibo específicos;

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

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

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

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

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

I - numeração sequencial e data;

II - órgãos produtor e custodiante do DC;

III - rol de documentos controlados; e

IV - local e assinatura.

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

I – numeração sequencial e data;

II - agentes públicos substituto e substituído;

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

IV - local e assinatura.

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

Seção III

Da Marcação

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

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

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

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

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

Seção IV

Da Expedição, Tramitação e Comunicação

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

I - serão acondicionados em envelopes duplos;

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

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

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

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

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

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

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

I - registrar o recebimento do documento;

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

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

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

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

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

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

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

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

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

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

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

Seção V

Da Reprodução

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

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

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

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

Seção VI

Da Preservação e da Guarda

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

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

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

Seção VII

Dos Sistemas de Informação

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

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

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

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

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

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

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

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

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

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

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

III - designação de sistemas criptográficos adequados a cada destinatário;

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

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

Seção VIII

Das Áreas, Instalações e Materiais

Art. 42. As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

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

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

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

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

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

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

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

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

V - recursos criptográficos; e

VI - explosivos, líquidos e gases.

Art. 46. Os órgãos ou entidades públicas encarregadas da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto, prova, produção, aquisição, armazenagem ou emprego de material de acesso

restrito expedirão instruções adicionais necessárias à salvaguarda dos assuntos a eles relacionados.

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

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

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

Seção IX

Da Celebração de Contratos Sigilosos

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

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

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

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

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

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

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

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

CAPÍTULO IV

DA INDEXAÇÃO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

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

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

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

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

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

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

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

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

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

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

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

a) reclassificação da informação resultante de reavaliação; ou

b) primeiro registro da classificação; e

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

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

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

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

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

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

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

Parágrafo único. Até o término do prazo previsto no **caput,** compete ao Gabinete de Segurança Institucional da Presidência da República acompanhar e prestar apoio técnico aos órgãos e entidades quanto à implementação dos recursos criptográficos baseados em algoritmo de Estado.

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

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

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

Art. 60. Ficam revogados:

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

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

Decreto nº 7.845, de 14 de novembro de 2012

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

Decreto nº 7.845, de 14 de novembro de 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 classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

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

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

[Local, data e assinatura]

[Duas testemunhas identificadas]

Decreto nº 7.845, de 14 de novembro de 2012

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.

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

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

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

CONSIDERANDO:

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

RESOLVE:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Art. 6 º Compete ao Posto de Controle:

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

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

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

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

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

Parágrafo único. O acesso à informação classificada em qualquer grau de sigilo à pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 7.845, de 2012, pelo

qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da Lei.

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

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

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

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

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

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

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

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

Art. 15 As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade,

demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

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

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

Art. 17 Cabe ao Gestor de Segurança e Credenciamento:

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

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

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

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

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

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

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

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

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

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

Art. 19 A fiscalização prevista no inciso VI do art. 3º do Decreto nº 7.845, de 2012, será realizada por intermédio de visitas técnicas de equipe do NSC, quando se fizer necessário, bem como, por acompanhamento dos relatórios de conformidade a esta Instrução Normativa e respectivas Normas Complementares,

que serão periodicamente enviados pelos Órgãos de Registro e Postos de Controle ao NSC.

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

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

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

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

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

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

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

JOSÉ ELITO CARVALHO SIQUEIRA

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Núcleo de Segurança e Credenciamento

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 APLICACÃO

Esta Norma Complementar se aplica no âmbito do Poder Executivo Federal.

SUMÁRIO

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 anos, levando-se em consideração as informações contidas no documento de indicação, citadas no item 5.5.1.2 desta Norma.

5.3 A pessoa natural poderá receber credencial de segurança, desde que atendidos ainda os seguintes requisitos:

5.3.1 Solicitação formal por qualquer autoridade referida no art. 9º da Instrução Normativa GSI/PR nº 02, de 2013, ou no § 2º do art. 30 do Decreto nº 7.724, de 2012, ao Gestor de Segurança e Credenciamento do órgão de registro da autoridade solicitante.

5.3.1.1 O Gestor de Segurança e Credenciamento poderá também dar início ao processo de credenciamento das pessoas naturais vinculadas ao seu respectivo órgão de registro, uma vez detectada a necessidade de conhecer.

5.3.1.2 Quando a pessoa natural for de entidade privada, a solicitação formal deverá ser realizada pelo diretor estatutário ou Gestor de Segurança e Credenciamento da mesma, ao GSC do Órgão de Registro Nível 1 com o qual mantenha vínculo de qualquer natureza.

5.3.2 Preenchimento do Formulário Individual de Dados para Credenciamento - FIDC, conforme modelo constante do Anexo A desta Norma, devidamente assinado.

5.3.3 Ser aprovada na investigação para credenciamento pelo órgão de registro com o qual mantenha vínculo de qualquer natureza.

5.4 Quando a necessidade de conhecer estiver relacionada à troca ou tratamento de informação classificada em qualquer grau de sigilo com país ou organização estrangeira, o credenciamento de segurança da pessoa natural somente poderá ser realizado se houver algum tratado, acordo, memorando de entendimentos ou ajuste técnico, específico para troca de informação classificada, firmado entre o país ou organização estrangeira e a República Federativa do Brasil, conforme previsto no art. 16 do Decreto nº 7.845, de 2012.

5.5 O processo de credenciamento de pessoas naturais deverá seguir as seguintes fases:

5.5.1 Fase da indicação

5.5.1.1 A fase de indicação do processo de credenciamento inicia-se com a solicitação formal citada no item 5.3.1 desta Norma, com a identificação por parte da autoridade

indicadora, da pessoa que tem necessidade de conhecer.

5.5.1.2 No documento de indicação deverão constar o grau de acesso à informação classificada pretendido, o documento referido no item 5.3.2 desta Norma, as atividades/funções a serem desenvolvidas pelo indicado que demandem o acesso à informação classificada, o prazo estimado de exercício, bem como a justificativa da autoridade indicadora para a necessidade de conhecer documentos classificados por parte da pessoa a ser credenciada e outras informações julgadas pertinentes.

5.5.1.3 O documento de indicação passa a compor o processo de credenciamento de segurança e será considerado documento pessoal, tratado conforme Seção V, do Capítulo IV, da Lei nº 12.527, de 2011 e Seção IV, do Capítulo III, do Decreto nº 7.845, de 2012.

5.5.1.4 O órgão de registro, de posse da demanda de credenciamento, verificará a conformidade e pertinência do processo e poderá então iniciar a fase de investigação de segurança.

5.5.2 Fase da investigação de segurança

5.5.2.1 A investigação de segurança tem como objetivo identificar o nível do risco potencial de quebra de segurança ao se permitir que a pessoa indicada acesse informação classificada no grau de sigilo indicado.

5.5.2.2 A investigação de segurança deverá ser realizada por órgão ou entidade pública competente para tal, integrante ou não da própria estrutura organizacional do órgão de registro solicitante, observado o disposto no parágrafo único do art. 8º e art. 14 do Decreto nº 7.845, de 2012.

5.5.2.3 De posse do processo de credenciamento encaminhado pelo órgão de registro solicitante, o órgão encarregado da investigação para credenciamento dará início a esta fase após conferir a documentação recebida e constatar a expressa autorização do indicado para realizar a investigação para o credenciamento.

5.5.2.4 O relatório de investigação será anexado ao processo de credenciamento de segurança, também tratado como informação pessoal, no qual constará parecer do responsável técnico, fundamentado no perfil do indicado, por intermédio de análise dos autos da investigação, indicando, em função do nível do risco potencial de quebra de segurança constatado, se o indicado está apto ou não para o credenciamento de segurança no grau solicitado.

5.5.2.5 Os autos e peças componentes da investigação serão realizados por servidor público ocupante de cargo efetivo ou militar de carreira, com competência profissional comprovada para atuar na área de inteligência, por policial ou por perito criminal, ou ainda, por profissionais de saúde, no caso de pareceres técnicos específicos desta área, a critério do responsável pelo relatório da investigação.

5.5.2.6 A investigação deverá avaliar, no mínimo, dados dos seguintes aspectos pessoais do indicado:

a) envolvimento com pessoas ou organizações associadas ao crime, terrorismo, tráfico, sabotagem e espionagem;

b) situação fiscal;

c) dados relacionados à situação criminal, cível e administrativa; e

d) situação eleitoral e do serviço militar.

5.5.2.7 Os autos da investigação deverão ser arquivados no órgão encarregado da investigação e tratados como documento pessoal, conforme Seção V, do Capítulo IV da Lei nº 12.527, de 2011, e Seção IV do Capítulo III do Decreto nº 7.845, de 2012.

5.5.2.8 O Relatório de Investigação - RI deverá ser anexado ao processo de credenciamento e encaminhado ao órgão de registro demandante, sendo tratado como documento pessoal, conforme Seção V do Capítulo IV da Lei nº 12.527, de 2011 e Seção IV do Capítulo III do Decreto nº 7.845, de 2012.

5.5.3 Fase do credenciamento

5.5.3.1 O ato do credenciamento é a homologação da permissão para o tratamento da informação classificada no grau solicitado, contudo, não exime o credenciado das responsabilidades administrativas, cíveis e penais quanto à manutenção da segurança dos ativos de informação classificada tratados, conforme legislação pertinente.

5.5.3.2 A credencial de segurança é concedida pela alta administração do órgão de registro, podendo ser delegado o ato de concessão, a critério da mesma, para o Gestor de Segurança e Credenciamento do órgão de registro, sendo vedada a subdelegação.

5.5.3.3 Com base no RI e em outras informações que se fizerem úteis, o órgão de registro poderá expedir a credencial solicitada, considerando o risco à segurança, o grau de acesso, o tempo de acesso e a necessidade de conhecer.

5.5.3.4 Conforme estabelecido por normatização interna do órgão de registro, a credencial de segurança, poderá ser publicada em ato administrativo do órgão, ou ainda, se necessária a sua materialização, expedida na forma impressa ou eletrônica, sendo neste caso considerada como material de acesso restrito.

5.5.3.5 Quando a atividade do credenciado for externa ao órgão ou entidade ao qual pertence e caso haja exigência de comprovação do credenciamento, poderá ser expedido um Certificado de Credencial de Segurança - CCS, conforme modelo constante do Anexo B a esta Norma, do qual constarão os dados previstos no item 5.5.3.8, com a aplicação do Selo Nacional sobre a assinatura.

5.5.3.6 A credencial de segurança deverá ser numerada em sequência anual, no âmbito do órgão de registro emissor.

5.5.3.7 O órgão de registro deverá informar a concessão da credencial de segurança à autoridade solicitante.

5.5.3.8 A credencial de segurança deverá conter no mínimo os seguintes dados:

a) número da credencial;

b) nome completo, número de registro ou de identidade e número de inscrição no Cadastro de Pessoas Físicas do Ministério da Fazenda (CPF) do credenciado;

c) órgão ou entidade com o qual o credenciado mantém vínculo;

d) cargo ou função do credenciado;

e) grau de acesso à informação classificada (Reservado, Secreto ou Ultrassecreto);

f) finalidade da credencial;

g) data prevista para o término de validade da credencial;

h) data de expedição da credencial; e

i) identificação da autoridade que emitiu a credencial.

5.5.3.9 A credencial de segurança, juntamente com o seu respectivo processo, deverá ser armazenada no órgão de registro que a emitiu, sendo facultativo o uso de ferramentas de

tecnologia da informação para este fim, desde que atendidos os requisitos mínimos de segurança previstos na legislação vigente.

5.6 A credencial de segurança poderá ser renovada ao término de sua validade, desde que obedecido o processo descrito nos itens 5.5.1, 5.5.2 e 5.5.3 da presente norma, sendo vedada a sua prorrogação.

5.6.1 É admitida a antecipação do processo de renovação da credencial de segurança, a critério do órgão de registro, para evitar a descontinuidade do credenciamento com o término de sua validade.

5.7 Os postos de controle deverão manter os registros atualizados de todas as credenciais de segurança emitidas para as pessoas naturais sob sua responsabilidade.

6 HABILITAÇÃO DE SEGURANÇA DE ÓRGÃO DE REGISTRO NÍVEL 1

6.1 A habilitação de segurança será concedida pelo NSC, para os ministérios ou órgãos públicos de nível equivalente que identificarem a necessidade de tratamento de informações classificadas, em qualquer grau de sigilo, mediante demanda a qualquer tempo.

6.2 A alta administração dos ministérios ou dos órgãos públicos de nível equivalente, requisitante da habilitação de segurança, formalizará sua intenção ao Gabinete de Segurança Institucional da Presidência da República – GSI/PR, incluindo a designação do Gestor de Segurança e Credenciamento, bem como seu suplente, conforme inciso II do art. 10 do Decreto nº 7.845, de 2012.

6.3 A designação do Gestor de Segurança e Credenciamento, e respectivo suplente, será considerada como documento de indicação para o credenciamento segurança, no grau ultrassecreto, dos indicados.

6.4 O NSC realizará o primeiro credenciamento de segurança do Gestor de Segurança e Credenciamento, e seu suplente, conforme processo previsto no item 5 desta Norma Complementar.

6.4.1 Os servidores designados para Gestor de Segurança e Credenciamento e suplente deverão encaminhar ao NSC o Formulário Individual de Dados para Credenciamento - FIDC, constante do Anexo A desta Norma, devidamente preenchido e assinado.

6.4.2 Após a habilitação de segurança do ORN1, os Gestores de Segurança e Credenciamento e suplentes subsequentes serão credenciados pelo próprio órgão de registro, conforme estabelecido por normatização interna do órgão e entidade do Poder Executivo Federal, observando a legislação específica em vigor.

6.4.3 A substituição do Gestor de Segurança e Credenciamento dos ORN1, por qualquer motivo, deve ser informada ao NSC, identificando o substituto e seus respectivos dados de contato.

6.5 O NSC informará ao órgão demandante a homologação da credencial de segurança do Gestor de Segurança e Credenciamento e seu suplente.

6.6 O GSC credenciado dará então prosseguimento ao credenciamento de segurança do seu Órgão de Registro Nível 1 solicitando a habilitação do posto de controle de acordo com o item 8 desta Norma

7 HABILITAÇÃO DE SEGURANÇA DE ÓRGÃO DE REGISTRO NÍVEL 2

7.1 A habilitação de segurança será concedida pelo ORN1, para seus órgãos e entidades públicas vinculadas que necessitarem tratar informações classificadas em qualquer grau de sigilo. A habilitação de segurança poderá ser concedida mediante demanda a qualquer tempo do órgão interessado ou por determinação do ORN1, por intermédio do credenciamento de segurança.

7.2 A alta administração do órgão requisitante do credenciamento de segurança formalizará a intenção de habilitação de segurança para a alta administração do ORN1, incluindo a designação do respectivo Gestor de Segurança e Credenciamento e seu suplente, conforme inciso II do art. 10 do Decreto nº 7.845, de 2012, bem como a respectiva categoria de credencial de segurança pretendida para os mesmos.

7.2.1 No caso da determinação de habilitação de segurança como ORN2, a alta 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.

7.5 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.

PESSOAL
(Quando preenchido)
ANEXO A

FORMULÁRIO INDIVIDUAL DE DADOS PARA CREDENCIAMENTO - FIDC

ÓRGÃO DE REGISTRO NÍVEL X

INSTRUÇÕES PARA O PREENCHIMENTO:

- Responda de forma precisa às questões apresentadas;
- Digite os dados diretamente no Formulário ou preencha o mesmo **em letras de forma** com **caneta azul ou preta**;
- Se não tiver resposta a dar a alguma(s) questão(ões), escreva a expressão **"NADA A RELATAR "**; e
- Os dados informados são considerados pessoais.

Foto 3x4
(atual)
Rosto frontal e
fundo branco

1. DADOS PESSOAIS:

Nome completo: _____

Data de nascimento: _____ / _____ / _____

Local de nascimento: _____ **UF:** _____ **País:** _____

Nacionalidades: _____

Estado Civil : _____

Documento de identificação: _____ **Tipo** _____

Data de expedição: _____ **Local de expedição:** _____

Identidade Funcional: _____ **Órgão:** _____

Cadastro de Pessoas Físicas: _____ **Cadastro INSS:** _____

Título de Eleitor: _____ **Zona:** _____ **Seção:** _____

Carteira Nacional de Habilitação: _____ **Emissão:** _____ **UF:** _____

Passaporte Nº: _____ **País Emissor:** _____

2. DADOS DE RESIDÊNCIA HABITUAL:

Endereço: _____

CEP _____ **Cidade** _____ **UF** _____ **País** _____

Telefones residenciais: _____

Telefones celulares: _____

Telefones funcionais:

E-mails: _____

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: _____ / _____ / _____

Local de nascimento: _____ **UF:** _____ **País:** _____

Nacionalidades: _____

Endereço: _____

CEP_____ **Cidade** _____ **UF** _____ **País** _____

Convive atualmente: Sim [ ] Não [ ]

5. DADOS DA MÃE:

Nome completo: _____

Data de nascimento: _____ / _____ / _____

Local de nascimento: _____ **UF:** _____ **País:** _____

Nacionalidades: _____

Endereço: _____

CEP_____ **Cidade** _____ **UF** _____ **País** _____

Convive atualmente: Sim [ ] Não [ ]

6. DADOS DO CÔNJUGE OU COMPANHEIRO(A):

Nome completo: _____

Data de nascimento: _____ / _____ / _____

Local de nascimento: _____ **UF:** _____ **País:** _____

Nacionalidades: _____

Endereço: _____

CEP_____ **Cidade** _____ **UF** _____ **País** _____

Convive atualmente: Sim [ ] Não [ ]

7. RESIDÊNCIAS ANTERIORES (Endereços residenciais do solicitante nos últimos dez anos):

Desde	**Até**	**Endereço:** _____ **CEP**_____ **Cidade** _____ **UF**_____ **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

16. OBSERVAÇÕES FINAIS (Relate qualquer fato que julgue necessário e oportuno para o processo de credenciamento):

_____

_____

_____

_____

17. DECLARAÇÃO PESSOAL:

EU _____ _____,_____

DEVIDAMENTE QUALIFICADO NO ITEM 1 (UM) DESTE FORMULÁRIO, DECLARO PARA OS FINS DESTE CREDENCIAMENTO DE SEGURANÇA, QUE:

A) TUDO QUE FOI MANIFESTADO POR MIM, NESTE QUESTIONÁRIO, É PURA EXPRESSÃO DA VERDADE;

B) 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 CREDENCIADOR, DURANTE A INVESTIGAÇÃO OU DURANTE O PERÍODO DE VALIDADE DA CREDENCIAL DE SEGURANÇA, QUALQUER ALTERAÇÃO POSTERIOR DOS DADOS ASSINALADOS NESTE QUESTIONÁRIO;

D) DECLARO CONHECER A LEGISLAÇÃO EM VIGOR E AS NORMAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, ESPECIALMENTE, AQUELAS RELATIVAS ÀS INFORMAÇÕES CLASSIFICADAS;

E) 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 PARA CREDENCIAMENTO SOBRE MINHA PESSOA, A FIM DE VERIFICAR SE EXISTE ALGUM REGISTRO QUE POSSA INDICAR RISCO À SEGURANÇA DA INFORMAÇÃO, EM ESPECIAL ÀS INFORMAÇÕES CLASSIFICADAS;

F) ACEITO A CONDIÇÃO DE SER OU NÃO APROVADO NA INVESTIGAÇÃO DE SEGURANÇA, RECONHECENDO QUE O MEU CREDENCIAMENTO, PARA TRATAMENTO DE INFORMAÇÕES CLASSIFICADAS, DEPENDERÁ DESSE RESULTADO.

_____,_____ de _____ de _____.

(Local) **(Data)**

_____

(Nome e assinatura do declarante)

Material de Acesso Restrito

(Quando preenchido)

ANEXO B

MODELO DE CERTIFICADO DE CREDENCIAL DE SEGURANÇA - CCS

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade expedidora)

CERTIFICADO DE CREDENCIAL DE SEGURANÇA Nº XXX

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 valida até ____ de _____ de _____.

_____, ____ de _____ de _____.
(Local) (Data)

Selo Nacional inserido conforme item **5.4.3.6** da

(Assinatura e carimbo da Autoridade responsável pelo Credenciamento)

Instrução Normativa GSI/PR nº 3, de 06 de março de 2013.

Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

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 nº 12.527, de 18 de novembro de 2011;
- o disposto no Decreto nº 3.505, de 13 de junho de 2000;
- o disposto no inciso II do *caput* do art. 70 do Decreto nº 7.724, de 16 de maio de 2012;
- o disposto no art. 40 e seu parágrafo único e no art. 56 do Decreto nº 7.845, de 14 de novembro de 2012;
- o disposto na Instrução Normativa GSI/PR nº 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. 1º 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. 2º 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 - **Algorítmo 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 ou decifração;

IV - **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;

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

VI - **Decifração**: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

VII - **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;

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

IX - **Recurso Criptográfico**: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

Art. 3º A Alta Administração dos órgãos e entidades do Poder Executivo Federal, sob pena de responsabilidade, deverá, no âmbito de sua competência, assegurar a implementação e utilização dos parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado, para criptografia da informação classificada, em qualquer grau de sigilo;

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem seguir o disposto nesta Instrução Normativa e na legislação vigente, sob pena de responsabilidade.

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

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

§ 1º Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, 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 nº 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;

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

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

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

II - realizar 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 nº 7.845, de 14 de novembro de 2012, e encaminhar relatório anual ao GSI/PR, conforme previsto no item 5.6.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013;

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

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

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

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

Art. 8º O GSI/PR prestará apoio técnico, previsto no art. 56 do Decreto nº 7.845, de 14 de novembro de 2012, devendo os órgãos e entidades do Poder Executivo Federal formalizarem a demanda junto ao GSI/PR no prazo de até cento e oitenta dias, conforme previsto no item 5.9.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013.

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

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

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem possuir credencial de segurança, ou excepcionalmente, assinar o Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 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

ANEXO

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

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

ORIENTAÇÕES 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 01 de 13 de junho de 2008
Norma Complementar 01/DSIC/GSIPR, de 13 de outubro de 2008
Norma Complementar 02/DSIC/GSIPR, de 13 de outubro de 2008
Norma Complementar 07/DSIC/GSIPR, de 14 de abril de 2010

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

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 RESPONSABILIDADES

2.1 A Alta Administração dos órgãos e entidades da APF, direta e indireta, é responsável pela utilização dos recursos criptográficos para a segurança das informações, principalmente as sigilosas, em conformidade com esta norma;

2.2 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,

2.3 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 I.

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 definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da APF, direta e indireta.

4 TERMOS E DEFINIÇÕES

Para os efeitos desta norma complementar, aplicam-se os seguintes termos e definições:

4.1 **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;

4.2 **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 da APF, direta e indireta, não comercializável;

4.3 **Chave Criptográfica**: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

4.4 **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;

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

4.6 **Decifração:** ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

4.7 **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, classificada como ultrassecreta, secreta ou reservada;

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

4.9 **Recurso Criptográfico:** sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

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 Informações Sigilosas

5.1.1 Recomenda-se o uso de recursos criptográficos baseados em algoritmo de Estado para cifração e decifração;

5.1.2 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;

5.1.3 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;

5.1.4 O credenciamento de estrangeiros para uso de recurso criptográfico baseado em algoritmo de Estado deve ser submetido ao GSI/PR;

5.1.5 É vedado ao Agente Responsável por recurso criptográfico nos órgãos e entidades da APF, direta e indireta:

5.1.5.1 utilizar recursos criptográficos em desacordo com esta norma, bem como, com a legislação em vigor; e

5.1.5.2 utilizar recursos criptográficos diferentes dos parâmetros e padrões mínimos definidos pelo órgão ou entidade da APF, direta e indireta, a que pertence.

5.2 Informações Classificadas

5.2.1 Toda a informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico baseado em algoritmo de Estado.

5.2.2 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 II desta norma.

5.2.3 Para informação classificada, em qualquer grau de sigilo, também deverá ser aplicado os itens 5.1.2, 5.1.3, 5.1.4 e 5.1.5.1.

5.3 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.

5.4 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.

5.5 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.

5.5.1 Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.5 poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:

a) 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

b) 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.

5.5.2 O não cumprimento do previsto no item 5.5 ou nas letras a e b do sub-item 5.5.1, poderá gerar responsabilidade administrativa, civil e penal, conforme legislação vigente.

5.6 Cabe à Alta Administração dos órgãos e entidades da APF:

5.6.1 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;

5.6.2 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;

5.6.3 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;

5.6.4 Informar ao GSI/PR, tempestivamente, o comprometimento do sigilo de qualquer recurso criptográfico baseado em algoritmo de Estado;

5.6.5 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,

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

5.7 Além do disposto nesta norma, os recursos criptográficos baseados em algoritmo de Estado podem ser objeto de regulamentação específica.

5.8 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 previsto no Anexo II, vedada sua postagem.

5.9 Dispositivos transitórios:

5.9.1 A Alta Administração dos órgãos e entidades da APF, direta e indireta, providenciará a adequação dos recursos criptográficos já em uso por ocasião da entrada em vigor da presente norma;

5.9.2 Os órgãos e entidades deverão adotar os recursos criptográficos baseados em algoritmo de Estado com parâmetros e padrões de que trata o no Anexo II no prazo de um ano a contar da publicação da presente norma; e,

5.9.3 Para o apoio técnico do GSI/PR previsto no item 5.4, especificamente devido ao cumprimento do prazo previsto no item 5.9.2 e art. 56 do Decreto 7.845, de14 de novembro de 2012, os órgãos e entidades têm o prazo de até cento e oitenta dias para a formalização da demanda junto ao Gabinete.

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

6 VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

ANEXO I
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 II

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

LEI Nº 8.159, DE 8 DE JANEIRO DE 1991.

Regulamento

Vide Decreto nº 4.553, de 27.12.02

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

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

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º - É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

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

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

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

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

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

Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos)

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 - Consideram-se documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas freqüentes.

§ 2º - Consideram-se documentos intermediários aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente.

§ 3º - Consideram-se permanentes os conjuntos de documentos de valor histórico, probatório e informativo que devem ser definitivamente preservados.

Art. 9º - A eliminação de documentos produzidos por instituições públicas e de caráter público será realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência.

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

CAPÍTULO III

DOS ARQUIVOS PRIVADOS

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

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

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

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

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

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

Art. 18 - Compete ao Arquivo Nacional a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Executivo Federal, bem como preservar e facultar o acesso aos documentos sob sua guarda, e acompanhar e implementar a política nacional de arquivos.

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

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

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

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

CAPÍTULO V

DO ACESSO E DO SIGILO DOS DOCUMENTOS PÚBLICOS

~~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)

Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos)

DISPOSIÇÕES FINAIS

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

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

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

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

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

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

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

FERNANDO COLLOR
Jarbas Passarinho

Este texto não substitui o publicado no D.O.U. de 9.1.1991 e retificado em 28.1.1991

DECRETO Nº 4.073, DE 3 DE JANEIRO DE 2002.

Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

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, vinculado ao Arquivo Nacional, criado pelo art. 26 da Lei nº 8.159, de 8 de janeiro de 1991, tem por finalidade definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo.

Art. 2º Compete ao CONARQ:

I - estabelecer diretrizes para o funcionamento do Sistema Nacional de Arquivos - SINAR, visando à gestão, à preservação e ao acesso aos documentos de arquivos;

II - promover o inter-relacionamento de arquivos públicos e privados com vistas ao intercâmbio e à integração sistêmica das atividades arquivísticas;

~~III - propor ao Chefe da Casa Civil da Presidência da República normas legais necessárias ao aperfeiçoamento e à implementação da política nacional de arquivos públicos e privados;~~

III - propor ao Ministro de Estado da Justiça normas legais necessárias ao aperfeiçoamento e à implementação da política nacional de arquivos públicos e privados; (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

IV - zelar pelo cumprimento dos dispositivos constitucionais e legais que norteiam o funcionamento e o acesso aos arquivos públicos;

V - estimular programas de gestão e de preservação de documentos públicos de âmbito federal, estadual, do Distrito Federal e municipal, produzidos ou recebidos em decorrência das funções executiva, legislativa e judiciária;

VI - subsidiar a elaboração de planos nacionais de desenvolvimento, sugerindo metas e prioridades da política nacional de arquivos públicos e privados;

VII - estimular a implantação de sistemas de arquivos nos Poderes Executivo, Legislativo e Judiciário da União, dos Estados, do Distrito Federal e nos Poderes Executivo e Legislativo dos Municípios;

VIII - estimular a integração e modernização dos arquivos públicos e privados;

IX - identificar os arquivos privados de interesse público e social, nos termos do art. 12 da Lei nº 8.159, de 1991;

~~X - propor ao Presidente da República, por intermédio do Chefe da Casa Civil da Presidência da República, a declaração de interesse público e social de arquivos privados;~~

X - propor ao Presidente da República, por intermédio do Ministro de Estado da Justiça, a declaração de interesse público e social de arquivos privados; (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

XI - estimular a capacitação técnica dos recursos humanos que desenvolvam atividades de arquivo nas instituições integrantes do SINAR;

XII - recomendar providências para a apuração e a reparação de atos lesivos à política nacional de arquivos públicos e privados;

XIII - promover a elaboração do cadastro nacional de arquivos públicos e privados, bem como desenvolver atividades censitárias referentes a arquivos;

XIV - manter intercâmbio com outros conselhos e instituições, cujas finalidades sejam relacionadas ou complementares às suas, para prover e receber elementos de informação e juízo, conjugar esforços e encadear ações;

XV - articular-se com outros órgãos do Poder Público formuladores de políticas nacionais nas áreas de educação, cultura, ciência, tecnologia, informação e informática.

Art. 3º São membros conselheiros do CONARQ:

I - o Diretor-Geral do Arquivo Nacional, que o presidirá;

II - dois representantes do Poder Executivo Federal;

III - dois representantes do Poder Judiciário Federal;

IV - dois representantes do Poder Legislativo Federal;

V - um representante do Arquivo Nacional;

VI - dois representantes dos Arquivos Públicos Estaduais e do Distrito Federal;

VII - dois representantes dos Arquivos Públicos Municipais;

VIII - um representante das instituições mantenedoras de curso superior de arquivologia;

IX - um representante de associações de arquivistas;

X - três representantes de instituições que congreguem profissionais que atuem nas áreas de ensino, pesquisa, preservação ou acesso a fontes documentais.

§ 1º Cada Conselheiro terá um suplente.

§ 2º Os membros referidos nos incisos III e IV e respectivos suplentes serão designados pelo Presidente do Supremo Tribunal Federal e pelos Presidentes da Câmara dos Deputados e do Senado Federal, respectivamente.

~~§ 3º Os conselheiros e suplentes referidos nos inciso II e V a X serão designados pelo Presidente da República, a partir de listas apresentadas pelo Chefe da Casa Civil da Presidência da República, mediante indicações dos dirigentes dos órgãos e entidades representados.~~

§ 3º Os conselheiros e suplentes referidos nos inciso II e V a X serão designados pelo Presidente da República, a partir de listas apresentadas pelo Ministro de Estado da Justiça, mediante indicações dos dirigentes dos órgãos e entidades representados. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

§ 4º O mandato dos Conselheiros será de dois anos, permitida uma recondução.

§ 5º O Presidente do CONARQ, em suas faltas e impedimentos, será substituído por seu substituto legal no Arquivo Nacional.

Art. 4º Caberá ao Arquivo Nacional dar o apoio técnico e administrativo ao CONARQ.

Art. 5º O Plenário, órgão superior de deliberação do CONARQ, reunir-se-á, em caráter ordinário, no mínimo, uma vez a cada quatro meses e, extraordinariamente, mediante convocação de seu Presidente ou a requerimento de dois terços de seus membros.

§ 1º O CONARQ funcionará na sede do Arquivo Nacional.

§ 2º As reuniões do CONARQ poderão ser convocadas para local fora da sede do Arquivo Nacional, por deliberação do Plenário ou **ad referendum** deste, sempre que razão superior indicar a conveniência de adoção dessa medida.

Art. 6º O CONARQ somente se reunirá para deliberação com o quorum mínimo de dez conselheiros.

Art. 7º O CONARQ poderá constituir câmaras técnicas e comissões especiais, com a finalidade de elaborar estudos, normas e outros instrumentos necessários à implementação da política nacional de arquivos públicos e privados e ao funcionamento do SINAR, bem como câmaras setoriais, visando a identificar, discutir e propor soluções para questões temáticas que repercutirem na estrutura e organização de segmentos específicos de arquivos, interagindo com as câmaras técnicas.

Parágrafo único. Os integrantes das câmaras e comissões serão designados pelo Presidente do CONARQ, **ad referendum** do Plenário.

Art. 8º É considerado de natureza relevante, não ensejando qualquer remuneração, o exercício das atividades de Conselheiro do CONARQ e de integrante das câmaras e comissões.

~~Art. 9º A aprovação do regimento interno do CONARQ, mediante proposta deste, é da competência do Chefe da Casa Civil da Presidência da República.~~

Art. 9º A aprovação do regimento interno do CONARQ, mediante proposta deste, é da competência do Ministro de Estado da Justiça. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

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 do Distrito Federal dos Poderes Executivo, Legislativo e Judiciário;

VII - os arquivos municipais dos Poderes Executivo e Legislativo.

§ 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, podem integrar o SINAR mediante acordo ou ajuste com o órgão central.

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 integridade 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 arquivístico 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 nas câmaras técnicas, câmaras setoriais e comissões especiais constituídas pelo CONARQ;

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 Distrito 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 função 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, instituído 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 mencionadas 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 integram 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 I

Das Comissões Permanentes de Avaliação de Documentos

Art. 18. Em cada órgão e entidade da Administração Pública Federal será constituída comissão permanente de avaliação de documentos, que terá a responsabilidade de orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor.

§ 1º Os documentos relativos às atividades-meio serão analisados, avaliados e selecionados pelas Comissões Permanentes de Avaliação de Documentos dos órgãos e das entidades geradores dos arquivos, obedecendo aos prazos estabelecidos em tabela de temporalidade e destinação expedida pelo CONARQ.

§ 2º Os documentos relativos às atividades-meio não constantes da tabela referida no § 1º serão submetidos às Comissões Permanentes de Avaliação de Documentos dos órgãos e das entidades geradores dos arquivos, que estabelecerão os prazos de guarda e destinação daí decorrentes, a serem aprovados pelo Arquivo Nacional.

§ 3º Os documentos relativos às atividades-fim serão avaliados e selecionados pelos órgãos ou entidades geradores dos arquivos, em conformidade com as tabelas de temporalidade e destinação, elaboradas pelas Comissões mencionadas no **caput**, aprovadas pelo Arquivo Nacional.

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 acondicionados, 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. O Ministério do Planejamento, Orçamento e Gestão deverá, tão logo sejam nomeados os inventariantes, liquidantes ou administradores de acervos para os órgãos e entidades extintos, solicitar à Casa Civil da Presidência da República a assistência técnica do Arquivo Nacional para a orientação necessária à preservação e à destinação do patrimônio documental acumulado, nos termos do § 2º do art. 7º da Lei nº 8.159, de 1991.~~

Art. 20. O Ministério do Planejamento, Orçamento e Gestão deverá, tão logo sejam nomeados os inventariantes, liquidantes ou administradores de acervos para os órgãos e entidades extintos, solicitar ao Ministro de Estado da Justiça a assistência técnica do Arquivo Nacional para a orientação necessária à preservação e à destinação do patrimônio documental acumulado, nos termos do § 2º do art. 7º da Lei nº 8.159, de 1991. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

~~Art. 21. A Casa Civil da Presidência da República, mediante proposta do Arquivo Nacional, baixará instrução detalhando os procedimentos a serem observados pelos órgãos e entidades da Administração Pública Federal, para a plena consecução das medidas constantes desta Seção.~~

Art. 21. O Ministro de Estado da Justiça, mediante proposta do Arquivo Nacional, baixará instrução detalhando os procedimentos a serem observados pelos órgãos e entidades da administração pública federal, para a plena consecução das medidas constantes desta Seção. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

Capítulo V

DA DECLARAÇÃO DE INTERESSE PÚBLICO E SOCIAL DE ARQUIVOS PRIVADOS

Art. 22. Os arquivos privados de pessoas físicas ou jurídicas que contenham documentos relevantes para a história, a cultura e o desenvolvimento nacional podem ser declarados de interesse público e social por decreto do Presidente da República.

§ 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 vigência 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. O CONARQ, por iniciativa própria ou mediante provocação, encaminhará solicitação, acompanhada de parecer, ao Chefe da Casa Civil da Presidência da República, com vistas à declaração de interesse público e social de arquivos privados pelo Presidente da República.~~

Art. 23. O CONARQ, por iniciativa própria ou mediante provocação, encaminhará solicitação, acompanhada de parecer, ao Ministro de Estado da Justiça, com vistas à declaração de interesse público e social de arquivos privados pelo Presidente da República. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

§ 1º O parecer será instruído com avaliação técnica procedida por comissão especialmente constituída pelo CONARQ.

§ 2º A avaliação referida no § 1º será homologada pelo Presidente do CONARQ.

~~§ 3º Da decisão homologatória caberá recurso das partes afetadas ao Chefe da Casa Civil da Presidência da República, na forma prevista na Lei nº 9.784, de 29 de janeiro de 1999.~~

§ 3º Da decisão homologatória caberá recurso das partes afetadas ao Ministro de Estado da Justiça, na forma prevista na Lei nº 9.784, de 29 de janeiro de 1999 (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

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 responsabilidade 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, objetivando 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 Chefe da Casa Civil da Presidência da República baixará instruções complementares à execução deste Decreto.~~

Art. 30. O Ministro de Estado da Justiça baixará instruções complementares à execução deste Decreto. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

~~Art. 31. Fica delegada competência ao Chefe da Casa Civil da Presidência da República, permitida a subdelegação, para designar os membros do CONARQ de que trata o § 3º do art. 3º.~~

Art. 31. Fica delegada competência ao Ministro de Estado da Justiça, permitida a subdelegação, para designar os membros do CONARQ de que trata o § 3º do art. 3º. (Redação dada pelo Decreto nº 7.430, de 2011) Vigência

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

Perguntas mais frequentes sobre o Tratamento da Informação Classificada e o Credenciamento de Segurança

Disponível no endereço: http://dsic.planalto.gov.br/perguntas-frequentes/perguntas-sobre-a-lai

1. Qual a diferença entre informação classificada e informação Sigilosa?

R: A informação classificada, de acordo com o artigo 24, *caput*, da Lei nº 12.527, de 18 de novembro de 2011, é aquela submetida a qualquer dos três graus de sigilo previstos no § 1º do citado artigo.

A informação sigilosa é aquela cuja restrição de acesso ocorre em virtude de sua classificação ou por hipótese legal de sigilo (artigo 22 da Lei nº 12.527, de novembro de 2011). Ex: Pessoal, bancária, etc.

"Toda informação classificada é sigilosa, porém nem toda informação sigilosa é classificada".

2. Quem deve proceder o tratamento da Informação Classificada?

R: Todos os órgãos e entidades do Poder Executivo Federal que produzirem ou custodiarem informação classificada deverão proceder ao tratamento dessa informação de acordo com a legislação em vigor (Lei nº 12.527, de 18 de novembro de 2011, Decreto nº 7.724, de 16 de maio de 2012 e Decreto nº 7.845, de 14 de novembro de 2012), e as *normas e diretrizes expedidas pelo GSI/PR*.

3. Qual é o Órgão responsável pela normatização da atividade de credenciamento de pessoas e empresas para o trato da informação classificada?

R: Conforme o artigo 6º, *caput*, e seu inciso I do Decreto nº 7.845, de 14 de novembro de 2012, e o artigo 70, inciso II do Decreto nº 7.724, de 16 de maio de 2012, compete ao GSI/PR expedir os atos complementares e estabelecer procedimentos para o credenciamento de segurança para o trato da informação classificada.

4. Como utilizar recursos criptográficos no tratamento da Informação Classificada?

R: Os recursos criptográficos para o trato da informação classificada deverão observar o disposto nas instruções normativas e normas complementares do GSI/PR, quanto à utilização de algoritmo de Estado, segundo os parâmetros e padrões mínimos estabelecidos para cada grau de sigilo vigente: reservado, secreto e ultrassecreto, conforme a Norma Complementar nº 09/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013.

5. O que é algoritmo de Estado?

R: Conforme definição dada pelo artigo 2º, inciso I do Decreto nº 7.845, de 14 de novembro de 2012, é uma 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.

6. Qual o perfil que deve possuir o Servidor que irá lidar com o tratamento da Informação Classificada?

R: Possuir conhecimento das normas e legislação do governo referente à segurança da informação e comunicações e estar familiarizado com as políticas e boas práticas de segurança em seu órgão, bem como ser credenciado para tal.

7. Qual a condição para que uma pessoa natural seja credenciada, ou uma empresa brasileira habilitada para a troca e tratamento de informação classificada com países estrangeiros?

R: Quanto às pessoas naturais, as condições estão previstas no artigo 12 do Decreto nº 7.845, de 14 de novembro de 2012.

Em relação à empresa brasileira, a habilitação para a troca e tratamento de informação classificada com países estrangeiros, fica condicionada ao previsto nos artigos 16 e 11 do Decreto nº 7.845, de 14 de novembro de 2012.

8. Quais os tratados ou acordos internacionais em que o GSI/PR deve participar das negociações em articulação junto ao MRE?

R: Somente aqueles que envolverem a troca de informações classificadas entre um país estrangeiro e o Brasil.

9. O que é o Núcleo de Segurança e Credenciamento?

R: É o órgão central de credenciamento e segurança instituído no âmbito do GSI/PR, pelo artigo 37 da Lei nº 12.527, de 18 de novembro de 2011 e regulamentado pelo Decreto nº 7.845, de 14 de novembro de 2012, que tem como missão principal, promover e propor a regulamentação do credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações classificada, normatizado pela **Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013**.

10. Qual é o objetivo e a finalidade de uma credencial de Segurança?

R: Credenciar pessoas e habilitar empresas, para o tratamento de informação classificada, por meio de um processo de credenciamento de segurança.

11. Que requisitos os órgãos e entidades públicos deverão atender para serem habilitados para o credenciamento de segurança?

R: São os previstos no artigo 10, *caput*, incisos I e II do Decreto nº 7.845, de 14 de novembro de 2012, bem como aqueles prescritos nos atos complementares publicados pelo GSI/PR, como a **Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013** e respectivas Normas Complementares.

12. O que são materiais de acesso restrito? Eles possuem grau de sigilo?

R: São aqueles que por sua natureza e emprego, deve ter os seus acessos restritos às pessoas autorizadas pelo órgão, como os previstos no artigo 45, caput, incisos I, II, III, IV, V do Decreto nº 7.845, de 14 de novembro de 2012.

Os materiais de acesso restrito não são classificados por grau de sigilo, mas terão o seu acesso restrito na forma do artigo 44 do Decreto nº 7.845, de novembro de 2012.

13. Que órgãos da Administração Pública Federal poderão ser habilitados como Órgão de Registro Nível 1?

R: Os prescritos no artigo 2º, inciso XIII do Decreto nº 7.845, de 14 de novembro de 2012, ou seja, ministérios ou órgãos de nível equivalente.

14. Em que circunstância poderá ser concedida habilitação de segurança para as empresas privadas e que requisitos a empresa privada deverá atender para tal?

R: Quando a empresa privada estiver em vias de assinar um contrato que envolva a troca de informação classificada com órgão ou entidade do Poder Executivo Federal ou empresa estrangeira, obedecido o previsto no artigo 11 do Decreto nº 7.845, de 14 de novembro de 2012.

15. Como poderá uma empresa privada receber habilitação de segurança?

R: Órgãos ou entidades da iniciativa privada somente poderão ser habilitados como Posto de Controle, uma vez atendidos os requisitos constantes do artigo 11 do Decreto nº 7.845, de 14 de novembro de 2012.

16. O que é o CIDIC?

R: Para se proceder à classificação da informação, necessário se faz o preenchimento do TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO - TCI, conforme ANEXO do Decreto nº 7.724 de 16 de maio de 2012. Dentre as informações que compõem o citado termo, tem-se: o Código de Indexação de

Documento que contém Informação Classificada - CIDIC.

17. Como os órgãos obterão o CIDIC?

R: O CIDIC deverá ser gerado pelo órgão ou entidade do Poder Executivo Federal, de acordo com os procedimentos descritos nos artigos 50, 51 e 52 do Decreto nº 7.845, de 14 de novembro de 2012. Maiores informações sobre o Número Único de Protocolo – NUP, bem como sobre a formatação e composição do CIDIC, poderão ser obtidas nos seguintes arquivos:

CIDIC COMPOSIÇÃO

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA - GSIPR

Composição do Código de Indexação de Documento que contém Informação Classificada – CIDIC
Artigos 51 e 52 do Decreto Nº 7.845, de 14/11/2012

CIDIC							
PRIMEIRA PARTE (NUP)		. SEGUNDA PARTE (28 ou 39 campos com caracteres alfanuméricos e separadores)					
Art. 51 NUP (Art. 6º da Port. nº 03 de 16/05/2003 do MPOG/SLTI)		Art. 52, I Grau de Sigilo	Art. 52, II Anexo II Categoria (VCGE)	Art. 52, III Data de Produção	Art. 52, IV Data de Desclassificação	Art. 52, V Indicação da Reclassificação	Art. 52, VI Data da Prorrogação (U)
Nº da Unidade ou órgão	Registro seqüencial/ ano-dig ver	U, S ou R	01 a 17	DD/MM/AAAA	DD/MM/AAAA	S ou N	DD/MM/AAAA
XXXXX	NNNNNN/AAAA-DV	U	06	05/12/2012	04/12/2037	N	Não preencher

11111.000001/2013-99.U.06.05/12/2012.04/12/2037.N

CIDIC FORMATAÇÃO ORIENTAÇÃO

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA - GSIPR

ORIENTAÇÕES GERAIS PARA FORMATAÇÃO DO CÓDIGO DE INDEXAÇÃO DE DOCUMENTO QUE CONTÉM INFORMAÇÃO CLASSIFICADA -CIDIC

(DECRETO Nº 7.845, DE 14.11.2012)

1. A 1ª parte do CIDIC deve prever número de posições que atendam ao Número Único de Protocolo – NUP, que é um código exclusivamente numérico;

2. A 2ª parte do CIDIC, separada da 1ª parte por um ".", iniciará sempre por um caracter alfabético ("U", "S" ou "R") e deverá prever até o máximo de 39 posições, com caracteres alfanuméricos e separadores;

3. Os separadores utilizados serão: "." e "/" para as datas;

4. Para as informações classificadas no grau reservado e secreto, a 2ª parte do CIDIC terá sempre 28 posições com caracteres alfanuméricos e separadores;

5. Para as informações classificadas no grau ultrassecreto, a 2ª parte do CIDIC terá 28 posições com caracteres alfanuméricos e separadores, enquanto não ocorrer prorrogação do prazo do sigilo;

6. Quando ocorrer a prorrogação do prazo de sigilo da informação classificada no grau ultrasecreto, a nova data deverá constar no final da 2ª parte do CIDIC, totalizando as 39 posições com caracteres alfanuméricos e separadores;

7. Exemplos:

a) **informação classificada no grau reservado, sem reclassificação:**
   NUP.R.06.05/12/2012.04/12/2017.N
b) **informação classificada no grau reservado, com reclassificação, reduzindo 1 ano do prazo de sigilo:**
   NUP.R.06.05/12/2012.04/12/2016.S
c) **informação classificada no grau secreto, sem reclassificação:**
   NUP.S.06.05/12/2012.04/12/2027.N
d) **informação classificada no grau secreto, com reclassificação, reduzindo 5 anos do prazo de sigilo:**
   NUP.S.06.05/12/2012.04/12/2022.S
e) **informação classificada no grau ultrassecreto, sem reclassificação e sem prorrogação do sigilo:**
   NUP.U.06.05/12/2012.04/12/2037.N
f) **informação classificada no grau ultrassecreto, com reclassificação, reduzindo 5 anos do prazo de sigilo, e sem prorrogação do sigilo:**
   NUP.U.06.05/12/2012.04/12/2032.S
g) **informação classificada no grau ultrassecreto, sem reclassificação, e com prorrogação de mais 20 anos de sigilo:**
   NUP.U.06.05/12/2012.04/12/2037.N.04/12/2057

NUP REFERÊNCIAS ADMINISTRATIVAS

REFERÊNCIAS ADMINISTRATIVAS DO NÚMERO ÚNICO DE PROTOCOLO – NUP

(1ª. Parte do CIDIC - DECRETO Nº 7.845, DE 14.11.2012)

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação **Portaria nº 3**, de 16 de maio de 2003. Orienta os órgãos da Presidência da República, Ministérios, autarquias e fundações integrantes do Sistema de Serviços Gerais - SISG, quanto aos procedimentos relativos às atividades de Comunicações Administrativas, para utilização do número único de processos e documentos. Disponível em: < http://www.comprasnet.gov.br/ legislacao/ portarias/ p03_03.htm>. Acesso em: 20 jan. 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. **Portaria nº 12**, de 23 de novembro de 2009. Altera a Portaria Normativa nº 5, de 19 de dezembro de 2002, que dispõe sobre os procedimentos gerais para utilização de protocolo, no âmbito da Administração Pública Federal, para os órgãos e entidades integrantes do Sistema de Serviços Gerais - SISG. Disponível em: < http://www.siga.arquivonacional.gov.br/ media/ siga/portaria_slti_n12_23_nov_2009.doc>. Acesso em: 25 jan. 2012.

BRASIL. Tribunal de Contas da União. **Acórdão nº 1.386**, de 09 de agosto de 2006.Avaliação do Programa Governo Eletrônico. Relator Ministro Valmir Campelo. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo, 2006. Disponível em: < http://portal2.tcu.gov.br/portal/pls/portal/docs/2056480.PDF>. Acesso em: 24 fev. 2012.

COMITÊ EXECUTIVO DO GOVERNO ELETRÔNICO (Brasil). **Resolução nº 13**, de 25 de novembro de 2002. Institui o Sistema de Acompanhamento de Processos do Governo Federal – PROTOCOLO.NET. Disponível em: <http://www.governoeletronico.gov.br/o-gov.br/legislacao/resolucoes>. Acesso em: 20 jan. 2012.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Resolução nº 25**, de 27 de abril de 2007. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: < http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?infoid=206&sid=46>. Acesso em: 20 jan. 2012.

Brasil. Ministério do Planejamento, Orçamento e Gestão.Secretaria de Logística e Tecnologia da Informação. **Padrão de dados, integração de protocolos do Governo Federal** : versão 1.0. Brasília: MP/SLTI, 2012.

---

18. Os órgãos do Poder Executivo Federal deverão gerar o CIDIC para os documentos que contenham informações classificadas produzidas anteriormente à publicação da Lei nº 12.527, de 18 de novembro de 2011, para fins de disponibilização dos mesmos na *internet* ?

R: Sim, em conformidade com o artigo 55 do Decreto nº 7.845, de 14 de novembro de 2012, para fins do disposto no artigo 45 do Decreto nº 7.724, de 16 de maio de 2012, que determina a disponibilização do CIDIC na *internet*.

19. Os processos de natureza Administrativa Disciplinar, por exemplo, deverão ser tratados como sigilosos (classificados) ou poderão ser tramitados tal qual restritos (uma vez que tem informações de cunho pessoal de agentes públicos)?

R: Documentos que contenham informações de cunho pessoal de agente público, deverão ser tratadas conforme previsto no inciso I do §1º do art. 31 da Lei

nº 12.527 de 18 de novembro de 2012, observando-se o previsto no §4º do mesmo artigo, sem prejuízo da Lei nº 9.784, de 29 de Janeiro de 1999, que regula o processo administrativo no âmbito da APF.

20. Poderá haver no órgão um departamento de triagem documental que abra as correspondências classificadas, digitalize-as e depois efetue sua distribuição? Seria um departamento de triagem de documentação confidencial?

R: Documento classificado em qualquer grau de sigilo somente pode ser aberto pelo destinatário. Quando o encarregado da triagem documental constatar no envelope interno tratar-se de documento classificado, deverá encaminhá-lo fechado de imediato para o destinatário (§1º do art. 29 do Dec. nº 7.845, de 14 de novembro de 2012). A digitalização e distribuição de um documento classificado, somente poderão ser realizadas, desde que atendidos o prescrito nos arts. 28, 30 e 31 do Dec. nº 7.845 de 14 de novembro de 2012).

21. Para os graus de sigilo Reservado e Secreto, pode-se utilizar qualquer algoritmo de criptografia (ex.: RSA com AES), contando que se obedeça os tamanhos mínimos de chave definidos no Anexo II da Norma Complementar nº 09 IN01/DSIC/GSIPR/2013?

R: Não. Está estabelecido tanto no Decreto nº 7.845, de 2012 quanto na Norma Complementar nº 09 IN01/DSIC/GSIPR, de 2013, homologada pela Portaria nº 3, de 2013, da Secretaria Executiva do Conselho de Defesa Nacional, que o algoritmo criptográfico de sigilo a ser utilizado para cifrar ou decifrar informação classificada em qualquer grau de sigilo, para uso exclusivo em interesse de serviço de Órgãos ou entidades da Administração Pública Federal (APF), direta ou indireta, deve ser algoritmo de Estado, de desenvolvimento próprio e não comercializável.

Os algoritmos de criptografia assimétricos como o RSA e os baseados em Curvas Elípticas são utilizados comumente para certificação digital e também para gerenciamento de chaves de comunicação (chaves simétricas). Estes sistemas não são utilizados para sigilo da informação de Governo. Algoritmos criptográficos assimétricos são utilizados em conjunto com algoritmos de sigilo, no caso, com algoritmo de Estado.

Portanto, a implementação de um sistema ou solução criptográfica pode utilizar para cifração e decifração de informação classificada no grau Reservado ou Secreto, por exemplo:

i. o RSA com algoritmo de Estado, ou

ii. sistemas baseados em Curvas Elípticas com algoritmo de Estado.

22. O algoritmo criptográfico terá que ser desenvolvido pelo governo Brasileiro?

R: Sim. O algoritmo criptográfico a ser utilizado para cifração e decifração da

informação classificada em qualquer grau de sigilo no âmbito do Governo deverá ser um algoritmo de Estado, desenvolvido pelo Estado.

23. Já existem algoritmos prontos para serem utilizados?

R: Sim. A ABIN/GSIPR poderá dar apoio técnico aos órgãos da Administração Pública Federal, direta ou indireta a partir de recomendações de como integrar um algoritmo de Estado às soluções vigentes no seu órgão.

24. Para o grau Ultrassecreto, já há algum algoritmo que pode ser utilizado?

R: A ABIN/GSIPR desenvolveu um sistema de Chaves aleatórias, que poderá ser utilizado, desde que seja customizado conforme a necessidade do órgão ou entidade da APF.

25. Como formalizar o pedido de apoio técnico ao GSI/PR conforme item 5.9.3 da NC 09 IN01/DSIC/GSIPR, de 2013?

R: A Alta Administração do órgão ou entidade da APF deverá formalizar o pedido do apoio técnico de que trata o item 5.9.3 da NC 09 IN01/DSIC/GSIPR, de 2013 mediante encaminhamento de correspondência oficial ao Secretário Executivo do GSI/PR.

26. Quem efetuará o credenciamento de segurança previsto no Art. 10 do Decreto nº 7.845, de 14 de novembro de 2012, nos órgãos e entidades do Poder Executivo federal que não tenham status de Ministério ou equivalente a estes?

R: Órgãos e entidades do Poder Executivo federal que não tenham status de Ministério ou equivalente poderão ser habilitados como Órgão de Registro Nível 2, pelo Ministério com o qual mantenha vínculo de qualquer natureza (Órgão de Registro Nível 1), e a partir daí, então, poderá proceder o credenciamento das pessoas naturais que com eles mantenham vínculo.

27. Haverá um curso para habilitar e capacitar os agentes públicos para o tratamento da informação classificada e o credenciamento de segurança?

R: O GSI/PR planeja realizar oficinas de capacitação para os órgãos da APF, em data a ser divulgada oportunamente.

28. Como os órgãos e entidades públicas poderão ser incluídos nos treinamentos, cursos e oficinas para capacitação no tocante operacional, a laborar com todos os itens que versam a Lei nº 12.527/11, Lei nº 9.507/97, Decreto nº 7.724/12, Decreto nº 7.845/12 e instrumentos normativos correlatos?

R: Os treinamentos coordenados pelo Departamento de Segurança da Informação e Comunicações - DSIC são sempre divulgadas no sítio do Departamento na internet (http://dsic.planalto.gov.br/). As solicitações de inclusão deverão ser encaminhadas ao Secretário-Executivo do GSI/PR.

29. Como e quando será utilizado o TCMS?

R: A utilização do TCMS, em caráter excepcional, encontra-se prevista na Seção IX do Decreto nº 7.845, de 14 de novembro de 2012, e seu modelo consta anexo ao citado Decreto.

30. Quais serão os documentos norteadores para a investigação, conforme solicitado pelo artigo 12 do Decreto nº 7.845/12?

R: Em conformidade com o art. 14 do Decreto em pauta, os órgãos e entidades do Poder Executivo federal que não tiverem competência aos procedimentos de investigação para credenciamento de segurança, poderão firmar ajustes, convênios ou termo de cooperação com outros órgãos ou entidades públicas que detenham tal competência. Soma-se a publicação da Instrução Normativa GSI/PR nº 02, de 05 de fevereiro de 2013, e oportunamente, publicará atos complementares que melhor nortearão os requisitos mínimos para credenciamento de segurança de pessoas físicas e jurídicas.

31. Como proceder com os documentos classificados anteriormente a publicação da lei nº 12.527/11?

R: O documento com informação classificada em qualquer grau de sigilo, produzido antes da Lei nº 12.527/11, receberá o CIDIC para fins de publicação do rol da internet (art. 45 do Decreto nº 7.724/12). Com relação aos documentos classificados no grau secreto e ultrassecreto de acordo com o art. 39 caput da Lei nº 12.527/11, os órgãos e entidades disporão de um prazo máximo de dois anos para reavaliação das classificações (com assessoramento da Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS, art. 34 do Decreto nº 7724/12), contado a partir da vigência da Lei nº 12.527/11.

32. Quais as informações que devem ser listadas no "rol das informações desclassificadas nos últimos doze meses" (conforme previsto no Inciso I, Art. 45, Decreto Nº 7845/2012)?

R: Nessa listagem deverão constar os números únicos de protocolo - NUP de todos os documentos desclassificados que possuíam Termo de Classificação de Informação - TCI, desde a entrada em vigor da Lei de Acesso à Informação.

33. Como preencher o campo RAZÕES PARA CLASSIFICAÇÃO do TCI (Termo de Classificação de Informação) em documentos classificados com data de produção anterior à LAI (Lei de Acesso à Informação)?

R: No campo RAZÕES PARA CLASSIFICAÇÃO do TCI de documentos legados, quando não for possível a recuperação histórica das razões, orienta-se a reprodução do texto contido na base legal do artigo 25 do Decreto nº 7.724/2012, conforme o campo FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO do TCI.

34. Há outras Comissões Permanentes de Avaliação de Documentos Sigilosos - CPADS já implantadas em outros órgãos?

R: As CPADS já existiam em órgãos que já classificavam a informação de acordo com o Decreto 4.553/2000 e foram instituídas segundo a Lei de Arquivos(Lei 8.159/1991). Os Órgãos que não tinham a prática de classificar documentos estão agora criando as suas CPADS.

35. Como implantar a Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS?

Resposta:

1. Designação formal do presidente da CPADS, que tenha articulação com as áreas do órgão que demandem classificação de informação, e com perfil de coordenador/gestor;
2. Designação formal dos demais membros e suplentes da Comissão, preferencialmente com 1 representante de cada área demandante de classificação da informação;
3. No mesmo ato de instituição da CPADS e designação de seus membros, A alta administração do órgão poderá o órgão estabelecer as responsabilidades e regular o funcionamento, periodicidade e demais procedimentos dos trabalhos da Comissão;
4. Providenciar a credencial de segurança para todos os membros da CPADS no nível ultrassecreto, pois todos terão necessidade de conhecer informação classificada em qualquer grau de sigilo. Tal demanda deverá ser interposta ao Gestor de Credenciamento de Segurança do órgão, neste caso da SG/PR, Órgão de Registro Nível 1. Em caráter transitório, enquanto se processa o credenciamento, os membros da CPADS poderão desempenhar suas funções na Comissão desde que assinem o Termo de Compromisso de Manutenção de Sigilo – TCMS, modelo Anexo I do Decreto 7.845/2012, conforme prescreve o Parágrafo Único do artigo 18 do mesmo Decreto.

36. Como se dará o credenciamento de segurança previsto na Instrução Normativa nº 02 do GSI/PR?

R: O GSI publicará em breve 3 (três) normas complementares à Instrução Normativa nº 2 do GSI/PR regulando os procedimentos para o credenciamento de pessoas naturais, órgãos públicos e empresas privadas.

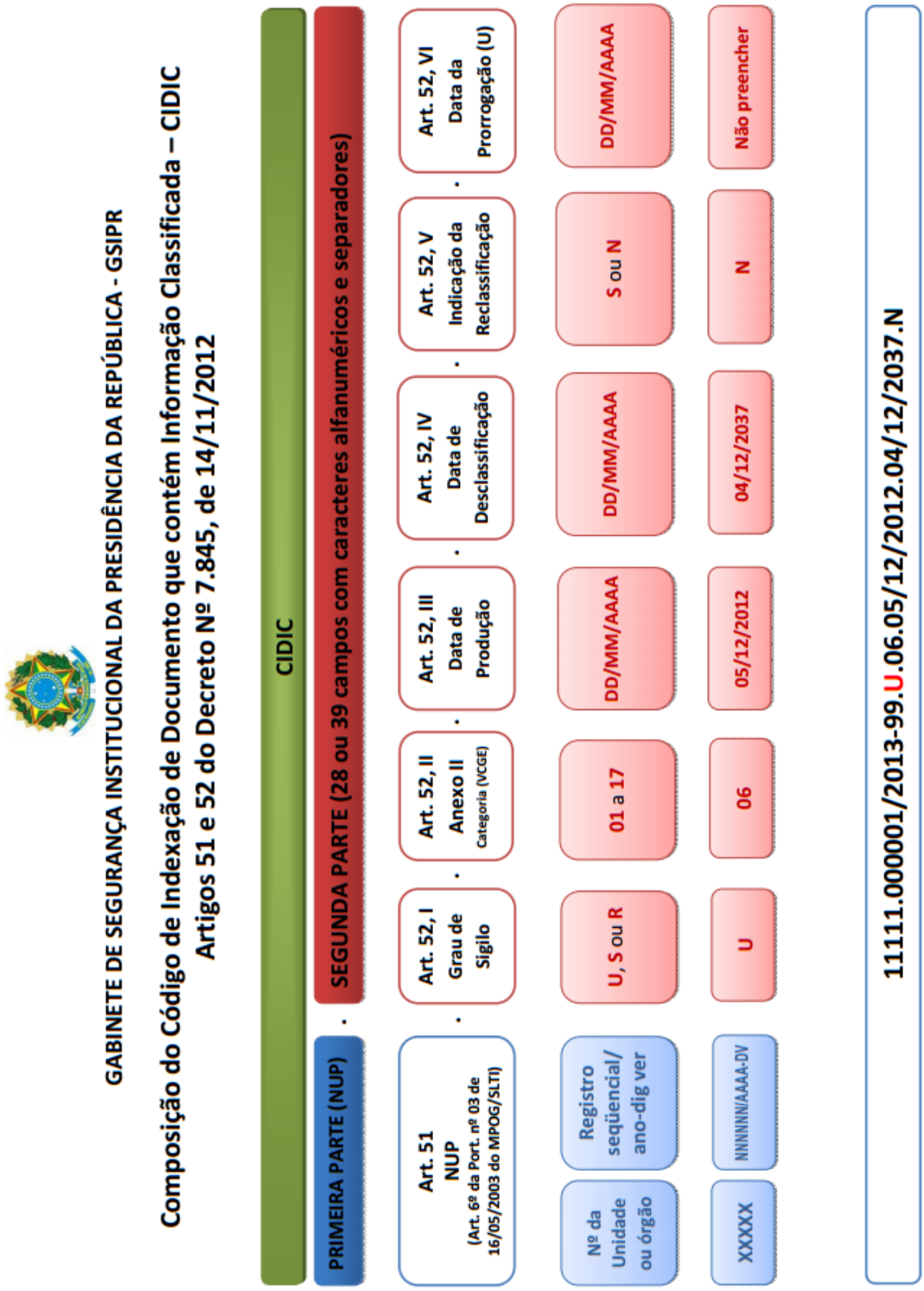
37. Quais são as atribuições do Gestor de Segurança e Credenciamento - GSC?

R: A competência do GSC está regulada pelo artigo 17 da Instrução Normativa nº 02 do GSI/PR. Para tanto, é desejável que o servidor designado para GSC

possua perfil compatível, ou seja, deve possuir conhecimento em Segurança da Informação, ascendência funcional que lhe permita articulação no âmbito da alta administração de seu órgão, bem como, possuir conhecimento da legislação pertinente.

Instruções para Composição do CIDIC e do NUP

1) **Composição do Código de Indexação de Documento que contém Informação Classificada – CIDIC:**



2) Orientações Para formatação do CIDIC:

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA - GSIPR

ORIENTAÇÕES GERAIS PARA FORMATAÇÃO DO CÓDIGO DE INDEXAÇÃO DE DOCUMENTO QUE CONTÉM INFORMAÇÃO CLASSIFICADA -CIDIC

(DECRETO Nº 7.845, DE 14.11.2012)

1. A 1ª parte do CIDIC deve prever número de posições que atendam ao Número Único de Protocolo – NUP, que é um código exclusivamente numérico;

2. A 2ª parte do CIDIC, separada da 1ª parte por um ".", iniciará sempre por um caracter alfabético ("U", "S" ou "R") e deverá prever até o máximo de 39 posições, com caracteres alfanuméricos e separadores;

3. Os separadores utilizados serão: "." e "/" para as datas;

4. Para as informações classificadas no grau reservado e secreto, a 2ª parte do CIDIC terá sempre 28 posições com caracteres alfanuméricos e separadores;

5. Para as informações classificadas no grau ultrassecreto, a 2ª parte do CIDIC terá 28 posições com caracteres alfanuméricos e separadores, enquanto não ocorrer prorrogação do prazo do sigilo;

6. Quando ocorrer a prorrogação do prazo de sigilo da informação classificada no grau ultrasecreto, a nova data deverá constar no final da 2ª parte do CIDIC, totalizando as 39 posições com caracteres alfanuméricos e separadores;

7. Exemplos:

a) **informação classificada no grau reservado, sem reclassificação:**
   NUP.R.06.05/12/2012.04/12/2017.N
b) **informação classificada no grau reservado, com reclassificação, reduzindo 1 ano do prazo de sigilo:**
   NUP.R.06.05/12/2012.04/12/2016.S
c) **informação classificada no grau secreto, sem reclassificação:**
   NUP.S.06.05/12/2012.04/12/2027.N
d) **informação classificada no grau secreto, com reclassificação, reduzindo 5 anos do prazo de sigilo:**
   NUP.S.06.05/12/2012.04/12/2022.S
e) **informação classificada no grau ultrassecreto, sem reclassificação e sem prorrogação do sigilo:**
   NUP.U.06.05/12/2012.04/12/2037.N
f) **informação classificada no grau ultrassecreto, com reclassificação, reduzindo 5 anos do prazo de sigilo, e sem prorrogação do sigilo:**
   NUP.U.06.05/12/2012.04/12/2032.S
g) **informação classificada no grau ultrassecreto, sem reclassificação, e com prorrogação de mais 20 anos de sigilo:**
   NUP.U.06.05/12/2012.04/12/2037.N.04/12/2057

3) Referências Administrativas do Número Único de Protocolo – NUP:

REFERÊNCIAS ADMINISTRATIVAS DO NÚMERO ÚNICO DE PROTOCOLO – NUP

(1ª. Parte do CIDIC - DECRETO Nº 7.845, DE 14.11.2012)

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação **Portaria nº 3**, de 16 de maio de 2003. Orienta os órgãos da Presidência da República, Ministérios, autarquias e fundações integrantes do Sistema de Serviços Gerais - SISG, quanto aos procedimentos relativos às atividades de Comunicações Administrativas, para utilização do número único de processos e documentos. Disponível em: < http://www.comprasnet.gov.br/ legislacao/ portarias/ p03_03.htm>. Acesso em: 20 jan. 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. **Portaria nº 12**, de 23 de novembro de 2009. Altera a Portaria Normativa nº 5, de 19 de dezembro de 2002, que dispõe sobre os procedimentos gerais para utilização de protocolo, no âmbito da Administração Pública Federal, para os órgãos e entidades integrantes do Sistema de Serviços Gerais - SISG. Disponível em: < http://www.siga.arquivonacional.gov.br/ media/ siga/portaria_slti_n12_23_nov_2009.doc>. Acesso em: 25 jan. 2012.

BRASIL. Tribunal de Contas da União. **Acórdão nº 1.386**, de 09 de agosto de 2006.Avaliação do Programa Governo Eletrônico. Relator Ministro Valmir Campelo. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo, 2006. Disponível em: < http://portal2.tcu.gov.br/portal/pls/portal/docs/2056480.PDF>. Acesso em: 24 fev. 2012.

COMITÊ EXECUTIVO DO GOVERNO ELETRÔNICO (Brasil). **Resolução nº 13**, de 25 de novembro de 2002. Institui o Sistema de Acompanhamento de Processos do Governo Federal – PROTOCOLO.NET. Disponível em: <http://www.governoeletronico.gov.br/o-gov.br/legislacao/resolucoes>. Acesso em: 20 jan. 2012.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Resolução nº 25**, de 27 de abril de 2007. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: < http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?infoid=206&sid=46>. Acesso em: 20 jan. 2012.

Brasil. Ministério do Planejamento, Orçamento e Gestão.Secretaria de Logística e Tecnologia da Informação. **Padrão de dados, integração de protocolos do Governo Federal** : versão 1.0. Brasília: MP/SLTI, 2012.

Para acessar e baixar a documentação acesse:

http://dsic.planalto.gov.br/NSC/Legislacao_Relacionada_a_LAI.pdf