
Segurança orgânica no CBMDF: aprimoramento da cultura de contrainteligência na corporação

Organic security in CBMDF: improving the corporate counterintelligence culture

David Dias Durães¹

Pérsio Moreira de Ataíde Ramos²

RESUMO

A Segurança Orgânica é um segmento da contrainteligência voltado para a proteção institucional, prevenindo ameaças de diversas naturezas. Esse segmento desempenha um papel essencial na preservação da elevada credibilidade social dos Corpos de Bombeiros Militares (CBMs). Este artigo tem como objetivo examinar os aspectos relacionados à Segurança Orgânica nas unidades operacionais do Corpo de Bombeiros Militar do Distrito Federal (CBMDF), fornecendo subsídios para o aprimoramento dessas medidas. Para isso, realizou-se pesquisa bibliográfica em legislações e literatura, análise documental dos Planos de Segurança Orgânica (PSOs) da corporação e aplicação de questionários aos comandantes das unidades, integrando os dados obtidos. A análise documental identificou 23 vulnerabilidades de segurança orgânica, classificadas conforme o tipo de ativo e suas respectivas ameaças. Além disso, as respostas dos gestores das unidades operacionais reforçaram a importância desse segmento, mas também evidenciaram falhas que se correlacionam com aquelas identificadas nos PSOs. Consta-se que a corporação possui um esboço do Planejamento de Desenvolvimento de Contrainteligência (PDCI), voltado ao desenvolvimento de uma mentalidade de contrainteligência entre os militares. O aprimoramento desse planejamento pode ser alcançado com a implementação das sugestões apresentadas ao longo deste estudo, fortalecendo a segurança orgânica da instituição.

Palavras-chave: ameaças adversas; cultura de contrainteligência; proteção institucional; segurança orgânica.

ABSTRACT

Organic Security is a segment of counterintelligence focused on institutional protection, preventing threats of various kinds. This segment plays an essential role in preserving the high social credibility of the Military Fire Departments (CBMs). This article examines aspects related to Organic Security in the operational units of the Military Fire Department of the Federal District (CBMDF), providing support for improving these measures. To this end, we conducted bibliographic research on legislation and literature, documented the corporation's Organic Security Plans (OSPs), and administered questionnaires to unit commanders, integrating the data obtained. The document analysis identified 23 organic security vulnerabilities, classified according to the type of asset and their respective threats. Furthermore, the responses from operational unit managers reinforced the importance of this segment but also highlighted flaws that correlate with those identified in the OSPs. The corporation has a draft Counterintelligence Development Plan (CDDP) designed to foster a counterintelligence mindset among military personnel. This plan can be improved by implementing the suggestions presented throughout this study, strengthening the institution's organizational security.

Keywords: adversary threats; counterintelligence culture; institutional protection; organic security.

¹ <http://lattes.cnpq.br/1922261225170620>

² <http://lattes.cnpq.br/9794593346365797>

1 Introdução

A Lei nº 9.883, de 1999, define que a Atividade de Inteligência abrange dois campos principais: a inteligência propriamente dita e a contrainteligência (Brasil, 1999). Esta última consiste, de forma resumida, em ações destinadas a neutralizar atividades de inteligência adversária, ou seja, estratégias voltadas à proteção da instituição e à preservação de seu conhecimento.

Dentro da contrainteligência, destaca-se a segurança orgânica, a qual, conforme descrito no Manual de Contrainteligência do Exército Brasileiro (2019, p. 23), refere-se a "um segmento da contrainteligência que orienta a adoção de medidas para prevenir e impedir ameaças de qualquer natureza dirigidas a pessoas, informações, materiais, instalações e estruturas físicas".

Ainda de acordo com o referido manual, esse segmento exige uma postura preventiva de todos os integrantes da organização, sendo essencial "o planejamento, a implementação e a manutenção de uma mentalidade voltada à contrainteligência em todos os níveis hierárquicos, a fim de garantir um grau adequado de proteção" (Exército Brasileiro, 2019, p. 23).

Nessa perspectiva, Ribeiro (2018) ressalta que o fortalecimento da cultura de segurança orgânica é indispensável, sobretudo em áreas mais sensíveis, como a segurança de pessoal e a proteção de informações. Esse compromisso não se limita aos profissionais que atuam diretamente na inteligência, mas deve ser compartilhado por todos os membros, assegurando a integridade e a credibilidade da corporação.

Diante desse contexto, este artigo analisa os aspectos relacionados à Segurança Orgânica nas unidades operacionais do Corpo de Bombeiros Militar do Distrito Federal (CBMDF). A relevância deste estudo reside na necessidade de fortalecer a cultura desse segmento dentro da corporação.

2 Fundamentos da Atividade de Inteligência

A atividade de inteligência, conforme estabelecido na legislação, tem como propósito coletar, analisar e disseminar informações relevantes para o processo decisório, além de contribuir para a segurança e proteção da sociedade (Brasil, 1999).

Essa atividade se desdobra em dois principais eixos: inteligência e contrainteligência. Enquanto a inteligência se concentra na produção de conhecimento para subsidiar decisões estratégicas, a contrainteligência tem o objetivo de "prevenir, identificar, obstruir e neutralizar ações adversas que possam comprometer a segurança de dados, informações e conhecimentos essenciais para a proteção do Estado e da sociedade" (Brasil, 2002, p. 1).

Dessa forma, percebe-se que, embora o sigilo seja um dos pilares da atividade de inteligência, a contrainteligência destaca a importância dessas medidas de segurança, que devem ser amplamente difundidas dentro da instituição para garantir a proteção e a integridade organizacional.

2.1 Ramos da Atividade de Inteligência

A atividade de inteligência, conforme a legislação vigente, é dividida em dois ramos distintos, porém interdependentes: a inteligência propriamente dita e a contrainteligência (Brasil, 1999).

No contexto da segurança pública, enquanto a inteligência se dedica à produção de conhecimento estratégico para subsidiar decisões, a contrainteligência tem o propósito de gerar informações que neutralizem ameaças e protejam tanto a atividade quanto a instituição à qual pertence (Brasil, 2021).

Dessa forma, é importante destacar que, apesar de possuírem funções diferentes, esses dois ramos são complementares. Almeida Neto (2009, p. 57) reforça essa relação ao afirmar que "para cumprir satisfatoriamente sua finalidade, a contrainteligência precisa constantemente produzir conhecimento não apenas sobre a inteligência adversa, mas também acerca das próprias vulnerabilidades da organização".

A Doutrina Nacional de Inteligência de Segurança Pública (DNISP) classifica a contrainteligência em três segmentos: segurança ativa, segurança orgânica e segurança de assuntos internos (MJSP, 2016). Segundo Pereira (2009), a segurança ativa refere-se a medidas ofensivas voltadas à identificação e neutralização de ameaças, enquanto a segurança orgânica engloba estratégias defensivas que garantem o funcionamento institucional e evitam ações adversas.

Já a segurança de assuntos internos, conforme definido na DNISP, é um conjunto de ações voltadas à produção de informações que auxiliam processos de correção dentro das instituições públicas. Por essa razão, embora alguns autores a classifiquem como parte do segmento orgânico, a doutrina oficial a trata como uma categoria própria (MJSP, 2016).

A Segurança Orgânica (SEGOR), regulamentada por legislação específica, consiste em um conjunto planejado de medidas para proteger os ativos institucionais, sejam eles tangíveis (como instalações, materiais e documentos) ou intangíveis (como informações e comunicações). Essa proteção se estende a diversas áreas, incluindo pessoal, operações de Inteligência de Segurança Pública (ISP), telemática e informática (Brasil, 2009).

Conforme Ribeiro (2018, p. 9), a SEGOR enfatiza a necessidade de proteger todos os ativos institucionais que possam ser alvo de ameaças, diferenciando entre aqueles de natureza concreta e os de caráter abstrato. Para garantir essa proteção, torna-se essencial realizar avaliações de risco, permitindo um equilíbrio entre as medidas adotadas e as reais necessidades institucionais, evitando tanto excessos quanto deficiências em sua aplicação (Pereira, 2009).

O Manual de Contrainteligência do Exército Brasileiro ressalta que, para alcançar um nível adequado de segurança, é fundamental a implementação de medidas voltadas para quatro áreas principais: Segurança dos Recursos Humanos, Segurança do Material, Segurança das Áreas e Instalações, e Segurança da Informação (Exército Brasileiro, 2019).

Diante desse contexto, a Segurança Orgânica, foco deste estudo, compreende um conjunto de normas e práticas destinadas a prevenir, detectar, conter e neutralizar ameaças que possam comprometer a integridade da organização (Brasil, 2009).

2.2 Atividade de Inteligência no CBMDF

No Corpo de Bombeiros Militar do Distrito Federal (CBMDF), a Atividade de Inteligência é conduzida pelo Centro de Inteligência (CEINT), órgão criado pelo Decreto Distrital nº 31.817/2010 e subordinado diretamente ao Comandante-Geral. O CEINT é responsável pelo planejamento, coordenação, supervisão e orientação das operações de inteligência, além de executar atividades voltadas à coleta e análise de dados para gerar informações estratégicas que auxiliem na tomada de decisões do Comando-Geral (Distrito Federal, 2010). De acordo com Santos (2015), suas funções abrangem os níveis operacional, tático e estratégico dentro da instituição.

No âmbito da contrainteligência, cabe ao CEINT contribuir para o planejamento da SEGUR da corporação, bem como levantar dados operacionais sobre riscos à vida e ao patrimônio, permitindo a adoção de medidas preventivas em conformidade com o artigo 6º do Decreto Distrital nº 31.817/10 (Distrito Federal, 2010).

Essas atribuições são sustentadas pelos Núcleos de Segurança Orgânica (NUSOR), formados por militares credenciados lotados nos órgãos de direção geral, setorial e de execução. Esses núcleos operam por meio de um canal técnico, possibilitando a interlocução e o compartilhamento de informações, conforme definido na Portaria nº 20, de 2022, que instituiu o Sistema de Inteligência Bombeiro Militar (SIBOM) (CBMDF, 2022).

Entretanto, a segurança orgânica não deve ser uma preocupação exclusiva das agências de inteligência, mas sim uma cultura disseminada por toda a corporação. Falhas nesse setor podem comprometer não apenas a integridade operacional, mas também a reputação institucional do CBMDF.

O Regimento Interno da corporação atribui à Seção de Contrainteligência (SECOI), vinculada ao CEINT, a responsabilidade de orientar os bombeiros militares quanto à implementação de medidas de contrainteligência. Essa atuação visa fortalecer a mentalidade da proteção institucional (CBMDF, 2020, p. 113).

No contexto operacional, o CBMDF dispõe de equipamentos portáteis de alto custo, como geradores elétricos, câmeras térmicas e desencarceradores, além de viaturas de alto valor, armamento institucional e armamento pessoal. Qualquer vulnerabilidade nas medidas de segurança pode resultar em impactos significativos para a corporação.

Dessa maneira, medidas preventivas são essenciais para mitigar possíveis prejuízos às instituições militares e ao Estado, tornando imprescindível a consolidação de uma cultura de segurança orgânica nos grupamentos do CBMDF. A adoção dessas práticas busca "garantir o funcionamento da instituição, prevenindo e impedindo ações adversas de qualquer natureza, por meio de um conjunto de medidas essencialmente defensivas" (Brasil, 2009, p. 1).

Por fim, é fundamental reconhecer a relevância do CBMDF para a sociedade, sua estrutura organizacional e os aspectos inerentes às suas atividades. Como destaca Ribeiro (2018), essa conscientização deve ser promovida em toda a corporação, incentivando servidores e órgãos internos a desenvolver e consolidar práticas eficazes dessas medidas de segurança em suas respectivas áreas de atuação.

3 Metodologia

Este estudo possui caráter aplicado e adota uma abordagem exploratória, descritiva e qualitativa dedutiva. Inicialmente, é realizada uma revisão bibliográfica, seguida da análise documental e da aplicação de um questionário como instrumento de coleta de dados. O objetivo é obter informações sobre os aspectos relacionados à segurança orgânica nas unidades operacionais da corporação.

A pesquisa documental, utilizada como base para a coleta de dados, foi realizada a partir de informações fornecidas pela Seção de Contrainteligência do Centro de Inteligência do CBMDF. Essa etapa focou na identificação de vulnerabilidades e ameaças à proteção institucional da corporação, utilizando como referência os Planos de Segurança Orgânica das Organizações Bombeiro-Militar (OBMs) operacionais.

Já o questionário foi direcionado aos comandantes dessas unidades, abordando diferentes aspectos desse segmento na corporação.

Por fim, buscou-se estabelecer uma relação entre as ameaças identificadas nas respostas dos questionários e os dados levantados na pesquisa documental. Essa correlação serviu como base para a proposição de um modelo voltado ao aprimoramento da cultura de segurança orgânica dentro da instituição.

4 Resultados e Discussão

Os dados desta pesquisa foram coletados e organizados conforme os métodos previamente descritos. No entanto, é relevante destacar que as vulnerabilidades identificadas em cada unidade operacional não serão apresentadas de forma individualizada. Isso se justifica pelo caráter sigiloso das informações abordadas neste artigo científico, cuja divulgação detalhada poderia comprometer a segurança dessas OBM.

Parte desses dados integra os PSOs das unidades, documentos restritos ao Centro de Inteligência e ao Comandante da Unidade, enquanto outros foram obtidos por meio dos questionários respondidos pelos gestores das respectivas OBM.

Dessa forma, os resultados serão expostos de maneira consolidada, permitindo uma visão abrangente das principais fragilidades e ameaças identificadas, que são comuns às unidades operacionais da corporação.

4.1 Análise das falhas de segurança orgânica e ameaças identificadas nos Planos de Segurança Orgânica

Para análise, a seção responsável disponibilizou um total de 22 (vinte e dois) PSOs, tanto em formato físico quanto digital, conforme informações fornecidas pelo CEINT. Entre eles, 6 (seis) eram referentes às unidades operacionais subordinadas ao Comando Operacional, que constituem o foco desta pesquisa. Esses documentos foram utilizados para identificar, de forma geral e sem menção específica às unidades, os principais pontos de vulnerabilidade das OBM.

Após a transcrição das fragilidades observadas no segmento em estudo, essas foram organizadas e categorizadas no Quadro 1, de acordo com os grupos de ativos aos quais estavam relacionadas. Além disso, foram identificadas as principais ameaças associadas a essas falhas, uma vez que representam riscos à proteção dos recursos institucionais.

Quadro 1 - Falhas identificadas nos PSOs as OBM's operacionais e ameaças inerentes

SEGURANÇA DOS RECURSOS HUMANOS		
Falha Identificada		Ameaça
1	Falta de treinamento para os militares da unidade acerca das rotinas de segurança	Comprometimento, de forma geral, da segurança da unidade, uma vez que a falta de capacitação em Segurança Orgânica aumenta os riscos inerentes a todos os grupos de ativo desse segmento, devido ao desconhecimento de seus preceitos básicos
2	Não ocorrem programas permanentes de conscientização	
3	Os militares e civis (terceirizados) recém-chegados não são submetidos a um processo educacional de segurança	
4	Insuficiência de efetivo para realizar ronda no local durante 24 horas	Ingresso e permanência de pessoas não autorizadas na unidade, uma vez que o serviço de ronda visa realizar o monitoramento contínuo das áreas e instalações da unidade, de modo que o efetivo precisa ser suficiente para que seja capaz de inibir as ameaças adversas
5	Não há um acompanhamento e o controle de prestadores de serviço no interior da unidade	Extravio de materiais e documentos e vazamento de dados restritos, visto que, pessoas estranhas à missão fim, são potenciais riscos à segurança da unidade
6	Quando os militares são movimentados da unidade militar, não ocorre de imediato o cancelamento dos perfis de acesso aos sistemas informatizados da unidade	Comprometimento da segurança da unidade, na medida em que os servidores movimentados se tornam estranhos àquelas unidades

SEGURANÇA DO MATERIAL		
Falha Identificada		Ameaça
7	As áreas sensíveis não possuem mecanismos de trancamento adicionais	Ingresso de pessoas não autorizadas, devido à ausência de mecanismos adicionais de barreira
8	Ausência de manutenção de 1º escalão nos armamentos	Acidente com arma de fogo, uma vez que a manutenção de 1º escalão, repassada nos cursos de formação de carreira, é requisito essencial para o perfeito funcionamento

SEGURANÇA DO MATERIAL		
Falha Identificada		Ameaça
9	Exposição de pertences pessoais nas gavetas sem tranca	Extravio de materiais e documentos, devido à ausência de barreiras de proteção
10	O claviculário não está localizado em área segura e seu acesso não é controlado por registro de retirada e entrega de chaves	Ingresso de pessoas não autorizadas a áreas sensíveis e acesso a chaves de viaturas e veículos

SEGURANÇA DAS ÁREAS E INSTALAÇÕES		
Falha Identificada		Ameaça
11	Ausência de Sentinela (Guarda)	Ingresso e permanência de pessoas não autorizadas na unidade
12	Fragilidade no acesso principal	
13	Janelas sem grades	
14	As barreiras não são capazes de detectar, dissuadir e retardar a ação adversa	
15	Não há um rígido controle de acesso nas entradas e saídas para pessoas e veículos	
16	Falta de identificação de "Área Militar" no perímetro	Aproximação ou dissimulação de pessoas estranhas à unidade, contribuindo para ameaça às instalações
17	Não há sistema de iluminação adicional para emergências	
18	Existência de vegetação que prejudica a visualização de possíveis invasores	
19	Iluminação externa precária	

SEGURANÇA DA INFORMAÇÃO		
Falha Identificada		Ameaça
20	Não existem regras para ingresso e uso de equipamentos de informática e periféricos particulares	Utilização dos equipamentos por pessoas não autorizadas, de modo a encontrar vulnerabilidades nos sistemas internos
21	Não há rotinas de backup	Perda de documentos e informações

SEGURANÇA DA INFORMAÇÃO		
Falha Identificada		Ameaça
22	Os rascunhos, computadores, pen drives e outros recursos auxiliares utilizados na produção dos documentos não são submetidos a controles de segurança	Acesso a documentos restritos por pessoas não autorizadas
23	Não há um sistema de alimentação de energia alternativo	Interrupção ou falhas do serviço de comunicação e informação da unidade, em caso de falta de energia da distribuidora

Fonte: O autor.

A análise dos PSOs possibilitou a identificação de 23 (vinte e três) vulnerabilidades relacionadas à segurança orgânica nas unidades operacionais da corporação, abrangendo tanto aspectos internos quanto externos das OBMs.

No contexto da SEGUR, o Manual de Contraineligência do Exército Brasileiro define ameaça como a interação entre três fatores: o agente (interno ou externo), sua motivação (isto é, a necessidade ou interesse que impulsiona suas ações) e sua capacidade de atuação (o potencial para concretizar determinada ação) (Exército Brasileiro, 2019).

Com base no Quadro 1, observa-se uma correspondência entre as falhas identificadas na segurança orgânica das unidades operacionais e suas principais deficiências. Nesse sentido, caso essas vulnerabilidades sejam exploradas por ameaças, a instituição pode ser exposta a riscos significativos, conforme aponta Castro (2022), podendo resultar em incidentes de segurança e impactos negativos para a organização.

Para mitigar essas ameaças, é essencial a implementação de medidas preventivas que sigam um ciclo estruturado de planejamento, execução, controle e retroalimentação (Exército Brasileiro, 2019). Nesse contexto, o Plano de Segurança Orgânica (PSO) surge como um dos principais instrumentos normativos para a proteção dos ativos institucionais e a prevenção de ações

adversas, sendo a base da análise realizada nesta pesquisa.

O PSO deve estabelecer diretrizes claras, incluindo a definição de responsabilidades, a identificação dos recursos disponíveis, a implementação de salvaguardas e a previsão de procedimentos para lidar com eventuais violações. Assim, a partir da identificação das deficiências, é fundamental a adoção de medidas corretivas destinadas à proteção dos ativos institucionais (Gonçalves, 2009).

Com base nos resultados analisados, verifica-se a necessidade de implementar medidas específicas para cada segmento da SEGUR, visando garantir a efetividade da prevenção e obstrução de ameaças.

No âmbito da Segurança das Áreas e Instalações, grupo de medidas onde foi constatado o maior número de falhas, algumas das principais medidas recomendadas pelo Manual de Contraineligência do Exército Brasileiro (2019) incluem a delimitação de áreas, a instalação de barreiras, a implementação de linhas de proteção, o controle de acesso, a detecção de intrusões, o monitoramento por alarmes e o emprego de equipamentos de segurança.

Já no grupo de medidas da Segurança dos Recursos Humanos, que também apresentou vulnerabilidades significativas, destaca-se a importância da ação de comando em todos os níveis, reforçando valores éticos e morais nos membros da instituição. Além disso, o desenvolvimento de uma mentalidade de Contraineligência em toda a estrutura organizacional é essencial para assegurar a proteção dos ativos institucionais (Exército Brasileiro, 2019).

A DNISP também ressalta a importância do Processo de Recrutamento Administrativo (PRA), cujo objetivo é selecionar, monitorar e, quando necessário, desligar profissionais do quadro institucional (MJSP, 2016). No CBMDF, essa diretriz é aplicada por meio da Sindicância de Vida Progressiva e Investigação Social e Funcional, obrigatória tanto no concurso público para ingresso na corporação quanto no processo seletivo do Curso de Especialização em Inteligência. Essas medidas visam garantir a idoneidade moral dos candidatos, conforme previsto no art. 11 do Estatuto dos Bombeiros Militares do CBMDF (Brasil, 1986).

Em relação à Segurança da Informação, conforme estabelecido pela DNISP, o foco está na proteção dos meios de comunicação e no resguardo de dados e conhecimentos, prevenindo interceptações e análises indevidas de informações transmitidas por texto, imagem ou som (MJSP, 2016). As principais medidas incluem segurança na transmissão (proteção física dos sistemas contra interceptação), segurança do conteúdo (dificultar o entendimento da informação por meio de criptografia) e segurança da informática (garantia da integridade e continuidade dos sistemas e controle de acessos).

Por fim, no que se refere à Segurança do Material, o Manual de Contraineligência do Exército Brasileiro recomenda a adoção de práticas que garantam a adequada conservação e armazenamento dos materiais em locais apropriados. A análise dos PSOs das unidades operacionais aponta para a necessidade de conscientização

dos integrantes da instituição, treinamentos específicos sobre o uso correto dos equipamentos, além de atenção especial à qualidade das soluções adotadas para garantir a proteção física dos materiais disponíveis (Exército Brasileiro, 2019).

4.2 Análise da Segurança Orgânica na percepção dos comandantes das OBMs operacionais

Para complementar a análise realizada por meio dos PSOs, foi aplicado um questionário em formato de formulário, direcionado aos comandantes das unidades operacionais da corporação, especificamente os Grupamentos Multiemprego e Grupamentos Especializados, que estão subordinados ao Comando Operacional e desempenham a missão principal da instituição. No total, participaram 31 (trinta e um) gestores.

Dentre os formulários recebidos, a grande maioria (96,8%) foi preenchida pelo próprio Comandante da Unidade ou pelo Subcomandante, reforçando a adequação do público-alvo escolhido, uma vez que esses gestores possuem conhecimento aprofundado da realidade de suas unidades. Entretanto, 87% desses militares não possuíam capacitação em Atividade de Inteligência.

A Atividade de Inteligência Bombeiro Militar tem como uma de suas principais funções assessorar o comando na tomada de decisões, utilizando técnicas especializadas (Prates, 2013). Além disso, conforme descrito na DNISP, a Inteligência de Segurança Pública (ISP) é um recurso essencial para subsidiar o processo decisório nos níveis político, estratégico, tático e operacional (MJSP, 2016).

Diante desse cenário, verifica-se a necessidade de fortalecer o conhecimento dos gestores sobre o tema, especialmente no âmbito da Contrainteligência, pois são esses profissionais que possuem a responsabilidade direta pela proteção dos ativos de suas unidades. Para isso, cursos e capacitações são fundamentais. Como destaca Prates (2013), a informação tem um papel estruturante dentro das organizações e serve como instrumento de gestão, exigindo uma compreensão precisa do valor e dos sistemas de informação.

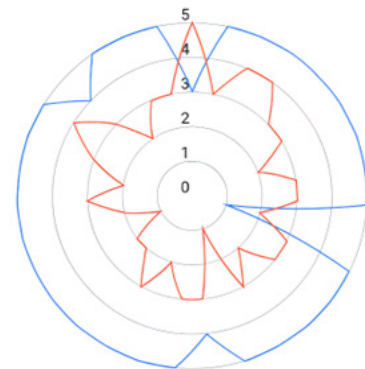
Apesar de apenas 13% dos comandantes entrevistados possuírem formação específica na área de inteligência, vale ressaltar que os oficiais combatentes do CBMDF cursam a disciplina de Atividade de Inteligência durante o Curso de Formação de Oficiais (CFO), conforme o Plano de Curso vigente a partir de 2012 e suas atualizações. Essa disciplina inclui uma unidade voltada à Contrainteligência, com o objetivo de fomentar a cultura de Segurança Orgânica e sua aplicação na rotina profissional (CBMDF, 2017).

Santos (2015) enfatiza que a capacitação dos gestores, especialmente no campo da proteção institucional, é essencial para desenvolver competências em proteção de dados e informações sigilosas, mitigação de riscos, bem como prevenção e resposta a incidentes de segurança. Essas habilidades são indispensáveis para assegurar a integridade institucional, considerando que as ameaças adversas são dinâmicas e estão em constante evolução.

Outro aspecto relevante identificado a partir dos questionários refere-se à percepção dos comandantes sobre a segurança orgânica na corporação. O Gráfico 1 ilustra a discrepância entre a importância atribuída a esse segmento e a avaliação sobre seu nível atual na instituição. Nessa representação visual, valores mais elevados (localizados nos círculos mais externos do gráfico radial) indicam tanto uma maior relevância do tema quanto uma melhor percepção de sua aplicação prática na corporação:

Gráfico 1 - Importância e nível atual da Segurança Orgânica, no CBMDF, pela ótica dos comandantes das OBMs

— Quão importante considera a Segurança Orgânica para a corporação?
— O quão acredita que se encontra o nível da Segurança Orgânica dentro da corporação?



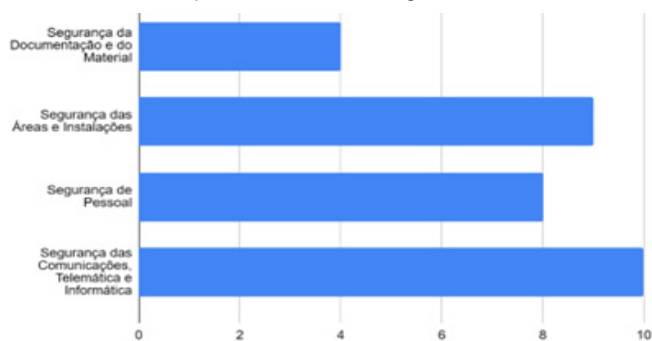
Fonte: O autor.

A segurança orgânica, conforme destacado por Almeida Neto (2009, p. 57), desempenha um papel essencial nas instituições, uma vez que busca “a prevenção das ameaças, principalmente, por meio do conhecimento das possíveis fontes de dano, além da detecção, identificação, avaliação e correção das vulnerabilidades do sistema e da organização”. No contexto das atividades dos CBMs, a importância da inteligência como suporte à preparação operacional foi ressaltada por Richardson (2010 apud Prates, 2013), que enfatiza, entre suas funções, o papel da contrainteligência na identificação de possíveis ameaças e mitigação de riscos.

No entanto, conforme ilustrado no Gráfico 1, que apresenta a percepção dos gestores sobre as avaliações insatisfatórias do nível atual da proteção institucional no CBMDF, Ribeiro (2018) ressaltava que, de maneira geral, o Brasil não possui uma cultura consolidada de segurança das instituições. Esse fator se evidencia apenas em situações adversas de grande impacto, expondo vulnerabilidades institucionais significativas e aumentando os riscos. Assim, de acordo com o autor, é essencial romper com a chamada subcultura do paliativo e implementar soluções concretas para fortalecer a segurança institucional.

Ainda no campo da proteção institucional, ao examinar o grupo de medidas considerado prioritário pelos comandantes das OBMs, verifica-se, no Gráfico 2, que a maior parte aponta a Segurança das Comunicações, Telemática e Informática (das Informações) como principal preocupação, seguida pela Segurança das Áreas e Instalações:

Gráfico 2 – Grupo de Medidas da Segurança Orgânica mais importante, na ótica dos gestores



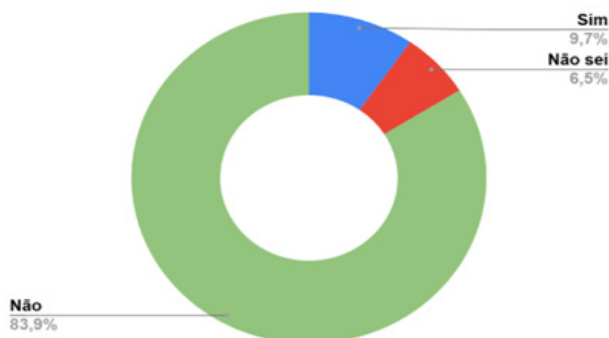
Fonte: O autor.

Em contraponto ao que foi apresentado no Gráfico 2, o Manual de Contraineligência do Exército Brasileiro destaca que os recursos humanos representam os ativos mais valiosos da instituição, devendo ser protegidos e preservados por meio da aplicação de procedimentos específicos de Segurança de Pessoal (Exército Brasileiro, 2019). No entanto, o referido manual também ressalta que as ações voltadas à proteção institucional em diferentes segmentos são interdependentes, permitindo, assim, a neutralização de possíveis ameaças.

Atualmente, a informação é amplamente reconhecida como um recurso essencial para o funcionamento eficaz de qualquer organização (Exército Brasileiro, 2019). Nesse sentido, autores como Cepik (2003) enfatizam a importância da Segurança da Informação, que se concentra na proteção dos meios que sustentam os processos informacionais, incluindo pessoas, documentos, materiais e instalações. Esse fator pode justificar a relevância atribuída pelos gestores a esse aspecto no Gráfico 2.

Dando continuidade à pesquisa, a análise do Gráfico 3, que trata da existência de um Plano de Segurança Orgânica, revela que apenas 9,7% dos gestores afirmaram que sua OBM dispõe desse documento, enquanto 6,5% declararam desconhecer sua existência:

Gráfico 3 - Existência do Plano de Segurança Orgânica na unidade



Fonte: O autor.

Conforme já mencionado, o Plano de Segurança Orgânica (PSO) é apresentado pelo Exército

Brasileiro como um dos alicerces do Planejamento de Desenvolvimento de Contraineligência, consolidando as diretrizes essenciais para a implementação da Segurança Orgânica dentro da instituição (Exército Brasileiro, 2019).

O Regimento Interno do CBMDF, em seu artigo 304, inciso XII, estabelece que cabe ao Centro de Inteligência “apoiar o planejamento da segurança orgânica dos diversos órgãos da Corporação, quando motivado”. Além disso, o artigo 306, inciso X, especifica que essa atribuição recai sobre a Seção de Contraineligência dentro da estrutura organizacional. No entanto, o regimento deixa claro que essa responsabilidade depende de uma solicitação formal, ou seja, os comandantes das unidades precisam identificar a necessidade do PSO e requisitar ao CEINT sua elaboração e posterior aplicação (CBMDF, 2020).

Na análise do questionário aplicado e considerando os dados apresentados nos Gráficos 4 e 5, constatou-se que 61,3% dos gestores relataram ter conhecimento de alguma falha na segurança orgânica da corporação. Além disso, 45,2% desses gestores afirmaram ter identificado tais falhas dentro das próprias unidades sob seu comando:

Gráficos 4 e 5 - Conhecimento dos comandantes acerca de falhas de Segurança Orgânica na corporação e em suas OBM



Fonte: O autor.

Após o relato sobre a ocorrência de falhas no segmento analisado, os comandantes foram solicitados a detalhar as situações em que esses problemas se

manifestaram. Nesse contexto, as falhas mencionadas, tanto as observadas na corporação quanto nas unidades sob a gestão dos entrevistados, apresentaram semelhanças com aquelas identificadas na análise dos PSOs.

Diante dessa convergência, o Quadro 2 apresenta as falhas reportadas pelos gestores, estabelecendo uma relação com as listadas no Quadro 1, que foram identificadas e numeradas a partir da análise dos PSOs. Além disso, o quadro também indica a qual segmento da SEGOR cada falha está associada:

Quadro 2 - Falhas de Segurança Orgânica relatadas pelos gestores e correlação com as identificadas nos PSOs³ e o segmento da Segurança Orgânica

Falha Identificada		Segmento da Segurança Orgânica
PSO ¹	Gestor	
22	Acesso e divulgação de documento restrito/sigiloso	Segurança da Informação
20	Falhas nos sistemas de comunicação	
21		
22		
23		
6	Baixa segurança do Sistema Eletrônico de Informações (SEI)	
22		
8	Manejo irregular de arma de fogo	Segurança do Material
10	Furto de viaturas	
12		
14		
15		
7	Extravio/ furto de materiais ou equipamentos	
9		
10		
13	Instalações prediais precárias	Segurança das Áreas e Instalações
11	Acesso indevido às unidades	
12		
14		
15		
11	Serviço de guarda ineficaz	Segurança dos Recursos Humanos
-	Surto psicótico de militar ²	

Fonte: O autor.

A partir da análise do Quadro 2, verifica-se que os grupos de medidas da SEGOR mais impactados, conforme a identificação de falhas pelos gestores, foram a Segurança da Informação, a Segurança do Material e a Segurança das Áreas e Instalações. Além disso, observa-se que a última falha reportada (surto psicótico de um militar) foi a única que não apresentou correspondência com aquelas identificadas nos PSOs.

Conforme já mencionado, com base na análise dos PSOs e no Manual de Contrainteligência do Exército Brasileiro, falhas ou deficiências na segurança orgânica, quando exploradas por

¹ As falhas identificadas pela análise dos PSOs estão relacionadas à numeração das apresentadas no Quadro

⁴ Não há correspondência dessa falha apresentada pelo gestor com alguma das identificadas pela análise dos PSOs

ameaças específicas, podem criar cenários de vulnerabilidade, resultando em incidentes que afetam a instituição (Exército Brasileiro, 2019).

Nesse contexto, Castro (2022) destaca que tais incidentes podem gerar impactos negativos na organização, tornando fundamental que, após a identificação das falhas, sejam implementadas medidas corretivas para proteger os ativos institucionais.

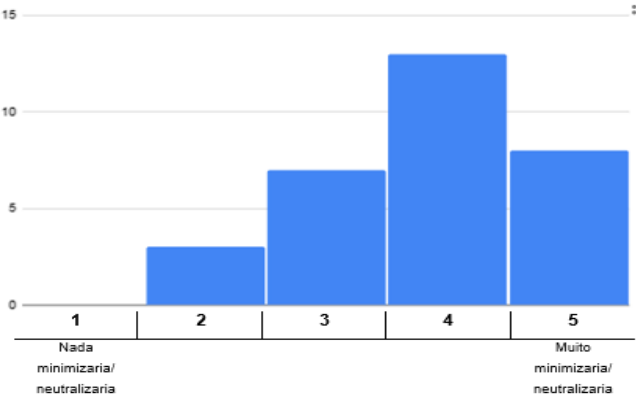
Além do Plano de Segurança Orgânica, o Exército Brasileiro dispõe, em seu manual, de outros documentos que integram o Plano de Desenvolvimento de Contrainteligência (PDCI), como o Plano de Monitoramento do PDCI, o Plano de Conscientização e o Plano de Treinamento Continuado. Dentre esses, os dois últimos se destacam no papel dos gestores, pois visam fomentar e fortalecer a mentalidade de contrainteligência entre os militares, contribuindo para o aprimoramento da proteção institucional e a mitigação das falhas identificadas (Exército Brasileiro, 2019).

No âmbito do CBMDF, as falhas de segurança relatadas pelos gestores devem servir como base para orientar as ações de segurança orgânica nas unidades, podendo, se necessário, motivar a atuação do Centro de Inteligência no planejamento desse segmento, conforme previsto no Regimento Interno da corporação (CBMDF, 2020).

Por fim, ao serem questionados sobre a possibilidade de minimizar ou neutralizar falhas na SEGOR por meio da instrução dos militares nesse segmento, os gestores responderam com base em uma escala, na qual valores mais altos indicam maior relação entre capacitação e redução das falhas.

Conforme apresentado no Gráfico 6, 67,74% dos comandantes apontaram uma correlação significativa, selecionando os valores mais elevados da escala (4 e 5), enquanto apenas 9,68% consideraram essa relação fraca, assinalando os valores mais baixos (1 e 2):

Gráfico 6 - Minimização ou neutralização das falhas de Segurança Orgânica na corporação após capacitação pessoal nesse segmento, pela ótica dos gestores



Fonte: O autor.

No Manual de Contrainteligência, o Exército Brasileiro detalha as etapas para o planejamento da segurança orgânica em uma instituição, estruturando-o em quatro planos, dos quais dois estão diretamente relacionados à capacitação de pessoal: o Plano de

Conscientização e o Plano de Treinamento Continuado (Exército Brasileiro, 2019).

Diversos autores concordam que o indivíduo é o elo mais vulnerável em qualquer sistema de segurança (Ribeiro, 2018; Gonçalves, 2009; Cepik, 2003). Sob essa perspectiva, para o fortalecimento da segurança institucional, é fundamental a implementação de ações cognitivas e afetivas que promovam ou aprimorem a cultura de contrainteligência entre os membros da organização, conscientizando-os sobre a relevância da adoção de procedimentos voltados à segurança institucional (Exército Brasileiro, 2019).

Seguindo essa mesma lógica, o Exército Brasileiro defende que os objetivos da contrainteligência sejam incorporados aos currículos dos diversos programas de instrução da instituição, com especial atenção à conscientização dos novos integrantes. O propósito central desses programas é “criar, desenvolver e manter a mentalidade de Contrainteligência, bem como transmitir os procedimentos preventivos para o tratamento de informações ou materiais sensíveis” (Exército Brasileiro, 2019, p. 91).

4.3 Modelo de aprimoramento da cultura de Segurança Orgânica

O Exército Brasileiro (EB) adota um planejamento específico para a Segurança Orgânica, denominado Planejamento de Desenvolvimento de Contrainteligência (PDCI), cujo objetivo principal é garantir a proteção dos ativos institucionais. Além disso, o PDCI visa fomentar uma mentalidade de contrainteligência, promovendo o fortalecimento das medidas de salvaguarda e proteção desses ativos. Para que esse processo seja efetivo, é essencial que todos os membros da organização estejam conscientizados sobre a cultura de segurança orgânica (Ribeiro, 2018).

Nesse contexto, Ribeiro (2018) destaca que o PDCI é composto por diversos elementos, incluindo o Programa de Conscientização e o Programa de Treinamento Continuado, que focam nos recursos humanos; as Normas de Controle, que abrangem a comunicação, os materiais e os equipamentos; além dos Serviços e Mecanismos de Segurança, da Estrutura de Gerência com Auditoria e Validação, dos Planos de Contingência e do Plano de Controle de Danos, voltados à proteção dos ativos, áreas e instalações.

Dessa forma, observa-se que cada setor possui diretrizes específicas para aprimorar a proteção dos ativos institucionais. Entre essas diretrizes, destacam-se os programas de capacitação, que incluem treinamentos, cursos e disciplinas, sendo fundamentais para o desenvolvimento do segmento em análise no que se refere aos recursos humanos.

O Manual de Contrainteligência do Exército Brasileiro destaca que o planejamento para o aprimoramento desse segmento considera que todos os membros da instituição possuem responsabilidades quanto à proteção da

organização. Assim, as medidas de segurança devem ser adaptadas às necessidades específicas de cada indivíduo e de sua área de atuação (Exército Brasileiro, 2019).

No âmbito do Corpo de Bombeiros Militar do Distrito Federal (CBMDF), o planejamento de segurança orgânica é elaborado pelo Centro de Inteligência, com atuação destacada da Seção de Contrainteligência (SECOI), conforme previsto no Decreto nº 31.817/2003 e no Regimento Interno da corporação (Distrito Federal, 2010; CBMDF, 2020).

Ao analisar a estrutura do PDCI do Exército Brasileiro, verifica-se que o CBMDF adota uma organização semelhante para esse segmento. No entanto, constatou-se a existência de apenas 22 PSOs na corporação, não abrangendo todas as unidades operacionais. Dessa forma, é necessário que os comandantes dessas unidades incentivem o Centro de Inteligência a desenvolver e implementar esses planos, garantindo a proteção dos ativos e a neutralização de possíveis ameaças (CBMDF, 2020).

O Plano de Conscientização tem como finalidade sensibilizar os militares sobre a importância da cultura de segurança, incentivando comportamentos voltados à proteção institucional (Exército Brasileiro, 2019). No CBMDF, uma estratégia de conscientização é executada por meio da publicação de mensagens de contrainteligência na página interna da corporação (Intranet), divulgadas pela Seção de Contrainteligência do CEINT.

Essas mensagens são fundamentais para criar e manter a mentalidade de contrainteligência, especialmente entre militares sem formação específica na área. Esse processo contribui diretamente para o fortalecimento da proteção institucional do CBMDF.

Já o Plano de Treinamento Continuado no CBMDF ocorre por meio de cursos de formação, aperfeiçoamento e especialização. No entanto, observa-se que esses cursos não abrangem todos os níveis hierárquicos. Atualmente, a disciplina de Atividade de Inteligência é ofertada apenas no Curso de Formação de Oficiais (CFO), não sendo abordada no Curso de Formação de Praças (CFP), que forma a maior parte do efetivo da instituição (CBMDF, 2017).

Essa limitação também se reflete nos cursos de aperfeiçoamento. Os Cursos de Aperfeiçoamento de Praças (CAP) e Altos Estudos para Praças (CAEP) não contemplam o tema, assim como o Curso de Aperfeiçoamento de Oficiais (CAO). Em contrapartida, o Curso de Altos Estudos para Oficiais (CAEO) inclui a disciplina de Inteligência Estratégica, embora com um enfoque gerencial voltado para a análise de cenários e apoio à tomada de decisões estratégicas, em vez da operacionalização da Atividade de Inteligência (Santos, 2015).

O Exército Brasileiro (2019), por sua vez, enfatiza que uma proteção institucional eficaz requer a criação, desenvolvimento e manutenção contínua da mentalidade de contrainteligência em toda a estrutura hierárquica. Para isso, é essencial que cada integrante assuma responsabilidades no que diz respeito a comportamentos,

ações preventivas e adesão a medidas de segurança.

O manual estabelece, ainda, que os objetivos da contrainteligência devem ser integrados aos currículos de instrução da organização, com abordagens diferenciadas para cada nível hierárquico. Esse conhecimento deve ser transmitido aos novos integrantes desde sua formação e ser constantemente reforçado ao longo da carreira, por meio dos Planos de Conscientização (Exército Brasileiro, 2019).

Nesse sentido, Ribeiro (2018) argumenta que, mesmo que as demais ações de SEGOR previstas no PDCI sejam implementadas, a mitigação efetiva das vulnerabilidades só será possível com o desenvolvimento de uma cultura de segurança orgânica entre os integrantes da instituição.

O autor sugere que a melhor forma de alcançar esse objetivo é incluir a disciplina de Atividade de Inteligência nos currículos de todos os cursos da organização, garantindo que os diferentes níveis hierárquicos tenham acesso ao conhecimento necessário para o fortalecimento da segurança na organização (Ribeiro, 2018).

Diante disso, ao avaliar os modelos de aprimoramento da cultura de segurança orgânica, verifica-se que o CBMDF, embora possua PSOs em algumas unidades e ações de conscientização, carece de um Plano de Treinamento Continuado abrangente, especialmente para as praças, que compõem quase 90% do efetivo (Brasil, 2009).

Para suprir essa lacuna e fortalecer a mentalidade de SEGOR na corporação, uma possível solução seria a inclusão de um componente curricular sobre Atividade de Inteligência no Curso de Formação de Praças. Essa medida permitiria o desenvolvimento da mentalidade de contrainteligência desde a formação inicial, incentivando a adoção de práticas preventivas e estratégicas alinhadas ao PDCI.

Outra alternativa viável seria a ampliação da divulgação de mensagens de contrainteligência para a tropa por meio de canais institucionais, como os planos de fundo dos computadores funcionais. Embora o CEINT já utilize a Intranet para esse fim, a intensificação dessa ação contribuiria para reforçar e disseminar a mentalidade de segurança orgânica entre os militares, alertando-os sobre riscos e incentivando comportamentos seguros no ambiente institucional.

5 Considerações Finais

A Segurança Orgânica, como um campo dedicado à proteção dos recursos institucionais por meio da prevenção de ameaças, exige de todos os membros da organização uma postura proativa. O desenvolvimento de uma mentalidade de contrainteligência é essencial para garantir um nível adequado de proteção, minimizando riscos e vulnerabilidades.

Os CBMs desfrutam de alta credibilidade social, sendo amplamente reconhecidos pela população. No entanto, a manutenção dessa confiança requer um planejamento estratégico voltado para a proteção institucional, assegurando a proteção dos ativos institucionais e a mitigação de possíveis ameaças adversas.

Ao analisar a Segurança Orgânica das unidades operacionais do CBMDF, identificaram-se falhas nesse segmento, evidenciadas tanto pela avaliação dos Planos de Segurança Orgânica existentes quanto pela percepção dos comandantes das Organizações Bombeiro-Militares (OBMs). Esse cenário demonstra que, embora haja um esboço de Planejamento de Desenvolvimento de Contrainteligência (PDCI) na corporação, faz-se necessário um modelo aprimorado, sendo que o objetivo desse aprimoramento deve ser o fortalecimento contínuo da mentalidade de contrainteligência entre os bombeiros militares.

REFERÊNCIAS

ALMEIDA NETO, W. R. **Inteligência e contra-inteligência no Ministério Público**. Belo Horizonte: Dictum, 2009;

BRASIL. **Decreto n.º 4.376, de 13 de setembro de 2002**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n.º 9.883, de 7 de dezembro de 1999, e dá outras providências. Brasília: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376compilado.htm. Acesso em: 18 maio 2023;

BRASIL. **Decreto n.º 10.777, de 24 de agosto de 2021**. Institui a Política Nacional de Inteligência de Segurança Pública. Brasília: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10777.htm. Acesso em: 20 abr. 2023;

BRASIL. **Lei n.º 7.479, de 2 de junho de 1986**. Aprova o Estatuto dos Bombeiros-Militares do Corpo de Bombeiros do Distrito Federal, e dá outras providências. Brasília: Presidência da República, 1986. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L7479compilado.htm. Acesso em: 12 maio 2023;

BRASIL. **Lei n.º 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. Brasília: Presidência da República, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em: 06 jun. 2023;

BRASIL. **Lei n.º 12.086, de 6 de novembro de 2009**. Dispõe sobre os militares da Polícia Militar do Distrito Federal e do Corpo de Bombeiros Militar do Distrito Federal, e dá outras providências. Brasília: Presidência da República, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12086.htm. Acesso em: 06 jun. 2023;

CBMDF. **Portaria n.º 31, de 05 de setembro de 2017**. Aprovação e publicação do projeto pedagógico do

Curso de Formação de Oficiais (CFO) e dá outras providências. Boletim Geral n.º 170, Brasília, 2017;

CBMDF. **Portaria n.º 24, de 25 de novembro de 2020.** Aprova o regimento interno do Corpo de Bombeiros Militar do Distrito Federal, revoga a Portaria n.º 6, de 15 de abril de 2020 e dá outras providências. Suplemento ao BG n.º 223, de 1º de dezembro de 2020. Brasília, 2020;

CBMDF. **Portaria n.º 20, de 05 de junho de 2022.** Institui o Sistema de Inteligência Bombeiro Militar - SIBOM, e aprova as normas gerais de organização e emprego. BG n.º 114, de 21 de junho de 2022. Brasília, 2022;

CEPIK, M. A. C. **Espionagem e democracia:** agilidade e Transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Fundação Getúlio Vargas, 2003;

DISTRITO FEDERAL. **Decreto n.º 31.817, de 21 de junho de 2010.** Regulamenta o inciso II, do artigo 10-B, da Lei n.º 8.255, de 20 de novembro de 1991, que dispõe sobre a Organização Básica do Corpo de Bombeiros Militar do Distrito Federal. Brasília: Sistema Integrados das Normas Jurídicas do DF, 2010. Disponível em: http://www.sinj.df.gov.br/sinj/Norma/63268/Decreto_31817_21_06_2010.html. Acesso em: 18 maio 2023;

EXÉRCITO BRASILEIRO. **Portaria n.º 076-COTER, de 09 de julho de 2019.** Aprova o Manual de Campanha EB70-MC 10.220 - Contrainteligência, 1ª Edição, 2019, e dá outras providências. Disponível em: http://www.sgex.eb.mil.br/sg8/003_manuais_carater_doutrinario/01_manuais_de_campanha/port_n_076_coter_09jul2019.html. Acesso em: 15 nov. 2022;

GONÇALVES, J. B. **Atividade de inteligência e legislação correlata.** Niterói: Impetus, 2009;

MJSP. Secretaria Nacional de Segurança Pública. **Doutrina Nacional de Inteligência de Segurança Pública.** Portaria nº 02, de 12 de janeiro de 2016, da Secretaria Nacional de Segurança Pública. Brasília: [s. ed.], 2016;

PEREIRA, C. V. **A atividade de inteligência como instrumento de eficiência no exercício do controle externo pelo Tribunal de Contas da União.** 2009. Monografia. (Curso de Pós-Graduação Lato Sensu de Especialização em Inteligência de Estado e Inteligência de Segurança Pública com Inteligência Competitiva) - Centro Universitário Newton Paiva, Minas Gerais, 2009;

PRATES, D. S. **A relevância da Atividade de Inteligência como ferramenta estratégica para o serviço operacional do CBMMG.** 2013. Trabalho de Conclusão de Curso (Curso de Formação de Oficiais

– Bacharelado em Ciências Militares) - Corpo de Bombeiros Militar de Minas Gerais, Belo Horizonte, 2013;

RIBEIRO, M. M. **Planejamento de desenvolvimento de segurança orgânica:** uma proposta para as unidades do CBMMA. 2018. Trabalho de Conclusão de Curso (Curso de Especialização em Gestão Pública) – Universidade do Sul de Santa Catarina, Florianópolis, 2018. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/11861/1/Artigo%20-%20Vers%C3%A3o%20final%20ap%C3%B3s%20defesa%20_Marcelo%20Martins%20Rib_eiro_.pdf. Acesso em: 18 maio 2023;

SANTOS, J. G. **Serviço de Inteligência:** uma análise do emprego da Inteligência Estratégica no processo decisório do Corpo de Bombeiros Militar do Distrito Federal. 2015. Trabalho de Conclusão de Curso (Curso de Altos Estudos para Oficiais Combatentes) - Corpo de Bombeiros Militar do Distrito Federal, Brasília, 2015.