GESTÃO DE RISCOS COMO LACUNA NAS OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

João Francisco Farinas e Silva[24]
Adriana Neves Gomes de Azevedo[25]
Renato Pires Moreira[26]

Resumo: O presente estudo tem por finalidade verificar a aplicabilidade da gestão de risco e as operações de inteligência de segurança pública. A metodologia baseou-se na pesquisa em fontes primárias e secundárias. Para tanto, foram realizados uma revisão bibliográfica referente à inteligência de segurança pública, operações de inteligência de segurança pública e gestão de riscos. A partir da observância da lacuna referente à gestão de riscos nas operações de inteligência, foi possível apresentar, com base na ISO 31000:2018 e *Committee of Sponsoring Organizations of the Treadway Commission*, a gestão de risco na execução das operações de inteligência. Por fim, elencou-se os possíveis benefícios da implementação da gestão de riscos nas operações de inteligência de segurança pública. A pesquisa ora apresentada visa contribuir com o aprimoramento das operações de inteligência de segurança pública, no que se refere a aplicação de normas e ferramentas que possam ser úteis ao seu desenvolvimento.

Palavras-chave: Segurança Pública. Atividade de inteligência. Inteligência de Segurança Pública. Operações de inteligência de Segurança Pública. Gestão de risco.

RISK MANAGEMENT AS A GAP IN PUBLIC SAFETY INTELLIGENCE OPERATIONS

Abstract: This study aims to verify the applicability of risk management and public security intelligence operations. The methodology was based on research from primary and secondary sources. To this end, a literature review was conducted regarding public security intelligence, public security intelligence operations and risk management. From the observance of the gap regarding risk management in intelligence operations, it was possible to present, based on ISO 31000:2018 and the Committee of Sponsoring Organizations of the Treadway Commission, the risk management in the execution of intelligence operations. Finally, the possible benefits of implementing risk management in public security intelligence operations were listed. The research presented here aims to contribute to the improvement of public security intelligence operations, with regard to the application of standards and tools that may be useful for their development.

Keywords: Public Security, Intelligence Activity, Public Security Intelligence, Public Security Intelligence Operations, Risk Management.

Recebido em 23 de junho de 2021	Aprovado em 09 de agosto de 2021

[24] Advogado concursado na Cemig. Especialização em Direito Tributário – FGV. Especialização em Inteligência de Segurança Pública pela Polícia Militar de Minas Gerais (PMMG).
http://lattes.cnpq.br/2355715189859936
http://lattes.cnpq.br/0769277596069483
E-mail: joaofarinas@gmail.com.

[25] Especialista em Direito Processual Civil - Faculdade Milton Campos, Especialista em Direito Tributário - CAD (Centro de Atualização em Direito - FGV), Especialista em Governança, Riscos, Compliance e Controle - CEDIN, MBA em Auditoria Interna e Práticas de Compliance.
https://orcid.org/0000-0002-3039-8131
http://lattes.cnpq.br/9557137649181664
E-mail: adrize_ng@yahoo.com.br.

[26] Mestrando no Programa de Pós-Graduação Gestão & Organização do Conhecimento (PPGGOC) da Escola de Ciência da Informação (ECI) da Universidade Federal de Minas Gerais (ECI/UFMG
https://orcid.org/0000-0002-5278-3460
https://orcid.org/0000-0002-4592-750X
E-mail: prof.renatopires@gmail.com.

1 INTRODUÇÃO

A inteligência de segurança pública vem sendo analisada diuturnamente por pesquisadores e acadêmicos. A partir do momento em que há uma série de ameaças e vulnerabilidades à segurança pública, torna-se viável uma discussão teórica capaz de suprir algumas lacunas atinentes às políticas públicas voltadas a essa atividade especializada.

Dentre algumas lacunas, cita-se a aplicação da gestão de riscos para as operações de inteligência de segurança pública no que tange às questões doutrinárias. A Doutrina Nacional de Inteligência de Segurança Pública (DNISP), apesar de descrever acerca da análise de riscos enquanto uma técnica acessória à produção do conhecimento de inteligência (BRASIL, 2015), não faz qualquer menção no aspecto da gestão de risco.

Operações de inteligência de segurança pública refere-se à obtenção de informações, dados e substratos fáticos de forma operacional, em que há profissionais designados e especializados nessa atividade, para cumprir a atividade de obtenção de dados e informações *in locu*, negados e/ou de difícil acesso.

Naturalmente, por tratar-se de atividade de risco e, no caso de possíveis falhas em sua execução, poderá ocasionar significativos prejuízos ao profissional de inteligência e à agência e inteligência. Assim, seria adequado uma análise e metodologia criteriosa dos riscos envolvidos para verificar a pertinência e viabilidade da operação a ser realizada.

Nesse sentido, o presente artigo tem como finalidade apresentar, sugestivamente, uma metodologia de gestão de risco aplicável às operações de inteligência de segurança pública no que tange à mitigação de riscos.

Como referencial teórico, foi utilizada a ISO 31000:18 e o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), normas referentes à gestão de risco, com vistas a compreender as metodologias de gestão de risco, atrelada à metodologia de produção do conhecimento aplicável à inteligência de segurança pública. A metodologia aqui apresentada firmou-se no modelo explicativo, analisando-se a gestão de risco e as operações de inteligência de segurança pública.

Trata-se de uma pesquisa descritiva baseada em fontes primárias e secundárias. Em que pese a relevância do tema em estudo para atingir os objetivos propostos, recorreu-se, também, a fontes extraoficiais em razão da atualidade do tema e da carência de dados oficiais pertinentes.

2 NOÇÕES DE OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

É inerente à atividade de inteligência de segurança pública a detecção de ameaças e vulnerabilidades, quanto à criminalidade, visto que essa tem evoluído para um nível de complexidade cada vez mais sofisticado (GOMES, 2018). Um dos objetivos da segurança pública é atuar na prevenção, de modo a mitigar os riscos a que a sociedade civil está exposta.

Diante de um cenário, cada vez mais volátil, incerto, complexo e ambíguo, torna-se imperioso o levantamento e análise, classificação e tratamento dos fatores de riscos, para que se empenhe recursos, pessoal e tempo adequado durante a realização das operações de inteligência de segurança pública. (GOMES, 2018).

Considerando-se os riscos aos quais as operações de inteligência de segurança pública estão expostas, a Gestão de Risco torna-se um instrumento imprescindível para respaldar e dar suporte à execução desta atividade, subsidiando com insumos informacionais à produção de conhecimento para fins de assessoramento do processo decisório.

No âmbito da segurança pública, a DNISP conceitua as operações de inteligência como o

conjunto de ações desta área destinadas à busca do dado negado e/ou disponível, de difícil acesso. Para realização dessa atividade especializada, há necessidade de se ter profissionais, métodos, técnicas e recursos especializados, haja vista a complexidade desse trabalho. (BRASIL, 2015).

Para os ramos da Inteligência de Segurança Pública (inteligência e contrainteligência) e das Operações de Inteligência de Segurança Pública, determina-se o intercâmbio de técnicas operacionais, desenvolvimento da doutrina de inteligência policial, desenvolvimento de qualificação da área operacional, bem como outras prioridades, de acordo com os incisos do Art. 3º do Decreto 9.489/2018.

O propósito de integrar a atividade de inteligência (inteligência e contrainteligência) e as operações de inteligência é otimizar o cumprimento da obtenção do dado negado, facilitar a assessoria nos mais variados níveis decisórios e potencializar, eficaz e eficientemente, as agências de inteligência (LIMA, 2010). Além deste reconhecimento em âmbito nacional e estadual, as operações de inteligência são o cerne da atividade de inteligência, vez que o emprego da técnica não necessariamente caracterizaria essa atividade, mas sim pelo emprego sigiloso, o que requer preparo e cuidado com os riscos envolvidos. (SOARES, 2015; GONÇALVES, 2018).

Quanto às buscas realizadas na obtenção dos dados pelas operações de inteligência, utilizam-se de dois tipos, sendo elas exploratórias ou sistemáticas. Exploratórias referem-se às "ações desenvolvidas para obter, em um curto intervalo de tempo, os dados indispensáveis à produção de conhecimento acerca de um fato ou situação, não se prolongando no tempo". As sistemáticas são as "ações que, em razão da necessidade de manter determinado alvo em constante acompanhamento, estende-se no tempo", requerendo mais preparo e planejamento para execução deste tipo de operação. (LIMA, 2010, p. 40).

A execução das operações de inteligência de segurança pública expõe os profissionais de inteligência que a executam a inúmeras situações de riscos que podem comprometer severamente a obtenção de dados, do executor da atividade e da própria agência de inteligência. É essencial que haja uma abordagem criteriosa quanto à metodologia e técnica propriamente dita, conjugada com uma concepção de trabalho em que se faça um procedimento que integre a eficiência, eficácia, gestão focada em resultado, com vistas à redução ao máximo de insucesso de alguns riscos de algum, aproximando-se, tal entendimento, da Gestão de Risco. (LIMA, 2010).

Nesse sentido, a atividade de inteligência de segurança pública deve ser bem estruturada para que a produção de conhecimento seja efetiva e eficaz, em especial, no que se refere às operações de inteligência. (GONÇALVES, 2018).

3 GESTÃO DE RISCO

A gestão de risco, nesse novo cenário, deve ser incorporada aos processos internos das operações de Inteligência de Segurança Pública, de modo a permitir a detecção das oportunidades e das fraquezas desses órgãos. O ponto de atenção deve estar voltado para o fato de que a sociedade está exposta a riscos cada vez mais complexos, sofisticados, interconectados e dinâmicos.

Nessa linha de raciocínio, conforme estabelece a ABNT NBR ISO 31000:2018, gestão de risco é aplicável a todas as organizações, para auxiliar a tomada de decisão, elaboração de estratégias e alcance de objetivos, aplicando-se prioritariamente à governança e liderança. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, p.

1). Segundo o COSO[27], a gestão de risco tem por finalidade desenvolver sistemas de controle interno eficazes e eficientes para as organizações, para adaptar os ambientes operacionais e negócios, mitigar riscos, apoiar as decisões que serão tomadas, bem como estruturar a governança, (BRASILIANO, 2018, p. 69). O foco principal desta norma é gerenciar os riscos contábeis (BRASILIANO, 2018, p. 66). No que tange o COSO *Enterprise Risk Management - integrated framework* (COSO-ERM)[28], versão mais atualizada, refere-se a um aprimoramento do COSO, melhorando o gerenciamento de riscos corporativos, propondo aplicações personalizadas a cada instituição e procura integrar ainda mais as áreas envolvidas com o risco. (BRASILIANO, 2018, p. 82).

Dessa feita, é necessário definir e compreender alguns conceitos tais como risco, fatores de risco, apetite ao risco, tolerância ao risco, dentre outros.

Risco, na perspectiva da ISO 31000:2018, é o efeito da incerteza nos objetivos, podem ser positivos, negativos ou ambos, aplicando-se em diferentes níveis e normalmente expresso em fatores de riscos, eventos potenciais, suas consequências e suas probabilidades. O COSO assevera que risco é "representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos", enquanto a "oportunidade é a possibilidade de que um evento ocorra e influencie favoravelmente a realização dos objetivos". (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2017, p. 16).

Fonte (fator) de risco é o elemento que tem o potencial para dar origem ao risco e o evento é a ocorrência ou mudança em um conjunto específico de circunstâncias. A consequência é o resultado de um evento que afeta os objetivos de uma organização. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, p. 2).

A diferença entre risco puro e risco especulativo está no fato de que o risco puro é aquele que envolve apenas a possibilidade de perda e o especulativo envolvendo chance de perda ou de ganho (BRASILIANO, 2018, p. 22).

O COSO ERM apresenta que o risco inerente é o risco que se apresenta a uma determinada organização na ausência total de qualquer medida gerencial que causasse alteração na probabilidade ou no impacto desse risco". (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2017, p. 16). Por outro lado, o risco residual é o "risco remanescente após a implementação de atividades de controle que visam reduzir sua probabilidade e/ou impacto". (BRASILIANO, 2018, p. 160).

Nesse sentido, cabe à administração considerar e avaliar o risco inerente, mas também, o risco residual. A avaliação de riscos deverá ser aplicada em primeiro lugar aos riscos inerentes, obedecendo um critério de criticidade. Após a aplicação de controles e das devidas respostas aos riscos residuais, a administração deverá considerar os riscos residuais. Por óbvio que o balizamento da aplicação de controle a um determinado risco se dá pelo apetite ao risco da organização.

O apetite de risco refere-se ao nível de riscos que uma instituição "dispõe-se a aceitar na busca de valor. O apetite de risco reflete a filosofia de gestão de riscos corporativos". (COMMITTEE OF SPONSORING ORGANIZATIONS OF

[27] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Trata-se de uma organização dedicada a ajudar outras instituições a melhorar o desempenho através do desenvolvimento de liderança inovadora que aprimora o controle interno, gestão de risco, governança e prevenção de fraudetivos. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary- Portuguese.pdf. Acesso em: 19 jul. 2021.

[28] A Estrutura define componentes essenciais de gerenciamento de risco corporativo, discute os principais princípios e conceitos dessa área, sugere uma linguagem comum de ERM e fornece uma direção e orientação claras para o gerenciamento de risco corporativo. https://www.coso.org/Pages/erm-integratedframework.aspx. Acesso em: 19 jul. 2021.

THE TREADWAY COMMISSION, 2017, p. 29), que deve estar alinhado com a tolerância ao risco para dar a resposta adequada ao risco". (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2017, p. 6). A tolerância ao risco, por seu turno, é o "desvio do nível do apetite ao risco", que será utilizado como alerta para evitar que a instituição "chegue ao nível estabelecido por sua capacidade". A capacidade de assumir riscos "será o nível máximo de risco que a organização pode suportar na perseguição aos seus objetivos". (BRASILIANO, 2018, p. 129), e, portanto, estará inserida no contexto de apetite de risco e tolerância ao risco.

As características e princípios que uma gestão de risco eficaz e eficiente deve possuir são: integração; estrutura e abrangente; personalizada; inclusiva; dinâmica; obter a melhor informação disponível; considerar os fatores humanos e culturais; e melhoria contínua. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 3-4), conforme explicado na ISO 31000:2018:

> a) Integrada. A gestão de riscos é parte integrante de todas as atividades organizacionais.
> b) Estruturada e abrangente. Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis.
> c) Personalizada. A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos.
> d) Inclusiva. O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.
> e) Dinâmica. Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.
> f) Melhor informação disponível. As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.
> g) Fatores humanos e culturais. O comportamento humano e a cultura influenciam significativamente todos os aspetos da gestão de riscos em cada nível e estágio.
> h) Melhoria contínua. A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 3).

A gestão de risco deve ser estruturada a fim de "apoiar a organização na integração de gestão de riscos em atividades significativas e funções", sendo calcada pela aplicação sequencial: da integração, concepção, implementação, avaliação e melhoria, tendo como difusor central a liderança e comprometimento. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 4).

A integração "apoia-se em uma compreensão das estruturas e do contexto organizacional"; a concepção, por sua vez, será o entendimento dos contextos externo e interno; a implementação será a efetiva estruturação aplicada da gestão de riscos; a avaliação será a análise da eficácia da estruturação da gestão de riscos; e, por fim, a melhoria que será o monitoramento e adaptação contínua para aprimorar a gestão de riscos aplicada até então (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 6-9).

O processo de gestão de risco é implementado pelo envolvimento da "aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do escopo, contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato dos riscos" (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 9).

A finalidade da comunicação e consulta "é auxiliar as partes interessadas pertinentes na

compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas" (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 10). É importante ressaltar que a comunicação e consulta ocorrem durante todas as etapas do framework apresentado pela ISO 31.000:2018.

A etapa do escopo, contexto e critérios tem o propósito de "personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado". Será necessária a definição do escopo das atividades de gestão de riscos, o entendimento dos contextos (externo e interno) no qual a instituição "procura definir e alcançar seus objetivos", e os critérios tais como quantidade e tipo de risco que a organização poderá assumir. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 10-11).

O processo de avaliação de riscos é o "processo global de identificação de riscos, análise de riscos e avaliação de riscos". Identificação de riscos serve para "encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos". Análise de riscos terá por finalidade a compreensão da natureza do risco e seu detalhamento, envolvendo as "incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia". Por fim, a avaliação de riscos servirá para apoiar as decisões, depois de realizadas as etapas anteriores. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 12-13).

O tratamento de riscos selecionará e implementará as opções para abordar os riscos, envolvendo um processo iterativo de: "formular e selecionar opções para tratamento do risco"; "planejar e implementar o tratamento de risco"; verificar a eficácia do tratamento; "decidir se o risco remanescente é aceitável"; se for aceitável, "realizar o tratamento adicional". (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 14).

O monitoramento e análise crítica deverão ser realizados durante todo o processo de gestão de riscos, com a finalidade de "assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo". (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 16).

O registro e relato tem por escopo que os resultados sejam relatados e documentados, visando fornecer subsídios para comunicar e melhorar a gestão de riscos, auxiliar a interação entre as partes envolvidas e a tomada de decisão. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 16).

4 GESTÃO DE RISCOS NAS OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Compreendidos os conceitos expostos, apresenta-se a metodologia da ISO 31.000:2018 de modo a aplicá-la às operações de inteligência de segurança pública. Cumpre esclarecer que o referido framework também é aplicável a outras técnicas e situações.

A gestão de risco procura implementar uma coordenação das atividades "para dirigir e controlar uma organização" quanto aos riscos estabelecidos nos parágrafos subsequentes para a execução desta operação. (ASSOCIAÇÃO BRASILEIRA DAS NORMAS TÉCNICAS, 2018, p. 1).

Atualmente, novas ameaças estão presentes nos mais variados ambientes, internos e/ou externos – tais como novas formas de operar o tráfico de drogas – as quais a segurança pública deverá oferecer respostas e, para que isso ocorra, estar munida do produto de inteligência, a fim de elaborar políticas de segurança pública mais eficazes e eficientes. (SILVA, 2016).

Para obter dados e informações com a finalidade de elaborar tal produto, caberá às operações de inteligência de segurança pública tal ofício. Frequentemente, essa necessita obter dados e/ou informações, negados e/ou de difícil acesso, de locais inóspitos nos quais podem ocorrer atividades criminosas.

A gestão de risco deverá ser aplicada nas operações exploratórias e sistemáticas, em todas as fases das operações de inteligência, ou seja, do planejamento das operações de inteligência, no estudo de situação e na elaboração e aprovação do plano de operações de inteligência. Entretanto, será no estudo de situação em que se deverá apresentar a gestão de risco, haja vista que neste estudo são "levantadas e analisadas as vantagens e desvantagens de cada linha de ação, sendo que, no final, o estudo culmina com uma proposta para o cumprimento da missão, que seja mais efetiva, menos arriscada, menos onerosa e menos invasiva". (FERRO, 2021, p. 97).

> O estudo de situação é uma análise dos fatores condicionantes da Operação de ISP, como a missão, o alvo, o ambiente onde será desenvolvida a operação, os recursos disponíveis, as ameaças, as oportunidades e outros, com vistas à elaboração de possíveis linhas de ação para o cumprimento da missão. (FERRO, 2021, p. 96).

Assim, é possível apresentar o processo de gestão de risco face à real necessidade da realização das operações de inteligência de segurança pública e, consequentemente, demonstrar os riscos e as fontes de riscos para a citada atividade especializada da atividade de inteligência.

Para a realização do processo de avaliação de riscos, será necessária a identificação dos riscos, sua análise e avaliação, competindo à etapa da Identificação "encontrar, reconhecer e descrever riscos que possam impedir" para que a operação seja realizada; à fase da análise caberá a compreensão da natureza e características dos riscos do reconhecimento operacional; e à avaliação competirá comparar os "resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional" da operação ora em estudo. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, p. 9-13).

De acordo com os termos e definições presentes na ISO 31000:2018, podem ser identificadas algumas fontes de risco falta de treinamento; terreno acidentado; sistemas de proteção audiovisual na localidade; ofendículos (GOMES, [S.d.]); falta de controle emocional; material impróprio para a operação; informação vazada sobre a operação; emboscada e armadilha. O Quadro 1 apresenta as descrições para cada fonte de risco.

Fonte de Risco	Descrição
FR1	Falta de treinamento
FR2	Terreno acidentado
FR3	Sistemas de proteção audiovisual na localidade
FR4	Ofendículos
FR5	Falta de controle emocional
FR6	Material impróprio para a operação
FR7	Informação vazada sobre a operação
FR8	Emboscada e armadilha

Quadro 1 – Fonte de Risco x Descrição
Fonte: Elaborado pelos autores, 2021.

Considerando as fontes de risco mencionadas no Quadro 1, se não tratadas devidamente, podem levar a concretização de vários riscos, tais como o risco de lesão e morte do agente, risco à imagem da instituição, comprometimento à implementação de políticas públicas, suspeitos e/ou criminosos saberem da operação, realização da operação em local errado, não obtenção de todas as informações do recrutado e, ainda, risco de captura do agente. O Quadro 2 resume a elaboração dos riscos a partir das fontes de risco.

Risco	Descrição	Origem
R1	Risco de morte do agente	FR1 + FR5 FR6
R2	Risco de lesionar o agente	FR2 + FR4 FR8 FR9
R3	Risco à imagem da instituição	FR8 + FR9
R4	Risco de comprometer a implementação de Políticas Públicas	FR6 FR8
R5	Risco dos suspeitos e/ou criminosos saberem da operação	FR7
R6	Risco de realizar a operação em local errado	FR1 + FR7 FR5
R7	Risco de não obter todas as informações do recrutado	FR1 + FR3 FR5
R8	Risco de captura do agente	FR1 FR2 FR3 FR4 FR5 FR6 FR7 FR8

Quadro 2 – Risco x Descrição x Origem
Fonte: Elaborado pelos autores, 2021.

Para classificação dos riscos, o R1 é de probabilidade muito baixa e altíssimo impacto. Entretanto, no caso de morte, isso causará impacto massivo; em relação ao R2, a probabilidade é média e o impacto baixo, pois lesionar-se é mais provável que a morte. Caso venha a ocorrer, a chance de prejudicar o andamento da operação é baixa; quanto ao R3, possui probabilidade média e altíssimo impacto. A concretização desse risco impactará negativamente a imagem da instituição; a ocorrência do R4 tem probabilidade muito baixa de se concretizar e seu impacto será médio, pois trata-se de operação de baixa complexidade e mesmo que haja insucesso, isso comprometerá apenas o alvo, mas não comprometerá significativamente a política pública, vez que há outros recursos e formas de implementação; já em relação ao R5, a probabilidade de ocorrência é muito baixa, mas de altíssimo impacto, vez que esse tipo de operação é sigilosa. Contudo, no caso de vazamento de informações, poderá haver um comprometimento da operação; o R6 possui probabilidade média de se concretizar e seu impacto, neste caso, será baixo, vez que a operação de inteligência tem por finalidade a obtenção de dados e informações tais como úteis. Portanto, a chance de ocorrer erro quanto a localização não é algo incomum. Contudo, mesmo que isso ocorra, não comprometerá tal atividade. O R7, por sua vez, possui probabilidade baixa e impacto alto. Realizada tal operação, os agentes são capazes de desvendar esconderijos e outros tipos de artimanhas. Mas, caso não obtenham todas as informações necessárias, a operação poderá sofrer prejuízo; por fim, o R8 apresentará baixa probabilidade e altíssimo impacto, caso venha se concretizar. É sabido que os agentes são preparados e planejam a execução de maneira apropriada, todavia, caso incorra em captura, a operação, o agente e a instituição serão severamente prejudicados.

Levando-se em consideração os riscos levantados, pode-se apresentar conforme a Matriz de Riscos de Probabilidade *versus* Impacto demonstrado no Quadro 3.

Nível de Risco			Impacto			
			1	2	3	4
			Muito baixo	Baixo	Médio	Alto
Probabilidade	1	Muito baixa		R4		R1; R5
	2	Baixa				R7; R8
	3	Média	R6	R2		R3
	4	Alta				

Quadro 3 – Matriz de Riscos de Probabilidade x Impacto
Fonte: Elaborado pelos autores, 2021.

Diante desse cenário, caberá à instituição estabelecer quais riscos está disposta a correr e implantar controles que possam mitigar os riscos críticos e/ou aqueles que ela não está disposta a correr. Nesse sentido, os tomadores de decisão, em relação à capacidade de assumir risco, poderão verificar o quanto efetivamente a instituição consegue suportar riscos para atingir o objetivo almejado no âmbito das operações de inteligência. Quanto à tolerância ao risco, esta deve ser evitada a todo o custo, visto que se trata do limite suportável antes que se atinja a capacidade total de se assumir um determinado risco (BRASILIANO, 2018, p. 129).

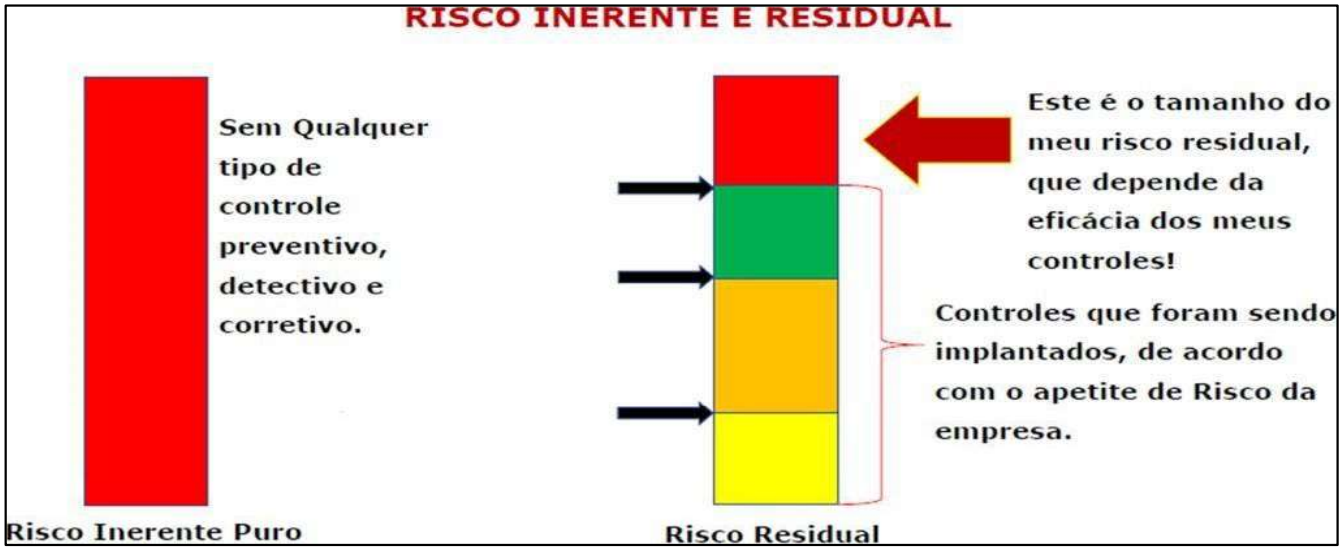

Figura 1 - Risco inerente e residual
Fonte: BRASILIANO (2018, p. 129)

O risco pode ser classificado em duas categorias. Risco inerente, ou seja, aquele risco que expõe um indivíduo ou organização sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou mitigar seu impacto. Por sua vez, o risco residual é o risco após a implementação de medidas de controle para o tratamento do risco. A figura 1 ilustra essa afirmação.

Riscos	Controle	Monitoramento
R1	Treinamento em nível operacional	A cada 6 meses
R2	Treinamento adequado; material adequado; e planejamento	A cada operação
R3	Planejamento adequado; e atuação das relações-públicas de modo efetivo	De modo permanente
R4	Atuação junto à sociedade para obter apoio; atuação junto às instituições públicas para obtenção de verbas suficientes para as operações; integração com outras áreas para a realização da referida operação.	De modo permanente
R5	Sigilo no planejamento e execução da operação	A cada operação
R6	Planejamento adequado	A cada operação
R7	Treinamento adequado; material adequado; e planejamento	A cada operação; e/ou a cada 6 meses
R8	Treinamento adequado; material adequado; e planejamento	A cada operação; e/ou a cada 6 meses

Quadro 4 – Controles aplicáveis para mitigar os riscos
Fonte: Elaborado pelos autores (2021).

Por fim, haverá o registro e o relato dos resultados obtidos pela aplicação deste procedimento à operação, procurando-se melhorar continuamente a sua execução. Encerrado o ciclo do processo de gestão de riscos, ele se repetirá e será atualizado permanentemente, ou seja, requer monitoramento contínuo.

Assim, os benefícios da aplicação da gestão de riscos nas operações de inteligência de segurança pública são fundamentais, haja vista que os tomadores de decisão poderão basear-se na análise dos riscos para melhorar o empenho de recursos materiais e humanos, tornando a atividade mais eficiente e eficaz.

5 CONSIDERAÇÕES FINAIS

As instituições de segurança pública, ao desempenhar suas funções, encontra-se exposta a riscos que podem comprometer seus objetivos estratégicos, principalmente, no que se refere ao enfrentamento à criminalidade. A inteligência de segurança pública, por intermédio do emprego das operações de inteligência de segurança pública, realiza ações com o emprego de técnicas especializadas com vistas à prevenção e repressão da criminalidade.

Para que a segurança pública possa neutralizar as ameaças decorrentes dessa nova realidade, será necessário municiar-se de dados e informações para empenhar recursos e pessoal no combate às organizações criminosas e a delitos, bem como para propor políticas de segurança pública. Para tanto, a produção de conhecimento deverá ser realizada de maneira criteriosa, identificando, avaliando e dando tratamento aos riscos que envolvem as operações de inteligência de segurança pública, para obtenção de dados e informações, bem como produto de inteligência, ou seja, o risco como conhecimento.

A identificação, avaliação e tratamento do risco são possíveis com a implementação do framework apresentado pela ISO 31000:2018 e COSO, que estabelecem procedimentos e ferramentas para essa atividade, auxiliando na elaboração das operações de inteligência de segurança pública e mitigação de riscos.

As operações de inteligência de segurança pública só atingirão seus objetivos estratégicos e operacionais, no que concerne, principalmente, na busca de dados e informações, se aplicar corretamente a gestão de riscos ao estruturar suas atividades. O levantamento dos riscos e o tratamento adequado aos seus fatores de riscos propiciará uma prestação do serviço de segurança pública maior eficiência e eficácia, visto que será possível a mitigação dos riscos que assolam seus agentes e a sociedade atual.

Diante do exposto, o presente artigo não tem a pretensão de exaurir o tema. Entretanto, conhecer, em linhas gerais, os benefícios decorrentes da aplicação da gestão de riscos nas operações de inteligência de segurança pública propiciam, certamente, maior eficiência e eficácia (produtividade; infalibilidade) com a finalidade de aprimorar esse setor de inteligência. É, portanto, notório que a gestão de riscos é imprescindível para subsidiar as decisões quanto ao combate à criminalidade e à implementação de políticas públicas de segurança pública, podendo servir para as polícias (e suas respectivas inteligências) e de práxis para a atividade de inteligência de segurança pública no Brasil.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000/2009**: gestão de riscos – princípios e diretrizes. Rio de Janeiro: ABNT, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 10 jul. 2019.

BRASIL. **Decreto nº 9.489, de 30 de agosto de 2018**. Regulamenta, no âmbito da União, a Lei nº 13.675, de 11 de junho de 2018, para estabelecer normas, estrutura e procedimentos para a execução da Política Nacional de Segurança Pública e Defesa Social. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9489.htm. Acesso em: 10 jun. 2019.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Doutrina nacional e inteligência de segurança pública**. 4. ed., rev. e atual. Brasília: Ministério da Justiça, 2015.

BRASILIANO Antônio Celso Ribeiro, **Inteligência em riscos**: gestão integrada em riscos corporativos. 2. ed. rev. Atual. São Paulo: Sicurezza, 2016.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Gerenciamento de riscos corporativos**: estrutura integrada. 2017. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary- Portuguese.pdf. Acesso em: 19 jul. 2021.

FERRO, Alexandre Lima. **Os direitos humanos como limites das operações de inteligência de segurança pública**. Brasília. Última Ratio, 2021.

GOMES, Luiz Flávio. O que são ofendículos? - Leandro Vilela Brambilla. **JusBrasil**, notícias. Disponível em: https://lfg.jusbrasil.com.br/noticias/2044230/o-que-sao-ofendiculos- leandro-vilela-brambilla. Acesso em: 15 set. 2019.

GOMES, Cleiton Ricardo Soares. Ameaça Assimétrica na Segurança Pública: Lições de Guerra Irregular para Inteligência de Operações Especiais. In: HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires (Orgs.). **Inteligência de segurança pública e cenários prospectivos da criminalidade**. Belo Horizonte. D'Plácido, 2018. Série Inteligência, Estratégia e Defesa Social.

GONÇALVES, Jonisval Brito. **Atividade de inteligência e legislação correlata**. 6.ed. Niterói, RJ. Impetus, 2018.

LIMA, Rinaldo de Azevedo. **A execução de despesa de caráter sigiloso no âmbito do sistema de inteligência da Polícia Militar de Minas Gerais**. 2010. Monografia (Especialização) – Academia de Polícia Militar de Minas Gerais, Fundação João Pinheiro, Belo Horizonte, 2010.

SILVA, Wilson. Os mais bizarros métodos usados para o tráfico de drogas: com submarinos e donuts cobertos com cocaína, os narcotraficantes abusam da criatividade para contrabandear seus produtos pela

América Latina. **Veja**, São Paulo, 28 ago. 2016. Disponível em: https://veja.abril.com.br/mundo/os-mais-bizarros-metodos-usados-para-o-trafico-de-drogas/. Acesso em: 10 ago. 2019.

SOARES, André. **Serviços secretos**: aspectos do emprego das operações sigilosas no estado democrático de direito. 3. ed. Washington: Amazon Digital Services LLC, 2015.