ACESSO À INFORMAÇÃO

O curso “Acesso à Informação” (Parceria OGU/Enap) demonstra as bases normativas, conceituais e operacionais que podem ser utilizadas na aplicação da Lei de Acesso à Informação (LAI), oferecendo subsídios aos cidadãos e à administração pública em geral para a realização consciente e eficiente de atos relacionados à essa área.

SUMÁRIO - MÓDULO 3 – CLASSIFICAÇÃO DE INFORMAÇÕES E DADOS ABERTOS

1. INTRODUÇÃO

2. INFORMAÇÕES CLASSIFICADAS

Diferentemente dos sigilos legais estudados no módulo 2, que são estabelecidos por legislações diversas, a classificação de informações é uma decisão administrativa. Isto é, a autoridade competente decide que a divulgação de determinada informação pode vulnerar a segurança da sociedade e do Estado, como estabelecido no seguinte trecho da Constituição Federal:

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

(...)

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

Percebe-se que a "segurança da sociedade e do Estado" pode parecer bastante abrangente. Nesse sentido, a LAI, ao regulamentar a classificação de informações, criou um rol exaustivo/ taxativo de nove hipóteses em que esse dispositivo pode ser aplicado, estabelecendo, inclusive, procedimentos e prazos específicos para a restrição de acesso a tais informações.

Bem, agora você deve estar se perguntando, mas quais informações podem ser classificadas? É disso que trataremos no tópico seguinte.

2.1. QUAIS INFORMAÇÕES PODEM SER CLASSIFICADAS?

A Lei de Acesso estabeleceu, portanto, nove hipóteses em que a administração pode determinar o sigilo de certa informação por determinado prazo. Nos termos do art. 23, são consideradas imprescindíveis a segurança da sociedade e do Estado, e, portanto, passíveis de classificação as informações cuja divulgação ou cujo acesso irrestrito possam:

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

- 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;

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

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

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

- 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;

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

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

- colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as).

Isso significa que, para classificar determinada informação, a Administração deve, necessariamente, enquadrar o sigilo em alguma dessas hipóteses, não havendo possibilidade de classificação com outros fundamentos. Ressalta-se que

IMPORTANTE

Não se esqueça! As informações protegidas por sigilos legais, informações pessoais, documentos preparatórios ou aquelas em que incidem as hipóteses do art. 13 do Decreto nº 7.724/2012 (isto é, aquelas que vimos no módulo 2) não devem ser classificadas! A restrição de acesso desse tipo de informação sigilosa independe de classificação, pois seu sigilo tem outros fundamentos. As informações passíveis de classificação são apenas aquelas que se enquadram nas nove hipóteses previstas nos artigos 23 e 24 da LAI!

SAIBA MAIS

Na Bulgária, a lei atribui ampla margem ao conceito de autoridade classificadora, permitindo a qualquer signatário do documento classificá-lo. Também, naquele país, poucos documentos referentes ao antigo serviço de segurança estão disponíveis no Arquivo Nacional. Já na República Tcheca, aprovou-se uma legislação que autoriza os cidadãos a obterem arquivos pessoais elaborados pela polícia secreta comunista. Nos EUA, o *Information Security Oversight Office* (uma divisão do Arquivo Nacional) fiscaliza o sistema de classificação. Em um levantamento feito em 2004, descobriu-se que foram erroneamente classificados 51% dos documentos examinados. Na Alemanha, o *Stasi Records Act* (1991) autorizou o acesso a arquivos da polícia secreta da antiga República Democrática da Alemanha (RDA). Disponibilizou-se material que foi produzido entre 1949 e 1990, composto de aproximadamente 28.400 áudios, 3.000 filmes e 1,6 milhão de fotografias. Tais registros estão organizados em uma linha de 111 quilômetros!

2.2 POR QUANTO TEMPO AS INFORMAÇÕES CLASSIFICADAS ESTÃO PROTEGIDAS?

As informações em poder dos órgãos e entidades públicas, observado o teor delas e em razão de imprescindibilidade do sigilo à segurança da sociedade ou do Estado, poderão ser classificadas em três diferentes graus:

- ultrassecreto, com prazo de sigilo de até 25 anos (único passível de prorrogação);
- secreto, com prazo de sigilo de até 15 anos; e
- reservado, com prazo de sigilo de até 5 anos.

A classificação da informação como ultrassecreta é a única passível de prorrogação, por até igual período (25 anos, totalizando o período máximo de 50 anos de classificação). As informações classificadas com os demais tipos de sigilo, após o prazo de validade da classificação, tornam-se de acesso público. Isso não significa, contudo, que os documentos não devam ser analisados de modo a proteger eventuais informações pessoais sensíveis ou cobertas por sigilo legal porventura presentes.

Mas esses prazos começam a contar a partir de quando?

A contagem tem por data inicial a **data de produção** do documento que registra a informação que está sendo classificada. Ou seja, se uma informação produzida há 10 anos for classificada como secreta na data de hoje, ela se tornará ostensiva em 5 anos. Isso significa, por exemplo, que um documento produzido há 6 anos não poderia ser classificado como "Reservado", uma vez que o prazo de sigilo desse grau (5 anos) já estaria expirado. Da mesma forma, classificar como "Secreto" um documento produzido há 20 anos também não produz efeito de sigilo.

2.3 QUAIS AUTORIDADES PODEM CLASSIFICAR INFORMAÇÕES?

Como em qualquer ato administrativo, a validade da decisão de classificação da informação está condicionada à competência daquele que decide pela classificação. A Lei de Acesso tratou de enumerar as autoridades que possuem essa prerrogativa.

A competência para classificação das informações varia de acordo com o grau (ultrassecreto, secreto e reservado), assim como acontece com os prazos. Isso ocorre, pois, não é toda e qualquer autoridade que pode estabelecer o sigilo de uma informação por 25 anos ou mesmo 5 anos.

São autoridades competentes para a classificação de informações no grau ULTRASSECRETO:

- O/A Presidente da República.
- O/A Vice-Presidente da República.
- Ministros e ministras de Estado e autoridades com as mesmas prerrogativas.
- Comandantes da Marinha, do Exército e da Aeronáutica.
- Chefes de Missões Diplomáticas e Consulares permanentes no exterior.

No caso de Comandantes da Marinha, do Exército e da Aeronáutica e dos Chefes de Missões Diplomáticas e Consulares permanentes no exterior, a prerrogativa de classificação está condicionada à ratificação expressa do titular máximo da pasta a que pertençam, em prazo máximo de 30 dias. Isso significa, por exemplo, que, se um Chefe de Missão Diplomática sediado no exterior decidir classificar determinado documento como ultrassecreto, essa decisão deverá ser referendada pelo Ministro das Relações Exteriores em até 30 dias depois da classificação.

Os Chefes de Missão Diplomática e os Comandantes figuram no rol de autorizados a classificar informação em razão da peculiaridade do tema com que atuam. Imagine se um chefe de missão diplomática no exterior fosse obrigado a solicitar autorização ao Ministro das Relações Exteriores sempre que houvesse necessidade de classificar uma informação em grau ultrassecreto. Nessa hipótese, até a autorização do Ministro, tal informação sensível não teria qualquer restrição de acesso. Sendo assim, essas autoridades possuem competência de estabelecer o sigilo em grau ultrassecreto, mas sua decisão deve ser referendada pelo respectivo Ministro de Estado.

A informação pode ser classificada como **SECRETA** pelos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista, assim como por todos os autorizados para classificação da informação como ultrassecreta.

A classificação no grau **RESERVADO,** por sua vez, poderá ser realizada por autoridades que exerçam funções de direção, comando ou chefia, de hierarquia equivalente ou superior ao nível DAS 101.5, do Grupo-Direção e Assessoramento Superiores, de acordo com regulamentação específica de cada órgão ou entidade, assim como por todos os demais qualificados para a classificação em grau secreto e ultrassecreto.

No âmbito do Poder Executivo federal, a classificação em grau reservado é suscetível de delegação, que poderá se dar ao ocupante de cargo de direção, comando ou chefia, por ato do dirigente máximo do órgão ou da entidade. A classificação feita por meio desse expediente deve ser acompanhada pela ciência do ato por parte da autoridade delegante, no prazo de 90 dias.

Finalmente, é importante que saibamos que a competência para a prorrogação de uma classificação ultrassecreta por até 25 anos **é prerrogativa exclusiva da Comissão Mista de Reavaliação de Informações (CMRI)[1].** Isto é, mesmo que a autoridade classificadora decida prorrogar a classificação de determinada informação ultrassecreta, ela não poderá fazêlo (mesmo que seja o(a) Presidente da República!). A CMRI é o colegiado competente para deliberar e decidir acerca da prorrogação do sigilo por mais 25 anos.
Nós já estudamos sobre a CMRI no módulo 1, você lembra? Tratamos da sua atuação como instância recursal dos pedidos de acesso à informação, dentre outros. Já neste módulo, em um tópico mais a frente, veremos as competências da CMRI no que se refere a informações classificadas!

Abaixo veja uma tabela com uma síntese das informações que foram apresentadas nesse subtópico.

[1] . A Comissão Mista de Reavaliação de Informações (CMRI) é um colegiado composto por membros de diversos órgãos do Poder Executivo federal, sob presidência da Casa Civil da Presidência da República. A CMRI recebe e decide recursos contra as decisões da CGU, sendo, portanto, a quarta e a última instância recursal prevista pela Lei de Acesso à Informação. Além de decidir esses recursos, a CMRI tem outras atribuições, dentre as quais a de estabelecer orientações para suprir lacunas na aplicação da LAI. Essas orientações são feitas sob a forma de Súmulas ou Resoluções. Ao todo, a CMRI já emitiu 7 Súmulas e 5 Resoluções, todas disponíveis em: http://www.acessoainformacao.gov.br/assuntos/recursos/recursos-julgados-a-cmri/ sumulas-e-resolucoes.

Classificação	Quem decide
Grau ultrassecreto (25 anos)	• Presidente da República. • Vice-Presidente da República. • Ministros de Estado e autoridades com as mesmas prerrogativas. • Comandantes da Marinha, do Exército e da Aeronáutica. • Chefes de Missões Diplomáticas e Consulares permanentes no exterior.
Grau secreto (15 anos)	• Todos os autorizados para o grau ultrassecreto. • Titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.
Grau reservado (5 anos)	• Todos os autorizados para os graus ultrassecreto e secreto. • Autoridades que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente.

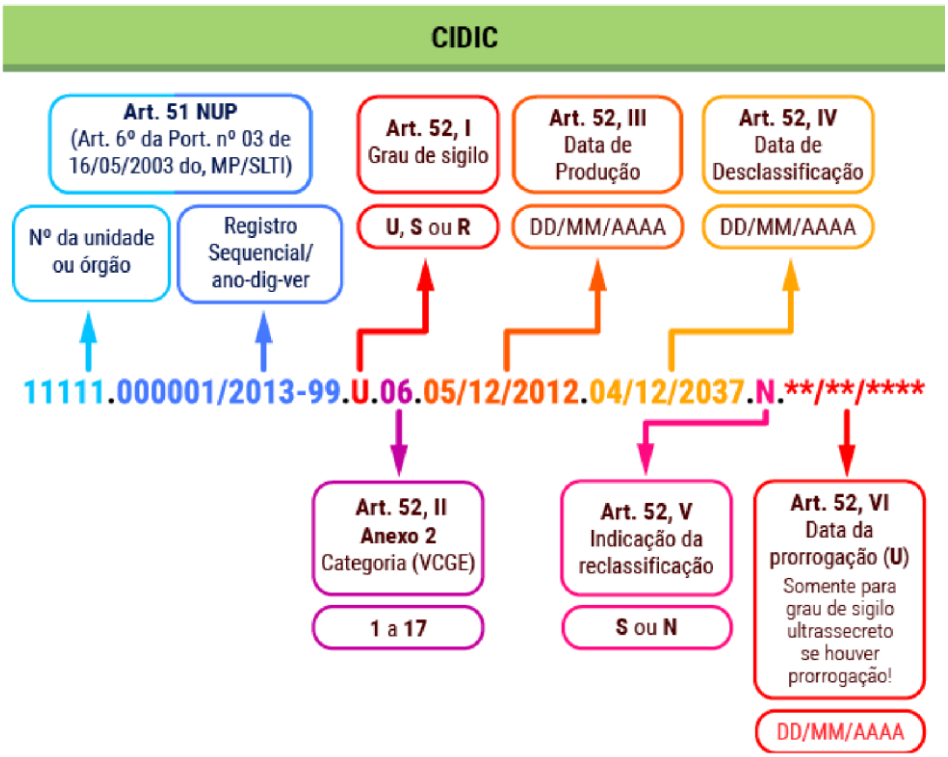
2.4 QUAIS SÃO OS PROCEDIMENTOS PARA A CLASSIFICAÇÃO DE INFORMAÇÕES?

No âmbito do Poder Executivo federal, a classificação de informação necessária à segurança da sociedade e do Estado é realizada por meio de um ato administrativo formal, denominado Termo de Classificação de Informação - TCI. O TCI é um documento público, recaindo restrição de acesso somente a um de seus campos: o campo "razões da classificação". Tal precaução é compreensível, pois é justamente nele que a autoridade deverá motivar a sua decisão de classificar, assinalando as razões conjunturais que a levaram a adotar determinada hipótese ou grau de sigilo.

O TCI é indexado por meio do Código de Indexação de Documento que contém Informação Classificada (CIDIC), conforme orientações existentes no Decreto nº 7.845/2012[2]. O CIDIC é composto por:

- número único de protocolo do documento ou processo (NUP);
- grau de sigilo (reservado - R, secreto - S ou ultrassecreto-U);
- categoria[3][4](01 a 17);
- data da produção da informação (DD/MM/AAAA);
- data de desclassificação da informação (data em que a informação será desclassificada - DD/MM/AAAA);
- indicação de reclassificação (sim - S ou não - N);
- data da prorrogação (DD/MM/AAAA).

Veja o gráfico a seguir:



[2] . O Decreto nº 7.845/2012 trata dos procedimentos para credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo. Aprenderemos mais sobre ele no próximo subitem.

[3] . Representam os aspectos ou temas correlacionados à informação classificada em grau de sigilo (Anexo II do Decreto nº

[4] .845/2012).

Para as informações classificadas nos graus reservado e secreto, a 2ª parte do CIDIC terá sempre 28 posições com caracteres alfanuméricos e separadores.

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. 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 as 39 posições com caracteres alfanuméricos e separadores.

2.5 TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Você sabe o que é tratamento de informação? De acordo com a definição da LAI (art. 4º, inciso V), tratamento da informação é o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

O acesso, a divulgação e o tratamento de informações classificadas são restritos a pessoas que possuem a necessidade de conhecê-las. Isso quer dizer que a pessoa, para o exercício de suas atribuições, deve precisar conhecer a informação classificada, além de possuir credencial de segurança (se ela não for uma das autoridades autorizadas pela LAI, conforme vimos no subitem 2.3).

Uma credencial de segurança é um documento obtido após um processo de credenciamento levado a cabo pelo Gestor de Segurança e Credenciamento do órgão ou entidade. Ao longo desse processo, o solicitante da credencial deverá obter anuência da sua chefia e encaminhar extenso formulário acerca de dados pessoais. Além disso, será realizada investigação de sua vida pregressa, de modo a verificar se aquela pessoa pode acessar esse tipo de informação sigilosa. Ao final desse processo, a credencial de segurança, emitida para nível reservado, secreto ou ultrassecreto, lhe garantirá o acesso a todos os documentos classificados naquele órgão (no respectivo grau de sigilo).

Contudo, nem todo mundo precisa passar por esse procedimento para conhecer informações classificadas. São duas as exceções:

- Considera-se que aquele que tenha a competência para classificar em determinado grau de sigilo seja habilitado de ofício para ter acesso às informações classificadas naquele grau de sigilo. Assim, por exemplo, um DAS 101.5 não precisaria se credenciar para ter acesso a informações classificadas em grau reservado; tampouco um Ministro de Estado precisaria credenciar-se para ter acesso a informações classificadas em grau de sigilo reservado.

- Em razão da dificuldade do processo e da necessidade de atendimento célere a algumas demandas, o acesso a informações em qualquer grau de sigilo por pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS), pelo qual a pessoa se obriga a manter o sigilo da informação. A não observância do sigilo pode resultar em responsabilidade penal, civil e administrativa, na forma da lei.

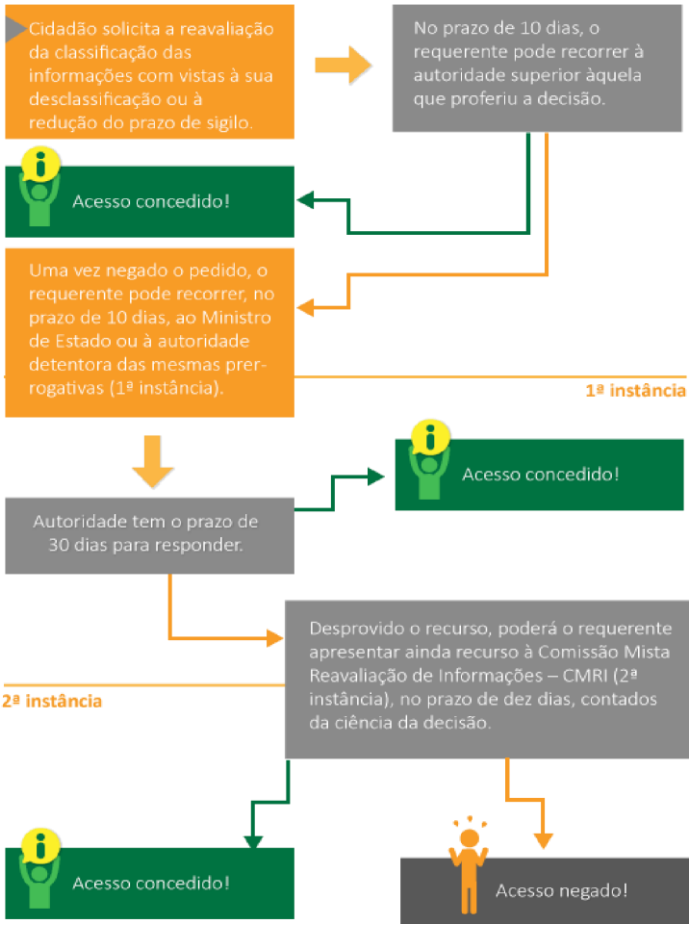
2.6 DESCLASSIFICAÇÃO E RECLASSIFICAÇÃO

Qualquer cidadão pode solicitar ao órgão ou entidade a desclassificação ou a reavaliação da classificação de informações classificadas com grau de sigilo. O Serviço de Informações ao Cidadão (SIC) é responsável pelo recebimento de pedidos de desclassificação ou reavaliação de classificação de informações. Esses pedidos seguem um fluxo diferente do estabelecido para pedidos de acesso à informação e não devem ser inseridos no sistema e-SIC, por este não estar adaptado ao fluxo desse tipo de pedido.

O órgão ou entidade pode obter os formulários para pedidos de desclassificação e de reclassificação, assim como os formulários para a apresentação de recursos contra a negativa do pedido, em http://www.acessoainformacao.gov.br/lai-para-sic/sic-apoio-orientacoes/formularios.

O pedido de desclassificação ou de reavaliação deve ser encaminhado à autoridade classificadora ou à autoridade hierarquicamente superior, que decidirá no prazo de trinta dias. Negado o pedido, o requerente poderá apresentar recurso no prazo de 10 dias, contado da ciência da negativa, ao Ministro de Estado ou à autoridade com as mesmas prerrogativas (1ª instância), que decidirá no prazo de 30 dias. Desprovido esse recurso, poderá o requerente apresentar ainda recurso à Comissão Mista Reavaliação de Informações - CMRI (2ª instância), no prazo de 10 dias, contado da ciência da decisão.

A seguir, observe o infográfico do processo de desclassificação e reclassificação.



A Comissão Mista de Reavaliação de Informações - CMRI é a instância recursal máxima tanto para os processos de pedidos de acesso à informação quanto para os processos de pedidos de desclassificação de informações. Veremos as competências da CMRI no que tange a informações classificadas no próximo tópico do curso.

Nos casos de pedido de acesso à informação em que o objeto de solicitação seja informação classificada com grau de sigilo, a negativa de acesso deve ser instruída com o fundamento legal da classificação, da autoridade classificadora e do CIDIC.

As informações classificadas também podem ser desclassificadas a qualquer momento pela autoridade que as tenha classificado ou por superior hierárquico, bem como nas reavaliações periódicas de informações classificadas.

2.7 COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES (CMRI)

Como vimos no subitem 4.4 do Módulo 1, a Comissão Mista de Reavaliação de Informações foi criada pela LAI e regulamentada pelo Decreto nº 7.724/2012. Além de instância recursal no âmbito dos pedidos de acesso à informação, a CMRI possui competências vinculadas ao tratamento de classificação de informações. São elas:

- Rever a classificação de documentos secretos e ultrassecretos: Em seu art. 35, parágrafo 3º, a LAI estabeleceu a obrigatoriedade de revisão de ofício (isto é, quando a Administração age sem necessidade de ser demandada) das informações classificadas a cada quatro anos. Tal revisão foi regulamentada por meio da Resolução CMRI nº 03, de 30 de março de 2016[5].

- Requisitar esclarecimentos sobre informações classificadas: quando as informações presentes no TCI não são suficientes, a CMRI pode solicitar ao órgão mais detalhes para subsídio de sua decisão.

- Decidir recursos sobre pedidos de desclassificação de informações: a CMRI é a última instância recursal no que se refere a pedidos de desclassificação de informações.

- Prorrogar, uma única vez por até 25 anos, o prazo de sigilo de documentos classificados em grau ultrassecreto: apenas a CMRI possui a competência de prorrogação de prazo de documentos ultrassecretos.

Além de ser a última instância recursal nos casos de pedidos de acesso à informação, a CMRI também é a última instância recursal em casos de pedidos de desclassificação de informações.

[5] . http://www.acessoainformacao.gov.br/assuntos/recursos/recursos-julgados-a-cmri/sumulas-e-resolucoes/resolucao-no03-de-30-de-marco-de-2016.

Ou seja, diferentemente da CGU, que não detém competência para analisar o mérito de pedidos que envolvam informações classificadas, os membros da CMRI devem se posicionar, em última instância, sobre o mérito das decisões de classificação.

Agora que você conhece as competências da CMRI, trataremos de outra comissão no próximo subtópico. Fique ligado nas diferenças e cuidado para não se confundir.

2.8 COMISSÃO PERMANENTE DE AVALIAÇÃO DE DOCUMENTOS SIGILOSOS (CPADS)

Para auxiliar no fluxo de classificação de informações, orienta-se que o órgão ou entidade constitua uma Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), colegiado previsto pelo Decreto nº 7.724/2012. A Comissão deve ser formada com a designação formal de seu presidente e dos demais membros e suplentes, preferencialmente com um representante de cada área demandante de classificação de informação. No mesmo ato de instituição da CPADS e designação de seus membros, a alta administração do órgão poderá estabelecer as responsabilidades e regular o funcionamento e a periodicidade das reuniões da Comissão.

A CPADS não tem o poder de classificar informações, mas deve ter atribuições como: opinar sobre a informação produzida no âmbito da sua atuação para fins de classificação em qualquer grau de sigilo; assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à desclassificação, à reclassificação ou à reavaliação de informação classificada em qualquer grau de sigilo; propor o destino final das informações desclassificadas, indicando os documentos para guarda permanente, com a observação do disposto na Lei nº 8.159, de 8 de janeiro de 1991; e subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo a ser disponibilizado na Internet. Isto é, a CPADS deve ser entendida como um órgão de assessoramento da entidade no que se refere à classificação de informações.

Como a CPADS opina sobre gestão documental em alguns casos específicos, nota-se que possui competência compartilhada com outra estrutura existente nos órgãos da Administração Pública: a Comissão Permanente de Avaliação de Documentos - CPAD, instituída pelo Decreto nº 4.073/2002, que regulamenta a Lei de Arquivos. É importante que, no ato de instauração da CPADS ou no seu Regimento Interno, seja estabelecida a forma de exercício de tais competências.

2.9 PUBLICAÇÃO DO ROL DE DOCUMENTOS CLASSIFICADOS E DESCLASSIFICADOS NA INTERNET

O órgão ou entidade deverá, anualmente, publicar, em sua página na Internet, o rol de documentos classificados e desclassificados, conforme descrito no artigo 45 do Decreto nº 7.724/2012:

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.

A divulgação do conteúdo estabelecido pelos incisos I e II do artigo 45 do Decreto nº 7.724/2012 deve ser realizada no menu da seção Acesso à Informação, no item Informações Classificadas. No item Informações Classificadas, deve constar texto explicativo sobre o objetivo de atender aos incisos I e II do Artigo 45 do Decreto nº 7.724/2012. Esse item deve apresentar também duas áreas específicas para a apresentação das listagens:

- Rol de informações desclassificadas: De acordo com a Resolução CMRI nº 02/2016, o rol de informações desclassificadas deve conter, no mínimo: a) dados que identifiquem o documento desclassificado, a exemplo do Número Único de Protocolo (NUP), do Código de Indexação de Documento que contém Informação Classificada (CIDIC), ou outro; b) grau de sigilo ao qual o documento desclassificado ficou submetido; e c) breve resumo do documento desclassificado.

- Rol de informações classificadas: O conteúdo dessa área deve apresentar o Código de Indexação de Documento que contém Informação Classificada (CIDIC); a categoria na qual se enquadra a informação (Anexo II do Decreto nº 7.845/2012); a indicação do dispositivo legal que fundamenta a classificação; a data da produção, a data da classificação e o prazo da classificação.

É recomendável que haja suficiente descrição do conteúdo/assunto dos documentos desclassificados, de modo que se torne viável, aos cidadãos em geral, solicitar acesso a esses documentos com base nesse critério.

Somente devem ser incluídas no "Rol de informações classificadas" as informações classificadas nos termos do §1º do art. 24 da Lei nº 12.527/2011, ou seja, classificadas como reservadas, secretas e ultrassecretas. Informações cujo sigilo se deve a outras legislações, como fiscal e tributário, assim como documentos preparatórios e informações pessoais, não estão sujeitos à divulgação no referido item.

2.10 CLASSIFICAÇÃO DA INFORMAÇÃO DURANTE O CURSO DO PROCESSO DE PEDIDO DE ACESSO À INFORMAÇÃO

A Súmula nº 3/2015 da Comissão Mista de Reavaliação de Informações (CMRI) prevê o julgamento, sem análise de mérito, do recurso correspondente, devido à classificação da informação ocorrida durante esse processo.

> ***Súmula CMRI nº 3/2015***
>
> *EXTINÇÃO POR CLASSIFICAÇÃO DA INFORMAÇÃO - Observada a regularidade do ato administrativo classificatório, extingue-se o processo cujo objeto tenha sido classificado durante a fase de instrução processual, devendo o órgão fornecer ao interessado o respectivo Termo de Classificação de Informação, mediante obliteração do campo 'Razões da Classificação.*

A classificação regular da informação constitui fato superveniente, portanto, a partir do qual a CGU não tem mais competência para analisar o mérito do recurso. Em decorrência disso, deve o processo ser extinto, nos termos do artigo 52 da Lei nº 9.784/1999, que tem aplicação subsidiária ao Decreto nº 7.724/2012, por força de seu artigo 75. A partir daí, o interessado deve, se assim entender adequado, ingressar com pedido específico de desclassificação de informação, que segue rito próprio, como já apresentado durante o curso.

Mas quando esse tipo de situação pode acontecer?

Digamos que um cidadão faça um pedido de acesso à informação e o órgão/entidade entenda que essa informação não pode ser concedida em virtude de algum sigilo legal. O cidadão recorre à CGU e, durante a instrução do recurso pela CGU, o órgão percebe que o fundamento legal apresentado está incorreto e que, na verdade, a informação deve ser classificada. Uma vez realizado o procedimento, a CGU perde a competência de julgar o mérito do recurso e o processo é extinto. Caso queira, o cidadão deve realizar pedido de desclassificação, que segue rito próprio.

3. DADOS ABERTOS

Nessa última etapa do curso, você irá conhecer sobre dados abertos e para iniciar nossos estudos veja a dica abaixo:

DICA

Como, em regra, os dados governamentais são públicos, é fundamental que os governos implementem políticas para disponibilizá-los. O Decreto nº 8.777/2016 institui essa política.

O Estado, no exercício de suas mais diversas atribuições, acumula uma infinidade de dados. Podemos pensar em diversos exemplos de entidades que dispõem de bancos de dados consideráveis: dentre outros tantos bancos de dados custodiados pelo Estado, por exemplo, a Receita Federal recebe milhares de informações sobre a situação fiscal dos contribuintes. O Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) realiza todo o processamento, controle e execução financeira, patrimonial e contábil do governo federal brasileiro. O Sistema de Gestão de Pessoas do Executivo Federal (SIGEPE) possui registro de todos os servidores públicos federais.

Naturalmente, esses bancos de dados são fonte de interesse dos cidadãos e, em atendimento ao princípio da máxima divulgação, é relevante quando esse tipo de informação pode ser disponibilizado.

O acesso a dados e informações, como vimos, foi regulamentado pela Lei de Acesso à Informação. Sendo assim, pedidos de acesso a bancos de dados são e eram tratados regularmente por meio da LAI.

O Decreto nº 8.777/2016 ressaltou a relevância desse tipo de acesso ao estabelecer a Política de Dados Abertos do Poder Executivo Federal. Tal dispositivo não apenas reforçou as diretrizes da LAI, como também trouxe novas obrigações de transparência ativa, apresentando os seguintes princípios e diretrizes:

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

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

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

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

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

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

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

Em seu anexo, por exemplo, o Decreto nº 8.777/2016 estabeleceu dados de interesse público cuja divulgação deveria ser priorizada pela Administração em até 180 dias da data de publicação do normativo. O decreto também estabeleceu que as entidades da Administração Pública federal direta, autárquica e fundacional devem elaborar Planos de Dados Abertos (no prazo de sessenta dias), com o objetivo de implementar e promover a abertura de dados de cada órgão:

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

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

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

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

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

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

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

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

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

O Decreto nº 8.777/2016 também previu que os pedidos de abertura de dados seguem os mesmos ritos e procedimentos estabelecidos pela LAI e pelo Decreto nº 7.724/2012 para os pedidos de acesso à informação, tal como vimos no Módulo 1.

Dessa forma, o Decreto nº 8.777/2016 vem reforçar o disposto na LAI ao criar novas obrigações de transparência ativa e de abertura de bancos de dados. Esse normativo contribui para o avanço da transparência, uma vez que, atualmente, nem todas as bases de dados podem ser acessadas pela população, em virtude de informações sigilosas lá contidas. Enquanto esses bancos de dados não são disponibilizados e/ou devidamente triados, em face de pedidos que envolvam bancos de dados, é importante verificar-se a eventual incidência de sigilos legais ou de restrições de acesso, bem como avaliar se a possibilidade de extração e os custos envolvidos

nessa operação são viáveis. Quanto mais dados e informações a população tiver a seu dispor, mais correlações e avaliações do governo poderão ser realizadas de forma qualitativa, ou seja, mais e melhor controle social!

SAIBA MAIS

O principal objetivo do Portal Brasileiro de Dados Abertos é ser o ponto central para acesso a dados públicos governamentais no Brasil. Há requisitos de acesso específicos:

a) Controle de acesso para publicação e modificação dos dados e metadados.

b) Garantia de manutenção da integridade dos dados.

c) Segurança quanto à origem dos dados e autenticidade.

De maneira simplificada, para que um conjunto de dados esteja apto a constituir a Infraestrutura Nacional de Dados Abertos, o responsável pelo repositório de dados do órgão deve garantir que esse conjunto de dados cumpra as seguintes condições gerais:

1. Os dados devem estar em seu formato mais bruto possível, ou seja, antes de qualquer cruzamento ou agregação. Mesmo que o órgão ou entidade ache importante e já tenha publicado alguma visão de agregação desses dados, existe grande valor no dado desagregado. Dessa forma o órgão ou a entidade pode publicar esses dados nas duas formas.

2. Os dados devem estar em formato aberto, não proprietário, estável e de amplo uso.

3. Não deve existir nenhum instrumento jurídico que impeça sua reutilização e redistribuição por qualquer parte da sociedade.

4. Para os dados que são estruturados ou estão em planilhas na sua fonte, deve-se preservar ao máximo a estrutura original. Por exemplo, não se deve publicar planilhas em arquivo PDF, nesse caso utilize CSV ou ODS.

5. É recomendável a disponibilização dos dados em diversos formatos.

6. Cada conjunto de dados deve possuir um identificador único e persistente, seguindo uma padronização de URL. Esse requisito é imprescindível para que esse conjunto de dados seja referenciável e eventualmente consumido automaticamente por um aplicativo.

7. É recomendável a utilização de considerações semânticas na definição URLs, de forma que seja possível deduzir o conteúdo de um conjunto de dados apenas lendo seu identificador.

8. É extremamente desaconselhável a utilização de mecanismos antirrobôs, como captchas, para acesso aos conjuntos de dados.

9. Considerando que é desejável facilitar a indexação dos dados por motores de busca, sendo essa uma importante forma de o cidadão encontrar os dados que procura, é

recomendável que os nomes dos arquivos sigam as boas práticas de formação de um slug [WIKIPEDIA http://en.wikipedia.org/wiki/Slug_%28web_publishing%29], tal como é realizado em muitas soluções de software para blog ou gerenciadores de conteúdo. Mais especificamente, o título deve ser convertido para slug da seguinte maneira:

a. substituem-se todos os caracteres acentuados pelos seus correspondentes não acentuados;

b. transformam-se todos os caracteres maiúsculos em minúsculos;

c. substituem-se cada sequência de um ou mais espaços por um único hífen ("-"). Usa-se hífen em lugar de sublinhados ("_"), pois estes fazem com que os mecanismos de busca tratem o texto como um só termo. O mesmo aconteceria caso fossem utilizadas palavras concatenadas, no modo chamado "CamelCase". Por outro lado, o hífen permite que as palavras sejam indexadas individualmente [https://www.youtube.com/watch?v=AQcSFsQyct8];

d. Cada conjunto de dados deve ter informações sobre seus dados e metadados. Deve ser possível recuperar o significado dos dados;

e. Para conjunto de dados muito grande, recomenda-se a divisão em conjuntos menores, permitindo uma fácil manipulação. Recomenda-se fazer a divisão pela dimensão temporal (ano ou mês), pela dimensão geográfica (estado ou município) ou por outra dimensão;

f. É desejável que o repositório dos dados possibilite a composição de filtros dentro da URL, seguindo algum padrão de API, permitindo que o usuário restrinja o volume dos dados para aqueles que ele deseja. (http://dados.gov.br/cartilha-publicacao-dados-abertos/)

4. REVISÃO

A Chegamos a mais um momento de revisão. Não deixe de fazer a leitura com atenção, é importante para seu aprendizado!

No Módulo 3, vimos que as informações imprescindíveis à segurança da sociedade e do Estado devem ser classificadas. Para isso, elas devem necessariamente ser compatíveis com uma das nove hipóteses de classificação apresentadas pelos art. 23 e 24 da LAI.

A classificação pode se dar em grau reservado (5 anos), secreto (15 anos) e ultrassecreto (25 anos). Esses prazos são contados da data de produção da informação e não a partir da decisão classificatória. Apenas a classificação em grau ultrassecreto pode ser prorrogada e a instância exclusivamente competente para essa prorrogação é a Comissão Mista de Reavaliação de Informações (CMRI).

Aprendemos que, para classificar determinada informação, é necessário produzir um Termo de Classificação de Informações (TCI), que deve conter o Código de Indexação de Documento que contém Informação Classificada (CIDIC). Aquela pessoa com necessidade de conhecer determinada informação classificada (e que não seja autorizada por lei) deve passar por um

processo de credenciamento de segurança ou, alternativamente, assinar um Termo de Compromisso de Manutenção de Sigilo (TCMS).

A CMRI, além das competências estudadas no Módulo 1, possui também diversas competências relativas aos procedimentos de classificação. Ela deve rever, de ofício, a classificação de documentos secretos e ultrassecretos a cada quatro anos. É a última instância recursal no que diz respeito aos pedidos de desclassificação de informações e, além disso, é o colegiado competente para decidir sobre a prorrogação de documentos ultrassecretos.

Vimos que o Decreto nº 7.724/2012 previu, também, a constituição da Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS). A CPADS deve ser entendida como um órgão de assessoramento da entidade no que se refere à classificação de informações.

Por fim, vimos que os órgãos devem publicar os róis de documentos classificados e desclassificados na internet e que, quando uma informação é classificada durante a instrução do recurso pela CGU, o processo é extinto e deve ser realizado pedido de desclassificação, que possui rito próprio. A CGU não possui competência para avaliar o mérito de uma decisão de classificação.

Além das informações classificadas, aprendemos sobre o Decreto nº 8.777/2016, que reforçou as obrigações de transparência ativa e de abertura de dados do Poder Executivo federal. Em sessenta dias a partir da edição de tal Decreto, os órgãos e entidades federais devem elaborar seus respectivos Planos de Dados Abertos, o que vai impulsionar a transparência e a publicidade governamental.

Espero que você tenha adquirido uma visão ampla, mas ao mesmo tempo detalhada, da Lei de Acesso à Informação e de sua implementação, desde 2012. A transparência e a publicidade ganharam um reforço muito importante a partir dessa lei, e seu fortalecimento deve sempre nortear a administração pública brasileira. Parabéns por concluir a leitura do módulo 3!

5. ENCERRAMENTO

6. REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Sueli Angelica do; AROUCK, Osmar. **Atributos da qualidade da informação e a lei de acesso à informação.** Anais do XXV Congresso Brasileiro de Biblioteconomia, Documentação e Ciência da Informação. Florianópolis, 2013.

BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mátires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional.** São Paulo: Saraiva, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988.**

BRASIL. **Decreto n. 6.932, de 11 de agosto de 2009. Dispõe sobre a simplificação do atendimento público prestado ao cidadão, ratifica a dispensa do reconhecimento de firma em documentos produzidos no Brasil, institui a "Carta de Serviços ao Cidadão" e dá outras providências.** Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9094.htm Acesso em 01 de março de 2018. Acesso em 01 de março de 2018.

BRASIL. **Decreto n. 7.724, de 16 de maio de 2012. Regulamenta a Lei n. 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.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm>. Acesso em 01 de março de 2018.

BRASIL. **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional, 2005.

BRASIL. **Instrução Normativa OGU/CGU n. 1, de 5 de novembro de 2014.** Disponível em: <http:/www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in-ogu-01-2014.pdf>. Acesso em 01 de março de 2018.

BRASIL. **Instrução Normativa SLTI/MPn. 4, de 12 de abril de 2012. Institui a Infraestrutura Nacional de Dados Abertos - INDA.** Disponível em: <http://dados.gov.br/instrucao-normativada-inda/>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 4.595 de 31 de dezembro de 1964. Dispõe sobre a Política e as Insti-tuições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4595.htm> Acesso em: Acesso em 01 de março de 2018.

BRASIL. **Lei n. 6.404, de 15 de dezembro de 1976. Dispõe sobre as Sociedades por Ações.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l6404compilada.htm>. Aces¬so em: Acesso em 01 de março de 2018.

BRASIL. **Lei n. 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB).** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8906.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 9.278, Regula o § 3° do art. 226 da Constituição Federal. Lei n. 9.278, de 10 de maio de 1996.** Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9278.htm> Acesso em 01 de março de 2018.

BRASIL**. Lei. n. 9.610 de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9784.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei n. 10.406 Institui o Código Civil. Lei n. 10.406, de 10 de janeiro de 2002**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm> Acesso em 01 de março de 2018.

BRASIL. **Lei n. 12.414 Lei do Cadastro Positivo, Lei n 12.414/11, de 09 de junho de 2009. Disciplina a formação e consulta a bancos de dados com informações de adim¬plemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm> Acesso em 01 de março de 2018.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 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.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 01 de março de 2018.

BRASIL. **Lei Complementar n. 105 de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em 01 de março de 2018.

BRASIL. **Portaria Interministerial CGU MP n. 140, de 16 de março de 2006. Disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet, e dá outras providências.** Disponível em: <http://www.cgu.gov.br/sobre/legislacao/arquivos/portarias/portaria_cgumpog_140_2006.pdf>. Acesso em 01 de março de 2018.

BRASIL. **Súmulas CMRI n. 1 a 6, de 27 de janeiro de 2015**. Disponível em: http://www.acessoainformacao.gov.br/assuntos/recursos/recursos-julgados-a-cmri/sumulas-eresolucoes. Acesso em 01 de março de 2018.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. São Paulo: Atlas, 2013.,
CONTROLADORIA-GERAL DA UNIÃO. **Acesso à Informação Pública: uma introdução à Lei n. 12.527/2011. Brasília: Imprensa Nacional, 2011.** Disponível em: <http://www.acessoainformacao.gov.br/central-de-conteudo/publicacoes/cartilhaacessoainformacao-1.pdf>. Acesso em 01 de março de 2018.

CUNHA FILHO, Márcio Camargo; XAVIER, Vítor César Silva. Lei de Acesso à Informação: teoria e prática. Rio de Janeiro: Lumen Juris, 2014.

FERNANDES, Bernardo Gonçalves. **Teoria Geral dos Direitos Fundamentais**. Bahia: Jus¬Podivm, 2012.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo.** São Paulo: Malheiros, 2013.

NOGUEIRA JÚNIOR, Alberto. **Cidadania e direito de acesso aos documentos administrativos**. Rio de Janeiro: Renovar, 2003.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** São Paulo: Malheiros, 2010.

TAVARES, André Ramos. In: DIMOULIS, Dimitri (org.) **Dicionário Brasileiro de Direito Constitucional**. São Paulo: Saraiva, 2012.

XAVIER, Vitor Cesar Silva; CUNHA FILHO, Márcio Camargo. **Lei de Acesso à Informação: Teoria e Prática**. Rio de Janeiro: Lumen Juris, 2014.