CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL
DEPARTAMENTO DE ENSINO, PESQUISA, CIÊNCIA E TECNOLOGIA
DIRETORIA DE ENSINO
CENTRO DE ESTUDOS DE POLÍTICA, ESTRATÉGIA E DOUTRINA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS

Cap. QOBM/Compl. ALINE LEAL **GENSCHOW**

PROPOSTA DE REGULAMENTAÇÃO DO TRATAMENTO DA INFORMAÇÃO CLASSIFICADA PRODUZIDA PELO CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL

BRASÍLIA
2020

Cap. QOBM/Compl. ALINE LEAL **GENSCHOW**

PROPOSTA DE REGULAMENTAÇÃO DO TRATAMENTO DA INFORMAÇÃO CLASSIFICADA PRODUZIDA PELO CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL

Trabalho monográfico apresentado ao Centro de Estudos de Política, Estratégia e Doutrina como requisito para conclusão do Curso de Aperfeiçoamento de Oficiais Complementares do Corpo de Bombeiros Militar do Distrito Federal.

Orientador: Ten. Cel. QOBM/Comb. GUSTAVO FERREIRA **TARRAGÔ**

BRASÍLIA
2020

Cap. QOBM/Compl. ALINE LEAL **GENSCHOW**

PROPOSTA DE REGULAMENTAÇÃO DO TRATAMENTO DA INFORMAÇÃO CLASSIFICADA PRODUZIDA PELO CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL

Trabalho monográfico apresentado ao Centro de Estudos de Política, Estratégia e Doutrina como requisito para conclusão do Curso de Aperfeiçoamento de Oficiais Complementares do Corpo de Bombeiros Militar do Distrito Federal.

Aprovado em: 21/01/2020

BANCA EXAMINADORA

_____

Ten-Cel. QOBM/Comb. Fábio Martins da Silva
Presidente

_____

Maj. QOBM/Comb. André Matos Pinto Cota
Membro

_____

Prof. Msc. Zilta Diaz Penna Marinho
Membro

_____

Ten-Cel QOBM/Comb. Gustavo Ferreira Tarragô
Orientador

CESSÃO DE DIREITOS

AUTORA: Aline Leal **Genschow** – Cap. QOBM/Compl.

TEMA: Proposta de regulamentação do tratamento da informação classificada produzida pelo Corpo de Bombeiros Militar do Distrito Federal

ANO: 2020

São concedidas ao Corpo de Bombeiros Militar do Distrito Federal as seguintes permissões referentes a este trabalho acadêmico:

- Reprodução de cópias;
- Empréstimo ou comercialização de tais cópias somente para propósitos acadêmicos e científicos;
- Disponibilização nos *sites* do Corpo de Bombeiros Militar do Distrito Federal.

A autora reserva outros direitos de publicação e nenhuma parte desse trabalho acadêmico pode ser reproduzida sem autorização por escrito da autora.

_____

Aline Leal **Genschow** - Cap. QOBM/Compl.

Dedico este trabalho ao meu avô Fernando A. Genschow.

AGRADECIMENTOS

Agradeço a Deus por ter me abençoado com a profissão dos meus sonhos. Servir ao Corpo de Bombeiros Militar do Distrito Federal é uma das minhas maiores paixões.

Agradeço ao meu marido, Cap. Fiuza, pela parceria durante toda a realização do Curso de Aperfeiçoamento de Oficiais, dentro e fora de sala de aula, especialmente após a descoberta da chegada do novo bebê.

Aos meus filhos, Gabriel e Lolla, e ao bebê que está chegando, Samuel, por serem as maiores fontes de alegria e gratidão e por encherem a minha vida do maior amor do mundo.

À minha família, especialmente à minha mãe Maria Luiza, agradeço pelo apoio incondicional e afetuoso no cuidado com meus filhos, essencial para a elaboração da pesquisa e para a conclusão do Curso.

Agradeço ao meu orientador, Ten. Cel. QOBM/Comb. Gustavo Ferreira Tarragô, pela disponibilidade, dedicação e interesse na condução da presente pesquisa. Por ser uma grande referência de chefia, de militar comprometido com a corporação, e especialmente por me inspirar a ser uma melhor profissional na atividade de inteligência.

Agradeço ao Ten. Cel. QOBM/Comb. Fábio Martins da Silva, pela colaboração contínua e por toda atenção dispensada no desenvolvimento do trabalho.

Aos meus colegas de turma, agradeço pelos momentos de descontração, que certamente tornaram os últimos meses mais leves e agradáveis. Agradeço pelas profundas reflexões e deixo registrada minha enorme admiração pela vontade e empenho em elevar o CBMDF em seu maior potencial.

“Nada pode ser amado ou odiado sem antes ser compreendido.”

Leonardo da Vinci.

RESUMO

O objetivo da presente pesquisa é propor a regulamentação do tratamento da informação classificada produzida pelo Corpo de Bombeiros Militar do Distrito Federal (CBMDF) diante da ausência de normatização interna após a publicação da Lei Federal nº 12.527/2011, da Lei Distrital nº 4.990/2012, dos Decretos Distritais nº 34.276/2013 e nº 35.382/2014 e das Portarias nº 05/2016 e 09/2016 da Casa Militar do Distrito Federal. Para isso foram abordados os aspectos relacionados à transparência, ao sigilo e o impacto de tais institutos na atividade de inteligência, bem como os principais dispositivos legais que contemplam o tratamento da informação classificada e os atos normativos congêneres produzidos por outros órgãos públicos. Dessa forma, a pesquisa está baseada no método dedutivo, caracterizando-se como aplicada, exploratória, qualitativa, bibliográfica e documental. A revisão de literatura e os resultados obtidos demonstram a necessidade de adoção de parâmetros a serem seguidos para uma adequada elaboração de ato normativo interno que respeite os limites impostos pelos princípios constitucionais aplicáveis e que seja apropriado para as atividades da caserna no que concerne ao tratamento da informação classificada.

Palavras-chave: Corpo de Bombeiros Militar do Distrito Federal. Lei de Acesso à Informação. Direito ao sigilo. Informação classificada.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
CAEO	Curso de Altos Estudos para Oficiais
CAO	Curso de Aperfeiçoamento de Oficiais
CBMDF	Corpo de Bombeiros Militar do Distrito Federal
CCS	Certificados de Credenciamento de Segurança
CEINT	Centro de Inteligência
CGU	Controladoria Geral da União
CIDIC	Código de Indexação de Documento que contém Informação Classificada
DF	Distrito Federal
DINT	Diretoria de Inteligência
DITIC	Diretoria de Tecnologia da Informação
EB	Exército Brasileiro
FA's	Forças Armadas
FIDC	Formulário Individual de Dados para Credenciamento
GSC	Gestor de Segurança e Credenciamento
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IGSAS	Instruções Gerais para a Salvaguarda de Assuntos Sigilosos
LAI	Lei de Acesso à Informação
NSC	Núcleo de Segurança e Credenciamento
NUP	Número Único de Protocolo
OM	Organização Militar
PC	Posto de Controle
SEI	Sistema Eletrônico de Informação
SEOPI	Secretaria de Operações Integradas
SI	Subsecretaria de Inteligência
SIC	Serviço de Informações ao Cidadão
SISBIN	Sistema Brasileiro de Inteligência
SSPDF	Secretaria de Estado de Segurança Pública do Distrito Federal
TCI	Termo de Classificação de Informação
TCMS	Termo de Compromisso de Manutenção de Sigilo

SUMÁRIO

1 INTRODUÇÃO

A promulgação da Constituição Federal de 1988 trouxe ao ordenamento jurídico brasileiro parâmetros gerais de acesso às informações oriundas de órgãos públicos, garantindo ao cidadão o conhecimento dos registros e atos da administração pública, conforme se verifica pela leitura dos dispositivos abaixo destacados:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e 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 de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestados no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
>
> [...]
>
> Art. 37º. A administração pública direta e indireta de qualquer dos poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência e, também ao seguinte:
>
> [...]
>
> § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulamentando especialmente:
>
> [...]
>
> II – o acesso dos usuários a registros administrativos e a informações sobre atos do governo, observado o disposto no artigo 5º, X e XXXIII;
>
> [...]
>
> Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
>
> [...]
>
> § 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.(CF, 1988).

Neste sentido, o legislador infraconstitucional editou a Lei Federal nº 12.527, de 18 de novembro de 2011, denominada Lei de Acesso à Informação (LAI) que cria procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios com o fim de garantir o acesso às informações a todos os cidadãos.

Em decorrência da edição da LAI em âmbito federal, foi publicada a Lei Distrital nº 4.990, em 12 de dezembro de 2012, que regula o acesso a informações no Distrito Federal.

Ato contínuo, foi publicado o Decreto Distrital nº 34.276/2013 que regulamenta, no âmbito do Poder Executivo do Distrito Federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados o grau e prazo de sigilo, conforme disposto na Lei Distrital nº 4.990/2012 e na Lei Federal nº 12.527/2011.

Foi publicado, ainda, o Decreto Distrital nº 35.382/2014, que regulamenta o art. 42 da Lei Distrital nº 4.990/2012 e dispõe sobre os procedimentos para credenciamento de segurança e o tratamento de informações ou dados classificados em qualquer grau de sigilo.

Por fim, a Casa Militar do Distrito Federal publicou as Portarias nº 05/2016 e 09/2016 que dispõem sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Distrital.

Diante de toda a legislação produzida desde a promulgação da Constituição Federal, compreende-se que, em regra, cabe ao Corpo de Bombeiros Militar do Distrito Federal (CBMDF), órgão da administração direta e integrante do Sistema de Segurança Pública do Distrito Federal (SSPDF), conferir acesso às informações produzidas em seu âmbito interno.

Contudo, a própria legislação estabelece as hipóteses excepcionais em que o sigilo das informações produzidas pela administração pública é necessário, motivo pelo qual se infere que também é atribuição do CBMDF regulamentar os procedimentos para a gestão da informação classificada ou sob restrição de acesso dentro da sua área de atuação.

Face ao exposto, o presente trabalho aborda a regulamentação do tratamento da informação classificada produzida pelo CBMDF diante da publicação da LAI e demais legislações que versam sobre os procedimentos adequados ao acesso à informação em âmbito federal e distrital.

1.1 Definição do problema

A Lei nº 12.527/2011 e as posteriores regulamentações Distritais que se fizeram presentes no ordenamento jurídico desde o ano de 2011 possibilitaram ao cidadão o direito fundamental de acesso à informação, obrigando os órgãos públicos da administração direta e indireta a conferirem publicidade aos seus atos e procedimentos, propiciando uma gestão transparente, com amplo acesso e divulgação.

Contudo, sabe-se que alguns desses atos e procedimentos produzidos pela administração pública estão investidos de informações sigilosas e devem ser submetidos à restrição de acesso em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou seja, devem ser submetidos a um tratamento específico.

Neste sentido, destaque-se que o artigo 7º, inciso IV, da Portaria nº 05/2016 da Casa Militar do Distrito Federal determina que os Gestores de Segurança e Credenciamento (GSC)[1] dos órgãos e entidades públicas devem propor à autoridade máxima a proposição de normas para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos.

Verifica-se, portanto, a necessidade de que cada órgão público conduza o tratamento das suas informações classificadas de acordo com suas particularidades e em consonância com a legislação vigente.

Assim, diante dos aspectos contemplados nos parágrafos anteriores, surge a pergunta problema norteadora do presente trabalho: de que forma o CBMDF pode normatizar o tratamento das suas informações classificadas, cumprindo o previsto nas normas que regulamentam o acesso à informação?

[1] Atualmente, o Gestor de Segurança e Credenciamento do CBMDF é o Comandante do Centro de Inteligência.

1.2 Justificativa

A escolha do presente tema foi motivada pela vivência profissional desta oficial, lotada no Centro de Inteligência (CEINT) do CBMDF, unidade que tem como atribuição legal preservar o sigilo institucional, promover e propor a regulamentação do tratamento de informações sigilosas e garantir a segurança de tais informações.

Outro ponto fundamental para a escolha do tema foi o trabalho monográfico apresentado pelo Tenente Coronel QOBM/Comb. Fábio Martins da Silva, atual Subcomandante do CEINT/CBMDF, como requisito para conclusão do Curso de Altos Estudos para Oficiais (CAEO) no ano de 2016.

Na oportunidade, o referido oficial superior discorreu sobre o cumprimento da LAI/DF por parte do CEINT/CBMDF, no que se refere ao tratamento das informações classificas, e concluiu pela necessidade de promoção de diversas adequações, no âmbito da Corporação, para ajustamento ao previsto na LAI e demais regulamentações.

Destaque-se que o trabalho apresentado em sede de CAEO, pelo Ten. Cel. QOBM/Comb. Fábio, possui um enfoque estratégico, de análise global e abrangente sobre a atuação do CEINT no âmbito do tratamento da informação classificada. Já o presente trabalho, apresentado em sede de Curso de Aperfeiçoamento de Oficiais (CAO), possui um enfoque tático e com o objetivo de criar condições para que as ações estabelecidas no planejamento estratégico sejam atingidas, por meio da proposta de regulamentação do tratamento da informação classificada produzida pelo CBMDF.

Ressalte-se, ainda, que o assunto é relevante uma vez que a LAI/DF foi publicada em dezembro de 2012, ou seja, há quase sete anos, e apesar da Corporação realizar o tratamento das informações classificadas de acordo com a legislação existente no ordenamento jurídico vigente, não produziu próprio ato normativo capaz de se adequar às particularidades institucionais.

1.3 Objetivos

1.3.1 Objetivo geral

Propor a regulamentação do tratamento da informação classificada produzida pelo CBMDF, com respaldo na Lei Federal nº 12.527/2011, na Lei Distrital nº 4.990/2012, nos Decretos Distritais nº 34.276/2013 e nº 35.382/2014, e nas Portarias nº 05/2016 e 09/2016 da Casa Militar do Distrito Federal, que tratam dos procedimentos adequados ao acesso à informação em âmbito federal e distrital.

1.3.2 Objetivos específicos

- Elencar os princípios constitucionais e legais que se relacionam ao acesso à informação e ao tratamento das informações classificadas;
- Apresentar um panorama sobre a transparência dos atos administrativos e a possibilidade de limitação de acesso por meio do sigilo;
- Verificar as consequências trazidas à atividade de inteligência por meio da edição da LAI;
- Apresentar os dispositivos legais que abordam o tratamento das informações classificadas em âmbito Federal e Distrital;
- Relacionar os principais dispositivos do Decreto nº 31.817/2010, que dispõe sobre a Organização Básica do CBMDF e do Regimento Interno do CEINT no que se referem ao tema em estudo;
- Apreciar os atos normativos já produzidos no âmbito de outros órgãos públicos.

1.4 Questões

Ao propor a regulamentação do tratamento da informação classificada produzida pelo CBMDF, demonstra-se relevante pontuar quais questões norteadoras foram utilizadas para desenvolvimento da pesquisa.

Quais princípios e conceitos doutrinários foram utilizados como pilares para elaboração da regulamentação do tratamento da informação classificada produzida pelo CBMDF?

Quais foram os impactos causados pela edição da LAI no que concerne a atividade de inteligência?

Quais dispositivos legais que se relacionam ao tratamento da informação classificada foram aplicados ao CBMDF para adequação à realidade da caserna?

Quais atos normativos já produzidos no âmbito de outras instituições trouxeram um direcionamento sobre a forma e o conteúdo da norma a ser elaborada?

1.5 Definição de termos

Gestor de segurança e credenciamento (GSC): responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle. (BRASIL, 2012).

Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. (BRASIL, 2011).

Órgão de registro nível 1: secretaria ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento (DISTRITO FEDERAL, 2014).

Órgão de registro nível 2: órgão ou entidade pública vinculada ao órgão de registro nível 1 e por este habilitado (DISTRITO FEDERAL, 2014).

Tratamento da informação classificada: conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo. (BRASIL, 2012).

2 REVISÃO DA LITERATURA

2.1 Princípios constitucionais aplicáveis

A Constituição Federal de 1988 elencou os princípios básicos da administração pública. Além disso, outros princípios que regulamentam a atividade do administrador público podem ser observados ao longo do texto constitucional e das demais normas congêneres.

No âmbito da presente pesquisa, os princípios da publicidade, transparência e da supremacia do interesse público apresentam destaque em razão da relevância para a temática relacionada à LAI.

Segundo Gonçalves e Varella (2018), percebe-se uma antinomia aparente entre os princípios em análise, não havendo, contudo, uma hierarquia entre eles. Assim, a solução para os conflitos apresentados deve ser encontrada a partir da análise do caso concreto, por meio de um verdadeiro processo de harmonização e ponderação entre os princípios.

2.1.1 Princípio da publicidade

Expressamente disposto no art. 37, *caput*, da Constituição Federal, esse princípio garante que os processos desenvolvidos pela administração sejam abertos ao acesso dos interessados (DI PIETRO, 2014).

Para Canotilho (2013, p. 887), o princípio da publicidade pode ser caracterizado como um direito fundamental, compreendido como “o dever estatal de promover amplo e livre acesso à informação como condição necessária ao conhecimento, à participação e a controle da Administração”.

Meireles (2007) acrescenta que a publicidade abrange toda a atuação estatal no que se refere à divulgação oficial de seus atos e também no que tange ao conhecimento da conduta interna de seus agentes.

Assim, percebe-se que a edição da LAI Federal, da LAI Distrital e dos Decretos regulamentadores está em consonância com a orientação trazida pelo princípio em apreço e trouxe contribuições significativas na alteração da dinâmica da transparência dos atos normativos.

Neste sentido, Heinen (2015, p. 42) esclarece que foram criados "inúmeros portais de transparência inseridos em específicos sítios virtuais, consistindo em um depósito de importantíssimas informações da dinâmica do Estado".

Ressalte-se, por fim, que o princípio da publicidade está intrinsecamente relacionado ao conceito de transparência, conforme afirma Bandeira de Mello (2008, p.114): "o princípio da publicidade consiste no dever que tem a administração de manter plena transparência em seus comportamentos".

2.1.2 Princípio da transparência

Como decorrência direta do princípio da publicidade, o princípio da transparência começou a ser celebrado no ordenamento jurídico brasileiro a partir da promulgação da Constituição Federal de 1988 e está inserido de forma implícita na Carta Magna.

Segundo Heinen (2015), a transparência atinge vários ramos do direito, que não apenas o direito administrativo, chegando a ser considerada como um verdadeiro dever da administração pública.

Para Martins Júnior (2010, p. 47), o princípio da transparência é composto pelos subprincípios da publicidade, da motivação, e da participação popular na gestão administrativa, e acrescenta:

> O princípio da transparência reúne funções materiais e instrumentais: aperfeiçoamento do caráter democrático do Estado (pela legitimidade do uso e do exercício do poder e da função pública), concretização da dignidade da pessoa humana, restauração da confiança na Administração Pública (pelas possibilidades de acesso e participação), parâmetro do controle da fidelidade do devido processo legal administrativo, garantia dos direitos dos administrados, recuso de obtenção de eficiência da ação administrativa mais próxima das demandas sociais e meio de maior adesão e consenso dos administrados às decisões administrativas. (MARTINS JÚNIOR, 2010, p. 47)

Dessa forma, a edição da LAI trouxe à administração pública elementos eficazes para aplicação do princípio da transparência nos processos e atos administrativos, permitindo a ampla participação do cidadão e o direito de fiscalizar a prestação de serviços públicos. Nas palavras de Heinen (2015, p. 61),

> Tal diploma legislativo, ao nosso sentir, causou uma autêntica revolução no limiar da Administração Pública, especialmente no que se refere à relação entre os Poderes Públicos e os administrados, porque trouxe uma nova roupagem neste liame jurídico. Ela tratou de balancear os interesses privados e públicos, e é justamente porque esta regra causou uma modificação por deveras intensa nas relações jurídico-administrativas, instaurando o paradigma da transparência de uma forma tão radical, que releva abordá-la de forma sistematizada e pormenorizada. (HEINEN, 2015, p.61)

2.1.3 Princípio da supremacia do interesse público

Nos termos do disposto no art. 2º, parágrafo único, inciso II, da Lei nº 9.784/99, o princípio da supremacia do interesse público corresponde ao "atendimento a fins de interesse geral, vedada a renúncia total ou parcial de poderes ou competência, salvo autorização em lei."

Conforme afirma Meirelles (2007, p. 103), o princípio em apreço está intimamente ligado ao princípio da finalidade, uma vez que "a primazia do interesse público sobre o privado é inerente à atuação estatal e domina-a, na medida em que a existência do Estado justifica-se pela busca do interesse geral."

Observa-se que a regulamentação de acesso à informação, especialmente no que tange ao tratamento da informação classificada, possui como pilar o princípio da supremacia do interesse público, pois garante à Administração Pública a proteção de determinadas informações consideradas imprescindíveis à segurança da sociedade e do Estado.

Neste sentido, demonstra-se oportuno apresentar a conclusão de Rodrigues (2014, p. 9) sobre a possibilidade de ponderação dos princípios anteriormente estudados (publicidade e transparência) em detrimento do princípio da supremacia do interesse público, a saber: "os princípios da publicidade e transparência compartilham dessa natureza relativa (as restrições constitucionais e legais os relativizam) comportando exceções válidas dentro da administração pública."

2.2 Definição de transparência e sua difusão no Brasil

A Constituição Federal em 1988 trouxe ao ordenamento jurídico brasileiro bases para a organização do Estado Democrático de Direito, com especial destaque ao instituto da transparência, que disciplina a participação popular nas atividades exercidas pela Administração direta e indireta.

Segundo Macedo (2014, p. 8), transparência está intrinsecamente ligada ao conceito de democracia e pode ser definida como uma "norma integrante do processo de consolidação democrática, que diz respeito à capacidade de disponibilizar informações por parte do governo para a sociedade e que pode ser avaliada por meio do estudo sobre a lei de acesso à informação."

Diante do texto constitucional, o acesso à informação passou a ser regra, e o sigilo, exceção. Assim, começaram a surgir no país os principais movimentos relacionados ao direito à informação e ao combate à corrupção, como a ONG Transparência Brasil, fundada no ano 2000, o Fórum de Direito de Acesso a Informações Públicas, com atividades desde o ano de 2004, a ONG internacional Artigo 19, presente no Brasil desde o ano de 2007, dentre outros.

Acompanhando a preocupação da sociedade civil diante dos assuntos relacionados ao tema, o Poder Executivo, por meio do Conselho de Transparência Pública e Combate à Corrupção, órgão coordenado pela Controladoria Geral da União (CGU), submeteu à deliberação do Congresso Nacional o projeto de Lei de Acesso à Informação Pública, em maio de 2009.

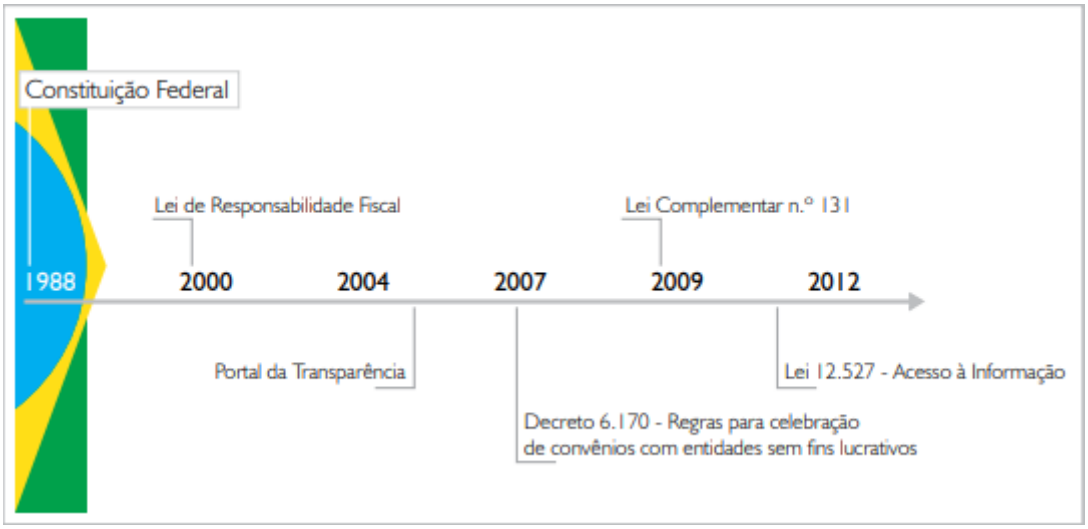
Após o transcurso de 23 (vinte e três) anos da promulgação da Constituição Federal, em 18 de novembro de 2011 a Lei nº 12.527 foi publicada, dispondo sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no texto constitucional.

Outras normas relacionadas ao acesso às informações públicas foram publicadas a partir da Constituição Federal de 1988, como por exemplo, a Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000, com acréscimos trazidos pela Lei Complementar nº 131/2009), e o Decreto que criou o Sistema de Gestão de

Convênios e Contratos de Repasse (Decreto nº 6.170/2007).

Além da edição das referidas normas, o Governo Federal, em novembro de 2004, lançou o Portal da Transparência do Poder Executivo Federal, que tem como objetivo apoiar a correta aplicação dos recursos públicos ao possibilitar o acompanhamento e fiscalização dos gastos da administração.

Figura 1 – Histórico de normativos que ampliaram o acesso à informação no Brasil



Fonte: Controladoria Geral da União (CGU)

Segundo Heinen (2015), a LAI trouxe uma nova realidade nas relações jurídico-administrativas, uma vez que impõe mecanismos específicos no sentido de permitir que o maior número possível de pessoas possa acessar os dados disponibilizados pela administração, além de garantir uma linguagem de fácil compreensão, por meio de técnicas de busca eficientes.

Macedo (2014) afirma que a partir dessa nova compreensão sobre o acesso à informação no país, os órgãos públicos passaram a ser vistos não como detentores das informações, mas como verdadeiros guardiões do bem público.

Assim, depreende-se que um dos objetivos principais da edição da LAI foi implementar um sistema de gestão transparente por meio da divulgação de informações de interesse público, além de facilitar o acesso das pessoas e reduzir custos com a prestação de informações.

2.3 Direito ao sigilo

Diante dos avanços trazidos pela LAI no que tange à publicidade dos atos administrativos, percebeu-se a necessidade de proteção de determinadas informações consideradas sigilosas. O próprio legislador infraconstitucional (BRASIL, 2011) conceitua informação sigilosa como “aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”

Para a doutrina, existe uma inevitável tensão entre o sigilo e a transparência, motivo pelo qual Rosseti (2012, p. 8) afirma que a LAI pode ser compreendida como um avanço sem precedentes no sentido de se efetivar o direito fundamental da liberdade de expressão, “mas há de ser compatibilizada com outros princípios e garantias que estão no mesmo nível constitucional de importância e são essenciais a existência e manutenção do próprio Estado e sociedade.”

Vilar-Lopes (2017, p.42), a partir do entendimento de que nenhum direito fundamental é absoluto, destaca que a LAI definiu “a ressalva constitucional do sigilo a partir do momento em que esta se mostra imprescindível à segurança da sociedade e do Estado”.

Para Rodrigues (2014, p. 15), as restrições à publicidade se apresentam como necessárias numa sociedade democrática, “sendo orientadas por direitos sociopolíticos supraindividuais como segurança nacional, da sociedade e do Estado (âmbito público) ou direitos personalíssimos como honra, intimidade ou vida privada (no âmbito privado).”

Calderon (2014), por sua vez, conclui que a utilização do sigilo por parte da administração pública deve ter sustentação em princípios sólidos e democráticos, para que seja capaz de justificar o aleijamento do direito de acesso à informação, reconhecido a partir de sua condição inafastável de direito fundamental.

Assim, o enfoque do presente trabalho é a garantia do direito ao sigilo em razão da especificidade de determinadas atividades exercidas pela Corporação, em especial pelo CEINT, consubstanciado no tratamento das informações classificadas no âmbito do CBMDF.

2.4 A atividade de inteligência e o acesso à informação

Entende-se como atividade de inteligência aquela que se destina a coletar, analisar e disseminar informações importantes para o processo decisório. Sua definição legal está disposta no artigo 1º, §2º, da Lei nº 9.883/1999, abaixo colacionado:

> Para os efeitos de aplicação desta Lei, entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado. (BRASIL, 1999).

Neste sentido, ao se regressar ao texto constitucional (artigo 5º, inciso XXXIII), verifica-se que o próprio legislador cita o parâmetro legal para o acesso à informação e dá destaque para sua exceção (direito ao sigilo), que passa a ser considerado norte da atuação da atividade de inteligência no país (VILAR-LOPES, 2017).

Gonçalves (2011 apud CALDERON, 2014, p.40) aponta os elementos essenciais ao conceito de inteligência, a saber:

> 1) a ideia de conhecimento processado – a partir de fontes (abertas ou não, chega-se a um produto de uma análise com base nos princípios e métodos da doutrina de inteligência;
>
> 2) o manuseio de informações sigilosas (dado negado) referentes a ameaças e oportunidades – reais ou potenciais – relacionadas a assuntos de interesse do tomador de decisão. A inteligência lida, necessariamente, com aspectos sigilosos;
>
> 3) o objetivo central, que é assegurar o processo decisório e, no caso da inteligência de Estado, salvaguardar os interesses nacionais. (GONÇALVES, 2011 apud CALDERON, 2014, p.40)

Diante disso, verifica-se que o acesso a informações sigilosas (ou a dados negados) é inerente à atividade de inteligência e a todo o processo através do qual o conhecimento é produzido. A própria Lei nº 9.883/99, que institui o Sistema Brasileiro de Inteligência (SISBIN) e cria a Agência Brasileira de Inteligência (ABIN), dispõe especificamente sobre o sigilo, nos termos seguintes:

> Art. 9º Os atos da ABIN, cuja publicidade possa comprometer o êxito de suas atividades sigilosas, deverão ser publicados em extrato.
>
> § 1º Incluem-se entre os atos objeto deste artigo os referentes ao seu peculiar funcionamento, como às atribuições, à atuação e às especificações dos respectivos cargos, e à movimentação dos seus titulares.
>
> § 2º A obrigatoriedade de publicação dos atos em extrato independe de serem de caráter ostensivo ou sigiloso os recursos utilizados, em cada caso.
>
> Art. 9º A - Quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los, pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado. (Incluído pela Medida Provisória nº 2.216-37, de 2001)
>
> § 1º O fornecimento de documentos ou informações, não abrangidos pelas hipóteses previstas no caput deste artigo, será regulado em ato próprio do Chefe do Gabinete de Segurança Institucional da Presidência da República (Incluído pela Medida Provisória nº 2.216-37, de 2001)
>
> § 2º A autoridade ou qualquer outra pessoa que tiver conhecimento ou acesso aos documentos ou informações referidos no caput deste artigo obriga-se a manter o respectivo sigilo, sob pena de responsabilidade administrativa, civil e penal, e, em se tratando de procedimento judicial, fica configurado o interesse público de que trata o art. 155, inciso I, do Código de Processo Civil, devendo qualquer investigação correr, igualmente, sob sigilo. (Incluído pela Medida Provisória nº 2.216-37, de 2001). (BRASIL, 1999)

Para Rosseti (2012, p. 33), os assuntos relacionados à atividade de inteligência são indispensáveis para a preservação do Estado e da sociedade, especialmente no que concerne à defesa nacional, soberania, relações internacionais, defesa interna, segurança pública, dentre outros; motivo pelo qual “o sigilo se impõe como um elemento fundamental para que o Estado, através de suas instituições legalmente competentes para tanto, atue em tais campos com sucesso, preservando os seus interesses e os da sociedade”.

Assim, enquanto o acesso à informação está intrinsecamente ligado à publicidade, a atividade de inteligência está ligada ao sigilo. Nos dizeres de Vilar-Lopes, (2017, p. 40),

> A LAI é outra importante fomentadora do controle da Atividade de Inteligência, que ajuda a manter a excepcionalidade do sigilo, e, ao mesmo tempo, busca garantir publicidade até mesmo de partes de documentos considerados sigilosos.
>
> Como se vê, a tensão entre publicidade, transparência, acesso à informação e sigilo é permanente, mas compatível, sobretudo em países democráticos que possuem um eficaz sistema de controle sobre a Inteligência de Estado.

> [...]
> Assim, assume-se que o sigilo inerente à atividade de inteligência não atrapalha o direito de acesso à informação; restando saber se essa compatibilidade jurídica encontra efetividade nas leis e políticas públicas brasileiras de acesso à informação. (VILAR-LOPES, 2017, p. 40),

Nessa perspectiva, Calderon (2014, p. 42) acrescenta, oportunamente, que “importante mecanismo que leva à compatibilização do sigilo com o princípio democrático é o controle da atividade de inteligência, a ser realizado de maneira eficaz tanto no âmbito externo quanto interno.”

Face ao exposto, entende-se que a legitimação das ações estatais sigilosas e sua compatibilidade com o Estado Democrático de Direito possibilita a continuidade da atividade de inteligência à luz da atual legislação de acesso à informação.

2.5 Legislação aplicada

Para o alcance do objetivo geral da presente pesquisa, demonstrou-se necessária a verificação cautelosa da legislação aplicada ao tema em análise, que teve sua origem na Constituição Federal de 1988 e sua evolução após 23 (vinte e três) anos, por meio da publicação da LAI e demais normas congêneres.

Em razão da delimitação do tema, serão abordados apenas os principais dispositivos das normas editadas em âmbito Federal e Distrital, aptos a contribuir com a construção de ato normativo próprio no que concerne especificamente ao tratamento da informação classificada produzida pelo CBMDF.

2.5.1 Lei nº 12.527/2011

Em 18 de novembro de 2011 foi publicada a Lei Federal nº 12.527, que cria procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios com o fim de garantir o acesso às informações a todos os cidadãos, denominada Lei de Acesso à Informação.

Sob a ótica de Calderon (2014, p. 44), a edição da LAI não representa efetivamente uma novidade ao ordenamento jurídico brasileiro, pois o texto

Constitucional de 1988 já trazia inovações a respeito do acesso à informação. A sua característica mais impactante reside no fato de que seus dispositivos representam mais do que simples conselhos, “mas mecanismos concretos de transparência ativa – divulgação espontânea de informações públicas, sem prévia solicitação – e de transparência passiva – divulgação de informações públicas mediante solicitação”.

A LAI pode ser classificada como uma norma geral, uma vez que se propõe a regular todas as hipóteses relativas ao acesso à informação, assim como as possibilidades de restrição, com caráter vinculante sobre todos os entes da federação. Nestes termos, o artigo 1º dispõe que os procedimentos abordados pela norma devem ser observados pela União, Estados, Distrito Federal e Municípios:

As importantes diretrizes que asseguram o direito fundamental de acesso à informação estão dispostas no art. 3º, a saber:

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
>
> I - observância da publicidade como preceito geral e do sigilo como exceção;
>
> II - divulgação de informações de interesse público, independentemente de solicitações;
>
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
>
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
>
> V - desenvolvimento do controle social da administração pública. (BRASIL, 2011)

Por se tratar de uma matéria não regulamentada anteriormente, a LAI trouxe definições para a compreensão dos novos procedimentos a serem adotados pelos órgãos públicos atingidos pela norma. Essas definições estão consubstanciadas em seu art. 4º e se referem a conceitos como informação sigilosa, informação pessoal, tratamento da informação, dentre outros.

> Art. 4º Para os efeitos desta Lei, considera-se:
>
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
>
> II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
>
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
>
> V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
>
> VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
>
> VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
>
> VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
>
> IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. (BRASIL, 2011)

O artigo 6º dispõe sobre as obrigações dos órgãos públicos destinatários da norma, que devem assegurar a gestão transparente da informação, bem como a proteção da informação sigilosa e da informação pessoal. O artigo 7º, por sua vez, enumera em um rol exemplificativo, as informações que devem ser fornecidas a todos os cidadãos.

A LAI Federal prevê, ainda, em seu artigo 15 e subsequentes, a possibilidade de revisão e recurso relativo à negativa de concessão de informação por parte do órgão competente.

Por meio dos artigos 21 e 22, o legislador infraconstitucional relaciona as hipóteses de restrições de acesso à informação.

> Art. 21. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.
>
> Parágrafo único. As informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso.
>
> Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público. (BRASIL, 2011)

Já o artigo 23 elenca quais informações são consideradas imprescindíveis à segurança da sociedade e do Estado e, portanto, passíveis de classificação.

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
>
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações. (BRASIL, 2011)

Os graus de sigilo das informações, as autoridades competentes para classificá-las, e a possibilidade de delegação estão dispostos nos artigos 24 e 27 e foram compilados no quadro a seguir, para melhor elucidação da matéria que se apresenta para análise:

Figura 2 – Graus de sigilo e autoridades classificadoras

Grau de sigilo	Autoridade Classificadora	Possibilidade de Delegação
Reservado	**INCISO I** Presidente da República; Vice Presidente; Comandante das FA's; Chefes das Missões Diplomáticas.	Não.
	INCISO II Autarquias, Fundações, Empresas Públicas e Sociedades de Economia Mista	
	INCISO III Funções de Direção, Chefia e Assessoramento (DAS 101.5)	
Secreto	**INCISOS I e II**	Sim.
Ultrassecreto	**INCISO I**	

Fonte: a autora.

Da simples análise da figura 2, percebe-se que a quantidade de autoridades com poder de classificar reduz na medida em que a sensibilidade das informações aumenta. Assim, enquanto várias categorias de autoridade podem classificar informações como reservadas, a classificação ultrassecreta é, em regra, exclusiva para as autoridades máximas.

No que concerne à delegação da classificação, a LAI prevê que seria possível a qualquer agente público apenas nas hipóteses de informações secretas ou ultrassecretas, não trazendo qualquer previsão em relação às informações reservadas. Neste sentido, Calderon (2014, p. 49) afirma que:

> De um lado, se as informações secretas e ultrassecretas podem sofrer delegação do poder classificatório, às informações reservadas também poderia ser dado semelhante tratamento, em nome da máxima jurídica de que "quem pode o mais, pode o menos." Por outro lado, a extensão do rol de autoridades classificadoras mediante delegação implica em dilatação das exceções ao direito fundamental de acesso à informação. A exegese dos direitos fundamentais determina que, em se tratando de exceções a essa categoria de direitos, a sua interpretação deve ser restritiva. (CALDERON, 2014, p. 49)

Diante de tal conflito normativo, o Decreto nº 7.724/2012, que foi editado com o objetivo de regulamentar a LAI, admitiu a delegação da classificação de informações reservadas a agente público que exerça "função de direção, comando ou chefia", nos termos do artigo 30, parágrafo 2º:

> Art. 30 [...]
> §2º O dirigente máximo do órgão ou entidade poderá delegar a competência para classificação no grau reservado a agente público que exerça função de direção, comando ou chefia (BRASIL, 2012).

Em relação aos prazos de classificação, as categorias de informações produzidas por órgãos públicos, elencadas no artigo 23 (questões de soberania e defesa, relações internacionais, estabilidade econômica e financeira do país, vida, segurança e saúde da população, atividades de inteligência, investigações ou fiscalizações em andamento, dentre outras), estão passíveis de sofrer restrição de acesso, tendo como marco inicial a data de sua produção, nos moldes do parágrafo 5º do artigo 24:

> Art. 24 [...]
>
> § 5º Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:
>
> I - a gravidade do risco ou dano à segurança da sociedade e do Estado; e
>
> II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final. (BRASIL, 2011)

Os prazos de restrição de acesso público às informações classificadas e a possibilidade de prorrogação estão consubstanciados no parágrafo 1º do artigo 24 e no artigo 35, e foram registrados na figura 3:

Figura 3 – Prazos para classificação de informações

Grau de sigilo	Prazo	Prorrogação
Reservado	5 anos	Sim, até o final do mandato presidencial (máximo de 8 anos) em situações de risco para o Presidente, Vice Presidente e seus familiares.
Secreto	15 anos	Não.
Ultrassecreto	25 anos	Sim, única prorrogação por prazo não maior de 25 anos, em casos de soberania nacional, por decisão da Comissão Mista de Reavaliação

Fonte: a autora.

Os artigos 25 e 26 abordam a proteção e o controle das informações sigilosas como dever do Estado e pontuam as providências necessárias ao conhecimento dos procedimentos de segurança para o tratamento dessas informações, nos termos seguintes:

> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção. (Regulamento)
>
> § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.
>
> § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.
>
> § 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.
>
> Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.

> Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei. (BRASIL, 2011)

Outro caso de acesso restrito, previsto no artigo 31, diz respeito ao tratamento das informações pessoais, conceituadas como aquelas relacionadas à "intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (BRASIL, 2011). Nesses casos específicos, o legislador estabeleceu o prazo de 100 (cem) anos para que as informações fiquem limitadas ao acesso do público, independentemente de classificação de sigilo. Excepcionalmente, os agentes públicos que tenham autorização legal para o acesso e a própria pessoa a quem se refere a restrição podem ter ciência do conteúdo restrito:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. (BRASIL, 2011).

Por fim, o artigo 32 e seguintes estipulam as condutas ilícitas que ensejam a responsabilidade do agente público ou militar no âmbito da LAI e as sanções aplicáveis, quais sejam:

> Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:
>
> I - advertência;
>
> II - multa;
>
> III - rescisão do vínculo com o poder público;
>
> IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a 2 (dois) anos; e
>
> V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade. (BRASIL, 2011).

2.5.2 Lei nº 4.990/2012

Após a edição da LAI Federal, em 12 de dezembro de 2012, foi publicada a Lei Distrital nº 4.990, que regula o acesso a informações no Distrito Federal, e que serve de parâmetro para o CBMDF, por ser um dos destinatários da norma.

A LAI Distrital praticamente reproduz toda a regulamentação da LAI Federal para o âmbito local, trazendo alguns ajustes para efetiva aplicação da norma no ente federativo.

Figura 4 – Comparativo LAI Federal x LAI Distrital

	LAI FEDERAL	LAI DISTRITAL
Destinatários da norma	Art. 1º, I e II	Art.1º, I e II Texto similar
Diretrizes	Art. 3º	Art. 3º Texto idêntico
Conceitos	Art. 4º	Art. 4º Texto idêntico
Obrigações dos órgãos públicos	Art. 6º	Art. 6º Texto idêntico
O acesso à informação engloba direitos	Art. 7º	Art. 7º Texto idêntico
Dever de divulgar informações de interesses coletivos	Art. 8º	Art.8º Texto similar
Pedido de acesso	Arts. 10 a 14	Arts. 14 a 18 Texto similar
Dos recursos	Arts. 15 a 20	Arts. 19 a 22 Texto similar
Informações passíveis de classificação	Art. 23	Art. 25 Texto idêntico
Prazos de classificação	Art. 24	Art. 26 Texto idêntico
Proteção e controle	Arts. 25 e 26	Arts. 27 e 28 Texto idêntico
Competência para classificar	Art. 27	Art. 29 Texto similar
Informações pessoais	Art. 31	Arts. 33 e 34 Texto similar
Das Responsabilidades	Arts. 32 e 33	Arts. 35 e 36 Texto similar

Fonte: a autora.

Ao se realizar um comparativo entres os textos normativos que regulamentam o acesso à informação em âmbito federal e distrital, algumas poucas diferenças podem ser observadas.

Neste sentido, cumpre-nos ressaltar que todo parâmetro de estudo do presente trabalho se amolda perfeitamente tanto à Lei nº 12.527/2011 quanto à Lei nº 4.990/2012.

2.5.3 Decreto nº 34.276/2013

Para fins de regulamentação da Lei nº 4.990/2012, foi publicado o Decreto Distrital nº 34.276/2013 que relaciona os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados o grau e prazo de sigilo, no âmbito do Poder Executivo do Distrito Federal.

O presente Decreto trouxe novos e importantes elementos para a efetivação do acesso à informação no Distrito Federal, que serão relacionados a seguir.

Enquanto a LAI Distrital limita-se a pontuar os destinatários da norma, o Decreto nº 34.276/2013 inclui aqueles que não estão abrangidos pela legislação de acesso à informação, a saber:

> Art. 6º O acesso à informação disciplinado neste Decreto não se aplica às:
>
> I - hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça;
>
> II - informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado, na forma do §1º do art. 7º da Lei nº 4.990, de 2012; e
>
> III - informações relativas à atividade empresarial de pessoas físicas ou jurídicas de direito privado obtidas por órgãos ou entidades distritais no exercício de atividade de controle, regulação e supervisão da atividade econômica cuja divulgação possa representar vantagem competitiva a outros agentes econômicos. (DISTRITO FEDERAL, 2013).

tAdemais, quanto às informações oriundas da atuação de mercado das empresas públicas, sociedades de economia mista e demais entidades que atuem em regime de concorrência, o referido Decreto dispõe, em seu artigo 5º, parágrafo único, que “serão divulgadas de modo a não afetar sua competitividade, governança corporativa e, quando houver, os interesses de acionistas minoritários.” (DISTRITO FEDERAL, 2013).

Nos Capítulos III e IV, o Decreto nº 34.276/2013 se propõe a elencar os procedimentos necessários à promoção da transparência ativa e passiva por parte dos órgãos do Distrito Federal.

Heinen (2015, p. 75 e 76) conceitua transparência ativa como “dever de o Estado, independentemente de qualquer solicitação, fornecer certos dados” e transparência passiva como aquela que ocorre “quando o cidadão provoca o ente público para que este forneça os dados requeridos”.

Neste sentido, todas as informações que devem ser divulgadas pelos órgãos distritais em seus sítios oficiais na rede mundial de computadores (transparência ativa) estão dispostas no parágrafo 1º do artigo 7º:

> Art. 7º [...]
>
> §1º Na divulgação das informações de que trata o caput, devem constar, no que couber, no mínimo:
>
> I - registro das competências e da estrutura organizacional, endereços, telefones e correio eletrônico institucional das respectivas unidades e horários de atendimento ao público;
>
> II - registro de quaisquer repasses ou transferências de recursos financeiros;
>
> III - registro das despesas;
>
> IV - resultados de inspeções e auditorias, prestações de contas e tomadas de contas especiais realizadas pelos órgãos de controle interno e externo, incluindo prestação de contas relativas a exercícios anteriores;
>
> V - informações concernentes a procedimentos licitatórios, com os respectivos editais, anexos e resultados, bem como a todos os contratos celebrados;
>
> VI - dados gerais para o acompanhamento de programas, ações, projetos e obras, com informações sobre sua execução, metas e indicadores, em linguagem de fácil compreensão;
>
> VII - respostas a perguntas mais frequentes feitas pela sociedade;
>
> VIII - dados e execução de programas de desenvolvimento social e habitacional;
>
> IX - critérios de alocação e de uso dos recursos decorrentes de fundos públicos;
>
> X - contratos de gestão firmados com entidades qualificadas como organizações sociais;

> XI - informações sobre controle e fiscalização de recursos públicos destinados a organizações não governamentais;
>
> XII - valores e critérios de transferência de recursos financeiros às unidades escolares e às diretorias regionais de ensino, por meio de suas respectivas unidades executoras;
>
> XIII - relação de reclamações contra fornecedores de produtos e de serviços;
>
> XIV - relatórios com avaliações e dados da execução e da utilização das gratuidades concedidas pelo Sistema de Transporte Público Coletivo do Distrito Federal às pessoas com deficiência e a seus acompanhantes;
>
> XV - relatórios com avaliação e dados da execução do Passe Livre Estudantil.
>
> XVI - contato da autoridade de monitoramento, designada nos termos do art. 45 da Lei nº 4.990, de 2012, bem como telefone, correio eletrônico e horário de atendimento do Serviço de Informações ao Cidadão - SIC. (DISTRITO FEDERAL, 2013).

Além disso, tais sítios oficiais na rede mundial de computadores devem atender aos requisitos constantes do art. 8º, que pretendem facilitar a utilização por parte dos cidadãos.

> Art. 8º [...]
>
> I - conter redirecionamento para sistema eletrônico do Sistema de Informações ao Cidadão, a ser disponibilizado pela Secretaria de Estado de Transparência e Controle do Distrito Federal ou, na impossibilidade de sua utilização, formulário para pedido de acesso à informação;
>
> II - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
>
> III - possibilitar gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
>
> IV - possibilitar acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;
>
> V - divulgar em detalhes os formatos utilizados para estruturação da informação;
>
> VI - garantir autenticidade e integridade das informações disponíveis para acesso;
>
> VII - manter atualizadas as informações disponíveis para acesso;
>
> VIII - indicar instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou a entidade;
>
> IX - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei Federal nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008;
>
> X - conter os seguintes instrumentos de acesso às informações arquivísticas do órgão ou da entidade:
>
> a) Código de Classificação de Documentos de Arquivo das atividades-meio e das atividades-fim;
>
> b) Tabela de Temporalidade e Destinação de Documentos das atividades-meio e das atividades-fim;

> c) Vocabulário Controlado de termos relativos aos documentos de arquivo das atividades-meio e das atividades-fim. (DISTRITO FEDERAL, 2013).

No que concerne à transparência passiva, o Decreto dispõe, em seu artigo 9º, que todos os órgãos do Distrito Federal devem criar um Serviço de Informações ao Cidadão (SIC), no âmbito das respectivas ouvidorias, com os seguintes objetivos: 1- atender e orientar o público quanto ao acesso a informações; 2- receber e registrar documentos e pedidos de acesso a informações; e 3- e informar sobre a tramitação de documentos nas suas respectivas unidades.

Quanto à competência para classificação da informação, o quadro abaixo apresentado se propõe a facilitar a compreensão sobre o tema.

Figura 5 – Autoridades classificadoras no DF

Grau de sigilo	Autoridade Classificadora	Possibilidade de Delegação
Reservado	**INCISO I** Governador; Vice Governador; Secretário de Estado ou autoridade equivalente.	Sim.
	INCISO II Titulares de autarquia, fundação, empresa pública ou sociedade de economia mista;	
	INCISO III Autoridades que exerçam funções de subsecretário ou de hierarquia equivalente.	
Secreto	**INCISOS I e II**	Não
Ultrassecreto	**INCISO I**	

Fonte: a autora.

Por fim, destaque-se que foi criado um procedimento específico para classificação de informação, nos termos do artigo 31, com redação dada pelo Decreto nº 36.690/2015, consubstanciado no Termo de Classificação de Informação – TCI, que seguirá anexo à informação e deverá conter:

> Art. 31. A decisão que classificar a informação em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo Único, e conterá o seguinte:
>
> I - código de indexação de documento;
>
> II - grau de sigilo;
>
> III - categoria na qual se enquadra a informação;
>
> IV - tipo de documento;
>
> V - data da produção do documento;

> VI - indicação de dispositivo legal que fundamenta a classificação;
>
> VII - razões da classificação, observados os critérios estabelecidos no art. 27;
>
> VIII - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 28;
>
> IX - data da classificação; e
>
> X - identificação da autoridade que classificou a informação. (DISTRITO FEDERAL, 2013).

Anexo ao Decreto nº 34.276/2013, é apresentado um modelo de TCI, de preenchimento obrigatório por parte de todos os órgãos do Distrito Federal que efetivamente classificarem uma informação em qualquer grau de sigilo.

2.5.4 Decreto nº 35.382/2014

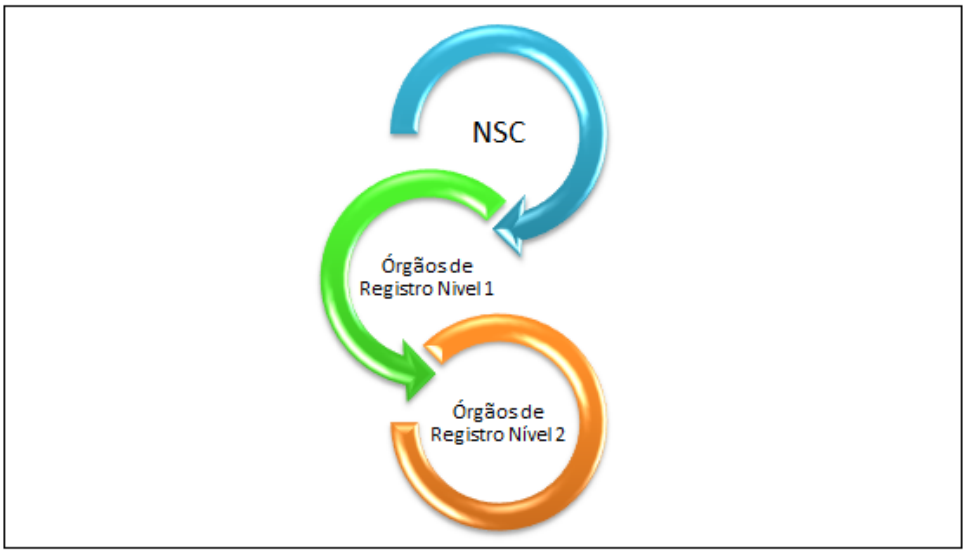
O Decreto Distrital nº 35.382/2014, que regulamenta o art. 42 da Lei Distrital nº 4.990/2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento (NSC), e institui o Comitê Gestor de Credenciamento de Segurança.

Com as alterações trazidas pelo Decreto nº 36.690/2015, o legislador distrital operacionalizou o NSC, no âmbito da Casa Militar do Distrito Federal, que tem como missões as dispostas em seu artigo 4º, a saber:

> Art. 4º Compete ao Núcleo de Segurança e Credenciamento:
>
> I – Habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada;
>
> II – Habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de documento controlado;
>
> III – Fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada;
>
> IV – Habilitar entidade privada que mantenha vínculo de qualquer natureza com a Casa Militar do Distrito Federal para o tratamento de informação classificada;
>
> V – Credenciar pessoa que mantenha vínculo de qualquer natureza com a Casa Militar do Distrito Federal para o tratamento de informação classificada; e
>
> VI – realizar inspeção e investigação para credenciamento de segurança necessária à execução do previsto nos incisos IV e V deste artigo. (DISTRITO FEDERAL, 2014)

Da leitura do indigitado dispositivo, verifica-se que o NSC é competente para habilitar órgãos capazes de credenciar outros órgãos, entidades públicas e privadas e pessoas para o tratamento da informação classificada. Neste sentido, esclarece-se que os órgãos de registro nível 1 são as secretarias (ou equivalentes) habilitados pelo NSC para credenciar outros órgãos, por sua vez denominados órgãos de registro nível 2, conforme compilado na figura abaixo:

Figura 6 – Funcionamento do credenciamento de órgãos para o tratamento da informação classificada.



Fonte: a autora

Ademais, o NSC é responsável por fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento da informação classificada no âmbito do Distrito Federal.

O Comitê Gestor de Credenciamento e Segurança, criado na esfera do NSC, é composto por representantes da Casa Militar do Distrito Federal, da Casa Civil do Distrito Federal, da Controladoria Geral do Distrito Federal, da Secretaria de Estado de Gestão Administrativa e Desburocratização do Distrito Federal e da Consultoria Jurídica do Distrito Federal, e tem como competências aquelas descritas no artigo 6º do Decreto em apreço:

> Art. 6º Compete ao Comitê Gestor de Credenciamento de Segurança do NSC:
>
> I – Propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada;

> II – Definir parâmetros e requisitos mínimos para:
>
> a) qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos do disposto nos artigos 11 e 12 deste Decreto;
>
> b) concessão de credencial de segurança para pessoas, nos termos do artigo 13 deste Decreto;
>
> III – Avaliar periodicamente o cumprimento do disposto neste Decreto. (DISTRITO FEDERAL, 2014)

Demais regras específicas relacionadas à segurança da informação classificada, ao acesso, ao controle e marcação do documento, à expedição, tramitação e comunicação, à reprodução, à segurança no arquivamento e na preservação, aos sistemas de informação, às áreas, instalações e materiais, à celebração de contratos sigilosos e à indexação de documento com informação classificada, estão inseridas no texto do Decreto nº 35.382/2014

Por fim, cumpre destacar que na data de 20 de dezembro de 2019 foi publicada a Lei nº 6.432, que transfere à Secretaria de Estado de Segurança Pública do Distrito Federal as atribuições previstas no artigo 42 da Lei nº 4.990/2012, anteriormente conferidas ao NSC da Casa Militar. Assim, o Decreto nº 35.382/2014, analisado no presente tópico, continua vigente até que seja adequado ao disposto na Lei nº 6.432/2019.

A Lei nº 6.432/2019 foi reproduzida em sua integralidade abaixo:

> .Art. 1º O caput do art. 42 da Lei nº 4.990, de 12 de dezembro de 2012, passa a vigorar com a seguinte redação:
>
> Art. 42. Cabem à Secretaria de Estado de Segurança Pública do Distrito Federal, na forma do regulamento, as seguintes atribuições:
>
> Art. 2 º As atribuições de que trata o art. 42 da Lei nº 4.990, de 2012, continuam sendo exercidas pelo Núcleo de Segurança e Credenciamento - NSC da Casa Militar até que sejam realizados os ajustes necessários à regulamentação desta Lei.
>
> Art. 3 º Os decretos de regulamentação do disposto no art. 42 da Lei nº 4.990, de 2012, vigentes à época da publicação desta Lei permanecem eficazes, naquilo que couber, até que sejam adequados ao disposto nesta Lei.
>
> Art. 4 º No prazo de até 10 dias contados da publicação desta Lei, a Secretaria de Estado de Segurança Pública do Distrito Federal apresentará proposta de decreto para sua regulamentação.
>
> Art. 5 º Esta Lei entra em vigor na data de sua publicação. (DISTRITO FEDERAL, 2019)

2.5.5 Portaria nº 05, de 29 de fevereiro de 2016

A Casa Militar do Distrito Federal publicou, em 29 de fevereiro de 2016, a Portaria nº 05, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Distrital.

Conforme mencionado no parágrafo anterior, tal normativo relaciona as diretrizes a serem adotadas pelos órgãos e entidades no âmbito do Poder Executivo Distrital, logo o CBMDF está abrangido pela norma.

Nos moldes do Decreto nº 35.382/2014, o NSC da Casa Militar do Distrito Federal habilita os órgãos de registro nível 1, que são as Secretarias ou órgãos de hierarquia equivalente. Tais órgãos, por sua vez, habilitam os órgãos de registro nível 2, que são os órgãos ou entidades públicas vinculados.

Conforme disposto nos artigos 3º e 4º da presente Portaria, são competências dos órgãos de registro de nível 1 e 2:

> Art. 3º O Órgão de Registro Nível 1, ao exercer as competências previstas no Decreto 35.382/2014, deve:
>
> I - encaminhar ao NSC, semestralmente e quando solicitado, relatórios sobre suas atividades de credenciamento, habilitação e seu funcionamento, bem como daqueles por ele habilitados;
>
> II - notificar o NSC, imediatamente, quando da quebra de segurança de informações classificadas: no próprio órgão, nos Órgãos de Registro nível 2 e nos Postos de Controle por ele habilitados.
>
> Art. 4º O Órgão de Registro Nível 2, ao exercer as competências previstas no Decreto 35.382/2014, deve:
>
> I - encaminhar ao Órgão de Registro Nível 1, conforme normativo próprio, relatórios de atividades;
>
> II - notificar o Órgão de Registro que o habilitou, imediatamente, quando da quebra de segurança de informações classificadas. (DISTRITO FEDERAL, 2016).

Ainda em consonância com as regras trazidas pelo Decreto nº 35.382/2014, ao Posto de Controle (habilitado pelo órgão de registro nível 1 para armazenamento de documento controlado) foram estabelecidas as seguintes competências:

> Art. 5º [...]
>
> I - armazenar e controlar as informações classificadas, inclusive as credenciais de segurança sob sua responsabilidade;

> II - manter a segurança lógica e física das informações classificadas sob sua guarda;
>
> III - encaminhar relatório de suas atividades ao Órgão de Registro que o habilitou, conforme normativo próprio;
>
> IV - notificar o Órgão de Registro que o habilitou, imediatamente, quando da quebra de segurança de informações classificadas por ele custodiadas. (DISTRITO FEDERAL, 2016).

Ademais, o artigo 7º da Portaria nº 05/2016 da Casa Militar dispõe que a habilitação dos órgãos e entidades públicas está condicionada à designação de um GSC, que será responsável pela:

> Art. 7º [...]
>
> I - manutenção da qualificação técnica necessária à segurança de informação classificada, em qualquer grau de sigilo, no âmbito do órgão ou entidade com a qual mantém vínculo;
>
> II - implantação, controle e funcionamento dos protocolos de Documentos Controlados – DC e dos documentos classificados;
>
> III - verificação da conformidade administrativa e do sigilo dos processos de credenciamento e habilitação dentro da competência do órgão ou entidade com a qual mantém vínculo;
>
> IV - proposição à autoridade máxima do órgão ou entidade com a qual mantém vínculo, de normas para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos;
>
> V - gestão dos recursos criptográficos, das Credenciais de Segurança e dos materiais de acesso restrito;
>
> VI - assessoramento ao órgão ou entidade com a qual mantém vínculo, para o tratamento de informações classificadas, em qualquer grau de sigilo;
>
> VII - promoção da capacitação dos agentes públicos responsáveis pelo tratamento de informação classificada, em qualquer grau de sigilo. (DISTRITO FEDERAL, 2016).

Por fim, a Portaria em apreço relaciona algumas regras gerais aplicáveis ao credenciamento de segurança, dentre as quais se destaca o disposto no artigo 15, que autoriza os órgãos da administração pública a expedir instruções complementares, no âmbito de suas competências, com a finalidade de detalhar suas particularidades e procedimentos relativos ao credenciamento de segurança e ao tratamento de informação classificada em qualquer grau de sigilo.

2.5.6 Portaria nº 09, de 10 de outubro de 2016

Dando continuidade às regras dispostas na Portaria nº 05/2016, a Casa Militar do Distrito Federal publicou, em 10 de outubro de 2016, a Portaria nº 09, que dispõe sobre os procedimentos do credenciamento de segurança para o tratamento

de informação classificada do NSC, dos órgãos no âmbito do Poder Executivo Distrital e das Entidades Privadas e dá outras providências.

A mesma lógica utilizada na interpretação da Portaria nº 05/2019 se aplica à Portaria nº 09/2016; portanto, depreende-se que o CBMDF também está abrangido pela norma em apreço.

Incialmente, a Portaria nº 09/2016 estabelece regras ao credenciamento de segurança de pessoas naturais, um procedimento realizado pelo NSC e pelos órgãos de registro. Assim, será conferida uma credencial de segurança associada à informação classificada que determinada pessoa vinculada ao órgão tem necessidade de conhecer.

A credencial de segurança da pessoa natural será concedida por um prazo máximo estabelecido e não superior a dois anos (podendo ser renovada a sua validade), depois de observadas as fases de indicação, de investigação de segurança e de credenciamento. Ademais, a sua concessão deverá atender os seguintes requisitos, dispostos no artigo 4º da Portaria em análise:

> Art. 4º [...]
>
> I - Solicitação formal por qualquer autoridade competente ao Gestor de Segurança e Credenciamento - GSC do órgão de registro solicitante;
>
> a) O GSC poderá também dar início ao processo de credenciamento das pessoas naturais vinculadas ao seu respectivo órgão de registro, uma vez detectada a necessidade de conhecer;
>
> b) Quando a pessoa natural for de entidade privada, a solicitação formal deverá ser realizada pelo diretor estatutário ou Gestor de Segurança e Credenciamento da mesma, ao GSC do Órgão de Registro Nível 1 com o qual mantenha vínculo de qualquer natureza.
>
> II - Preenchimento do Formulário Individual de Dados para Credenciamento - FIDC, conforme modelo constante do Anexo "A" desta Portaria; e
>
> III - Aprovação da investigação para credenciamento pelo órgão de registro com o qual mantenha vínculo. (DISTRITO FEDERAL, 2016).

Para fins de investigação relacionada à pessoa natural que receberá a credencial de segurança, o artigo 11 da Portaria nº 09/2016 dispõe que devem ser analisados os seguintes aspectos pessoais: envolvimento com pessoas ou organizações associadas ao crime, terrorismo, tráfico, sabotagem e espionagem; situação fiscal; dados relacionados à situação criminal, cível e administrativa; e situação eleitoral e do serviço militar.

Quanto à habilitação de segurança do órgão de registro nível 1, o dirigente máximo da secretaria ou órgão público equivalente deverá solicitá-la à Casa Militar do Distrito Federal, bem como a designação do GSC.

Assim, o NSC realiza o credenciamento do GSC (e seu suplente) do órgão solicitante, por meio de encaminhamento de um Formulário Individual de Dados para Credenciamento (FIDC). Ato contínuo, o GSC já credenciado deve dar prosseguimento à habilitação de segurança do seu órgão de registro nível 1, solicitando a habilitação do Posto de Controle (PC).

Nos termos do artigo 24 da Portaria em análise, a habilitação de segurança de PC deve ser concedida para os órgãos e entidades públicas que com eles mantenham vínculo de qualquer natureza e que tratarem informações classificadas em qualquer grau de sigilo. Obrigatoriamente, cada órgão de registro deve possuir ao menos um PC.

O artigo 25 da Portaria 09/2016 estabelece a seguinte qualificação técnica dos PCs:

> Art. 25 [...]
>
> I - estar localizado em área de acesso restrito, conforme previsão legal;
>
> II - possuir meios de armazenamento de documentos físicos e eletrônicos com nível de segurança compatível com os graus de sigilo e volume;
>
> III - possuir estrutura física adequada para o armazenamento e preservação dos documentos físicos e eletrônicos;
>
> IV - possuir planos e procedimentos de contingência de forma a assegurar a continuidade dos processos essenciais no caso de falhas ou sinistros;
>
> V - possuir meios de comunicação segura compatível com os graus de sigilo;
>
> VI - possuir suas redes de dados e seus sistemas de tecnologia da informação adequadamente protegidos de ataques eletrônicos, sendo que os equipamentos que armazenem informações classificadas não devem estar conectados à rede corporativa do órgão;
>
> VII - possuir sistemas alternativos de proteção da infraestrutura crítica relacionada com os ativos de informação e materiais de acesso restrito sob sua responsabilidade de armazenamento e controle;
>
> VIII - atender aos princípios de disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação e materiais de acesso restrito sob sua responsabilidade;
>
> IX - possuir protocolo exclusivo para documentos classificados, e quando necessário, de Documentos Controlados;
>
> X - possuir restrição ao uso de máquinas fotográficas, gravadores de vídeo e áudio, ou similares, tais como câmeras de dispositivos móveis no interior das instalações do PC;

> XI - possuir quadro de pessoal capacitado para o tratamento de informação classificada; e
>
> XII - possuir recursos criptográficos para armazenamento e transmissão de informação classificada em conformidade com as normas estabelecidas pela Casa Militar da Governadoria do Distrito Federal. (DISTRITO FEDERAL, 2016).

Importante ressaltar que, nos termos do artigo 28, o documento que solicita a habilitação do PC, encaminhado pelo GSC, deve conter o endereço, os meios de contato, a declaração expressa da total aderência às qualificações técnicas necessárias à segurança da informação classificada. Ademais, tanto o NSC quanto os órgãos de registro poderão realizar inspeções para a verificação da qualificação técnica do PC.

O artigo 45 relaciona as hipóteses de descredenciamento das pessoas naturais, quais sejam:

> Art. 45 [...]
> I - término de validade da credencial de segurança;
> II - falecimento;
> III - cessar a necessidade de conhecer;
> IV - transferência de órgão ou entidade;
> V - aposentadoria, passagem para a reserva ou inatividade;
> VI - licenciamento;
> VII - suspeita ou quebra de segurança; ou
> VIII - a critério do órgão de registro ao qual estiver vinculada. (DISTRITO FEDERAL, 2016).

Já o descredenciamento de órgão ou entidade pública pode ocorrer a pedido; em razão de extinção, fusão, secção ou mudança de subordinação; quando cessar a necessidade de tratar informação classificada; por suspeita ou quebra de segurança; ou a critério do órgão de registro que homologou a habilitação, nos termos do artigo 46.

Por fim, o artigo 54 dispõe que o GSC de órgão ou entidade pública é responsável por promover a gestão da segurança e do credenciamento dos órgãos de registros, dos postos de controle e das pessoas naturais sob sua responsabilidade no que se refere às informações classificadas, bem como, por gerir, acompanhar e avaliar as atividades previstas na competência do seu órgão ou entidade.

2.6 Atribuições do Centro de Inteligência do CBMDF no que se refere ao tratamento da informação classificada.

Em 21 de junho de 2010, foi publicado o Decreto Distrital nº 31.817, que dispõe sobre a organização básica do CBMDF, mais especificamente no que concerne aos órgãos de apoio e de execução, conforme determinado pelo artigo 10-B, inciso II, da Lei nº 8.255/1991.

As competências do CEINT estão previstas no artigo 6º do mencionado Decreto, dentre as quais se destacam aquelas relacionadas ao tratamento das informações classificadas:

> Art. 6º Compete ao Centro de Inteligência do CBMDF, órgão responsável por planejar, orientar, coordenar e controlar as atividades de inteligência, bem como executar ações relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Comando-Geral da Corporação, em conformidade com a Doutrina Nacional de Inteligência de Segurança Pública, além do previsto no artigo 4º deste decreto:
>
> [...]
>
> IV – administrar os bancos de dados de classificação sigilosa disponibilizados ao Centro de Inteligência;
>
> [...]
>
> VI – preservar o sigilo institucional e governamental sobre necessidades de informações, fontes, fluxos, métodos, técnicas e capacidades de inteligência das agências encarregadas da gestão da segurança pública;
>
> [...]
>
> XII – confeccionar, dar publicidade e arquivar o Boletim Reservado da Corporação, bem como recolher e incinerar as cópias difundidas; (DISTRITO FEDERAL, 2010)

Em consonância com as atribuições legais relativas ao CEINT, o CBMDF editou a Portaria nº 28, de 17 de maio de 2011, que aprova o seu Regimento Interno e dispõe:

> Art. 6º À Seção de Inteligência (SEINT) compete:
>
> [...]
>
> V - monitorar fatos e situações referentes à segurança interna nos movimentos organizados nos meios políticos, trabalhistas e educacionais, bem como em publicações existentes sobre movimentos populares, opiniões públicas, veículos de comunicação e assuntos sigilosos;
>
> [...]
>
> Art. 9º À Seção de Contra-Inteligência (SECOI) compete:
>
> [...]
>
> IX - realizar o credenciamento e descredenciamento dos bombeiros militares do CEINT nos sistemas integrados de informação, aos quais esse CENTRO tenha acesso;

> Art. 16 À Seção de Apoio Administrativo (SEAAD) compete:
> [...]
> VIII - confeccionar, dar publicidade e arquivar o boletim reservado da Corporação, bem como recolher e incinerar as cópias difundidas;
> [...]
> XV - controlar e manter organizado e atualizado o arquivo sigiloso do CEINT; (CBMDF, 2011)

Nestes termos, percebe-se que a natureza das atividades do CEINT/CBMDF está intrinsecamente relacionada à utilização de informações sigilosas, desde a sua produção até a sua eventual difusão ou arquivamento.

Assim, depreende-se que compete ao CEINT, além de realizar o tratamento das informações classificadas em grau de sigilo nos moldes estabelecidos pela LAI Distrital e posteriores Decretos regulamentadores, apresentar ato normativo próprio capaz de uniformizar e definir critérios objetivos sobre o acesso a informações restritas, com a finalidade de se garantir o necessário tratamento de determinadas informações submetidas a um controle especial.

2.7 Atos normativos de outros órgãos públicos

Diante da publicação da regulamentação da LAI Federal e Distrital, alguns órgãos públicos tiveram a iniciativa de elaborar os próprios atos normativos com o escopo de proteger suas informações classificadas ou sob restrição de acesso. Destaque-se, oportunamente, que ainda que a LAI Federal tenha sido publicada há 8 (oito) anos, poucos órgãos públicos efetivamente regulamentaram a matéria em seu âmbito de atuação.

Demonstra-se relevante observar quais foram as melhores práticas adotadas no que se refere ao controle e tratamento dispensados às informações com restrição de acesso para fins de implementação da regulamentação no âmbito do CBMDF.

Para tanto, foram analisados os seguintes atos normativos: Portaria nº 32, de 19 de agosto de 2013, do Gabinete de Segurança Institucional da Presidência da República, Portaria nº 11, de 20 de fevereiro de 2018, da Casa Militar do Distrito Federal e a Portaria nº 1.067, de 08 de setembro de 2014, que aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (IGSAS) - do Exército Brasileiro.

2.7.1 Portaria nº 32, de 19 de agosto de 2013 – Gabinete de Segurança Institucional da Presidência da República

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que tem como competência principal assistir diretamente o Presidente da República no desempenho de suas atribuições no que concerne a assuntos militares e de segurança, editou a Portaria nº 32, de 19 de agosto de 2013, que regula os procedimentos relacionados ao credenciamento de segurança e tratamento de informação classificada em seu âmbito de atuação.

Inicialmente, a Portaria prevê que todas as secretarias e departamentos que compõem a estrutura do GSI/PR devem possuir em suas dependências um PC para o tratamento de suas informações classificadas. Cada um dos PCs tem como atribuição realizar o protocolo interno de documentos classificados, bem como o tratamento da informação classificada sob sua responsabilidade.

> Art. 2º As secretarias e departamentos integrantes do Gabinete de Segurança Institucional da Presidência da República - GSI/PR e o Núcleo de Segurança e Credenciamento - NSC deverão possuir um Posto de Controle - PC em suas dependências para o tratamento de informação classificada no âmbito de sua competência.
>
> § 1º O PC do Núcleo de Segurança e Credenciamento atenderá também às necessidades de tratamento de informação classificada do Departamento de Segurança da Informação e Comunicações - DSIC.
>
> § 2º O PC do Departamento de Gestão e de Articulação Institucional - DGES atenderá também às necessidades de tratamento de informação classificada da Secretaria-Executiva e Gabinete do Ministro-Chefe. (GSI/PR, 2013)

O artigo 3º estabelece as competências da ABIN como Órgão de Registro Nível 1 e 2, enquanto o artigo 4º dispõe que as secretarias e departamentos do GSI deverão informar os quais os servidores são indicados para as funções de GSC.

> Art. 3º A Agência Brasileira de Inteligência - ABIN deverá ser habilitada como Órgão de Registro Nível 2 - ORN2 vinculada ao GSI/PR.
>
> § 1º Fica delegada à ABIN a competência de Órgão de Registro Nível 1 conforme Art. 7º do Decreto nº 7.845, de 2012.
>
> § 2º É vedada a subdelegação de competência para o tratado no parágrafo 1º deste artigo.
>
> § 3º A habilitação da ABIN será realizada conforme previsto no item 7 da NC01/IN02/NSC/GSI/PR, de 2013.

> Art. 4º As secretarias e departamentos integrantes do GSI/PR deverão informar os respectivos servidores indicados para as funções de Gestores de Segurança e Credenciamento - GSC, titulares e suplentes, ao NSC para o credenciamento de segurança dos mesmos.
>
> § 1º O credenciamento do GSC, titular e suplente, será realizado conforme previsto no item 5 da NC01/IN02/NSC/GSI/PR, de 2013.
>
> § 2º O previsto no caput e § 1º será repetido para toda substituição de GSC, titular e suplente. (GSI/PR, 2013)

Os artigos 5º, 6º e 7º da Portaria apresentam regras simples de homologação da habilitação dos PCs e dos GSCs, como por exemplo, a publicação em Boletim de Acesso Restrito.

> Art. 5º O NSC habilitará os PC das Secretarias e departamentos integrantes do GSI/PR conforme item 8 daNC01/IN02/NSC/GSI/PR, de 2013, no que couber.
>
> Art. 6º A homologação da habilitação de segurança dos PC das secretarias e departamentos integrantes do GSI/PR e ABIN serão publicadas no Boletim de Acesso Restrito - BAR, conforme Art. 2º da Portaria nº 18, de 2013.
>
> Parágrafo único - A homologação da habilitação de segurança de ORN2 ou PC subordinados à ABIN será regulada pela própria Agência.
>
> Art. 7º A homologação do credenciamento de segurança dos GSC, titulares e suplentes, das secretarias e departamentos integrantes do GSI/PR serão publicados em BAR, conforme Art. 2º da Portaria nº18, de 2013. (GSI/PR, 2013).

Os artigos 8º e 9º, por sua vez, elencam as competências dos PCs habilitados no âmbito do GSI, quais sejam:

> Art. 8º Cabe ao PC de cada secretaria e departamento integrante do GSI/PR, além do previsto no Art. 9º do Decreto nº 7.845,de 2012, e Art. 6º da IN02/NSC/GSI/PR, de 2013:
>
> I. realizar no âmbito secretaria/departamento o protocolo interno de documentos classificados; e
>
> II. realizar o tratamento da informação classificada sob sua responsabilidade estritamente de acordo com a legislação em vigor.
>
> Art. 9º As áreas e estruturas que contiverem informação classificada ou material de acesso restrito deverão ser consideradas como áreas de acesso restrito conforme Seção VIII, do Decreto nº 7.845, de 2012.
>
> § 1º Os PC das secretarias e departamentos integrantes do GSI e o NSC são áreas de acesso restrito.
>
> § 2º As secretarias e departamentos integrantes do GSI/PR poderão delimitar áreas de acesso restrito adicionais, contíguas ou não aos seus respectivos PC, inclusive em outras instalações no país, conforme o caput, para o tratamento de informação classificada e salvaguarda de material de acesso restrito, desde que em consonância com a legislação em vigor.
>
> § 3º As secretarias e departamentos integrantes do GSI/PR que possuírem áreas de acesso restrito que não correspondam aos seus respectivos PC deverão designar servidor público civil ou militar que desempenhe função na

> referida área, credenciado, como responsável pela segurança da informação e comunicações da área. (GSI/PR, 2013)

Neste sentido, além da referida Portaria determinar que as áreas e estruturas que contiverem informação classificada ou material de acesso restrito devem ser consideradas como áreas de acesso restrito, conforme disposto no artigo 9º, também destaca que apenas o pessoal credenciado poderá entrar nesses locais.

Nos termos do artigo 11, as visitas externas só podem ocorrer se autorizadas pelo GSC da área e com assinatura, pelos visitantes, de TCMS.

Todo o processo de credenciamento de segurança está disposto nos artigos 12 a 17, que resumidamente apontam para a necessidade de adoção de critérios rígidos no que concerne ao registro e assinatura do TCMS dos servidores públicos civis e militares que devam conhecer a informação classificada.

> Art. 12. Os servidores públicos civis e militares das secretaria se departamentos integrantes do GSI/PR que necessitarem tratar informação classificada, em qualquer grau de sigilo, serão credenciados pelo NSC conforme previsto no item 5 daNC01/IN02/NSC/GSI/PR, de 2013.
>
> Parágrafo único - Os servidores públicos civis e militares das secretarias e departamentos integrantes do GSI/PR que necessitarem tratar informação classificada, em qualquer grau de sigilo, poderão assinar Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 7.845, de 2012, enquanto decorrer o prazo necessário para o procedimento previsto no caput.
>
> Art. 13 A identificação da necessidade de conhecer informação classificada, em qualquer grau de sigilo, será informada ao GSC da secretaria ou departamento integrantes do GSI/PR para início do processo de credenciamento de segurança das pessoas naturais que mantenham vínculo de qualquer natureza com o GSI/PR.
>
> Art. 14. O GSC da secretaria/departamento formalizará o pedido de credenciamento por intermédio de memorando ao NSC encaminhando o Formulário Individual de Dados para Credenciamento-FIDC, devidamente preenchido e assinado pelo indicado, constante no Anexo A da NC01/IN02/NSC/GSI/PR, de 2013.
>
> Parágrafo Único - O memorando previsto no caput deverá atender o previsto no item 5.5.1.2 da NC01/IN02/NSC/GSI/PR, de 2013.
>
> Art. 15. A homologação do credenciamento de segurança de servidores públicos civis e militares das secretarias e departamentos integrantes do GSI/PR será publicada no BAR, conforme Art. 2º da Portaria nº 18 do GSI/PR, de 2013.
>
> Art. 16. A ABIN realizará a fase de investigação de segurança de servidores públicos civis e militares das Secretarias e departamentos integrantes do GSI/PR, prevista no item 5.5.2 da NC01/IN02/NSC/GSI/PR, de 2013, mediante demanda do NSC.
>
> Art. 17. Fica delegada ao Gestor de Segurança e Credenciamento do GSI/PR a competência do ato de concessão da credencial de segurança

> emitida pelo NSC, conforme item 5.5.3.2 da NC01/IN02/NSC/GSI/PR, de 2013.
>
> Parágrafo Único. Fica delegada ao Gestor de Segurança e Credenciamento do GSI/PR a competência da expedição da habilitação de segurança previstas nos itens 8.13 e 9.10 da NC01/IN02/NSC/GSI/PR, de 2013. (GSI/PR, 2013)

Quanto à infraestrutura dos servidores de dados, concentradores de rede e centros de processamento que integram os sistemas de tecnologia da informação que tratem de informação classificada em qualquer grau de sigilo, os artigos 18 a 21 relacionam os serviços de protocolo inerentes ao seu compartilhamento.

Por fim, os artigos 22 e seguintes estabelecem que ABIN poderá regular internamente os processos de credenciamento de segurança e tratamento de informações classificadas bem como a emissão de Certificados de Credenciamento de Segurança (CCS):

> Art. 22. A autoridade credenciada ex officio, conforme o Art.9º da IN02/NSC/GSI/PR, de 2013, que tenha necessidade de tratar informação classificada em grau de sigilo superior ao qual é credenciada, deverá encaminhar solicitação de credenciamento no grau de sigilo necessário ao GSC da secretaria ou departamento integrante do GSI/PR com o qual mantenha vínculo.
>
> Art. 23. A ABIN poderá regular internamente os processos de credenciamento de segurança e tratamento de informações classificadas.
>
> Art. 24. A emissão de certificados de credenciamento de segurança - CCS de servidores públicos civis e militares das secretarias e departamentos integrantes do GSI/PR, quando necessário, será realizada pelo NSC.
>
> Parágrafo Único. A ABIN poderá regular internamente a emissão de CCS.
>
> Art. 25. As secretarias e departamentos do GSI/PR deverão adotar providências no sentido de que os servidores públicos civis ou militares que tratem informação classificada em suas áreas de atuação, conheçam as normas em vigor relacionas ao credenciamento de segurança e à Segurança da Informação e Comunicações. (GSI/PR, 2013)

2.7.2 Portaria nº 11, de 20 de fevereiro de 2018 – Casa Militar do Distrito Federal

A Casa Militar do Distrito Federal publicou, em 20 de fevereiro de 2018, as diretrizes e procedimentos a serem adotados para o credenciamento de segurança e o tratamento da informação classificada em grau de sigilo por todas as suas unidades administrativas.

A figura do GSC, anteriormente mencionado no âmbito do Decreto Distrital nº 35.382/2014, aparece nos artigos 3º e 4º da presente Portaria como competente para conceder credencial de segurança emitida pelo NSC.

> Art. 3º A homologação do credenciamento de segurança do Gestor de Segurança e Credenciamento - GSC, titular e suplente, deve ser publicada no Boletim de Acesso Restrito como Material de Acesso Restrito.
>
> Art. 4º Fica delegada ao GSC da Casa Militar a competência para conceder a credencial de segurança emitida pelo Núcleo de Segurança e Credenciamento - NSC, conforme art. 14, § 2º, da Portaria n.º 09, de 10 de outubro de 2016. (DISTRITO FEDERAL, 2018)

O artigo 5º, por sua vez, dispõe que os militares e servidores públicos civis que necessitarem tratar informação classificada em grau de sigilo devem ser credenciados pelo NSC e estão obrigados a assinar o TCMS.

> Art. 5º Os militares e os servidores públicos civis das unidades administrativas integrantes da CM/GDF que necessitarem tratar informação classificada em grau de sigilo devem ser credenciados pelo NSC, consoante o disposto na Portaria n.º 09, de 10 de outubro de 2016.
>
> Parágrafo único. Os militares e os servidores públicos civis das unidades administrativas integrantes da CM/GDF que necessitarem tratar informação classificada em grau de sigilo devem assinar o Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme modelo constante no Anexo I desta Portaria, o qual vigorará enquanto decorrer o prazo necessário para o procedimento previsto no caput. (DISTRITO FEDERAL, 2018)

Os artigos 6º, 7º e 8º estão relacionados ao início do processo de credenciamento, a necessidade de publicação da homologação do credenciamento em Boletim de Acesso Restrito e a realização da fase de investigação de segurança de militares e servidores públicos civis das unidades administrativas integrantes da Casa Militar.

> Art. 6º A identificação da necessidade de conhecimento da informação classificada em grau de sigilo será informada ao GSC para o início do processo de credenciamento de segurança das pessoas naturais que mantenham vínculo de qualquer natureza com a CM/GDF.
>
> Art. 7º A homologação do credenciamento de segurança de militares e servidores públicos civis das unidades administrativas integrantes da CM/GDF deve ser publicada no Boletim de Acesso Restrito como Material de Acesso Restrito.
>
> Art. 8º O NSC deve realizar a fase de investigação de segurança de militares e servidores públicos civis das unidades administrativas integrantes da CM/GDF, prevista na Portaria n.º 09, de 10 de outubro de 2016. (DISTRITO FEDERAL, 2018)

O artigo 9º estabelece que a classificação da informação em grau de sigilo deve ser formalizada com o preenchimento do TCI, que deverá acompanhar a informação classificada como primeira folha da documentação, acondicionado em envelope lacrado. Ademais, o servidor ou autoridade classificadora deverá emitir 3 (três) cópias do TCI, com as razões de classificação tarjadas ou suprimidas, devendo:

> Art. 9º A classificação da informação em grau de sigilo deve ser formalizada com o preenchimento do Termo de Classificação de Informação - TCI, conforme Anexo Único do Decreto n.º 34.276, de 11 de abril de 2013.
>
> § 1º O TCI deve acompanhar a informação classificada, como primeira folha da documentação, devendo ser acondicionado em envelope lacrado.
>
> § 2º A autoridade classificadora ou servidor por ela credenciado deve emitir 3 (três) cópias do TCI, com as razões de classificação deste termo tarjadas ou suprimidas, devendo:
>
> I- Anexar a primeira cópia à informação a qual se refira, de forma ostensiva;
>
> II- Encaminhar a segunda cópia para o Posto de Controle – PC ao qual estiver vinculado no prazo máximo de 30 (trinta) dias da data de classificação;
>
> III- Manter arquivada na unidade administrativa correspondente a terceira cópia (DISTRITO FEDERAL, 2018).

Nos termos do disposto no Decreto Distrital nº 35.382/2014, para classificar a informação por meio de um TCI, é necessária a criação de um Núcleo Único de Protocolo (NUP), que compõe o Código de Indexação de Documento (CIDIC), gerado por meio da abertura de um processo no Sistema Eletrônico de Informação (SEI), nos termos do artigo 10.

> Art. 10. O Número Único de Protocolo - NUP que compõe o Código de Indexação de Documento - CIDIC, conforme disposto no Capítulo IV do Decreto n.º 35.382, de 29 de abril de 2014, deve ser gerado por meio da abertura de processo no Sistema Eletrônico de Informação - SEI, designado como 'NUP para composição do CIDIC'.
>
> § 1º O NUP é o número do processo gerado pelo SEI-GDF.
>
> § 2º A autoridade classificadora ou servidor por ela credenciado deve encaminhar o processo SEI para a unidade CM/SUSIC/DCRED com a cópia do TCI, mencionada no inciso II do §2º do art. 9º desta Portaria, digitalizada em formato PDF.
>
> § 3º O processo SEI não deve conter nenhuma informação classificada em grau de sigilo até que a informação seja desclassificada.
>
> § 4º A informação classificada em grau de sigilo, quando desclassificada, deve ser inserida no processo SEI vinculado ao processo de geração do NUP. (DISTRITO FEDERAL, 2018).

Destaque-se, oportunamente, que os parágrafos 3º e 4º do supracitado artigo 10 apontam que o processo SEI gerado para fins de criação do NUP não deve conter nenhuma informação classificada em grau de sigilo até que a informação seja desclassificada. Apenas no momento da desclassificação a informação deverá ser inserida no referido processo.

O artigo 11 estabelece que a autoridade classificadora deverá tramitar a informação em envelope lacrado e o artigo 12 estabelece que toda a informação classificada em grau de sigilo deverá ser acompanhada de um Termo de Custódia, preenchido pelo custodiante.

> Art. 11. A autoridade classificadora ou servidor por ela credenciado deve tramitar a informação classificada em grau de sigilo em envelope lacrado, com a cópia ostensiva do TCI anexado na parte externa, para fins de guarda no PC correspondente.
>
> Art. 12. Toda informação classificada em grau de sigilo deve ser acompanhada pelo Termo de Custódia, conforme modelo contido no Anexo II, devendo ser preenchido pelo custodiante, podendo o remetente reproduzir uma cópia como forma de recibo. (DISTRITO FEDERAL, 2018).

Por fim, o artigo 15 dispõe que todas as unidades administrativas devem possuir ou estarem vinculadas a um PC para tratamento de informação classificada em grau de sigilo. O NSC será responsável por habilitar o PC das unidades administrativas integrantes da Casa Militar do Distrito Federal.

2.7.3 Instruções Gerais para a Salvaguarda de Assuntos Sigilosos – Exército Brasileiro

Em 8 de setembro de 2014 foi publicada a Portaria nº 1.067, que aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (IGSAS) - (EB10-IG-01.011) no âmbito do Exército Brasileiro (EB).

Como um dos pioneiros na regulamentação interna referente ao tratamento da informação classificada, o EB elaborou uma extensa norma, abordando os mais diversos aspectos relacionados ao tema, em consonância com a LAI Federal e seu Decreto regulamentador, nº 7.724/2012.

Assim como a LAI Federal, a IGSAS elencou, em seu artigo 2º, um extenso rol de conceitos úteis à compreensão da norma. Alguns desses conceitos

são reproduções de outros já apresentados ao ordenamento jurídico nas normas anteriores, como: classificação, desclassificação, grau de sigilo, informação classificada e informação sigilosa.

Em seu artigo 3º, o EB relaciona quais informações serão mantidas sob restrição de acesso, independentemente de classificação. Nos artigos 4º e 5º, que tratam respectivamente dos graus de sigilo e de quais informações são consideradas imprescindíveis à segurança da sociedade e do Estado, reproduziu-se integralmente o teor da LAI Federal.

> Art. 3º O Exército Brasileiro manterá sob restrição de acesso, independentemente de classificação, o documento, a área ou a instalação sob sua custódia, que contenha:
>
> I - informação classificada;
>
> II - informação desclassificada que continue sob restrição de acesso;
>
> III - informação pessoal;
>
> IV - informação protegida por legislação específica como de natureza sigilosa, tal como sigilo bancário, fiscal ou patrimonial, etc;
>
> V - processo judicial sob segredo de justiça;
>
> VI - identificação do denunciante que origine procedimento investigativo;
>
> VII - papel de trabalho e procedimento relativo a ações de controle e de inspeção correcional ou de qualquer espécie de ação investigativa, nos termos do § 3º do art. 26 da Lei nº 10.180, de 6 de fevereiro de 2001;
>
> VIII - relatório e nota técnica decorrente de investigação, auditoria, fiscalização, e outros documentos relativos à atividade de correição;
>
> IX - informação referente a projeto de pesquisa e desenvolvimento científico ou tecnológico de interesse da Defesa Nacional;
>
> X - documento preparatório;
>
> XI - documento ou informação de natureza técnica, produzido por órgão ou entidade não vinculado, ainda que não se caracterize a custódia;
>
> XII - área e instalação que contenha informação classificada ou sob restrição de acesso;
>
> XIII - informação constante de manual de instrução ou de documento que trate do emprego de material de acesso restrito;
>
> XIV- materiais de acesso restrito; e
>
> XV - correspondência pessoal, e outras abrangidas pelas demais hipóteses legais de sigilo.
>
> Parágrafo único. Cabe às autoridades mencionadas nos art. 9º e 10 destas IG definir a adoção de medidas de restrição de acesso, dentro dos preceitos estabelecidos nos dispositivos legais vigentes.
>
> Art. 4º Os graus de sigilo para a classificação de informação são:
>
> I - RESERVADO;
>
> II - SECRETO; e
>
> III - ULTRASSECRETO.
>
> Art. 5º Somente será passível de classificação a informação considerada imprescindível à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possa:
>
> I - pôr em risco a defesa, a soberania ou a integridade do território nacional;

> II - prejudicar ou pôr em risco a condução de negociação ou as relações internacionais do País, ou a que tenha sido fornecida em caráter sigiloso por outro Estado e Organismo Internacional;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a plano ou operação estratégica das Forças Armadas;
>
> VI - prejudicar ou causar risco a projeto de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistema, bem, instalação ou área de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituição, de alta autoridade nacional ou estrangeira e seus familiares; ou
>
> VIII - comprometer atividade de Inteligência, bem como de investigação ou fiscalização em andamento, relacionada com a prevenção ou repressão de infrações. (EB, 2014)

Quanto à gravidade do risco ou dano à segurança da sociedade e do Estado, a IGSAS pontuou em seu artigo 7º quais informações são consideradas ultrassecretas (inciso I), secretas (inciso II) e reservadas (inciso III).

> Art. 7º Quanto à gravidade do risco ou dano à segurança da sociedade e do Estado:
>
> I - a informação de grau de sigilo ULTRASSECRETO é aquela cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave, tal como a referente a (à):
>
> a) soberania e à integridade territorial nacionais;
>
> b) relações internacionais do País;
>
> c) plano e operação militar que afetem as letras “a” e “b” do presente inciso;
>
> d) projeto de pesquisa e desenvolvimento científico e tecnológico de interesse da Defesa Nacional; e
>
> e) programa econômico.
>
> II - a informação de grau de sigilo SECRETO é aquela cujo conhecimento não autorizado possa acarretar dano grave, tal como a referente a (à):
>
> a) sistema;
>
> b) instalação;
>
> c) programa;
>
> d) projeto;
>
> e) plano ou operação de interesse da Defesa Nacional;
>
> f) assunto diplomático e de Inteligência; e
>
> g) plano ou seus detalhes.
>
> III - a informação de grau de sigilo RESERVADO é aquela cujo conhecimento não autorizado possa acarretar dano, tal como a que frustre ou comprometa:
>
> a) objetivo de interesse do Poder Executivo;
>
> b) objetivo ou atividade de interesse do Comando do Exército; e
>
> c) plano, operação ou objetivo nele previsto ou referido. (EB, 2014)

Os prazos máximos de restrição estão previstos no artigo 8º e seguem inteiramente a lógica disposta na LAI Federal.

> Art. 8º Os prazos máximos de restrição de acesso à informação classificada vigoram na data de sua produção e são os seguintes:
> I - para o grau de sigilo ULTRASSECRETO: 25 (vinte e cinco) anos;
> II - para o grau de sigilo SECRETO: 15 (quinze) anos; e
> III - para o grau de sigilo RESERVADO: 5 (cinco) anos.
> § 1º Somente a informação classificada no grau de sigilo ULTRASSECRETO é passível de prorrogação, uma única vez, de prazo de restrição de acesso.
> § 2º A informação que puder colocar em risco a segurança do Presidente e do Vice-Presidente da República e respectivos cônjuges e filhos (as) será classificada no grau de sigilo RESERVADO e ficará sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.
> § 3º Poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, observados os prazos máximos de classificação.
> § 4º Transcorrido o prazo máximo de classificação, a informação tornar-se-á, automaticamente, de acesso público dentro das prescrições da legislação vigente, observadas as restrições de acesso previstas no art. 3º destas IGSAS. (EB, 2014)

Por sua vez, as competências para classificar as informações tratadas no âmbito do EB, dispostas nos artigos 9º e 10º, estão relacionadas no quadro a seguir:

Figura 7 – Autoridades classificadoras no EB

Grau de sigilo	Autoridade Classificadora	Possibilidade de Delegação
Reservado	Comandante do EB.	Sim.
	Comandante, Chefe ou Diretor de OM ou Oficial-General.	Não.
Secreto	Comandante do EB.	Não.
Ultrassecreto	Comandante do EB, devendo ser ratificada pelo Ministro da Defesa.	

Fonte: a autora.

Os procedimentos para classificação da informação incluem a emissão do TCI, que conterá os itens dispostos no artigo 11º da Instrução:

> Art. 11. A decisão de classificar a informação deverá ser formalizada pela emissão de TCI, que conterá os seguintes itens:
> I - código de indexação de documento;
> II - grau de sigilo;
> III - categoria na qual se enquadra a informação;
> IV - tipo de documento;
> V - data da produção do documento;

> VI - indicação de dispositivo legal que fundamenta a classificação;
>
> VII - razão da classificação, observados os critérios estabelecidos no art. 6º;
>
> VIII - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 8º;
>
> IX - data da classificação; e
>
> X - identificação da autoridade que classificou a informação.
>
> § 1º A informação prevista no inciso VII do caput deverá ser mantida no mesmo grau de sigilo da informação classificada.
>
> § 2º A informação somente será considerada classificada após a assinatura do respectivo TCI.
>
> § 3º O TCI é único para cada documento classificado.
>
> § 4º Para confecção do TCI, a informação a ser classificada deverá receber número único de protocolo/número único de documento (NUP/NUD), mesmo que não seja um documento padrão, como esboço, desenho, mapa, carta, fotografia, imagem, negativo ou slide.
>
> § 5º A competência para a assinatura do TCI é das autoridades previstas nos art. 9º e 10.
>
> § 6º O TCI deverá ser confeccionado em duas vias, conforme modelo contido no anexo “F” destas IG. (EB, 2014).

O EB estabeleceu uma diferença para a tramitação do documento reservado e dos documentos classificados no grau de sigilo secreto e ultrassecreto, conforme se verifica por meio da leitura dos artigos 12 a 14, a seguir colacionados:

> Art. 12. O documento RESERVADO terá a 1ª via do TCI arquivada na OM que o produziu, a fim de possibilitar sua atualização e controle (desclassificação ou redução do prazo).
>
> Parágrafo único. A 2ª via do TCI seguirá anexada à informação.
>
> Art. 13. Para a classificação da Informação nos graus de sigilo SECRETO e ULTRASSECRETO deverão ser seguidos os seguintes procedimentos:
>
> I - o Comandante Militar de Área (C Mil A), Chefe ou Diretor de Órgão de Direção Geral (ODG), Órgão de Direção Setorial (ODS) ou Órgão de Assistência Direta e Imediato (OADI) deverá analisar a proposta de classificação nos graus de sigilo SECRETO e ULTRASSECRETO de suas OM subordinadas;
>
> II - confirmada a necessidade de se classificar nesses graus de sigilo, enviar proposta de TCI pela rede segura do Exército à Comissão Permanente de Avaliação de Documentos Classificados do Exército (CPADC/CIE);
>
> III - a CPADC/CIE imprimirá o TCI e o encaminhará, juntamente com o “resumo explicativo”, ao Gabinete do Comandante do Exército (Gab Cmt Ex) para assinatura do Comandante; e
>
> IV - o Gab Cmt Ex devolverá o TCI assinado à CPADC/CIE, que adotará os seguintes procedimentos:
>
> a) para a informação no grau de sigilo ULTRASSECRETO, encaminhará o TCI ao Ministro da Defesa para ratificação no prazo de trinta dias, contados da data de classificação;
>
> b) para a informação no grau de sigilo SECRETO, encaminhará cópia do TCI à Comissão Mista de Reavaliação de Informações (CMRI), instituída nos termos do § 1º do art. 35 da Lei nº 12.527/2011, no prazo de trinta dias, contados da data de classificação;
>
> c) enviará cópia assinada do TCI ao comando correspondente; e

> d) arquivará o TCI original.
>
> Art. 14. Na confecção do TCI para a informação no grau de sigilo SECRETO ou ULTRASSECRETO deverão ser observados os seguintes aspectos:
>
> I - na proposta de TCI, os campos “RAZÕES PARA A CLASSIFICAÇÃO” e “DATA DE CLASSIFICAÇÃO”, devem estar em branco;
>
> II - a proposta de TCI deve ser acompanhada de “resumo explicativo”;
>
> III - o “resumo explicativo” deve seguir o modelo do anexo “I”; devendo conter:
>
> a) o assunto de que trata o documento;
>
> b) a proposta de razão para a classificação;
>
> c) os riscos observados que comprometam a segurança da sociedade e do Estado, assim como, a visualização dos possíveis danos à segurança da sociedade e do Estado; e
>
> IV - o “resumo explicativo” consubstanciará as razões para se classificar o documento, devendo ser preciso e conciso. (EB, 2014)

Os artigos 15 e 16 relacionam os aspectos essenciais para a formação do código que deve acompanhar todas as informações classificadas produzidas pelo órgão, o CIDIC.

> Art. 15. A Informação classificada receberá o Código de Indexação de Documento que contém Informação Classificada (CIDIC), conforme modelo constante do anexo “F”.
>
> Art. 16. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada e será estruturado em duas partes:
>
> I - a primeira parte do CIDIC será composta pelo Número Único de Protocolo (NUP), originalmente cadastrado conforme legislação de gestão documental; e
>
> II - a segunda parte do CIDIC será composta dos seguintes elementos:
>
> a) grau de sigilo: indicação do grau de sigilo, ULTRASSECRETO (U), SECRETO (S) ou RESERVADO (R), com as iniciais na cor vermelha;
>
> b) categoria: indicação, com dois dígitos, da categoria relativa ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme anexo II do Decreto nº 7.845/2012;
>
> c) data de produção do documento classificado: registrar a data de produção do documento, no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);
>
> d) data de desclassificação do documento: registrar a potencial data de desclassificação desse documento, efetuada no ato de desclassificação, no formato 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 de documento classificado, respectivamente, conforme as seguintes situações:
>
> 1) reclassificação de documento resultante de reavaliação; ou
>
> 2) primeiro registro da classificação.
>
> f) indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.
>
> § 1o O documento classificado, quando de sua desclassificação, manterá apenas o NUP.

> § 2o Não será utilizada tabela de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso a documento classificado, sob pena de pôr em risco sua proteção.
>
> § 3o No que concerne à gestão documental, deverá ser guardado o histórico de alterações do CIDIC. (EB, 2014)

Quanto à possibilidade de desclassificação e reavaliação da informação classificada, o EB elaborou as normas descritas nos artigos 17 a 21, que demonstram a possibilidade de alteração da classificação da informação em diversas oportunidades, desde que realizados pela autoridade classificadora ou por autoridade hierarquicamente superior.

> Art. 17. A classificação da informação será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.
>
> Parágrafo único. Para o cumprimento do disposto no caput, além do previsto no art. 6º, deverá ser observado:
>
> I - o prazo máximo de restrição de acesso à informação, previsto no art. 8º;
>
> II - o prazo máximo de quatro anos para revisão de ofício da informação classificada no grau de sigilo ULTRASSECRETO ou SECRETO, previsto no inciso I do caput do art. 47 do Decreto nº 7.724, de 16 de maio de 2012;
>
> III - a permanência das razões da classificação;
>
> IV - a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e
>
> V - a peculiaridade da informação produzida no exterior por autoridade ou agente público.
>
> Art. 18. Os procedimentos para reavaliação e desclassificação de informação classificada serão os previstos nas IG para Avaliação e Controle de Documentos Classificados do Exército.
>
> Art. 19. O pedido de desclassificação ou de reavaliação da classificação de informação poderá ser apresentado ao órgão ou entidade, independente de existir prévio pedido de acesso à informação.
>
> § 1º O pedido de que trata o caput será endereçado à autoridade classificadora, que tomará uma decisão no prazo de trinta dias.
>
> § 2º No caso de informação produzida por autoridade ou agente público no exterior, o requerimento de desclassificação e reavaliação será apreciado pela autoridade hierarquicamente superior que estiver em território brasileiro.
>
> Art. 20. Negado o pedido de desclassificação ou de reavaliação da informação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contado da ciência da negativa, primeiramente perante o Comandante do Exército e, em caso de negativa, ao Ministro de Estado da Defesa.
>
> § 1º Será apresentada uma decisão no prazo de trinta dias após a apreciação do recurso.
>
> § 2º Desprovido o recurso de que trata o caput, poderá o requerente apresentar recurso à Comissão Mista de Reavaliação de Informações, instituída nos termos do § 1º do art. 35 da Lei nº 12.527/2011, no prazo de dez dias, contado da ciência da decisão.

> Art. 21. A decisão sobre a desclassificação, a reclassificação ou a redução do prazo de sigilo de informação classificada deverá constar da capa do processo, se houver, e do campo apropriado no TCI. (EB, 2014)

Nos artigos 22 a 26, o EB elencou as demais situações com restrição de acesso, como informações pessoais, informações referentes a projetos de pesquisa e desenvolvimento científico ou tecnológico, informações contidas em documentos preparatórios, dentre outros, que não são objeto do presente estudo, motivo pelo qual se entendeu ser dispensável a reprodução de tais dispositivos.

As medidas de controle da informação classificada estão dispostas nos artigos 37 a 66 e envolvem aspectos como o acesso, os documentos e materiais controlados e as marcações de sigilo. Em razão da extensa quantidade de dispositivos editados pelo EB, destacam-se a seguir apenas os mais relevantes ao estudo da matéria.

> Art. 37. Compete ao Cmt, Ch ou Dir de OM manter o pessoal sob suas ordens atualizado sobre as medidas de controle da informação classificada ou sob restrição de acesso em vigor.
>
> Art. 38. Qualquer militar ou servidor, que tenha conhecimento de uma situação na qual uma informação classificada ou sob restrição de acesso possa estar ou venha a ser comprometida, deverá informar tal fato ao seu chefe imediato e/ou à autoridade responsável pela proteção da mesma.
>
> Art. 39. Qualquer militar ou servidor, que tenha extraviado documento ou material classificado ou sob restrição de acesso, deverá participar imediatamente ao seu chefe imediato e/ou à autoridade responsável pela custódia.
>
> Parágrafo único. Idêntica providência deverá ser tomada quando se encontre ou se tenha conhecimento de que foi achado documento ou material classificado ou sob restrição de acesso.
>
> [..]
>
> Art. 44. O acesso à informação classificada é estritamente funcional e independe de grau hierárquico do militar, sendo, contudo, obrigatório o credenciamento de segurança compatível, de acordo com as normas de credenciamento vigentes.
>
> § 1º O acesso de militar ou civil a documento ou material sob restrição de acesso exige a assinatura de Termo de Compromisso e Manutenção de Sigilo (TCMS) previsto no anexo “E” destas Instruções Gerais, não havendo necessidade de concessão de credenciamento de segurança.
>
> § 2º Cabe ao Cmt, Ch ou Dir, no âmbito de sua OM, regular o acesso, considerando os seguintes aspectos:
>
> I - necessidade do serviço;
>
> II - necessidade de conhecer; e
>
> III - nível de credenciamento
>
> Art. 45. O acesso à informação classificada, por pessoa não credenciada ou não autorizada por legislação, poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção do Sigilo (TCMS), conforme modelo constante do anexo “E”, pelo qual a pessoa se

> obrigará a manter sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.
>
> Art. 46. Os demais acessos previstos na legislação em vigor serão concedidos de acordo com o que prescreve a Lei nº 12.527/2011, seus decretos e legislação específica do Exército sobre o assunto.
>
> Paragrafo único. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.
>
> [...]
>
> Art. 61. A marcação do grau de sigilo de um documento deverá constar de todas as suas páginas, observadas as seguintes formalidades:
>
> I - a marcação será centralizada, no alto e no rodapé de cada página, em cor contrastante com a do documento, utilizando-se, preferencialmente, a cor vermelha conforme modelo constante do anexo “C”; e
>
> II - somente deverá ser usada outra cor para assinalar a classificação sigilosa quando o documento, pela sua natureza, não permitir que se obtenha o contraste desejado. (EB, 2014)

Quanto à segurança da informação, a Portaria em apreço apresenta de maneira extensa e cautelosa inúmeros artigos que tratam da segurança no processo seletivo, no desempenho da função, no desligamento da função, da segurança da documentação, da produção, da expedição e recepção, do manuseio, do arquivamento, da eliminação, do material, do transporte, da eliminação de material controlado, das áreas e instalações, das comunicações, da remessa ou transmissão, do conteúdo e da tecnologia da informação, dentre os quais merecem destaque:

> Art. 67. A avaliação de cargo ou função, com o objetivo de determinar o seu grau de sensibilidade, bem como a investigação de segurança, necessária para o desempenho de uma função ou cargo sensível, deverá estar de acordo com a norma para a concessão de credencial de segurança vigente.
>
> Art. 68. A função ou cargo que trate com informação classificada ou sob restrição de acesso deverá ser compartimentada, a fim de restringir o acesso, considerando a necessidade de conhecer.
>
> [...]
>
> Art. 70. O credenciamento para o desempenho de cargo ou função deverá ocorrer antes do início do desempenho da mesma e estar de acordo com a norma para concessão de credencial de segurança vigente.
>
> Art. 71. O Cmt, Ch ou Dir de OM deverá verificar:
>
> I - comportamento e/ou vulnerabilidade incompatível com o cargo ou função;
>
> II - descontentamento no desempenho da função; e
>
> III - vulnerabilidades em relação ao recrutamento e/ou aliciamento adversos.
>
> Art. 72. Após o desligamento de um militar ou servidor de um cargo ou função que exige credenciamento de segurança, sempre que possível, o Cmt, Ch ou Dir de OM deverá:
>
> I - manter, em banco de dados, para contato futuro, o endereço de ex-integrante, possibilitando o acompanhamento do militar ou do servidor que ocupava função sensível;
>
> II - solicitar ao ex-integrante a exclusão de todas as pastas e arquivos temporários, por ele produzidos no (s) computador(es) existente(s) na OM;

III - solicitar ao ex-integrante que informe, de imediato, qualquer tentativa de cooptação que venha a ser alvo; e

IV - informar o militar e o servidor desligado que o sigilo das informações que tomou conhecimento deverá ser mantido, de acordo com o Termo de Compromisso de Manutenção do Sigilo, assinado no início do desempenho da função, termo este que deverá permanecer arquivado na OM.

Art. 73. As medidas de segurança da documentação previstas nestas IG devem ser adotadas para as fases de produção, expedição, recepção, manuseio, arquivamento e eliminação.

Art. 74. As medidas de segurança da documentação devem ser adotadas para toda a documentação classificada ou sob restrição de acesso.

Parágrafo único. A publicação de ato normativo relativo à informação classificada ou sob restrição de acesso, esta devido a sigilo legal ou judicial, poderá limitar-se, quando necessário, aos respectivos números, data de expedição ou ementas, redigidos de modo a não comprometer o seu sigilo. obedecidas as seguintes prescrições:

I - é permitida a remessa por intermédio dos correios, desde que registrado;

II - é permitida a remessa por intermédio de mala diplomática;

III - pode ser empregado mensageiro, desde que credenciado.

§ 1º A expedição, a condução e a entrega de documento impresso com informação classificada em grau de sigilo ULTRASSECRETO será efetuada pessoalmente, por mensageiro credenciado, sendo vedada sua postagem.

§ 2º O mensageiro deverá ser instruído sobre como proceder quando pressentir qualquer tipo de ameaça ou incidente que possa resultar em comprometimento do sigilo do documento ou do material transportado.

[...]

Art. 82. Na expedição do documento impresso classificado ou de acesso restrito deverão ser observadas as seguintes prescrições:

I - o documento a ser expedido deverá ser acondicionado em envelope duplo;

II - o envelope externo deverá conter apenas a função do destinatário e seu endereço, sem qualquer anotação que indique o grau de sigilo ou o motivo da restrição de acesso ao seu conteúdo;

III - no envelope interno deverá ser inscrito o nome e a função do destinatário, o seu endereço e, claramente indicado, o grau de sigilo ou o motivo da restrição de acesso ao conteúdo do documento, de modo a ser visto logo que removido o envelope externo;

IV - o envelope interno deverá ser lacrado e o documento classificado ou sob restrição de acesso far-se-á acompanhado de um recibo; e

V - o recibo destinado ao controle da expedição/recepção e da custódia do documento classificado ou sob restrição de acesso deverá conter, necessariamente, indicação sobre o remetente, o destinatário e o número ou outro indicativo que identifique o documento.

Art. 83. O expediente que encaminha documento classificado ou sua cópia não será classificado, desde que não contenha frações significativas deste.

§ 1º Como medida complementar de segurança para o trâmite e manuseio desse tipo de expediente, deverá constar, em vermelho, ou na impossibilidade, em negrito, no campo “assunto” um dos seguintes textos, “encaminhamento de DOCUMENTO CLASSIFICADO” ou “encaminhamento de DOCUMENTO SOB RESTRIÇÃO DE ACESSO”.

§ 2º O trâmite eletrônico destes documentos será conforme previsto no art. 123 destas IG.

Art. 84. Quando, inicialmente, for necessário que somente o destinatário tome conhecimento do assunto tratado, o envelope interno deverá conter,

além do nome do destinatário, a inscrição "PESSOAL", precedendo a indicação da restrição ou classificação, quando houver.

[...]

Art. 87. Após despacho da autoridade competente, deverá ser confeccionado um registro onde ficarão anotados todos os dados identificadores da divisão/seção onde tramitou ou foi distribuído o documento classificado ou sob restrição de acesso e do militar ou do servidor que teve contato com a documentação.

Parágrafo único. Além do efeito de protocolo, o registro indicará a tramitação e o responsável pela custódia do documento.

Art. 88. Ao responsável pelo recebimento de documento classificado ou sob restrição de acesso incumbe:

I - verificar e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao destinatário, o qual informará ao remetente; e

II - proceder ao registro do documento e ao controle de sua tramitação, conforme previsto no art. 87 destas IG.

Art. 89. Recebido o documento impresso classificado ou sob restrição de acesso, o recibo anexado ao mesmo deverá ser assinado e datado pelo destinatário e devolvido ao remetente.

Parágrafo único. A remessa do recibo não deve ser feita com características de sigilo.

Art. 90. O destinatário de documento impresso classificado ou sob restrição de acesso deverá comunicar ao remetente qualquer indício de violação do documento, tal como rasuras, irregularidades de impressão ou de paginação.

Art. 91. O documento classificado ou sob restrição de acesso somente poderá ser manuseado por pessoa credenciada que tenha a necessidade de conhecer seu conteúdo e devidamente autorizada pelo Cmt, Ch ou Dir da OM.

Parágrafo único. Para tal, deve-se correlacionar o grau de sigilo com a categoria da credencial de segurança de quem manuseará o documento classificado ou sob restrição de acesso.

Art. 92. Todo o documento classificado ou sob restrição de acesso deverá ser manuseado pelo menor número possível de pessoas, a fim de tornar mais efetiva a sua segurança.

[...]

Art. 99. O documento classificado ou sob restrição de acesso deverá ser guardado em condições especiais de segurança.

[...]

Art. 100. É importante, também, que se estabeleçam procedimentos relativos à evacuação da documentação classificada ou sob restrição de acesso em situações de emergência.

Parágrafo único. Esta medida requer o estabelecimento de prioridades, de responsabilidades e a determinação antecipada de local alternativo para abrigar os documentos a serem salvos.

[...]

Art. 118. Caberá ao Cmt, Ch ou Dir a definição, a demarcação, a sinalização, a segurança e a concessão de acesso à área restrita, no âmbito de sua OM (seção, divisão, departamento, etc).

§ 1º Para tanto, deverá ser elaborada norma de controle de acesso às áreas restritas, com a finalidade de normatizar procedimentos.

§ 2º As áreas de Inteligência, Tecnologia da Informação, Jurídica, Cibernética, Comunicações, Ciência e Tecnologia, Guerra Eletrônica e as consideradas vitais para o pleno funcionamento da OM, tais como reserva

> de armamento, paiol, caixa d'água, central elétrica, dentre outras, deverão ser consideradas de acesso restrito.
>
> § 3º A norma de controle de acesso, citada no caput deste artigo, deverá contemplar a proibição da entrada de pessoas conduzindo máquina fotográfica, filmadora, celular, gravador ou qualquer meio de captura de imagens e sons, em área e instalação que seja armazenado documento ou material classificado ou sob restrição de acesso, sem a autorização expressa do Cmt, Ch ou Dir.
>
> § 4º Para efeito deste artigo, não é considerado visitante o ingresso de agente público ou o particular que, oficialmente, execute atividade pública diretamente vinculada à elaboração de estudo ou trabalho considerado sigiloso. (EB, 2014)

Por fim, a referida Portaria contempla em seus anexos diversos modelos de documentos a serem utilizados na elaboração de documentos classificados.

3 METODOLOGIA

3.1 Classificação da pesquisa

A pesquisa científica tem como objetivo estudar e compreender determinado fato com a finalidade de encontrar uma solução para um problema, por meio de um procedimento científico específico, sistemático e controlado. Considerando os procedimentos utilizados no desenvolvimento deste trabalho, a presente pesquisa foi classificada conforme apresentado a seguir.

3.1.1 Quanto à natureza

Apesar da existência de discussão de ideias, conhecimentos e técnicas no bojo da pesquisa, essa é classificada como aplicada em razão da apresentação de um resultado final (produto), que poderá ser utilizado em situações práticas do cotidiano da Corporação.

3.1.2 Quanto ao método

O método de abordagem aplicado no desenvolvimento da presente pesquisa foi o dedutivo, uma vez que foram estudadas legislações e doutrinas referentes ao tema, bem como o trabalho monográfico do Tenente Coronel QOBM/Comb. Fábio Martins da Silva, apresentado como requisito para conclusão do Curso de Altos Estudos para Oficiais Combatentes do CBMDF no ano de 2016.

3.1.3 Quanto aos objetivos

Quanto aos objetivos, a pesquisa caracterizou-se como exploratória, pois foi realizada uma revisão de literatura dos autores que tratam da Lei de Acesso à Informação e a consulta às legislações pertinentes ao tema.

3.1.4 Quanto à abordagem

Quanto à abordagem, a pesquisa teve como método a realização de uma investigação que considerou aspectos subjetivos, sendo, portanto, classificada como qualitativa.

3.1.5 Quanto aos procedimentos técnicos

Quanto aos procedimentos técnicos, trata-se de uma pesquisa bibliográfica e documental de análise da doutrina e legislação existentes sobre o assunto abordado.

O procedimento adotado para a coleta de dados foi a compilação das legislações que regulam o tratamento de informação classificada, emanadas pelo Poder Legislativo, os subsequentes atos normativos editados por instituições competentes, além dos conceitos doutrinários relacionados ao tema.

Após a reunião robusta das legislações pertinentes ao assunto, foram discutidos os aspectos imprescindíveis à produção de ato normativo interno, relacionados aos objetivos específicos, que deram ensejo à elaboração de Minuta de Portaria, produto final do trabalho monográfico.

Destaque-se, oportunamente, que a autora optou por não realizar entrevistas ou questionários por entender que nenhum desses procedimentos acrescentaria informação ou conteúdo relevante ao presente estudo. A problemática da necessidade de elaboração de norma interna foi abordada por meio da verificação das legislações já utilizadas no ordenamento jurídico vigente e a solução apresentada não demandava a manifestação de outros servidores.

4 RESULTADOS E DISCUSSÃO

Com a finalidade de subsidiar a discussão do presente estudo, toda a coleta de dados realizada e os resultados obtidos serão apresentados nos parágrafos que se seguem. Para tanto, demonstra-se oportuno destacar que o objetivo principal dessa pesquisa foi propor a regulamentação do tratamento da informação classificada produzida pelo CBMDF por meio da delimitação dos objetivos específicos, estrategicamente selecionados abaixo para conduzir a presente discussão.

4.1 Princípios constitucionais relacionados ao acesso à informação e ao tratamento da informação classificada

Para compreender o alcance e as implicações da edição da LAI no ordenamento jurídico brasileiro, iniciou-se a revisão de literatura com a abordagem dos princípios constitucionais aptos a justificar tanto o acesso à informação quanto a sua restrição, partindo da premissa da inexistência de direitos absolutos.

A LAI apresentou-se como uma norma precursora no sentido de retirar o administrado da posição de mero destinatário dos atos estatais, fazendo-o assumir o protagonismo diante das funções exercidas pelo Poder Público, celebrando dessa forma os caros princípios da publicidade e da transparência.

Contudo, ainda dentro da normatização trazida pela LAI, surge a necessidade estatal de não permitir o protagonismo do administrado em relação a determinados assuntos de caráter restrito, dando margem à utilização do princípio da supremacia do interesse público.

Neste sentido, enquanto os princípios da publicidade e da transparência são concebidos como verdadeiros pilares do Estado Democrático de Direito, criando, como consequência lógica, a obrigação para os órgãos públicos de disponibilizar as informações de interesse coletivo, o princípio da supremacia do interesse público se apresenta como garantidor da existência de determinados limites para o direito de acesso à informação.

Ressalte-se que parte expressiva da doutrina posiciona-se favoravelmente à aplicação do princípio da supremacia do interesse público sobre o particular em detrimento de outros princípios. Nos dizeres de Bandeira de Mello (2008, p.45):

> [...] trata-se de um verdadeiro axioma reconhecível no moderno Direito Público. Proclama a superioridade do interesse da coletividade, firmando a prevalência dele sobre o particular, como condição até mesmo da sobrevivência e asseguramento deste último. É pressuposto de uma ordem social estável, em que todos e cada um possa sentir-se garantidos e resguardados. (BANDEIRA DE MELLO, 2008, p.45)

Assim, o aparente conflito entre transparência (regra) e sigilo (exceção) pode ser discutido no patamar dos princípios constitucionais, a partir da análise do caso concreto, em que a razoabilidade conduzirá à conclusão de qual dos direitos juridicamente protegidos tem maior relevância: a garantia da ampla informação ou a necessidade de restringi-la.

4.2 Panorama geral sobre a transparência dos atos administrativos no Brasil e a limitação de acesso por meio do sigilo

Para desenvolver esse assunto, inicialmente conceituou-se transparência como a possibilidade de que qualquer cidadão tenha acesso às informações mantidas pelo governo, fazendo parte integrante do próprio processo democrático.

A difusão da transparência no Brasil está relacionada com a promulgação da Constituição Federal em 1988 e com o posterior surgimento de diversos movimentos relacionados ao direito à informação e ao combate à corrupção, tendo como significante marco normativo a publicação da LAI em 18 de novembro de 2011.

Diante deste cenário, entende-se que a administração pública passou a ser garantidora do acesso à informação aos cidadãos, tornando-se inadmissível a existência, em um Estado Democrático de Direito, de um governo sem transparência.

Contudo, ainda em sede de revisão de literatura, demonstrou-se imperativa a compatibilização da transparência e publicidade dos atos administrativos com a salvaguarda das informações consideradas sigilosas, não restando dúvidas quanto à inevitabilidade de que determinadas informações sofram limitações.

O próprio legislador aponta no texto da LAI quais são as informações que devem ser sofrer restrições de acesso: aquelas classificadas por autoridades como sigilosas e as que tratarem de informações pessoais[2].

As informações pessoais dizem respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais; e possuem acesso restrito, independentemente da classificação como sigilosas. Contudo, tais informações não se apresentam como questão central do presente estudo.

A discussão que se apresenta para análise, capaz de contribuir para o alcance dos objetivos gerais e específicos da presente pesquisa, se relaciona diretamente com as informações sigilosas que precisam ser submetidas a um processo rígido de tratamento.

Face ao exposto, ainda que o escopo da LAI seja a garantia da transparência dos atos de governo, o debate sobre a restrição do acesso a determinadas informações demonstra-se como ponto fundamental para a segurança da sociedade e especialmente para a atividade de inteligência, tema que será abordado a seguir.

[2] O rol de informações aptas a sofrer restrição de acesso, abrangido pela LAI, contempla apenas as hipóteses de proteção de informações pessoais e aquelas essenciais à segurança da sociedade e do Estado. Contudo, em situações excepcionais previstas na Constituição Federal ou em legislação ordinária diversa, podem ser estabelecidas outras restrições legislativas, como é o caso do segredo de justiça, do segredo industrial, do sigilo das comunicações, do sigilo de dados, do sigilo da fonte, do sigilo das votações, do sigilo do inquérito policial, do sigilo profissional, do sigilo fiscal e bancário, do sigilo da área das telecomunicações, do sigilo quando decretado estado de sítio, do sigilo da proposta apresentada em procedimento licitatório, dentre outros.

4.3 Consequências para a atividade de inteligência em razão da edição da LAI

No âmbito da revisão de literatura, destacou-se que a utilização de informações sigilosas é inerente à atividade de inteligência e a todo o processo através do qual o conhecimento é produzido, motivo pelo qual a edição da LAI teria causado enormes impactos na área.

O problema apresentado com a vigência da LAI no ordenamento jurídico brasileiro abrangeria uma aparente incompatibilidade da atividade de inteligência com os princípios democráticos constitucionalmente celebrados que permeiam especialmente o direito de acesso à informação.

De fato, as ações sigilosas são características marcantes dos serviços de inteligência, o que facilmente poder-se-ia levar à conclusão de que institutos como transparência e publicidade entrariam em colisão frontal com o sigilo. Apesar disso, nas palavras de Vilar-Lopes (2017, p. 47), a simples existência de informações sigilosas

> não obsta o exercício de uma efetiva gestão pública e de um efetivo controle social da informação, ainda mais quando o tema do sigilo das informações carrega consigo um vasto arcabouço legal e institucional de mecanismos de controles interno e externo. (VILAR-LOPES, 2017. P. 47).

Calderón (2014) reconhece no sigilo uma grande importância para a execução de determinadas atividades estatais e para a preservação da própria sociedade, especialmente no que concerne à diplomacia, à política, à defesa da soberania e à segurança pública, dentre outros assuntos afetos à atividade de inteligência.

Todavia, para que uma informação seja tratada de forma sigilosa em sintonia com os ditames constitucionais e legais, é imprescindível que exista um parâmetro de controle. É exatamente para isso que a LAI foi editada: para estabelecer regras para a classificação de informações estatais, prazos e formas de controle por meio de mecanismos seguros, institucionalizados e publicamente reconhecidos.

Entende-se que o equilíbrio entre o direito de acesso à informação e a atividade de inteligência é possível e reforça a democracia no país. Ainda que

alguma informação necessite ter seu acesso restringido para o adequado exercício dos órgãos de inteligência, o que se objetiva ao final é a produção de conhecimento em nível estratégico para assessoramento do processo decisório pátrio.

Assim, o Estado Democrático de Direito e a atividade de inteligência se legitimam e devem conviver harmonicamente para fins do cumprimento do disposto na LAI e na Constituição Federal.

Diante do exposto, como consequência da edição da LAI não se verifica a limitação da atividade de inteligência, e sim a adoção de procedimentos específicos, padronizados e regulamentados, especialmente no que concerne ao tratamento da informação classificada.

Especificamente em relação à atividade exercida pelo CEINT/CBMDF, alguns impactos foram observados diretamente na rotina do órgão, sobretudo diante das regras trazidas pelas Portarias nº 05/2016 e nº 09/2019, da Casa Militar do Distrito Federal. Contudo, tais consequências serão detalhadas no tópico seguinte em razão da necessidade de análise da abrangência das legislações pertinentes ao tema.

4.4 Dispositivos legais que abordam o tratamento da informação classificada em âmbito Federal, Distrital e no CBMDF

A partir da leitura das legislações pertinentes ao tema, quais sejam: Lei Federal 12.527/2011, Lei Distrital nº 4.990/2012, Decreto Distrital nº 34.276/2013, Decreto Distrital nº 35.382/2014, Portaria nº 5, de 29 de fevereiro de 2016 e Portaria 09, de 10 de outubro de 2016, ambas editadas pela Casa Militar do Distrito Federal, verifica-se que o tratamento da informação classificada teve uma ampla e minuciosa abordagem por parte do legislador infraconstitucional. Os aspectos mais relevantes dos referidos atos normativos, destacados na revisão de literatura, serão analisados e discutidos nos parágrafos seguintes.

Inicialmente, tanto a LAI Federal quanto a LAI Distrital tratam das diretrizes que asseguram o direito fundamental de acesso à informação. Merece realce aquela que estabelece a publicidade como preceito geral e sigilo como exceção, por ser um dos pilares do tratamento da informação e por encontrar origem

no texto Constitucional, conforme disposto no inciso XXXIII do artigo 5º:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que são prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. (BRASIL, 1988).

A máxima “publicidade como regra e o sigilo como exceção” apresenta-se como um verdadeiro preceito geral que norteia toda a sistemática e interpretação da LAI e demais atos normativos, e conduz à composição das demais diretrizes, quais sejam: a divulgação de informações de interesse público, independentemente de solicitações; utilização de meios de comunicação viabilizados pela tecnologia da informação; fomento ao desenvolvimento da cultura de transparência na administração pública e o desenvolvimento do controle social da administração pública.

Nesse aspecto, Heinen (2015, p. 118) afirma que as diretrizes relacionadas na LAI Federal (e integralmente reproduzidas na LAI Distrital) constituem uma verdadeira “tábua de valores ao acesso aos dados públicos, confiando padrões axiológicos à compreensão do restante das regras”.

Em relação às informações passíveis de classificação, cujo conteúdo dever ser conhecido por um número restrito de pessoas, a LAI Distrital, nos exatos termos da LAI Federal, elencou aquelas consideradas imprescindíveis à segurança da sociedade e do Estado, que demandam sigilo por razões estratégicas relativas à existência, manutenção e desenvolvimento do próprio Estado.

Exige-se, de tal forma, a edição de um ato administrativo apto a classificar a informação como sigilosa, devendo estar fundamentada em uma das oito hipóteses taxativas discriminadas no artigo 23 da Lei nº 12.527/2011, ou no artigo 25 da Lei nº 4.990/2012, a depender da esfera de atuação do órgão classificador.

Observando-se o grau de imprescindibilidade em relação à segurança do Estado e da sociedade, a informação poderá ser classificada como reservada, secreta e ultrassecreta nos prazos máximos de 05, 15 e 25 anos, respectivamente. Assim, verifica-se que a LAI vincula o grau da informação a um maior ou menor

prazo de sigilo. Acrescente-se, oportunamente, que tais regras criadas pela LAI Federal devem obrigatoriamente ser reproduzidas por todos os entes federativos, não sendo admitida a adoção de outros níveis de sigilo em legislações internas.

Aliás, é importante mencionar que a LAI estabeleceu prazos máximos de restrição de acesso, o que permite ao gestor público (autoridade classificadora) estabelecer limites inferiores, utilizando como parâmetro o interesse público da informação e o critério menos restritivo possível, considerando a gravidade do risco ou o dano à segurança da sociedade e do Estado, nos termos do parágrafo 5º do artigo 24.

No que concerne à competência para classificar uma informação, as autoridades descritas no texto legal são aquelas relacionadas à abrangência de atuação de cada órgão. Atendendo à diretriz “publicidade como regra e o sigilo como exceção”, o legislador previu uma quantidade reduzida de autoridades aptas a classificar e utilizou como parâmetro a sensibilidade de cada informação.

Ademais, ao classificar uma informação, a autoridade deverá, necessariamente, motivar e justificar tal ato, de acordo com o disposto na regulamentação em apreço e em plena consonância com um dos princípios administrativos mais celebrados pelo sistema jurídico pátrio, o princípio da motivação.

No que tange aos Decretos Distritais regulamentadores da Lei nº 4.990/2012, percebe-se que o legislador preocupou-se em elaborar regras sobre o credenciamento de segurança e o tratamento das informações classificadas, com dispositivos sobre os cuidados a serem adotados quando um documento sigiloso é tratado, a marcação do sigilo no documento, as inscrições nos envelopes que guardam os documentos, o código de indexação, a indicação do prazo de sigilo, dentre outros.

O TCI, previsto no artigo 31 do Decreto nº 34.276/2013, é o ato que concretiza a classificação da informação pela autoridade. Assim, a decisão de classificação, consubstanciada no TCI, é de caráter puramente declaratório, uma vez que não altera a natureza da informação, apenas garante o seu sigilo.

Dentre as informações que devem estar dispostas no TCI, destaca-se a exigência de inserção de duas datas distintas: a data de produção do conhecimento e a data da classificação. Dessa forma, considera-se adequada a realização de classificação posteriormente ao pedido de acesso à informação. Assim, mesmo que o pedido de acesso a determinada informação ocorra antes da classificação, a autoridade pode classificá-la e negar o acesso ao cidadão demandante, desde que preenchidos os critérios exigidos para a classificação.

Quanto à obrigatoriedade de utilização de credencial de segurança para acesso a documento classificado, regulamentada por meio do Decreto nº 35.382/2014, oportuno ressaltar que a necessidade de conhecer é condição essencial para efetivação do ato, nos termos do artigo 24:

> Art. 24. O acesso, a divulgação e o tratamento de documento controlado somente poderão ser concedidos à pessoa que tenha necessidade de conhecê-lo e que possua Credencial de Segurança no grau apropriado e na forma deste Decreto.
>
> § 1º A necessidade de conhecer, de que trata este artigo, decorre do efetivo exercício de cargo, função ou atividade.
>
> § 2º O acesso, concedido à determinada pessoa, deverá ser continuamente reavaliado pelo dirigente, que o cancelará tão logo deixe de ser preenchida qualquer condição estabelecida para sua concessão. (DISTRITO FEDERAL, 2014)

Contudo, o próprio Decreto estabeleceu uma hipótese em que a emissão de credencial de segurança seria dispensável, mediante a assinatura de TCMS, “pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa”, nos termos do artigo 26.

Quanto às regras trazidas pelas Portarias nº 05/2016 e 09/2016, da Casa Militar do Distrito Federal, importante destacar que o CBMDF foi credenciado pelo NSC como órgão de registro nível 1, recebendo, assim, as competências previstas nas referidas normas, quais sejam: 1- encaminhamento semestral (ou a qualquer momento, quando solicitado) ao NSC, de relatórios sobre suas atividades de credenciamento, habilitação e funcionamento; e 2- notificação imediata ao NSC quando ocorrer a quebra de segurança de informações classificadas na sua esfera de atuação.

Além do credenciamento do CBMDF como órgão de registro nível 1, após a edição das supracitadas Portarias, o PC foi credenciado dentro do CEINT, sendo de sua competência, portanto, o armazenamento, o controle e a manutenção da segurança de todas as informações classificadas no âmbito do CBMDF, o que necessariamente o obriga a cumprir a qualificação técnica mínima exigida pelo artigo 25 da Portaria nº 09/2016, conforme quadro abaixo apresentado:

Figura 8 – Impactos causados ao CEINT/CBMDF após o credenciamento como Posto de Controle

Inciso	Exigência	Cumprimento pelo CEINT
I	Estar localizado em área de acesso restrito.	A edificação em que se localiza o CEINT não é exclusiva, sendo compartilhada com outra unidade da Corporação e separada apenas por uma parede. Para adentrar o Centro, existem duas possibilidades: a porta de entrada principal, que dá acesso a uma antessala (com monitoramento por circuito fechado de televisão) ou a porta dos fundos, que dá acesso à sala do Comandante da unidade, único que a utiliza.
II	Possuir meios de armazenamento de documentos físicos e eletrônicos com nível de segurança compatível com os graus de sigilo e volume.	O armazenamento físico do CEINT é realizado por meio cofres e armários simples de madeira com chave. O armazenamento eletrônico é feito por meio de um sistema particular de guarda de arquivos em servidor próprio. Também são feitos backups de documentos em discos rígidos (HD) e trancados nos cofres.
III	Possuir estrutura física adequada para o armazenamento e preservação dos documentos físicos e eletrônicos.	Servidor do CEINT é adequado para a demanda da unidade no que se relaciona ao armazenamento e preservação dos documentos eletrônicos. Contudo, a unidade não possui um dispositivo capaz de fornecer energia elétrica (nobreak) por tempo superior a 15 minutos, o que ocasiona seu desligamento e inacessibilidade, ficando suscetível a perda de dados. Ademais, o CEINT possui cofres de ferro e armários de madeira (com chaves) adequados ao armazenamento de arquivos físicos, O CEINT não possui monitoramento por câmeras para verificação da data, hora e militar que acessa

		qualquer dos arquivos de documentos físicos e eletrônicos.
IV	Possuir planos e procedimentos de contingência de forma a assegurar a continuidade dos processos essenciais no caso de falhas ou sinistros.	O único procedimento de salvaguarda dos documentos eletrônicos é o backup automático do servidor realizado diariamente às 04h00. Diante de qualquer pane no servidor do CEINT, a única equipe capacitada para solucionar está lotada na Diretoria de Tecnologia da Informação (DITIC), e não no próprio Centro de Inteligência. Não existe plano ou procedimento para a salvaguarda da estrutura física da unidade.
V	Possuir meios de comunicação segura compatível com os graus de sigilo	Os meios de comunicação utilizados pelos militares lotados no CEINT são os telefones fixos das seções, telefones móveis funcionais e particulares, correios eletrônicos corporativos e particulares, e aplicativos de mensagens instantâneas. A única comunicação segura (criptografada) utilizada no CEINT é com a Subsecretaria de Inteligência (SI) da Secretaria de Estado de Segurança Pública/DF e com a Diretoria de Inteligência (DINT) da Secretaria de Operações Integradas (SEOPI), do Ministério da Justiça e Segurança Pública.
VI	Possuir suas redes de dados e seus sistemas de tecnologia da informação adequadamente protegidos de ataques eletrônicos, sendo que os equipamentos que armazenem informações classificadas não devem estar conectados à rede corporativa do órgão.	A rede do CEINT é independente e própria, e todos os computadores da unidade acessam essa rede. Apenas dois computadores do Centro acessam o domínio do CBMDF: um do Comandante do Centro e outro da área administrava.
VII	Possuir sistemas alternativos de proteção da infraestrutura crítica relacionada com os ativos de informação e materiais de acesso restrito sob sua responsabilidade de armazenamento e controle	O sistema alternativo de proteção utilizado no CEINT é uma *Virtual Private Network* (VPN), compreendida como uma rede de comunicações privada construída sobre uma rede de comunicações pública. O CEINT também possui em seus sistemas um *Firewall* (dispositivo de segurança que monitora o tráfego que entra e sai da rede).
VIII	Atender aos princípios de	No que concerne aos pilares da

	disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação e materiais de acesso restrito sob sua responsabilidade.	segurança da informação, o CEINT adota os seguintes princípios: 1. Confidencialidade: a única comunicação segura utilizada é com a SI/SSPDF e com a DINT/SEOPI, do Ministério da Justiça e Segurança Pública. Ademais, o CEINT adota medidas adequadas a restrições de acesso a determinado dados. 2. Integridade: apenas as informações trocadas com a SI/SSPDF e a DINT/SEOPI estão completamente protegidas de sofrer alterações durante seu tráfego, armazenamento ou processamento. 3. Disponibilidade: a informação armazenada eletronicamente no sistema particular de guarda de arquivos está disponível apenas ao usuário que utiliza a rede própria do CEINT ou uma VPN e que tenha necessidade de conhecer. 4. Autenticidade: todos os documentos oriundos da unidade estão identificados pela sua autoria, mantendo a veracidade da informação.
IX	Possuir protocolo exclusivo para documentos classificados, e quando necessário, de Documentos Controlados.	O CEINT utiliza um protocolo de documentos controlados específico, conforme determinado pelo Decreto nº 7.845/2012, que é o Código de Indexação de Documento que contém Informação Classificada (CIDIC)
X	Possuir restrição ao uso de máquinas fotográficas, gravadores de vídeo e áudio, ou similares, tais como câmeras de dispositivos móveis no interior das instalações do PC.	O CEINT não realiza esse tipo de restrição.
XI	Possuir quadro de pessoal capacitado para o tratamento de informação classificada.	A Gerência do Núcleo de Segurança e Credenciamento da Casa Militar do Distrito Federal realizou uma capacitação com todos os militares do CEINT para fins de conhecimento das disposições previstas na LAI e demais atos normativos decorrentes.
XII	Possuir recursos criptográficos para armazenamento e transmissão de informação classificada em conformidade com as normas estabelecidas pela Casa Militar do Distrito Federal.	O CEINT utiliza sistema de decodificação no recebimento e envio de documentos criptografados para SI/SSPDF e DINT/SEOPI.

Fonte: a autora.

Ademais, o Comandante do CEINT foi designado como GSC da Corporação, sendo responsável pelos procedimentos relativos ao tratamento de informações classificadas no âmbito da caserna, nos termos do artigo 7º da Portaria nº 05/2016, dentre os quais destaque-se a proposição à autoridade máxima do órgão ou entidade com a qual mantém vínculo, de normas para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos.

Sendo assim, o GSC do CBMDF (ou seja, o Comandante do CEINT) deve propor ao Comandante Geral a edição de norma interna para o tratamento das informações classificadas, o que se apresenta como ponto central da elaboração da presente pesquisa. Entretanto, para que tal norma interna seja apresentada e publicada de modo a cumprir todas as disposições legais, e especialmente, de forma a alcançar o objetivo a que se propõe, demonstra-se relevante toda a discussão exposta neste estudo.

A simples reprodução de normas anteriores que tratam da temática em apreço mostra-se desnecessária e ineficaz. Diante de tudo o que foi estrategicamente selecionado nas legislações abordadas, percebe-se a necessidade de elaboração de um ato normativo interno que descreva especificamente:

A- a atuação do CBMDF como órgão de registro nível 1;

B- as autoridades competentes no CBMDF para classificar a informação;

C- as possíveis delegações de competência para classificação de informação;

D- o papel central do CEINT como PC do tratamento das informações classificadas;

E- normas para o tratamento da informação classificada e o acesso às áreas, instalações e materiais de acesso restrito;

F- as atribuições dos demais órgãos do CBMDF no que concerne ao tratamento das informações classificadas em seus respectivos âmbitos de atuação e a necessária articulação com o CEINT em todas as etapas de tal atividade.

4.5 Influência dos atos normativos produzidos no âmbito de outros órgãos públicos

A Constituição Federal ocupa posição de destaque e fundamento de validade de todas as demais normas do ordenamento jurídico, e a partir de suas premissas são elaborados os atos normativos infraconstitucionais (leis complementares, ordinárias, delegadas, medidas provisórias e decretos legislativos)

Abaixo das leis, encontram-se as normas infralegais, dentre as quais as Portarias se apresentam como atos administrativos-normativos que manifestam a vontade do Estado com fundamento em uma lei, regulamento ou decreto anterior.

O Gabinete de Segurança Institucional da Presidência da República, o Exército Brasileiro e a Casa Militar do Distrito Federal optaram por publicar suas respectivas Portarias que abordam o tratamento da informação classificada com respaldo nas Leis de Acesso a Informação (LAI Federal no caso do GSI e do EB e LAI Distrital no caso da Casa Militar) e nos Decretos Regulamentadores.

O conteúdo das três Portarias estudadas apresenta algumas divergências. Enquanto as Portarias do GSI e do EB reproduzem boa parte do texto da LAI Federal, trazendo alguns procedimentos particulares de seus órgãos internos, a Portaria da Casa Militar do Distrito Federal abordou de maneira objetiva e direta a atuação das unidades subordinadas no que tange ao tratamento da informação classificada.

Outros órgãos da Administração Pública elaboraram manuais práticos com o objetivo de auxiliar autoridades, servidores e demais colaboradores a identificar os tipos de informações públicas, conhecer suas classificações, realizar procedimentos quanto à gestão de informações classificadas, dentre outras atividades. Entretanto, tais manuais não foram incluídos no presente trabalho em razão da ausência de contribuição de conteúdo e forma para a elaboração do produto final da presente pesquisa, que será apresentado em formato de Portaria, nos moldes das publicadas pelo GSI, EB e Casa Militar.

5 CONSIDERAÇÕES FINAIS

Diante da minuciosa análise das legislações que abordam o tratamento da informação classificada, tendo como ponto de partida a Lei Federal nº 12.527/2011, seguida da Lei Distrital nº 4.990/2012, passando pelos Decretos Distritais nº 34.276/2013 e nº 35.382/2014, chega-se ao texto da Portaria nº 5/2016, em que a Casa Militar do Distrito Federal expressamente determina que o Gestor de Segurança e Credenciamento do CBMDF (ou seja, o Comandante do Centro de Inteligência) proponha ao Comandante Geral a edição de norma interna para o tratamento das informações classificadas.

Assim, ainda que a LAI Federal tenha sido editada no ano de 2011, apenas em 29 de fevereiro de 2016, com a vigência da Portaria nº 05, da Casa Militar do Distrito Federal, tornou-se terminantemente necessária a regulamentação do tratamento da informação classificada produzida pelo CBMDF, o que encorajou a elaboração do presente trabalho monográfico.

Neste contexto, a pesquisa demonstrou quais os parâmetros devem ser seguidos para uma adequada elaboração de ato normativo que respeite os limites impostos pelos princípios constitucionais aplicáveis, que possibilite o adequado exercício da atividade de inteligência dentro da Corporação, que esteja em perfeita consonância com a legislação pátria aplicável ao tema e que encontre harmonia com os atos normativos produzidos por outros órgãos congêneres.

A presente pesquisa evidenciou, ainda, as relevantes atribuições do Centro de Inteligência como unidade central do tratamento da informação classificada e a sua competência para a condução dos procedimentos relacionados ao armazenamento e controle dos documentos controlados no âmbito do CBMDF.

Alguns óbices foram verificados no que concerne ao cumprimento integral das exigências dispostas nas legislações exaustivamente discutidas, em especial as Portarias nº 5/2016 e nº 09/2019, em que a Casa Militar do Distrito Federal determina o atendimento de alguns requisitos, especialmente no que concerne à qualificação técnica dos Postos de Controle.

Para que o CEINT possa estar adequado ao que determina a Casa Militar, a pesquisa evidenciou algumas providências a serem adotadas, como a utilização de espaço físico próprio, o incremento no armazenamento de documentos físicos e eletrônicos, a adoção de meios de comunicação compatíveis com os graus de sigilo, dentre outros.

Diante do exposto, conclui-se que a elaboração de uma regulamentação do tratamento da informação classificada produzida pelo CBMDF, em paralelo com a adequação técnica do Centro de Inteligência como Posto de Controle, possibilitará grandes avanços no que concerne às inovações trazidas pela Lei de Acesso à Informação e demais normas decorrentes.

6 RECOMENDAÇÕES

O presente trabalho monográfico teve como finalidade servir de subsídio para a elaboração de um produto que se apresente como uma solução ao problema abordado, levando-se em consideração todos os aspectos analisados, motivo pelo qual serão apresentadas algumas recomendações.

A primeira recomendação é a edição de ato normativo que aborde especificamente o tratamento da informação classificada produzida pelo CBMDF, por meio de proposta elaborada pelo Comandante do Centro de Inteligência e referendada pelo Comandante Geral, conforme texto apresentado no Apêndice A, consolidado em uma Minuta de Portaria.

A Minuta de Portaria apresentada contempla a atuação do CBMDF como órgão de registro nível 1, a competência do Comandante Geral para fins de classificação de informação, as possíveis delegações de competência para classificação de informação, o papel central do CEINT como Posto de Controle do tratamento das informações classificadas, as normas para o tratamento da informação classificada e o acesso às áreas, instalações e materiais de acesso restrito e as atribuições dos demais órgãos do CBMDF no que concerne ao tratamento das informações classificadas em seus respectivos âmbitos de atuação e a necessária articulação com o CEINT em todas as etapas de tal atividade.

A segunda recomendação concerne à adequação do Centro de Inteligência do CBMDF às exigências previstas no artigo 25 da Portaria nº 09/2016, uma vez que a unidade está credenciada como o Posto de Controle da Corporação e deve cumprir a qualificação técnica mínima exigida.

Assim, sugere-se:

i. A transferência das seções localizadas no prédio do Quartel do Comando Geral para uma edificação própria, que não faça divisa com outros órgãos da Corporação, cumprindo a exigência que determina que o PC esteja localizado em área de acesso restrito;

ii. A segregação das seções de inteligência, contrainteligência, e administrativa, que atualmente estão dispostas em uma área comum, sem paredes divisórias, o que prejudica a compartimentação da atividade;

iii. A utilização de monitoramento por circuito fechado de televisão em toda a unidade;

iv. O incremento nos meios de armazenamento de documentos eletrônicos, por meio de aquisição de dispositivos mais eficazes capazes de fornecer energia elétrica (nobreak);

v. A elaboração de planos e procedimentos de contingência de forma a assegurar a continuidade dos processos em caso de falhas ou sinistros;

vi. A implementação de meios de comunicação seguros e compatíveis com os graus de sigilo utilizados na unidade, em observância ao princípio da confidencialidade e da integralidade;

vii. O desenvolvimento de um sistema seguro de armazenamento eletrônico de arquivos que possa ser disponibilizado aos militares do CEINT em qualquer local, e não apenas quando estiverem conectados na rede do Centro; e

viii. A elaboração de um plano específico para o rígido controle no que concerne utilização de máquinas fotográficas, gravadores de vídeo e áudio, ou similares, tais como câmeras de dispositivos móveis no interior das instalações do Posto de Controle.

Por fim, recomenda-se que a presente pesquisa seja classificada com grau de sigilo adequado, observada a legislação em vigor.

REFERÊNCIAS

BANDEIRA DE MELLO, Celso Antônio. **Curso de direito administrativo**. 25. Ed. São Paulo: Malheiros, 2008.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em:<http:www.planalto.gov.br>. Acesso em: 05AGO2019.

_____. Comando do Exército. **Portaria nº 1.067, de 08 de setembro de 2014**. Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011). 1ª Edição, 2014. Publicado na Separada ao Boletim do Exército, nº 37, de 12 de setembro de 2014.

_____. Presidência da República. **Decreto nº 7.724, de 16 de maio de 2012.**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Disponível em: <www.planalto.gov.br.>. Acesso em: 02OUT2019.

_____. Presidência da República. **Decreto nº 7.845, de 12 de novembro de 2012.**. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Disponível em: <www.planalto.gov.br.>. Acesso em: 19NOV2019.

_____. Presidência da República. **Lei nº 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: <www.planalto.gov.br.>. Acesso em: 08OUT2019.

_____. Presidência da República. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, do art. 216 da Constituição Federal, altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <www.planalto.gov.br.>. Acesso em: 05AGO2019.

_____. Presidência da República. **Portaria nº 32, de 19 de agosto de 2013.** Regula procedimentos relacionados ao credenciamento de segurança e tratamento de informação classificada no âmbito do Gabinete de Segurança Institucional da Presidência da República. Publicado no Diário Oficial da União nº 160, de 20 de agosto de 2013.

CALDERON, Mariana Paranhos. **Lei de acesso à informação e seu impacto na atividade de inteligência**. Campinas, SP: Millennium Editora, 2014.

CANOTILHO, J.J. Gomes; MENDES, Gilmar F; SARLET, Ingo W.; STRECK, Lenio L. (Coords), **Comentários à Constituição do Brasil.** São Paulo: Saraiva/Almedina, 2013.

CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL. **Portaria nº 28, de 17 de maio de 2011.** Aprova o Regimento do Centro de Inteligência do CBMDF. Brasília, DF, maio de 2011. Publicada no Boletim Reservado nº 20, de 17 mai. 2011.

DA COSTA JR, Paulo José. **O Direito de Estar Só: Tutela Penal da Intimidade.** 4ª Ed. São Paulo: Revista dos Tribunais, 2007.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** 27ª Ed. São Paulo: Atlas, 2014.

DISTRITO FEDERAL. Casa Militar. **Portaria nº 05, de 29 de fevereiro de 2016.** Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Distrital. Publicado no Diário Oficial do Distrito Federal, 2016.

_____. Casa Militar. **Portaria nº 09, de 10 de outubro de 2016.** Dispõe sobre os procedimentos do credenciamento de segurança para o tratamento de informação classificada do Núcleo de Segurança e Credenciamento - NSC, dos Órgãos no âmbito do Poder Executivo Distrital e das Entidades Privadas e dá outras providências. Publicado no Diário Oficial do Distrito Federal, 2016.

_____. Casa Militar. **Portaria nº 11, de 20 de fevereiro de 2018.** Regula os procedimentos relacionados ao credenciamento de segurança e ao tratamento de informação classificada em grau de sigilo no âmbito da Casa Militar da Governadoria do Distrito Federal. Publicado no Diário Oficial do Distrito Federal, 2018.

_____. **Decreto Distrital nº 31.817, de 21 de junho de 2010.** Regulamenta o inciso II, do artigo 10-B, da Lei nº 8.255, de 20 de novembro de 1991, que dispõe sobre a Organização Básica do Corpo de Bombeiros Militar do Distrito Federal. Brasília, DF, junho de 2010. Disponível em: <www.sinj.df.gov.br.>. Acesso em: 05AGO2019.

_____. **Decreto Distrital nº 34.276, de 11 de abril de 2013.** Regulamenta a Lei nº 4.990, de 12 de dezembro de 2012, dispõe sobre 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, todos da Constituição Federal de 1988. Disponível em: <www.fazenda.df.gov.br.>. Acesso em: 05AGO2019.

_____. **Decreto Distrital nº 35.382, de 29 de abril de 2014.** Regulamenta o art. 42, da Lei nº 4.990, de 12 de dezembro de 2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências. Disponível em: <www.fazenda.df.gov.br.>. Acesso em: 05AGO2019.

_____. **Lei Distrital nº 4.990, de 12 de dezembro de 2012.** Regula o acesso a informações no distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18 de novembro de 2011, e dá outras providências. Disponível em: <www.fazenda.df.gov.br.>. Acesso em: 05AGO2019.

_____. **Lei Distrital nº 6.432, de 20 de dezembro de 2019.** Altera o caput do art. 42 da Lei nº 4.990 , de 12 de dezembro de 2012, que regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18 de novembro de 2011, e dá outras providências. Disponível em: <www.fazenda.df.gov.br.>. Acesso em: 09JAN2020.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os Desafios da Administração Pública na Disponibilização de Dados Sensíveis. **Revista Direito GV**, São Paulo, v. 14, n. 2, p. 513-536, maio-ago 2018.

HEINEN, Juliano. **Comentários à Lei de Acesso à Informação: Lei nº 12.527/2011.** 2. Ed. ver. e atual. Belo Horizonte: Fórum, 2015.

MACEDO, V. R. . **Causas e Origens da Transparência no Brasil.** In: II Semana de Pós-Graduação em Ciência Política, 2014, São Carlos. GT6 - Política Internacional, 2014.

MARTINS JÚNIOR, Wallace Paiva. **Transparência Administrativa: Publicidade, Motivação e Participação Popular.** 2. ed. São Paulo: Saraiva, 2010.

MEIRELES, Hely Lopes. **Direito Administrativo Brasileiro**. 33ª Edição. São Paulo: Malheiros Editores, 2007.

RODRIGUES, João Gaspar. Publicidade, Transparência e Abertura na Administração Pública. **Revista de Direito Administrativo**. Rio de Janeiro, v. 266, p. 89-123, maio-ago 2014.

ROSSETI, Disney. **As atividades de inteligência de estado e de polícia e a lei de acesso a informação no contexto do estado democrático de direito.** Brasília, DF, 2012. 132f. Dissertação de mestrado – Centro Universitário de Brasília, 2012.

VILAR-LOPES, Gills. Quando o Segredo é a Regra: Atividade de Inteligência e Acesso à Informação no Brasil. **Revista Brasileira de Inteligência**. Brasília, Abin, n.12, p.35-49, dezembro 2017.

APÊNDICES

APÊNDICE A

Minuta de Portaria

MINUTA DE PORTARIA

ATO DO COMANDANTE-GERAL DO CBMDF

PORTARIA Nº ___, DE ___ DE _____ DE 2020.

Regula os procedimentos relacionados ao tratamento de informação classificada em grau de sigilo e ao credenciamento de segurança no âmbito do Corpo de Bombeiros Militar do Distrito Federal.

O COMANDANTE-GERAL, no uso das atribuições que lhe confere o art. 7º, incisos II, III, V e VI, do Decreto Federal nº 7.163, de 29 abr. 2010, que regulamenta o art. 10-B, inciso I da Lei nº 8.255, de 20 nov. 1991, que dispõe sobre a organização Básica do CBMDF; concomitante com o art. 58 do Decreto Distrital nº 34.276, de 11 de abril de 2013, e com o art. 62 do Decreto Distrital nº 35.382, de 29 de abril de 2014, RESOLVE:

Art. 1º Ficam aprovadas as diretrizes e os procedimentos relacionados ao tratamento da informação classificada em grau de sigilo e ao credenciamento de segurança no âmbito do Corpo de Bombeiros Militar do Distrito Federal - CBMDF.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º As unidades do CBMDF deverão assegurar que os militares que tratem informação classificada em grau de sigilo tenham conhecimento do teor da Lei nº 4.990, de 12 de dezembro de 2012, do Decreto Distrital nº 34.276, de 11 de abril de 2013, do Decreto Distrital nº 35.382, de 29 de abril de 2014, da Portaria nº 5, de 29 de fevereiro de 2016 e da Portaria nº 9, de 10 de outubro de 2016, ambas editadas pela Casa Militar do Distrito Federal.

Art. 3º A informação no âmbito do CBMDF, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade e do Estado, poderá ser classificada no grau ultrassecreto, secreto ou reservado.

Parágrafo único. Os prazos máximos de restrição de acesso à informação classificada vigoram na data de sua produção e são os seguintes:

I- para o grau de sigilo ultrassecreto: 25 (vinte e cinco) anos;

II- para o grau de sigilo secreto: 15 (quinze) anos;

III- para o grau de sigilo reservado: 5 (cinco) anos.

Art. 4º A classificação de informação é de competência:

I - nos graus ultrassecreto e secreto, da seguinte autoridade:

a) Comandante-Geral.

II - no grau de reservado:

a) a autoridade referida no inciso I;

b) Subcomandante-Geral;

c) Comandante Operacional;

d) Chefe do Estado-Maior-Geral;

e) Controlador;

f) Chefes de Departamentos;

g) Ajudante Geral;

h) Comandante do Centro de Inteligência;

i) Comandante do Núcleo de Custódia.

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

§2º O Comandante-Geral poderá delegar a competência para classificação no grau reservado aos militares que exerçam função de direção, comando ou chefia, vedada a subdelegação.

§3º Os militares que não possuam competência para classificar informação e que ocasionalmente tenham acesso a documento ou material classificado deverão encaminhar para seu chefe imediato para fins de remessa a uma das autoridades previstas nos incisos I e II do presente artigo.

Art. 5º Os pedidos de acesso à informação deverão obedecer à sistemática estabelecida pelos artigos 12 a 24 do Decreto Distrital nº 34.276, de 11 de abril de 2013.

Art. 6º Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento tratamento do grau de sigilo mais elevado, ficando assegurado o acesso às partes não classificadas por meio de certidão, extrato ou cópia, com ocultação da parte sob sigilo.

Art. 7º A classificação das informações será reavaliada pela autoridade classificadora, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.

Parágrafo único. Negado o pedido de desclassificação ou de reavaliação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contado da ciência da negativa, à autoridade hierarquicamente superior, que decidirá no prazo de trinta dias.

Art. 8º O acesso, a divulgação e o tratamento de informação classificada em qualquer grau de sigilo ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam credenciadas segundo as normas fixadas pela presente Portaria, sem prejuízo das atribuições de agentes públicos autorizados por lei.

Art. 9º A segurança da informação classificada é de responsabilidade do militar que tenha acesso a estas informações, constituindo condutas ilícitas que ensejam responsabilidade civil, administrativa e penal previstas no art. 35 da Lei 4.990/2012.

Art. 10. Não poderá ser negado acesso às informações necessárias à tutela judicial ou administrativa de direitos fundamentais.

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

CAPÍTULO II

DO GESTOR DE SEGURANÇA E CRECENCIAMENTO

Art. 11. O Gestor de Segurança e Credenciamento – GSC do CBMDF é responsável por promover a gestão da segurança e do credenciamento dos postos de controle e dos bombeiros militares da Corporação no que se refere ao tratamento das informações classificadas em grau de sigilo, nos termos do artigo 7º da Portaria nº 05/2016, da Casa Militar do Distrito Federal.

Art. 12. O GSC e seu suplente serão nomeados pelo Comandante-Geral e deverão possuir a credencial de segurança para acesso a informações até o grau de sigilo ultrassecreto.

Parágrafo único. Os atos de nomeação ou substituição do GSC e seu suplente serão publicados em Boletim Geral da Corporação e deverão ser informados ao Núcleo de Segurança e Credenciamento da Casa Militar do Distrito Federal.

Art. 13. É de competência do GSC a publicação anual, até o dia 1º de maio, em sítio oficial na Internet:

I - rol das informações desclassificadas do exercício anterior;

II - rol das informações classificadas em cada grau de sigilo no exercício anterior, o qual 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, bem como informações genéricas sobre os solicitantes.

Art. 14. Para cumprimento do previsto no artigo 13, as autoridades do CBMDF competentes para classificar e desclassificar documentos deverão informar ao GSC, até o dia 1º de abril, o previsto nos itens I, II e III do referido artigo.

CAPÍTULO III
DO POSTO DE CONTROLE

Art 15. O Posto de Controle do CEINT é credenciado pelo Núcleo de Segurança e Credenciamento da Casa Militar do Distrito Federal como primeiro posto de controle do CBMDF, sendo responsável pelo controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza e pela garantia da segurança de informação classificada sob sua responsabilidade, nos termos do artigo 5º da Portaria nº 05/2016, da Casa Militar do Distrito Federal.

§1º A critério do GSC, outras unidades do CBMDF também poderão ser habilitadas como posto de controle.

§2º Até a criação dos outros postos de controle, todas as informações classificadas produzidas pelas unidades do CBMDF deverão ser encaminhadas ao CEINT para fins de controle e arquivamento.

§3º Após a criação de outros postos de controle, todos os documentos classificados produzidos pelas unidades do CBMDF deverão ser encaminhados ao posto de controle a que estiverem subordinadas.

§4º Após a criação de outros postos de controle, sendo verificado que existem documentos classificados no posto de controle primário de competência de tramitação e armazenamento de um novo posto, serão tais documentos remetidos por meio de um Termo de Transferência de Guarda de documentos ou materiais controlados.

Art. 16. O chefe do posto de controle localizado no CEINT será o Comandante do Centro e deverá possuir credencial de segurança para acesso a informações até o grau de sigilo ultrassecreto.

Parágrafo único. Os chefes dos demais postos de controle das OBMs habilitadas pelo GSC deverão possuir credenciamento de segurança no grau de sigilo reservado.

Art. 17. O GSC é o responsável pela verificação da qualificação técnica mínima exigida dos postos de controle a serem habilitados no âmbito do CBMDF, nos termos do artigo 25 da Portaria nº 09/2016, da Casa Militar do Distrito Federal.

CAPÍTULO IV

DO CREDENCIAMENTO E DESCREDENCIAMENTO DE BOMBEIROS MILITARES

Art. 18. Os militares do CBMDF que tratem de informação classificada em grau de sigilo serão indicados pelas autoridades previstas no artigo 4º da presente Portaria, e deverão solicitar o respectivo credenciamento ao GSC, por meio do encaminhamento do Termo de Compromisso e Manutenção do Sigilo – TCMS, conforme modelo constante no Anexo I da presente Portaria.

§1º A homologação do credenciamento de segurança dos militares deverá ser publicada no Boletim de Acesso Restrito.

§2º A credencial de segurança será concedida para o bombeiro militar considerando-se o cargo e a função que ele irá exercer, bem como a necessidade de conhecer.

§3º O acesso à informação, classificada em qualquer grau de sigilo, por militar não credenciado poderá, excepcionalmente, ser permitido mediante assinatura do TCMS, pelo qual o militar se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

Art. 19. A credencial de segurança estará sempre associada à informação classificada que o militar poderá acessar, em razão da necessidade de conhecer, e terá validade máxima de 2 (dois) anos.

§1º Após o término da validade da credencial de segurança, o bombeiro militar deverá passar por um novo processo de credenciamento.

§2º Em casos específicos a credencial de segurança poderá ser expedida por prazo de validade inferior a 2 (dois) anos.

Art. 20. O Comandante-Geral, o GSC e o seu suplente, e o Comandante do CEINT possuem credencial de segurança de acesso a informações emitida *ex offício* até o grau de sigilo ultrassecreto.

Parágrafo único. As autoridades listadas no inciso II do art. 4 possuem credencial de segurança emitida *ex officio* para o grau de sigilo reservado, não necessitando passar pelo processo de credenciamento de segurança.

Art. 21. O descredenciamento de segurança de bombeiro militar poderá ocorrer em virtude de um dos seguintes motivos:

I- término da validade da credencial de segurança;

II - falecimento;

III - cessar a necessidade de conhecer;

IV - exoneração da função;

V - passagem para a reserva ou inatividade;

VI - licenciamento;

VII - comprometimento da segurança; ou

VIII - a critério do GSC.

CAPÍTULO V

DOS PROCEDIMENTOS PARA A CLASSIFICAÇÃO DE INFORMAÇÃO

Art. 22. A classificação da informação em qualquer grau de sigilo deverá ser formalizada com o preenchimento do Termo de Classificação de Informação – TCI, conforme modelo constante no Anexo II da presente Portaria.

§1º A informação somente será considerada classificada após a assinatura do respectivo TCI.

§2º A competência para assinatura do TCI é das autoridades previstas no artigo 4º da presente Portaria.

§3º O TCI deve acompanhar a informação classificada, como primeira folha da documentação.

§4º A autoridade classificadora deverá emitir 3 (três) cópias do TCI, com as razões de classificação suprimidas ou tarjadas, devendo:

I- Anexar a primeira cópia à informação a qual se refira;

II- Encaminhar a segunda cópia ao posto de controle no prazo máximo de 30 (trinta) dias da data de classificação;

III- Arquivar a terceira cópia na unidade.

§5º Ao final da tramitação da informação classificada, esta deverá ser encaminhada ao posto de controle para fins de arquivamento.

Art. 23. O TCI receberá o Código de Indexação de Documento que contém Informação Classificada (CIDIC), conforme Anexo II da presente Portaria.

Art 24. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada, e será estruturado em duas partes:

I- A primeira parte do CIDIC será composta pelo Número Único de Protocolo (NUP), que deve ser gerado por meio da abertura de processo no Sistema Eletrônico de Informação - SEI, designado como ‘Gestão da Informação: Informações Classificadas’, observados os seguintes aspectos:

a) O NUP é o número do processo gerado pelo SEI-GDF;

b) A autoridade classificadora ou militar por ela credenciado deve encaminhar o processo SEI para a unidade CBMDF/CEINT/SECOI com a cópia do TCI, digitalizada em formato PDF;

c) O processo SEI não deve conter nenhuma informação classificada em grau de sigilo até que a informação seja desclassificada;

d) A informação classificada em grau de sigilo, quando desclassificada, deverá ser inserida no processo SEI que originou o NUP e remetida ao posto de controle.

II- A segunda parte do CIDIC será composta dos seguintes elementos:

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

b) categorias: indicação, com dois dígitos, da categoria relativa ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), em cumprimento ao Anexo Único do Decreto nº 35.382/2014;

c) data de produção da informação classificada: registro da data de produção da informação classificada no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

d) data de desclassificação da informação classificada: registro da potencial data de desclassificação da informação classificada, efetuado no ato da classificação, no formato 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:

1) reclassificação da informação resultante de reavaliação; ou

2) primeiro registro da classificação.

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

§2º Para fins de gestão documental, deverá ser guardado o histórico das alterações do CIDIC.

CAPÍTULO VI

DA TRAMITAÇÃO

Art. 25. O documento classificado poderá ser encaminhado eletrônica ou fisicamente, nos termos do artigo 33 do Decreto 35.382/2014, obedecidas as seguintes prescrições:

§1º A transmissão de informação classificada poderá ser realizada por meio eletrônico, desde que obrigatoriamente criptografado, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, dentro da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

§2º A transmissão de informação classificada poderá ser realizada por meio físico, sendo permitida a remessa pessoal, por intermédio dos correios ou por malote, observadas as seguintes prescrições:

I - o documento a ser expedido deverá ser acondicionado em envelope duplo (ambos lacrados);

II - o envelope externo deverá conter apenas a função do destinatário e seu endereço, sem qualquer anotação que indique o grau de sigilo ou o motivo da restrição de acesso ao seu conteúdo;

III - no envelope interno deverá ser inscrito o nome e a função do destinatário, o seu endereço e, claramente indicado, o grau de sigilo ou o motivo da restrição de acesso ao conteúdo do documento, de modo a ser visto logo que removido o envelope externo;

IV - no envio pelos correios, o envelope deverá ser enviado por meio de carta registrada com aviso de recebimento;

V - no envio por remessa pessoal, por malote, o envelope interno deverá ser lacrado e o documento classificado far-se-á acompanhado de um recibo;

VI - o recibo destinado ao controle da expedição/recepção e da custódia do documento classificado deverá conter, necessariamente, indicação sobre o remetente, o destinatário e o número ou outro indicativo que identifique o documento;

VII - quando, inicialmente, for necessário que somente o destinatário tome conhecimento do assunto tratado, o envelope interno deverá conter, além do nome do destinatário, a inscrição "PESSOAL", precedendo a indicação da restrição ou classificação, quando houver.

Art. 26. A autoridade que receber a informação classificada deverá manter um registro onde ficarão anotados todos os dados identificadores da unidade onde tramitou ou foi distribuído o documento classificado e do militar que teve contato com a documentação e o responsável pela custódia.

Art. 27. Ao responsável pelo recebimento de documento classificado incumbe:

I - verificar e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao destinatário, o qual informará ao remetente; e

II - proceder ao registro do documento e ao controle de sua tramitação, conforme previsto no art. 26 desta Portaria.

Art. 28. Recebido o documento impresso classificado, o recibo anexado a ele deverá ser assinado e datado pelo destinatário e devolvido ao remetente.

Parágrafo único. A remessa do recibo não deve ser feita com características de sigilo.

Art. 29. A cópia ou o extrato de documento classificado deverá receber um código numérico ou alfanumérico específico para cada destinatário, a fim de identificar a origem de um possível vazamento e facilitar o seu controle.

§1º O código citado no caput deverá ser colocado no corpo do texto, em cada página de todo o documento, sendo visível e de fácil identificação em qualquer reprodução gráfica realizada.

§2º No documento original deverá constar a relação de todos os destinatários com os seus respectivos códigos.

Art. 30. O responsável pela cópia de documento classificado deverá destruir a cópia inservível ou qualquer outro elemento que possa dar origem à cópia não autorizada do todo ou de parte do documento original.

Art. 31. Sempre que a cópia de documento classificado for efetuada em copiadora ou em impressora, instalada em local diferente daquele onde foi produzido o documento original, deverá, esta operação, ser acompanhada do militar responsável pelo documento para, durante esta fase, garantir a manutenção do sigilo.

Art. 32. À cópia ou ao extrato de documento classificado será atribuída a classificação ou a situação de restrição de acesso igual àquela atribuída ao documento que lhe deu origem.

Art. 33. Essa Portaria entra em vigor na data de sua publicação.

ANEXO I

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO – TCMS

Eu, _____, matrícula nº _____, identidade nº _____, emitida em __/__/____, pelo(a) _____, CPF nº _____, filho de _____, residente e domiciliado no(a) _____, perante _____, declaro ter ciência da legislação sobre o tratamento de informação classificada, cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, nos termos da Lei Distrital nº 4.990, de 12 de dezembro de 2012, e do Decreto Distrital nº 35.382, de 29 de abril de 2014, e me COMPROMETO, no desempenho de minhas funções junto à _____ (local de trabalho), a:

a) guardar o sigilo sobre todos os assuntos e atividades dos quais tenha conhecimento ou tido acesso;

b) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos por qualquer Órgão do Poder Executivo do Distrito Federal e preservar o seu sigilo, de acordo com a legislação vigente;

c) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

d) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

e) não copiar ou reproduzir, por qualquer meio ou modo, informações classificadas em qualquer grau de sigilo e/ou informações relativas aos materiais de acesso restrito que venha a ter acesso, salvo por autorização da autoridade competente.

Declaro, ainda, estar ciente da aplicação da Legislação Especial e Comum, sem prejuízo de outras sanções de natureza disciplinar que possam advir pelo não cumprimento do presente termo. E por estar de acordo, assino-o na presença da autoridade abaixo identificada.

_____, ____ de _____ de _____.

(Local) (Data)

_____

(Assinatura do declarante)

_____

(Assinatura da autoridade solicitante previstas no artigo 4º da presente Portaria)

ANEXO II

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

(GRAU DE SIGILO)

<table>
<tr><th colspan="2">TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO</th></tr>
<tr><td colspan="2">ÓRGÃO/ENTIDADE: (1)</td></tr>
<tr><td colspan="2">CÓDIGO DE INDEXAÇÃO: (2)</td></tr>
<tr><td colspan="2">GRAU DE SIGILO: (3)</td></tr>
<tr><td colspan="2">CATEGORIA: (4)</td></tr>
<tr><td colspan="2">TIPO DE DOCUMENTO: (5)</td></tr>
<tr><td colspan="2">DATA DE PRODUÇÃO: (6)</td></tr>
<tr><td colspan="2">FUNDAMENTAÇÃO LEGAL PARA CLASSIFICAÇÃO: (7)</td></tr>
<tr><td colspan="2">RAZÕES PARA CLASSIFICAÇÃO:</td></tr>
<tr><td colspan="2">PRAZO DE RESTRIÇÃO DE ACESSO: _____ anos. Até ____/____/_____.</td></tr>
<tr><td colspan="2">DATA DE CLASSIFICAÇÃO: (8)</td></tr>
<tr><td rowspan="2">AUTORIDADE CLASSIFICADORA</td><td>Nome:</td></tr>
<tr><td>Cargo:</td></tr>
<tr><td rowspan="2">AUTORIDADE RATIFICADORA
(quando aplicável)</td><td>Nome:</td></tr>
<tr><td>Cargo:</td></tr>
<tr><td rowspan="2">DESCLASSIFICAÇÃO EM: _____/_____/_____
(quando aplicável)</td><td>Nome</td></tr>
<tr><td>Cargo:</td></tr>
<tr><td rowspan="2">RECLASSIFICAÇÃO EM: _____/_____/_____
(quando aplicável)</td><td>Nome:</td></tr>
<tr><td>Cargo:</td></tr>
<tr><td>REDUÇÃO DE PRAZO EM: _____/_____/_____</td><td>Nome:</td></tr>
</table>

(quando aplicável)	Cargo:
PRORROGAÇÃO DE PRAZO EM: _____/_____/_____ (quando aplicável)	Nome Cargo:
Assinatura da Autoridade Classificadora: _____	
_____ ASSINATURA DA AUTORIDADE RATIFICADORA _____ ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO _____ ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO _____ ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO _____ ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO	

Legenda:

(1) OBM que produziu

(2) CIDIC - Exemplo: 00053-00000001/2020-00.R.05.01/01/2020.01/01/2025.N

(3) Reservado, Secreto ou Ultrassecreto.

(4) No campo “categoria” deve ser registrado o número 05, que equivale à categoria “Defesa e Segurança”.

(5) Ofício, memorando, relatório, etc.

(6) Data da assinatura do documento

(7) Uma das hipóteses do artigo 25 da Lei nº 4.990/2012.

(8) Data de assinatura do TCI