



## 1. FINALIDADE

- 1.1. Estabelecer os preceitos para a Gestão da Informação de natureza pública e sigilosa, no âmbito da Casa da Moeda do Brasil – CMB.

## 2. ABRANGÊNCIA

- 2.1. Administradores, Empregados da CMB, Terceirizados, Jovens Aprendizizes Estagiários e qualquer cidadão ou entidade, pública ou privada que venham a produzir ou usufruir de informações da CMB em suas dependências ou fora destas.

## 3. REFERÊNCIAS

- 3.1. Decreto nº 7.724, de 16 de maio de 2012;
- 3.2. Lei nº 6.404, de 15 de dezembro de 1976;
- 3.3. Lei nº 10.406, de 10 de janeiro de 2002 – Código Civil;
- 3.4. Lei nº 11.101, de 09 de fevereiro de 2005;
- 3.5. Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional;
- 3.6. Lei Complementar nº 105, de 10 de janeiro de 2001;
- 3.7. Lei nº 9.279, de 14 de maio de 1996;
- 3.8. Lei nº 9.609, de 19 de fevereiro de 1998;
- 3.9. Lei nº 9.610, de 19 de fevereiro de 1998;
- 3.10. Lei nº 12.527, de 18 de novembro de 2011;
- 3.11. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
- 3.12. Consolidação das Leis de Trabalho - CLT;
- 3.13. Constituição da República Federativa do Brasil de 1988 - CRFB.
- 3.14. Política de Segurança da Casa da Moeda do Brasil - CMB.

## 4. CONCEITOS

- 4.1. Para efeitos desta Norma consideram-se os seguintes conceitos:
  - 4.1.1. Acesso à Informação: direito de qualquer pessoa, física ou jurídica, de obter informações produzidas ou custodiadas pela Administração Pública, observado o disposto na Lei nº 12.527/2011 e no Decreto nº 7.724/2012, independentemente de motivação, de forma gratuita, ressalvadas as hipóteses de sigilo legal ou de restrição de acesso previstas na legislação;
  - 4.1.2. Classificação da Informação: no âmbito da Lei de Acesso à Informação, entende-se como ato da autoridade classificadora, a prática, de ofício ou por

provocação, de atribuir, alterar ou suprimir o grau de sigilo de uma informação. Esse ato pode se materializar nas seguintes modalidades:

- I. Classificação: atribuição inicial do grau de sigilo a uma informação;
- II. Desclassificação: cancelamento de qualquer grau de sigilo atribuído;
- III. Reclassificação: alteração do grau de sigilo anteriormente atribuído;
- IV. Reavaliação: altera o prazo de sigilo, mantendo-se o grau previamente estabelecido.

- 4.1.3. Conceito do menor privilégio: concessão de autorizações estritamente em função da necessidade do desempenho de uma atividade ou fim específico;
- 4.1.4. Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada nem credenciada;
- 4.1.5. Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
- 4.1.6. Documento arquivístico: documento produzido (elaborado ou recebido) independente do formato, do suporte ou natureza, no curso de uma atividade prática, como instrumento ou resultado de tal atividade e retido para ação ou referência;
- 4.1.7. Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
- 4.1.8. Gestão da Informação: processo de negócio (macroprocesso) cujo escopo é gerir adequadamente as informações criadas na empresa e as informações recebidas de entes externos com a devida proteção da informação, considerando os aspectos legais e de negócio. A gestão da informação contempla os seguintes processos:
  - I. Classificação da Informação, segundo a LAI e segundo legislação própria que resguarde sigilo;
  - II. Tratamento da Informação;
  - III. Disponibilização da Informação;
  - IV. Publicação da Informação;
  - V. Acesso à Informação.
- 4.1.9. Informação sigilosa: informação submetida, temporariamente, à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, bem como aquelas protegidas por outras hipóteses

legais de sigilo, nos termos da Lei nº 12.527/2011 e do Decreto nº 7.724/2012;

- 4.1.10. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- 4.1.11. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- 4.1.12. Proteção da Informação: garantir a disponibilidade, autenticidade e integridade adequada da informação;
- 4.1.13. Requerimentos: demandas formalmente apresentadas ao Serviço de Informação ao Cidadão - SIC da CMB, nos termos da Lei nº 12.527/2011 e do Decreto nº 7.724/2012, que podem consistir em:
  - I. Pedidos de acesso a informações;
  - II. Recursos contra decisão de indeferimento de acesso ou não fornecimento das razões da negativa;
  - III. Pedidos de desclassificação e reclassificação de informações;
  - IV. Reclamações contra omissões no regular processamento dos requerimentos elencados de “I” a “III”.
- 4.1.14. Responsável pela informação (Proprietário da Informação): indivíduo responsável por assegurar que as informações e os ativos associados aos recursos de processamento da informação estejam adequadamente classificados;
- 4.1.15. Rotulação da informação: identificação aplicada nos documentos, onde constam o nível de classificação, a hipótese legal que subsidia a classificação, o responsável pela informação e o grupo de acesso atribuído às mesmas;
- 4.1.16. Tratamento da informação: conjunto de ações referentes à produção, recepção, autuação, tramitação, acesso, reprodução, publicação e guarda da informação;
- 4.1.17. Termo de Classificação de Informação – TCI: documento padronizado, elaborado pela autoridade classificadora competente, que formaliza a atribuição de grau de sigilo a uma informação, contendo, no mínimo, o assunto, a categoria na qual se enquadra, o fundamento legal, a data da classificação, o prazo de sigilo e a identificação da autoridade que a classificou, nos termos da Lei nº 12.527/2011 e do Decreto nº 7.724/2012.

## 5. ORIENTAÇÕES GERAIS

### 5.1. Classificação da Informação, segundo a LAI:

- 5.1.1. A classificação da informação deve ser feita buscando o grau menor de sigilo possível, considerando sua imprescindibilidade quanto à segurança da sociedade ou do Estado, os efeitos que a atribuição de determinada classificação trará às atividades da CMB, aos órgãos externos interessados e à sociedade em geral;
- 5.1.2. A classificação deverá ser realizada pela autoridade competente quando a informação gerada lhe for apresentada, observada a data da produção da informação e os procedimentos estabelecidos nesta Norma;
- 5.1.3. Deverá ser preservado o sigilo em relação à informação classificada como Ultrassegreda, Segreda, ou Reservada por outro órgão ou entidade competente para tanto;
- 5.1.4. A classificação das informações, segundo a LAI, será realizada pelas autoridades competentes conforme graus determinados a seguir:

V. Ultrassegredo: Ministro de Estado;

VI. Segredo: Presidente da CMB;

VII. Reservado: Diretores, podendo ser delegada aos Superintendentes, vedada a subdelegação.

- a) As informações que devam ser classificadas em graus de sigilo secreto e ultrassegredo devem necessariamente passar pelos graus inferiores, reclassificando-se por requerimento da autoridade de menor grau hierárquico até que se obtenha, caso concordem as autoridades subsequentes, o grau de sigilo adequado;
- b) As informações que devam ser classificadas no grau ultrassegredo serão remetidas pelo Presidente da CMB ao Ministro da Economia para reclassificação, devidamente fundamentadas e já classificadas como segredas;
- c) As informações que devam ser classificadas no grau secreto serão remetidas pela Diretoria do Departamento responsável ao Presidente da CMB para reclassificação, devidamente fundamentadas e já classificadas como reservadas;
- d) O Presidente da CMB, após classificar uma informação no grau de secreto de que trata a LAI submeterá cópia do respectivo TCI à

- Comissão Mista de Reavaliação de Informações, no prazo de 30 (trinta) dias, conforme dispõe o artigo 32, do Decreto 7.724/2012;
- e) A classificação de informação de que trata o subitem 5.1.4.III, deverá ser informada à Autoridade de Monitoramento da LAI no âmbito da CMB, no prazo de 30 (trinta) dias.
- 5.1.5. Os prazos máximos de restrição de acesso à informação são os seguintes:
- I. Ultrassecrta: 25 (vinte e cinco) anos;
  - II. Secreta: 15 (quinze) anos;
  - III. Reservada: 5 (cinco) anos.
- a) Alternativamente aos prazos previstos acima, 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.
- 5.1.6. A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou ofício, nos termos do Decreto 7.724/2012, para desclassificação, reclassificação ou redução do prazo de sigilo.
- 5.2. Classificação da Informação segundo legislação própria que resguarde sigilo e que trate da confidencialidade das informações de direito privado da CMB:
- 5.2.1. Na classificação da informação submetida ao regime jurídico de direito privado, deve-se buscar o grau de sigilo menos restrito possível, considerando a informação que, se divulgada, puder causar risco de desvantagem à CMB em relação aos seus concorrentes no mercado;
- 5.2.2. O processo de Classificação da Informação consiste em: Classificação, Rotulação e Tratamento;
- 5.3. Toda informação no âmbito da CMB, principalmente a que puder conferir vantagem competitiva, controle estratégico a outrem, e/ou puder comprometer a atuação da CMB deve ser classificada no momento de sua criação, por ocasião da inclusão em um processo ou em algum ambiente da CMB ou quando for identificado que ainda não possui uma classificação;
- 5.4. A informação deve ser classificada de acordo com a sua natureza e sensibilidade para o adequado controle do acesso;
- 5.5. A informação que não passou pelo processo de classificação é considerada informação não classificada, devendo ser classificada imediatamente quando manipulada;

- 5.6. A classificação deve ser feita pelo empregado que cria ou manipula inicialmente a informação, sendo a esse empregado atribuído o papel de responsável pela informação.
- 5.6.1. No caso de substituição do responsável pela informação, o novo titular deve receber as mesmas permissões que o anterior sobre as informações classificadas.
- 5.7. O acesso à informação classificada deve ser restrito às pessoas que dela necessitam para o desempenho de suas atividades de trabalho;
- 5.8. Para classificação da informação na CMB, ficam estabelecidos os seguintes níveis de classificação:

| Níveis de Classificação    | Descrição                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Público<br>(Verde)         | Informações que podem ou devem ser divulgadas publicamente por interesse da CMB. Ex.: Informações divulgadas à sociedade, mídias de comunicação externas, ao mercado etc.                                                                                                                                                  |
| Interno<br>(Laranja)       | Informações que devem ser divulgadas apenas internamente, a colaboradores, determinados grupos ou áreas. Ex.: Normas corporativas, campanhas internas, informações de projetos, pesquisas de mercado, relatórios de desempenho, indicadores das áreas etc.                                                                 |
| Confidencial<br>(Vermelho) | Informações acessíveis apenas para pessoas selecionadas e que requerem tratamento especial, cuja divulgação não autorizada ou acesso indevido pode comprometer segredos comerciais/industriais dos negócios da CMB, gerar prejuízos financeiros, legais, contratuais, bem como na reputação, imagem ou estratégias da CMB. |

- 5.9. Deve ser aplicado em local visível, de acordo com o meio onde se encontra a informação (Processos físicos, processos eletrônicos, e-mails, arquivos digitais etc.), um rótulo informando o nível de classificação, a hipótese legal (se aplicável), a data de classificação, o responsável pela classificação e os grupos de acesso padrão que possuem acesso a mesma;

- 5.10. O rótulo da informação, sempre que possível, deve receber cores equivalentes ao seu nível de classificação para facilitar a identificação da classificação;
- 5.11. Toda informação classificada deve receber controles físicos e lógicos adequados para preservar sua confidencialidade;
- 5.12. Documentos que contenham informações classificadas em diferentes níveis, devem receber a classificação mais restritiva existente em seu conteúdo;
- 5.13. Quando uma informação classificada for transmitida verbalmente, o responsável pela informação deve comunicar aos participantes da comunicação, o nível de classificação e os cuidados necessários para o tratamento.
- 5.14. Quando necessário, o responsável pela informação deve reclassificar a informação;
  - 5.14.1. Em caso de indisponibilidade do responsável pela informação, a reclassificação de uma informação pode ser realizada pelo seu superior imediato.
- 5.15. Para fins de compatibilidade com outras definições de classificação, o responsável pela informação deverá selecionar no sistema de destino, um grau de proteção igual ou superior ao que a informação foi classificada na CMB;
- 5.16. Feita a classificação e a correta identificação por meio da rotulação, qualquer pessoa que tiver acesso à informação, buscando preservar a sua disponibilidade, integridade e confidencialidade, deve certificar de fazer o tratamento adequado.
  - 5.16.1. São sigilos submetidos ao regime jurídico de direito privado e previstos em legislação própria, tais como:
    - I. Sigilo comercial/empresarial (artigo 155, §2º, Lei 6.404/76, artigo 169, Lei 11.101/2005, artigos 1.190 e 1.191 do Código Civil);
    - II. Sigilo fiscal (artigo 198 do Código Tributário Nacional);
    - III. Sigilo bancário (artigo 1º, Lei Complementar n.105/2001);
    - IV. Segredo Industrial (Lei 9.279/1996);
    - V. Direito Autoral (Lei 9.610/1998);
    - VI. Propriedade Intelectual (Lei 9.609/1998);
    - VII. Documentos preparatórios à decisão futura (artigo 7º, §3º, Lei 12.527/2011);
    - VIII. Sigilo de Processo Administrativo Disciplinar (artigo 29, §4º, CLT);
    - IX. Sigilo de informações pessoais (Lei nº 13.709/2018).

## 5.17. Das Informações da CMB Passíveis de Classificação

5.17.1. As informações, em regra, são públicas, porém as informações abaixo relacionadas devem ser observadas com especial atenção, pois podem merecer algum grau de sigilo:

- I. Impressão e acabamento automatizado de cédulas;
- II. Moedas do meio circulante brasileiro e moedas comemorativas;
- III. Informações técnicas de insumos de processos;
- IV. Especificações técnicas de processos, produtos e matérias primas referentes ao Banco Central do Brasil – BACEN, ao Departamento de Polícia Federal – DPF, ao Ministério de Relações Exteriores – MRE, à Receita Federal do Brasil – RFB, à Empresa Brasileira de Correios e Telégrafos – ECT e outras instituições clientes e/ou parceiras da CMB;
- V. Informações referentes a sistemas de rastreabilidade;
- VI. Documentos oriundos de Plano de Trabalho (acordo de cooperação técnica);
- VII. Projetos artísticos de cédulas e moedas nacionais e internacionais;
- VIII. Matrizes e processos de fabricação de matrizes de cédulas e moedas nacionais;
- IX. Processo de desenvolvimento e customização de sistemas, gestão de conteúdo e conhecimento, de infraestrutura e de Tecnologia da Informação e Comunicação – TIC;
- X. Processo de acompanhamento de projetos de investimento;
- XI. Processos (relatórios de atendimento; relatórios conclusivos; atas; depoimentos) e controles da Comissão de Ética;
- XII. Processos de Relatório de Auditoria Interna (contendo relatórios anuais e trimestrais, fluxogramas de processos ligados às estratégias de negócios, papéis de trabalho e plano de providência);
- XIII. Informações constantes do Plano Anual de Atividades de Auditoria Interna – PAINT;
- XIV. Informações constantes do Relatório Anual de Atividades de Auditoria Interna – RAINTE;
- XV. Registro da pesquisa de mercado;



XVI. Os valores constantes nos termos de referência nas licitações por pregão em que o pregoeiro entenda necessária sua preservação até o momento da fase da aceitação da proposta;

XVII. Procedimentos investigativos e processos correccionais.

## 6. DIRETRIZES

6.1. A classificação de informações, nos termos da Lei nº 12.527/2011 e do Decreto nº 7.724/2012, deverá ser realizada caso a caso, mediante análise individual e decisão fundamentada da autoridade competente, com registro no respectivo TCI.

6.2. É vedada a classificação genérica ou por categoria de documentos sem a devida justificativa.

6.2.1. Nas informações que não se sujeitam aos prazos de sigilo incluem-se os segredos industriais, comerciais e demais informações que, se divulgados, tragam desvantagem à CMB no mercado nacional e internacional.

6.3. A decisão de classificar uma informação, em qualquer grau de sigilo, nos termos da Lei nº 12.527/2011 e do Decreto nº 7.724/2012, deverá ser formalizada no Termo de Classificação da Informação – TCI, contendo, no mínimo:

6.3.1. Código de indexação de documento;

6.3.2. Grau de sigilo;

6.3.3. Categoria na qual se enquadra a informação;

6.3.4. Tipo de documento;

6.3.5. Data da produção do documento;

6.3.6. Indicação de dispositivo legal que fundamenta a classificação;

6.3.7. Razões de classificação;

6.3.8. Indicação do prazo de sigilo, contando em anos, meses ou dias, ou do evento que defina o seu termo final;

6.3.9. Data de classificação;

6.3.10. Identificação da autoridade que classificou a informação.

I. O TCI deverá acompanhar a informação classificada e ser assinado pela autoridade competente;

II. As razões de classificação previstas no inciso VII deverão receber o mesmo grau de sigilo atribuído à informação principal.

6.4. Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento tratamento do grau de sigilo mais elevado, ficando assegurado o acesso às partes não classificadas e/ou desclassificadas por meio de certidão, extrato ou cópia.

## 6.5. Tratamento da Informação

6.5.1. Quando do tratamento da informação sigilosa, devem ser atendidos, no mínimo, os seguintes requisitos e procedimentos:

- I. Rotular quanto ao sigilo classificado;
- II. Anexar o TCI;
- III. Incluir advertência sobre restrição de acesso, se aplicável;
- IV. Identificar usuários ou grupos de segurança autorizados;
- V. Identificar numeração e total em cada página, se aplicável;
- VI. Autorizar acesso apenas aos usuários previamente identificados;
- VII. Aplicar medidas de proteção lógica e física que garantam o acesso exclusivo pelos usuários autorizados;
- VIII. Manter sigilo sobre o conteúdo da informação para usuários não autorizados;
- IX. Transportar (interna e externamente) somente com autorização da autoridade classificadora ou autoridade hierarquicamente superior;
- X. Registrar em controle próprio o respectivo grau de sigilo;
- XI. No caso de eliminação, fazê-la de forma irrecuperável.
  - a) Poderá ser elaborado extrato, certidão ou cópia parcial com ocultação das partes sob sigilo de documentos sigilosos, para sua divulgação ou execução, mediante consentimento expresso da autoridade classificadora, autoridade hierarquicamente superior ou destinatária para dispor sobre o assunto;
  - b) Na ocorrência de perda efetiva ou suspeita de quebra de sigilo, deve-se comunicar formalmente à chefia imediata;
  - c) Os documentos e processos sigilosos serão inventariados anualmente, mediante lavratura de termo de inventário.

6.5.2. Cabe ao interessado, quando da entrega de documentação à CMB, formular, destacadamente, de modo a facilitar sua visualização, requerimento de tratamento reservado de informações ou de documentos que se enquadrem nas hipóteses desta Norma, apresentados em qualquer suporte.

- I. O requerimento referido acima será apreciado pela autoridade classificadora com competência para apreciar a informação recebida, que poderá confirmar a classificação do documento, dado ou informação como sigilosa, observadas as hipóteses previstas no subitem 5.3.1 desta Norma.

- 6.5.3. Os documentos e processos encaminhados à CMB originados de outros órgãos ou entidades públicas com chancela de sigilo tramitarão com esse caráter.
- I. Em caso de solicitação de desclassificação, reclassificação ou reavaliação de informação encaminhada à CMB, deverá ser informado ao requerente o órgão de origem responsável pela classificação.
- 6.6. Da Disponibilização da Informação
- 6.6.1. É assegurado o direito de acesso pleno a documentos públicos, observado o disposto na legislação em vigor, especialmente a LAI.
- 6.6.2. A CMB manterá, independentemente de classificação, acesso restrito a informações e documentos, que estejam sob seu controle e posse, que envolvam:
- I. Intimidade, vida privada, honra e imagem de pessoas;
- II. Sigilo fiscal, patrimonial e/ou bancário;
- III. Processos judiciais sob segredo de justiça;
- IV. Identificação de denunciante que tenha procurado a Ouvidoria da CMB – OUVID para relatar irregularidade;
- V. Relatórios e/ou notas técnicas decorrentes de atividades internas da CMB, quando ainda não concluídos;
- VI. Conteúdos de natureza técnica produzidos por outros órgãos e entidades, desde que estejam em poder da CMB, mas não possuam característica de custódia.
- 6.7. A classificação, desclassificação, reavaliação ou reclassificação de informação em qualquer grau de sigilo deverá ser formalizada no TCI.
- 6.7.1. Os atos de classificação, desclassificação, reavaliação ou reclassificação da informação, bem como o prazo de restrição de acesso determinado, devem sempre ser motivados;
- 6.7.2. Negado o pedido de desclassificação ou de reavaliação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de 10 (dez) dias, contado da ciência da negativa, ao Presidente da CMB;
- 6.7.3. A desclassificação de dados ou informações sigilosas será automática depois de transcorridos os prazos ou termos previstos na decisão de classificação.
- 6.8. Do Tratamento da Informação Sigilosa
- 6.8.1. O sigilo de uma informação classificada deve ser resguardado durante todas as etapas de seu ciclo de existência, tais como:

- I. Criação, aquisição e recebimento;
  - II. Registro, tramitação, expedição e demais formas de utilização;
  - III. Cópia, impressão, e demais formas de reprodução;
  - IV. Guarda;
  - V. Transmissão por correio eletrônico e demais meios de comunicação eletrônica;
  - VI. Transmissão pela palavra falada, incluindo telefonia móvel, correio de voz ou secretárias eletrônicas;
  - VII. Arquivamento;
  - VIII. Eliminação.
- 6.9. A responsabilidade pela guarda e tramitação de documento sigiloso será do emissor do documento – TCI - ou empregado por ele formalmente designado, que promoverá meios para a aplicação dos procedimentos descritos na presente Norma.
- 6.9.1. Compete à respectiva Diretoria manter controle, via inventário específico para este fim, de responsáveis pela guarda e tramitação de documentos sigilosos de sua alçada.
- 6.10. Os órgãos que necessitarem acesso a documentos sigilosos deverão solicitá-lo, fundamentadamente, ao responsável pela guarda do documento sigiloso;
- 6.11. O emissor do TCI é o responsável pela decisão sobre a concessão de acesso ao documento sigiloso e, em caso positivo, será concedido pelo responsável pela guarda diretamente ao signatário da solicitação.
- 6.11.1. O responsável pela guarda deverá abrir e registrar, em processo específico de controle de responsáveis pela guarda e tramitação de informações sigilosas, no mínimo, a data e nome do solicitante do pedido de acesso ao documento sigiloso;
- 6.11.2. Os empregados que tiverem acesso a qualquer informação sigilosa, ficam obrigados a resguardar o seu sigilo, mesmo após o desligamento de suas funções ou emprego.
- 6.12. Caberá ao responsável pela guarda, conservação e manutenção de documentos sigilosos, em qualquer fase de arquivo, o inventário, no mínimo anual;
- 6.13. Os documentos classificados como sigilosos não deverão ter suas imagens públicas no Sistema de Gestão Documental, porém neste deverá ser público o TCI e responsável pela sua guarda, com vistas a garantir a sua rastreabilidade, conferindo governança destes documentos;

- 6.14. Quando o documento sigiloso estiver em um processo, neste deverá constar quais páginas são sigilosas e o responsável pela sua guarda, junto com o TCI preenchido;
- 6.15. Quando todo o processo estiver classificado como sigiloso, deverá constar no Sistema de Gestão Documental esta menção e o responsável pela sua guarda, junto com o TCI preenchido;
- 6.16. Os documentos classificados em algum grau de sigilo, deverão ter a indicação do grau de sigilo em todas as suas páginas, em local que não inviabilize a leitura;
- 6.17. É proibida, por qualquer meio, a reprodução de cópias, salvo, mediante autorização do emitente ou superior, respeitados os níveis de alçada para assuntos sigilosos.
  - 6.17.1. As cópias autorizadas deverão ser registradas, numeradas e controladas com os mesmos cuidados dispensados aos originais.
- 6.18. Do Acesso à Informação pelo Público Externo
  - 6.18.1. O cidadão poderá ter acesso a informações da CMB por meio de requerimento endereçado ao Serviço de Informação ao Cidadão.
    - I. O pedido de acesso à informação deverá conter:
      - a) Nome do requerente;
      - b) Número de documento de identificação válido e CPF;
      - c) Especificação, de forma clara e precisa, da informação requerida;
      - d) Endereço físico ou eletrônico do requerente, para recebimento de comunicações ou da informação requerida.
    - II. Não serão atendidos pedidos de acesso à informação:
      - a) Genéricos;
      - b) Desproporcionais ou desarrazoados;
      - c) 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.
    - III. São vedadas exigências relativas aos motivos do pedido de acesso à informação;
    - IV. A negativa de acesso à informação deverá ser justificada e consubstanciada em decisão a ser encaminhada ao requerente.
      - a) Quando for negado acesso à informação por ser ela parcialmente classificada, é assegurado o acesso à parte não classificada e/ou desclassificada por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

- V. As solicitações externas de vista e cópia de processos que tratem de licitação em curso serão atendidas pelo Departamento de Contratações – DEGEC e as solicitações de vista e cópia de processos disciplinares, pela Corregedoria da CMB – CORREG;
- VI. O atendimento e a orientação do público poderão ser feitos pelo e-mail sic@cmb.gov.br, pelo telefone (21) 2814-2937, por via postal ou presencial no Parque Fabril da CMB no horário de 8h até as 16h30;
- VII. Recebida a solicitação, o Serviço de Informação ao Cidadão - SIC verificará se a informação está disponível para entrega imediata, devendo enviar ao cidadão, em caso positivo;
- VIII. Em caso negativo, o SIC encaminhará solicitação ao Departamento responsável, que terá prazo de 5 (cinco) dias úteis para responder a mesma.
  - a) Caso a resposta do Departamento não atenda à solicitação do cidadão, o SIC encaminhará o caso para a Autoridade de Monitoramento da LAI no âmbito da CMB, que decidirá em 48 (quarenta e oito) horas sobre a remessa da solicitação à Diretoria competente.
- IX. No caso de indeferimento de acesso a informações ou do não fornecimento das razões da negativa do acesso, o requerente poderá interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da decisão, dirigido à Autoridade de Monitoramento da LAI no âmbito da CMB.
  - a) A Autoridade de Monitoramento da LAI no âmbito da CMB verificará se o recurso atende os requisitos formais.
    - 1. Em caso positivo, solicitará informações ao Departamento responsável e decidirá em 5 (cinco) dias a contar da apresentação pelo cidadão.
  - b) Em caso de novo indeferimento, o cidadão poderá interpor recurso, no prazo de 10 (dez) dias, ao Presidente da CMB, que decidirá em 5 (cinco) dias.
- X. No caso de omissão de resposta, o requerente poderá interpor reclamação no prazo de 10 (dez) dias a contar do trigésimo dia da apresentação do pedido de acesso à informação, dirigido à Autoridade de Monitoramento da LAI no âmbito da CMB.

a) Autoridade de Monitoramento da LAI no âmbito da CMB verificará se o recurso atende os requisitos formais.

1. Em caso positivo, solicitará informações ao SIC e decidirá em 5 (cinco) dias a contar da apresentação pelo cidadão.

XI. Desprovidos o recurso ou a reclamação disposto em “IX” e “X”, ou não atendidos no prazo estipulado para resposta, o requerente poderá interpor recurso, no prazo de 10 (dez) dias, a contar da ciência da resposta ou do transcurso de prazo, dirigido à Controladoria Geral da União – CGU, que terá prazo de 5 (cinco) dias, a contar do recebimento, para decidir.

a) Em caso de indeferimento, o cidadão poderá oferecer recurso à Comissão Mista de Reavaliação de Informações – CMRI do Poder Executivo Federal, no prazo de 10 (dez) dias.

#### 6.19. Da Publicação dos Atos Sigilosos

6.19.1. A publicação anual dos atos sigilosos de que dispõe a Lei de Acesso à Informação limitar-se-á ao rol das informações classificadas em cada grau de sigilo, que deverá conter:

- I. Código de indexação de documento;
- II. Categoria na qual se enquadra a informação;
- III. Indicação de dispositivo legal que fundamenta a classificação;
- IV. Data da produção, data da classificação e prazo da classificação.

6.19.2. Na ocorrência de publicação de atos sigilosos, está se limitará aos seus respectivos números de indexação, setores de tramitação, datas de expedição e ementas, redigidas de modo a não comprometer o sigilo.

#### 6.20. Da Guarda

6.20.1. Os documentos de natureza sigilosa serão guardados em condições especiais de segurança que garantam, quanto ao acesso, restrição e controle.

6.20.2. Os agentes públicos da CMB encarregados da custódia de documentos, dados ou informações de natureza sigilosa, nas suas ausências, deverão passar a seus substitutos todos os documentos, dados ou informações sob sua responsabilidade, devidamente conferidos.

### 7. RESPONSABILIDADES

#### 7.1. Caberá ao SIC

7.1.1. Atender e orientar o público quanto ao acesso a informações;

7.1.2. Receber os requerimentos;

- 7.1.3. Registrar e protocolizar os requerimentos na Plataforma Integrada de Ouvidoria e Acesso à Informação (Fala.Br) do Poder Executivo Federal, nas situações autorizadas por esta Norma;
- 7.1.4. Informar sobre a tramitação de requerimentos;
- 7.1.5. Verificar a disponibilidade imediata da informação, de modo a conceder ao requerente o acesso no momento da solicitação da informação;
- 7.1.6. Enviar as respostas recebidas aos requerentes;
- 7.1.7. Orientar os requerentes sobre as possibilidades de recurso em casos de negativa ou ausência de resposta;
- 7.1.8. Informar ao requerente quando houver pedido de dilação de prazo para a resposta;
- 7.1.9. Disponibilizar vista e cópia de processos administrativos em trâmite na CMB.
- 7.2. Caberá ao Comitê de Segurança da Informação e Comunicações – COSIC
  - 7.2.1. Avaliar e propor soluções e requisitos de proteção física e lógica das informações geridas pela CMB;
  - 7.2.2. Definir as diretrizes para classificação da informação na CMB;
  - 7.2.3. Elaborar conteúdos de conscientização e sensibilização quanto à operacionalização da Classificação da Informação em função desta Norma;
  - 7.2.4. Analisar os casos não previstos nesta Norma.
- 7.3. Caberá ao DETIC
  - 7.3.1. Implementar e manter os controles de acesso lógico de acordo com a solicitação do empregado responsável pela informação;
  - 7.3.2. Viabilizar os recursos para classificação e rotulação da informação em meios digitais;
- 7.4. Caberá ao DELOG
  - 7.4.1. Viabilizar os recursos para classificação e rotulação da informação em documentos arquivísticos emitidos/recebidos no Sistema Eletrônico de Informações;
- 7.5. Caberá ao Responsável pela Informação
  - 7.5.1. Classificar e rotular todas as informações sob sua responsabilidade;
  - 7.5.2. Definir e periodicamente realizar a análise crítica das classificações e restrições de acesso, levando em conta as políticas de controle de acesso aplicáveis;
  - 7.5.3. Dirimir qualquer dúvida em relação à classificação da informação realizada por ele;



- 7.5.4. Promover a reclassificação da informação sempre que aplicável, seja para aumento do grau de sigilo em função do conceito do menor privilégio ou da diminuição de grau em função de publicidade.