



Política para Classificação da Informação

Versão 2.0

Abril de 2024

Controle de Versão

Versão	Data	Nome	Ação
2.0	04/2024	José Vicente dos Santos	Atualização

Sumário

1. INTRODUÇÃO.....	3
2. ÂMBITO DE APLICAÇÃO	3
3. DEFINIÇÕES	3
4. DETERMINAÇÕES	6
5. DISPOSIÇÕES FINAIS	18
ANEXO 1 – TERMO DE CLASSIFICAÇÃO DA INFORMAÇÃO – TCI	21
ANEXO 2 - TÍTULO E FORMATO DE APRESENTAÇÃO DO CIDIC	25
ANEXO 3 - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS	29
ANEXO 4 - QUADRO EXEMPLIFICATIVO DE TIPOS DE INFORMAÇÃO SIGILOSA E DE EMBASAMENTO LEGAL	30

1. INTRODUÇÃO

Este manual tem por finalidade definir os procedimentos de classificação, de proteção e de divulgação da informação sigilosa e restrições de acesso relacionadas à documentação da AC NACIONAL e de suas Autoridades de Registro (AR) vinculadas, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011, Decreto nº 7.724, de 16 de maio de 2012 e o Decreto nº 7.845, de 14 de novembro de 2012.

2. ÂMBITO DE APLICAÇÃO

Todos os órgãos da Empresa e Autoridades de Registro vinculadas.

3. DEFINIÇÕES

Para efeito desta Norma, entende-se por:

- a) Ambiente Restrito e Controlado: espaço físico ou virtual no qual são adotadas medidas (preventivas de segurança) necessárias à limitação do acesso, bem como à efetivação desses acessos aos ativos de informação e seu respectivo controle;
- b) Ativo de Informação: conjunto de dados, informações, documentos e recursos de informação que agregam valor ao patrimônio da organização;
- c) Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
- d) Classificação da Informação: atribuição de grau de sigilo a ativos de informação nos termos da Lei nº 12.527/2011;

- e) Comissão Mista de Reavaliação de Informações: comissão externa instituída nos termos do Art. 46 do Decreto nº 7.724/2012, que decidirá no âmbito da administração pública federal sobre o tratamento e a classificação de informações classificadas como “ultrassegredo” e “segredo”;
- f) Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS: comissão interna à AC NACIONAL, instituída nos termos do Art. 34 do Decreto nº 7.724/2012, que tem a atribuição de assessorar, opinar, propor e subsidiar a autoridade classificadora;
- g) Confidencialidade: garantia de que a informação é acessível somente por usuários autorizados;
- h) Desclassificação: cancelamento da classificação atual de um ativo de informação pela autoridade competente ou por transcurso de prazo;
- i) Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
- j) Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
- k) Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- l) Informação Classificada em grau de sigilo: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassegreda, secreta ou reservada, em consonância com a Lei nº 12.527/2011;
- m) Informação Pessoal: aquela relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
- n) Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade, do Estado ou da Empresa, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- o) Informação ostensiva: é a informação não-sigilosa relacionada com as hipóteses do dever – por parte do gestor – de praticar a transparência ativa (dever de publicidade) e a transparência passiva (dever de prestar a informação solicitada);

- p) Integridade: qualidade da informação sobre a qual se tenha certeza de sua não modificação, inclusive quanto à origem, trânsito e destino;
- q) Marcação: ação de inscrever, no documento ou repositório, o grau de sigilo associado à informação sigilosa, classificada ou não;
- r) Reclassificação: alteração da classificação do ativo de informação pela autoridade classificadora;
- s) Reservado: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 05 (cinco) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado;
- t) Secreto: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 15 (quinze) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado;
- u) Segredo de Negócio: informação sigilosa relacionada à atividade econômica exercida pela AC NACIONAL cujo vazamento possa afetar o equilíbrio do negócio, seja em termos de vantagem competitiva, ou que possa de algum modo prejudicar o planejamento e a execução dos serviços, nos termos da Lei de Propriedade Industrial (Lei nº 9.297/2001, código penal, Lei nº 12.737);
- 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;
- w) Ultrassegredo: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 25 (vinte e cinco) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado; e
- x) Usuário: qualquer empregado, estagiário, adolescente aprendiz, contratado ou preposto contratado (terceirização), cliente ou fornecedor que detenha autorização para acesso e uso, por qualquer meio, aos ambientes de TIC DA AC NACIONAL.

4. DETERMINAÇÕES

4.1. A informação será protegida visando assegurar sua disponibilidade, autenticidade, integridade e confidencialidade. A AC NACIONAL exercerá a publicidade de seus atos como preceito geral e o sigilo como exceção, em duas modalidades diversas:

a) o sigilo decorrente do disposto na Lei de Acesso à Informação (Lei nº 12.527/2011);

b) o sigilo decorrente de legislação específica, conforme estabelecido pela própria Lei de Acesso à Informação;

4.2. Informação sigilosa classificada em grau de sigilo em conformidade pela Lei nº 12.527/2011

4.2.1 As informações podem ser classificadas com grau de sigilo “ultrassegredo”, “segredo” ou “reservado”, em função do seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado.

4.2.1.1 A informação gerada pela AC NACIONAL, que não for passível de divulgação, poderá ser classificada com os seguintes graus de sigilo:

a) “segredo”; ou

b) “reservado”.

4.2.2 A informação poderá ser classificada com grau de sigilo “segredo” ou “reservado” quando for considerada imprescindível à segurança da sociedade ou do Estado, e cuja divulgação e acesso irrestrito possam:

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

b) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País;

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

d) pôr em risco a vida, a segurança ou a saúde da população;

e) oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

f) prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

g) 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;

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

i) comprometer as atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

4.2.3 São passíveis de classificação com grau de sigilo “secreto” e “reservado”, as informações cuja restrição, a critério da autoridade competente que as trate (conforme item 4.5.2), lhes seja conferida de modo fundado e documentado, mediante preenchimento dos documentos e observância dos requisitos adiante tratados.

4.3 Informação sigilosa protegida por legislação específica.

4.3.1 As informações cujo sigilo decorre de outras hipóteses previstas em legislação específica, somente serão classificadas em grau de sigilo se atenderem ao disposto no item 4.2.2, devendo, em hipótese contrária, ser tratadas nos termos das respectivas leis.

4.3.1.1 São consideradas sigilosas, as informações protegidas em legislação específica, a exemplo do sigilo profissional, do sigilo fiscal ou do sigilo bancário, do segredo de negócios, do segredo de justiça dentre outras, conforme Anexo 4 – Quadro Exemplificativo de Tipos de Informação Sigilosa e de Embasamento Legal.

4.3.2 A informação de cliente custodiada pela AC NACIONAL é considerada sigilosa, por identificar-se com o conteúdo da locução “elementos manipulados” do Art. 8º da Lei nº 5.615/1970, salvo se houver sido previamente classificada em grau de sigilo pelo cliente.

4.3.3 A informação que envolva potencial violação de segredo industrial, comercial ou de negócio, gerando risco ou perda efetiva de vantagem competitiva para a AC NACIONAL, de acordo com o Art. 22 da Lei nº 12.527/2011 é considerada sigilosa.

4.3.4 As informações sigilosas protegidas por outras hipóteses legais de sigilo, terão seu prazo de restrição de acesso observado na conformidade de cada disposição legal específica.

4.4 Informação pessoal

4.4.1 As informações pessoais terão acesso restrito apenas ao titular e aos que a manipulam por necessidade de serviço, independente de eventual sobreposição de outras restrições (sigilo ou classificação em grau de sigilo).

4.4.2 Será facultado ao empregado ou aos prestadores de serviço, aos estagiários, aos requisitados e aos dirigentes que o solicitem o acesso a documentos e a suportes físicos contendo os próprios dados pessoais e funcionais ou o acesso aos dados de terceiros quando houver ordem judicial nesse sentido, ou em casos de previsão legal ou autorização do titular.

4.4.3 O acesso a informações pessoais deve ser tratado em conformidade com o prescrito nos Arts. 55 a 62 do Decreto nº 7.724/2012, no tocante a restrição de acesso a agentes autorizados, acesso limitado a terceiros mediante autorização prévia do titular, observância do direito de acesso ao cônjuge, ascendentes e descendentes, respeito aos direitos fundamentais de privacidade, intimidade e proteção à imagem, inexistência de restrição de acesso em caso de apuração de irregularidades ou levantamento de fatos históricos, devido processo legal, uso de termo de responsabilidade, trato de informação das entidades do terceiro setor, responsabilidade do agente público etc., de acordo com o disposto nos Art. 55 a 62 do Decreto nº 7.724/2012.

4.4.4 As informações pessoais têm prazo de restrição de acesso de 100 anos.

4.5 Classificação por grau de sigilo, prazo de sigilo, reclassificação e desclassificação

4.5.1 O critério para classificação de uma informação DA AC NACIONAL nos graus de sigilo “secreto” e “reservado” deve restringir-se ao indispensável, considerando que é adotado como preceito geral a publicidade e o sigilo como exceção

4.5.2 Terão competência para classificar, reclassificar e desclassificar as informações, no âmbito DA AC NACIONAL, por grau de sigilo:

a) “secreto”: o Diretor-Presidente;

b) “reservado”: o Diretor-Presidente, o Diretor-Superintendente, os Diretores, sendo possível a delegação.

4.5.2.1 O limite de possibilidade para a delegação de que trata a alínea “b”, do item 4.5.2 corresponde, nos termos da Lei, aos cargos equivalentes ao nível DAS 101.5.

4.5.2.1.1 A competência equivalente, no âmbito DA AC NACIONAL, em fevereiro de 2016, é a dos ocupantes de função comissionada do nível GFC 46 do Grupo II da Tabela de Gratificação de Função de Confiança.

4.5.2.1 É vedada, nos termos do Decreto nº 7.724/2012, Art. 30, § 1º, a delegação da competência de classificação no grau de sigilo “secreto”.

4.5.2.2 A autoridade que classificar informação no grau de sigilo “secreto” ou “reservado” deverá, nos termos do Decreto nº 7.724/2012, Art. 31, preencher o

Termo de Classificação de Informação – TCI conforme Anexo 1 – Termo de Classificação da Informação - TCI.

4.5.2.2.1 No caso do documento “secreto” o TCI preenchido deve ser encaminhado à Comissão Mista de Reavaliação de Informações, no prazo de 30 (trinta) dias corridos, contados a partir da data de classificação.

4.5.3 Os prazos máximos de classificação vigoram a partir da data de sua produção e são os seguintes, de acordo com o grau de sigilo:

a) “secreto”: 15 (quinze) anos;

b) “reservado”: 5 (cinco) anos;

4.5.3.1 Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, seja relativamente ao termo do prazo original ou ao termo do prazo de prorrogação, a informação será desclassificada.

4.5.3.2 O prazo máximo de classificação em grau de sigilo poderá ser prorrogado por uma única vez. 4.5.3.3 A classificação das informações será reavaliada pela autoridade classificadora, por autoridade hierarquicamente superior ou por Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS, por força de ofício ou mediante solicitação, com vistas à sua reclassificação ou desclassificação.

4.5.4 Termo de Classificação da Informação - TCI

4.5.4.1 A classificação de informação nos graus de sigilo “secreto” ou “reservado” deverá ser formalizada no Termo de Classificação de Informação – TCI conforme Anexo 1.

4.5.4.2 O Termo de Classificação de Informação – TCI, conforme Anexo 1, será mantido com o mesmo grau de sigilo da informação classificada.

4.5.4.3 O Termo de Classificação de Informação - TCI, conforme Anexo 1, deverá conter o histórico dos eventos relativos a ratificação, desclassificação e reavaliação do grau de sigilo da informação.

4.5.4.4 Cada documento classificado com grau de sigilo “secreto” ou “reservado”, deverá possuir uma numeração própria, conhecida como “Código de Indexação de Documento que contém Informação Classificada (CIDIC)”, conforme Anexo 2 - Formato de Apresentação do CIDIC.

4.5.4.4.1 O código CIDIC é um código exclusivamente numérico e é gerado pela Área responsável pela gestão da publicação do rol de informações classificadas e desclassificadas e de relatórios estatísticos sobre a Lei nº 12.527/2011.

4.6 Proteção e controle de informações sigilosas

4.6.1 A geração, o acesso, a divulgação e o tratamento de informação pessoal, sigilosa (classificada ou não) ficarão restritos às pessoas que tenham necessidade de conhecê-la por dever de ofício e que sejam devidamente autorizadas pelo Titular da Unidade Organizacional responsável por sua guarda e manipulação.

4.6.2 O acesso à informação sigilosa, classificada ou não, cria a obrigação para aquele que a obteve de resguardar seu sigilo.

4.6.3 A pessoa física ou entidade privada que, em razão de qualquer vínculo com a AC NACIONAL, executar atividade de tratamento de informação sigilosa adotará as providências necessárias para que seus empregados, contratados, prepostos ou representantes observem as condições estabelecidas entre as partes em termo de sigilo, conforme modelo do Anexo 3 – Modelo de Termo de Compromisso de Manutenção de Sigilo – TCMS.

4.6.4 Nas reuniões em que serão produzidas ou manipuladas informações sigilosas, pessoais e classificadas deverão ser adotados controles de segurança para acesso ao ambiente, aos documentos, às anotações, às mídias e aos demais recursos utilizados.

4.6.5 Caberá às Unidades Organizacionais coordenar o adequado tratamento a ser dado às informações sigilosas, pessoais e classificadas e zelar para que sejam armazenadas e arquivadas em ambiente com acesso restrito e controlado.

4.6.6 No caso dos documentos classificados com grau de sigilo, a despeito da obrigatoria marcação e da obrigatoria forma de tratamento, a origem do sigilo decorre da Lei e da natureza da informação e não da “marcação”, em si.

4.6.7 Para os documentos sigilosos e pessoais não-classificados, o sigilo decorre de Lei, enquanto que sua marcação e tratamento, no âmbito DA AC NACIONAL, podem ser definidos pelo Titular da Unidade Organizacional, em cada caso concreto.

4.7 Marcação de ativos de informação sigilosa

4.7.1 Marcação de documentos classificados como “secreto” e “reservado”

4.7.1.1 Documentos classificados devem receber a seguinte marcação:

- a) em todas as páginas do documento e nas capas, se houver, no cabeçalho e no rodapé;
- b) as páginas devem ser numeradas seguidamente, devendo cada uma conter, também, a indicação do total de páginas que compõem o documento; e
- c) a marcação em extratos de documentos, rascunhos, esboço e desenho sigiloso deve obedecer ao prescrito nos itens anteriores.

4.7.1.2 Os meios de armazenamento portáteis de dados (tipo pendrive, DVD e outros) devem receber a marcação obrigatoria correspondente à informação ali contida em local visível e adequado, sem prejuízo dos devidos controles de acesso.

4.7.1.3 Os meios de armazenamento de informação classificada em repositório não-portável receberão a marcação obrigatoria pela forma mais adequada, inclusive mediante aplicação de rótulo na interface do controle de acesso respectivo.

4.7.2 Marcação de documentos sigilosos não classificados

4.7.2.1 Os documentos pessoais ou que contenham informações protegidas por legislação específica, conforme disposto no item 4.3, e as informações pessoais (Art. 31 da Lei de Acesso à Informação) serão tratados nos termos da lei que rege tal hipótese de sigilo, embora possam, a critério do Titular da Unidade Organizacional, receber marcação e tratamento específicos compatíveis com a Lei de origem e com a natureza da informação protegida.

4.7.2.1.1 A marcação para os documentos de que trata o item 4.7.1.2 poderá ser feita facultativamente, a critério do Titular da Unidade Organizacional, mediante o uso da expressão “sigiloso”.

4.7.2.1.2 A marcação, caso seja determinada, deve ser feita em todas as páginas do documento e nas capas, se houver, apenas no cabeçalho.

4.7.2.2 O caráter “facultativo” da marcação não desobriga o gestor de observar:

- a) adequação do caso concreto com a Lei que o fundamenta;
- b) ausência de ambiguidade na marcação;
- c) a prevenção de marcações paradoxais;
- d) a prevenção de qualquer confusão com as marcações legais obrigatórias (informação sigilosa classificada) e com as demais marcações opcionais (informação sigilosa não classificada); e) tratamento coerente com a hipótese de sigilo; e
- f) abstenção de uso da palavra “sigiloso” para qualquer outra hipótese restritiva que não se enquadre nas hipóteses constantes do Anexo 3 – Quadro Resumo de Tipos de Informação Sigilosa e de Embasamento Legal.

4.7.2.3 A decisão discricionária sobre aplicar ou não a marcação de que trata o subitem anterior não implica dúvida sobre a natureza sigilosa do objeto de marcação, que decorre, em qualquer caso, das respectivas Leis.

4.7.2.4 O gestor deve zelar, em seu ambiente de trabalho, para que seus colaboradores não atuem de forma contraditória com o tratamento da informação sigilosa, aplicando tratamento adequado também aos esboços, rascunhos, provas, lembretes e informações paralelas e correlatas ao objeto de sigilo.

4.7.2.5 Os meios de armazenamento portáteis de dados podem opcionalmente receber a marcação correspondente à informação ali contida em local visível e adequado, sem prejuízo dos devidos controles de acesso.

4.7.2.6 Os meios de armazenamento de informação sigilosa em repositório nãoportável receberão a marcação facultativa pela forma mais adequada, inclusive mediante aplicação de rótulo na interface do controle de acesso respectivo.

4.8 Tratamento de documentos sigilosos

4.8.1 O tratamento da informação sigilosa, que não é tão regrado como o tratamento da informação classificada, deve ser objeto de cuidado e de definições, ritos e processos estabelecidos pelo Titular da Unidade Organizacional, de modo a atender à demanda da Lei

específica e a não frustrar os princípios fundantes estabelecidos na Lei de Acesso à Informação, o que implica guarda adequada, uso de mecanismos de proteção, criptografia, quando seja o caso, adoção de ambiente restrito e controlado.

4.8.2 Ferramentas corporativas que forneçam opção de criptografia para conteúdos definidos na respectiva política e normas de segurança (uso seguro do correio etc.) podem ser utilizados independentemente de o documento ser classificado ou sigiloso, mas sua utilização deve se restringir a conteúdo objeto de serviço e em hipótese alguma a conteúdo de natureza particular.

4.8.3 O Titular da Unidade Organizacional que constitua repositório inadequado à guarda segura de informação sigilosa sujeita-se à responsabilidade decorrente de sua escolha.

4.9 Uso e disseminação de documentos sigilosos

4.9.1 Uso e disseminação de documentos classificados

4.9.1.1 Os documentos classificados como “secreto” ou “reservado”, quando da expedição e comunicação, devem obedecer às seguintes prescrições:

- a) ser acondicionados em envelopes duplos;
- b) não constar qualquer indicação do grau de sigilo ou do teor do documento no envelope externo;
- c) ser apostos o destinatário e a marcação “secreto” ou “reservado”, de modo a serem identificados logo que removido o envelope externo;
- d) fechar, lacrar e expedir o envelope interno mediante recibo, que deve indicar, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento; e

e) inscrever a palavra PESSOAL no envelope externo sempre que o assunto for considerado de interesse exclusivo e pessoal do destinatário;

4.9.1.2 A comunicação de documento “secreto” ou “reservado” pode ser feita por outros meios, desde que sejam utilizados recursos de criptografia compatíveis com o grau de sigilo do documento, conforme previsto nos Art. 28 e 40 do Decreto nº 7.845/2012.

4.9.1.3 O encaminhamento de informação via documento “secreto” ou “reservado” pode ser feita por outros meios que não “físicos”, desde que sejam utilizados recursos de criptografia

compatíveis com o grau de sigilo do documento, conforme previsto nos Art. 28 e 40 do Decreto nº 7.845/2012.

4.9.1.4 A adoção corporativa de qualquer ferramenta ou recurso de criptografia é vedada, salvo com prévia autorização da COGSI e disponibilidade do algoritmo de controle depositado na unidade competente à disposição da Coordenação-Geral de Gestão da Segurança da Informação - COGSI, de modo a garantir a possibilidade de superação da proteção, para fins de forense computacional ou para adoção de medidas de competência das áreas táticas de segurança.

4.9.1.5 O acesso às áreas, instalações e materiais que contenham informações classificadas como “secreto” e “reservado” ou que demandem proteção, nos termos da seção VIII do capítulo III do Decreto 7.845/2012 deve ser regulado e tratado de forma compatível, com acesso restrito e controlado, de acordo com o disposto no referido Decreto.

4.9.2 Uso e disseminação de documentos sigilosos não-classificados

4.9.2.1 As informações sigilosas podem ser acessadas pelos usuários destinatários, de acordo com decisão do agente gerador do documento sigiloso e limitado pelos sistemas de controle de acesso, inclusive criptografia comum autorizada, quando seja o caso.

4.9.2.2 Os documentos sigilosos são de circulação interna controlada no âmbito da AC NACIONAL e de acesso restrito aos que tenham necessidade de saber e atributo de acesso.

4.9.2.2.1 Em situações excepcionais, o agente gerador do documento sigiloso pode encaminhar o documento a usuários externos à AC NACIONAL, com os devidos controles e garantia de rastreabilidade.

4.10 Reprodução de documentos classificados

4.10.1 A reprodução do todo ou de parte de documento “secreto” ou “reservado” deve ter o mesmo grau de sigilo do documento original.

4.10.2 O responsável pela produção ou reprodução de documento “secreto” ou “reservado” deve providenciar a eliminação de notas manuscritas, carbonos, provas ou qualquer outro recurso, que possam dar origem a cópia não autorizada do todo ou parte.

4.10.3 Sempre que a preparação, impressão ou, se for o caso, reprodução de documento “secreto” ou “reservado” for efetuada em tipografias, impressoras, oficinas gráficas ou

similares, essa operação deve ser acompanhada por agente credenciado ou que tenha assinado o TCMS, que será responsável pela garantia do sigilo durante a confecção do documento, observado o disposto no item anterior.

4.10.4 A reprodução do todo ou de parte de mídia magnética, óptica e eletrônica contendo dados classificados como “secreto” ou “reservado” deve ter o mesmo grau de sigilo do original.

4.10.5 O responsável pela reprodução deve ser agente credenciado ou que tenha assinado o TCMS, e deve manter o sigilo da operação, observado o disposto no item anterior.

4.10.6 Os arquivos temporários porventura gerados durante o processo de produção do documento devem ser eliminados ao final da operação.

4.11 Registro, tramitação e guarda de informação classificada

4.11.1 As informações classificadas com grau de sigilo “ultrassecreto”, “secreto” ou “reservado” em sistemas de informação devem:

- a) ser armazenadas em equipamento, ambiente ou estrutura que ofereça grau de segurança compatível com grau de sigilo;
- b) utilizar sistema de tecnologia da informação atualizado de forma a prevenir ameaças de quebra de segurança;
- c) utilizar canal seguro isolado física ou logicamente, além de controle de acesso adequado se o equipamento, ambiente ou estrutura estiver conectado a Internet ou rede interna;
- d) utilizar recursos criptográficos adequados ao grau de sigilo; e
- e) garantia de autenticidade do usuário mediante certificado digital.

4.11.2 Cabe ao responsável pelo recebimento de documento “ultrassecreto”, “secreto” ou “reservado”:

- a) verificar a integridade e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao seu superior hierárquico e ao destinatário, o qual deve informar imediatamente ao remetente;
- b) proceder o registro do documento e o controle de sua tramitação, mediante cadastramento enumerado no sistema corporativo de recebimento de correspondência externa sem intromissão ou violação de seu conteúdo ou de seu sigilo classificado;

b.1) o tratamento dado à correspondência classificada recebida deve garantir os mesmos requisitos de segurança prescritos na Lei e na regulamentação para tramitação segura da informação classificada em meios físicos;

c) abster-se de abrir o envelope interno da correspondência, que deve ser aberto exclusivamente pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior; c1) Nos casos em que o envelope interno traga a marca “PESSOAL”, representantes ou autoridades hierárquicas não estarão autorizados ao acesso;

d) comunicar o recebimento da correspondência ao remetente no menor prazo possível;

e) manter ou guardar os documentos sob condições especiais de segurança, pela forma protetiva previamente definida para essa finalidade; e

f) transmitir a guarda ou custódia de documentos, devidamente conferidos, quando da passagem ou transferência de responsabilidade em caso de substituição dos responsáveis.

4.12 Avaliação, preservação e eliminação

4.12.1 A atividade de avaliação quanto à manutenção da classificação original, reclassificação ou desclassificação deve ser realizada de modo idêntico ao descrito no item 4.5.

4.12.2 As informações classificadas com grau de sigilo “ultrassegredo”, “segredo” e “reservado” e seus respectivos documentos, não devem ser eliminados.

4.13 Eliminação de informação e documentos sigilosos não classificados

4.13.1 A eliminação de informações sigilosas não-classificadas ou de seu respectivo documento, pode ser feita desde que sejam observados os procedimentos e regras de preservação de documentos de guarda permanente (se for o caso) definidos pela área responsável pela gestão documental e arquivística, em conformidade com a Lei 8.159/2012 e sua regulamentação.

4.13.2 Para os documentos sigilosos não-classificados, a eliminação poderá ser feita quando do recebimento de autorização para tal emitida pelo Titular da

Unidade Organizacional, em observância aos procedimentos definidos pela área responsável pela gestão documental e arquivística e utilizando o processo de sanitização, na forma da Norma SG 027 – Sanitização de Dados em Ativos de Informação, quando couber.

4.13.3 A eliminação a que se refere o item 4.13 envolve os procedimentos de deleção segura (para documentos em meio eletrônico) e de trituração física (para documentos em papel).

4.14 Do tratamento da informação ostensiva com dever de transparência passiva e ativa

4.14.1 Independentemente da obrigação de o gestor tratar adequadamente a informação “não sigilosa” ou “ostensiva”, “sigilosa”, “pessoal” e “classificada em grau de sigilo”, deve, ainda assim, em atenção ao disposto no Art. 6º, II, da Lei 12.527/2011, atuar no sentido de proteger a informação ostensiva, no âmbito da organização, no tocante à sua disponibilidade, autenticidade e integridade.

4.14.2 Sem prejuízo do princípio da transparência, que constitui regra, na Lei de Acesso à Informação, o Titular da Unidade Organizacional e os gestores das unidades atuarão também, no sentido de proteger a informação pública ostensiva com dever de transparência passiva, de acordo com seu juízo de oportunidade e conveniência, promovendo:

a) descrição e controle das informações de uso interno (normas, campanhas de divulgação, políticas, recomendações de trato de assuntos internos etc.);

b) descrição e controle das informações cuja não-disseminação seja conveniente ao negócio (regras de controle de acesso, senhas, topologias, plantas internas etc.); e

c) descrição por dever de lealdade (não-pessoal) aos objetivos do negócio, estabelecendo melhores práticas de proteção e resguardo de informações sensíveis imprescindíveis às práticas de gestão (questões gerenciais em trato, discussões estratégicas, estudos e ensaios para tomada de decisão etc.).

4.14.3 Na hipótese de haver demanda de informação do tipo tratado em 4.14.2 por via estranha à do “Sistema de Informação ao Cidadão” DA AC NACIONAL, o empregado ou o gestor que receber a demanda reportar-se-á, pelo percurso hierárquico da respectiva área, ao Titular da Unidade Organizacional para que este, consultando as instâncias técnicas e hierárquicas correlatas, adote as providências necessárias ao melhor tratamento possível da demanda.

4.14.4 Nas hipóteses de demanda formulada via “Sistema de Informação ao Cidadão”, o tratamento será aquele disciplinado na lei e nas regras de funcionamento da estrutura corporativa.

5. DISPOSIÇÕES FINAIS

5.0 Qualquer empregado que venha a extraviar ou constatar o extravio de documento ou informação sigilosa deverá comunicar, com brevidade, o fato à chefia imediata ou ao responsável pela custódia do documento ou da informação.

5.1.1 Idêntica providência deverá adotar o empregado que encontrar ou tiver conhecimento de documento ou informação sigilosa.

5.2 Os empregados responsáveis pela custódia de documentos, materiais, áreas e informações de natureza sigilosa estarão sujeitos às regras referentes ao sigilo profissional, em razão do ofício (dever de lealdade e probidade) e às regras referentes ao Código de Ética DA AC NACIONAL.

5.3 Os empregados que infringirem esta Norma estão sujeitos às penalidades constantes na Norma que trata do Regime Disciplinar – Apuração de Responsabilidades e Aplicação de Penalidades.

5.4 A cessão de documentos sigilosos à Administração Pública direta e indireta deverá ser avaliada pelo Titular da Unidade Organizacional, sob orientação da Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS.

5.5 Caberá a Superintendência de Logística, sob orientação da Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS, definir os controles para trâmite de documentos compatíveis com o grau de sigilo.

5.6 Caberá às Unidades de Operações definir os controles para armazenamento, tráfego, processamento e deleção segura das informações que se encontrem em meio eletrônico, ótico ou magnético, compatíveis com o grau de sigilo, de acordo com a norma SG 027 – Sanitização de Dados em Ativos de Informação.

5.7 Os recursos de criptografia citados nesta Norma deverão ser homologados pela Empresa, de modo geral, e, no caso de tratamento de informações classificadas em grau de sigilo, deverá ser utilizada criptografia baseada em algoritmo de Estado para cifração e decifração das informações classificadas com grau de sigilo “secreto” e “reservado”.

5.8 A autenticidade da identidade do usuário da rede que acesse informações classificadas com grau de sigilo “ultrassegredo”, “secreto” ou “reservado” deverá ser garantida, no mínimo, pelo uso de certificado digital e isolados ou ligados a canal de comunicação seguro e protegido por recursos criptográficos.

5.9 Os sistemas que tratam informações classificadas com grau de sigilo “secreto” e “reservado” deverão contar com controle e registro dos acessos e das transações realizadas.

5.10 Competirá às Unidades Organizacionais da Empresa definir o acervo de informações sigilosas inerentes à área de atuação e a forma de atuação.

5.11 Competirá às Unidades Organizacionais da Empresa, considerando o princípio valorativo da informação sigilosa, definir o perfil e competência de acesso ao respectivo acervo.

5.12 Competirá às Unidades Organizacionais da Empresa gestoras de sistemas e de ferramentas de suporte que sustentam a geração, a tramitação e a armazenagem de informação promover as adequações necessárias à implantação desta Norma.

5.13 Os casos não tratados nesta Norma deverão ser encaminhados à Coordenação Geral de Gestão da Segurança da Informação – COGSI que, ademais, prestará apoio e orientação às Unidades Organizacionais também no tocante ao disposto nos itens 5.10, 5.11 e 5.12.

5.14 O responsável pela gestão e publicação do rol de informações classificadas e desclassificadas providenciará perante as áreas competentes a aquisição ou desenvolvimento da ferramenta ou solução que gerará o número CIDIC de que trata o item 4.5.5.3.1, com oficialidade e auditabilidade, para efeito de cumprimento da lei e garantia de seus controles.

5.15 É vedado o uso de informação sigilosa em trabalhos acadêmicos ou técnico-científicos paralelos ao negócio DA AC NACIONAL, ainda que de boa-fé.

5.15.1 Havendo dúvida sobre a incidência de sigilo legal, o interessado poderá obter do Titular da Unidade Organizacional competente avaliação prévia, crítica e formal sobre a incidência de

sigilo e, mediante manifestação dessa autoridade, fazer uso pleno ou restrito da informação, conforme o caso, para os fins pretendidos.

5.16 A informação sigilosa ou a informação classificada que tramitem em meio digital, quando disponível tecnologia corporativa para tanto e no menor prazo possível, deverá ser tratada mediante implementação, gerenciamento e manutenção de metadados que garantam o controle de acesso, temporalidade, segregação de papéis, dentre outros atributos, de modo a que a crítica e identificação do documento sigiloso, como tal, ocorra necessariamente antes de acessos acidentais ou equívocos, prevenindo indisponibilidades, acessos indevidos, falhas de reavaliação do sigilo e de sua temporalidade.

ANEXO 1 – TERMO DE CLASSIFICAÇÃO DA INFORMAÇÃO – TCI

Unidade	Cód. Indexação	Data da publicação
Grau de Sigilo (4) <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; width: 60px; height: 30px; margin-right: 10px;"></div> <div style="display: flex; gap: 10px;"> <input type="checkbox"/> Secreto <input type="checkbox"/> Reservado </div> </div>	Categoria (5)	
Tipo de Documento (5) <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; width: 60px; height: 30px; margin-right: 10px;"></div> <div style="display: flex; gap: 10px;"> <input type="checkbox"/> Ofício <input type="checkbox"/> Carta <input type="checkbox"/> Memorando <input type="checkbox"/> Relatório <input type="checkbox"/> </div> </div> Outro: <u>(Especificar)</u>		
Prazo da Restrição de Acesso (9)	Data de Classificação o (8)	
Fundamento Legal para Classificação (6)		
Razões para a Classificação (7)		
Autoridade Classificadora (10) Nome: _____ Cargo: _____ Assinatura: _____		
Autoridade Ratificadora (11) Nome: _____		

Cargo: _____	
Assinatura: _____	
Desclassificação em (12) ____/____/____ —	Nome: _____ _____ _____
	Cargo: _____ _____ _____ Assinatura: _____ _____
Reclassificação em (13) ____/____/____ —	Nome: _____ _____ _____ Cargo: _____ _____ _____ Assinatura: _____ _____
Redução de prazo em (14) ____/____/____ —	Nome: _____ _____ _____ Cargo: _____ _____ _____ Assinatura: _____ _____
Prorrogação do prazo em (15) ____/____/____ —	Nome: _____ _____ _____ Cargo: _____ _____ _____ Assinatura: _____ _____

(Instrução de Preenchimento)

- (1) Unidade da AC NACIONAL: nome da unidade/área de emissão, ou responsável pela desclassificação, reclassificação, redução do prazo ou CPADS.
- (2) Código de Indexação: conforme Anexo 6.
- (3) Data de Produção: DD/MM/AAAA (data de criação do documento).
- (4) Grau de Sigilo: secreto ou reservado.
- (5) Categoria: categoria na qual se enquadra a informação de acordo com o VCGE – Vocabulário Controlado de Governo Eletrônico, conforme Anexo 2 – Formato de apresentação do CODIC.
- (5) Tipo de Documento: ofício, carta, memorando, relatório ou outro documento que deve ser especificado.
- (6) Fundamento Legal para Classificação: indicar o inciso do Art. 23 da Lei No. 12.527/2011 (item 4.2.2.1 da Norma).
- (7) Razões para a Classificação: motivo da classificação, desclassificação, reclassificação, ou redução do prazo.
- (8) Data de Classificação: DD/MM/AAAA, data em que a autoridade competente classificou a informação.
- (9) Prazo da Restrição de Acesso: DD/MM/AAAA
- (10) Autoridade Classificadora, contemplando:
 - Nome: nome completo da autoridade;
 - Cargo: cargo da autoridade.
- (11) Autoridade Ratificadora (quando aplicável), contemplando:
 - Nome: nome completo da autoridade responsável pelo ato;
 - Cargo: cargo da autoridade responsável pelo ato.
- (12) Desclassificação em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável desclassificou a informação, contemplando:
 - Nome: nome completo da autoridade responsável pelo ato;
 - Cargo: cargo da autoridade responsável pelo ato;

- Assinatura: assinatura da autoridade responsável pelo ato.

(13) Reclassificação em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável reclassificou a informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

(14) Redução do prazo em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável reduziu o prazo da classificação da informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

(15) Prorrogação do prazo em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável prorrogou o prazo da classificação da informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

ANEXO 2 - TÍTULO E FORMATO DE APRESENTAÇÃO DO CIDIC

O formato de apresentação do Código de Indexação de Documento que contém Informação Classificada (CIDIC) obedece às regras constantes neste Anexo, de acordo com os artigos 50 a 54 do Decreto nº 7.845/20122, cujo modelo é exemplificado é mostrado a seguir:

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 sequencial/ano-dig ver	U, S ou R	01 a 17	DD/MM/AAAA	DD/MM/AAAA	S ou N	DD/MM/AAAA
XXXXX	NNNNN/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							

1. A 1ª parte do CIDIC corresponde ao Número Único de Protocolo – NUP do documento que contém a informação.
2. A 2ª parte do CIDIC é separada da 1ª parte por um “.” e contém o seguinte formato:
 - a) Grau de sigilo – um caractere alfabético (“U”, “S” ou “R”), de acordo com o grau de sigilo ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível.
 - b) Categoria: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme tabela a seguir:

LIDERSIS SISTEMAS E TECNOLOGIAS DA INFORMAÇÃO Ltda.

CNPJ nº 11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras - Brasília (DF). CEP 71953-000 Telefone:(61) 3204-

4997 – Celular/Whatsapp: (61) 99245-3140 correspondente@acnacional.com.br Página 24 de 30

CATEGORIAS	CÓDIGO
	NUMÉRICO
Agricultura, extrativismo e pesca	1
Ciência, informação e Comunicação	2
Comércio, Serviços e Turismo	3
Cultura, Lazer e Esporte	4
Defesa e Segurança	5
Economia e Finanças	6
Educação	7
Governo e Política	8
Habitação, Saneamento e Urbanismo	9
Indústria	10
Justiça e Legislação	11
Meio ambiente	12
Pessoa, família e sociedade	13
Relações internacionais	14
Saúde	15
Trabalho	16
Transporte e trânsito	17

LIDERSIS SISTEMAS E TECNOLOGIAS

DA INFORMAÇÃO Ltda. CNPJ nº

11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras

- Brasília (DF). CEP 71953-000 Telefone: (61) 3204-4997 –

Celular/Whatsapp: (61) 99245-3140

correspondente@acnacional.com.br Página **26 de 31**

c) 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).

d) 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).

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

f) Reclassificação da informação resultante de reavaliação ou primeiro registro da classificação;

g) 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.

3. Os separadores utilizados serão: “.” e “/” (este último, 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 ultrassecreto, a nova data deverá constar no final da 2ª parte do CIDIC, totalizando 39 posições com caracteres alfanuméricos e separadores.

Termo de Compromisso de Manutenção de Sigilo – TCMS:

Eu, [nome completo da pessoa], [nacionalidade], CPF nº [número do CPF], documento de identificação nº [número do documento de identificação], emitido pelo [nome do Órgão

LIDERSIS SISTEMAS E TECNOLOGIAS
DA INFORMAÇÃO Ltda. CNPJ nº

11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras
- Brasília (DF). CEP 71953-000 Telefone: (61) 3204-4997 –
Celular/Whatsapp: (61) 99245-3140

correspondente@acnacional.com.br Página 27 de 31

Expedidor] na data [DD/MM/AAAA],

situado em [endereço], perante à Autoridade Certificadora NACIONAL, declaro ter ciência da legislação sobre o tratamento de informação classificada (Lei nº 12.527/2011, Decreto nº 7.724/2012 e Decreto nº 7.845/2012) cuja divulgação possa causar risco ou dano à segurança das informações da Empresa e de seus clientes, comprometendo-me a guardar o sigilo e a:

- a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pela AC NACIONAL 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;
- 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 DA AC NACIONAL, salvo autorização da autoridade competente.

LIDERSIS SISTEMAS E TECNOLOGIAS

DA INFORMAÇÃO Ltda. CNPJ nº

11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras

- Brasília (DF). CEP 71953-000 Telefone: (61) 3204-4997 –

Celular/Whatsapp: (61) 99245-3140

correspondente@acnacional.com.br Página 28 de 31

ANEXO 3 - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

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] – [UF], [dia] de [mês] de [ano].

[NOME COMPLETO DA PESSOA]

[nome completo da Testemunha 1]

[nome completo da Testemunha]

ANEXO 4 - QUADRO EXEMPLIFICATIVO DE TIPOS DE INFORMAÇÃO SIGILOSA E DE EMBASAMENTO LEGAL

Tipo	Característica	Embasamento Legal
Classificada em grau de sigilo	Classificada	
	Ultrassegredo - Prazo máximo de restrição de acesso de 25 anos	Art. 23 e 24 da Lei 12.527/2011
	Segredo - Prazo máximo de restrição de acesso de 15 anos	Art. 23 e 24 da Lei 12.527/2011
	Reservado - Prazo máximo de restrição de acesso de 5 anos	Art. 23 e 24 da Lei 12.527/2011
Protegida por legislação específica (*)	Sigilo decorrente do negócio DA AC NACIONAL	
	Elementos manipulados de cliente	Art. 8 da Lei 5.615/1970
	Sigilo decorrente de direitos de personalidade	
	Sigilo fiscal	Art. 198 da Lei 5.172/1966
	Sigilo bancário	Art. 1 da Lei 105/2001
	Sigilo comercial	§ 2 do Art. 155 da Lei 6.404/1976
	Sigilo empresarial	Art. 169 da Lei 11.101/2005
	Sigilo contábil	Art. 1.190 e 1.191 da Lei 5.869/1973
	Sigilo de processo e procedimentos	
	Segredo de justiça no processo penal	§ 6º do Art. 201 da Lei 3.689/1941
	Informação de natureza patrimonial	
	Segredo industrial (segredo de negócio)	Lei 9.279/1996 (Art. 22 da Lei 12.527/2011)
	Direito autoral	Lei 9.610/1998
	Propriedade intelectual - software	Lei 9.609/1998

LIDERSIS SISTEMAS E TECNOLOGIAS

DA INFORMAÇÃO Ltda. CNPJ nº

11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras

- Brasília (DF). CEP 71953-000 Telefone: (61) 3204-4997 –

Celular/Whatsapp: (61) 99245-3140

correspondente@acnacional.com.br Página 30 de 31

Pessoal	Prazo máximo de restrição de 100 anos quando se referir à intimidade, vida privada, honra e imagem	Art. 31 da Lei 12.527/2011
	Restrição discricionária de acesso a documento preparatório	§ 3º do Art. 7 da Lei 12.527/2011
	Sigilo do procedimento administrativo disciplinar em curso	Art. 2º, V, e 46 da Lei 9.784/1999
	Sigilo de inquérito policial	Art. 20 da Lei 3.689/1941
	Segredo de justiça no processo civil	Art. 155 da Lei 5.869/1973

**LIDERSIS SISTEMAS E TECNOLOGIAS
DA INFORMAÇÃO Ltda. CNPJ nº**

11.717.421/0001-54

Edifício Pátio Capital, Sala 1309. QS 03 Lotes 3/9. Bairro Águas Claras
- Brasília (DF). CEP 71953-000 Telefone: (61) 3204-4997 –
Celular/Whatsapp: (61) 99245-3140

correspondente@acnacional.com.br Página **31** de **31**