CORPO DE BOMBEIROS MILITAR DE SANTA CATARINA
UNIVERSIDADE DO ESTADO DE SANTA CATARINA

CENTRO DE ENSINO BOMBEIRO MILITAR
CENTRO DE CIÊNCIAS DA ADMINISTRAÇÃO E SOCIOECONÔMICAS

CURSO DE ALTOS ESTUDOS ESTRATÉGICOS
ESPECIALIZAÇÃO EM GESTÃO PÚBLICA: ESTUDOS ESTRATÉGICOS EM ATIVIDADE BOMBEIRIL

RICARDO RIBEIRO

GESTÃO DE RISCOS PARA POLÍCIA MILITAR DE SANTA CATARINA: FOCO NA PROTEÇÃO DE POLICIAIS MILITARES AMEAÇADOS

FLORIANÓPOLIS
2018

Ricardo Ribeiro

Gestão de riscos para Polícia Militar de Santa Catarina: foco na proteção de policiais militares ameaçados

Monografia apresentada ao Curso de Altos Estudos Estratégicos e ao Curso de Especialização em Gestão Pública: Estudos Estratégicos em Atividade Bombeiril, do Centro de Ensino Bombeiro Militar (CBMSC) e do Centro de Ciências da Administração e Socioeconômicas (ESAG - UDESC) como requisito parcial para a obtenção do grau de Especialista em Gestão Pública: Estudos Estratégicos em Atividade Bombeiril.

Orientador: Prof. Maurício C. Serafim, Dr.
Coorientador: Cel PM Adilson Luiz da Silva, Esp.

Florianópolis
2018

Ficha de identificação da obra elaborada pelo autor com orientações da Biblioteca CBMSC

Ribeiro, Ricardo
Gestão de riscos para Polícia Militar de Santa Catarina: foco na proteção de policiais militares ameaçados. / Ricardo Ribeiro. -- Florianópolis : CEBM, 2018.
93 p.

Monografia (Curso de Altos Estudos Estratégicos) – Corpo de Bombeiros Militar de Santa Catarina, Centro de Ensino Bombeiro Militar, Curso de Altos Estudos Estratégicos, 2018.
Orientador: Prof. Maurício C. Serafim, Dr.; Cel. PM Adilson Luiz da Silva, Esp.

1. Segurança pública. 2. Gerenciamento de risco. 3. Organização criminosa. I. Serafim, Maurício C.; Silva, Adilson Luiz. II. Gestão de riscos para Polícia Militar de Santa Catarina: foco na proteção de policiais militares ameaçados.

RICARDO RIBEIRO

GESTÃO DE RISCOS PARA POLÍCIA MILITAR DE SANTA CATARINA: FOCO NA PROTEÇÃO DE POLICIAIS MILITARES AMEAÇADOS

Monografia apresentada ao Curso de Altos Estudos Estratégicos e ao Curso de Especialização em Gestão Pública: Estudos Estratégicos em Atividade Bombeiril, do Centro de Ensino Bombeiro Militar (CBMSC) e do Centro de Ciências da Administração e Socioeconômicas (UDESC) como requisito parcial para a obtenção do grau de Especialista em Gestão Pública: Estudos Estratégicos em Atividade Bombeiril.

Banca Examinadora:

Orientador:

_____

Prof. Maurício Custódio Serafim, Dr.
UDESC

Coorientador:

_____

Cel PM Adilson Luiz da Silva, Esp.
PMSC

Membros:

_____

Profa. Patrícia Vendramini, Dra.
UDESC

_____

Ten Cel PM Emerson Fernandes, Esp.
PMSC

Florianópolis, 12 de novembro 2018.

Dedico este trabalho à minha mulher, pelo incentivo, amor e companheirismo, aos meus pais, pelo apoio e dedicação, e a Deus, por ter me dado força física e mental para perseverar, não apenas neste curso, mas ao longo de toda a minha carreira na PMSC.

AGRADECIMENTOS

Agradeço a Deus, por ter me dado força para perseverar e concluir esse curso. À minha mulher, Juliana, pelo incentivo, amor e carinho. Aos meus pais, Aldemar e Mara, pelo apoio e dedicação ao longo deste período de estudo, quando retornei ao convívio diário da família. Ao Comandante-Geral da Corporação, Cel PM Carlos Alberto de Araújo Gomes Junior, ao Comandante-Regional, Cel PM Dirceu Neundorf, e à Diretora de Ensino da PMSC, Cel PM Claudete Lehmkuhl, assim como, ao Comando-Geral da CBMSC, Cel BM João Valério Borges, por terem me concedido a oportunidade de realizar o CAEE/2018. À Profa. Patrícia Vendramini, coordenadora do curso, e toda sua equipe, pelo esforço dispendido para que o curso mantivesse o grau de excelência da Esag/UDESC. Ao Prof. Valério Turnes, pelo incentivo em manter o tema do trabalho e pela colaboração com a pesquisa. Ao amigo Alisson Martinelli Silva pelo habitual apoio. Aos amigos que me ajudaram e motivaram a realizar o curso, especialmente ao amigo Maj PM Jorge Hebert Echude Silva Filho, Maj PM Marcus Vinícius dos Santos, Ten Cel BM Vandervan Nivaldo da Silva Vidal e Ten Cel PM Emerson Fernandes. Ao meu amigo Major PM Cristiano Medeiros, que me sugeriu o tema desta pesquisa. Ao Ten Cel PM André Alves, por ter fornecido informações e documentos essenciais para a pesquisa. Ao amigo Ten Cel BM Fabiano de Souza, pela parceria e toda ajuda das inúmeras atividades de aula. Aos meus colegas de turma do CAEE/2018, pela gentileza e cordialidade dispendida durante os dois meses de convívio. Ao meu orientador, Prof. Maurício Custódio Serafim, pelo conhecimento transmitido durante a elaboração deste trabalho. Ao meu coorientador, Cel PM Adilson Luiz da Silva, Chefe da Agência Central de Inteligência da PMSC, pelos conhecimentos repassados e valiosa contribuição na pesquisa, não apenas com a orientação de fontes, como também com a disponibilização e materiais e acesso a informações indispensáveis para o estudo. Aos demais oficiais e praças da ACI e toda inteligência da PMSC, em especial, Cap PM Dumith, Ten PM Paes e Cb PM Samuel pela colaboração na pesquisa.

“Ao tombarem a serviço da Lei
Nossos bravos heróis destemidos
Esquecidos soldados da grei
Jamais sejam por nós esquecidos.”
(Canção da PMSC, Ten Cel Roberto Kel)

RESUMO

A atividade policial militar é, por essência, uma atividade de risco. Os perigos e incertezas que envolvem o serviço policial militar são incontáveis. O risco, enquanto fato inerente à atividade policial, não é novidade. Por outro lado, a segurança pública de Santa Catarina passou a se defrontar com uma profunda alteração na criminalidade em razão do crescimento das facções criminosas, as quais se tornaram mais ousadas e violentas nos últimos anos. Destaca-se que entre 2012 e 2017 membros de facções criminosas executaram cinco séries de atentados no Estado. Na última delas, entre o final do mês de agosto e início do mês de setembro de 2017, 03 (três) integrantes das forças de segurança estaduais foram assassinados, dentre eles, dois policiais militares. Este trabalho valeu-se de pesquisas exploratórias, principalmente de dados secundários, por meio de pesquisa documental e bibliográfica, mas também de dados primários, coletados por meio de formulação de questionário, a fim de identificar um sistema de barreiras capaz de mitigar os perigos à segurança pessoal dos integrantes da Corporação e familiares, especialmente os advindos de ameaças oriundas de membros de organizações criminosas. Ao final, concluiu-se que foram atingidos os objetivos do trabalho ao se sugerir um modelo de sistema de gestão de riscos para policiais militares ameaçados da PMSC, fundamentado na Norma ISO 31.000 (2009), que terá o objetivo eliminar ou reduzir riscos à vida, à integridade física e psicológica e ao patrimônio de policiais militares e seus familiares decorrentes de ameaças relacionadas à atividade policial militar, identificando, analisando e avaliando os riscos, a fim de subsidiar a decisão sobre medidas de tratamento a serem adotadas, mantendo rigoroso controle sobre as ameaças identificadas e efeito das medidas de tratamento tomadas.

Palavras-chave: Segurança pública. Gerenciamento de risco. Organização criminosa.

ABSTRACT

The police activity is, by its essence, a risky activity. The hazards and uncertainties surrounding the military police service are countless. The risk, as an inherent fact of police activity, is nothing new. On the other hand, the public security of Santa Catarina has come to face a profound change in criminality due to the growth of criminal factions, which have become more daring and violent on the lately years. It is stand out that between 2012 and 2017 members of criminal factions executed five series of attacks in the State. On the latest, between the end of August and the beginning of September 2017, 03 (three) members of the state security forces were murdered, including two military police officers. This work has been based on exploratory research, mainly secondary data, through documentary and bibliographic research, but also of primary data, collected through out a questionnaire formulation, in order to identify a system of barriers capable of mitigating the hazards to the personal safety of members of the Force and their families, especially those arising from threats of criminal organizations associates. At the end, it was concluded that the objectives of the work were achieved by suggesting a model of risk management system for threatened military police officers of the PMSC, based on ISO 31,000 (2009), which will aim to eliminate or reduce risks to life, to the physical and psychological integrity and patrimony of military police officers and their families resulting from threats related to military police activity, identifying, analyzing and assessing the risks, in order to support the decision on treatment measures to be adopted, maintaining strict control over the threats identified and the effect of the treatment measures taken.

Keywords: Public security. Risk management. Criminal organization.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE SIGLAS

ABIN - Agência Brasileira de Inteligência

ACI/PMSC – Agência Central de Inteligência da Polícia Militar de Santa Catarina

Ag Temp – Agente Temporário

ALESC – Assembleia Legislativa de Santa Catarina

AS/NZS – Australiana/Neozelandesa

Cap – Capitão

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Cb - Cabo

CBMSC – Corpo de Bombeiros Militar de Santa Catarina

CISI - Coordenadoria de Inteligência e Segurança Institucional (MPSC)

CRFB – Constituição da República Federativa do Brasil

CTISP – Corpo Temporário de Inativos da Segurança Pública

CV – Comando vermelho (facção criminosa)

DNISP - Doutrina Nacional de Inteligência de Segurança Pública

DSIPJ - Departamento de Segurança Institucional do Poder Judiciário

FERMA – Federação Europeia de Associações de Gerenciamento de Riscos

GEBN - Guarnição Especial de Braço do Norte

GECT - Guarnição Especial de Curitibanos

GEIB - Guarnição Especial de Imbituba

GEIC - Guarnição Especial de Polícia Militar de Içara

GESA - Guarnição Especial de Santo Amaro da Imperatriz

IBGC – Instituto Brasileiro de Governança Corporativa

ISP - Inteligência de Segurança Pública

Maj - Major

MCDA-C – Multicritério em Apoio a Decisão Construtivista

MPSC – Ministério Público de Santa Catarina

OPM – Organização policial militar

ORM – Gerenciamento de Riscos Operacionais

PCC – Primeiro comando da capital (facção criminosa)

PCRC – Primeiro comando revolucionário catarinense (facção criminosa)

PGC – Primeiro grupo catarinense (facção criminosa)

PGJ – Procuradoria Geral de Justiça

PM – Polícia Militar

PMSC – Polícia Militar de Santa Catarina

POP – Procedimento Operacional Padrão

PSI/MP - Política de Segurança Institucional do Ministério Público

PSI/MPSC - Plano de Segurança Institucional do MPSC

RPM – Região policial militar

SINASPJ - Sistema Nacional de Segurança do Poder Judiciário

SISBIN - Sistema Brasileiro de Inteligência

SISP - Subsistema de Inteligência de Segurança Pública

Ten - Tenente

Ten Cel – Tenente-coronel

TJSC – Tribunal de Justiça de Santa Catarina

VSAT – Ferramenta de Autoavaliação de Vulnerabilidade

SUMÁRIO

1 INTRODUÇÃO

No dia 28 de agosto de 2017, por volta das 19h, o Cabo da Polícia Militar (Cb PM) Joacir Roberto Vieira, 43 anos, foi assassinado quando estava de folga, em uma loja de calçados, localizada no Bairro Jarivatuba, em Joinville. Dois dias depois, em 30 de agosto de 2017, outro policial militar, Edson Abílio Alves, também de folga do serviço, foi assassinado em frente a uma padaria localizada no Bairro Monte Alegre, em Camboriú. Ambos os crimes ocorreram por ordem de líderes da mesma facção criminosa, denominada Primeiro Grupo Catarinense, PGC[1].

Na mesma semana destes homicídios, em agosto de 2017, integrantes do PGC praticaram uma série de atentados contra policiais militares no Estado. Inúmeros policiais militares sofreram atentados ou foram ameaçados de alguma forma. Muitos deles tiveram suas residências alvejadas por disparos de arma de fogo.

Apesar da resposta rápida e enérgica por parte dos escalões de comando da Polícia Militar de Santa Catarina (PMSC), fazendo cessar os atentados, este cenário conturbado tornou ainda mais evidente o novo panorama vivenciado na Segurança Pública de Santa Catarina. Organizações criminosas conseguiram se instalar e ganhar capilaridade nos estabelecimentos prisionais e comunidades do Estado a ponto de se tornar um fator de risco para os integrantes dos órgãos de Segurança Pública, na medida em que usam de ameaças e atentados como forma de demonstração de força e de tentativa de intimidação de agentes públicos (SILVA, 2018).

O que se propõe com a presente pesquisa é estudar e apresentar um modelo de gestão de riscos para policiais militares ameaçados que possa ser adotado na PMSC.

Na visão de MORAES (2010, pag. 11) “a gestão dos riscos consiste em buscar e organizar informações adequadas e necessárias para implementar as medidas de controle capazes de minimizar a vulnerabilidade dos sistemas organizacionais”.

[1] No final de agosto e início de setembro de 2017, membros da facção criminosa PGC realizaram uma série de atentados contra integrantes de forças de segurança do Estado de Santa Catarina. Dois policiais militares e um agente prisional foram assassinados (SILVA, 2018). Na seção 4.2.2 deste trabalho há um resumo sobre as cinco séries de atentados praticados por facções criminosas no Estado entre 2012 e 2017.

A presente monografia foi dividida em 06 (seis) capítulos. No primeiro, além desta breve introdução, será apresentado o problema, a justificativa, os objetivos e a contribuição da pesquisa para PMSC.

O segundo capítulo será destinado ao referencial teórico, com a apresentação de conceitos de risco e de gestão de riscos, além do detalhamento de normas, modelos e etapas da gestão de riscos. Ainda serão analisados modelos e práticas de gestão de riscos do Tribunal de Justiça de Santa Catarina (TJSC) e do Ministério Público de Santa Catarina (MPSC), que podem servir de paradigma para a PMSC.

O terceiro capítulo terá a finalidade de expor os procedimentos metodológicos empregados na pesquisa.

No quarto capítulo serão apresentados os dados sobre a PMSC, sobre a atividade de inteligência da corporação e sobre o crescimento das organizações criminosas no Estado, incluindo informações sobre as cinco séries de atentados praticados por membros de facções criminosas em Santa Catarina.

Ainda no quarto capítulo serão apresentados dados de uma pesquisa empírica realizada pelo autor, que apurou o número de registros de policiais militares ameaçados nos últimos doze meses em Santa Catarina. Ao final deste capítulo serão descritos os modelos e práticas de gestão de riscos que melhor se ajustam às necessidades da PMSC.

No quinto capítulo será exposta uma proposta de implementação de um sistema de gestão de riscos para PMSC, apresentando os resultados da pesquisa sobre os modelos e práticas que podem ser adotadas na instituição, e no último as conclusões da pesquisa.

1.1 DESCRIÇÃO DA SITUAÇÃO PROBLEMA

1.1.1 Formulação do problema

Dentre as práticas e modelos de gestão de riscos existentes, quais as que melhor atendem às necessidades da PMSC, levando-se em consideração as características da Polícia Militar de Santa Catarina e o novo cenário da atuação de facções criminosas no Estado?

1.1.2 Justificativa

A atividade policial militar é, por essência, uma atividade de risco. Os perigos e incertezas que envolvem o serviço policial militar são incontáveis. O risco, enquanto fato inerente à atividade policial, não é novidade. Entretanto, o crescimento das facções criminosas é um fenômeno relativamente novo no Estado de Santa Catarina que, somado aos recentes atentados perpetrados contra policiais militares, tornaram imprescindível a implementação de um sistema de barreiras capaz de mitigar os perigos ao serviço policial militar, especialmente, no tocante à segurança pessoal dos integrantes da Corporação.

A gerência de riscos encontra seu marco histórico logo após a Segunda Guerra Mundial, quando chefes de segurança de grandes empresas e seguradoras dos Estados Unidos e da Europa buscavam um método para apurar os perigos reais e potenciais que possibilitasse reduzir os custos com pagamentos de prêmios de seguro e aumentar a proteção das empresas (BRASILIANO, 2003).

Nos anos 80, acidentes tecnológicos levaram autoridades governamentais a perceberem a necessidade de adotar sistemas de gestão de riscos, que já vinham sendo usados na indústria bélica, aeronáutica e nuclear e foram incorporados em processos industriais, principalmente na indústria de petróleo, química e petroquímica, inclusive, como requisito legal para obtenção de licenças ambientais.

No Brasil, o surgimento da necessidade de estabelecer métodos de gestão de riscos se deu em 1984, após o rompimento de uma tubulação de gasolina, na Vila Socó, no município de Cubatão, no Estado de São Paulo, que deixou cerca de 500 (quinhentas) vítimas, sendo 93 (noventa e três) fatais (GIOVANNI, 2010).

Com o passar do tempo a gestão de riscos se consolidou nos ambientes organizacionais, tanto públicos, quanto privados. Todavia, somente em 2001, após os trágicos eventos de 11 de setembro, o governo dos EUA definiu estratégias visando proteger estruturas críticas (ROSA, 2010).

Hodiernamente, há inúmeros modelos de gestão de riscos definidos em normas e bibliografias especializadas que podem servir de paradigma para PMSC.

Neste contexto, o presente trabalho assume relevância científica ao pesquisar uma metodologia destinada a criar um sistema de gestão de riscos para policiais militares ameaçados no âmbito da Polícia Militar de Santa Catarina.

Destarte, por via de consequência, o estudo é importante porque visa resguardar a vida, a integridade física e/ou o patrimônio de policiais militares ameaçados.

Vale observar que há um segundo ponto de preocupação institucional nas ameaças contra policiais militares que diz respeito ao impacto na sociedade. Isto se dá porque a intimidação de agentes públicos acarreta em sensação de insegurança para comunidade em geral, que se sente desprotegida quando percebem que até mesmo os integrantes das instituições de segurança estão em perigo.

1.2 OBJETIVOS

1.2.1 Objetivo geral

O objetivo geral desse projeto será o de propor a implementação de um sistema de gestão de riscos para Polícia Militar de Santa Catarina, específico para tratar de ameaças contra policiais militares, descrevendo modelos e práticas recomendáveis à Corporação.

1.2.2 Objetivos específicos

- Pesquisar modelos e normas de gestão de riscos, apresentando os conceitos relacionados ao tema;
- Apresentar a estrutura da Polícia Militar de Santa Catarina e da atividade de inteligência na Corporação;
- Caracterizar a atuação das facções criminosas no Estado de Santa Catarina;
- Pesquisar dados sobre os registros de ameaças contra policiais militares registradas nos últimos 12 (doze) meses pelas AI da PMSC.
- Propor diretrizes para implementação de um sistema de gestão de riscos.

1.3 CONTRIBUIÇÃO DO TRABALHO

De forma bastante objetiva, o foco principal do estudo é pesquisar um sistema de gestão de riscos voltado a tratar ameaças contra policiais militares. Portanto, a contribuição principal do trabalho será propor uma metodologia que permita eliminar

ou mitigar os riscos de ameaças contra policiais militares, das quais se percebe um aumento nos últimos anos em razão do crescimento das facções criminosas no Estado de Santa Catarina.

Além disso, caso implementado, o sistema de gestão de riscos pode ter outras utilidades relevantes, tais como:

– Criar ou aprimorar as ferramentas de coleta de informações sobre ameaças contra policiais militares;

– Explicitar as vulnerabilidades de policiais militares ameaçados, impulsionando a criação de métodos para minimizá-las;

– Subsidiar os gestores sobre as medidas de controle a serem adotadas, para que o recurso empregado seja proporcional ao risco;

– Servir de fonte de informação em processos decisórios da Corporação;

– Criar uma expertise na Corporação sobre sistema de gestão de riscos, sendo que, futuramente, poderá ser aproveitada em outros processos e/ou atividades da Corporação.

2. REFERENCIAL TEÓRICO

Neste capítulo serão apresentados os resultados da pesquisa sobre o processo de gestão de riscos, das normas, principais modelos existentes e conceitos relacionados, além de práticas de gestão de riscos no TJSC e MPSC.

Não obstante, da análise dos modelos existentes, será destacado aquele que melhor se ajusta às necessidades da PMSC.

Destarte, este capítulo foi estruturado da seguinte forma: conceito de risco; conceito de gestão de riscos; etapas de gestão de riscos; comunicação e consulta; identificação de riscos; análise de riscos; avaliação de riscos; tratamento do risco; monitoramento e análise crítica; registro de processos de gestão de riscos, e; modelos de gestão de riscos em outras instituições.

2.1 CONCEITO DE RISCO

A norma ISO 31.000 (2009) traz o conceito de risco como o “efeito da incerteza nos objetivos”, podendo ser descrito como a combinação da consequência de um evento e a probabilidade de sua ocorrência, sendo probabilidade a “chance de algo acontecer” e consequência o “resultado de um evento que afeta os objetivos”.

A ideia de risco está, portanto, diretamente relacionada ao estado mental da incerteza sobre determinado evento. Ao tratar de risco nas organizações, Lunkes (2010) conceitua risco como a incerteza relacionada aos ganhos e perdas que podem ou não ocorrer a partir de decisões tomadas.

Bernstein (1997), escritor da obra “Desafio aos Deuses, a fascinante história do risco”, traz a mesma ideia de incerteza, ao afirmar que risco não significa propriamente um perigo, mas a incerteza sobre o futuro.

Rosa (2010), ao realizar pesquisa sobre Gerenciamento de Riscos voltado à Segurança Empresarial, constatou que o conceito de risco é universal.

Em geral, as bibliografias especializadas trazem a probabilidade da ocorrência de um evento e suas consequências como variáveis do risco. Porém, percebe-se que, conforme o autor ou à área de estudo, as nomenclaturas existentes na conceituação de risco mudam. Ainda assim o sentido do conceito permanece inalterado, como no empregado na área de defesa civil, onde a doutrina aduz que

risco sugere uma matriz que inclui a probabilidade da ocorrência de uma ameaça e o impacto ou consequências, podendo ser “formalmente definido como um produto da probabilidade de ocorrência de uma ameaça (perigo) pelas consequências que isto provoca.” (RIO GRANDE DO SUL, UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL UFRGS, 2016, pag. 84).

Observa-se que o risco traz uma vertente negativa e uma positiva, sendo que, “as vantagens e oportunidades devem ser vistas não só no contexto da própria atividade, mas também em relação às muitas e diversas partes interessadas que podem ser afetadas, doravante designadas por intervenientes (*stakeholders*).” (FERMA, 2002, p.2).

2.2 CONCEITO DE GESTÃO DE RISCOS

A ideia de o risco poder acarretar em prejuízos ou danos impulsionam as organizações a buscar conhecimento para mitigar a tais prejuízos, reais ou potenciais (ROSA, 2010). Esse estímulo conduz as organizações a realizarem a gestão de riscos, atividade destinada a dirigir e controlar uma organização no que for inerente a riscos (ISO, 2009).

Na visão de Moraes (2010, pag. 11) “a gestão dos riscos consiste em buscar e organizar informações adequadas e necessárias para implementar as medidas de controles capazes de minimizar a vulnerabilidade dos sistemas organizacionais. ”

Observa-se que os termos “gestão de riscos” e “gerenciar riscos” são muitas vezes utilizados como sinônimos. Para a norma ISO 31.000 (2009) enquanto a gestão de riscos refere-se à arquitetura, ou seja, os princípios, a estrutura e o processo do gerenciamento de riscos, gerenciar riscos trata-se do emprego da referida arquitetura em riscos específicos.

Conforme Moraes (2010, p.11) o sistema de gestão de riscos atua justamente nas duas variáveis do risco, denominada por ele como frequência e gravidade:

> O Sistema de gestão de riscos irá atuar nas duas vertentes do risco, a frequência e a gravidade, lembrando que os componentes da perda potencial são: magnitude, probabilidade de ocorrência do evento e nível de exposição. A intervenção na frequência irá ocorrer na implementação das medidas de controle que possam minimizar a probabilidade de ocorrência das causas. A intervenção na vertente da gravidade irá ocorrer através da elaboração de plano de emergência/contingência e dimensionamento de recursos para minimizar os impactos.

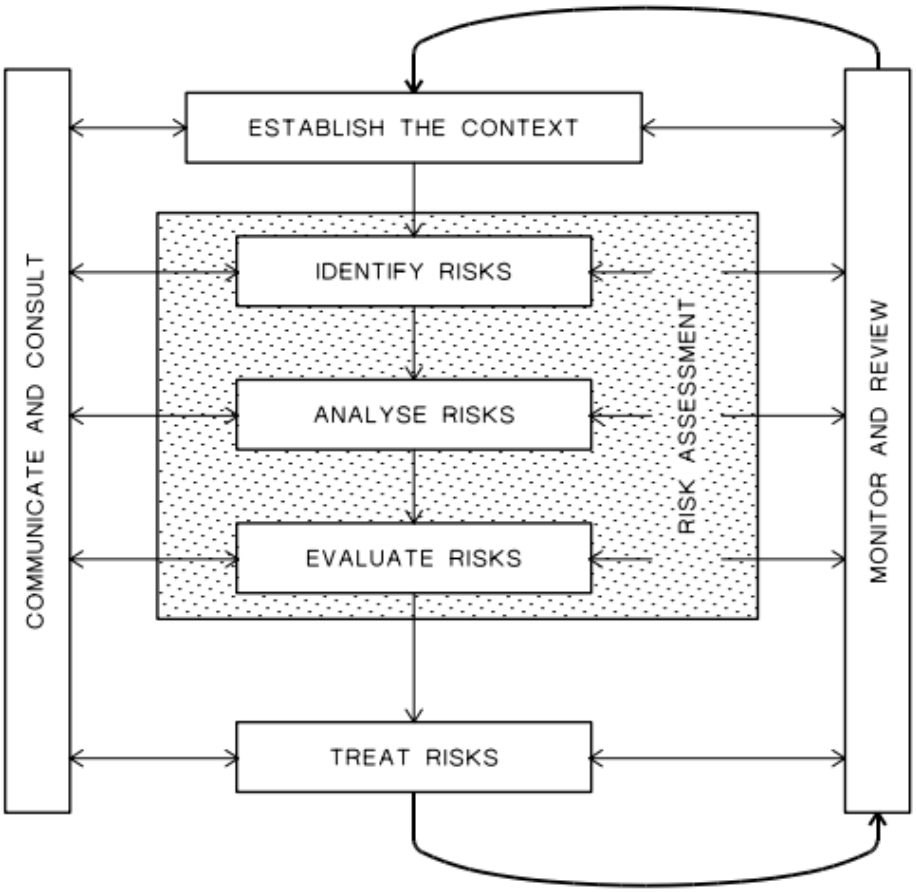
Vale frisar que a identificação e o tratamento dos riscos são essenciais para a uma boa gestão de riscos em qualquer organização (FERMA, 2002).

2.3 NORMAS, MODELOS E ETAPAS DA GESTÃO DE RISCOS

As etapas de um processo de gestão de riscos podem variar a depender do modelo adotado. Em aprofundada pesquisa sobre o assunto, Rosa (2010) apresenta uma série de normas e modelos de sistemas de gestão de riscos. O trabalho de Rosa sintetizou as etapas da gestão de riscos em cada um dos modelos propostos, da seguinte forma:

Norma AS/NZS 4360:2004 (AS/NZS, 2004, apud ROSA, 2010): [1] Comunicar e consultar; [2] Estabelecer o contexto; [3] Identificar os riscos; [4] Analisar os riscos; [5] Avaliar os riscos; [6] Tratar os riscos; [7] Monitorar e revisar. Na Figura 1 está estampado o fluxo das etapas desta norma.

Figura 1 - Processo de gestão de riscos da Norma AS/NZS 4360:2004



Fonte: AS/NZS 4360:2004 (AS/NZS 4360:2004). p. 09

Norma de gestão de riscos FERMA (FERMA, 2002, apud ROSA, 2010): [1] Modificação; [2] Definição dos objetivos estratégicos da organização; [3] Avaliação do risco; [4] Comunicação do risco; [5] Decisão; [6] Tratamento do risco; [7] Comunicação do risco residual; [8] Monitoramento; [9] Auditoria formal. A figura 2 facilita a visualização do processo de gestão de riscos proposto pela Norma FERMA.

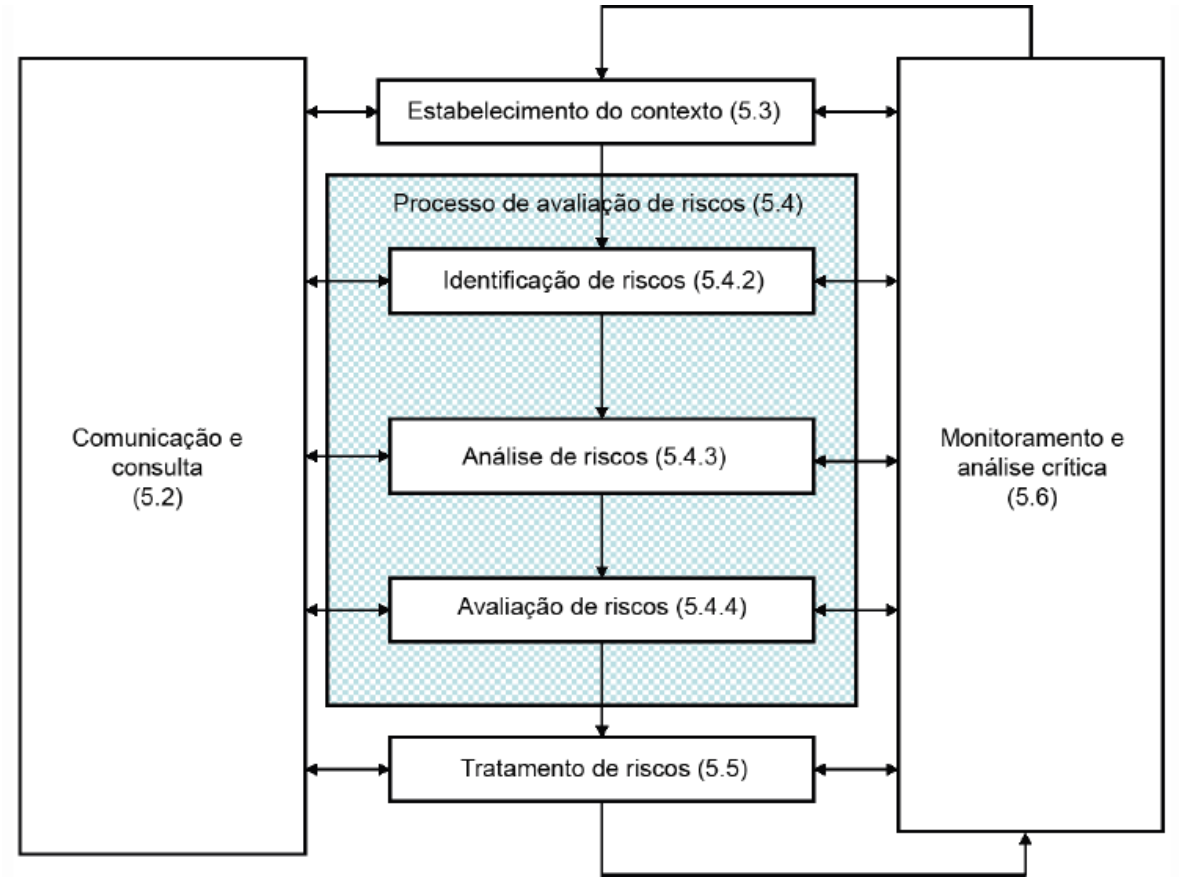
Figura 2 – Processo de gestão de riscos da Norma FERMA

Fonte: FERMA (2002). p. 05.

Norma ISO 31.000 – *Risk management principles and guidelines on implementation* (ISO, 2009, apud ROSA, 2010): [1] Comunicar e consultar; [2] Estabelecer o contexto; [3] Avaliação dos riscos (identificar os riscos, analisar os riscos e estimar os riscos; [4] Tratar os riscos; [5] Monitorar e consultar. Ressalta-se que a Norma ISO 31.000 (2009) é essencial nesta pesquisa, uma vez que ela servirá de base para o modelo proposto para PMSC. Sendo assim, após listar os modelos

de gestão de riscos pesquisados, será retomada a análise dos processos descritos na Norma ISO 31.000, detalhando cada uma de suas etapas, apresentadas na Figura 3.

Figura 3 – Processos de gestão de riscos da Norma ISO 31.000 (2009)



Fonte: ISO 31.000 (2009). p. 14.

Modelo de gerenciamento de riscos corporativos (IBGC, 2007, apud ROSA, 2010): [1] Identificação e classificação dos riscos; [2] Avaliação dos riscos; [3] Mensuração dos riscos; [4] Tratamento dos riscos; [5] Monitoramento dos riscos; [6] Informação e comunicação.

Risk management process (ROPER, 1999, apud ROSA, 2010): [1] Avaliação do ambiente; [2] Avaliação das ameaças; [3] Avaliação das vulnerabilidades; [4] Avaliação dos riscos; [5] Determinar opções de contramedidas.

Process vulnerability analyis (BAYBUTT, 2002, apud ROSA, 2010): [1] Análise de ameaça; [2] Processo de análise da vulnerabilidade; [3] Considerar o que pode ser feito para reduzir a probabilidade de concretização do risco.

Manual de análise de riscos para a segurança empresarial (BRASILIANO, 2003, apud ROSA, 2010): [1] Identificação do risco; [2] Análise dos riscos; [3] Matriciamento dos riscos; [4] Definição de soluções.

Risk analysis (BRODER, 2006, apud ROSA, 2010): [1] Identificação dos riscos; [2] Identificação das ameaças; [3] Mensuração dos riscos; [4] Quantificação e priorização das perdas potenciais; [6] Análise dos custos/benefícios.

Vulnerability self assessment tool – VSAT (BRODER E TUCKER, 2006, apud ROSA, 2010): [1] Identificação dos recursos; [2] Determinação da criticidade; [3] Identificação da ameaça; [4] Identificação de contramedidas existentes; [5] Determinação do nível de risco; [6] Determinação da probabilidade de falhas; [7] Determinação das vulnerabilidades; [8] Determinação de quais riscos são aceitáveis; [9] Determinação de contramedidas; [10] Análise dos custos/benefícios; [11] Desenvolvimento de plano de continuidade.

Operational risk management – ORM (BRODER E TUCKER, 2006, apud ROSA, 2010): [1] Identificação do perigo; [2] Estimar o risco; [3] Analisar contramedidas existentes; [4] Definir decisões de controle; [5] Implementar as decisões de controle; [6] Supervisionar e revisar.

CARVERS + SHOCK (BRODER E TUCKER, 2006 apud ROSA, 2010): [1] Criticidade; [2] Acessibilidade; [3] Recuperabilidade; [4] Vulnerabilidade; [5] Efeito; [6] Reconhecimento; [7] Choque.

Security risk assessment and management process (BIRINGER, MATALUCCI E O'CONNOR, 2007, apud ROSA, 2010): [1] Identificar os ambientes a serem avaliados; [2] Analisar as ameaças; [3] Analisar as consequências; [4] Analisar o gerenciamento dos sistemas de segurança; [5] Estimar o risco; [6] Matriciar os riscos; [7] Definir estratégias de redução dos riscos.

Além dos modelos descritos no trabalho de Rosa (2010), é possível encontrar outros modelos com etapas bem definidas. Para Moraes (2010), por exemplo, antes de iniciar as etapas da gestão de riscos, deve-se estabelecer o contexto da análise, identificando tarefas, atividades, processos de trabalho e prática de avaliação. Após isso, deve-se atender os requisitos expostos a seguir: [1] Identificação dos perigos; [2] Identificação das medidas de controle existentes e sua aplicabilidade; [3] Sugestão de medidas de controle, inclusive de hierarquia OHS de controle; [4] Implementação das novas medidas de controle; [5] Avaliação da eficácia das medidas de controle implementadas, e; [6] Monitoramento e revisão do programa.

O curso de capacitação em gestão de riscos voltado à defesa civil, esclarece que a gestão de riscos tem a finalidade de reduzir os impactos de ameaças e, por via de consequência, a ocorrência de possíveis desastres (UFRGS, 2016). A referida capacitação propõe um ciclo contínuo de gestão de riscos e gerenciamento de desastres, com as seguintes fases: [1] Prevenção; [2] Mitigação; [3] Preparação; [4] Resposta, e; [5] Recuperação.

Dentre as várias opções apresentadas acima, o modelo proposto pela norma ISO 31.000 (2009), em razão da sua destinação a todos os tipos de organização e atividades, é o que se apresenta como mais adequado para gestão de riscos de policiais militares ameaçados.

Desta forma, será analisada cada uma das fases propostas pela norma ISO 31.000, porém, extrapolando os conceitos estabelecidos na referida norma, buscando paralelos em outras normas e na bibliografia existente.

2.3.1 Comunicação e consulta

A norma ISO 31.000 (2009) esclarece que a comunicação e consulta deve ser realizada em todas as fases do processo de gestão de riscos, sendo que desde a fase inicial de estabelecimento de contexto, até o tratamento do risco, deve haver comunicação e consulta a todas as partes interessadas, internas e externas.

A FERMA (2002) foi ainda mais enfática, ao detalhar os desdobramentos da comunicação do risco a cada um dos possíveis *stakeholders*, internos e externos, estabelecendo que cada indivíduo deve:

> - Compreender o seu nível de responsabilização relativamente a riscos individuais;
> - Compreender de que forma podem contribuir para a melhoria contínua da gestão de riscos;
> - Compreender que a gestão de riscos e a sensibilização para a existência de riscos são elementos chave da cultura da organização;
> - Comunicar, sistemática e imediatamente, à direção de topo os riscos novos ou falhas constatadas nas medidas de controle existentes. (FERMA, 2002, pag. 11).

Assim como fizeram as normas ISO 31.000 (2009) e FERMA (2002), é importante que futuras normas ou protocolos de gestão de riscos para policiais militares ameaçados na PMSC tragam a comunicação e consulta como uma etapa contínua, descrevendo a relevância da troca de informações ao longo de todo o

processo de gestão de riscos e apontando as obrigações de cada um dos *stakeholders*.

2.3.2 Estabelecimento do contexto

O estabelecimento do contexto é etapa de suma importância no processo de gestão de riscos. É nessa fase que “a organização articula seus objetivos, define os parâmetros externos e internos a serem levados em consideração ao gerenciar o risco e estabelece o escopo e os critérios de risco para o restante do processo.” (ISO, 2009, pag. 15).

A norma AS/NZS 4360 (2004), que apresenta um modelo aproximado ao da ISO 31.000 (2009), destaca que nesta fase deve-se estabelecer o contexto no campo estratégico, organizacional e de gestão de riscos, sendo que os critérios estabelecidos servirão de fundamentação para análise e avaliação do risco.

Conforme a ISO 31.000 (2009), é necessário estabelecer o contexto externo e interno. As análises desses ambientes, externo e interno, devem focar em todos os aspectos que possam impactar nos objetivos da organização. Para ilustrar, no contexto externo, devem ser incluídos aspectos como: culturais (ambiente social, político, legal, técnico e econômico), agentes e tendências, relacionamentos e percepções de partes interessadas externas (ISO, 2009; MORAES, 2010).

Traçando um paralelo, um protocolo de gestão de riscos para policiais militares ameaçados deve se preocupar em enumerar todos os fatores que possam impactar no objetivo de salvaguarda do efetivo policial militar, seus familiares e patrimônio, incluindo, especialmente, o acompanhamento sistemático do sistema de inteligência da PMSC (SIPOM) quanto às atividades de organizações criminosas, dentro e fora do Estado.

2.3.3 Macro fase do processo de avaliação dos riscos

O processo de avaliação dos riscos trata-se de uma “macro fase” que engloba a identificação dos riscos, a análise dos riscos e a avaliação dos riscos (ISO, 2009). Destaca-se que a avaliação de riscos é apenas uma das partes do processo de avaliação de riscos. A terminologia em inglês *risk assessment*, para o processo de avaliação de riscos, e *risk evaluation*, para a avaliação de riscos, ajuda na distinção.

2.3.4 Identificação dos riscos

A identificação dos riscos é um processo elaborado que envolve, sucintamente, a busca, o reconhecimento e a descrição dos riscos. É necessário que a identificação inclua todos os riscos, mesmo aqueles que as fontes não estejam sob o controle da organização e ainda que as fontes ou causas dos riscos possam não ser evidentes (ISO, 2009). Neste processo, as fontes de risco, as áreas de impacto, os eventos e suas causas e consequências devem ser identificadas e listadas, a fim de se enumerar os eventos capazes de influenciar nos objetivos da organização (FERMA, 2002; ISO, 2009).

É imprescindível orientar todos os integrantes da organização a não desprezar ameaças identificadas, sendo que todas as ameaças e informações correlatas devem ser reportadas, mesmos aquelas que não pareçam ter importância, pois, a análise do conjunto das informações permitirá entender a realidade (BRASIL, CONSELHO NACIONAL DE JUSTIÇA CNJ, 2018).

Na PMSC há mecanismos que podem contribuir na identificação de riscos relacionados às ameaças contra policiais militares, tais como, o Net-Denúncia, o Disque-Denúncia, o sistema de ouvidoria e o atendimento de emergências (190), que podem ser utilizados como meios de coleta de informações sobre ameaças. Além disso, o sistema de inteligência (SIPOM), por si só, gera um fluxo natural das informações que faz com que riscos identificados sejam levados ao conhecimento dos gestores da Corporação. Entretanto, convém que a norma interna de gestão de riscos vise orientar para que todos os riscos que acarretem em ameaças contra policiais militares sejam identificados e enumerados.

2.3.5 Análise de riscos

O processo de análise de riscos perpassa, inicialmente, por compreender a natureza do risco e, depois, por determinar o nível de risco, fornecendo fundamentos para avaliação do risco e subsidiando as decisões sobre o tratamento do risco. As decisões encontram subsídios nas consequências e probabilidade da ocorrência do evento (risco), o que é feito na fase de análise de riscos. Para tanto, é preciso identificar os fatores que afetam as causas e consequências dos riscos, sabendo-se que um evento pode ter mais de uma causa e várias consequências (ISO, 2009).

Sua aplicação destina-se a entender a natureza dos riscos e a mensuração do nível de risco com a finalidade de adotar medidas de segurança que mantenham os riscos em níveis aceitáveis (ROSA, 2010).

Portanto, a análise de riscos visa saber a probabilidade da ocorrência do evento e mensurar seus impactos. Todavia, Brasiliano (2003) esclarece que o grande desafio da análise de riscos é encontrar suporte na ciência e aponta duas categorias de métodos científicos para a tarefa: objetivos e subjetivos.

Os métodos objetivos referem-se à análise da probabilidade por processos estatísticos e devem ser usados quando há um padrão delineado a partir de um consistente histórico de eventos ocorridos. Por outro lado, quando não há um padrão gerado por dados consistentes, deve-se recorrer a métodos subjetivos. Essa metodologia encontra embasamento científico com a adoção de critérios preestabelecidos e escala de valor, com atribuição de graus por equipe multidisciplinar, estabelecendo-se níveis de criticidade a partir da avaliação subjetiva da probabilidade (BRASILIANO, 2003).

Rosa (2010, p. 90) aponta ferramentas que podem ser empregadas para mensuração do risco de forma científica:

> A mensuração do grau de risco constitui-se, segundo os artigos que integram o referencial teórico, em um processo onde inicialmente busca-se conhecimento sobre como os riscos possam impactar o ambiente empresarial, qual a frequência com que são concretizados e quais as consequências com suas concretizações, para estes fins são sugeridas ferramentas como: (i) árvores de falhas, (ii) método AHP, (iii) método Delphi, (iv) brainstorming, (v) investigação de incidentes, dentre outros (FERMA, 2002; SUH e HAN, 2002; BIRINGER et al., 2007). Após esta etapa, com o conhecimento obtido ou gerado, são emitidos pareceres, onde os riscos são classificados segundo níveis de criticidade pré-estabelecidos. Tais níveis podem ser exemplificados como: 9i) crítico; (ii) alto; (iii) médio; (iv) baixo (ROPER, 1999; AS/NZS, 2004).
> Todos os artigos que integram o referencial teórico desta pesquisa apresentam escalas do tipo Likert, classificando os riscos de acordo com suas especificações.

É fundamental que um protocolo de gestão de riscos para policiais militares ameaçados destaque a necessidade de utilizar critérios científicos para mensuração dos riscos, podendo se valer das ferramentas relacionadas na pesquisa de Rosa (2010), ou seja: árvores de falhas, método AHP, método Delphi, *brainstorming*, investigação de incidentes, entre outros.

O Conselho Nacional de Justiça (CNJ) elaborou um guia destinado à análise e gerenciamento de riscos de magistrados. Este guia apresenta uma visão prática da análise de riscos, orientando a realizar a análise das variáveis que concorrem para existência do risco, ameaças e vulnerabilidades, de forma isolada.

Segundo o guia, quanto à ameaça é preciso determinar a viabilidade, partindo da delimitação dos fatos e suas circunstâncias e da identificação dos atores. Posteriormente, deve-se verificar a existência de padrões, apurar a motivação e os desencadeadores da potencial violência, buscar dados sobre comportamento, sentimentos e personalidade do ameaçador, avaliar a credibilidade, tanto das fontes, quanto das informações, e, por fim, identificar se o agente ameaçador tem capacidade operacional para realizar o ataque. No tocante à vulnerabilidade, o guia orienta o analista de risco a focar nos aspectos de segurança da vida e do trabalho do magistrado, que são divididos em quatros eixos: local de trabalho, local de residência, itinerários e hábitos (CNJ, 2018).

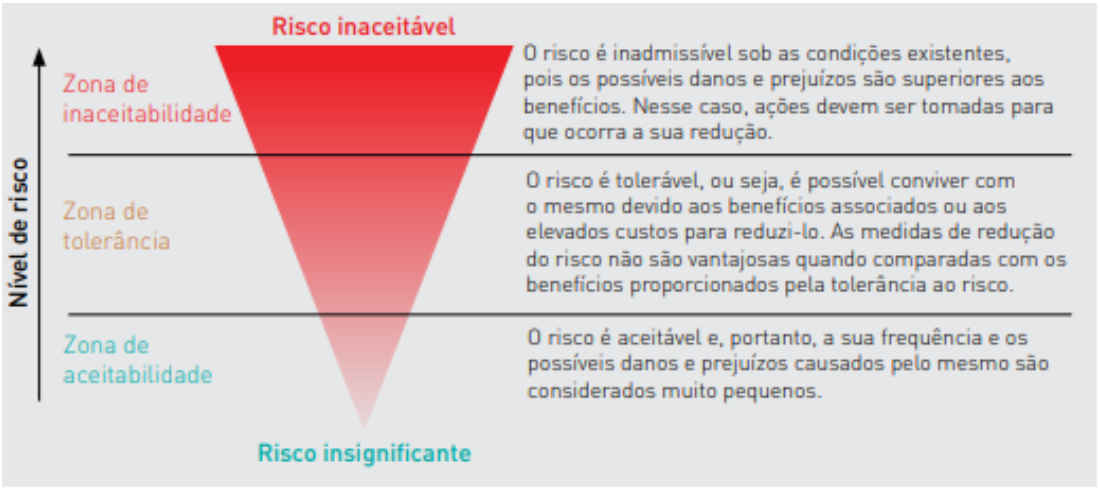
2.3.6 Avaliação de riscos

A avaliação dos riscos fundamenta-se na análise dos riscos e destina-se a subsidiar a tomada de decisão sobre os seguintes aspectos do tratamento dos riscos: a) quais riscos precisam de tratamento; b) qual é a prioridade para implementação do tratamento de riscos, de acordo com os níveis dos riscos encontrados e do contexto estabelecido (ISO, 2009).

Quanto maior for a quantidade de riscos existentes em uma organização, maior será a importância de avaliá-los como forma de subsidiar as decisões sobre quais riscos devem ser tratados de forma imediata, quais podem aguardar a liberação de recursos para iniciar o tratamento e quais demandam apenas de acompanhamento.

Neste contexto, com relação à necessidade de tratamento, o Manual de Capacitação em Defesa Civil (UFRGS, 2016) apresenta um esquema representativo da diferenciação de risco aceitável, tolerável e inaceitável, demonstrado na Figura 4.

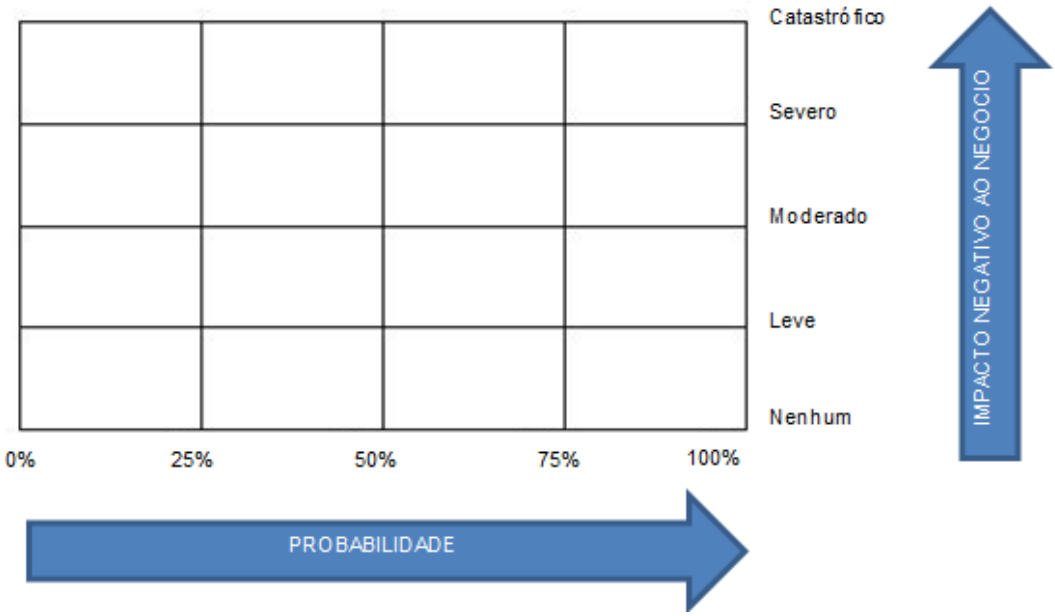
Figura 4 - Esquema representativo da diferenciação entre risco aceitável, tolerável e inaceitável



Fonte: Adaptado do EP Consult Energies apud UFRGS (2016). p. 87.

Para facilitar a percepção dos níveis dos riscos para o gestor, Brasiliano (2003) propõe que, após a fase de análise dos riscos, deva-se elaborar uma matriz de vulnerabilidade. Com o matriciamento dos dados colhidos na mensuração dos riscos é possível ter uma "fotografia" dos danos esperados e visualizar de forma clara as fragilidades existentes, pois, conforme o posicionamento do risco na matriz é possível identificar facilmente a probabilidade da ocorrência do evento e qual seria o grau de impacto negativo para a organização que, conforme Figura 5, foi classificado em: catastrófico, severo, moderado, leve e nenhum.

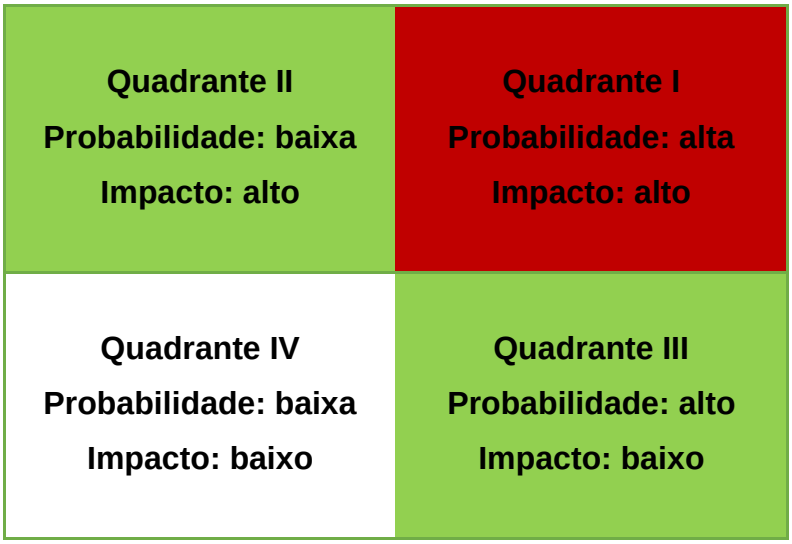
Figura 5 - Matriz de Vulnerabilidade



Fonte: Brasiliano (2003). p. 158.

Brasiliano (2003), divide a matriz de vulnerabilidade em quadrantes estratégicos, de acordo com a probabilidade de ocorrência e a severidade do impacto, conforme ilustrado na Figura 6.

Figura 6 – Quadrantes da Matriz de Vulnerabilidade



Fonte: Adaptado de Brasiliano (2003). p. 159.

Os riscos do quadrante I apresentam alta probabilidade de ocorrência e poderão gerar consequências severas, por isso, necessitam de tratamento imediato. Os riscos do quadrante II têm pouca probabilidade de ocorrer, mas podem resultar em impactos graves, motivo pelo qual devem ser monitorados rotineira e sistematicamente. Já os riscos do quadrante III não podem gerar consequências graves, mas tem alta probabilidade de ocorrer. Para elas deve haver um planejamento com respostas rápidas e testadas em um plano de contingência. Por fim, os riscos do quadrante IV possuem baixa probabilidade de ocorrer e baixo grau de impacto, devendo apenas ser administrados em caso de ocorrência (BRASILIANO, 2003).

Além dos parâmetros destacados acima, Brasiliano (2003) também ressalta que é possível inserir diversos riscos em uma mesma matriz a fim de compará-los e facilitar a decisão sobre a priorização do tratamento.

Neste sentido, convém que em um protocolo de gestão de riscos para policiais ameaçados seja prevista a avaliação dos riscos com emprego de matrizes de vulnerabilidade, como forma de subsidiar a decisão sobre quais riscos devem ser

tratados imediatamente e quais riscos devem ser acompanhados, bem como, permitir a confecção de uma lista de prioridade para o tratamento dos riscos.

2.3.7 Tratamento de riscos

A etapa de tratamento de riscos envolve analisar os resultados da avaliação de riscos, selecionar uma ou mais opções para modificar os riscos e implementar as opções selecionadas (ISO, 2009). Portanto, o tratamento de riscos envolve um processo decisório sobre quais “ferramentas” serão empregadas para alterar o risco avaliado, a fim de torná-lo aceitável mediante o contexto previamente analisado.

Pode-se resumir o “tratamento de risco como um processo de seleção e implementação de medidas para modificar um risco” (FERMA, 2002, pag. 10), tendo como elemento principal a redução ou eliminação do risco.

O tratamento de riscos é um processo cíclico, que envolve: a) avaliação do tratamento de riscos já realizado; b) decisão se os níveis de risco residual são toleráveis; c) se não forem toleráveis, a definição e implementação de um novo tratamento para os riscos residuais; d) avaliação da eficácia desse tratamento (ISO, 2009).

Nesta fase deve ser elaborado um plano de tratamento a partir da decisão do gestor, que deverá optar sobre como irá intervir nos riscos com vistas a modificá-los. A ISO 31.000 (2009) apresenta um rol, não exaustivo, de opções: a) ação de evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco; b) tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade; c) remoção da fonte de risco; d) alteração da probabilidade; e) alteração das consequências; f) compartilhamento do risco com outra parte ou partes, e; g) retenção do risco por uma decisão consciente e bem embasada.

É importante que na seleção das opções para o tratamento dos riscos leve-se em conta o equilíbrio entre o risco avaliado e os custos e esforços para implementação do tratamento, bem como, que o próprio tratamento implementado pode gerar novos riscos à organização (ISO, 2009).

A norma FERMA (2002) estabelece os requisitos mínimos para o tratamento de risco, sendo: 1) proporcionar um funcionamento eficaz e eficiente da organização; 2) garantir controles internos eficazes, e; 3) cumprir leis e regulamentos.

Impende destacar que o terceiro requisito da norma FERMA (2002) deve ser adotado em qualquer diretriz sobre gestão de riscos na PMSC, pois, como estamos tratando de administração pública, temos que levar em consideração que somente é permitido ao administrador fazer aquilo que a lei determina (MEIRELES, 2007), portanto, as ações de tratamento adotadas na Corporação devem encontrar amparo na legislação vigente.

As decisões sobre as opções de tratamento devem ser documentadas em um plano de tratamento de riscos. Trata-se de um documento formal que deve incluir: a) as razões para a seleção das opções de tratamento, inclusive os benefícios que se espera obter; b) os responsáveis pela aprovação do plano e os responsáveis pela implementação do plano; c) ações propostas; d) os recursos requeridos, incluindo contingências; e) medidas de desempenho e restrições; f) requisitos para a apresentação de informações e de monitoramento, e; g) cronograma e programação. (IS0, 2009).

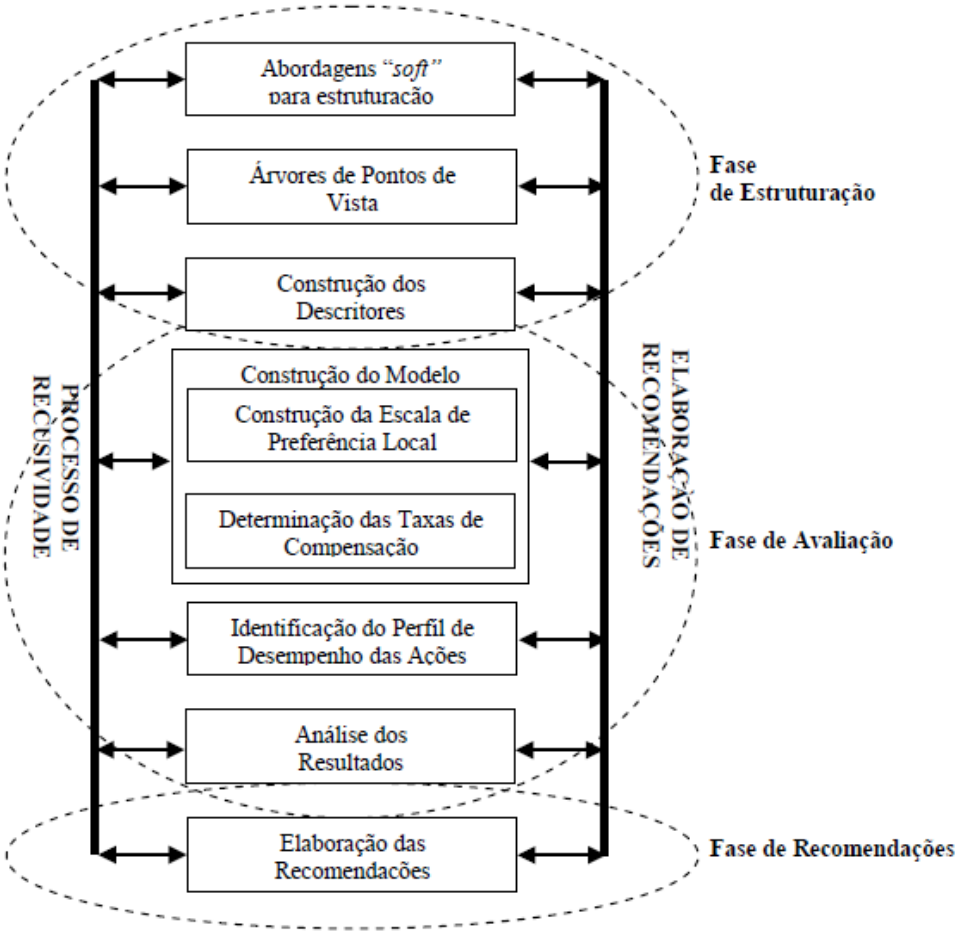
Para tomada de decisão sobre os instrumentos de intervenção, Rosa (2010) sugere o emprego da metodologia multicritério em apoio à decisão – construtivista (MCDA-C), que pressupõe a realização de três macro fases, exposta na Figura 7: fase de estruturação, fase de avaliação e fase de recomendação.

Cada uma das fases estabelecidas pela MCDA-C tem uma finalidade bem delineada, conforme esclarecido por Rosa (2010, p.103):

> A primeira fase destina-se a compreensão do problema e do contexto em que está inserido, por meio da geração do conhecimento nos decisores, representada por uma estrutura hierárquica de valor (KEENEY, 1992) que explicita, de forma estruturada, as preocupações dos envolvidos no processo, a partir das quais as alternativas serão avaliadas. Na segunda fase, com o apoio de um modelo matemático, essas alternativas são, efetivamente, avaliadas. E na terceira e última fase, são propostas ações de aprimoramento daqueles objetivos com maior contribuição no desempenho do contexto avaliado, além de se estabelecer a robustez do modelo construído, mediante a análise de sensibilidade.

A MCDA-C está permeada de subjetividade do decisor, porém, estruturada de forma científica. Sobre isso, Roy e Vanderpoonten (1996 apud ROSA, 2010) destacam a importância de sopesar os interesses, valores e percepções do decisor, além de suas interações com o meio e com o próprio problema.

Figura 7 – Fases do MCDA-C



Fonte: Ensslin et. al (2000) apud Rosa (2010). p. 102.

Ao tratar sobre os critérios para definição das formas de tratamento a serem adotadas na Corporação, o Chefe da Agência de Inteligência da PMSC observou que as recomendações da norma ISO 31.000 (2009) são perfeitamente ajustáveis à realidade e necessidade da PMSC e ressaltou que a metodologia MCDA-C apresenta-se como a mais víavel para delinear as formas de tratamento a serem adotadas, ressaltando que os planos de ação devem ter foco na proteção do policial vítima da ameaça (SILVA, 2018).

2.3.8 Monitoramento e análise crítica

É importante que o processo de gestão de riscos conte com constante monitoramento e análise crítica com a finalidade de:

> - garantir que os controles sejam eficazes e eficientes no projeto e na operação;
> - obter informações adicionais para melhorar o processo de avaliação dos riscos;
> - analisar os eventos (incluindo os “quase incidentes”), mudanças, tendências, sucessos e fracassos e aprender com eles;
> - detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades, e;
> - identificar os riscos emergentes (ISO, 2009, p.20).

Trata-se, portanto, de uma fase que segue do início ao fim do processo de gestão de riscos e que tem finalidade não apenas de controle, mas também de avaliação e correção de desvios. Para Brasiliano (2003) é necessário estabelecer uma fase cíclica de controle e avaliação, devendo-se preocupar em estabelecer padrões, acompanhar os resultados, comparar os resultados atuais com os padrões estabelecidos e tomar ações corretivas para ajustar o desempenho atual ao padrão estabelecido.

Neste sentido, a normatização do monitoramento e análise crítica torna-se imprescindível para o sucesso de um sistema de gestão de riscos para policiais militares ameaçados no âmbito da PMSC, sendo que, para aprimorar a análise, pode ser adotada a participação de um membro externo neste processo, conforme aduz a norma AS/NZS 4360 (2004).

2.3.9 Registro do processo

O registro é necessário para garantir a rastreabilidade do processo de gestão de riscos, para tanto, a norma ISO 31.000 ressalta que decisões sobre a criação de registros devem levar em consideração os seguintes aspectos (ISO, 2009):

> - a necessidade da organização de aprendizado contínuo;
> - os benefícios da reutilização de informações para fins de gestão;
> - os custos e os esforços envolvidos na criação e manutenção de registros;
> - as necessidades de registros legais, regulatórios e operacionais;
> - o método de acesso, facilidade de recuperação e meios de armazenamento;
> - o período de retenção; e
> - a sensibilidade das informações.

Portanto, além de contribuir no aprimoramento do processo de gestão de riscos, os registros são essenciais para tornar o sistema auditável. No âmbito da

PMSC, tendo em vista a natureza pública do órgão, a manutenção de registros trata-se de condição *sine qua non* em qualquer atividade desenvolvida na instituição.

2.4 MODELOS DE GESTÃO DE RISCOS EM OUTRAS INSTITUIÇÕES

2.4.1 Práticas no Tribunal de Justiça de Santa Catarina

Em 2010, percebendo uma profunda mudança na criminalidade tratada pelo Judiciário brasileiro, tornando-se comuns os casos de crimes organizados, corrupção em todas as esferas de poder, tráfico internacional de armas, drogas e pessoas, além de redes de lavagem de dinheiro e, ante ao aumento na frequência de atentados e ameaças contra magistrados, o Conselho Nacional de Justiça (CNJ) regulamentou, por meio da Resolução Nº 104, de 06 de abril de 2010, um série de medidas administrativas para a segurança de magistrados. Dentre elas, a de instituir, nos tribunais, comissões de segurança permanente, e de “elaborar o plano de proteção e assistência dos juízes em situação de risco e conhecer e decidir pedidos de proteção especial, formulados por magistrados. ” (CNJ, 2010).

Em 2013, diante da necessidade de implementar uma política uniforme de segurança institucional e de adotar um programa nacional para segurança de magistrados, o CNJ instituiu o Sistema Nacional de Segurança do Poder Judiciário (SINASPJ). Conforme a Resolução Nº 176, de 10 de junho de 2013, o SINASPJ é constituído pelas Comissões de Segurança Permanente dos Tribunais de Justiça e Militares, dos Tribunais Regionais Federais, Eleitorais e do Trabalho, pelo Comitê Gestor do Conselho Nacional de Justiça e pelo Departamento de Segurança Institucional do Poder Judiciário (DSIPJ), ligado diretamente à presidência do CNJ. Na mesma resolução, o CNJ recomendou que os tribunais se ajustassem ao SINASPJ e criassem suas respectivas comissões de segurança permanente (CNJ, 2013).

Frente às recomendações do CNJ e ao cenário que se impunha, com aumento nos riscos no exercício da magistratura, o Tribunal de Justiça de Santa Catarina (TJSC) criou, em 2014, o Conselho de Segurança Institucional (SANTA CATARINA, TRIBUNAL DE JUSTIÇA DE SANTA CATARINA TJSC, 2014) e, posteriormente, constituiu o Núcleo de Inteligência e Segurança Institucional (NIS),

composto por uma divisão de inteligência e uma divisão de contrainteligência (TJSC, 2018), por meio da Resolução GP Nº 10, de 21 de março de 2018.

Atualmente o NIS é coordenado pelo Desembargador Sidney Eloy Dalabrida, tendo como chefe da divisão de inteligência o Delegado PC Mauro Cândido dos Santos Rodrigues e como chefe da divisão de contrainteligência o Ten Cel PM Emerson Fernandes. O corpo técnico é formado por policiais militares, policiais civis e servidores do TJSC (TJSC, 2018b).

A referida resolução aduz que o principal motivo para criação do NIS foi a necessidade de resguardar a integridade física e psíquica de magistrados e de servidores do Judiciário catarinense, em razão do desempenho de suas funções, em face do cenário de risco oriundo do fortalecimento das facções criminosas e do aumento da violência nas comarcas catarinenses, destacando que:

> o modelo de segurança institucional a ser implantado, por meio do emprego de metodologia específica, é capaz de prestar serviço eficiente de proteção pessoal a magistrados e servidores em potencial ou real situação de risco, bem como exercer controle razoável das vulnerabilidades em torno das estruturas judiciárias críticas; a premência na adoção de medidas tendentes a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da instituição e de seus integrantes, inclusive no que tange a sua imagem e reputação. (TJSC, 2018).

O detalhamento da competência do NIS está exposto no art 3º da Resolução GP Nº 10, de 21 de março de 2018, sendo:

> Art. 3º Compete ao Núcleo de Inteligência e Segurança Institucional:
> I - prestar assessoria ao Presidente do Tribunal de Justiça e ao Conselho de Segurança Institucional nos assuntos relacionados à inteligência e à segurança institucional;
> II - propor ao Conselho de Segurança Institucional a edição de normas de segurança institucional;
> III - cumprir as deliberações do Conselho de Segurança Institucional;
> IV - planejar e executar atividade profissional de proteção de magistrados, seus familiares e de servidores em situação de risco decorrente do exercício da atividade funcional;
> V - implementar e realizar cursos de autoproteção para magistrados e servidores do Poder Judiciário do Estado de Santa Catarina;
> VI - proceder a análises de risco, subsidiando a autoridade competente com conhecimento de inteligência a respeito da segurança institucional;
> VII - elaborar diagnósticos de segurança em torno das instalações do Poder Judiciário do Estado de Santa Catarina;
> VIII - adotar e recomendar medidas de prevenção para redução das vulnerabilidades;
> IX - subsidiar as áreas administrativas responsáveis pela elaboração de projetos de construção e reformas de espaços pertencentes ao Poder Judiciário do Estado de Santa Catarina com conhecimento em segurança institucional;

> X - sugerir a implantação de mecanismos para aprimoramento da segurança institucional em todos os níveis, inclusive quanto à admissão, contratação e desligamento de pessoal;
> XI - adotar as medidas necessárias à fiscalização, detecção, análise, tratamento e correção de incidentes de segurança;
> XII - realizar atividades de inteligência e contrainteligência;
> XIII - fomentar a cultura da segurança institucional entre os membros do Poder Judiciário do Estado de Santa Catarina;
> XIV - desenvolver rotinas de boas práticas em segurança institucional;
> XV - propor ao Conselho de Segurança Institucional a celebração de termos de cooperação e convênios com o Ministério Público, órgãos de segurança pública, defesa nacional, justiça e cidadania, entre outras instituições cujas atribuições estejam alinhadas aos objetivos do Conselho de Segurança Institucional;
> XVI - expedir e praticar os atos administrativos e gerenciais necessários ao exercício de suas atribuições;
> XVII - planejar e realizar cursos e treinamentos de seu quadro de pessoal;
> XVIII - acionar e coordenar as ações da polícia judiciária, no âmbito de suas atribuições, nos casos que envolvam a prevenção ou reação a potencial ou real violação à segurança de magistrados, seus familiares e de servidores, do patrimônio e de dados do Poder Judiciário do Estado de Santa Catarina;
> XIX - atuar junto aos organismos de inteligência e contrainteligência;
> XX - representar o Poder Judiciário do Estado de Santa Catarina nas comissões, comitês, agências, órgãos e grupos relacionados com a atividade de inteligência e segurança institucional;
> XXI - instaurar os procedimentos próprios relacionados à inteligência e segurança institucional;
> XXII - executar outras atividades que lhe forem pertinentes, no âmbito de suas atribuições. (TJSC, 2018, grifo do autor).

Conforme informado pelo Chefe da divisão de contrainteligência do NIS (informação verbal)[2], apesar de a estrutura ter sido criada recentemente, o NIS possui capacidade operacional para realizar análise de riscos em todos os casos em que são identificadas ameaças contra integrantes do Poder Judiciário catarinense, bem como, de propor e adotar medidas de tratamento quando necessárias. Porém, ainda há que se aprimorar o serviço e, justamente por isso, o TJSC está investindo em capacitação de pessoal e aquisição de equipamentos e viaturas para o núcleo, sendo que a visão de futuro é contar com pessoal bem treinado, equipamento e viaturas de ponta para atividade e uma ferramenta de tecnologia da informação que auxilie na análise de riscos, possibilitando a mensuração dos riscos e registro de todas as ações e decisões tomadas.

O Chefe da contrainteligência do NIS mencionou que nos casos de necessidade de serviços de escolta pessoal, o TJSC condiciona a prestação do serviço à assinatura de termo de compromisso pelo magistrado ou servidor ameaçado (ver modelo no Anexo A), conforme Resolução GP Nº 2, de 12 de janeiro

[2] Informações obtidas com Ten Cel PM Emerson Fernandes, chefe da Divisão de Contrainteligência do NIS/TJSC, no dia 10 de outubro de 2018.

de 2016 (TJSC, 2016). Para os casos de dispensa da segurança pessoal, também há a necessidade de assinatura de um termo próprio (ver modelo no Anexo B).

Há que se observar que o NIS segue uma metodologia para realizar análise de riscos. Essa metodologia está formalizada, de forma resumida, em um guia de análise de riscos para magistrados elaborado pelo DSIPJ (CNJ, 2018), onde há instruções de como se mensurar os riscos a partir da análise isolada dos dois fatores descritos como variáveis do risco, ou seja, da ameaça e da vulnerabilidade. A partir da análise destas duas variáveis, o guia recomenda a elaboração de um relatório de análise de riscos, contendo: objeto; objetivo; atividades desenvolvidas e conclusão. Em seguida, conforme o grau de risco, deve-se confeccionar um plano de segurança, com a finalidade de reduzir o risco em três frentes: reduzir o grau de ameaça; reduzir as vulnerabilidades, e; aumentar as capacidades.

O guia do CNJ (2018) exemplifica algumas das medidas de tratamento a serem adotadas a partir da análise de riscos:

> Um plano de segurança, a partir da avaliação de risco, pode propor medidas diversas como: *briefing* de segurança com magistrado e familiares, reforço da segurança orgânica, acionamento da comunidade de inteligência para detectar eventuais ameaças/atentados com relatórios periódicos, disponibilização de números de emergência para pronto atendimento no caso de eventos suspeitos; escolta em deslocamentos pontuais considerados sensíveis; segurança integral 24 horas; escolta diária para deslocamentos a trabalho; restrição de atividades com deslocamentos noturnos, participação em eventos sem controle de acesso, atividades físicas solitárias em locais públicos; mudança de lotação; afastamento temporário das atividades laborais; melhorias decorrentes de análises técnicas na residência e no local de trabalho dos magistrados; instalação de dispositivos, tais como, botão de pânico; vigilância dissimulada; veículos blindados; colete balístico; levantamento de rotas seguras; mudança de rotinas; adoção de procedimentos preventivos.

O mesmo guia ainda sugere que o plano de segurança seja composto por: objetivo; responsável; prazos; medidas de segurança; atividades; ações compartilhadas entre órgãos; ciência e compromisso do protegido com o plano.

Vale mencionar que o CNJ também confeccionou um guia de segurança pessoal para magistrados (CNJ, 2017), com uma série de dicas de medidas de segurança, como no deslocamento a pé ou de carro, no local de trabalho, na vida pessoal, entre outros.

Das práticas observadas pelo TJSC quanto à gestão de riscos de seus integrantes, que podem servir de paradigma para a PMSC, destacam-se:

- Estruturação de um núcleo de segurança institucional responsável diretamente pela atividade, tendo um membro do alto escalão do tribunal como coordenador;

- Normatização da atividade;

- Detalhamento das atribuições;

- Adoção de um guia para análise de riscos específico para integrantes do órgão;

- Descrição das medidas de tratamento;

- Busca por capacitação dos responsáveis pela gestão;

- Investimento em equipamentos e viaturas próprias para o NIS;

- Visão de futuro em contar com pessoal bem treinado, equipamento e viaturas de ponta para atividade e uma ferramenta de tecnologia da informação que auxilie na análise de riscos, possibilitando a mensuração dos riscos e registro de todas as ações e decisões tomadas.

- Adoção de um modelo de termo de compromisso para integrantes do órgão ameaçados (Anexo A);

- Adoção de um modelo de termo de dispensa de segurança pessoal (Anexo B).

2.4.2 Práticas no Ministério Público de Santa Catarina

O MPSC normatizou a Política de Segurança Institucional e o Plano de Segurança Institucional, por meio de atos da Procuradoria Geral de Justiça (informação verbal)[3].

A Política de Segurança Institucional e o Plano de Segurança Institucional do MPSC (PSI/MPSC) foram instituídos por meio do Ato Nº 519/2009/PGJ do MPSC, de 01 de outubro de 2009, e tem, dentre suas finalidades, a salvaguarda de documentos e informações sigilosas e a criação de normas de segurança institucional, orgânica e ativa (SANTA CATARINA, MINISTÉRIO PÚBLICO DE SANTA CATARINA MPSC, 2009).

[3] Informação verbal colhida no dia 15 de outubro de 2018, com Ten Cel PM André Alves, Chefe do setor de Contrainteligência da Coordenadoria de Inteligência e Segurança Institucional do Ministério Público (CISI/MPSC).

O PSI/MPSC estabeleceu competência à Coordenadoria de Inteligência e Segurança Institucional (CISI) para a instauração de procedimento no caso de ameaça a membro ou servidor do Ministério Público, e seus familiares, sendo que para regular os procedimentos de proteção pessoal nestes casos foi editado o Ato 591/2015/PGJ (MPSC, 2015).

O Ato 591/2015/PGJ trata sobre gestão de riscos, especialmente sobre medidas de tratamento a serem adotadas em caso de ameaça a integrantes do MPSC ou familiares:

> Art. 4º Para a gestão do risco, poderão ser efetuados levantamentos de dados e informações, notadamente por meio de entrevistas dos envolvidos e de testemunhas, pesquisas em bases de dados, inspeções locais e contatos com órgãos de segurança e de inteligência de outras instituições.
> Art. 5º Autorizada medida de proteção pessoal, que deverá ser precedida de planejamento técnico, operacional e logístico, os membros, servidores ou familiares beneficiados deverão se submeter às seguintes condições:
> I - evitar exposição desnecessária ou a frequência a ambientes onde possa ser potencializado o risco a que se encontra exposto;
> II - acatar as recomendações estabelecidas pela equipe de segurança designada pela CISI;
> III - informar, com antecedência, a agenda de trabalho e particular à equipe de segurança para possibilitar a avaliação do risco e da conveniência da manutenção da atividade ou sua adequação;
> IV - orientar os familiares, quando for o caso, sobre o cumprimento das recomendações técnicas estabelecidas pela equipe de segurança;
> V - comunicar, de imediato, qualquer situação indicativa de ameaça ou hostilidade;
> VI - retirar perfil e/ou informações constantes de redes sociais, quando for recomendado pela equipe de segurança; e
> VII - prestar todas as informações solicitadas pela equipe de segurança visando à identificação, à neutralização e ao monitoramento da situação de risco;
> Art. 6º Na hipótese de descumprimento das regras de segurança previstas no art. 5º deste Ato, o Coordenador da CISI poderá suspender a medida de proteção adotada, comunicando ao beneficiário e ao Procurador-Geral de Justiça com antecedência.
> Art. 7º De acordo com a gravidade do risco ou da ameaça, além do grau de dificuldade em preveni-la ou neutralizá-la, poderão ser adotadas ainda, isolada ou cumulativamente, entre outras, as seguintes medidas de proteção:
> I - segurança aproximada no local de trabalho;
> II - segurança aproximada na residência;
> III - acompanhamento e segurança aproximada nos deslocamentos relacionados ao desempenho das atividades institucionais;
> IV - acompanhamento e segurança aproximada nos deslocamentos, ainda que não relacionados com o exercício da atividade funcional;
> V - atividade de proteção, cobertura e vigilância; e
> VI - varredura eletrônica e inspeção ambiental. (MPSC, 2015).

Notadamente, a regulamentação do MPSC encontra vários pontos positivos que podem servir de paradigma para PMSC, pois, estabelece competência ao órgão

responsável pela gerência de riscos, no caso a CISI, e padroniza os procedimentos e medidas de tratamento a serem adotadas.

Outro ponto de destaque na gestão de riscos do MPSC voltado à segurança institucional é o uso de uma ferramenta da tecnologia da informação para o registro e análise dos dados.

O MPSC utiliza a plataforma do Sistema de Inteligência Multimercado Neoway (SIMM). Trata-se de uma ferramenta de "*big data*" que reúne, organiza e integra dados de inúmeras fontes e fornece informações para a análise, sendo que, o MPSC contratou serviço de uma empresa especializada para definir os critérios de análise e a ancoragem do sistema, processo realizado com auxílio da MCDA-C. O software analisa um grande volume de dados sobre três aspectos da segurança dos integrantes do MPSC: segurança do local de trabalho; segurança pessoal e histórico de eventos críticos. Esses dados são inseridos no aplicativo "*Security Performance*" e, como resultado da análise, o sistema apresenta dados quantitativos e demonstrações gráficas sobre a segurança do local de trabalho e pessoal dos membros do MPSC, incluindo uma matriz de risco para cada promotor ou procurador de justiça do Estado. O Ten Cel PM André Alves relatou que "o sistema apoia no processo decisório e permite que o CISI atue preventivamente na gestão de riscos e não apenas de forma reativa como ocorria no passado, mas, há que se levar em consideração a dificuldade na coleta de dados, que foi feita *in loco*, nos 179 (cento e setenta e nove) locais de atuação do MPSC em todo o Estado, tarefa que durou quatro meses para ficar pronta. Para a PMSC a sugestão é focar na segurança pessoal dos policiais militares com ameaças identificadas reduzindo o grupo a ser acompanhado e priorizando aqueles que estão em maior risco". (Informação verbal)[4].

Além da análise da performance da segurança dos membros do MPSC, o software disponibiliza o aplicativo "*Security Events Management",* específico para situações críticas. "Nada mais é do que um botão de pânico que pode ser instalado no celular, *tablet*, *notebook* ou *PC*, para fácil acionamento dos meios de resposta em situações de risco de membro do MPSC", conforme explicou o Ten Cel PM André Alves.

[4] Informação verbal colhida no dia 22 de outubro de 2018, com Ten Cel PM André Alves, Chefe do setor de contrainteligência da CISI/MPSC.

Vale dizer que a Política de Segurança Institucional do MPSC foi replicada para todo o país por meio da Resolução Nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público (CNMP), que instituiu a Política de Segurança Institucional do Ministério Público (PSI/MP), prevendo, entre outras atividades, a “atuação preventiva e proativa, de modo a possibilitar antecipação às ameaças e ações hostis e sua neutralização”. (BRASIL, CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO CNMP, 2016).

3 PROCEDIMENTOS METODOLÓGICOS

Elucidar a metodologia adotada, além de obrigação formal em qualquer trabalho monográfico, trata-se de questão essencial para realização do estudo, pois, é imprescindível que a pesquisa seja desenvolvida por meio do “concurso do conhecimento disponível e a utilização cuidadosa de métodos, técnicas e outros processos científicos. ” (GIL, 2002, p.17).

Para o sucesso da pesquisa, “importa, acima de tudo, que o investigador seja capaz de conceber e de pôr em prática um dispositivo para elucidação do real, isto é, no seu sentido mais lato, um método de trabalho. ” (QUIVY; CAMPENHOUDT, 2005, p. 15).

Método, na visão de Lakatos e Marconi (2006, p.86), traduz-se no “conjunto das atividades sistemáticas e reacionais que, com maior segurança e economia, permite alcançar o objetivo – conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista. ”

Buscando delinear diretrizes de um sistema de gestão de riscos para policiais militares ameaçados no âmbito da PMSC, a pesquisa adotou o método de abordagem dedutivo, partindo de uma premissa geral para uma premissa específica.

Quanto ao tipo, a pesquisa foi definida como exploratória que, na visão de Gil (2002, p. 41), tem por “objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou construir hipóteses. ”

A técnica empregada na pesquisa foi, predominantemente, documental e bibliográfica, sendo que a coleta de dados foi realizada principalmente por meio de dados secundários, que são aqueles obtidos, por exemplo, de obras bibliográficas ou de relatórios de pesquisas anteriores sobre o tema (RICHARDSON, 1999).

Segundo Gil (2002, p. 44), pesquisa bibliográfica:

> [...] é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Boa parte dos estudos exploratórios pode ser definida como pesquisas bibliográficas. As pesquisas sobre ideologias, bem como aquelas que se propõem à análise das diversas posições acerca de um problema, também costumam ser desenvolvidas quase exclusivamente mediante fontes bibliográficas. Não obstante, ademais da revisão bibliográfica, será realizada a pesquisa documental, entendida pela pesquisa de materiais que não receberam tratamento analítico.

O período de pesquisa bibliográfica e documental se deu entre agosto e outubro de 2018. Foram pesquisadas obras especializadas e trabalhos acadêmicos nos acervos físicos e digitais das bibliotecas da UDESC, da PMSC e do BMSC, de documentos e dados na ACI/PMSC, no TJSC e no MPSC, além dos materiais de aula do CAEE/2018, principalmente, da disciplina de Inteligência de Segurança Pública. Foram pesquisados trabalhos acadêmicos nos acervos digitais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Ainda foram realizadas pesquisas a documentos, legislação e dados diversos, principalmente, pela intranet da PMSC e pelo site da ALESC.

As palavras-chave utilizadas para pesquisa nas plataformas de buscas digitais, especialmente da CAPES, foram “gerenciamento de risco” e seu correspondente em inglês “*risk management*”, além de outros termos para buscas a documentos ou leis específicas.

Não obstante, foram realizadas coletas de dados primários, por meio do questionário de pesquisa juntado no apêndice A, destinado a levantar dados sobre as ameaças contra policiais militares em Santa Catarina registradas nos últimos doze meses, correspondente ao período de outubro de 2017 a setembro de 2018.

O questionário foi enviado no dia 27 de setembro de 2018, através do aplicativo google *forms,* para as 35 (trinta e cinco) AI de batalhões e guarnições especiais da PMSC, cuja área de circunscrição corresponde a todo o território do Estado.

O prazo para a resposta foi estipulado inicialmente até o dia 04 de outubro de 2018, porém, com o objetivo de colher o maior número de dados, houve prorrogação do prazo de resposta até dia 17 de outubro de 2018, sendo que todas as AI responderam ao questionário.

Na seção 4.2.3 deste trabalho foram apresentados os dados coletados na pesquisa e as análises das respostas.

4 CARACTERIZAÇÃO, DIAGNÓSTICO E ANÁLISE DA REALIDADE ESTUDADA

Esse capítulo será dividido em três seções, a fim de buscar a caracterização, o diagnóstico e a análise da realidade estudada.

A primeira destina-se a estabelecer uma caracterização da Polícia Militar de Santa Catarina, demonstrando alguns dados da organização, sua missão constitucional e contextualizando o serviço de inteligência, responsável pela segurança orgânica da Corporação.

A segunda busca identificar as facções criminosas que atuam no Estado, descrever as cinco séries de atentados praticadas por facções criminosas em Santa Catarina e, ainda, apresentar dados sobre ameaças contra policiais militares registradas nos últimos doze meses pelas AI da Corporação.

A última seção visa analisar os modelos de gestão de riscos descritos no referencial teórico do presente trabalho, a fim de identificar o modelo que melhor atenda às necessidades da PMSC frente à realidade atual da instituição e do detalhamento do problema descrito.

4.1 A POLÍCIA MILITAR DE SANTA CATARINA

A Polícia Militar de Santa Catarina, órgão da administração direta do Estado, vinculada à Secretaria da Segurança Pública, foi criada em 05 de Maio de 1835 pelo então Presidente da Província de Santa Catarina, Feliciano Nunes Pires. O ato de criação, Lei Provincial Nº 12, denominou a Corporação como Força Policial e atribuiu como missão a manutenção da ordem e da tranquilidade pública, bem como, de atender às requisições judiciárias e policiais. A motivação política da criação da "Força Policial" foi a necessidade de substituir os Corpos de Guardas Municipais Voluntários, então considerados ineficazes (SANTA CATARINA, POLÍCIA MILITAR DE SANTA CATARINA PMSC, 2018).

Apesar da descrição sucinta da missão da Corporação, a PMSC, desde sua criação, sempre teve uma missão ampla e complexa. Ainda no período do Império a Força Policial atuava no atendimento de ocorrências policiais de natureza mais simples, como vias de fato e desentendimentos, no patrulhamento das ruas visando à manutenção da ordem pública, cumprindo ordens judiciais, e até em apoio ao

Exército Brasileiro, em conflitos internos e externos, tais como a Guerra dos Farrapos e a Guerra do Paraguai (PMSC, 2018).

Com o passar do tempo, as missões da PMSC só fizeram aumentar em número e complexidade. Algumas atribuições tornaram-se tão específicas e complexas que deram origem a divisões especializadas dentro da Instituição, como é o caso da Polícia Militar Ambiental, da Polícia Militar Rodoviária e do Batalhão de Aviação da Polícia Militar.

O entendimento sobre a atual missão, da relevância e amplitude dos serviços prestados pela PMSC, revestem-se de especial importância para a compreensão das características da Corporação, o que é essencial para o presente estudo, motivo pelo qual será exposta a missão constitucional e legal da PMSC.

4.1.1 Missão constitucional e legal

Atualmente a missão da Polícia Militar de Santa Catarina está definida na CRFB, em leis esparsas e na Constituição do Estado de Santa Catarina.

Na CRFB (Constituição da República Federativa do Brasil CRFB, 1988), a missão das polícias militares é definida da seguinte forma:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal;
> II - polícia rodoviária federal;
> III - polícia ferroviária federal;
> IV - polícias civis;
> V - polícias militares e corpos de bombeiros militares.
> [...]
> § 5º Às polícias militares cabem a polícia ostensiva e a preservação da ordem pública; aos corpos de bombeiros militares, além das atribuições definidas em lei, incumbe a execução de atividades de defesa civil.

A CRFB/1988 inaugurou a expressão polícia ostensiva justamente para conferir exclusividade à Polícia Militar e determinar a ampliação da competência das polícias militares que, até então, realizavam apenas o policiamento ostensivo. Com isso as polícias militares brasileiras ganharam autorização constitucional para atuar nas quatro fases do exercício de poder de polícia: a ordem de polícia, o consentimento de polícia, a fiscalização de polícia e a sanção de polícia (TEZA, 2011).

Portanto, a atribuição das polícias militares de polícia ostensiva é bem mais ampla do que a atividade de policiamento ostensivo, pois, esta atua em apenas uma das fases do poder de polícia (a fiscalização), conforme definição do Decreto 88.777, R-200 (BRASIL, 1983):

> O policiamento ostensivo é ação exclusiva das Polícias Militares em cujo emprego o homem ou fração de tropa engajados sejam identificados de relance, quer pela farda quer pelo equipamento, ou viatura, objetivando a manutenção da ordem pública. São tipos desse policiamento, a cargo das Polícias Militares ressalvadas as missões peculiares das Forças Armadas, os seguintes:
> - ostensivo geral, urbano e rural;
> - de trânsito;
> - florestal e de mananciais;
> - rodoviário e ferroviário, nas estradas estaduais;
> - portuário;
> - fluvial e lacustre;
> - de radiopatrulha terrestre e aérea;
> - de segurança externa dos estabelecimentos penais do Estado.

Por seu turno, o art. 3º do Decreto-Lei 667, de 02 de julho de 1969, que reorganizou as Polícias Militares e os Corpos de Bombeiros Militares dos Estados e do Distrito Federal, atribuiu às Polícias Militares a manutenção da ordem pública e a exclusividade do policiamento ostensivo fardado:

> Art. 3º - Instituídas para a manutenção da ordem pública e segurança interna nos Estados, nos Territórios e no Distrito Federal, compete às Polícias Militares, no âmbito de suas respectivas jurisdições:
> a) executar com exclusividade, ressalvas as missões peculiares das Forças Armadas, o policiamento ostensivo, fardado, planejado pela autoridade competente, a fim de assegurar o cumprimento da lei, a manutenção da ordem pública e o exercício dos poderes constituídos;
> b) atuar de maneira preventiva, como força de dissuasão, em locais ou áreas específicas, onde se presuma ser possível a perturbação da ordem;
> c) atuar de maneira repressiva, em caso de perturbação da ordem, precedendo o eventual emprego das Forças Armadas;
> d) atender à convocação, inclusive mobilização, do Governo Federal em caso de guerra externa ou para prevenir ou reprimir grave perturbação da ordem ou ameaça de sua irrupção, subordinando-se à Força Terrestre para emprego em suas atribuições específicas de Polícia Militar e como participante da Defesa Interna e da Defesa Territorial;
> e) além dos casos previstos na letra anterior, a Polícia Militar poderá ser convocada, em seu conjunto, a fim de assegurar à Corporação o nível necessário de adestramento e disciplina ou ainda para garantir o cumprimento das disposições deste Decreto-lei, na forma que dispuser o regulamento específico. (BRASIL, 1969)

Quanto ao conceito de ordem pública, muitos autores apresentam ideias bastante simplistas, afirmando que se trata da “ausência de desordem, a paz, de

que resultaram a incolumidade de pessoa e do patrimônio". (FERREIRA FILHO, 1994, p. 82 apud LAZZARINI, 2003, p. 143).

Para Lazzarini (1999), ordem pública traz um conceito vago e amplo, que vai muito além da manutenção da ordem nas ruas, mas que envolve uma determinada ordem moral que garanta o mínimo de condições essenciais à vida em sociedade, sendo constituída dos seguintes elementos: segurança dos bens e das pessoas, da salubridade e a tranquilidade.

O panorama sobre ordem pública exposto por Lazzarini teve uma evolução na visão de Nazareno Marcineiro, que acrescentou a dignidade da pessoa humana como elemento da ordem pública. Vejamos os conceitos dos elementos constitutivos da ordem pública na visão destes dois autores:

> SEGURANÇA PÚBLICA, que é o estado antidelitual que resulta da observância dos preceitos tutelados pelos códigos penais comuns e pela lei das contravenções penais com ações de polícia preventiva ou repressiva típicas (...);
> TRANQÜILIDADE PÚBLICA, que exprime o estado de ânimo tranquilo, sossegado, sem preocupações nem incômodos. Que traz às pessoas uma serenidade, uma paz de espírito;
> SALUBRIDADE PÚBLICA, cuja expressão designa, também, o estado de sanidade e de higiene de um lugar, em razão de qual se mostram propícias às condições de vida de seus habitantes, e;
> DIGNIDADE DA PESSOA HUMANA, que vem aflorando em recentes debates internacionais, visa atribuir ao Estado, no uso do seu poder de polícia, restringir a possibilidade de alguém se sujeitar ou sujeitar alguém a situação aviltante ou constrangedora, em nome da preservação da dignidade da pessoa humana. (LAZZARINI apud MARCINEIRO, 2009, p. 76).

Na legislação estadual, a missão da PMSC está consubstanciada no art. 107 da Constituição do Estado de Santa Catarina, que traz uma série de atribuições que demonstram a amplitude da competência da instituição e a importância dos serviços prestados para o povo barriga verde:

> Art. 107 — À Polícia Militar, órgão permanente, força auxiliar, reserva do Exército, organizada com base na hierarquia e na disciplina, subordinada ao Governador do Estado, cabe, nos limites de sua competência, além de outras atribuições estabelecidas em Lei:
> I - exercer a polícia ostensiva relacionada com:
> a) a preservação da ordem e da segurança pública;
> b) o radiopatrulhamento terrestre, aéreo, lacustre e fluvial;
> c) o patrulhamento rodoviário;
> d) a guarda e a fiscalização das florestas e dos mananciais;
> e) a guarda e a fiscalização do trânsito urbano;
> f) a polícia judiciária militar, nos termos de lei federal;

> g) a proteção do meio ambiente; e Φ ADI Nº 5520 ∗ EC nº 33 – art. 107 (NR) ∗ EC nº 63 – §§ 3º e 4º do art. 107 (AC) - 99 –
> h) a garantia do exercício do poder de polícia dos órgãos e entidades públicas, especialmente da área fazendária, sanitária, de proteção ambiental, de uso e ocupação do solo e de patrimônio cultural;
> II - cooperar com órgãos de defesa civil; e
> III - atuar preventivamente como força de dissuasão e repressivamente como de restauração da ordem pública. (SANTA CATARINA, 1989).

Visando cumprir a missão institucional e buscando atender às necessidades do povo Catarinense, ao longo do tempo a PMSC instalou quartéis e implementou serviços especializados em todo território de Santa Catarina. A seguir serão apresentados dados gerais sobre o efetivo da instituição.

4.1.2 Efetivo

Após uma breve visão sobre a missão e as atribuições da PMSC fica claro que a Instituição precisa contar com uma estrutura reforçada e bem articulada, condizente com a complexidade da missão que lhe foi atribuída.

Atualmente, a PMSC conta com 10.348 (dez mil e trezentos e quarenta e oito) policiais militares na ativa que trabalham nos 295 (duzentos e noventa e cinco) municípios do Estado. Além disso, há 1.464 (um mil e quatrocentos e sessenta e quatro) policiais militares da reserva remunerada contratados pelo programa CTISP[5] e 191 (cento e noventa e um) Ag Temp[6]. Há ainda que se considerar que o total de inativos[7] chega a 9.277 (nove mil e duzentos e setenta e sete), já incluídos os inativos do programa CTISP (informação verbal[8])

Considerando que qualquer integrante da instituição, quer seja ele policial militar da atividade ou inatividade, do CTISP ou Ag Temp, está suscetível a sofrer ameaças em razão da função que exerce ou exerceu, quanto maior o número de efetivo, maior será a complexidade da tarefa da gestão de riscos para policiais militares ameaçados, motivo pelo qual é necessário um sistema eficiente, que conte

[5] O CTISP é regulado pela Lei Complementar Nº 380, de 03 de maio de 2007, e, na polícia militar, é formado por policiais militares da inatividade, contratados em caráter temporário para executar funções de guarda, assessoria e outras previstas na legislação (SANTA CATARINA, 2007).
[6] São jovens, de 18 a 23 anos, contratados por certame público para atender às demandas das Centrais de Emergências, Centrais de Vídeomonitoramento e Serviços Administrativos nas OPM, em caráter temporário (um ano, prorrogável por mais um) sendo denominados de Agentes Temporários de Serviço Administrativo (SANTA CATARINA, 2005).
[7] Para os militares estaduais não há aposentadoria, estando previsto na legislação as situações de inatividade: reserva remunerada e reforma (SANTA CATARINA, 2007).
[8] Informação verbal coletada no dia 13 de outubro de 2018, com Major PM Marcus Vinicius dos Santos, Chefe do setor de gerenciamento de recursos humanos da PMSC.

com ferramentas da tecnologia da informação e evite o dispêndio de recursos em medidas de tratamento desnecessárias.

4.1.3 Organograma e articulação

Os órgãos que compõe o organograma da Corporação são os de: comando-geral, direção setorial, órgãos de apoio, coordenadorias, órgãos de execução e órgãos de execução especializados[9].

Órgãos de comando-geral: Comando-Geral, Subcomando-Geral e Estado Maior-Geral.

Órgãos de direção setorial: Agência Central de Inteligência (ACI), Centro de Comunicação Social (CCS), Corregedoria-Geral (CORREG G), Diretoria de Apoio Logístico e Finanças (DALF), Diretoria de Instrução e Ensino (DIE), Diretoria de Pessoal (DP), Diretoria de Saúde e Promoção Social (DSPS), Diretoria de Tecnologia da Informação (DTI).

Órgãos de apoio: Academia de Polícia Militar da Trindade (APMT), Centro de Formação e Aperfeiçoamento de Praças (CFAP), Centro de Armazenamento e Distribuição (CAD), Centro de Material Bélico (CMB), Centro de Motomecanização e Transporte (CMT), Centro de Engenharia (CENG), Centro de Seleção, Ingresso e Estudos de Pessoal (CESIEP), Colégio Policial Militar Feliciano Nunes Pires (unidades em Florianópolis, Lages, Joinville e Blumenau), Museu Lara Ribas e Hospital da Polícia Militar (HPM).

Coordenadorias: Coordenadoria Estadual do Proerd[10] e Coordenadoria Estadual do SOS Desaparecidos.

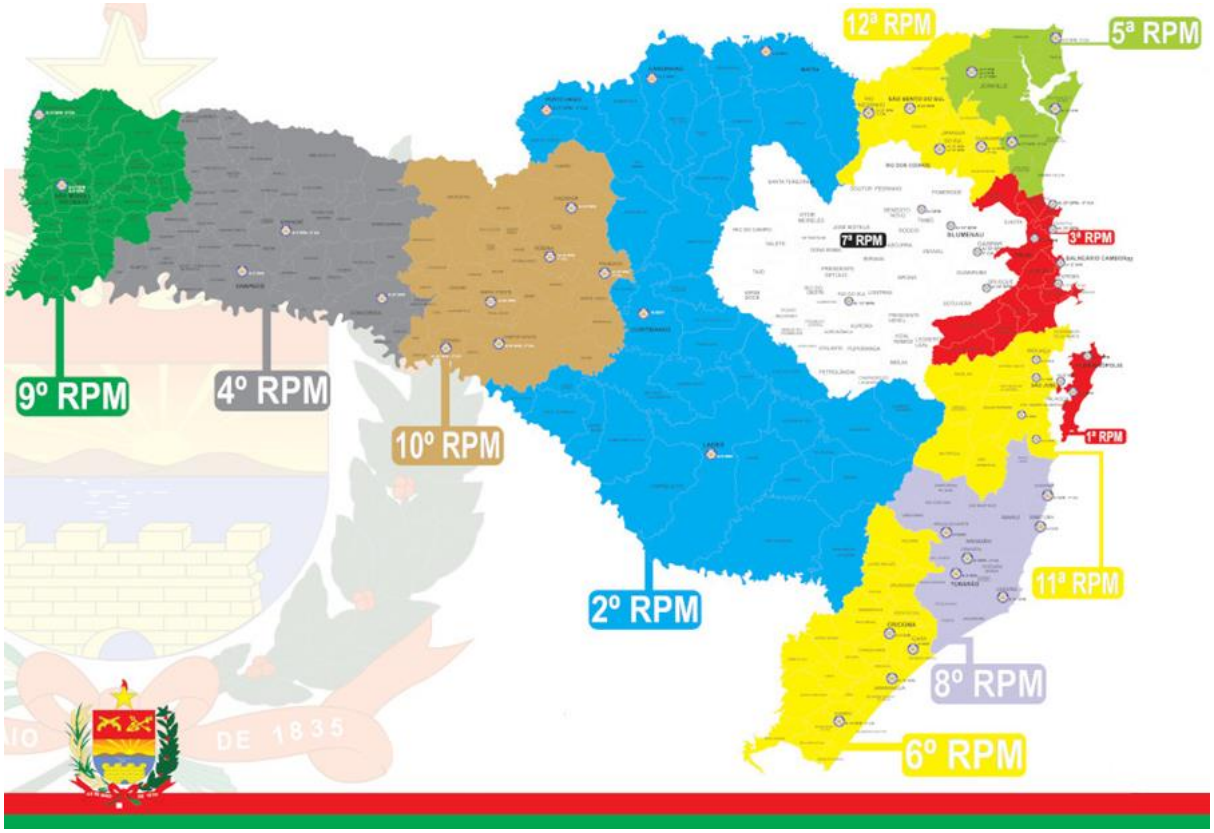
Órgãos de execução: 12 (doze) Regiões Policiais Militares, composta por batalhões ou guarnições especiais, companhias, pelotões e grupamentos e Comandos especializados. Estes órgãos operacionais estão instalados em praticamente todos os municípios de Santa Catarina, sendo que há municípios há várias OPM instaladas. A figura 8 representa a articulação atual da PMSC e facilita a visualização da divisão territorial do Estado em circunscrições regionais.

---

[9] A Lei de Organização Básica da PMSC (LOB) carece de atualização, sendo que há um projeto de LOB pronto no Estado Maior Geral. As informações desta seção são do conhecimento empírico do autor.

[10] Programa Educacional de Resistência às Drogas e à Violência.

Figura 8: Articulação da PMSC em Regiões de Polícia Militar



Fonte: Silva (2018).

Ainda há os órgãos de execução especializados:

Comando de Polícia Militar Rodoviária (CPMR): 1º Batalhão de Polícia Militar Rodoviária (1º BPMRv – Florianópolis), 2º Batalhão de Polícia Militar Rodoviária (2º BPMRv – Lages).

Comando de Polícia Militar Ambiental (CPMA – Florianópolis), 1º Batalhão de Polícia Militar Ambiental (1º BPMA – Florianópolis), 2º Batalhão de Polícia Militar Ambiental (2º BPMA – Chapecó) e Batalhão de Ajuda Humanitária (BAH – Florianópolis).

Comando de Apoio Especializado da Polícia Militar (CAEPM): Batalhão de Aviação da Polícia Militar (BAPM – Florianópolis), Batalhão de Operações Policiais Especiais (BOPE - São José), Companhia de Policiamento com Cães (Cia Pol Cães - São José), Regimento de Polícia Militar Montada de Santa Catarina (RPMMon - São José) e Grupamento de Polícia de Choque (GPChq – Florianópolis).

Assim como a quantidade de efetivo, o número e a distribuição geográfica das OPM serão desafios para atividade de gestão de riscos, pois, dificultará a execução de medidas de tratamento e, até mesmo, a análise de riscos, a exemplo da

verificação de vulnerabilidades do local de trabalho ou de aspectos da vida do ameaçado.

4.1.4 A atividade de inteligência na PMSC

Em âmbito nacional, a atividade de inteligência é regulada pela Lei Nº 9.883, de 07 de dezembro de 1999, que instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência (ABIN) no centro do sistema (BRASIL, 1999), sendo que, à luz da referida 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.

O SISBIN é composto de diversos órgãos e pontos de interesse, sendo que o Subsistema de Inteligência de Segurança Pública (SISP) é apenas uma das ramificações do sistema.

A Doutrina Nacional de Inteligência de Segurança Pública (DNISP) conceitua a atividade de Inteligência de Segurança Pública (ISP) da seguinte forma:

> A atividade de Inteligência de Segurança Pública (ISP) é o exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisão, para o planejamento e execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que atentem à ordem pública, à incolumidade das pessoas e do patrimônio. (BRASIL, 2016).

O SISP tem seu órgão central na Coordenação-Geral de Inteligência da SENASP e destina-se a fornecer informações “aos respectivos governos para a tomada de decisões no campo da segurança pública, mediante a obtenção, análise e disseminação da informação útil, e salvaguarda da informação contra acessos não autorizados. ” (SILVEIRA, 2012, p. 30).

Para tanto, o SISP promove a integração entre parceiros estratégicos como órgão de defesa (Ministério da Defesa e Forças Armadas) órgão de Segurança Pública, (federais e estaduais, Polícia Federal, Polícia Rodoviária Federal, Polícias

Militares, Polícias Civis), departamentos de administração prisional, órgãos de segurança internacionais, entre outros (SILVEIRA, 2012).

A PMSC conta com seu próprio sistema de inteligência, o SIPOM, o qual tem a finalidade de:

> "integrar as ações de planejamento e execução da atividade de inteligência na Polícia Militar de Santa Catarina, com a finalidade de subsidiar as decisões do comando da Polícia Militar, em todos os níveis, nos assuntos de interesse institucional, atinentes às ações de polícia ostensiva e relativos à preservação da ordem pública. (SANTA CATARINA, POLÍCIA MILITAR DE SANTA CATARINA PMSC, 2018b)

O órgão central do SIPOM é a Agência Central de Inteligência (ACI). A ACI foi criada pela Portaria Nº 204 de 29 de maio de 2002 e está vinculada diretamente ao Comando-Geral da PMSC, principal usuário/destinatário de seu produto final (informação qualificada). Não obstante, a ACI também está ligada, por canal técnico[11], a todas as Agências de Inteligência[12] da Corporação, à 2ª Seção do Estado Maior[13] da PMSC (PM-2) e a todos agentes de inteligência da Corporação, uma vez que todos integram o sistema (SILVA, 2018).

Conforme organograma exibido na Figura 9, atualmente o SIPOM conta com 63 (sessenta e três) Agências de Inteligência, sendo: 51 (cinquenta e uma) Agências de OPM Operacional (Batalhão, Cia ou Pelotão), 08 (oito) Agências-Regionais, 03 (três) Agências Especiais (ligadas aos Comandos Especializados[14] ou assessorias[15]) e a Agência Central.

---

[11] Canal técnico é a denominação dada à comunicação entre Agências de Inteligência de um mesmo sistema ou da Agência Central de um determinado Sistema (ou subsistema) com Agências do mesmo sistema ou, ainda, da comunicação entre agências centrais de sistemas (ou subsistemas) diversos, sem que haja necessidade da tramitação da comunicação/documentação pelos canais hierárquicos convencionais da administração pública (SILVA, 2018). A comunicação é realizada normalmente por meio de um documento de inteligência (pedido de busca, relatório de inteligência, entre outros).

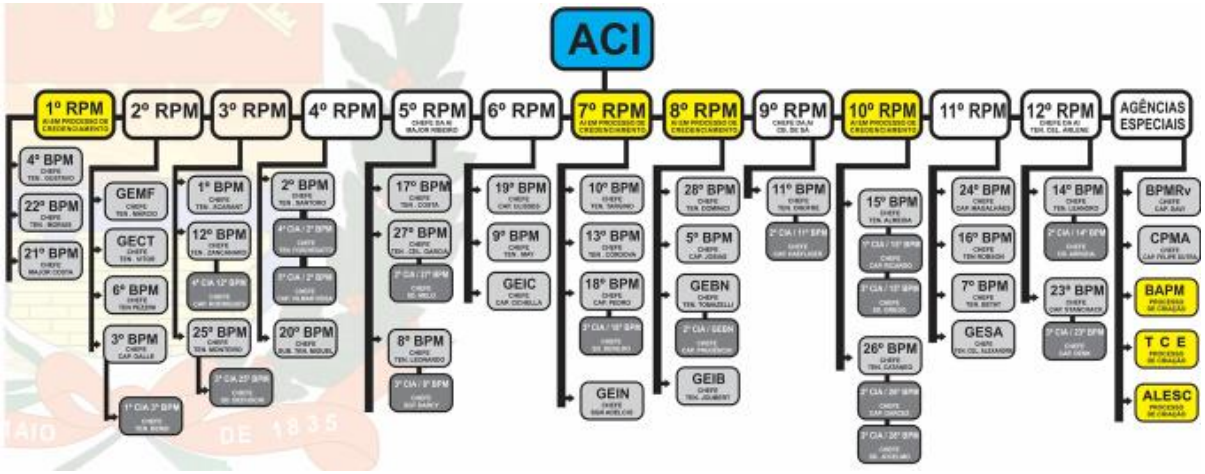
[12] As Agências de Inteligência (AI), são órgãos voltados à produção de conhecimento e assessoramento nos diversos níveis dentro da estrutura da Polícia Militar, desde que devidamente credenciadas ao SIPOM (PMSC, 2018b).

[13] A 2ª Seção do Estado Maior (PM-2), subordinada diretamente ao Chefe do Estado Maior, tem por objetivo o assessoramento nos campos econômico, político, psicossocial e militar de interesses da Corporação; planejamento estratégico e coordenação dos trabalhos de elaboração e atualização das normas referentes à atividade de inteligência (PMSC, 2018b).

[14] Batalhão de Polícia Militar Rodoviária e Comando de Polícia Militar Ambiental. No Batalhão de Avião da Polícia Militar a AI está em criação (SILVA, 2018).

[15] Foi implementada a agência do Tribunal de Contas do Estado (TCE) e está em implementação da AI da Assembleia Legislativa de Santa Catarina (ALESC). Também há tratativas para criação no Tribunal de Justiça de Santa Catarina (TJSC) e no Ministério Público de Santa Catarina (MPSC), conforme Silva (2018).

Figura 9: Organograma das AI da PMSC



Fonte: Slide de aula de Inteligência de Segurança Pública do CAEE/2018 (SILVA, 2018, p. 83)

Impende mencionar que, em razão do caráter sigiloso do serviço de inteligência não serão exibidos neste trabalho dados que possam colocar em risco a atividade ou seus integrantes, tais como: número de efetivo da inteligência, detalhes sobre recursos materiais e dados que possam tornar identificáveis os integrantes do serviço de inteligência (nomes, características de veículos, endereços, entre outros).

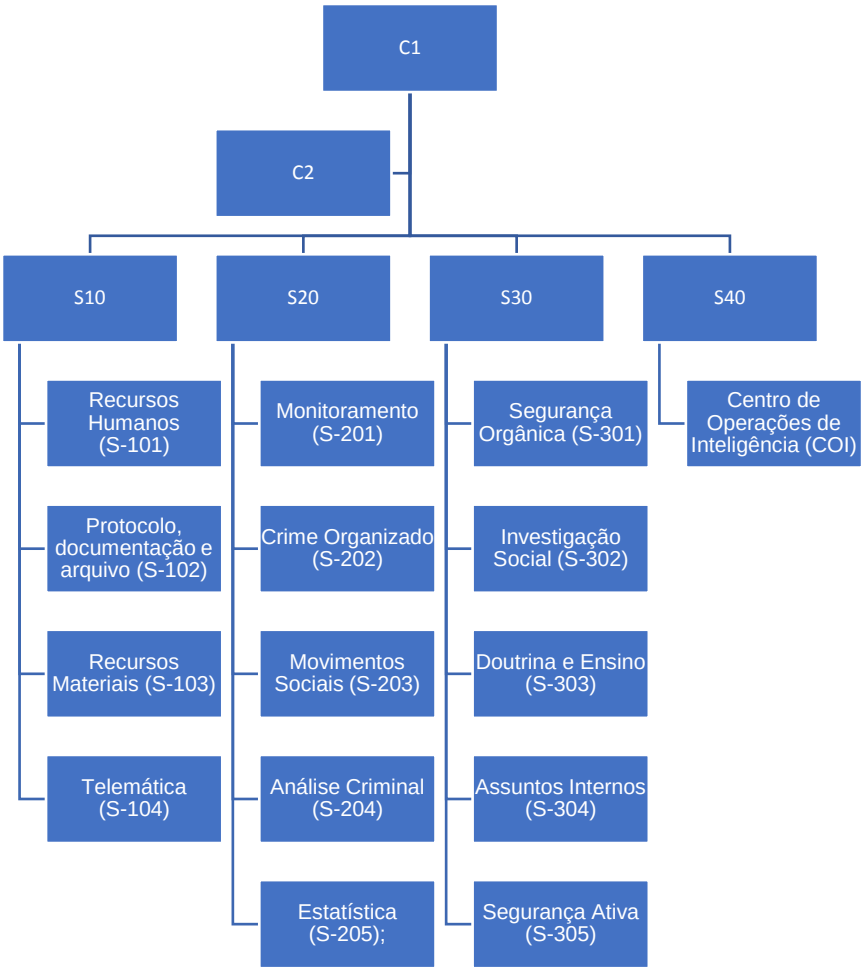
Entretanto, sobre os recursos e estrutura do sistema destaca-se que a ACI é a única agência do Estado com uma estruturação completa, fato que permite a divisão das atividades que fazem parte do serviço de inteligência, sendo subdividia da seguinte forma (SILVA, 2018):

- Chefia (C1)
- Subchefia (C2)
- Seção de Apoio Administrativo (S10)
- Seção de Inteligência (S20)
- Seção de Contrainteligência (S30)
- Centro de Operações de Inteligência (S40 - COI)

Nas demais AI da PMSC geralmente não há divisão tão clara de atividades e, muitas vezes, o mesmo agente é empregado nas atividades de inteligência e contrainteligência (SILVA, 2018).

Na Figura 10 está exposto o organograma interno da ACI.

Figura 10: Organograma interno da ACI



Fonte: Adaptado pelo autor de Silva (2018).

4.1.4.1 A contrainteligência

A ISP possui dois ramos de atividades: inteligência e contrainteligência. Enquanto a inteligência está voltada à produção de conhecimentos de interesse da Segurança Pública, a contrainteligência dedica-se a proteger a informação produzida de acessos não autorizados, a proteger a própria atividade de inteligência e seus integrantes, a proteger a instituição a que pertence e os profissionais que fazem parte, bem como, em produzir conhecimentos para neutralizar a inteligência adversa (SILVEIRA, 2012).

A Portaria 229/PMSC/2018 (PMSC, 2018c) trata a atividade de contrainteligência no âmbito da PMSC da seguinte forma:

> É o ramo da atividade de Inteligência que objetiva prevenir, detectar, obstruir, neutralizar e reprimir a inteligência adversa, bem como ações de

> qualquer natureza que constituam ameaça à salvaguarda de dados e conhecimento de interesse da segurança da sociedade e da instituição.

Conforme a Portaria Nº 229/PMSC/2018, que estabeleceu a diretriz de inteligência da PMSC, são segmentos da contrainteligência: Segurança orgânica, segurança ativa e assuntos internos (SILVA, 2018).

Para fins do presente estudo o interesse recai sobre a segurança orgânica, definida na Portaria Nº 229/PMSC/2018 (PMSC, 2018c), como sendo “o conjunto de normas, medidas e procedimentos de caráter eminentemente defensivo, destinado a garantir o funcionamento da instituição, de modo a prevenir e obstruir as ações adversas de qualquer natureza.”

A segurança orgânica envolve a segurança de pessoal, das instalações, das operações de inteligência, da documentação, da tecnologia da informação, das comunicações e do material (SILVA, 2018).

Por seu turno, a segurança de pessoal pode ser definida da seguinte forma:

> “Conjunto de medidas objetivamente voltadas para os recursos humanos, no sentido de assegurar comportamentos adequados à salvaguarda de conhecimentos e/ou dados sigilosos, e tem por finalidade, particularmente, prevenir e obstruir as ações adversas de infiltração, recrutamento e entrevista.” (SILVEIRA, 2012).

Portanto, conclui-se que na estrutura do serviço de inteligência, cabe à contrainteligência a produção de conhecimento voltada à proteção da instituição e de seus integrantes, devendo recair a este ramo de atividade a gestão de riscos de policiais militares ameaçados.

Ademais, da análise do serviço de Inteligência da PMSC, constatou-se que o serviço possui capilaridade por todo Estado, estando presente em todos os Batalhões e algumas OPM de outros níveis (regionais, companhias, etc.), bem como, que possui uma Agência Central bem estruturada, vinculada diretamente ao Comando-Geral da Corporação e com ligação a todos os demais agentes e agências do SIPOM por meio de canal técnico, fato que dá agilidade ao sistema.

4.2 ENTENDENDO O CONTEXTO DA SITUAÇÃO-PROBLEMA

Esta seção será destinada a detalhar a situação-problema, identificando as facções criminosas que atuam em Santa Catarina, expondo as cinco séries de

atentados praticados por facções criminosas contra integrantes das forças de segurança do Estado e as ameaças contra policiais militares registradas no último ano pelas Agências de Inteligência da PMSC. Com isso, pretende-se entender os impactos da atuação das facções criminosas na segurança pessoal dos policiais militares, verificar a dimensão do problema e relacionar os métodos de tratamento de risco que são empregados atualmente pelas OPM.

4.2.1 As facções criminosas atuantes em Santa Catarina

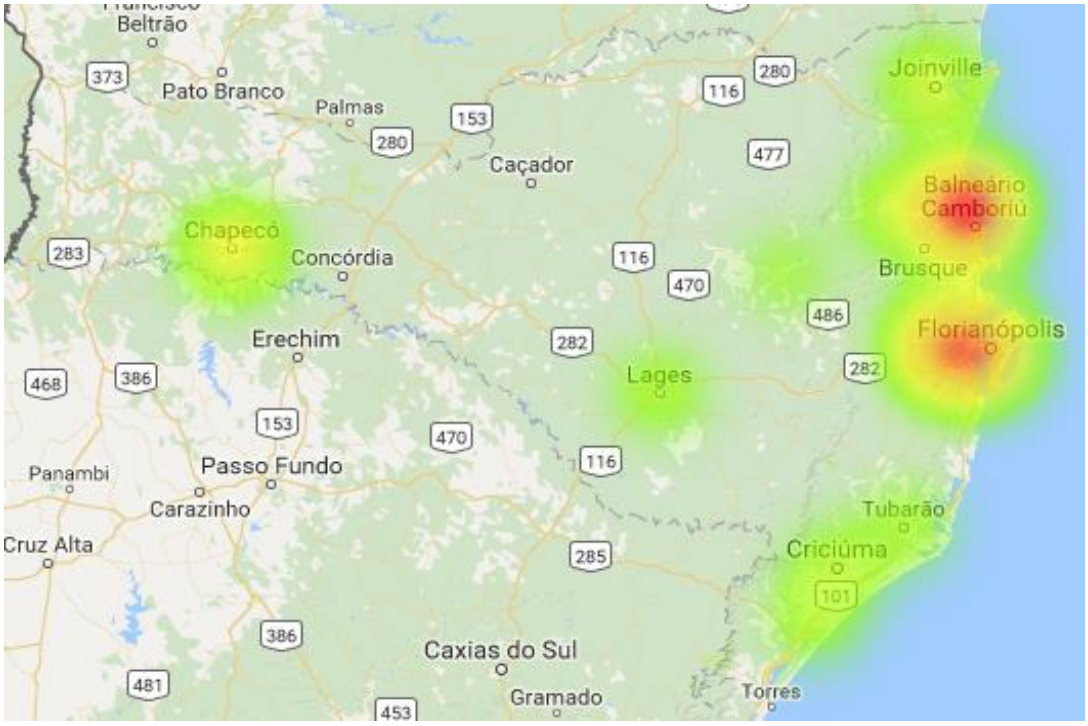
O Comando Vermelho (CV) despontou em 1979, como a primeira facção criminosa do Brasil. Seu surgimento ocorreu na unidade prisional de Cândido Mendes, no Estado do Rio de Janeiro, numa junção de criminosos e presos políticos. O CV chegou a ser considerada a maior organização criminosa do país - e ainda é a maior do Rio de Janeiro -, porém, com o passar do tempo surgiram grupos dissidentes, que se tornaram rivais e diminuíram o poder criminoso do CV. O CV está concentrado no Rio de Janeiro, tendo alguns poucos membros (geralmente presos) em outros estados, porém, em 2009 o CV realizou parceria com o Primeiro Grupo Catarinense (PGC) em Santa Catarina (COSTA, 2014) .

Atualmente, o Primeiro Comando da Capital (PCC), em razão da sua capacidade financeira, alto grau de organização das práticas criminosas e do seu poder bélico, é julgado pelos serviços de inteligência como a maior organização criminosa do Brasil. Apesar de ter sido criado na Casa de Custódia de Taubaté, unidade prisional que fica a 180 km da cidade de São Paulo, em 31 de agosto de 1993, o PCC ganhou capilaridade por todo território nacional e possui membros em Santa Catarina (a maioria presos), porém, em Santa Catarina a facção criminosa com maior número de afiliados é o PGC. Até 2014 o PCC e o PCG mantinham boas relações. Neste ano as referidas facções tornaram-se rivais, sendo que o PGC se aproximou do CV (SILVA, 2018).

O PGC foi criado em 03 de março de 2003, na ala de segurança máxima da penitenciária de Florianópolis, alinhando-se às ideologias do CV e do PCC. Posteriormente, as lideranças do PGC foram transferidas para o Complexo Penal no município de São Pedro de Alcântara, que passou a ser o quartel general da facção. No ano de 2007, após uma série de mortes no complexo de São Pedro de Alcântara, treze presos, líderes do PGC, foram transferidos para unidades prisionais federais,

onde tiveram contato com líderes do CV e PCC. No ano seguinte a liderança do PGC retornou a Santa Catarina, entretanto, manteve os contatos com as facções criminosas do Rio de Janeiro e São Paulo. Com isso houve um crescimento da facção, tanto dentro, quanto fora das unidades prisionais (COSTA, 2014; SILVA, 2018). A Figura 11 demonstra os municípios com maior incidência de atuação do PGC nas unidades prisionais.

Figura 11 – Mapa de incidência da atuação do PGC em unidades prisionais do Estado



Fonte: Slide de aula de Inteligência de Segurança Pública (SILVA, 2018).

A facção denominada Primeiro Comando Revolucionário Catarinense (PCRC) foi fundada em 2012, no Presídio de Joinville, na chamada “galeria do seguro”, onde são alocados presos ameaçados pelos demais reeducandos. Até o momento, já foram registrados membros do PCRC em nove presídios de Santa Catarina, demonstrando crescimento desta facção, sendo que a liderança está dividida nos presídios de Joinville e Itajaí (SILVA, 2018).

Conforme asseverou Silva (2018), há registro de membros de pelo menos 10 (dez) facções criminosas diferentes em estabelecimentos prisionais de Santa Catarina. Além das facções já mencionadas, PGC, PCC, PCRC e CV, foram identificadas presenças de afiliados das seguintes facções nos ergástulos do Estado: Comando Leal (CL); Família do Norte (FDN); Amigos dos Amigos (ADA);

Força Revolucionária Catarinense (FRC); País Livre (PL), e; Serpente Negra Catarinense (SNC).

4.2.2 As cinco séries de atentados praticadas por membros de facções criminosas no Estado

Entre 2012 e 2017 as facções criminosas promoveram cinco séries de atentados em Santa Catarina, sendo que as duas últimas foram direcionadas a atingir, principalmente, integrantes das forças de segurança do Estado. O quadro 1 apresenta um pequeno resumo destes atentados.

Quadro 1 – Resumo das cinco séries de atentados praticados por facções criminosas

Série/Período	Fato	Resultados/Danos
1ª Série - Novembro 2012	No dia 26 de outubro de 2012 a Agente Prisional Deise Alves foi assassinada por supostos membros do PGC. Ela trabalhava na Penitenciária de São Pedro de Alcântara, onde o marido era diretor. O fato fez aumentar o rigor no sistema prisional, especialmente na Penitenciária de São Pedro de Alcântara, onde estavam os líderes do PGC. A liderança da facção emitiu a ordem para os ataques, que foram perpetrados por 11 dias. 48 (quarenta e oito) suspeitos foram presos ou apreendidos.	69 (sessenta e nove) ocorrências registradas; 27 (vinte e sete) ônibus incendiados;
2ª Série – Janeiro e Fevereiro de 2013	A segunda série de ataques foi entendida como uma continuação ou consequência da primeira. No final de janeiro iniciaram as ordens de ataque. O Governo do Estado solicitou ajuda da Força Nacional, que atuou dentro dos estabelecimentos prisionais. 57 (cinquenta e sete) suspeitos foram presos ou apreendidos. 40 (quarenta) líderes do PGC foram transferidos para Penitenciária Federal de Mossoró (RN).	119 (cento e dezenove) ocorrências registradas; 47 (quarenta e sete) ônibus incendiados.
3ª Série – Maio e Abril de 2014	Diferente das demais ocasiões, nesta série de atentados não houve o chamado “salve geral”, ou seja, uma ordem para ataques indiscriminados. Desta vez houve ordens específicas para incendiar ônibus. Os atentados duraram cerca de 09 (nove) dias.	15 (quinze) ocorrências contabilizadas; 03 (três) ônibus incendiados.
4ª Série - Setembro e Outubro de 2014	O fato mais marcante desta série de atentados foi a mudança de objetivo dos criminosos. Desta vez as ordens determinavam ataques diretos a integrantes das forças de segurança do Estado. As ações duraram 29 (vinte e nove) dias e persistiram mesmo após ações enérgicas por parte do poder público, como operações policiais intensas e continuadas, além de transferência de presos. Os fatos ocorreram durante o período eleitoral, aumentando a repercussão e a sensação de insegurança por parte da comunidade.	147 (cento e quarenta e sete) ocorrências registradas; 30 (trinta) ataques contra integrantes das forças de Segurança, sendo 24 (vinte e quatro) contra policiais militares (veículos e residências incendiados ou alvejados por projetil de arma de fogo); 01 (um) Agente Prisional aposentado foi morto em

		Criciúma; 47 (quarenta e sete) ônibus incendiados; 02 (duas) mulheres gravemente feridas durante fuga de suspeitos de disparar arma de fogo contra uma base da PM.
5ª Série – Agosto e Setembro de 2017	A quinta e última série de ataques foi a mais violenta sobre o ponto de vista do número de assassinatos de integrantes das forças de segurança do Estado. Durante o período dos ataques foi percebido um acirramento da rivalidade PCC/PGC, fato que tornou a situação ainda mais conturbada.	91 (noventa e uma) ocorrências contabilizadas; 31 (trinta e um) ataques contra integrantes das forças de Segurança; 02 (dois) Policiais Militares foram mortos, sendo um em Joinville e outro em Camboriú. 01 (um) Agente do DEAP assassinado em Joinville

Fonte: Elaborada pelo autor com dados de Silva (2018).

Da análise do quadro acima, pode-se constatar que com o passar do tempo facções criminosas aumentam a violência dos seus atentados e tendem a concentrar suas ações criminosas nos integrantes das forças de segurança do Estado.

Impende mencionar que somente no ano de 2017, 03 (três) policiais militares foram assassinados no Estado, sendo eles:

- Cb PM Joacir Roberto Vieira , vítima de homicídio, no dia 28 de agosto de 2017, no Município de Joinville/SC.
- Sgt PM RR[16] Edson Abílio Alves, vítima de homicídio, no dia 30 de agosto de 2017, no Município de Camboriú/SC.
- Cb PM Everaldo Soares de Campos, vítima de homicídio, no dia 11 de setembro de 2017, no município de Guabiruba/SC.

4.2.3 As ameaças contra policiais militares registradas no último ano no Estado

A fim de apurar dados sobre ameaças contra policiais militares registradas no último ano pelo serviço de inteligência da PMSC, foi realizada pesquisa para coleta de dados primários, por meio da formulação de um questionário e encaminhamento a todas as 35 (trinta e cinco) AI de batalhões e guarnições especiais da Corporação, cuja área de circunscrição corresponde a todo território do Estado.

[16] Reserva remunerada

O período de doze meses pesquisado corresponde de outubro de 2017 a setembro de 2018.

O questionário foi enviado através do aplicativo google *forms*[17] no dia 27 de setembro de 2018 com prazo de resposta até 04 de outubro de 2018, porém, com o objetivo de colher o maior número de dados, houve prorrogação do prazo de resposta até dia 17 de outubro de 2018, sendo que todas AI responderam.

Observa-se que, que em razão do exíguo tempo para pesquisa, não foram coletados os dados das agências das OPM especializadas, das agências regionais e das agências especializadas.

A primeira questão foi do tipo aberta, em busca de um dado quantitativo, sendo perguntado: quantos policiais militares lotados na sua respectiva Unidade sofreram algum tipo de ameaça, explícita ou velada, direta ou indireta, nos últimos 12 (doze) meses (considerar toda a área de circunscrição atual do Batalhão)?

No quadro 2 constam os dados de resposta da questão 1.

Quadro 2 - Dados de resposta da questão 01 do questionário de pesquisa

OPM	**Município**	**Situação da resposta**	**Número de policiais militares ameaçados**
1º BPM	Itajaí	Respondido	5
2º BPM	Chapecó	Respondido	1
3º BPM	Canoinhas	Respondido	0
4º BPM	Florianópolis (região central e sul da ilha)	Respondido	5
5º BPM	Tubarão	Respondido	6
6º BPM	Lages	Respondido	2
7º BPM	São José	Respondido	1
8º BPM	Joinville (centro e zona norte)	Respondido	5
9º BPM	Criciúma	Respondido	10
10º BPM	Blumenau	Respondido	3
11º BPM	São Miguel do Oeste	Respondido	2
12º BPM	Bal. Camboriú	Respondido	4
13º BPM	Rio do Sul	Respondido	5
14º BPM	Jaraguá do Sul	Respondido	5
15º BPM	Caçador	Respondido	0
16º BPM	Palhoça	Respondido	6
17º BPM	Joinville (zona sul)	Respondido	14
18º BPM	Brusque	Respondido	3
19º BPM	Araranguá	Respondido	0
20ºBPM	Concórdia	Respondido	0
21º BPM	Florianópolis (norte da ilha)	Respondido	6
22º BPM	Florianópolis (região continental)	Respondido	5
23º BPM	São Bento do Sul	Respondido	1
24º BPM	Biguaçu	Respondido	0
25º BPM	Navegantes	Respondido	1

[17] Para confecção dos formulários *google forms* o autor foi assistido pelo Cb PM Samuel, da ACI/PMSC.

26º BPM	Herval do Oeste	Respondido	4
27º BPM	São Francisco do Sul	Respondido	5
28º BPM	Laguna	Respondido	0
GECT	Curitibanos	Respondido	0
GEMFA	Mafra	Respondido	0
GEIC	Içara	Respondido	6
GEIB	Imbituba	Respondido	2
GEBN	Braço do Norte	Respondido	2
GESA	Santo Amaro da Imperatriz	Respondido	0
GEIN	Indaial	Respondido	1
		Total	**110**

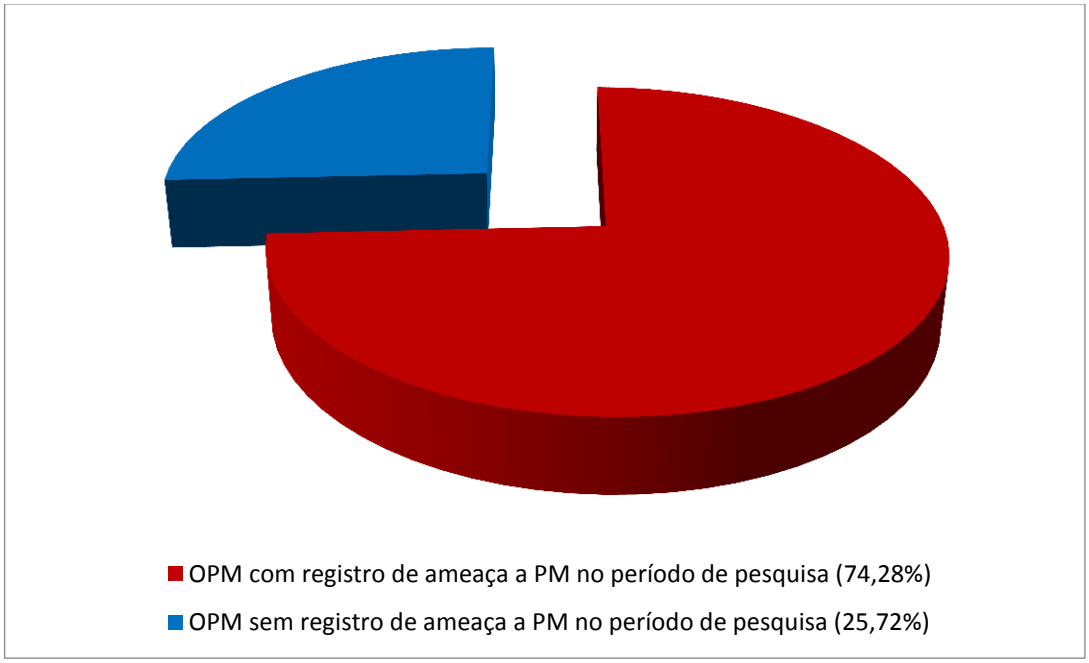
Fonte: Elaborado pelo autor, 2018.

Da análise das respostas à primeira questão da pesquisa foi possível concluir que:

Nas OPM respondentes, 110 (cento e dez) policiais militares foram ameaçados no período de pesquisa. Observa-se que um mesmo policial militar pode ter recebido mais de uma ameaça, inclusive de fontes diversas, porém, a intenção da pesquisa foi de identificar o número de policiais militares que podem necessitar de alguma medida especial de proteção;

74,28% das OPM respondentes tiveram pelo menos um registro de ameaça contra policial militar no período de referência da pesquisa, entre outubro de 2017 e setembro de 2018, conforme demonstrado no Gráfico 1;

Gráfico 1 - Percentual de OPM respondente com registro de ameaças a policiais militares no período

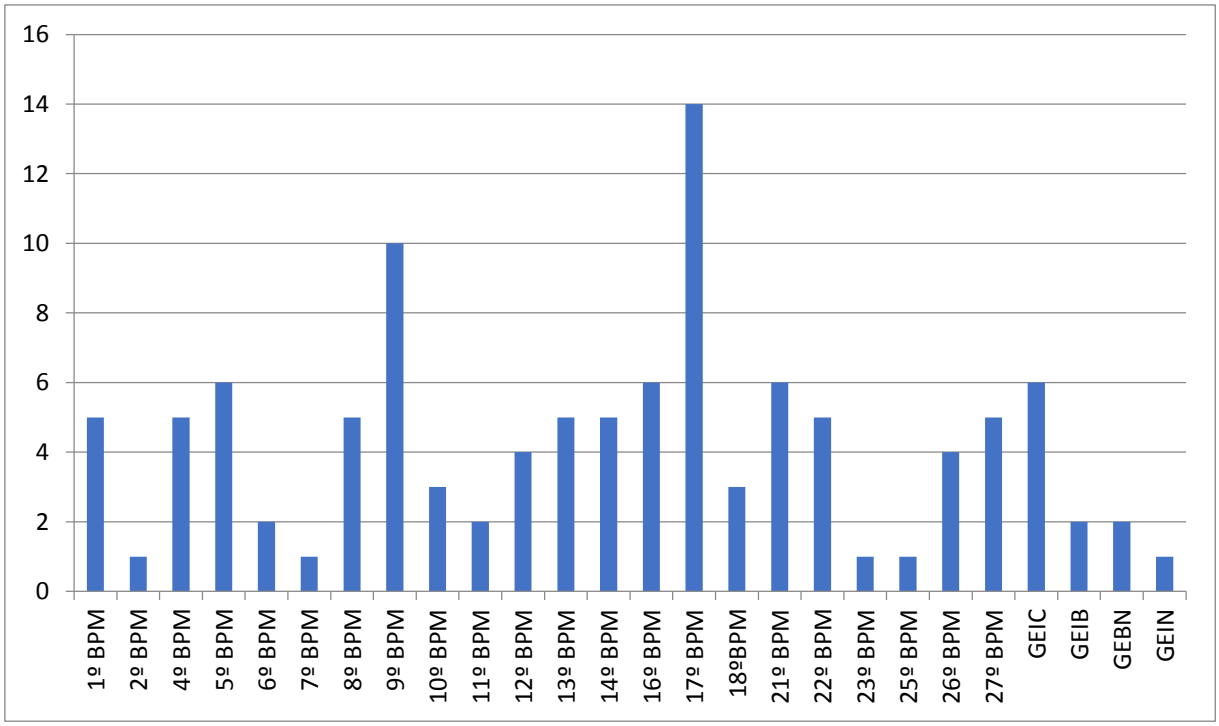


Fonte: Elaborado pelo autor, 2018.

Apesar de ter se mostrado um problema quase que comum a todas OPM, as OPM de Joinville (8ºBPM e 17ºBPM), com 19 (dezenove) casos, de Florianópolis (4ºBPM, 21ºBPM e 22ºBPM), com 16 (dezesseis) casos, e de Criciúma (9ºBPM), com 10 (dez) casos, destacaram-se pela grande quantidade de policiais militares ameaçados no período de pesquisa.

Observa-se uma correlação entre os municípios com maior incidência de ameaças, demonstrado no Gráfico 2, com os que aparecem no mapa de incidência de atuação da facção criminosa PGC nas unidades prisionais, apresentado na Figura 11, porém, esses mesmos municípios apresentam outros fatores que podem ter influenciado nos dados apurados, como população e índices de criminalidade acima da média estadual, fatos que devem ser analisados de forma conjuntural, sendo identificado, neste ponto, necessidade de realização de pesquisa específica para o entendimento deste problema.

Gráfico 2 – Número de PM ameaçados no período de pesquisa por OPM com incidência



Fonte: Elaborado pelo autor, 2018.

Por fim, foi constatado que há registro de ameaças a policiais militares em todas as regiões do Estado, conforme Quadro 3, porém, as regionais que apresentam maior incidência de caso são a 5ªRPM, 1ªRPM, 6ªRPM, 7ªRPM, 3ªRPM e 8ªRPM.

Quadro 3 – Número de registro de ameaças distribuído por RPM.

RPM	**Município-sede**	**Total de registros**
1ªRPM	Florianópolis	16
2ªRPM	Lages	2
3ªRPM	Bal. Camboriú	10
4ªRPM	Chapecó	1
5ªRPM	Joinville	24
6ªRPM	Criciúma	16
7ªRPM	Blumenau	12
8ªRPM	Tubarão	10
9ªRPM	São Miguel do Oeste	2
10ªRPM	Joaçaba	4
11ªRPM	São José	7
12ªRPM	Jaraguá do Sul	6
	Total	110

Fonte: Elaborado pelo autor, 2018.

A segunda questão foi do tipo fechada, tendo sido dirigida apenas para as AI que respondessem à questão 1 pela inexistência de registro de ameaça contra policial militar no período de pesquisa, visando entender se de fato a AI não tomou conhecimento ou se não há controle sobre as ameaças sofridas por integrantes da OPM, sendo perguntado: Caso não haja registro de ameaças contra policiais militares na Unidade:

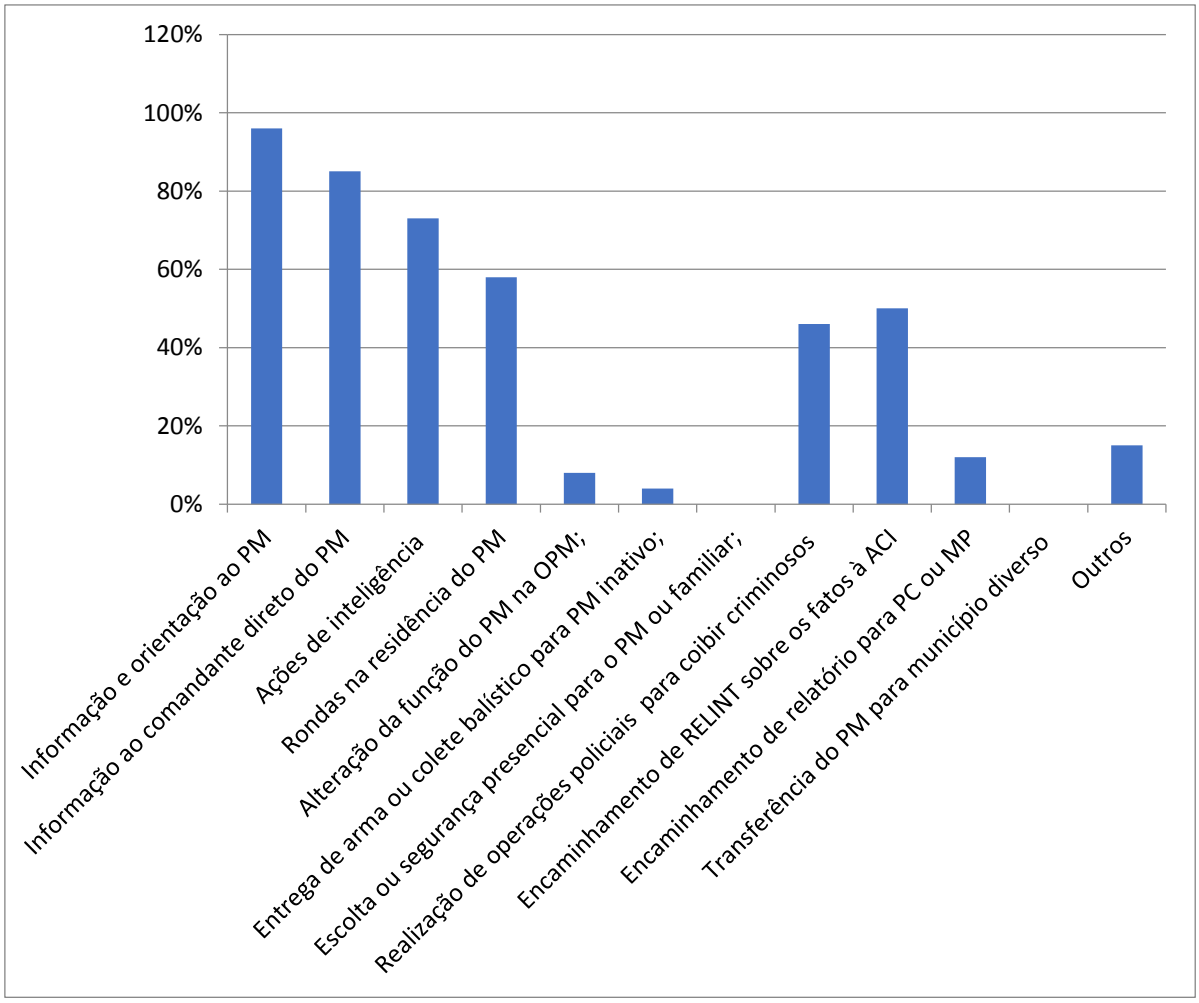
As respostas possíveis eram: [1] A AI não mantém controle sobre ameaças contra policiais militares na Unidade; [2] A AI não tomou conhecimento sobre ameaças contra policiais militares no período em pesquisa.

Nas repostas foi constatado que as 09 AI que informaram não ter registro de policial militar ameaçado no período de pesquisa marcaram a segunda resposta, ou seja, não há falta de controle sobre as informações que chegam ao conhecimento das AI. Entretanto, é possível que ameaças ocorridas no período de pesquisa não tenham sido identificadas ou notificadas para as AI, uma vez que não há um sistema adequado de registro e comunicação dos riscos.

A terceira questão também foi do tipo fechada, porém, permitindo uma alternativa aberta (outros), tendo sido perguntado: caso haja registros, informar quais das medidas abaixo foram adotadas pelo Comando da Unidade para evitar a concretização da ameaça ou proteger o(s) policial(is) militar(es) ameaçado(s).

As opções eram: [1] Informação e orientação ao policial militar ameaçado; [2] Informação ao comandante direto do policial militar ameaçado; [3] Ações de inteligência para produzir conhecimento sobre a ameaça; [4] Realização de rondas na residência do policial militar ameaçado; [5] Alteração da função do policial militar ameaçado na OPM; [6] Entrega de arma ou colete balístico para policial militar da reserva remunerada; [7] Escolta ou segurança presencial para o policial ameaçado ou familiar; [8] Realização de operações policiais (barreira, varredura,...) específica para coibir criminosos ou organização criminosa envolvida na ameaça; [9] Encaminhamento de RELINT sobre os fatos à ACI; [10] Encaminhamento de relatório sobre a ameaça para Polícia Civil ou Ministério Público para que os fatos sejam investigados; [11] Transferência do policial militar para OPM em município diverso do local da ameaça; [12] Outros (especificar todas as demais medidas tomadas).

Gráfico 3 - Medidas de tratamento adotadas pelas OPM respondentes



Fonte: Elaborado pelo autor, 2018.

Nessa questão foi permitido ao respondente marcar múltiplas respostas, já que para um mesmo caso de ameaça podem ser tomadas várias medidas de tratamento. Desta forma, o Gráfico 3 aponta a porcentagem de OPM que adotaram cada uma das medidas de tratamento enumeradas. Observa-se que na construção do Gráfico 3 foram considerados os dados apenas das 26 (vinte e seis) OPM que relataram casos de ameaça contra policial militar no período.

Apesar de não haver um protocolo formalizado para gestão de riscos, constata-se que a maioria das AI adotam medidas similares, sendo as principais: informação e orientação ao policial militar ameaçado; informação ao comandante direto do policial militar ameaçado; ações de inteligência para produzir conhecimento sobre a ameaça; realização de rondas na residência do policial militar ameaçado; realização de operações policiais (barreira, varredura,...) específica para coibir criminosos ou organização criminosa envolvida na ameaça, e; encaminhamento de RELINT sobre os fatos à ACI.

De outro lado, verifica-se que nenhuma OPM optou pela escolta ou segurança presencial para o policial ameaçado ou familiar ou por transferência do policial militar para OPM em município diverso do local da ameaça, bem como, que poucas OPM adotaram a medida de entrega de arma ou colete balístico para policial militar da reserva remunerada.

Observa-se que apenas quatro AI informaram ter adotado outras medidas tratamento. Uma das AI apenas detalhou sobre critérios para confecção de RELINT. As outras três informaram ter adotado as seguintes medidas: registro policial; prisão dos autores, e; informação verbal ao MP e Judiciário.

Portanto, observa-se que naturalmente há uma padronização dos tipos de medidas de tratamento adotadas pelas OPM, porém, há necessidade de estabelecer formalmente os critérios ou parâmetros para escolha de tais medidas e dar segurança jurídica aos envolvidos por meio da normatização da atividade de gestão de riscos.

Em suma, concluiu-se com a pesquisa que 110 (cento e dez) policiais militares de Santa Catarina foram ameaçados no período de pesquisa (outubro de 2017 e setembro de 2018), sendo que o número pode ser bem mais elevado em razão da inexistência de um sistema que facilite a identificação e a comunicação dos riscos. Estes casos ocorreram em todas as regiões do Estado, atingido 74,28% das OPM de área (batalhões e guarnições especiais).

Joinville (8ºBPM e 17ºBPM) com 19 (dezenove) casos, Florianópolis (4ºBPM, 21ºBPM e 22ºBPM) com 16 (dezesseis) casos, e Criciúma (9ºBPM) com 10 (dez) casos, destacaram-se pela grande quantidade de policiais militares ameaçados no período de pesquisa.

Sobre as medidas de tratamento, apesar de não haver uma padronização formal, há muita semelhança entre as medidas adotadas pelas OPM do Estado, bem como, mesmo sem um sistema formal de gestão de riscos, as OPM costumam adotar práticas de mitigação de riscos, demonstrando capacidade operativa para atividade. Tais fatos facilitarão na implementação de um sistema de gestão de riscos na Corporação.

4.3 MODELOS E PRÁTICAS RECOMENDÁVEIS À PMSC

Diante do objetivo deste trabalho, em propor a implementação e apresentar diretrizes, de um sistema de gestão de riscos para a Polícia Militar de Santa Catarina, específico para tratar de ameaças contra policiais militares, foram pesquisados modelos e normas e gestão de riscos e experiências de outros órgãos. O ponto de partida da pesquisa encontrou amparo no estudo de Rosa (2010), resultando na exposição das principais normas e modelos existentes, a citar: Norma AS/NZS 4360:2004 (AS/NZS, 2004, apud ROSA, 2010), Norma de gestão de riscos FERMA (FERMA, 2002, apud ROSA, 2010), Modelo de gerenciamento de riscos corporativos (IBGC, 2007, apud ROSA, 2010), *Risk management process* (ROPER, 1999, apud ROSA, 2010), *Process vulnerability analyis* (BAYBUTT, 2002, apud ROSA, 2010), Manual de análise de riscos para a segurança empresarial (BRASILIANO, 2003, apud ROSA, 2010), *Risk analysis* (BRODER, 2006, apud ROSA, 2010), *Vulnerability self assessment tool* – VSAT (BRODER; TUCKER, 2006, apud ROSA, 2010), *Operational risk management,* – ORM (BRODER; TUCKER, 2006, apud ROSA, 2010), CARVERS + SHOCK (BRODER; TUCKER, 2006, apud ROSA, 2010), *Security risk assessment and management process* (BIRINGER; MATALUCCI; O'CONNOR, 2007, apud ROSA, 2010).

Além desses, ainda foram apresentados os modelos de Moraes (2010) e o do curso de capacitação em gestão de riscos voltado à defesa civil (UFRGS, 2016).

Dentre todos esses modelos, o apresentado na Norma ISO 31.000 – *Risk management principles and guidelines on implementation* (ISO, 2009), certamente é

o que melhor atende às necessidades da PMSC, pois, assim como aduz a norma, foi concebido para aplicação em todos os níveis, estratégico, tático e operacional e para uso em todos os segmentos organizacionais, quer sejam eles públicos ou privados, razão pela qual a conclusão foi por recomendar que a Norma ISO 31.000 seja utilizada como parâmetro na PMSC para gestão de riscos para policiais militares ameaçados, principalmente quanto aos seus princípios e operacionalização, naquilo que for aplicável.

Em face desta conclusão, foi detalhada a operacionalização do processo proposto pela Norma ISO 31.000, descrevendo as seguintes etapas: comunicação e consulta; estabelecimento do contexto; identificação de riscos; análise de riscos; avaliação de riscos; tratamento de riscos; monitoramento e análise crítica; registro do processo (ISO, 2009).

Não obstante, considerando a complexidade do problema e as características da Corporação apresentadas neste capítulo, contata-se que é necessário que o setor responsável pelo gerenciamento de riscos tenha recursos, humanos e materiais, para realização da tarefa e, ainda, ter “capilaridade”, ou seja, estar presente em todos os órgãos da Corporação. Neste sentido, o serviço de inteligência da PMSC reúne as características para a missão, pois, está presente em todos os órgãos operacionais da instituição e possui pessoal familiarizado com análise de dados, tarefa correlata com a análise de riscos.

Ademais, é atribuição da contrainteligência, ramo da inteligência, proteger a informação produzida de acessos não autorizados, proteger a própria atividade de inteligência e seus integrantes, proteger a instituição a que pertence e os profissionais que fazem parte, bem como, em produzir conhecimentos para neutralizar a inteligência adversa (SILVEIRA, 2012).

Da análise das práticas adotadas pelo TJSC quanto à gestão de riscos de seus integrantes e do que apresenta o guia de análise de riscos para magistrados elaborado pelo DSIPJ (CNJ, 2018), foram adaptadas as seguintes propostas para a PMSC:

- Estruturação de um núcleo de gestão de riscos na ACI, ligado diretamente ao Chefe da ACI;

- Elaboração de um POP para normatizar e detalhar as atribuições de cada responsável, bem como, descrever as medidas de tratamento possíveis;

- Elaboração de guias para análise de riscos específico para PMSC e para segurança pessoal de policiais militares;

- Promover a capacitação dos responsáveis pela gestão;

- Investimento em equipamentos e viaturas próprias para a atividade;

- Visão de futuro em contar com pessoal bem treinado, equipamento e viaturas de ponta para atividade e uma ferramenta de tecnologia da informação que auxilie na análise de riscos;

- Adoção de um modelo de termo de compromisso para integrantes do TJSC ameaçados (Anexo A);

- Adoção de um modelo de termo de dispensa de segurança pessoal (Anexo B).

5 PROPOSTA DE IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE RISCOS PARA PMSC COM FOCO NA PROTEÇÃO DE POLICIAIS MILITARES AMEAÇADOS

Considerando o cenário contextualizado, neste capítulo pretende-se propor a implementação de um sistema de gestão de riscos para policiais militares ameaçados no âmbito da PMSC, com fundamento em toda pesquisa de dados da Corporação, do detalhamento da situação-problema e da análise dos modelos de sistemas de gestão de riscos, formalizadas neste trabalho. Trata-se, portanto, do ponto central do estudo.

Para tanto, serão apresentadas propostas de diretrizes sobre os seguintes aspectos do sistema: objetivo e denominação do sistema; ISO 31.000 como norma balizadora do sistema; composição do sistema; atribuições, e; operacionalização.

5.1 OBJETIVO E DENOMINAÇÃO DO SISTEMA

O sistema de gestão de riscos para policiais militares ameaçados da PMSC terá por objetivo eliminar ou reduzir riscos à vida, à integridade física e psicológica e ao patrimônio de policiais militares e seus familiares decorrentes de ameaças relacionadas à atividade policial militar, identificando, analisando e avaliando os riscos, a fim de subsidiar a decisão sobre medidas de tratamento a serem adotadas, mantendo rigoroso controle sobre as ameaças identificadas e efeitos das medidas de tratamento tomadas.

Sugere-se a seguinte denominação para o sistema: PROTEGE PMSC - Sistema de proteção para policiais da Polícia Militar de Santa Catarina.

5.2 ISO 31.000 COMO NORMA BALIZADORA

Considerando que na presente pesquisa a Norma ISO 31.000 (ISO, 2009) demonstrou ser o modelo que mais se ajusta às necessidades da PMSC, sugere-se que a referida norma sirva de parâmetro nos processos de gestão de riscos da Corporação, observando-se aos seguintes princípios adaptados da norma:

a) A proteção do policial militar ou familiar ameaçado;
b) Agregar valor à PMSC como instituição;

c) Ser parte integrante da tomada de decisões sobre medidas de tratamento envolvendo policial militar ameaçado;
d) Abordar explicitamente as ameaças contra policiais militares, suas consequências e vulnerabilidades, as incertezas e as oportunidades;
e) Ser sistemática, estruturada e oportuna na proteção do policial militar;
f) Ter como base as melhores informações disponíveis na Corporação;
g) Considerar fatores humanos e culturais da PMSC;
h) Propiciar o fluxo de informação e a consulta entre as partes interessadas, independentemente de níveis hierárquicos da Corporação;
i) Ser dinâmica, interativa e capaz de reagir a mudanças na Corporação ou sociedade;
j) Utilizar-se da tecnologia da informação no processo de gestão do conhecimento;
k) Considerar a análise de contexto e o perfil de risco da profissão policial militar;
l) Manter rigoroso registro e controle sobre as informações e atividades desenvolvidas;
m) Incorporar-se ao serviço de inteligência da PMSC.

5.3 COMPOSIÇÃO DO SISTEMA

Considerando o modelo da ISO 31.000, naquilo que é compatível com a realidade da PMSC e o exemplo prático da TJSC, onde a coordenação do NIS é realizada por um Desembargador ligado diretamente à Presidência do Tribunal, propõe-se que a coordenação geral da operacionalização do sistema fique a cargo do Chefe da ACI, criando-se um núcleo de coordenação de gestão de riscos para policiais militares ameaçados na ACI, ligado diretamente ao Chefe da ACI e designando agentes de inteligência das AI como responsáveis pela gerência de riscos em nível local. Ainda é recomendável que integrem o sistema, de forma extraordinária, os órgãos que possam contribuir no aprimoramento da atividade, resultando na seguinte composição:

I – Coordenador-Geral do sistema, Chefe da ACI;

II – Núcleo de coordenação de gestão de riscos para policiais militares ameaçados, na ACI;

III – Gerenciadores de riscos de policiais militares ameaçados em nível local, nas AI;

IV – Órgãos extraordinários de apoio administrativo, técnico ou operacional.

Ressalta-se que o sistema de gestão de riscos, trata-se de uma ferramenta de auxílio à tomada de decisão (ISO, 2009), portanto, a decisão sobre as medidas de tratamento a serem adotadas caberá aos usuários do sistema, ou seja, aos comandantes de nível local (GP PM, Pel PM, Cia PM, BPM), de RPM, ou Comandante-Geral.

5.4 ATRIBUIÇÕES

É importante que as atribuições de cada responsável sejam detalhadas em um Procedimento Operacional Padrão (POP). Para exemplificar, segue uma listagem de atribuições sugeridas à ACI:

a) Apresentar ao Comando-Geral da PMSC uma proposta de um POP específico para gestão de riscos de policiais militares ameaçados, detalhando a operacionalização da atividade e as atribuições de cada responsável, bem como, descrever as medidas de tratamento possíveis;
b) Promover revisões periódicas do referido POP após sua aprovação pelo Comando-Geral;
c) Estabelecer os “níveis de ancoragem” empregados na mensuração dos riscos e critérios de padronização de medidas de tratamento conforme o grau do risco identificado;
d) Padronizar documentos da atividade, tais como: relatório de análise de riscos, plano de tratamento, termo de compromisso para policiais militares ameaçados, termo de dispensa de proteção pessoal, entre outros.
e) Servir de órgão central de fiscalização, controle e consulta do sistema;
f) Capacitar os Agentes de Inteligência do SIPOM e Comandantes de OPM;
g) Manter o fluxo de informações, especialmente com o Comando-Geral da Corporação;
h) Promover última avaliação de riscos nos casos em que a decisão sobre a medida de tratamento couber ao Comando-Geral da Corporação;

i) Apresentar ao Centro de Inovação e à Diretoria de Tecnologia da Informação da PMSC os dados necessários para o desenvolvimento de softwares ou ferramentas tecnológicas que:
    a. Auxilie no registro e comunicação dos riscos identificados e na análise de riscos, possibilitando sistematizar a mensuração dos riscos, fluxo das informações e registro de todas as decisões tomadas e medidas executadas;
    b. Contribua no tratamento dos riscos, tais como: na localização e acompanhamento de policiais militares ameaçados por equipe de proteção; acionamento de guarnições por botões de pânico via aplicativo de celular; videomonitoramento de residências de policiais ameaçados, entre outros.
    c. Outras inovações que aprimorem a atividade;
j) Apresentar proposta à DIE para inclusão das disciplinas de autoproteção e gestão de riscos nos cursos de formação e aperfeiçoamento da Corporação;
k) Apresentar à DALF proposta para aquisição de viaturas e equipamentos, bem como, dotação orçamentária própria da atividade.

5.5 OPERACIONALIZAÇÃO

Empregando como parâmetro o processo descrito na Norma ISO 31.000 (ISO, 2009), sugere-se que a operacionalização da gestão de riscos para policiais militares ameaçados siga as seguintes etapas:

a) Comunicação e consulta: a comunicação e consulta deve ser prevista como etapa contínua, descrevendo a relevância da troca de informações ao longo de todo o processo de gestão de riscos e apontando as obrigações de cada uma das partes interessadas;
b) Estabelecimento do contexto: devem ser descritas todas as ameaças decorrentes do serviço policial militar que possam impactar no objetivo de salvaguarda da vida, da saúde e do patrimônio do efetivo policial militar e familiares, incluindo, especialmente, o acompanhamento sistemático do sistema de inteligência (SIPOM) da PMSC quanto às atividades de organizações criminosas, dentro e fora do Estado.

c) Identificação de riscos: todas as ameaças, decorrentes da função policial militar, que possam acarretar em prejuízos a policiais militares e/ou familiares, quer sejam elas diretas ou indiretas, ostensivas ou veladas, de autor conhecido ou anônimo, devem ser identificadas para o início do processo de avaliação dos riscos (macro fase de identificação dos riscos, análise dos riscos e avaliação dos riscos). O resultado desta etapa deve ser o registro da ameaça identificada.

d) Análise de riscos: etapa destinada a analisar as variáveis do risco, ou seja, ameaça e vulnerabilidade (CNJ, 2018). Dada a complexidade desta etapa, a exemplo do que fez o CNJ sugere-se a elaboração de um guia para análise de riscos para policiais militares ameaçados. Não obstante, para mensuração dos riscos devem ser empregados critérios científicos, podendo se valer das ferramentas relacionadas na pesquisa de Rosa (2010), ou seja: árvores de falhas, método AHP, método Delphi, brainstorming, investigação de incidentes, entre outros. O resultado desta etapa deve ser a elaboração de um relatório de análise de riscos, destinado a subsidiar a avaliação de riscos e, posteriormente, a etapa de tratamento de riscos. Vale apresentar a sugestão de padronização de relatório da cartilha do CNJ, com o seguinte conteúdo: objeto; objetivo; atividades desenvolvidas e conclusão.

e) Avaliação de riscos: fundamenta-se na análise dos riscos e destina-se a subsidiar a tomada de decisão sobre os seguintes aspectos do tratamento dos riscos: a) quais riscos precisam de tratamento; b) qual é a prioridade para implementação do tratamento de riscos, de acordo com os níveis dos riscos encontrados e do contexto estabelecido (ISO, 2009). O resultado dessa etapa deve ser a apresentação de uma matriz de vulnerabilidade (BRASILIANO, 2003), e a de uma lista de prioridade para o tratamento dos riscos, que servirá para subsidiar a decisão sobre quais riscos devem ser tratados imediatamente e quais riscos devem ser acompanhados.

f) Tratamento de riscos: Etapa onde são definidas e adotadas as medidas de tratamento dos riscos (ISO, 2009), ressaltando que cabe ao decisor definir quais das medidas de tratamento propostas pelo gerenciador de riscos serão adotadas. O ideal é que haja uma padronização das medidas de tratamento, as quais devem ser proporcionais ao nível do risco avaliado,

além de observar os aspectos da legalidade. Os objetivos desta etapa são: reduzir o grau de ameaça; reduzir as vulnerabilidades, e; aumentar as capacidades. (CNJ, 2018). O resultado desta etapa deve ser um plano de tratamento de riscos. Trata-se de um documento formal que deve incluir: as razões para a seleção das opções de tratamento, incluindo os benefícios que se espera obter; os responsáveis pela aprovação do plano e os responsáveis pela implementação do plano; ações propostas; os recursos requeridos, incluindo contingências; medidas de desempenho e restrições; requisitos para a apresentação de informações e de monitoramento, e; cronograma e programação. (IS0, 2009). Sugere-se o modelo proposto pelo CNJ (2018), contendo: objetivo; responsável; prazos; medidas de segurança; atividades; ações compartilhadas entre órgãos; ciência e compromisso do protegido com o plano. Destaca-se a necessidade de adotar modelos de termo de compromisso para policiais militares ameaçados e de termo de dispensa de segurança pessoal, conforme modelos do TJSC (Anexos A e B).

g) Monitoramento e Análise Crítica: etapa que segue do início ao fim do processo de gestão de riscos e que tem finalidade não apenas de controle, mas também de avaliação e correção de desvios.
h) Registro do processo: deve ser mantido registro sobre todos os riscos identificados, das análises e decisões tomadas e das medidas de controle adotadas e, ainda, dos resultados obtidos.

Ressalta-se que devem ser considerados os critérios de legalidade, viabilidade e oportunidade para se padronizar as medidas de tratamento a serem adotadas na PMSC, sendo sugerida a análise das seguintes medidas: [1] Informação e orientação ao policial militar ameaçado; [2] Informação ao comandante direto do policial militar ameaçado; [3] Ações de inteligência para produzir conhecimento sobre a ameaça; [4] Realização de rondas na residência do policial militar ameaçado; [5] Alteração da função do policial militar ameaçado na OPM; [6] Entrega de arma ou colete balístico para policial militar da reserva remunerada; [7] Segurança presencial para o policial ameaçado ou familiar; [8] Escolta em itinerários específicos; [9] Realização de operações policiais (barreira, varredura,...) específica para coibir criminosos ou organização criminosa envolvida

na ameaça; [10] Encaminhamento de RELINT sobre os fatos à ACI; [11] Encaminhamento de relatório sobre a ameaça à Polícia Civil ou Ministério Público para que os fatos sejam investigados; [12] Transferência do policial militar para OPM em município diverso do local da ameaça, podendo ser de forma voluntária ou por necessidade do serviço, conforme o caso.

Por fim, destaca-se a necessidade de desenvolver softwares para facilitar a operacionalização do sistema e contribuir no tratamento de riscos, sendo que, a exemplo da prática do MPSC, é interessante que haja um aplicativo para análise do risco e outro para ser utilizado em situações críticas (botão de pânico).

6 CONCLUSÃO

Nos últimos anos a segurança pública de Santa Catarina passou a se defrontar com uma profunda alteração na criminalidade em razão do crescimento das facções criminosas.

Entre 2012 e 2017 membros de facções criminosas executaram cinco séries de atentados no Estado. Na última delas, entre o final do mês de agosto e início do mês de setembro de 2017, 03 (três) integrantes das forças de segurança estaduais foram assassinados, dentre eles, dois policiais militares.

Diante deste cenário, este trabalho valeu-se de pesquisas exploratórias, principalmente de dados secundários, por meio de pesquisa documental e bibliográfica, mas, também de dados primários, por meio de formulação de questionário, com a finalidade de identificar um sistema de barreiras capaz de mitigar os perigos à segurança pessoal dos integrantes da Corporação e familiares, especialmente os advindos de ameaças oriundas de membros de organizações criminosas.

Com amparo na pesquisa de Rosa (2010), foram listadas as principais normas e modelos de gestão de riscos, sendo concluído que o modelo apresentado na Norma ISO 31.000 – r*isk management principles and guidelines on implementation* (ISO, 2009), é o que melhor atende às necessidades da PMSC, pois, assim como aduz a norma, foi concebido para aplicação em todos os níveis, estratégico, tático e operacional, e para uso em todos os segmentos organizacionais, quer sejam eles públicos ou privados, razão pela qual foi sugerido que a Norma ISO 31.000 seja utilizada como parâmetro na gestão de riscos para policiais militares na PMSC.

Por meio de coleta de dados primários sobre ameaças a policiais militares no Estado, concluiu-se que 110 (cento e dez) policiais militares de Santa Catarina foram ameaçados no período de pesquisa (outubro de 2017 e setembro de 2018), sendo que o número pode ser bem mais elevado em razão da inexistência de um sistema que facilite a identificação e a comunicação dos riscos. Estes casos ocorreram em todas as regiões do Estado, atingindo 74,28% das OPM de área (batalhões e guarnições especiais). Joinville (8ºBPM e 17ºBPM) com 19 (dezenove) casos, Florianópolis (4ºBPM, 21ºBPM e 22ºBPM) com 16 (dezesseis) casos, e Criciúma

(9ºBPM) com 10 (dez) casos, destacaram-se pela grande quantidade de policiais militares ameaçados no período de pesquisa.

Na pesquisa ainda foi verificado que apesar de não haver uma padronização formal, há muita semelhança entre as medidas de tratamento adotadas pelas OPM do Estado, bem como, mesmo sem um sistema formal de gestão de riscos, as OPM costumam adotar práticas de mitigação de riscos, demonstrando capacidade operativa para a atividade.

Da análise da estrutura da Corporação, apurou-se que o quantitativo de efetivo da Corporação de 10.348 (dez mil e trezentos e quarenta e oito) policiais militares da ativa, 1.464 (um mil e quatrocentos e sessenta e quatro) do CTISP e 191 (cento e noventa e um) Ag Temp e a distribuição deste efetivo por quase todo o Estado, são fatores que tornarão a atividade de gestão de riscos mais complexas.

Por outro lado, foi verificado que a atividade de gestão de riscos é, por essência, atribuição da contrainteligência, ramo da atividade de inteligência, sendo que o fato de o serviço de inteligência da PMSC estar presente em todos os batalhões e guarnições especiais do Estado facilitará a execução da missão.

Foram analisados os modelos de gestão de riscos adotados pelo TJSC e pelo MPSC e destacadas as práticas que podem ser aplicadas à PMSC.

No capítulo 5 foram apresentadas as propostas de diretrizes para um sistema de gestão de riscos com foco na proteção de policiais militares ameaçados, com a seguinte denominação sugerida: PROTEGE PMSC - Sistema de proteção para Policiais da Polícia Militar de Santa Catarina.

Sendo assim, conclui-se que foram atingidos os objetivos do trabalho ao se sugerir um modelo de sistema de gestão de riscos para policiais militares ameaçados da PMSC, fundamentado na Norma ISO 31.000 (2009), que terá o objetivo de eliminar ou reduzir riscos à vida, à integridade física e psicológica e ao patrimônio de policiais militares e seus familiares decorrentes de ameaças relacionadas à atividade policial militar, identificando, analisando e avaliando os riscos, a fim de subsidiar a decisão sobre medidas de tratamento a serem adotadas, mantendo rigoroso controle sobre as ameaças identificadas e efeito das medidas de tratamento tomadas.

REFERÊNCIAS

AZ/NZS – AUSTRALLIAN STANDARDS / NEW ZELAND STANDARDS, A. N. Z. **AS/NZS 4360:2004:** *Risk management. New Zealand*: Standard Australian e Standard New Zealand, 2004.

BERNSTEIN, Peter L. **Desafio aos deuses:** a fascinante história do risco. 3. ed. Tradução Ivo Korytowski. Rio de Janeiro: Campos, 1997.

BRASIL. Conselho Nacional de Justiça CNJ. **Guia de análise e gerenciamento de riscos de magistrados.** 2018. Disponível em: <http://www.cnj.jus.br/files/conteudo/ arquivo/ 2018/07/876d201cdcdf1c10c55b072f74df803a.pdf>. Acesso em: 10 out 2018.

_____. Conselho Nacional de Justiça CNJ. **Guia de segurança pessoal para magistrados**. 2017. Disponível em: <http://www.cnj.jus.br/files/conteudo/arquivo/ 2017/09/e3e89ee45236107bcfcb1ea810826b16.pdf>. Acesso em: 10 out 2018.

_____. Conselho Nacional de Justiça CNJ. Resolução Nº 104, de 06 de abril de 2010. Disponível em: < http://www.cnj.jus.br///images/atos_normativos/ resolucao/ resolucao_104_06042010_16092014170744.pdf>. Acesso em: 11 out 2018.

_____. Conselho Nacional de Justiça CNJ. Resolução Nº 176 de 10 de junho de 2013. Institui o sistema nacional de segurança do Poder Judiciário e dá outras providências. Disponível em: <http://www.cnj.jus.br/atos-normativos?documento=/ 1772>. Acesso em: 11 out 2018.

_____. Conselho Nacional do Ministério Público CNMP. Resolução Nº 156 de 13 de dezembro de 2016. Institui a política de segurança institucional e o sistema nacional de segurança institucional do Ministério Público, e dá outras providências. Disponível em: <http://www.cnmp.mp.br/portal/images/Resolucoes/ Resolu%C3%A7%C3%A3o-156.pdf>. Acesso em: 16 out 2018.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ constituicaocompilado.htm>. Acesso em: 29 set. 2018.

_____. Decreto-Lei Nº 667, de 02 de julho de 1969. Reorganiza as Polícias Militares e Corpos de Bombeiros Militares dos Estados, dos Territórios e do Distrito Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 3 jul. 1969. Disponível em <http://www.planalto.gov.br/ ccivil_03/DecretoLei/Del0667.htm>. Acesso em: 29 set. 2018.

_____. Decreto no 88.777, de 30 de setembro de 1983. Aprova o regulamento para as polícias militares e corpos de bombeiros militares (R-200). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 4 out. 1983.Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D88777.htm>. Acesso em: 29 set. 2018.

_____. Lei Nº 9.883, de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 8 dez. 1999. Disponível em: <http://www.planalto.gov.br/ccivIl_03/LEIS/ L9883.htm> Acesso em: 29 set. 2018.

_____. Ministério da Justiça. Secretaria Nacional de Segurança Pública SENASP. Portaria Nº 2, de 12 de Janeiro de 2016. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 25 jan. 2016. Aprova a Doutrina Nacional de Segurança Pública. Disponível em: <http://www.lex.com.br/legis_27083673_PORTARIA_N_2_/ DE_12_DE_JANEIRO_DE_2016.aspx>. Acesso em: 29 set. 2018.

BRASILIANO, Antônio Celso Ribeiro. **Manual de planejamento**: gestão de riscos corporativos. São Paulo: Sicurezza, 2003.

COSTA, Diego Marzo. **A atividade de inteligência na PMSC e o enfrentamento às facções criminosas**: uma proposta de procedimento operacional padrão. 2014. 56 f. Monografia (Especialização em Administração de Segurança Pública da Escola Superior de Administração e Gerência) - Universidade do Estado de Santa Catarina, Florianópolis, 2014.

FERMA – FEDERAÇÃO EUROPÉIA DE ASSOCIAÇÕES DE GERENCIAMENTO DE RISCOS. **Norma de gestão de riscos**. Reino Unido: Ferma, 2002.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4.ed. São Paulo: Atlas, 2002.

LAKATOS, E.M.; MARCONI, M.A. **Fundamentos de metodologia científica**. 6. Ed. São Paulo: Atlas, 2006.

LAZZARINI, Álvaro. **Estudos de direito administrativo**. 2. ed. São Paulo: Editora Revista dos Tribunais, 1999.

LUNKES, Rogério João. **Controle de Gestão:** estratégico, tático, operacional, interno e de risco. São Paulo: Atlas, 2010.

MARCINEIRO, Nazareno. **Polícia comunitária:** construindo segurança nas comunidades. Florianópolis: Insular, 2009.

MEIRELES, Hely Lopes et al. **Direito administrativo brasileiro**. 33. Ed. São Paulo: Editora Malheiros, 2007.

MORAES, Giovanni. **Sistema de gestão de riscos – princípios e diretrizes – ISO 31.000/2009**: Comentada e ilustrada. Rio de Janeiro: GVC, 2010.

PORTELA, Geraldo. **Gerenciamento de riscos na indústria de petróleo e gás:** offshore e onshore. Rio de Janeiro: Elsevier, 2015.

QUIVY, Raymond; CAMPENHOUDT, Luc Van. **Manual de investigação em ciências sociais**. 4. ed. Lisboa: Gradiva, 2005.

RICHARDSON, Roberto Jarry. **Pesquisa social:** métodos e técnicas. São Paulo: Atlas, 1999.

ROSA, Izaiais Otacílio da. **Gerenciamento de riscos afins à segurança empresarial:** a estruturação de um modelo de avaliação fundamento segundo uma visão construtivista. 2010. 327 p. Dissertação (Mestrado em Engenharia da Produção) – Universidade Federa de Santa Catarina, Florianópolis, 2010.

ROY, B., VANDERPOONTEN, D. **The European School of MCDA:** Emergences, basic features and current works. Journal of Multicriteria Decision Analysis. V.5, p. 23-28, 1996.

SANTA CATARINA. **Constituição do Estado de Santa Catarina**. Disponível em: <http://www.alesc.sc.gov.br/legislacao>. Acesso em: 24 set. 2018.

_____.Lei complementar Nº 302, de 28 de outubro de 2005. Institui o serviço auxiliar temporário da Polícia Militar e no Corpo de Bombeiros Militar. **Diário Oficial [do] Estado de Santa Catarina**, Florianópolis, SC, 28 out. 2005.Disponível em: <http://leis.alesc.sc.gov.br/html/2005/302_2005_lei_complementar_promulgada.htm> . Acesso em 09 Out 2018.

_____.Lei complementar Nº 380, de 03 de maio de 2007. Dispõe sobre o corpo temporário de inativos da Segurança Pública no Estado. **Diário Oficial [do] Estado de Santa Catarina**, Florianópolis, SC, 03 maio 2007. Disponível em: <http://leis.alesc.sc.gov.br/html/2007/380_2007_lei_complementar.html>. Acesso em 09 Out 2018.

_____.Lei Nº 6.218, de 10 de fevereiro de 1983. Dispõe sobre o Estatuto dos policiais militares do Estado de Santa Catarina, e dá outras providências. **Diário Oficial [do] Estado de Santa Catarina**, Florianópolis, SC, 11 fev. 1983. Disponível em: <http://leis.alesc.sc.gov.br/html/1983/6218_1983_lei.html>. Acesso em: 09 Out 2018.

_____. Ministério Público de Santa Catarina MPSC. Ato Nº 519/PGJ/2009, de 01 de outubro de 2009. Institui a Política de Segurança Institucional e o Plano de Segurança Institucional e dá outras providências. Disponível em: https://www.mpsc.mp.br/atos-e-normas/detalhe?id=272. Acesso em: 16 out 2018.

_____. Ministério Público de Santa Catarina MPSC. Ato 591/PGJ/2015. Dispõe sobre o procedimento de proteção pessoal de membros e servidores do Ministério Público e seus familiares no âmbito do Ministério Público de Santa Catarina. Disponível em: <https://www.mpsc.mp.br/atos-e-normas/detalhe?id=1858>. Acesso em: 16 out 2018.

_____. POLÍCIA MILITAR DE SANTA CATARINA – PMSC. Plano estratégico. 2017. Disponível em: <http://www.pm.sc.gov.br/fmanager/pmsc/upload /master/PlanoEstrategico.pdf>. Acesso em 25 set 2018.

_____. Polícia Militar de Santa Catarina PMSC. Florianópolis, 2018. Apresenta um resumo da história da PMSC. Disponível em: <http://www.pm.sc.gov.br/institucional/historia>. Acesso em: 29 set. 2018.

_____. Polícia Militar de Santa Catarina PMSC. Portaria Nº 228/PMSC/2018. Aprova o regulamento do sistema de inteligência da Polícia Militar de Santa Catarina (SIPOM). **Diário Oficial [do] Estado de Santa Catarina**, Florianópolis, SC, 12 jul. 2018b. Disponível em: <https://www.jusbrasil.com.br/diarios/198949694/doesc-12-07-2018-pg-4?ref=next_button>. Acesso em 17 out. 2018.

_____. Polícia Militar de Santa Catarina PMSC. Portaria Nº 229/PMSC/2018. Institui a diretriz de inteligência da Polícia Militar de Santa Catarina. **Diário Oficial [do] Estado de Santa Catarina**, Florianópolis, SC, 12 jul. 2018c. Disponível em: <https://www.jusbrasil.com.br/diarios/198949694/doesc-12-07-2018-pg-4?ref=next_button>. Acesso em 17 out. 2018.

_____. Secretaria Estadual da Defesa Civil SDC. **Gestão de riscos de desastres**. Florianópolis: Secretaria Estadual da Defesa Civil, [201_].

_____. Tribunal de Justiça de Santa Catarina TJSC. Florianópolis, 2018. Trata do núcleo de segurança institucional do TJSC (NIS). Disponível em: <https://www.tjsc.jus.br/nucleo-de-inteligencia-e-seguranca-institucional>. Acesso em: 09 out 2018.

_____. Tribunal de Justiça de Santa Catarina TJSC. Resolução GP Nº 2, de 12 de janeiro de 2016. Institui o protocolo de segurança a ser adotado nos casos de magistrados ou de servidores colocados em situação de risco... Disponível em: <https://www.tjsc.jus.br/documentacao>. Acesso em: 09 out 2018.

_____. Tribunal de Justiça de Santa Catarina TJSC. Resolução GP Nº 10 de março de 2018. Cria o Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça de Santa Catarina. Disponível em: < https://www.tjsc.jus.br/nucleo-de-inteligencia-e-seguranca-institucional>. Acesso em: 11 out 2018.

SILVA, Adilson Luiz da. Inteligência de Segurança Pública. 2018. Notas de aula.

SILVEIRA, José Luiz Gonçalves da et al. **Inteligência de segurança pública:** um novo paradigma à proteção do cidadão. Florianópolis: Polícia Militar de Santa Catarina; Imprensa Oficial do Estado de Santa Catarina, 2012.

TEZA, Marlon Jorge. **A Polícia Militar na assembleia nacional constituinte capítulo da segurança pública**. In: _____. Temas de Polícia Militar: novas atitudes da polícia ostensiva na ordem pública. Florianópolis: Darwin, 2011, pp. 96-114.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL - UFRGS (BRASIL). **Capacitação em gestão de riscos**. Centro Universitário de Estudos e Pesquisas sobre Desastres. – 2ed. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2016.

APÊNDICE A – Questionário

Srs. Chefes de AI, o Major PM Ricardo Ribeiro está realizando pesquisa sobre sistema de gestão de riscos para policiais militares ameaçados no âmbito da PMSC, sob a orientação do Prof. Dr. Maurício Custódio Serafim e do Coronel PM Adilson Luiz da Silva, realizada para coletar dados para produção de trabalho monográfico, requisito para formação no Curso de Altos Estudos Estratégicos (CAEE/2018), Curso de Pós-Graduação Lato Sensu, “Especialização em Gestão Pública: Estudos Estratégicos no Corpo de Bombeiros Militar de Santa Catarina”.

Considerando que a Agência Central de Inteligência (ACI) tem interesse na pesquisa, pois, está em desenvolvimento um protocolo de gestão de risco para policiais militares na Corporação, solicito que seja preenchido o questionário abaixo até dia 04/10/2018.

Para fins dessa pesquisa, devem ser consideradas apenas as informações dos últimos 12 (doze) meses, sendo que a coleta de dados deve ser realizada apenas nos arquivos internos da seção.

1) Quantos policiais militares lotados na sua respectiva Unidade sofreram algum tipo de ameaça, explícita ou velada, direta ou indireta, nos últimos 12 (doze) meses (considerar toda área de circunscrição atual do Batalhão)?

_____ (número de policiais militares ameados nos últimos 12 (doze) meses na área da Unidade);

2) Caso não haja registro de sobre ameaças contra policiais militares na Unidade, informar:

[ ] A AI não mantém controle sobre ameaças contra policiais militares na Unidade;

[ ] A AI não tomou conhecimento sobre ameaças contra policiais militares no período em pesquisa.

3) Caso haja registros, informar quais das medidas abaixo foram adotadas pelo Comando da Unidade para evitar a concretização da ameaça ou proteger o(s) policial(is) militar(es) ameaçado(s):

[ ] Informação e orientação ao policial militar ameaçado;

[ ] Informação ao comandante direto do policial militar ameaçado;

[ ] Ações de inteligência para produzir conhecimento sobre a ameaça;

[ ] Realização de rondas na residência do policial militar ameaçado;

[ ] Alteração da função do policial militar ameaçado na OPM;

[ ] Entrega de arma ou colete balístico para policial militar da reserva remunerada;

[ ] Escolta ou segurança presencial para o policial ameaçado ou familiar;

[ ] Realização de operações policiais (barreira, varredura,...) específica para coibir criminosos ou organização criminosa envolvida na ameaça;

[ ] Encaminhamento de RELINT sobre os fatos à ACI.

[ ] Encaminhamento de relatório sobre a ameaça para Polícia Civil ou Ministério Público para que os fatos sejam investigados;

[ ] Transferência do policial militar para OPM em município diverso do local da ameaça;

[ ] Outros (especificar todas as demais medidas tomadas)

_____

ANEXO A – Termo de compromisso para integrantes do TJSC ameaçados

TERMO DE COMPROMISSO

(ANEXO I – Resolução GP n. 2 de 12 de janeiro de 2016)

Dados pessoais
Nome
Lotação atual
Endereço
Telefone/fax
Endereço residencial
Telefone(s)
Estado civil
Veículo(s) e placas
Tipo sanguíneo
Problema de saúde importante ( ) não ( ) sim qual?
Uso de remédio controlado ( ) não ( ) sim
Um nome e telefone para contato

Na presente data declaro ter conhecimento do teor da Resolução GP n. 2/2016 e tomo ciência da decisão do Conselho de Segurança Institucional (CSI) a respeito das medidas de assistência e/ou segurança pessoal que serão empregadas para garantir a minha integridade física. Por livre e espontânea vontade, assumo o compromisso de acatar as obrigações abaixo elencadas, sob pena de suspensão ou perda definitiva da proteção:

Obedecer às orientações e recomendações técnicas estabelecidas pela(s) equipe(s) de segurança durante o cumprimento da minha rotina pessoal;

Fornecer com antecedência e quando solicitado, ao CSI ou à(s) equipe(s) de segurança dados e rotinas da minha atuação profissional e, caso ainda necessário, dos meus familiares;

Comunicar imediatamente à(s) equipe(s) de segurança qualquer circunstância incomum ou alteração no ambiente que possa servir de indicativo de ameaça iminente;

Comunicar imediatamente ao CSI e à(s) equipe(s) de segurança qualquer mudança nas rotinas já informadas;

Comunicar imediatamente ao CSI alterações e/ou informações levadas a meu conhecimento sobre o caso sob investigação;

Comunicar ao CSI para que analise os compromissos pessoais e profissionais já assumidos que podem ir de encontro com o teor deste Termo;

Não frequentar bares, boates, restaurantes, hotéis, praças desportivas, espetáculos públicos, shopping centers ou qualquer outro local com aglomeração de pessoas;

Não comparecer a qualquer evento de natureza social que exponha a risco ou possa dificultar ou impedir a atuação da equipe de segurança pessoal;

Não divulgar à mídia ou concorrer para que sejam divulgadas informações a respeito das medidas de proteção em andamento, bem como imagens e rotinas da minha atuação profissional;

Não divulgar, de forma geral, inclusive a pessoas próximas, qualquer informação relacionada aos mecanismos e ferramentas de investigação e proteção aplicados, salvo se precedido de consulta e aprovação do CSI;

Não criar e/ou manter perfis atualizados e com disponibilidade pública de acesso a imagens e/ou dados pessoais em redes sociais na internet;

Evitar estender as atividades jurisdicionais no foro após o expediente forense;

Obedecer a outras recomendações que porventura sejam decididas no curso da assistência.

Cidade de , de de 201 .

_____

Assinatura

RECEBIDO EM:

DESPACHO

ANEXO B – Termo de dispensa de segurança pessoal do TJSC

TERMO DE DISPENSA DE SEGURANÇA PESSOAL

(ANEXO II – Resolução GP n. 2 de 12 de janeiro de 2016)

Na presente data, eu_____,
( ) magistrado ou servidor, submetido à proteção pessoal designada/sugerida pelo Conselho de Segurança Institucional (CSI), por livre e espontânea vontade e em conformidade com os termos da Resolução GP n. 2/2016, DISPENSO, formalmente, a assistência e/ou segurança pessoal/escolta colocada à minha disposição.

Cidade de_____,____ de_____ de 201__ .

_____

Assinatura

RECEBIDO EM: DESPACHO